



Delinea

Privilege Manager

Documentation © 10.8.x



Table of Contents

Introduction to Privilege Manager	37
What's New in Privilege Manager 10.8	37
Feature Overview	38
Active Directory and Azure Active Directory	38
Agent & OS Reports	38
Application Discovery for Administrative or Root Privileges	38
Automated Local Account Password Rotation	38
Centralized Application & Execution Event Logging	38
Child Process Control	38
Custom & Scheduled Reports	38
Define Local Group Membership	38
End-user Justification & Admin Approval Workflow	38
Flexible Policy Deployment Configuration	38
High Availability & Load Balancing	38
Local Admin Rights Removal	38
Local User Account Management	38
Local User & Group Activity Auditing	38
Privilege Manager Mobile App	38
Real-time Application Analysis Reputation Check	38
Responsive & Actionable Reporting Dashboard	38
Reverse Proxy	38
Sandboxing	39
ServiceNow	39
Symantec Enterprise Platform (SEP)	39
SysLog / SIEM	39
System Center Configuration Manager (SCCM)	39
Tailored Block, Elevation, Justification, and Monitoring Policies	39
User Account Control (UAC) Override	39
Windows & Mac Account Discovery on Endpoints	39
Least Privilege Explained	40
10.8 User Interface Introduction	41
Glossary	42
Privilege Manager Reference Architecture Diagrams	44
Component Definition	44
Single Site with Minimum HA	44
<i>Overview</i>	44

<i>Requirements</i>	44
<i>Virtual IP/Virtual Computer Object Requirements</i>	44
<i>Diagram</i>	44
Single Side Minimum HA (Reverse Proxy/Azure Bus)	45
<i>Overview</i>	45
<i>Requirements</i>	45
<i>Virtual IP/Virtual Computer Object Requirements</i>	45
<i>Diagram</i>	46
Multi Site Minimum HA/DR - Lower Cost/Manual Failover	47
<i>Overview</i>	47
<i>Requirements</i>	47
<i>Virtual IP/Virtual Computer Object Requirements</i>	47
<i>Diagram</i>	47
Multi Site Average HA/DR - Average Cost/Manual Failover	48
<i>Overview</i>	48
<i>Requirements</i>	49
<i>Virtual IP/Virtual Computer Object Requirements</i>	49
<i>Diagram</i>	49
Best HA/DR - Highest Cost/Manual Failover	50
<i>Overview</i>	50
<i>Requirements</i>	51
<i>Virtual IP/Virtual Computer Object Requirements</i>	51
<i>Diagram</i>	51
Integration with Secret Server	53
Single Site with Minimum HA	53
<i>Overview</i>	53
<i>Requirements</i>	53
<i>Diagram</i>	53
Single Site with Minimum HA and Separate RabbitMQ	54
<i>Overview</i>	54
<i>Requirements</i>	54
<i>Diagram</i>	54
Multiple Site with Manual Failover	55
<i>Overview</i>	55
<i>Requirements</i>	55
<i>Diagram</i>	56
Multiple Site with Manual Failover and Separate RabbitMQ	56
<i>Overview</i>	56
<i>Requirements</i>	57
<i>Diagram</i>	57

Multiple Site with Automatic Failover	58
<i>Overview</i>	58
<i>Requirements</i>	59
<i>Diagram</i>	59
Multiple Site with Automatic Failover and Separate RabbitMQ	60
<i>Overview</i>	60
<i>Requirements</i>	61
<i>Diagram</i>	61
Best Multiple Site with Automatic Failover and Separate RabbitMQ	62
<i>Overview</i>	62
<i>Requirements</i>	62
<i>Diagram</i>	62
Platforms	64
Privilege Manager on macOS	65
<i>Best Practices Preference Panes</i>	66
<i>Best Practices System Preferences</i>	67
Error Behavior of Preference Panes	67
User Based Behavior of Preference Panes	67
<i>Standard User</i>	67
<i>Admin User</i>	67
<i>Best Practices Printer Installs</i>	68
<i>Date & Time Preference Pane</i>	69
Standard User - System Defaults	69
Standard User - Managed by Policy	69
Local Administrator User - Not Managed by a Policy	69
<i>Energy Saver Preference Pane</i>	70
Standard User - System Defaults	70
Standard User - Managed by Policy	70
Local Administrator User - Not Managed by a Policy	70
<i>Network Preference Pane</i>	71
Standard User - System Defaults	71
Standard User - Managed by Policy	71
Local Administrator User - Not Managed by a Policy	71
<i>Preference Pane macOS</i>	72
Targeting Preference Panes	72
Catalina Preference Pane Behavior	72
macOS Extensions	73
<i>Kernel Extension (KEXT) vs. System Extension (SYSEX)</i>	73
<i>Leveraging the AuthorizationDB</i>	73
<i>Using a Privacy Preference Policy Control Configuration Profile Payload</i>	73

<i>Legacy Extensions (KEXT)</i>	73
Effect on Privilege Manager Customers by Apple Deprecating Kernel Extensions in macOS	73
How is this Going to Affect Privilege Manager?	73
Catalina KEXT Warning	73
<i>System Extensions (SYSEX)</i>	74
Catalina	74
Big Sur	75
macOS File/Folder Access	78
<i>Workaround via MDM Solution</i>	78
macOS Secure Token	79
<i>Agent Configuration</i>	79
macOS Privilege Manager Sudo Plugin	81
<i>Sudo Plugin Installation</i>	81
Privilege Manager on Windows	82
Client System Settings	83
<i>Add Devices</i>	83
<i>Add Printers</i>	83
<i>Backup the Systems</i>	83
<i>Change the Date and Time</i>	83
<i>Change Network Adapter Settings</i>	83
<i>Defragment the Disk</i>	83
<i>Install Language Packs</i>	83
<i>Monitor Performance</i>	83
The Privilege Manager UI	84
Gauges	84
<i>What is a Gauge?</i>	84
Reports and Gauges Available	84
Navigation and Controls	85
<i>Search, Notification, Help, User Menus</i>	85
<i>Pin to Navigation Tree</i>	85
<i>Table Grid Contents</i>	86
<i>Switches</i>	86
<i>Main Menu</i>	86
Chevrons	87
<i>Computer Groups</i>	87
<i>Admin Menu</i>	87
Notifications	88
Alerts	89
<i>Endpoint Specific Alerts</i>	89
Manage Approvals	90

Getting Started Overview - On-premises	91
Preliminary Configuration	91
Rollout Recommendation	91
Local Security	91
Application Control	91
Integrations	91
Reports & Troubleshooting	91
Catalogs & Reference Guides	91
Getting Started Overview - Cloud	92
<i>Cloud Specific vs. On-prem</i>	92
<i>Rollout Recommendation</i>	92
<i>Local Security</i>	92
<i>Application Control</i>	92
<i>Integrations</i>	92
<i>Reports & Troubleshooting</i>	92
<i>Catalogs & Reference Guides</i>	92
Cloud Quickstart Guide	93
<i>Initial Setup</i>	93
<i>Getting Started Screen</i>	95
Privilege Manager Cloud Login	97
Initial Login	98
Getting Started Banner	98
Home	99
Licensing	100
Cloud Licenses	100
Installing New Licenses - On-premises Only	100
<i>Steps for Standalone Privilege Manager Installation</i>	100
<i>Steps for Combined Secret Server + Privilege Manager Installation</i>	100
Converting from Trial Licenses	101
Expired Licenses	101
Client vs. Server Licenses	101
<i>License Expired or Exceeded License Count</i>	101
10.7 and up Reset Licensing	101
Installation and Upgrades	102
Privilege Manager System Requirements	103
Minimum Requirements	103
Recommended Requirements	103
Client Requirements	103
Details	103
Ports/Agent Access Information	103

Anti Virus Exclusions	104
Directories	104
Exclusions for Web Server	104
<i>Temporary ASP.NET Files</i>	104
Exclusions for Database Server	104
<i>SQL Server Data Files</i>	104
<i>SQL Server Backup Files</i>	104
<i>SQL profiler trace files</i>	104
Exclusions for Managed Endpoints	104
<i>Request Run As Administrator Registry Key</i>	104
<i>Client Item Database</i>	104
<i>Privilege Manager Application Control Agent Service</i>	104
Software Downloads	105
Server Software	105
Agent Software	105
<i>Windows Endpoints</i>	105
<i>macOS Endpoints</i>	105
Product Installation - Basic	106
<i>Prerequisites</i>	106
ASP.NET Website	106
SQL Server Database	106
Administrative Access	106
Additional Recommendations	106
<i>Download the Latest Version of PM Installer</i>	106
<i>Running the Installer</i>	106
<i>Installing Connectors or the API</i>	110
Manual Installation	111
<i>Download Privilege Manager Application Files</i>	111
Zip File Extraction Tool	111
<i>Manual Installation (no setup.exe)</i>	111
Installing as a Virtual Directory	111
Integrated Security=False	112
Integrated Security=True	112
<i>Continue: Installing as a Virtual Directory</i>	112
Installing as a Website	115
<i>Completing Privilege Manager Installation from Website</i>	115
Item Encryption	116
<i>What this means for Privilege Manager</i>	116
Agent Installation	117
Agent Install Codes	118

<i>Using the SetAMSServer.ps1 Script</i>	118
Agent System Requirements	119
<i>Supported Windows Operating Systems (both 32- and 64-bit):</i>	119
<i>MacOS Agent</i>	119
<i>Directory Services Agent</i>	119
<i>Windows Management Framework download locations</i>	119
Windows Management Framework 2.0 or newer	119
.NET 4.0 Framework or newer	119
.NET 2.0 Framework SP1	119
<i>Ports/Agent Access Information</i>	119
Bundled Install	120
<i>Rollout to Multiple Systems</i>	120
<i>Silent Install</i>	120
Windows Agents	121
<i>Individual Agent Installers for Privilege Manager</i>	121
Hardened Agents	121
64-bit Windows Operating Systems	121
<i>Installation Command Lines</i>	121
32-bit Windows Operating Systems	121
<i>Installation Command Lines</i>	121
Directory Services Agent (AD)	122
<i>Prerequisites</i>	122
<i>Directory Services Agent Installation</i>	122
macOS Agents	124
<i>Installing macOS Agents</i>	124
Directly	124
<i>Unsupported Version Messages</i>	124
Using an Unattended Install Method	125
<i>Network File Share</i>	125
<i>Distribution Tool</i>	125
<i>After Initial Deployment</i>	126
<i>Uninstalling an Agent</i>	126
Bundled Core and Directory Services Agents	127
<i>Installing the Thycotic Directory Services Installer Bundle</i>	127
Agent Uninstall via Command Line	128
<i>Manual Uninstall Steps</i>	128
Upgrades	129
<i>What's New in Privilege Manager 10.8</i>	129
<i>Setting up the NuGet Source</i>	129
<i>Updating Privilege Manager</i>	129

Primary Node	129
Secondary Nodes	131
Offline Upgrades	132
Offline Upgrades - Combined	133
Upgrading from Arellia Management Server 8.2 to Privilege Manager 10.4 and up	134
<i>Automatic Steps</i>	134
<i>Manual Steps</i>	134
Best Practices for Upgrades	135
<i>DB Backup</i>	135
<i>TMS Folder Backup</i>	135
<i>Repair Solution</i>	135
Privilege Manager Agents	136
Agent Hardening (Windows)	136
Post Agent Installation	136
<i>Agent Diagnostics</i>	136
Agent Encryption	137
Elevated Processes	137
Pertaining to All Agents	139
Setting the Privilege Manager Server Address	140
<i>Setting the Privilege Manager Server (TMS) Address via PowerShell</i>	140
<i>Changing the Privilege Manager Server (TMS) Address via the Registry Editor</i>	140
VM Deployments	141
<i>Identifying Agents to The Console</i>	141
Persistent VMs	141
Dynamic VMs	141
Multiple VMs Collapsed to a Single Resource	141
<i>Pool of Values to Support Multiple VMs</i>	141
<i>Managing Agent Trust and Certificates</i>	141
<i>Minimizing Time Between VDI Deployment and Policy Enforcement</i>	141
<i>Licensing Concerns with Windows 10 Amazon Workspaces</i>	142
Connecting Agents to the Privilege Manager Server via Group Policy	143
<i>Un-Installing Old Templates</i>	144
Agent Trust Revocation	145
<i>Revoking the Trust from the Server</i>	145
<i>Revoking the Trust for the Computer Resource</i>	145
Agent Uninstall Script	146
<i>Using a PowerShell Script to Uninstall an Agent</i>	146
How to prevent Backwards Compatibility for Agents v10.4 and earlier	147
<i>Resolve</i>	147
Configuring for a Test Environment	148

Agent Specific Tasks	149
<i>Windows Remote Client Scheduled Commands</i>	149
<i>MacOS Remote Client Scheduled Commands</i>	149
Agents on Windows Systems	150
Windows Agent Utility	151
<i>Status Button</i>	151
<i>Register Button</i>	151
<i>Update Button</i>	151
<i>View Cache Button</i>	151
<i>View Logs</i>	152
<i>Export Logs Button</i>	152
<i>Agents Troubleshooting</i>	153
<i>Agent updateclientitems.ps1 Error</i>	154
<i>Agent Registration Issue</i>	155
Detailed Information	155
<i>Using a PowerShell Script</i>	155
<i>Client Item List Downloads</i>	157
Resolve	157
<i>Advanced Messages not Working for Child Processes of Microsoft Edge</i>	158
Detailed Information	158
Workaround	158
<i>Endpoint Issues</i>	159
Policy Troubleshooting	159
<i>Policies Not Getting Updated</i>	159
<i>Specific Files or Applications Not Being Elevated or Blocked</i>	159
Pre-10.7.1 Agent Hardening	160
<i>Editing the Agent Service Start / Stop Control (Windows) Policy</i>	160
<i>Restore Default Agent Permissions</i>	160
Agent Hardening 10.7.1 and up	163
<i>Editing the Restrict Account Permissions on Agent Services (Windows) Policy</i>	163
Agents on macOS Systems	165
MacOS Agent Utility Preference Pane	166
<i>Accessing the Agent Utility</i>	166
<i>General Tab</i>	166
Registering/Modifying an Agent	167
<i>Client Items Tab</i>	168
Modify Update Agent Commands (MacOS) Policy	170
Terminal Commands	171
<i>Command Usage</i>	171
Finding Logs for Troubleshooting	172

Using an MDM Profile for your Agent	173
SYSEX	173
SYSEX Allow Info	173
SYSEX PPC Profile Info	173
KEXT	173
KEXT Allow Info	173
KEXT PPC Profile Info	173
<i>Troubleshooting on macOS Endpoints</i>	175
<i>How to Recover an Unresponsive macOS Endpoint</i>	176
<i>Catalina FileSystemWatcher Issue</i>	177
Privilege Manager Administration	178
Actions	179
<i>Creating a New Action Manually</i>	179
Windows Specific Actions	181
Adjust Process Rights Action	182
Adjust Process Rights Action Settings Explained	182
<i>What is a Restricted SID?</i>	182
<i>When to use restricted ID</i>	182
<i>Using Apply Restricted SID</i>	182
<i>How to Add Windows Permissions</i>	182
<i>How to Use Well-known Accounts</i>	182
<i>Example Scenario</i>	183
Additional Options Explained	183
<i>Enabling Unrestricted Token Use</i>	183
Adjust Process Right for Resource Monitor	183
<i>Related Item - Policy</i>	183
ActiveX Installer Action	185
Parameters	185
Application Classification Action	186
Apply Application Compatibility Fix Action	187
Parameters	187
Deny File Access Action	188
Parameters	188
Deny Files Read and Write Access Message	188
Deny Windows Hooking Action	189
Windows Hooking Message	189
Encrypt Application Files Action	190
Parameters	190
Endpoint Group Member Approval Action	191
Related Topics	192

<i>Execute Application Action</i>	193
Parameters	193
<i>Group Member Approval Action</i>	194
<i>Sandbox Action</i>	195
Parameter	195
<i>Set Environment Variable Action</i>	196
Parameters	196
<i>Set Process Security Descriptor Action</i>	197
Parameters	197
<i>macOS Specific Actions</i>	198
<i>Allow Copy Action (MacOS)</i>	199
Parameters	199
<i>Display Advanced User Message Action (MacOS)</i>	200
Parameters	200
<i>Just-in-Time Group Membership Action</i>	201
<i>Message Actions</i>	202
Basic vs. Advanced Messages	202
Types of Advanced Message Actions	202
<i>Advanced Feedback Messages</i>	202
<i>Authentication Justification Message Action</i>	202
<i>Group Member Authenticated Message Action</i>	202
<i>Justify Application Elevation Action</i>	202
<i>Justify Application Message Action</i>	203
<i>Approval Request Messages</i>	203
<i>Approval Request Form Action</i>	203
<i>Approval Request (with Offline Fallback) Form Action</i>	203
<i>No Required Input Messages</i>	204
<i>Application Denied Message Action</i>	204
<i>Application Denied Notification Action</i>	204
<i>Application Warning Message Action</i>	204
Types of Basic Messages	205
<i>Deny Execute Message</i>	205
<i>Deny Files Read and Write Access Message</i>	205
<i>Windows Hooking Message</i>	205
<i>Limit Process Rights for New Applications Message</i>	205
<i>Remove Rights Message</i>	205
<i>Quarantine Message</i>	205
<i>Deny Execute Action</i>	206
Deny Execute Message	206
<i>Deny Execute Message</i>	207

Customization	207
<i>Display Advanced Message Action</i>	209
Parameters	209
Examples	209
<i>Display User Message Action</i>	210
Parameters	210
Examples	210
<i>Create Custom Notifications</i>	211
Enable View as XML	211
Customizing the Application Denied Notification Action	211
Editing the Text in the UI	212
Editing the Text via XML	213
Updating the Policy with the new Action	213
Action Message Localization	215
<i>Example for Spanish</i>	215
List of Default Actions	216
<i>Actions Catalog</i>	216
macOS	216
Windows	216
Configuration Feeds	218
Exclude File Extensions during File Hashing	219
<i>Create File Exclusion through Config Feed</i>	219
<i>Manually Test on Endpoint</i>	220
Ignoring macOS Updates	221
<i>Configuration Feeds</i>	221
<i>Enabling the Policies</i>	221
<i>Resetting the Policy</i>	221
<i>Scheduling</i>	221
Configuration	223
<i>Advanced Tab</i>	224
<i>File Inventory Solution</i>	225
<i>Monitor Settings</i>	226
Monitor Worker Role	226
Ping Interval	226
Base Local Address	226
Timeout	226
<i>Privilege Manager Application Programming Interface</i>	227
<i>General System Settings</i>	228
Save Performance Counters	228
Load On Demand Flags	228

Session Timeout	228
<i>Session Timeout Warning</i>	228
Allow Agent Certificate Mismatch	228
Maximum Application Event Count	228
Prevent Legacy Agent Registration (10.4 and older)	228
Max Time Skew	228
Inactivity Timeout	228
Encryption Provider	228
Command Timeout	228
System Secret Vault	228
Password Complexity for Standard Users	228
Validate Agent Event Signatures	229
<i>ServiceBus Settings</i>	230
Connectivity Mode	230
<i>Proxy Settings</i>	231
Proxy Server	231
Proxy Server Credential	231
Port	231
Use Proxy Server	231
<i>Privilege Manager Solution</i>	232
<i>Authentication Tab</i>	233
<i>Credentials Tab</i>	234
<i>User Credentials and Roles</i>	235
Create User during Installation	235
<i>Discovery Tab</i>	236
<i>Foreign Systems</i>	237
Foreign Systems Tab	237
Integrations	237
<i>Thycotic Foreign Systems</i>	237
<i>AD Integration</i>	237
<i>Third-Party Foreign Systems Integration</i>	237
Thycotic Products Integrations	238
Setting up Integration between Privilege Manager and Secret Server	239
<i>Verify Web Services are Enabled in Secret Server</i>	239
<i>Setup Authentication Data in Privilege Manager</i>	239
<i>Configure Privilege Manager Credential Vault (optional)</i>	240
<i>Password Migration</i>	240
<i>Important Notes</i>	241
<i>Templates</i>	241
Integration between Privilege Manager and Privileged Behavior Analytics	242

<i>PBA System Settings Details</i>	242
<i>Setting Up PBA Integration on Privilege Manager</i>	242
<i>Downloading and Installing the PBA Config Feed</i>	242
<i>Setting up the PBA SysLog Foreign System</i>	242
<i>Using the PBA Send Tasks</i>	243
<i>Enable Send Application Events to PBA</i>	244
Active Directory Integration	246
Active Directory Synchronization	247
<i>Set-up AD Default User Credential</i>	247
<i>Setup Foreign Systems</i>	247
<i>Viewing Imported Users and Groups</i>	250
Setting Up Azure Active Directory Integration in Privilege Manager	251
<i>Prerequisites</i>	251
<i>Setting up Azure AD with Privilege Manager</i>	251
<i>Steps in the Azure Portal</i>	251
<i>Steps in your Privilege Manager Instance</i>	254
<i>Set-up Foreign Systems</i>	254
<i>Viewing Imported Users and Groups</i>	255
<i>Import Users and Groups via Privilege Manager Task</i>	256
<i>Create Scheduled Task for Users/Groups Synchronization</i>	257
Third-Party Foreign Systems Integration	258
Set-up Cylance Integration	259
<i>Cylance Connector Installation Steps (On-prem only)</i>	259
<i>Configuring the Cylance Connector</i>	259
<i>Create a Cylance Security Rating Filter</i>	260
<i>Create a Cylance Policy</i>	261
Set-up Microsoft System Center Configuration Manager (SCCM) Integration	262
<i>Create a Credential</i>	262
<i>Connecting to SCCM</i>	262
<i>Import Computers</i>	262
<i>Verify the Computers have been Imported (optional)</i>	263
<i>Create a Collection</i>	263
<i>Inventory Software Packages</i>	264
<i>Create a SCCM Package Content Filter</i>	264
Set-up ServiceNow Integration	266
<i>Foreign System Configuration</i>	266
<i>ServiceNow Steps</i>	267
<i>Define Policy and Actions</i>	267
<i>Using an Approval Request (with ServiceNow Request ItemNumber) Form Action</i>	268
<i>Using an Endpoint Group Member Authenticated Message Action</i>	269

<i>Integration Workflow</i>	271
<i>Create Approval Request Items Task</i>	271
<i>How to create ServiceNow Approval Request Items Task</i>	271
<i>Variables</i>	271
<i>CreateExecuteAppApprovalRequest</i>	271
<i>Script Input</i>	272
<i>Script Output</i>	272
<i>GetExecuteAppApprovalRequestStatus</i>	272
<i>Script Input</i>	272
<i>Script Output</i>	272
<i>CancelExecuteAppApprovalRequest</i>	272
<i>Inputs</i>	272
<i>Outputs</i>	272
<i>Required Integration Points</i>	272
<i>What Can Change vs. What Must Remain</i>	272
Set-up Symantec Management Platform (SMP) Integration	273
<i>Create a Credential</i>	273
<i>Connecting to SMP</i>	273
<i>Import Computers</i>	273
<i>Verify the Computers have been Imported (optional)</i>	274
<i>Create a Collection</i>	274
<i>Inventory Software Packages</i>	275
<i>Create a SMP Package Content Filter</i>	275
Set-up SMTP Connection	277
<i>SMTP in Cloud Environments</i>	277
<i>Configuring the SMTP Connection</i>	277
<i>Setting up Email Alerts</i>	277
<i>Approval Requests</i>	277
Set-up SysLog Connection	278
<i>Configuring SysLog Connection</i>	278
<i>Setting up SysLog Server Tasks</i>	278
<i>Template Options</i>	279
<i>Data Sources</i>	279
<i>Troubleshooting if SysLog Option is Missing under Foreign Systems</i>	279
Set-up VirusTotal Connection	280
<i>VirusTotal API Key</i>	280
<i>Install VirusTotal</i>	280
General Tab	281
Policy Targeting	281
Approval Types	281

Approval Processes	281
Markdig.Syntax.Inlines.LinkInline	281
<i>History Tab</i>	282
Looking at Details	282
<i>Drilling Down</i>	282
Item Change History Report	283
<i>Reputation Tab</i>	284
Cylance Rating Provider	284
VirusTotal Rating Provider	284
Diagnostics Page	285
File Upload	286
Filters	287
<i>Types of Filters</i>	287
Create A Copy - How to Use Filter Templates	288
Creating a New Filter Manually	288
<i>More Options Menu for Filters</i>	289
<i>Creating New Filters using Event Discovery</i>	289
Resource Targets and Collections	292
<i>User Defined Resource Targets</i>	292
Interface to View or Create/Modify User Defined Targets	292
<i>Performance Considerations</i>	292
<i>Active Directory as Related to Resource Targets</i>	292
<i>Assigning Policies to Targets</i>	293
<i>Collections</i>	294
Using RegEx in Filters	295
List of Default Filters	296
<i>Win32 Executable Filters</i>	296
<i>Commandline Filters</i>	297
<i>Environment Filters</i>	297
<i>Network Location Filters</i>	297
<i>Parent Process Filters</i>	297
<i>Secondary File Filters</i>	298
<i>Security Rating Filters</i>	298
<i>Time of Day Filters</i>	298
<i>User Context Filters</i>	298
<i>File Filters</i>	298
Application Compatibility File Filters	298
Manifest Filters	298
File Owner Filters	298
File Specification Filters	298

Security Catalog Filters	300
<i>Miscellaneous Filters</i>	300
App Bundle Filters	300
Coff Header Filters	300
File Parameter Collections	300
Mach-O Header Filters	300
<i>Filter Types and Descriptions</i>	301
Common Filter Characteristics	301
<i>Filter Change History</i>	301
How to Search for Filters	301
Application Filters	303
Blank Win32 Executable Filter	304
<i>Parameters</i>	304
<i>Examples</i>	304
Commandline Filter	305
<i>Search for Commandline Filters</i>	305
<i>Create a new Commandline Type Filter</i>	305
<i>Parameters</i>	306
<i>Examples</i>	306
Download Source Filter	307
<i>Parameters</i>	307
<i>Examples</i>	307
Environment Variable Filter	308
<i>Parameters</i>	308
<i>Examples</i>	308
Network Location Filter	309
<i>Parameters</i>	309
<i>Examples</i>	309
Parent Process Filter	310
<i>Parameters</i>	310
<i>Examples</i>	310
<i>Using Secondary File Filters</i>	311
<i>Via File Inventory</i>	311
<i>Via Policy Wizard</i>	311
<i>Examples</i>	311
<i>Best Practice Using a Secondary File Filter</i>	312
<i>Using File Inventory</i>	312
<i>Executables File Example</i>	315
<i>Creating the Policy</i>	315
<i>Script Execution File Example</i>	318

<i>Creating the Policy</i>	318
<i>Verifying the Policy Works</i>	320
Security Rating Filter	322
<i>Parameters</i>	322
<i>Examples</i>	323
Signed File Filter	324
<i>Parameters</i>	324
<i>Examples</i>	324
Time of Day Filter	325
<i>Parameters</i>	325
<i>Examples</i>	325
Using User Context Filters	326
<i>On-Premise</i>	326
<i>Cloud</i>	326
File Filters	327
Application Compatibility Filter	328
<i>Parameters</i>	328
Application Manifest Filter ("Manifest Filter")	329
<i>Parameters</i>	329
File Collection Security Catalog Filter	330
<i>Parameters</i>	330
File Existence Filter	331
<i>Parameters</i>	331
File Owner Filter	332
<i>Parameters</i>	332
File Specification Filter	334
<i>Parameters</i>	334
<i>Additional Filters</i>	334
File Type Filter	335
<i>Parameters</i>	335
Internet Zone Filter	336
<i>Parameters</i>	336
Security Catalog Filter	337
<i>Parameters</i>	337
Unable to Access Cortana and Search for Windows 10	338
<i>How to Resolve</i>	338
Inventory Filters	339
File Collection from List of Sha1 Hashes Filter	340
<i>Parameters</i>	340
File Scan Results Filter (Computer)	342

<i>Parameters</i>	342
File Scan Results Filter (Policy)	343
<i>Parameters</i>	343
MSI File Contents Filter	344
<i>Parameters</i>	344
<i>Viewing, Editing, and Saving the Parameters</i>	344
MSI Package Contents Filter	346
<i>Parameters</i>	346
<i>Viewing and Editing the Package Parameters</i>	346
<i>Viewing and Adding the Resource(s)</i>	347
Package Contents Filter	348
<i>Parameters</i>	348
<i>Viewing and Editing the Package Parameters</i>	348
<i>Adding the Resource(s)</i>	349
Security Catalog Contents Filter	350
<i>Parameters</i>	350
Virtual Disk File Contents Filter	351
<i>Parameters</i>	351
Virtual Disk Package Contents Filter	352
<i>Parameters</i>	352
MacOS Specific Filters	353
<i>Creating macOS Filters Manually</i>	353
<i>List of MacOS Filters</i>	353
<i>Application Filter Types</i>	353
<i>File Filter Types</i>	353
<i>List of Default Filters for Event Discovery</i>	353
<i>Available Preference Pane Filters</i>	354
Application Bundle Filter	355
<i>Pre-10.7.1 Example</i>	355
<i>Parameters</i>	355
<i>Info.plist Example for Photos</i>	356
Default App Bundles File Specification Filter	357
<i>Example</i>	357
Default File Specification (MacOS)	358
<i>Example</i>	358
<i>Preference Pane Filters</i>	359
<i>Date and Time Preference Pane Filter</i>	360
<i>Energy Saver Preference Pane Filter</i>	361
<i>Network Preference Pane Filter</i>	362
Default Applications Folder (MacOS)	363

System Applications Folder (MacOS)	364
Default Applications Bundle Filter (MacOS)	365
macOS Executables	366
System Application Bundles Filter (MacOS)	367
Folders	368
<i>Policies Folder Overview</i>	368
<i>Tasks Folder Overview</i>	368
<i>Reports Folder Overview</i>	368
<i>Resources Folder Overview</i>	368
Export Items	370
<i>Exporting Items</i>	370
Specific Policy Export	370
Folder Exports	370
Importing Items	372
<i>Using Import Items</i>	372
<i>Using Diagnostics Upload Items File</i>	372
Licenses	373
<i>On-Premises</i>	373
<i>Cloud</i>	373
Server Logs	374
<i>Details</i>	374
<i>Search by CorrelationID</i>	375
Personas	377
<i>Viewing your Personas</i>	377
<i>Creating a Persona</i>	377
Resource Explorer	379
<i>Example for Discovered Files</i>	380
<i>Example for User Resource</i>	382
<i>Error Message after Deleting a User Resource</i>	384
Roles	385
<i>Privilege Manager Administrators</i>	385
<i>Privilege Manager Field Engineering</i>	385
<i>Privilege Manager Helpdesk Users</i>	385
<i>Privilege Manager MacOS Administrators</i>	385
<i>Privilege Manager Users</i>	385
<i>Privilege Manager Windows Administrators</i>	385
<i>Creating/Deleting Roles</i>	385
Application Roles	387
Setup	388
Tasks	389

<i>Client Tasks</i>	390
<i>Basic Inventory</i>	391
Basic Inventory (Initial, Windows)	391
Basic Inventory (Windows)	391
Basic Inventory (Initial, Mac OS)	391
Basic Inventory (Mac OS)	392
<i>Cleanup Agent Inventory Transfer</i>	393
Cleanup Agent Inventory Transfers (Windows)	393
<i>Cleanup Sent Privilege Manager Events</i>	394
Cleanup sent Privilege Manager Events (Windows)	394
Cleanup sent Privilege Manager Events (Mac OS)	394
<i>COM Inventory Policy</i>	395
<i>Configure Privilege Manager Remove Programs</i>	396
<i>Default File Inventory Policy</i>	397
Default File Inventory Policy (Windows)	397
Default File Inventory Policy (MacOS)	397
<i>Ensure UAC Override Setting (Windows)</i>	398
<i>Local User Inventory Policy</i>	399
Local User Inventory Policy	399
Local User Inventory Policy (MacOS)	399
<i>Perform Resource Discovery</i>	400
Perform Resource Discovery (Windows)	400
Perform Resource Discovery (Mac OS)	400
<i>Retry Errored TMS Events</i>	401
Retry errored TMS Events (Windows)	401
Retry errored TMS Events (Mac OS)	401
<i>Scheduled Check for Pending Tasks</i>	402
Scheduled Check Pending Client Tasks - Internet Clients (Windows)	402
<i>Scheduled Registration</i>	403
Scheduled Registration (Windows)	403
Scheduled Registration - Internet Clients (Windows)	403
Scheduled Registration (Mac OS)	403
<i>Set Agent Log Size</i>	405
<i>Shared Folder Inventory Policy</i>	406
<i>Update Agent Commands</i>	407
Update Agent Commands (Windows)	407
Update Agent Commands (Mac OS)	407
<i>Update Applicable Policies</i>	408
Update Applicable Policies (Windows)	408
Update Applicable Policies - Internet Clients (Windows)	408

Update Applicable Policies (Mac OS)	408
<i>Update Provisioned Resource Client Items</i>	410
Update Provisioned Resource Client Items (Windows)	410
Update Provisioned Resource Client Items (MacOS)	410
<i>User Logon Inventory Policy</i>	411
<i>Windows Server Inventory Policy</i>	412
<i>Server Tasks</i>	413
Component Based List of Default Tasks	413
<i>Helpdesk Tasks</i>	414
<i>Infrastructure Scheduled Activities</i>	415
<i>Scheduled Tasks</i>	417
AD Import and Synchronization Tasks	417
Task Parameter Conflicts	417
<i>E-mail Reports Task</i>	418
Tasks Launching Executables	421
<i>Example Scenario</i>	421
<i>Workaround</i>	421
Maintenance	422
<i>Maintenance Tasks</i>	422
Assign Orphaned Agent Uploads	422
Delete Old Performance Counter Events	422
Initialize Item Change History	422
LSS Migration Tasks	422
Purge Agent and Gauge Data for Deleted Computers	422
Purge Duplicate Computers	422
Purge Maintenance - Agent Logs	422
Purge Maintenance - Application Control Events	422
Purge Application Control Events older than	422
Purge Maintenance - Audit Events	422
Purge Maintenance - Completed File Upload Sessions	422
Purge Maintenance - Files Undiscovered	423
Purge Maintenance - Incomplete File Upload Sessions	423
Purge Maintenance - Message History	423
Purge Maintenance - Orphaned Local Users and Groups	423
Purge Old Computers	423
Reset Licensing	424
<i>Using the Reset Licensing Task</i>	424
Users	425
<i>How to Manually Add Thycotic One Users</i>	425
<i>How to Manually Add Standard Users</i>	425

<i>How to Manually Add API Client Users</i>	427
<i>Add Roles to a User</i>	427
Password Complexity Enforcement	430
Tools Menu	431
Password Disclosure	432
<i>Using the Disclose Password Tool</i>	432
Computer Groups	434
Local Security	435
<i>Computer Groups</i>	435
<i>Local Groups</i>	435
<i>Local Users</i>	435
Create New Computer Group	436
Local Groups	438
<i>Create New Local Group</i>	438
<i>Manage Local Groups</i>	438
Statistics	439
Audit	439
Local Users	440
<i>Create New Local User</i>	440
<i>Password Management: Randomize Local Account Passwords</i>	441
<i>Reports Relating to Managed Accounts</i>	441
Shared Folder Inventory	443
<i>Enable the Policy</i>	443
Disable Local Guest Accounts	444
Logon User Tracking	445
<i>Viewing the Resource</i>	446
Migrate Local Security Policies	447
<i>Migration Steps</i>	447
macOS Computers	450
<i>macOS Specific Policies</i>	451
Actions Supported by macOS Agents (Kernel vs System Extensions)	451
<i>Agent Behavior with Actions</i>	451
<i>Allow Copy to Install Applications</i>	452
Updating Existing Policies to Use the Copy Install Application Filter	453
Updating the Endpoint	453
Expected User Experience	454
<i>Deny Zoom Application</i>	455
File Inventory	455
Assign to Policy	456
Updating the Endpoint	457

Policy Verification	457
<i>Determine Admin Requirement</i>	458
Creating the Policy	458
<i>Require Justification - FireFox</i>	460
Updating the Endpoint	460
Expected User Experience	461
<i>macOS Approval Process</i>	462
Application Approval Request Message Action	462
Deny Execute	462
Deny Execute and Deny Execute Message Action	462
Deny Execute and Application Denied Message Action	462
Application Justification Message Action	462
Application Warning Message Action	462
<i>Move to Trash Bin Policy</i>	463
<i>Application Self-elevation</i>	464
Configuring Application Self-elevation	464
How to Request an Application Run as Administrator	464
Troubleshooting: Verify the Finder Extension is Installed	464
<i>Finder Extension and Drive Type Extensions</i>	465
<i>macOS Application Approval Process via Sudo Plugin</i>	466
Example: Elevate Applications Executed from Folder	466
<i>Endpoint Interaction</i>	466
<i>Privilege Manager Console Interaction</i>	466
<i>Endpoint Interaction</i>	468
<i>Following Approval</i>	468
<i>Following Denial</i>	468
<i>Adding macOS Agents to a Computer Testing Group</i>	469
Creating a MacOS Test Computer Group	469
Setting Up Monitoring Policies for macOS	469
<i>Inventinging .pkg Files</i>	472
Windows Computers	474
Application Control	475
<i>Dashboard</i>	475
Monitoring - Learning Mode Policies	476
<i>Creating a Monitoring Policy</i>	476
<i>Discover Applications that Require Administrator Rights</i>	476
<i>View Policy Results</i>	477
<i>Discover All Events on Test Endpoints</i>	477
Sending Policies to Endpoints	479
<i>View Deployment Status</i>	480

<i>Update Policies on an Endpoint using Powershell (prior version 10.7)</i>	480
<i>Agent Event Log Viewer</i>	480
Agent Policy State	481
Using RegEx in Policies and Filters	482
<i>Special RegEx Characters</i>	482
Escape Example	482
Wildcard Example	482
<i>File Name Examples</i>	482
Match with Wildcard before the File Name	482
Match File Name Containing String and File Type	482
Match with Wildcard at end of File Name and before File Type	482
Match with Wildcard in the Middle of Two Strings	482
Match with Wildcard at End of File Type	482
<i>File Path Examples</i>	482
Wildcard at the End of the Path	482
Wildcard in IP Address for Network File Path	483
Wildcard for Application Updates for all Users	483
Deleting Items	484
Exclusion of Users on Policies	485
<i>Targeting Administrators with the Exclusion</i>	485
<i>Targeting new Local Groups (not built-in)</i>	485
<i>Policies</i>	487
Using Policy Templates	487
Overview of the Configuration Process	487
Collecting File Data	487
Points to Consider	487
<i>Policy Enforcement</i>	488
Continue Enforcing	488
Continue Enforcing Policies for Child Processes	488
Stage 2 Processing	488
Applies to All Processes	488
Skip Policy Analysis at Start-up	488
Using the Policy Wizard	489
<i>Using a Blank Policy</i>	489
Creating a Monitoring Policy	491
Creating a Controlling Allow Policy for macOS	493
Creating a Controlling Block Policy for macOS	495
Creating a Controlling Elevation Policy for macOS	496
Creating a Controlling Allow Policy for Windows	498
Creating a Controlling Block Policy for Windows	500

Creating a Controlling Elevation Policy for Windows	501
Creating a Controlling Restrict Policy for Windows	502
Full Policy Wizard Diagram	504
<i>What's on the Policy Page</i>	506
Policy Activation	506
Policy Details	506
Conditions	506
Actions	506
Show Advanced	506
<i>Priority</i>	507
Why Policy Priority Matters	507
<i>Deny MMC.EXE Policy setup</i>	507
Allow specific MMC Snap-in	507
Test this use case	508
<i>List of Default Policies</i>	509
Process Hardening	509
System Options	509
Privilege Management	509
Application Analysis	509
Windows Policies	509
macOS Policies	509
Automatic Elevation via Windows Client System Settings	510
ActiveX	510
Firewall	510
General	510
<i>Not Enabled</i>	511
<i>Example Policies</i>	512
Approval Policies	513
Offline Approvals	514
<i>Creating an Offline Approval Policy</i>	514
<i>Endpoint Offline Approval</i>	514
<i>Privilege Manager Offline Approval</i>	515
Help Desk Approvals	517
<i>Creating a Helpdesk Policy</i>	517
<i>Workflow</i>	517
<i>Approve requests</i>	517
Google Authenticator	518
XML for Challenge Response Message Action	519
Allow Listing Policies	522
Git App with File Upload	523

MS Security Catalog	525
Elevation Policies	527
Application Execution Requires Approval	528
<i>Create a Policy using this Filter</i>	528
<i>To Approve Requests</i>	529
Elevate MSI Files on the Network Share	530
<i>Option 1</i>	530
<i>Option 2</i>	530
Network Share Applications	532
<i>Applying Administrator Rights to a Network Share</i>	532
<i>Creating the Filter</i>	532
<i>Creating the New Policy</i>	532
<i>Using the UNC Elevation Policy Template</i>	532
Setting up ActiveX Policies	534
<i>Creating the Policy</i>	534
UAC Override Policy	537
<i>Using the Default Policy</i>	537
User Justification Required to Run	539
Elevating the Privilege Manager Remove Programs Utility Policy	541
Monitoring Policies	542
Catch-All Policy	543
Reputation Checking	545
<i>Creating Security Rating Filter</i>	545
<i>Creating User's Downloads Location, Temp Dir, and Collection Filters</i>	546
<i>Creating a Policy</i>	547
<i>Viewing a File Security Ratings Report</i>	548
Blocking Policies	549
Catch-all Deny	550
iTunes with File Upload	551
Quarantine Specified Malware	552
Specific Applications	554
<i>Using File Inventory</i>	554
<i>Using the Policy Wizard</i>	554
File Inventory	555
Policy Events	557
Best Practices	558
What's First	558
<i>Event Discovery</i>	558
<i>Never Disable Event Discovery</i>	558
Purpose of Event Notifications	558

Best Practices	558
Examples	559
<i>Send Policy Feedback</i>	559
<i>Don't Send Policy Feedback</i>	559
Events Maintenance	560
Manually Purge Events	560
Maximum Event Count: Basics	561
<i>Maximum Event Count: Additional Information</i>	561
Reports	562
Data Records Displayed	562
Export Options	562
Reports and Queries	564
View the Existing Reports in Privilege Manager	564
Determine the SQL Query Object Used by a Report	564
View the SQL Query in Privilege Manager	566
<i>Access and Edit the Query from the Folder View</i>	566
<i>Resolved Query</i>	567
<i>Results</i>	568
Change History Report	569
Domain Users in Administrator Group	570
Logon Session Summary Report	571
Using the Collect Windows Logon Events Client Task	571
Performance Reporting	573
Setting up Performance Reporting	573
Primary User	574
How to Find the Primary User for a Specific Machine	574
Default Update Primary User for Collection	574
Application User Activity	575
How to...	576
Best Practices	577
<i>Active Directory Import - On-prem vs Cloud</i>	578
On-premises	578
Cloud	578
Full vs Differential Synchronization	578
Expected Performance	578
<i>Status</i>	578
Azure AD Imports	578
<i>Users/Groups</i>	578
<i>Import Azure AD Resources</i>	578
<i>Import Specific Azure AD Users and Groups</i>	579

<i>Device Import</i>	579
On-Premises vs. Cloud	579
Troubleshooting AD Sync	580
Authentication	580
Duplicates	580
<i>Resource Type Keys</i>	581
<i>Global Account Details - SID</i>	581
<i>Availability</i>	581
<i>Global Windows Users - User Id & Domain Name</i>	581
<i>Availability</i>	581
<i>Azure AD - Device ID</i>	582
<i>Send Azure AD Domain Info</i>	582
<i>Limitations</i>	582
<i>Registry/Certificates</i>	582
Privilege Manager Disaster Recovery	584
Maintaining Privilege Manager in a Disaster	584
<i>Simple Installation and Architecture</i>	584
<i>Restoring from Backup</i>	584
<i>Restoring Privilege Manager from a Backup</i>	584
<i>High Availability</i>	584
Summary & Additional Support Resources	584
Using a Service Account to run the IIS App pool	585
<i>Creating a Domain Service Account</i>	585
<i>Granting Access to SQL Database</i>	585
<i>Assigning Identity of Application Pool(s) in IIS</i>	586
<i>Granting Folder Permissions</i>	587
<i>Configuring User Rights Assignment</i>	588
<i>Setting User Rights Assignment on the Domain</i>	588
<i>Setting User Rights Assignment Locally</i>	589
Prevent Read and Write Access to File Types or Locations	590
<i>Create a Deny File Access Action</i>	590
<i>Create an Application Control Policy</i>	590
<i>Test Access</i>	592
Securing the IIS Server	593
<i>Patches and Updates</i>	593
<i>Services</i>	593
<i>Protocols</i>	593
<i>Accounts</i>	593
<i>Files and Directories</i>	593
<i>Shares</i>	593

<i>Ports</i>	593
<i>Registry</i>	593
<i>Auditing and Logging</i>	593
<i>Sites and Virtual Directories</i>	593
<i>Script Mappings</i>	593
<i>ISAPI Filters</i>	594
<i>IIS Metabase</i>	594
<i>Server Certificates</i>	594
<i>Machine.config</i>	594
<i>Code Access Security</i>	594
<i>Other Check Points</i>	594
<i>Other Considerations</i>	594
Infrastructure	595
Privilege Manager High Availability Setup	596
<i>Pre-Requisites</i>	596
System Requirements Overview	596
Using the Installer to Install/Confirm Pre-Requisites	596
<i>Manual Set-up of Secondary Node</i>	596
Folder Permissions to C:\Windows\Temp	600
Folder Permissions to the Privilege Manager Application Folder	601
Permission to Certificate Private Key (prior to 10.6 only)	602
Verify Login on Secondary Node	602
<i>Re-encrypt ConnectionStrings.config</i>	602
Setting up Internet Connected Clients	603
<i>Azure Service Bus Queue Configuration</i>	603
<i>Setting up the Service Bus Foreign System</i>	603
<i>Configuring Agents to Use the Service Bus</i>	604
Using regedit	604
Using PowerShell	604
Moving SQL DB	605
<i>Moving the Privilege Manager DB</i>	605
Step 1: Backup and Restore the Database	605
Step 2: Connect to the new database (configure the database connection details)	605
Setting up a Reverse Proxy	606
<i>System Specifications</i>	606
<i>Server Configuration</i>	606
Testing Agent URLs	608
<i>Agent Configuration</i>	609
Maintenance	610
How to Purge Computers	611

Purging Action Items Table	613
<i>Creating a Scheduled Event for Purging</i>	613
Using the Remove Programs Utility	615
<i>Using the Configure Privilege Manager Remove Programs Policy</i>	615
Configuring the Remove Programs Utility	615
<i>Use the Utility</i>	616
Troubleshooting	617
Markdig.Syntax.Inlines.LinkInline	617
Agents Troubleshooting	617
Endpoint Troubleshooting	617
Markdig.Syntax.Inlines.LinkInline	617
Markdig.Syntax.Inlines.LinkInline	617
Markdig.Syntax.Inlines.LinkInline	617
Markdig.Syntax.Inlines.LinkInline	617
Errors	618
Common Errors	619
<i>Access Denied</i>	619
<i>Server Error in...</i>	619
<i>SSL Connectivity or Certificate Issues</i>	619
Trusting an SSL Certificate on a Client Machine (KB)	619
Granting Permissions on New SSL Certificate for Privilege Manager (KB)	619
<i>To grant permissions manually, follow these steps</i>	619
<i>Grant Read Access to the account(s) that TMS is running under</i>	619
<i>Tasks Stuck at Ready</i>	620
<i>CPU Issue</i>	620
<i>System Critical Error</i>	620
Error: Space Allocation	621
<i>Resolving the Error</i>	621
Installation Hangs with Error: Worker Role Monitor received exception during ping	622
<i>Resolve</i>	622
Error: Invalid product identifier:	625
<i>Resolve</i>	625
Notify User Justification failed	627
<i>Resolve</i>	627
UI Storage Error	628
<i>Resolution</i>	628
Installation and Upgrade Issues	629
10.5 Folder Permissions - MachineKeys	630
Installation Issues	631
<i>Internet Connection</i>	631

<i>.NET Dependency</i>	631
<i>IIS not Installed</i>	632
<i>HTTPS Binding Error</i>	632
<i>PowerShell Error</i>	632
<i>Secret Server and Privilege Manager Installed</i>	633
<i>Error in DB File Path</i>	633
<i>Outdated Browser</i>	634
<i>Integrated Authentication Error</i>	634
Retrieving the COM Class Factory Error	636
<i>Resolve</i>	636
Performance Issues	637
Increase Boot-up Performance	638
<i>Enable Pausing Policy Analysis during Boot-up</i>	638
Unable to Access Privilege Manager	639
<i>Resolve</i>	639
Privilege Manager Logs	641
Where are My Server Logs	642
Where are My Agent Logs	643
SQL Server Transaction Log	644
User Interface and Ports	645
<i>Connectivity</i>	645
Troubleshoot with Tools	646
Using Thycotic Monitor	647
Using Process Explorer for Troubleshooting a Policy	649
<i>Detailed Troubleshooting Steps</i>	649
Using Process Hacker for Troubleshooting	651
Privilege Manager Mobile Application	652
Detailed Instruction Topics	652
Configure Azure Active Directory	653
Configure the Service Bus for Mobile	655
Creating a Service Bus and Queue in the Azure Portal	655
Adding the Service Bus as a Foreign System	655
Install and Configure the Mobile Console in Privilege Manager	657
Install the Privilege Manager Mobile Console	657
Set the Client ID and Tenant ID	657
Configure the Notification Settings	658
Authentication Provider Warning	660
Mobile App Install and Sign In	661
Troubleshooting	661
Use the Mobile Application	662

Approval requests	662
Password Disclosure	662
Alerts	662
Release Notes	664
10.8.2 Release Notes	665
Enhancements	665
<i>Security</i>	665
<i>macOS</i>	665
Agent Pertaining to Big Sur and Catalina	665
Bug Fixes	665
Known Issues	665
<i>macOS Specific</i>	665
10.8.1 Release Notes	666
Enhancements	666
<i>Cloud</i>	666
Bug Fixes	666
<i>Cloud</i>	666
<i>macOS</i>	666
Known Issues	666
<i>macOS Specific</i>	666
10.8.0 Release Notes	667
Enhancements	667
<i>macOS Specific Features</i>	667
<i>Public API</i>	667
<i>Cloud Specific Features</i>	667
Bugs Fixed	667
<i>macOS Specific</i>	667
<i>Agent Updates</i>	667
Known Issues	667
<i>macOS Specific</i>	668
10.7.1 Release Notes	669
Enhancements	669
<i>macOS Specific Features</i>	669
<i>Cloud Specific Features</i>	669
Bug Fixes	669
<i>Agent Updates</i>	669
Known Issues	670
10.7 On-prem Release Notes	671
Enhancements	671
Bug Fixes	671

Known Issues	672
10.6 On-prem Release Notes	673
Enhancements	673
Bug Fixes	673
Known Issues	673
10.6 Cloud Release Notes	674
Enhancements	674
Bug Fixes	674
Limitations in Privilege Manager Cloud 10.6 vs. On-prem	674
Known Issues	675
10.5 and Previous Releases	676
10.5.4	676
<i>Enhancements</i>	676
<i>Bug Fixes</i>	676
10.5.000003	676
<i>Bug Fixes</i>	676
<i>Mac Agent Updates (version 10.5.12)</i>	676
10.5.000001	676
<i>Bug Fixes</i>	676
10.5.000000	677
<i>Overview</i>	677
Important for Secret Server Combined Upgrades	677
<i>10.5 Agent Upgrades</i>	677
<i>Enhancements</i>	677
<i>Bug Fixes</i>	677
<i>Known Issues</i>	677
10.4.001233	677
<i>Bug Fixes</i>	677
10.4.001231	677
<i>Enhancements</i>	677
<i>Bug Fixes</i>	677
10.4.000000	678
<i>Enhancements</i>	678
<i>Bug Fixes</i>	678
<i>Known Issues</i>	678
10.3.000014	678
<i>Enhancements</i>	678
<i>Bug Fixes</i>	679
10.3.000000	679
<i>Enhancements</i>	679

10.2.000000	679
<i>Enhancements</i>	679
10.1.000000	679
<i>Enhancements</i>	679
<i>Bug Fixes</i>	679
Documentation Changelog	680
May 2021	680
January 2021	680
December 2020	680
October 2020	680
<i>Group Member Based Approvals</i>	680
August 2020	680
<i>New Related Docs</i>	680
<i>Restructure of Contents</i>	680
July 2020	682
June 2020	682

Privilege Manager is an endpoint least privilege and application control solution for Windows and macOS, capable of supporting enterprises and fast-growing organizations at scale. Mitigate malware and modern security threats from exploiting applications by removing local administrative rights from endpoints. The two major components are Local Security and Application Control.

Using Privilege Manager, administrators can automatically discover local administrator privileges and enforce the principle of least privilege through policy-driven actions. Those policy-driven actions include

- blocking, elevating, monitoring, allowing
- application quarantine, sandbox, and isolation,
- application privilege elevation, and
- endpoint monitoring

All this is seamless for users, reduce IT/desktop support workload, and support compliance obligations.

Privilege Manager does not require Secret Server or any other Thycotic product to run. Secret Server's vaulting and workflow capabilities can be extended to privileged endpoint accounts when the two products are used together.

The typical Privilege Manager user is part of an IT team that is tasked with implementing and overseeing a company's security business requirements and framework. In the Privilege Manager product this role is known as the Privilege Manager Administrator. Although there are a few other kinds of [Privilege Manager user roles](#) that may use Privilege Manager now and then for minor tasks, the Privilege Manager Administrator is the main user of Privilege Manager.

It is useful (although not necessary) for Privilege Manager Administrators to be familiar with the basics of IT administration, such as the Group Policy feature from Microsoft.

What's New in Privilege Manager 10.8

The 10.8 release of Privilege Manager introduces a new user interface, providing a redesigned user experience, simplifying many major areas and typical workflow processes when setting up application policies or local security.

To preview the enhancements made to the user interface, please view this [video](#).

Switching between the new and old UI post upgrade is not available.

Feature Overview

For those organizations leveraging [Active Directory \(AD\)](#) and/or [Azure AD](#) as their identity authentication and authorization service, deploying a least privilege program that works seamlessly with AD is absolutely critical. Privilege Manager integrates with AD so administrators can synchronize Domain Objects such as computers, OUs, and security groups from AD with their application control policies. Privilege Manager can leverage the user, group and privilege associations managed by Active Directory in its policy deployment and ensure unauthorized changes to AD made by endpoint users – such as adding a user to a local administrator account – can be blocked automatically and in real time.

The [Privilege Manager Agents](#) are a critical component of Thycotic's application control, giving you the ability to evaluate the health and status in real time. Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and endpoint operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

The most powerful applications installed on endpoints are those that require administrator credentials or root privileges to run. Privilege Manager discovers all applications that run on endpoints through its Learning Mode, giving you a precise snapshot of how these applications are used before you implement any changes. You can set up Discovery policies to target any new application action that requires administrator or root access, so no privileged action goes unnoticed.

Non-Domain Endpoint Support - Privilege Manager provides management and application control support for endpoints even if they are not associated with your organizational network. Because it utilizes agents it can manage endpoints outside the network – such as those used by vendors, contractors, and partners - with the same dexterity and precision control as those within the network.

Rotate [local account passwords](#) on endpoints based on a pre-defined, fully customizable schedule, ensuring that password best practices are followed.

Privilege Manager can record all executable events on managed endpoints so you can review, search, and analyze these logs in a unified manner without leaving the console.

Child processes are those that execute from within a file such as a PDF and are frequently how malware executes on an endpoint. Privilege Manager allows you to prohibit execution of Child Processes to ensure unknown executables are restricted on your organization's network.

Privilege Manager's ability to quickly generate fully customized reports and schedule the execution and delivery of these reports is essential to maintaining a real-time understanding of every aspect of your least privilege program.

Review and manage local groups, including Group membership. This powerful capability prevents Group membership changes from being made on an endpoint, as all changes must be made via the Privilege Manager console.

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

Enforce least privilege through policies for application control. You'll start with access to a broad library of out-of-the-box policies, all of which are completely customizable. Layered policies create the parameters that dictate precisely how privileges are accessed across your network. They define what actions people can run, and where. When policy conditions are met, Privilege Manager automatically applies an action (e.g. blocking, monitoring, application elevation, etc.) on one or multiple assets.

Web server clustering provides both [high availability and load balancing](#) by allowing multiple web servers to run Privilege Manager software. A clustered environment is key in disaster recovery scenarios as you can automatically failover to a separate web server with no downtime. Additionally, performance can be improved through load balancing by having multiple servers processing requests simultaneously.

Privilege Manager can automatically revoke all local administrative privileges on endpoints so you can adhere to a least privilege policy. With application-level privilege elevation, user-level privileges are not required and people can still access all the systems they need.

You can [manage all local users](#) on all endpoints across your organization, including the automatic rotation of local user password(s), all from a central console.

The ability to audit and review the activity of local users and groups is essential to retroactively identify problematic activity and reduce risk. Privilege Manager lets you swiftly review and search across all User and Group activity associated with privilege escalation on every managed endpoint.

The [Privilege Manager mobile app](#) for iOS and Android lets you manage endpoints, configure policies, process approvals, and receive event alerts via a mobile device so you can learn of requests and address issues quickly.

Privilege Manager integrates with reputation checking software like [VirusTotal](#) to provide application analysis in real time. This unique feature allows for reputation analysis of any unknown applications in order to mitigate risk of endpoint attacks from ransomware, zero-day attacks, drive-by downloads, and other unknown malicious software. With Privilege Manager, all applications that meet a general condition (i.e. executed from a specific directory or directories, file names, types, or any applications that are disassociated with existing policies) can be sent to VirusTotal for a reputation check and analysis.

Successful application control demands that you have a complete, real-time understanding of the status and activity of all endpoints. Privilege Manager provides a unified reporting dashboard so you can quickly evaluate the status of endpoints, review activity logs and event data, and access a broad library of reports. Responsive and fully configurable, Privilege Manager's dashboard reporting enables you to quickly drill down into reports across any dimension (time, geo-region, OS, status...) to evaluate activities and trends. From the dashboard you can also set up automated alerts to stay informed of potential problems.

Many organizations choose to protect their Privilege Manager web server by restricting it from direct outbound internet access. To secure your environment according to best practices, it is not enough to simply set your server offline because

Privilege Manager still will communicate directly to agents across your network that DO have direct internet access, therefore attackers can potentially use the connection between your endpoint agent and Privilege Manager to breach your web server. To prevent this direct connection between agent endpoints and your Privilege Manager web server, Privilege Managers allows for the setup of a [Reverse Proxy](#) machine with limited permissions. A properly configured Reverse Proxy will act as a buffer between Privilege Manager agents and the Privilege Manager server to limit server exposure.

Sandboxing quarantines applications so they are not allowed to execute, or only allowed to execute in a limited way so they don't touch any system folders or underlying OS configurations. Privilege Manager supports sandboxing for applications that are not known, to ensure they do not negatively impact productivity or introduce threats to the endpoint or network.

Many organizations leverage ticketing systems to streamline their support workflow and like to view and report on all support requests within a single system. Privilege Manager can be fully integrated into [ServiceNow](#), so support requests and IT responses can be managed, tracked, and reported via the ticketing system itself.

For those organizations utilizing the [Symantec Endpoint Protection](#) or Symantec Endpoint Protection Cloud solution for allow listing and reputation, Privilege Manager can utilize the SEP allow list and reputation engine to inform and prescribe its provision of application control capabilities across endpoints.

You can integrate your least privilege and application control program with a SIEM tool or other cyber security reporting and analytics services and tools. Privilege Manager can push out [SysLog](#) messages on a fully configurable schedule to any application or service that accepts the SysLog format.

Privilege Manager can integrate with [Microsoft System Center Configuration Manager](#) and scan SCCM software delivery "packages" for applications that can be allow listed by Privilege Manager.

Privilege Manager supports allowing trusted applications, blocking to deny known malicious applications based on attributes, file hash, location, or certificates, and monitoring to prevent unknown applications from running. Monitoring provides a system for discovering the unknowns and adding an action that hinges on a reputation check. Distinct from allowing applications to run with default user level privileges, an elevation policy applies admin credentials to specified applications. This type of policy is often paired, so that employees can perform trusted tasks that require administrator credentials to complete, like installing a trusted application (Adobe) or device (printer), without involving IT support.

By only elevating application privileges based upon specific policies and criteria, Privilege Manager ensures people don't use Microsoft's UAC capabilities to grant a dangerous or unknown application administrative rights under any circumstance.

Privilege Manager identifies all local accounts on agent-installed endpoints and flags those with local admin rights, including hidden or hardcoded admin privileges. A single, comprehensive view makes management easy.

Least Privilege Explained

Least Privilege is a security-driven management philosophy that models a system where all employees are given the minimum level of access rights necessary to carry out their job functions on endpoint machines. This is to protect each machine from malicious applications, rogue employees, or attackers. Privileged local admin or root accounts on endpoints give unfettered access to the entire endpoint and can potentially be used to access other computers, domain resources, and critical servers unless a least privilege security model is implemented. But implementing Least Privilege can be difficult for IT teams to enforce because there are plenty of daily, trusted activities that employees must perform that require access to privileged credentials.

Privilege Manager's toolset is two-fold. First, Local Security discovers all accounts that exist on endpoints and allows Privilege Manager Administrators to control the exact membership of every local group. This will ensure the correct admin and root accounts are permanently set. Additionally, credentials will be controlled by enforcing password rotation on those accounts.

Second, Application Control allows Privilege Manager administrators to manage application activity on endpoint machines. Applications that require admin rights or root access can be automatically elevated, allowed applications are allow listed, and malicious applications are blocked.

In other words, tailoring a robust, role-based Application Control system is key to keeping your organization's employees working both securely and effectively, without notable disruptions. But managing local administrator and root accounts through Local Security is arguably the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.

Every implementation looks different when configuring Privilege Manager to work best for your organization. The key is to know your goal and be smart about getting there. The [Getting Started section](#) will walk you through beginning configurations for both Local Security and Application Control.

10.8 User Interface Introduction

The 10.8 release of Privilege Manager introduces a new user interface, providing a redesigned user experience, simplifying many major areas and typical workflow processes when setting up application policies or local security.

To preview the enhancements made to the user interface, please view this [video](#).

Switching between the new and old UI post upgrade is not available.

Refer to [The Privilege Manager UI](#) for an overview of the main UI components.

Glossary

Action - An action is not required in a policy. A policy can be designed, for example, to simply listen for specific application activity, and provide auditing information back to Privilege Manager. However, to apply controls to a process (executable), one defines an action in the policy.

Some common actions include:

- Adjust process rights,
- Add administrative rights,
- Remove administrative rights,
- Deny application execution,
- Require user justification - user provides a reason why they need to run the application,
- Application warning,
- Bypass UAC prompt,
- Require workflow approval - user needs approval to run an application, etc.

Agent - An agent is installed on every endpoint in your network and will 1) Receive and apply defined policies to govern application/process execution on the endpoint, 2) Execute tasks on the endpoint and feed audit and inventory data back to Privilege Manager.

Agent BaseUrl - The agent must be set to communicate directly with Privilege Manager. There exists a registry entry that is set upon agent installation - this registry key is called BaseUrl.

Agent Registration - The Privilege Manager agent completes a registration process when it initially contacts Privilege Manager following installation, but also at regular configurable intervals. So, registration occurs regularly.

Arellia - Arellia was the original name for Privilege Manager. Because of this, many file paths and back end notations include the term Arellia or AMS instead of Privilege Manager or TMS.

Computer Groups - (also called Resource Targets) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Condition - Policy Conditions contain one or more filters that defines what a policy is 'listening' for. If the condition is satisfied in a policy, then an action is applied.

Config Feeds - Config Feeds can be found on the ADMIN page access from the Privilege Manager main page. Configuration feeds allow Thycotic to deliver new components to Privilege Manager. Simply click through the options in the Config Feeds page starting with the Select Items button and download anything appropriate. Once the item is downloaded, it is immediately available in Privilege Manager.

Dashboard - Dashboard is the term for Privilege Manager's landing page, or Home screen.

Event - Any notable file data on your network that is targeted by Privilege Manager is called an Event.

Discovery - Discovery is a term used by Thycotic for any information that is scanned or "found" on a network and imported or used by our products.

Least Privilege - Least Privilege is a security strategy organized around best practices. When effectively implemented, an organization's employees can navigate their network system with the lowest level of privileges. Higher credentials are flexibly (and often automatically) granted or denied based on users and the tasks being performed. This dynamic strategy significantly reduces the threat of security breaches across an organization without interfering with daily operations.

Filter - The Policy Condition lists one or more filters. A filter is defined to identify many things about an executable or process, or 'situation' when an executable or process is initiated.

Common Filters include:

- File specifications,
- Network location,
- Directory location,
- Application reputation,
- Application digital certificate,
- Time of day, User context (what AD security group a user belongs),
- Download source,
- Drive type,
- File owner,
- Internet Zone,
- Security Catalogs, etc.

Inclusion Filter/Exclusion Filter - When a filter is placed in the Inclusion Filters or Exclusion Filters under the Conditions tab of a policy definition, it can be used to explicitly include or exclude what is defined in the filter with respect to a policy. (I.e. Exclusion: apply this policy only if the user is NOT an administrator; Inclusion: apply this policy only if the computer is on the company network; Inclusion: apply this policy only to applications signed by a specific company's digital certificate, etc.)

Persona - Personas manage sets of privileges that are assigned to users on specific Windows computers or Computer Groups. A Persona includes a set of pre-defined filters and provide an easy way to assign policies based on Computer Groups and users. Filter parameters in a Persona are limited and specifically designed to be applied to Windows administrative users.

Policy - A set of conditions (Filters) that, when met, will apply an action to managed resources (target computers).

- **Blocking** - Type of policies that will deny an application from running based on a determined set of criteria.
- **Catch-All** Policy - A Catch-All policy is a type of Learning Mode policy that will gather information about any unknown events that happen in your network.
- **Elevation Policy** - An Elevation Policy will allow specified applications to run with administrator credentials.
- **Monitoring** - Monitoring is a dynamic method of managing applications that might not be included on a safelist or blocklist. Instead of trying to anticipate every executable users will run, you can apply a flexible policy that includes actions or reputation checking for unknown applications.
- **Non-Blocking** - Types of policies that will allow applications to run according to normal user credentials. This is often considered a neutral policy to specify trusted applications.

Policy Priority - Policies are evaluated in a certain order for each application that runs. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent.

RDP Monitor - Discontinued with version 10.6. The RDP Monitor is used to configure the Enhanced Session Monitoring feature in Secret Server. It is found in Privilege Manager because this feature uses the agent architecture defined by Privilege Manager, however this feature typically is not used in a Privilege Manager PoC.

Reputation Engine - Privilege Manager can call upon a reputation engine (e.g. VirusTotal) in real-time to check an application's public reputation. One can create a reputation checking policy in Privilege Manager through Monitoring policies. This type of policy can take application information and send it to the engine in real-time and act on the application based on the returned reputation. For example, if the reputation engine returns a BAD grade, the application can be denied. It is recommended to apply this type of policy to specific directories where new or unknown applications might reside - like the Downloads, TEMP, or Desktop directory.

Resource Targets - (also called Computer Groups) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Scheduled Tasks - A Privilege Manager policy may be defined to be applied based on a schedule. These items run using the Task Scheduler on each endpoint, and are only accessible by Privilege Manager administrators.

Secret Server - Secret Server is a second Thycotic product that many IT teams use to securely manage privileged accounts and passwords in an organization. Privilege Manager and Secret Server are separate products but often used together for a holistic approach to network security. The two products are highly integrated and some of the features cross between products. For example, the Secret Server license page houses Privilege Manager licenses, and Secret Server clients rely on Privilege Manager agent (RDP Monitor) when using the advanced session recording feature.

Send Policy Feedback - Send Policy Feedback is a setting that can be enabled for any policy that sends information to Privilege Manager. This is used in Learning Mode Policies and often valuable during testing, configuration, or auditing projects.

TMS - TMS is shorthand for Thycotic Management Server. It is an umbrella term for our base application layer that Privilege Manager runs on top of.

VirusTotal – The VirusTotal reputation service is supported by Privilege Manager as a reputation engine. A free VirusTotal API key will need to be obtained to use VirusTotal in Privilege Manager. Note that the free API has limits and may not be appropriate for a production environment that functions with over four requests per minute.

App User - These are the users connecting to your Privilege Manager websites. These users will be limited to the users that perform administrative tasks (admins), to use the solution in a helpdesk role, or to perform approvals or audits.

Privilege Manager Agents - These is used for application control and local user/group management.

Load Balancers - Load balancers are often involved in the solution to help distribute web traffic to more than one web server. Local and Global load balancers, if available, may be used in the solution to further lower potential application downtime during upgrades, patching, and single site failures.

Web Server - This is a primary component of the solution. Our web servers use IIS 7 and newer and will only work on Windows Server 2008 R2 - Windows Server 2016. For multiple web server (clustered) solutions, the web application itself can be made cluster aware and does not require being built as part of an IIS farm. Each web server acts as its own stand alone web server.

Database Server - This is a primary component of the solution. Microsoft SQL Server hosts the Privilege Manager databases. We are compatible only with SQL Server 2012 or newer running on Windows Server 2012 R2 - Windows Server 2016. The Thycotic databases can be put on a stand alone server, a FCI, or preferably using an AlwaysOn AG for clustered environments. The databases can be added to an existing production SQL cluster or instance, but proper sizing of the environment should be done. Windows authentication only is advised.

Reverse Proxy / Azure Service Bus - A properly configured Reverse Proxy will act as a buffer between Privilege Manager agents and the Privilege Manager server(s) to limit server exposure. Use nginx, F5, or Windows Application Request Routing 3.0 and URL Rewrite in IIS on a DMZ Server, to prevent a direct connection between Agent endpoints and your Privilege Manager web server(s). Alternatively, Azure Bus can be used, to prevent Agent endpoints connecting directly to your Privilege Manager web server(s).

Secret Server - Optionally, Secret Server can be installed with Privilege Manager to use an authentication source and a storage vault for Privilege Manager credentials. Using Secret Server as the authentication source for Privilege Manager allows MFA options for login. Also, application role assignment can be assigned in Secret Server. If using Secret Server features (beyond authentication and vault storage for Privilege Manager), Secret Server should be on separate servers - for this, see [Secret Server + Privilege Manager Architectures](#).

Note: Every component of Privilege Manager can be made highly available to ensure a redundant architecture and to scale for future growth.

Privilege Manager can be setup for various types of authentication methods:

- Azure Active Directory Authentication
- NTLM for local webserver authentication
- ThycoticOne for Cloud Instances

Overview

- Minimum Cost HA Configuration.
- Single Site design, no native DR capacity. DR can be provided by means of VM replication if subnets are spanning locations, otherwise re-ip + DNS changes may be necessary.
- Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a dedicated AlwaysOn availability group configuration.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.
- Optionally, Privilege Manager can be integrated with Secret Server (installed on the same web servers or, preferably, on dedicated servers) for authentication and as a storage vault for Privilege Manager credentials. If using Secret Server features (beyond authentication and vault storage for Privilege Manager), Secret Server should be on separate servers.

Requirements

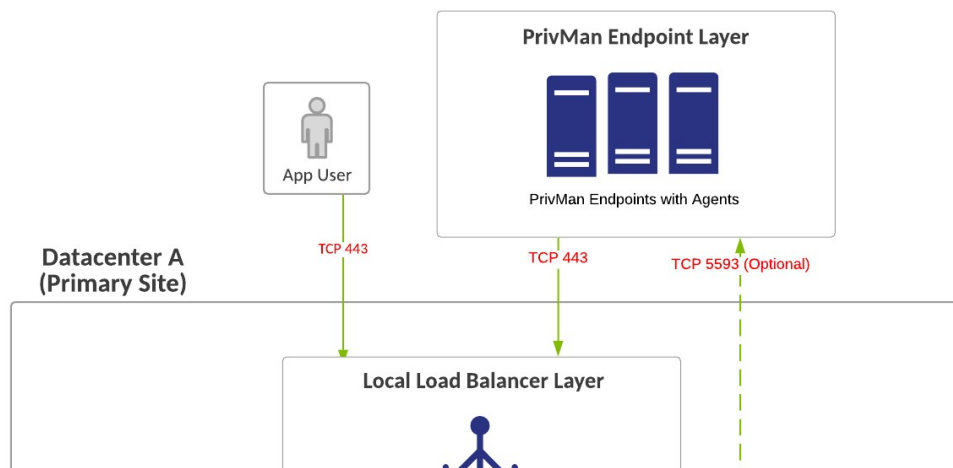
- SQL Standard Edition – Basic Availability Group Configuration.
- Local load balancers can be utilized for all web server nodes.
- Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures.
- SQL Quorum Ports - <http://dsfnet.blogspot.com/2013/04/windows-server-clustering-sql-server.html>

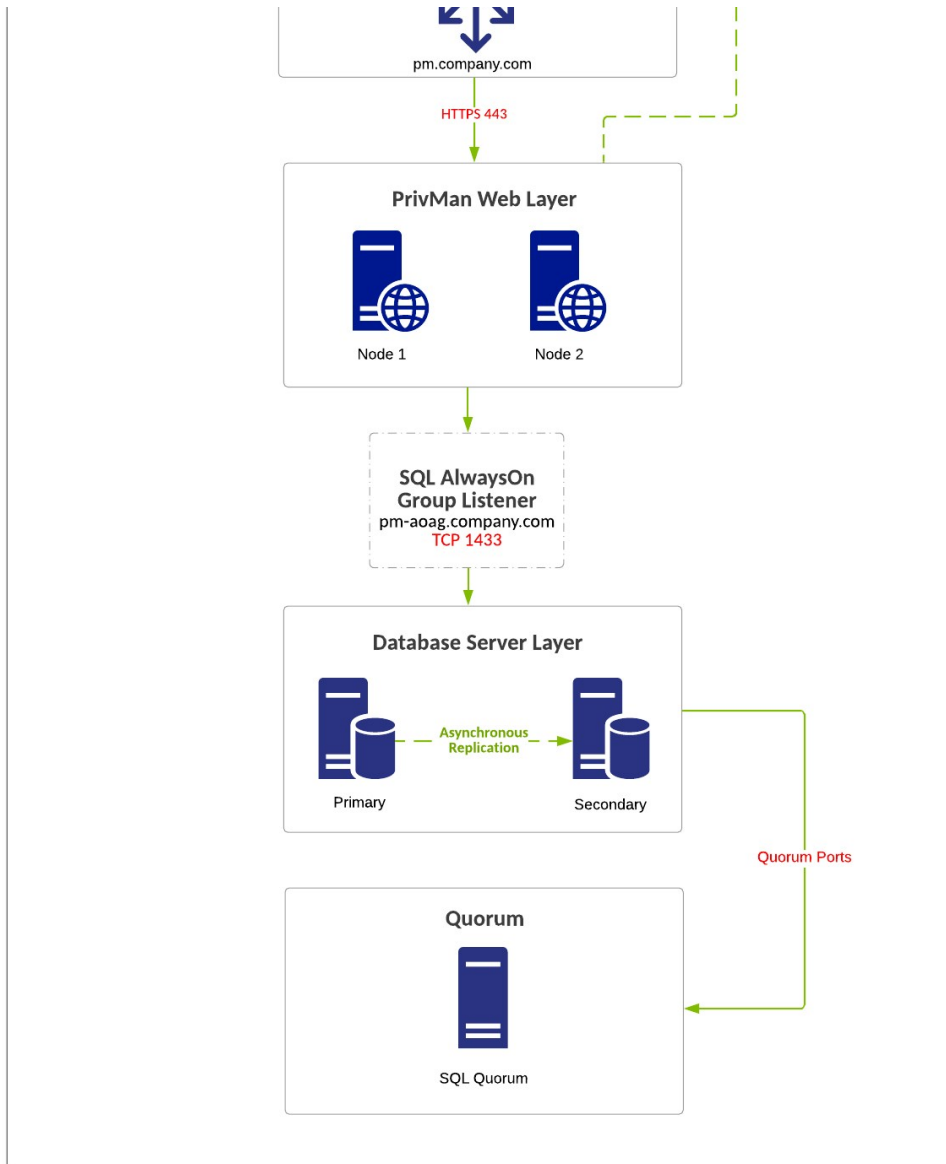
Virtual IP/Virtual Computer Object Requirements

- pm.company.com:443 (Load Balancer).
- pm-aoag.company.com:1433 (created as part of SQL AlwaysOn Configuration).
 - pm-aoag.company.com computer object/Virtual IP.
- Windows Failover Cluster Object (created as part of Windows Failover Clustering Configuration).
 - computer object/Virtual IP.
 - 1 additional virtual IP addresses may be required as part of Windows Failover Cluster for single site design for the network configuration of the Failover Cluster.

Diagram

Note: The reference for this diagram is A-1.





Overview

- Minimum Cost HA Configuration.
- Single Site design, no native DR capacity. DR can be provided by means of VM replication if subnets are spanning locations, otherwise re-ip + DNS changes may be necessary.
- Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a dedicated AlwaysOn availability group configuration.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.
- Optionally, Privilege Manager can be integrated with Secret Server (installed on the same web servers or, preferably, on dedicated servers) for authentication and as a storage vault for Privilege Manager credentials. If using Secret Server features (beyond authentication and vault storage for Privilege Manager), Secret Server should be on separate servers.

Requirements

- SQL Standard Edition – Basic Availability Group Configuration.
- Local load balancers can be utilized for all web server nodes.
- Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures.
- SQL Quorum Ports - <http://dsfnet.blogspot.com/2013/04/windows-server-clustering-sql-server.html>

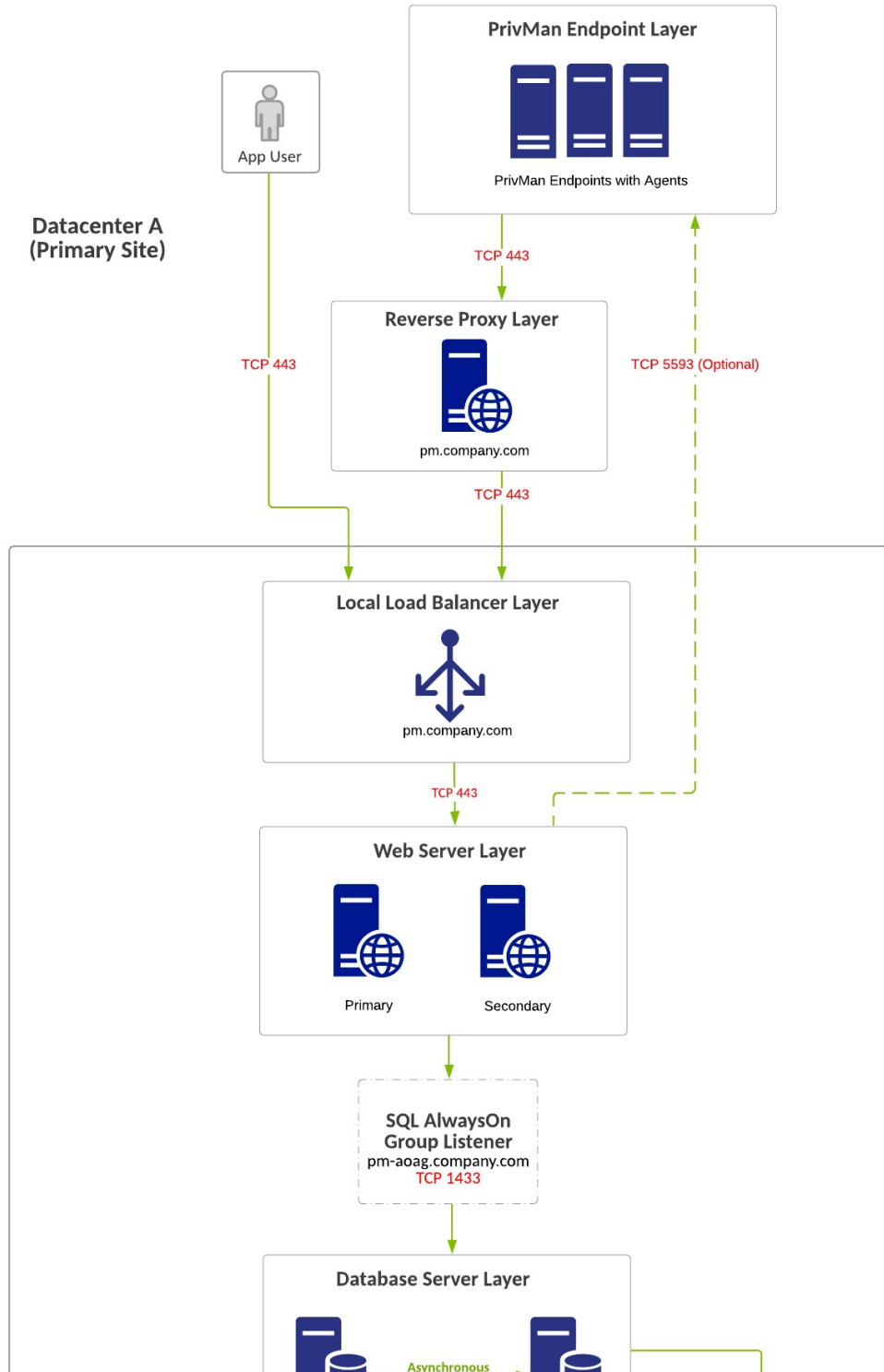
Virtual IP/Virtual Computer Object Requirements

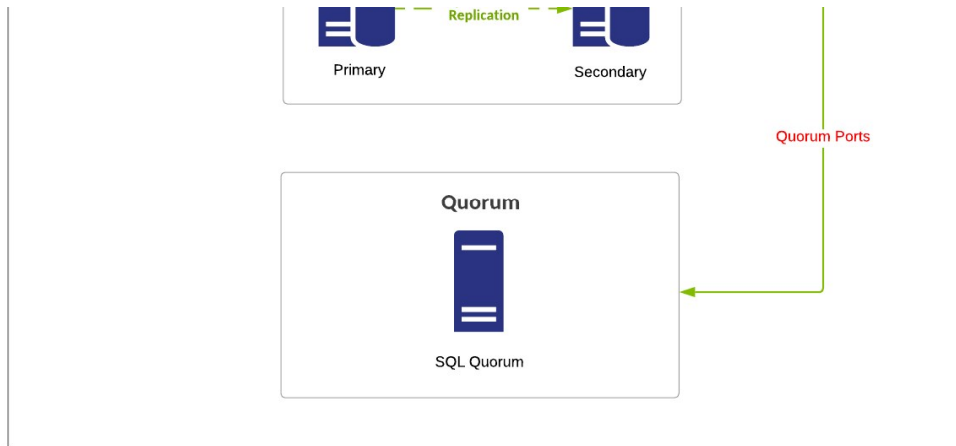
- pm.company.com:443 (Load Balancer).
- pm-aoag.company.com:1433 (created as part of SQL AlwaysOn Configuration).
 - pm-aoag.company.com computer object/Virtual IP.
- Windows Failover Cluster Object (created as part of Windows Failover Clustering Configuration).

- o computer object/Virtual IP.
- o 1 additional virtual IP addresses may be required as part of Windows Failover Cluster for single site design for the network configuration of the Failover Cluster.

Diagram

Note: The reference for this diagram is A-2.





Overview

- Minimum Cost HA Multi-Site Configuration – Lower Infrastructure Footprint for DR..
- Multi-Site Design. SQL AlwaysOn configurations will be asynchronous for Privilege Manager database.
- DR site acts at temporary site only with no intention for long-term usage. Services in DR site being down can incur downtime.
- If a Global Load Balancer is not used, the Reverse Proxy and App Users will need to be directed to the DR Web Node, typically via DNS or IP updates.
- Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a dedicated AlwaysOn availability group configuration.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself. Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a separate AlwaysOn availability group configuration.

Requirements

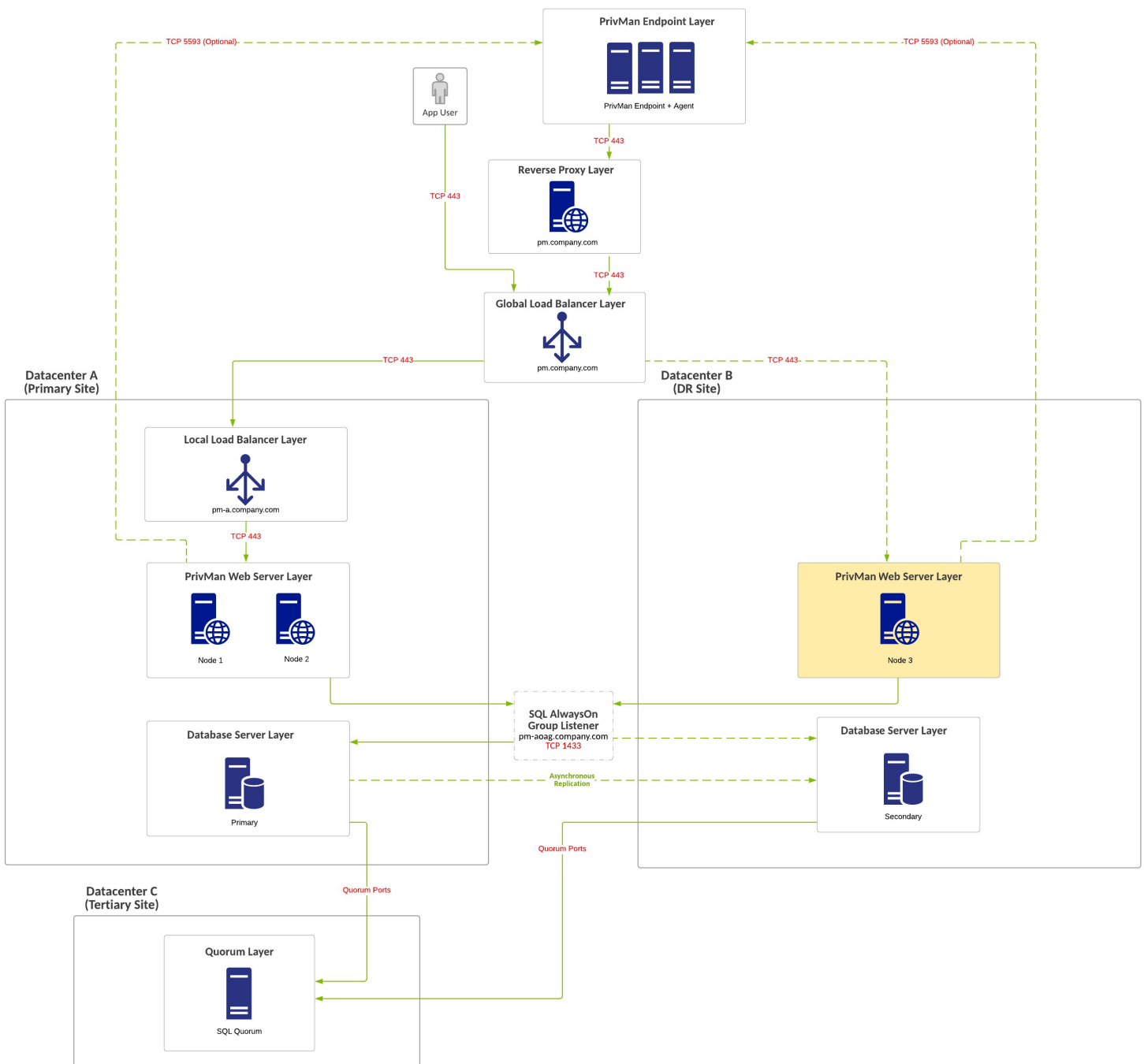
- SQL Standard Edition – Basic Availability Group Configuration.
- If no Global Load Balancers Exist due to costs/infrastructure missing, local load balancers can be utilized for all web server nodes but DNS change may be required if primary location goes offline.
- Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures.
- SQL Quorum Ports - <http://dsfnet.blogspot.com/2013/04/windows-server-clustering-sql-server.html>

Virtual IP/Virtual Computer Object Requirements

- pm.company.com:443 (Load Balancer).
 - pm-a.company.com (Local Load Balancer).
- pm-aoag.company.com:1433 (created as part of SQL AlwaysOn Configuration).
 - pm-aoag.company.com computer object/Virtual IP.
- Windows Failover Cluster Object (created as part of Windows Failover Clustering Configuration).
 - computer object/Virtual IP.
 - 1 additional virtual IP addresses may be required as part of Windows Failover Cluster for single site design for the network configuration of the Failover Cluster.

Diagram

Note: The reference for this diagram is B.



Overview

- Average Cost HA Multi-Site Configuration - Lower Infrastructure Footprint for DR.
- Multi-Site Design. SQL AlwaysOn configurations will be asynchronous for Privilege Manager database.
- Secondary SQL Node at Primary Site for Planned Failover "Patching", Secondary SQL Node in DR Site for Unplanned Failover.
- DR site can act as permanent secondary site for long term use.
- Database requires manual failover at primary or DR location.
- Global Load Balancers are configured to force all traffic to go to primary site unless primary site is down (priority group activation).
- Web node in DR Site is inactive and manually activated when failover is needed.
- If the data centers have low latency between networks, it may be possible to leave the PrivMan web server in DR online, active, and processing work.
- Some customers may choose to use a separate web reverse proxy, as shown, or azure service bus configuration for Privilege Manager agent TCP 443 communication.
- Optionally, Privilege Manager can be integrated with Secret Server (installed on the same web servers or, preferably, on dedicated servers) for authentication and as a storage vault for Privilege Manager credentials. If using Secret

Server features (beyond authentication and vault storage for Privilege Manager), Secret Server should be on separate servers.

Requirements

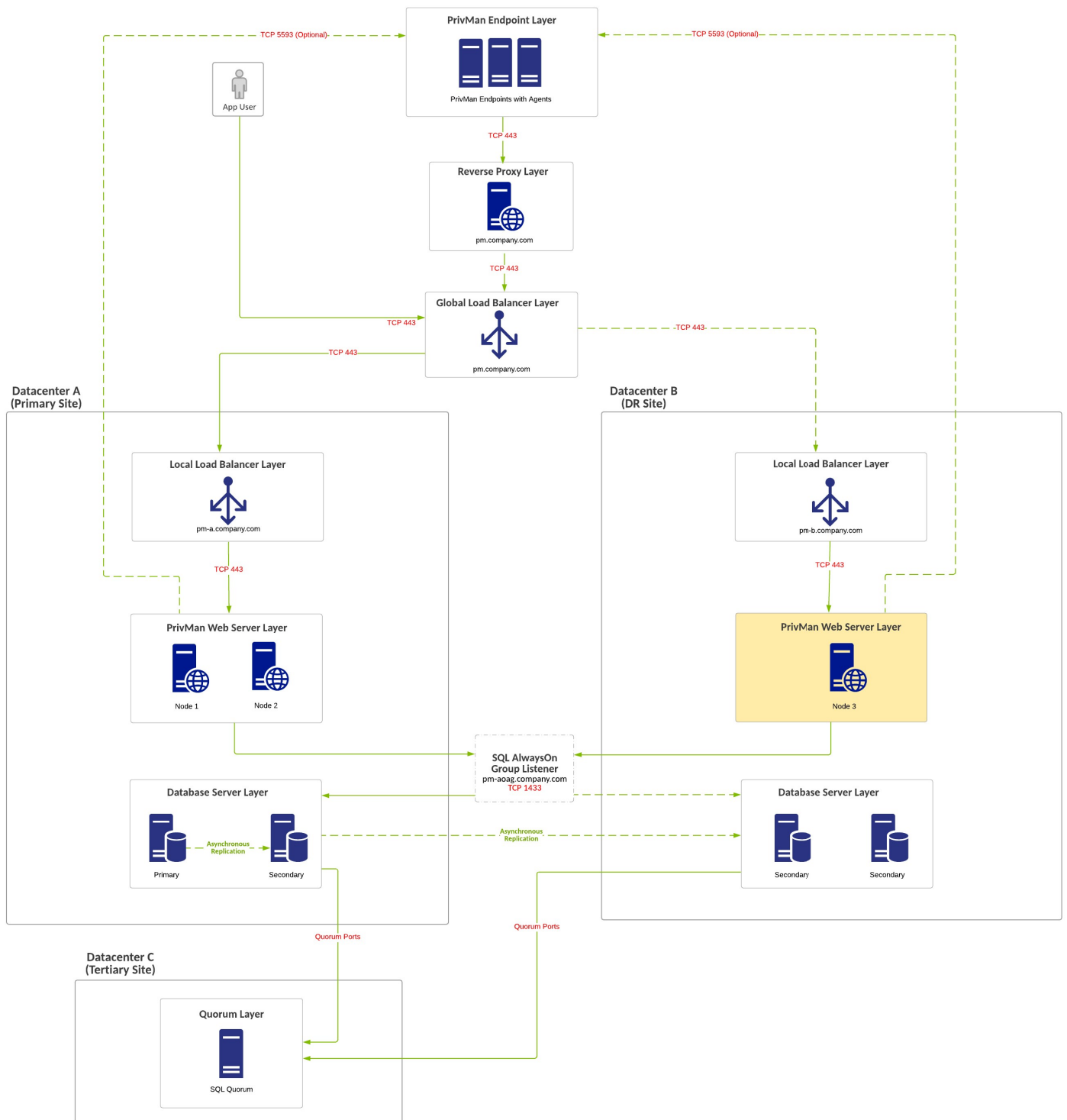
- SQL Standard Edition.
- Global and Local Load Balancers.
- Configuring a file share witness for SQL quorum voting is recommended. A cloud witness or DFSR share is recommended for witness configuration. Simultaneous failure of both SQL nodes in the primary location can cause the failover cluster to not survive.
- SQL Quorum Ports - <http://dsfnet.blogspot.com/2013/04/windows-server-clustering-sql-server.html>

Virtual IP/Virtual Computer Object Requirements

- pm.company.com:443 (Global Load Balancer).
 - pm-a.company.com:443 (Local Load Balancer).
 - pm-b.company.com:443 (Local Load Balancer).
- pm-aoag.company.com:1433 (created as part of SQL AlwaysOn Configuration).
 - pm-aoag.company.com computer object/Virtual IP.
 - 2 virtual IP addresses may be required as part of this configuration.
- Windows Failover Cluster Object (created as part of Windows Failover Clustering Configuration).
 - computer object/Virtual IP.
 - 2 additional virtual IP addresses may be required as part of Windows Failover Cluster for single site design for the network configuration of the Failover Cluster representing both networks at each respective site.

Diagram

Note: The reference for this diagram is C.



Overview

- Highest Cost HA Multi-Site Configuration – Higher Infrastructure Footprint in DR.
- Multi-Site Design. SQL AlwaysOn configurations will be asynchronous for Privilege Manager database.
- Secondary SQL Node at Primary Site for Planned Failover "Patching", Secondary SQL Node in DR Site for Unplanned Failover.

- DR site can act as permanent secondary site for long term use.
- Database requires manual failover at primary or DR location.
- Global Load Balancers are configured to force all traffic to go to primary site unless primary site is down (priority group activation).
- Web nodes in DR Site is inactive and manually activated when failover is needed.
- If the data centers have low latency between networks, it may be possible to leave the PrivMan web server in DR online, active, and processing work.
- Some customers may choose to use a separate web reverse proxy, as shown, or azure service bus configuration for Privilege Manager agent TCP 443 communication.
- Optionally, Privilege Manager can be integrated with Secret Server (installed on the same web servers or, preferably, on dedicated servers) for authentication and as a storage vault for Privilege Manager credentials. If using Secret Server features (beyond authentication and vault storage for Privilege Manager), Secret Server should be on separate servers.

Requirements

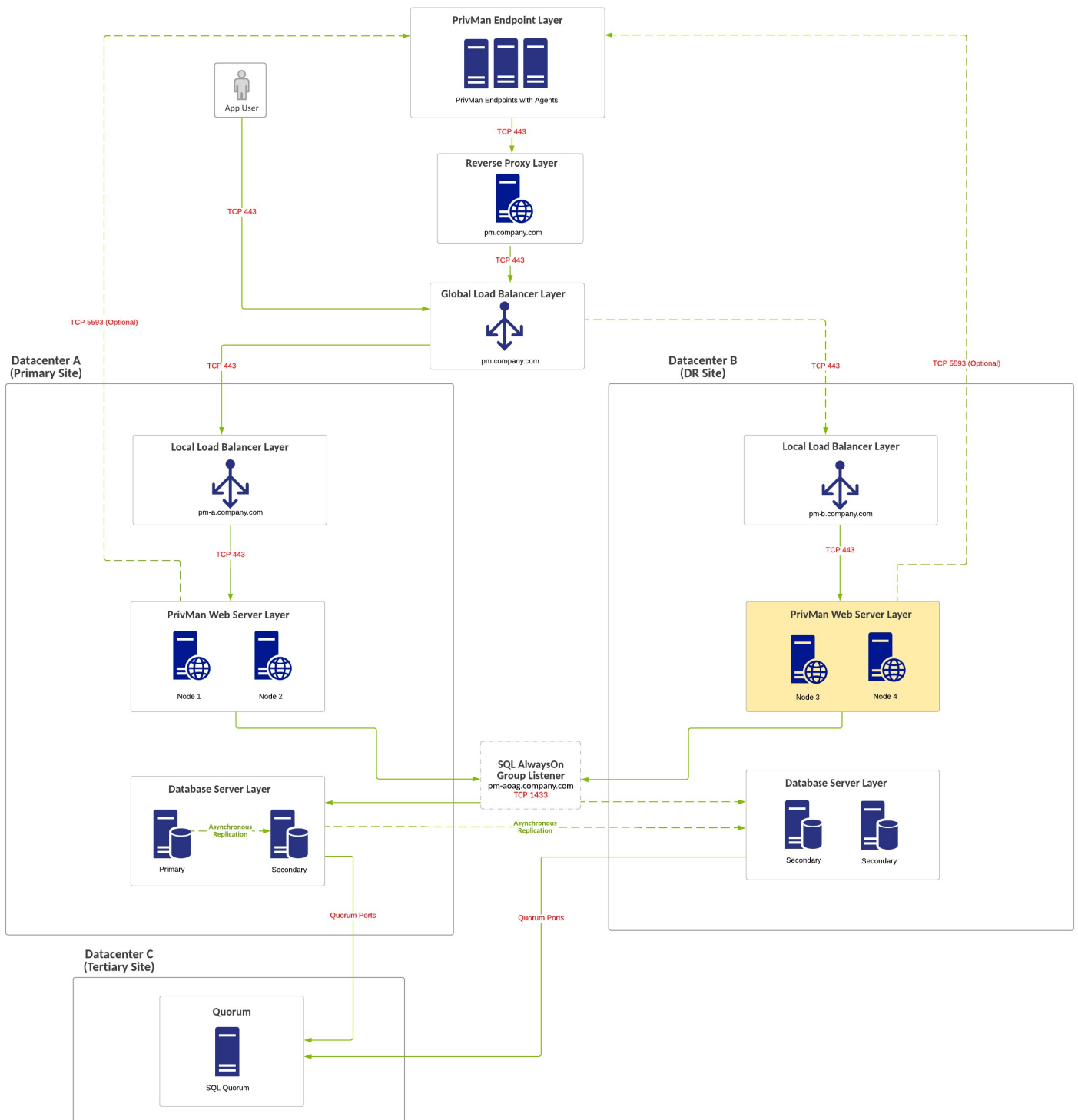
- SQL Standard Edition.
- Global and Local Load Balancers.
- Configuring a file share witness for SQL quorum voting is recommended. A cloud witness or DFSR share is recommended for witness configuration. Simultaneous failure of both SQL nodes in the primary location can cause the failover cluster to not survive.
- SQL Quorum Ports - <http://dsfnet.blogspot.com/2013/04/windows-server-clustering-sql-server.html>

Virtual IP/Virtual Computer Object Requirements

- pm.company.com:443 (Global Load Balancer).
 - pm-a.company.com:443 (Local Load Balancer).
 - pm-b.company.com:443 (Local Load Balancer).
- pm-aoag.company.com:1433 (created as part of SQL AlwaysOn Configuration).
 - pm-aoag.company.com computer object/Virtual IP.
 - 2 virtual IP addresses may be required as part of this configuration.
- Windows Failover Cluster Object (created as part of Windows Failover Clustering Configuration).
 - computer object/Virtual IP.
 - 2 additional virtual IP addresses may be required as part of Windows Failover Cluster for single site design for the network configuration of the Failover Cluster representing both networks at each respective site.

Diagram

Note: The reference for this diagram is D.



Integration with Secret Server

Privilege Manager and Secret Server integration is supported in a co-hosted setting when installed on the same server or on separate servers. If integrated on separate servers, Privilege Manager communicates with Secret Server via Secret Server's REST API.

The benefits of Privilege Manager's integration with Secret Server include:

- Secret Server can be the authentication source for Privilege Manager, which:
 - Adds Secret Server's MFA login options to Privilege Manager logins.
 - Gives one place for role assignments for both products.
- Allows Privilege Manager to use Secret Server as a storage container. If Secret Server is used as a storage container for Privilege Manager credentials, Privilege Manager
 - creates Secrets for each local credential managed by Privilege Manager.
 - creates Secrets for each Configuration Credential stored in Privilege Manager. This includes credentials used for Foreign Systems, such as AD Sync, ServiceNow, etc.
 - does not pull any changes for these Secrets. Privilege Manager only stores the credentials in Secret Server to utilize Secret Server's workflow options for other users to view.

When Secret Server is used as the authentication source for Privilege Manager, Role Permissions assigned in Secret Server are important and determine user access levels in Privilege Manager. Without Secret Server integration, Privilege Manager uses NTLM for WebServer and Azure AD as possible authentication sources.

Note: If you are a current customer with support hours for Thycotic Professional Services, you can discuss any of these diagrams in detail with one of our Professional Services Solutions Architects.

Overview

- Minimum-cost configuration with no shared storage requirement.
- RabbitMQ (for SS) is installed on the SS Web servers (typically in a cluster).
- Single-site design with no native DR capacity. DR can be provided by VM replication if subnets are spanning locations. Otherwise Re-IP + DNS changes may be necessary.
- PM is installed on separate Web servers.
- PM can integrate with SS for authentication and credential storage.
- PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.

Note: Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.

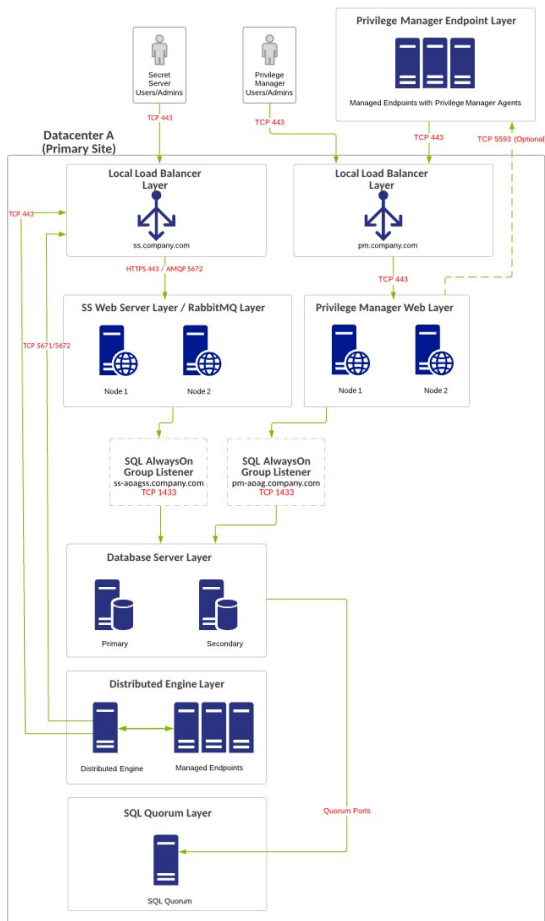
Requirements

- SQL Standard Edition with a basic availability group configuration.
- You can use local load balancers for all Web server nodes.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting.

Diagram

Note: The reference for this diagram is A-1.

Figure: Single Site with Minimum HA



Overview

- Minimum-cost HA configuration with no shared storage requirement.
 - RabbitMQ (for SS) is installed on the SS Web servers (typically in a cluster).
 - Single-site design with no native DR capacity. DR can be provided by VM replication if subnets are spanning locations. Otherwise Re-IP + DNS changes may be necessary.
 - PM is installed on separate Web servers.
 - PM can integrate with SS for authentication and credential storage.
 - PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.
- Note:** Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.
- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

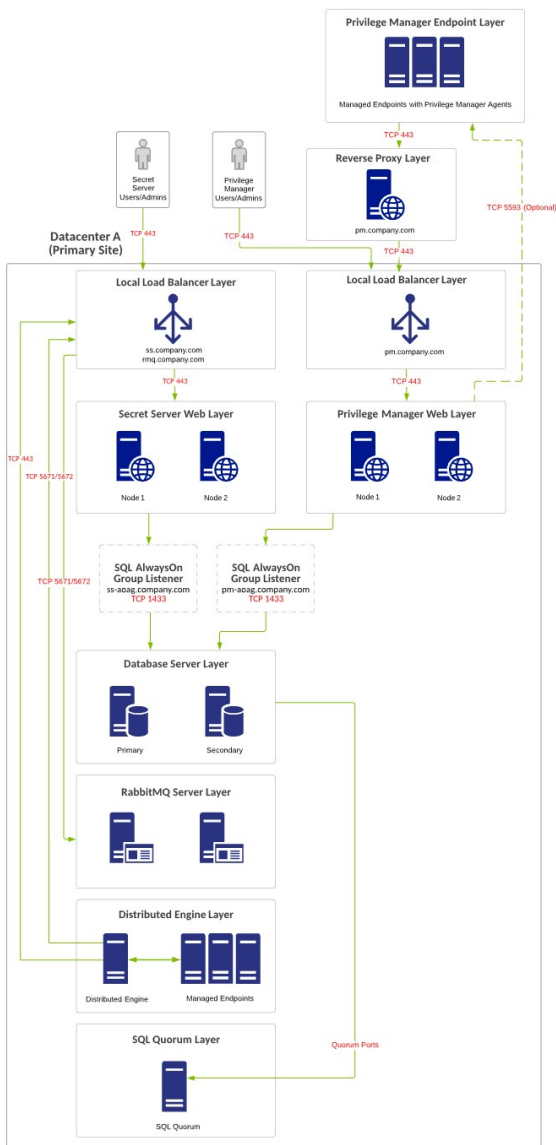
Requirements

- SQL Standard Edition with a basic availability group configuration.
- You can use local load balancers for all Web server nodes.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting.

Diagram

Note: The reference for this diagram is A-2.

Figure: Single Site with Minimum HA and Separate RabbitMQ



Overview

- Minimum-cost HA configuration with no shared storage requirement.
- RabbitMQ (for SS) is installed on the SS Web servers (typically in a cluster).
- SQL AlwaysOn configurations are either synchronous or asynchronous for the SS database and asynchronous only for the PM database.
- DR site acts as a temporary site only with no long-term use. Services in DR site being down can incur downtime.
- PM is installed on separate Web servers.
- PM can integrate with SS for authentication and credential storage.
- PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.

Note: Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.

- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

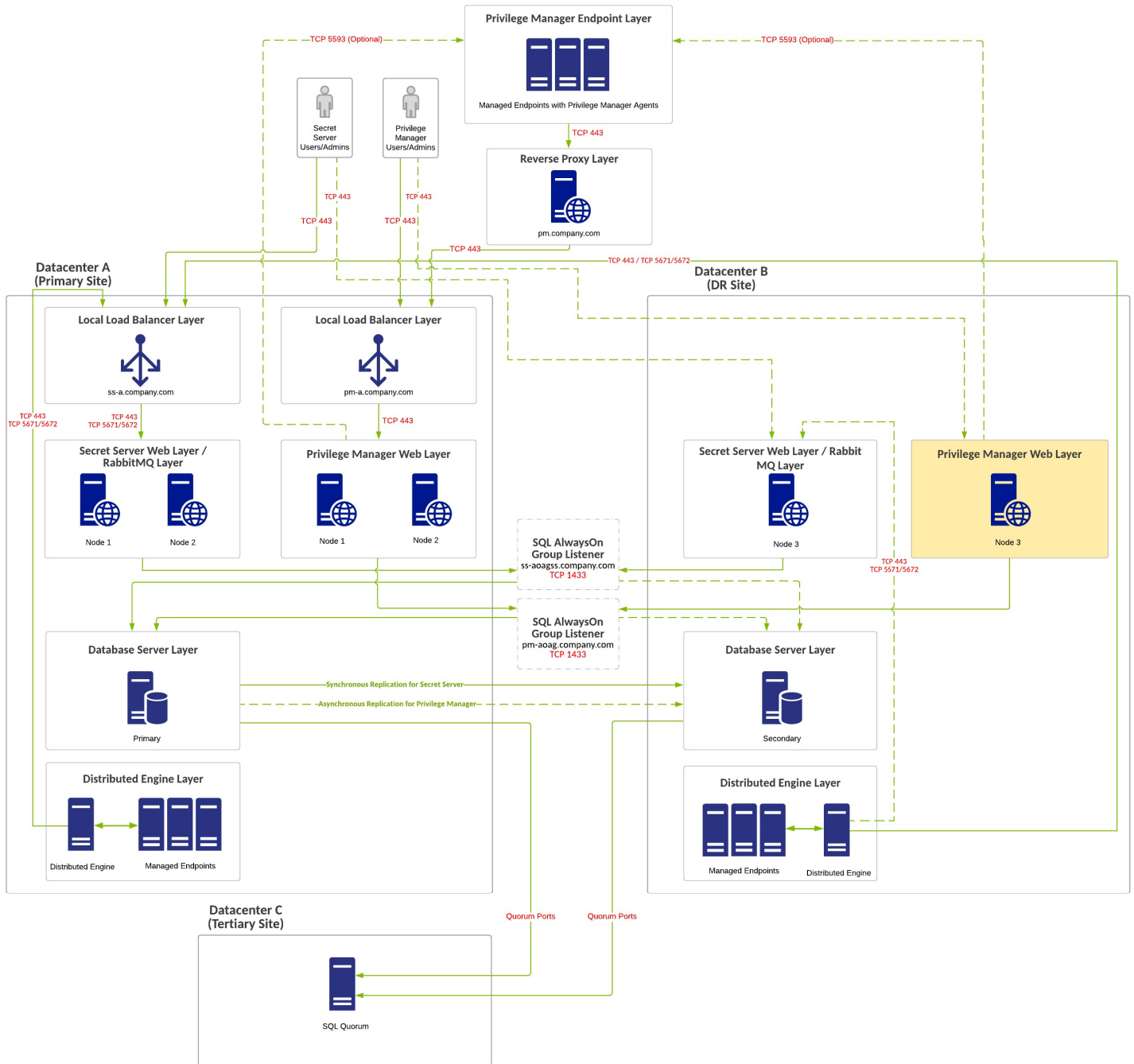
Requirements

- SQL Standard Edition with a basic availability group configuration.
- If global load balancers are not available due to cost or limited infrastructure, you can use local load balancers for all Web server nodes, but DNS change may be required if primary location goes offline.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting.

Diagram

Note: The reference for this diagram is B-1.

Figure: Multiple Site with Manual Failover



Overview

- Minimum-cost HA configuration with no shared storage requirement.
- RabbitMQ (for SS) is installed on the SS Web servers (typically in a cluster).
- SQL AlwaysOn configurations are either synchronous or asynchronous for the SS database and asynchronous only for the PM database.

- DR site acts as a temporary site only with no long-term use. Services in DR site being down can incur downtime.
- PM is installed on separate Web servers.
- PM can integrate with SS for authentication and credential storage.
- PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.
 - Note:** Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.
- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

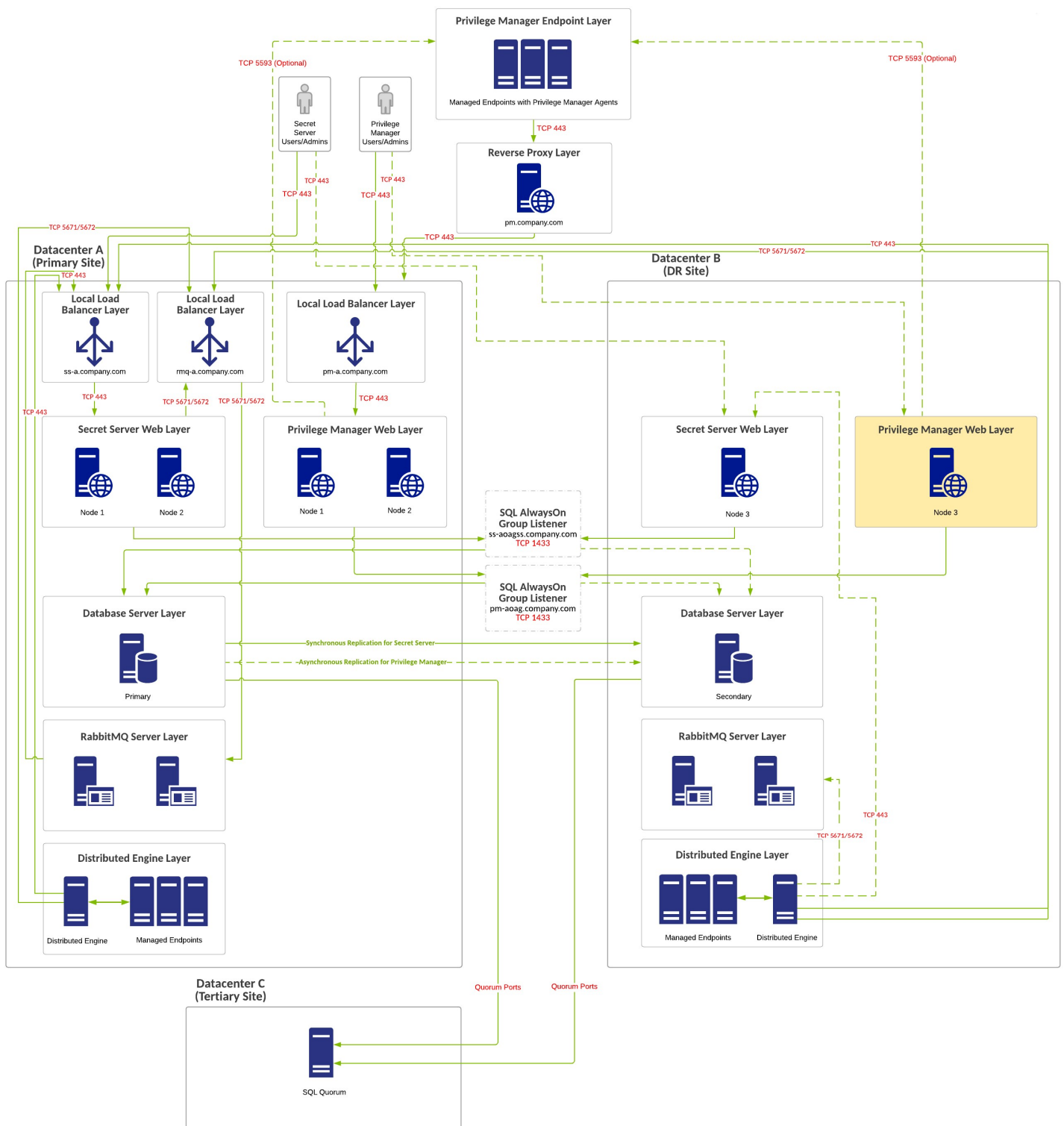
Requirements

- SQL Standard Edition with a basic availability group configuration.
- If global load balancers are not available due to cost or limited infrastructure, you can use local load balancers for all Web server nodes, but DNS change may be required if primary location goes offline.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting. We recommend a cloud witness.

Diagram

Note: The reference for this diagram is B-2.

Figure: Multiple Site with Manual Failover and Separate RabbitMQ



Overview

- Improved HA configuration with no shared storage requirement.

- RabbitMQ (for SS) is installed on the SS Web servers (typically in a cluster).
 - SQL AlwaysOn configurations are either synchronous or asynchronous for the SS database and asynchronous only for the PM database.
 - DR site acts as a temporary site only with no long-term use. Services in DR site being down can incur downtime.
 - PM is installed on separate Web servers.
 - PM can integrate with SS for authentication and credential storage.
 - PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.
- Note:** Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.
- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

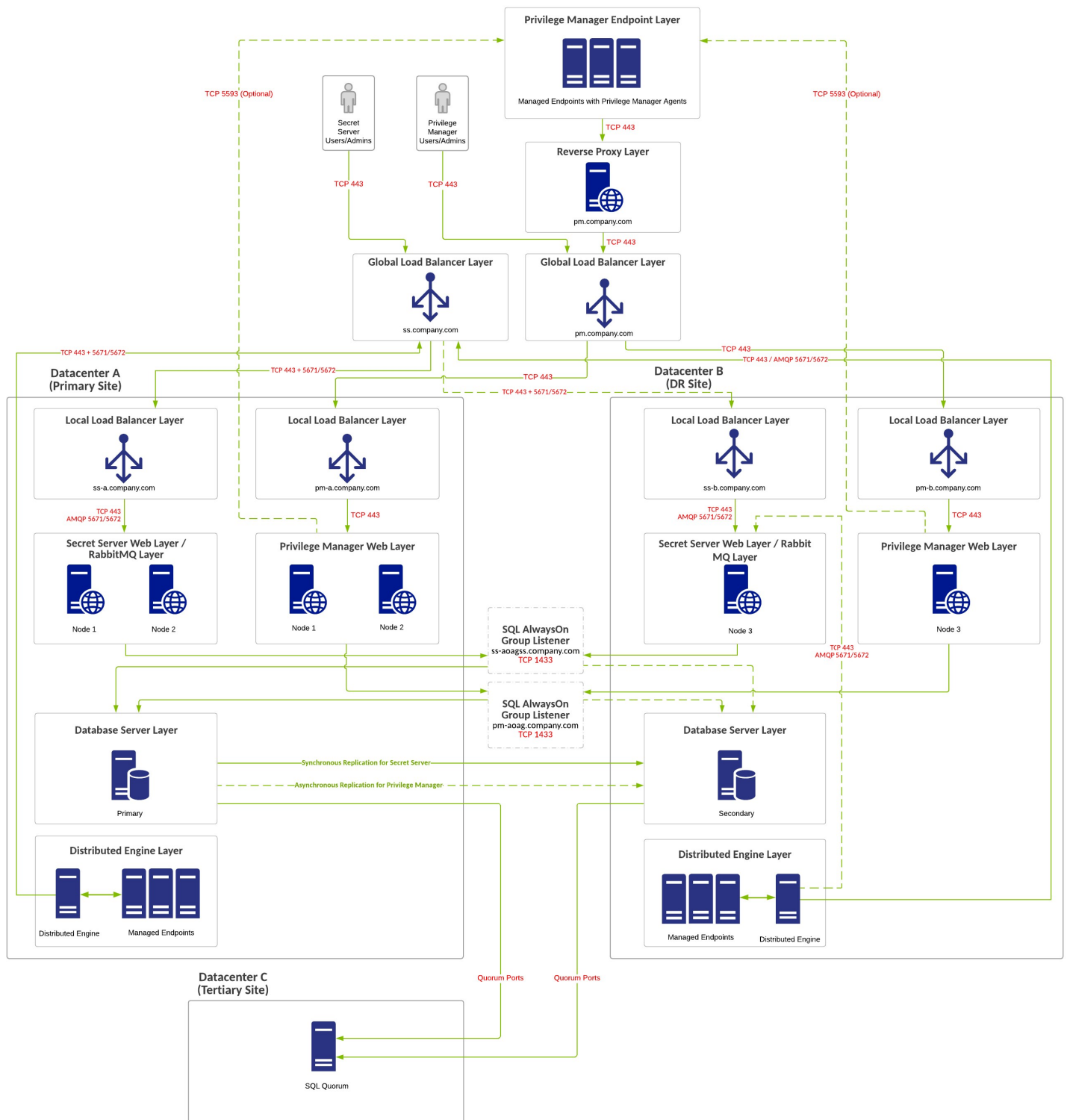
Requirements

- SQL Standard Edition with a basic availability group configuration.
- If global load balancers are not available due to cost or limited infrastructure, you can use local load balancers for all Web server nodes, but DNS change may be required if primary location goes offline.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting. We recommend a cloud witness.

Diagram

Note: The reference for this diagram is C-1.

Figure: Multiple Site with Automatic Failover



Overview

- Improved HA configuration with no shared storage requirement.

- RabbitMQ (for SS) is installed on dedicated servers (typically in a cluster).
- SQL AlwaysOn configurations are either synchronous or asynchronous for the SS database and asynchronous only for the PM database.
- DR site acts as a temporary site only with no long-term use. Services in DR site being down can incur downtime.
- PM is installed on separate Web servers.
- PM can integrate with SS for authentication and credential storage.
- PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.

Note: Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.

- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

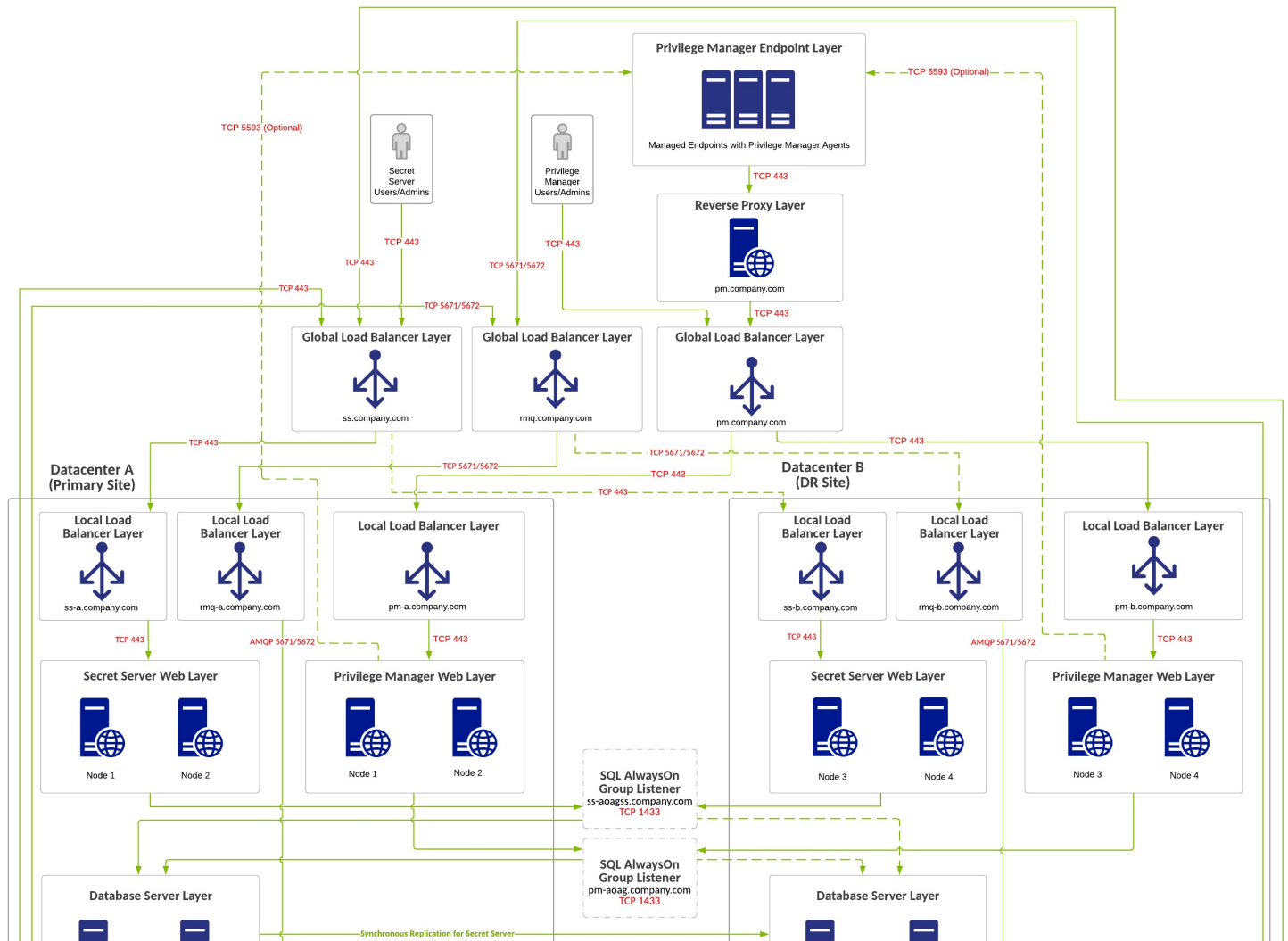
Requirements

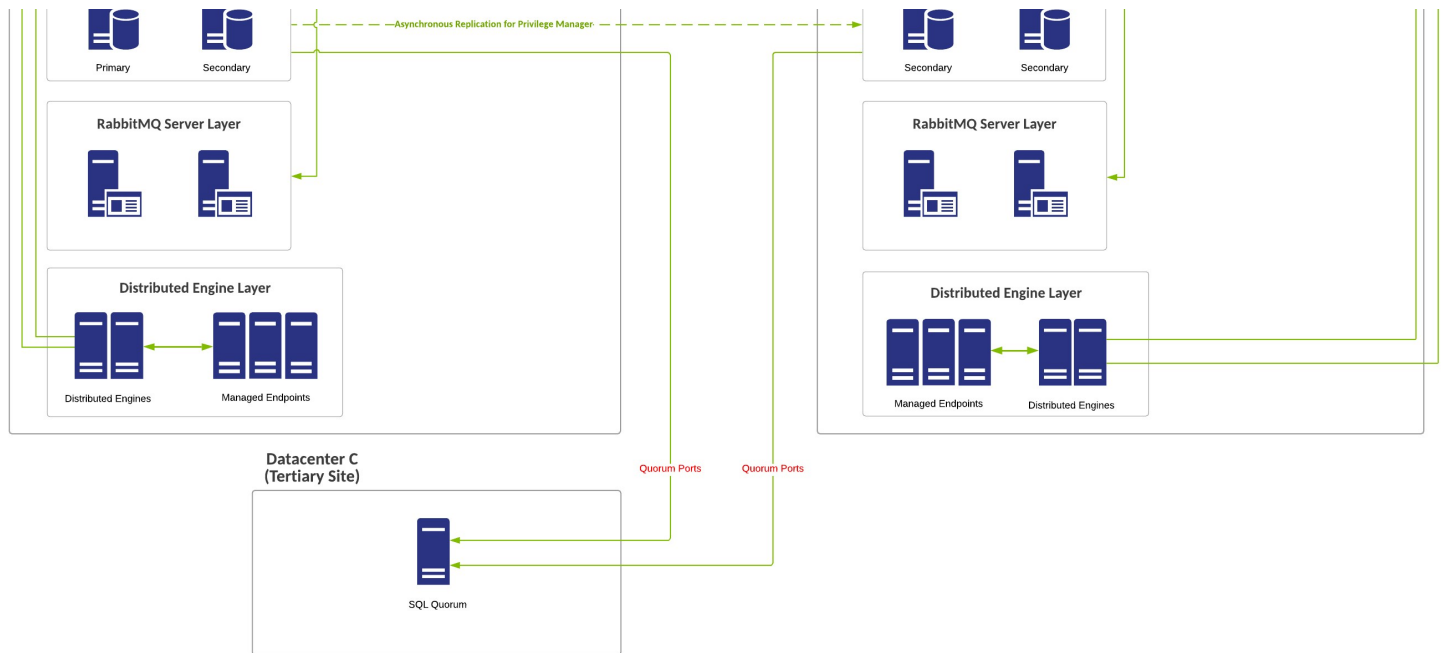
- SQL Enterprise Edition.
- Global and local load balancers.
- If global load balancers are not available due to cost or limited infrastructure, you can use local load balancers for all Web server nodes, but DNS change may be required if primary location goes offline.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting. We recommend a cloud witness.
- [Distributed Engine Ports](#).
- [SQL Quorum Ports](#).

Diagram

Note: The reference for this diagram is C-2.

Figure: Multiple Site with Automatic Failover and Separate RabbitMQ





Overview

- Best HA configuration with no shared storage requirement.
- RabbitMQ (for SS) is installed on dedicated servers (typically in a cluster).
- SQL AlwaysOn configurations are either synchronous or asynchronous for the SS database and asynchronous only for the PM database.
- DR site acts as a temporary site only with no long-term use. Services in DR site being down can incur downtime.
- PM is installed on separate Web servers.
- PM can integrate with SS for authentication and credential storage.
- PM can reside on the same database servers as SS or on separate ones, but SS and PM should not share the same database.

Note: Due to SQL basic availability groups with the Standard Edition, you need to have multiple SQL instances and a separate AlwaysOn availability group configuration.

- You can use a separate Web reverse proxy or Azure service bus configuration for Privilege Manager agent TCP 443 communication.

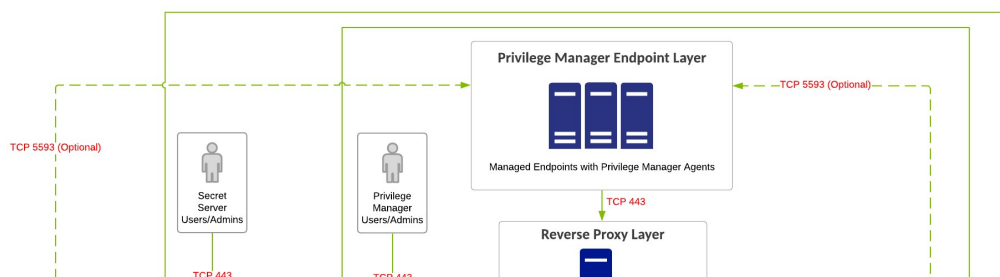
Requirements

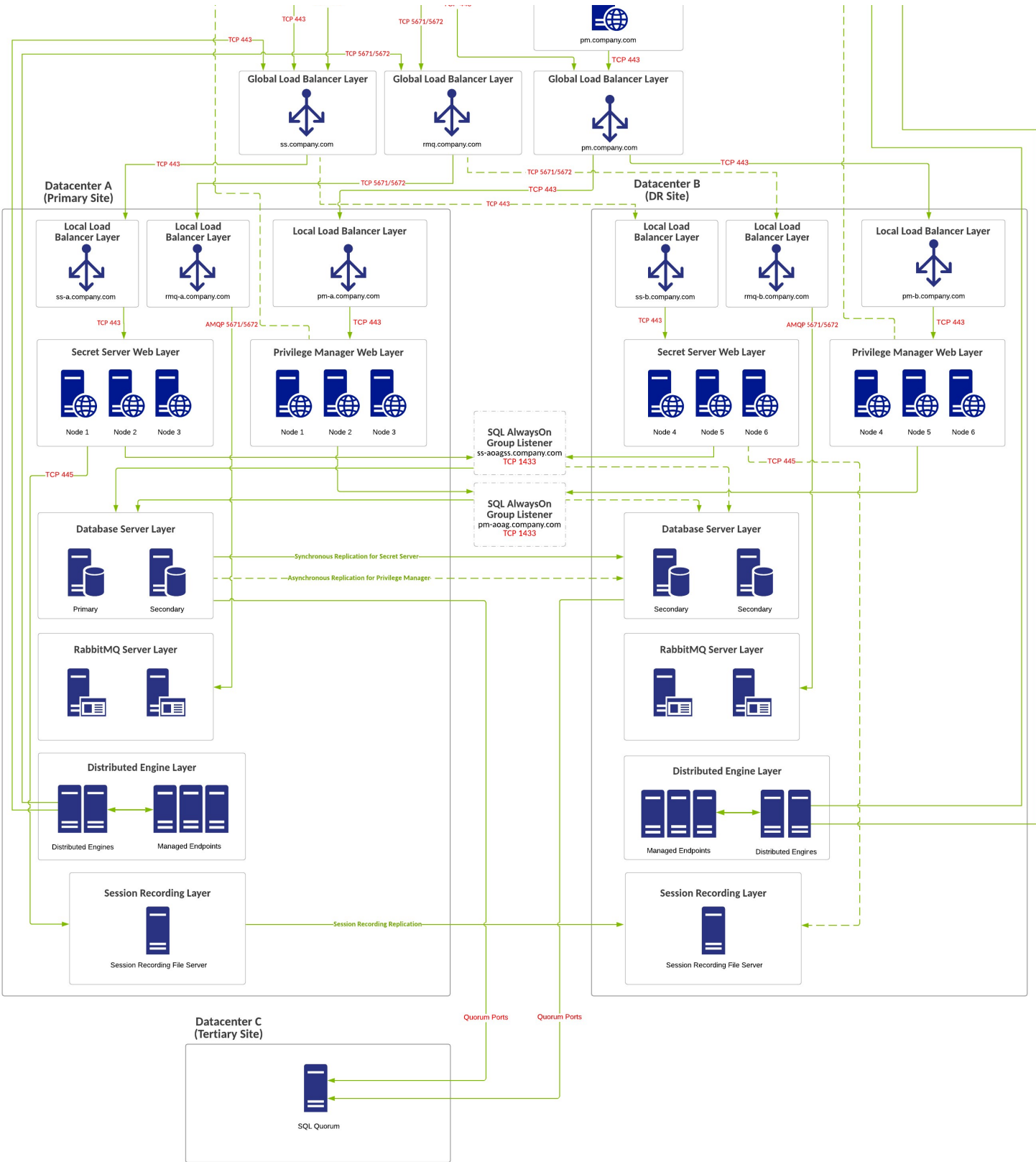
- SQL Enterprise Edition.
- Global and local load balancers.
- If global load balancers are not available due to cost or limited infrastructure, you can use local load balancers for all Web server nodes, but DNS change may be required if primary location goes offline.
- For SQL to stay online during single-node unplanned failures, you must configure a file-share witness for SQL quorum voting. We recommend a cloud witness.
- [Distributed Engine Ports](#).
- [SQL Quorum Ports](#).

Diagram

Note: The reference for this diagram is C-3.

Figure: Best Multiple Site with Automatic Failover and Separate RabbitMQ





Platforms

Although Privilege Manager provided feature parity across all supported operating system, there are best practices and some functional areas that differ and are detailed in this section's topics.

For platform specific details, refer to:

- [macOS](#)
- [Windows](#)

On macOS endpoints, best practices around system panes and user file and folder access varies from how these areas are managed on other operating system endpoints.

Recent changes introduced with Catalina and completed with Big Sur required a new approach from Privilege Manager.

The following topics are available to provide details on platform specific information:

- [macOS Extensions](#)
- [File/Folder Access](#)
- [Sudo Plugin](#)
- [Secure Token](#)
- [Best Practices Preference Panes](#)

Best Practices Preference Panes

This best practices section pertains to all macOS versions from **El Capitan** to (and including) **Catalina**.

Thycotic supports elevation without having to enter admin credentials for these preference panes:

- Date & Time
- Energy Saver
- Network

Other preference panes should not be used in elevation policies based on the nature of their function within the system. They can be elevated, but for certain actions, admin credentials may still be required. Changing those preference panes' settings should really be done by administrators only and not standard users, as designed by Apple®.

All macOS preference panes can be used in deny policies.

This section contains macOS specific user interface topics.

- [Best Practices System Preferences](#)
- [Best Practices Printer Installs](#)
- [Date & Time Preference Pane](#)
- [Energy Saver Preference Pane](#)
- [Network Preference Pane](#)
- [Preference Pane macOS](#)

Best Practices System Preferences

On macOS systems, users (Admin and Standard) can customize the System Preferences based on their macOS role scope. Details about macOS based customizations via the system preferences can be found at <https://support.apple.com/guide/mac-help/change-system-preferences-mh15217/mac>.

With Privilege Manager you can implement policies that provide application control to deny execution of all preference panes. Run as root policies are only supported and recommended for management of the following preference panes:

- [Date & Time](#)
- [Energy Saver](#)
- [Network](#)

The following rules apply for policy managed preference panes:

- If we have no policy for a given preference pane, the authorization for it is left to its system default.
- A preference pane's default authorization is restored when a policy for it is disabled/deleted.
- Managed preference pane defaults are restored on an uninstall.

Note: For preference panes that display the padlock icon, if you click the padlock to close it, you are required to enter admin credentials to unlock it again. Due to the way macOS caches preference pane authorizations, if a standard user has clicked the padlock icon, they will have to close and reopen System Preferences for the policy evaluation to be performed again.

Error Behavior of Preference Panes

When a particular preference pane is opened in the System Preferences application, XPC bundles for that particular preference pane are opened. These XPC bundles remain open until the System Preferences application is completely closed.

This behavior can result in apparent failed policy evaluations. Opening a preference pane that has previously been opened and evaluated without closing the System Preferences application following the initial opening, results in the policy evaluation not triggering again for that particular preference pane due to the XPC bundle remaining open.

For example, if you have a policy that requires approval of Date & Time preference pane changes and our notification dialog is cancelled and then Date & Time is opened again, our notification dialog is not presented to the user again. Instead, a sheet dialog indicates that the preference pane can't be loaded. In order to trigger policy evaluation again, System Preferences must be closed and then reopened.

User Based Behavior of Preference Panes

Standard User

Without an active policy, preference panes appear locked and standard users are not able to make changes. The exception is the Date & Time preference pane. Standard users are allowed to edit the clock appearance. Any changes here are specific to the user's session and can be modified without clicking the locked padlock icon despite what the text next to the icon says.

With an active policy, depending on its action, the following happens for:

- **Deny Execute | Deny Execute Message | Application Denied** - The user is presented with a dialog indicating they are denied running the preference pane. Depending on the usage of Deny Execute Message versus Application Denied Message and the version of macOS, each one may appear twice.
- **Application Justification** - The user is presented with the justification dialog. Once the user enters a justification and clicks Continue, all controls on the pane are enabled. Any changes made are saved. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane.
- **Application Warning** - The user is presented with the warning dialog. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. When the user clicks Continue, all controls on the pane are enabled and any changes made are saved.
- **Application Approval Request** - The user should be presented with the approval dialog. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. Once the user enters a reason and clicks Continue, the dialog for waiting for approval is displayed. If the user clicks Cancel in the waiting dialog, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. Depending on the Approval action (Allow or Deny), the following takes place:
 - **Allow** - All controls on the pane are enabled. Any changes made are saved.
 - **Deny** - macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane.

The following preference panes require admin credentials to make changes and should not be managed with a run as root policy that triggers a user dialog for justification or approvals:

- Parental Controls,
- [Printers & Scanners](#),
- Security & Privacy,
- Sharing,
- Time Machine, and
- Users & Groups

Admin User

Local admin users should not be managed by any policies requiring user interaction when the policy is triggered. For macOS endpoints the only type of policy would be to demote administrative rights for a particular preference pane by simply denying access.

Best Practices Printer Installs

To install and manage printers via the Printers and Scanners preference pane, standard users on macOS should be added as members of the **lpadmin** group. You can use Privilege Manager's [LSS user and group management features](#) to assist with this.

On macOS, adding a printer can happen in three ways. Two of those can be allowed through an elevation policy enabling a user to add a printer via

- an .app installation file directly or
- a .pkg driver installation directly.

The third option is where the Printers and Scanners preference pane is used to manually add a printer based on existing printer drivers. Refer to the link below for more information.

Under the first scenario, the application that is performing the install and configuration of the printer may prompt for admin credentials. If this is the case, you may need a policy that allows the application or applications provider by the printer vendor.

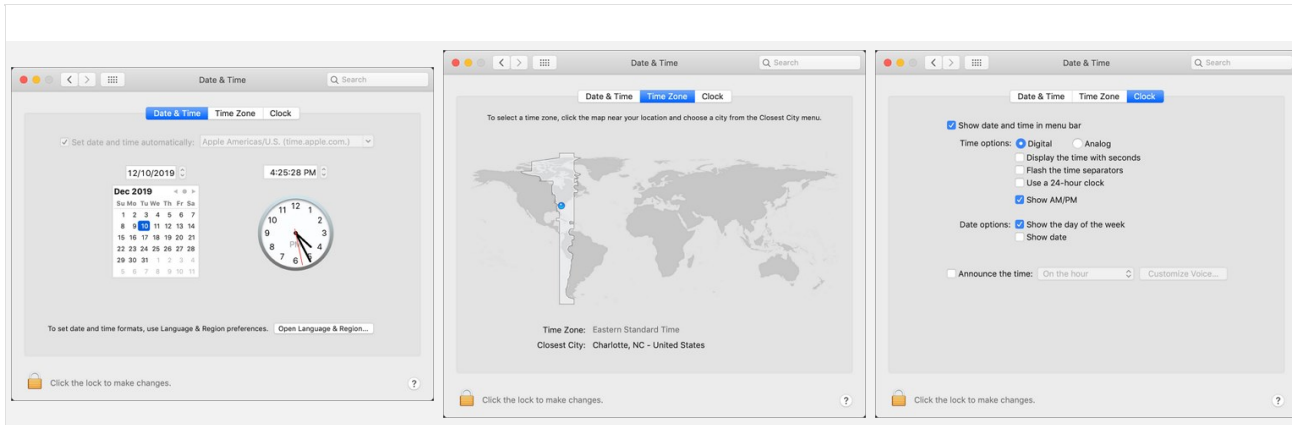
Refer to <https://support.apple.com/guide/mac-help/add-a-printer-on-mac-mh14004/10.15/mac/10.15> for the latest printer setup information from Apple.

Date & Time Preference Pane

Standard User - System Defaults

For standard users when Date & Time is not managed by a policy,

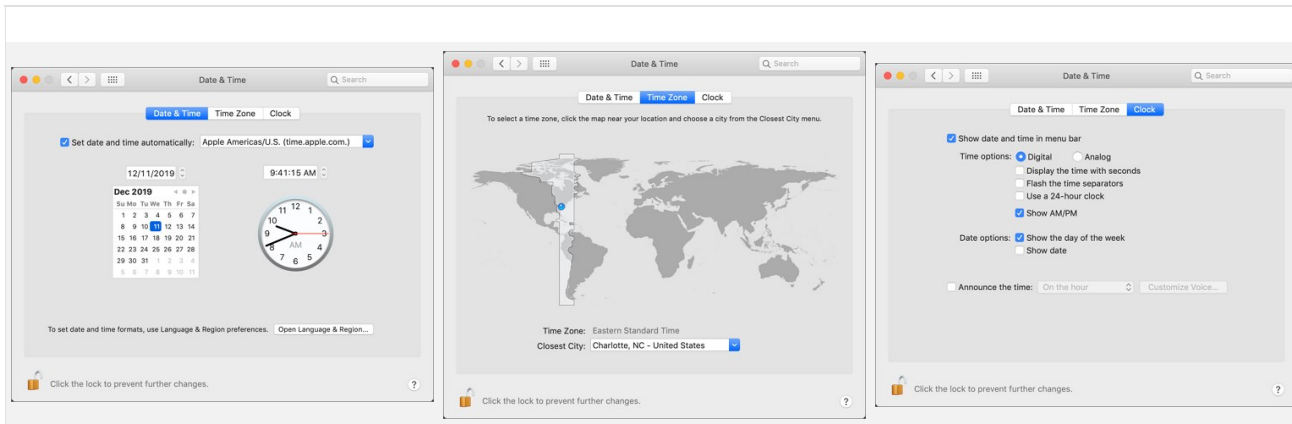
- all controls on the Date & Time tab are disabled and the padlock icon is closed.
- all controls on the Time Zone tab are disabled and the padlock icon is closed.
- all controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

For standard users when Date & Time is managed by a policy to run as root,

- all controls on the Date & Time tab are enabled and changes are saved.
- all controls on the Time Zone tab are enabled and changes are saved.
- all controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the padlock icon appears locked, by clicking on it a prompt is triggered to enter admin credentials. Once those admin credentials are entered, the padlock icon is unlocked and changes can be made.

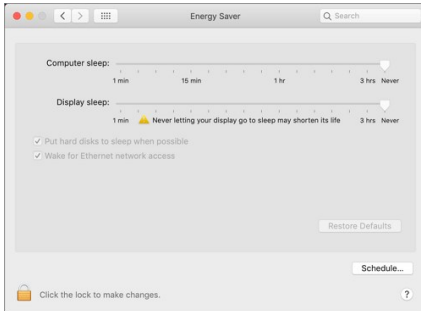
Using a policy to run as root is not necessary for local admin users.

Energy Saver Preference Pane

Standard User - System Defaults

For standard users when Energy Saver is not managed by a policy.

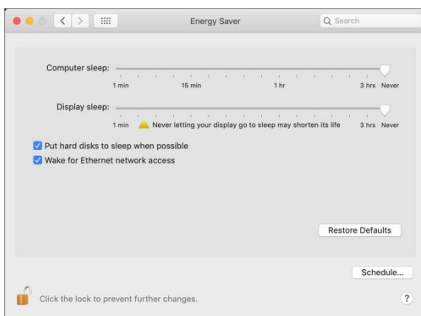
- all controls are disabled and the padlock icon is closed.
- Clicking the Schedule... button shows a panel with disabled controls.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

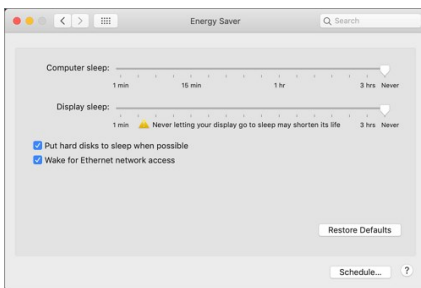
For standard users when Energy Saver is managed by a policy to run as root.

- all controls are enabled and changes are saved.
- Clicking the Schedule... button shows a panel with enabled controls. Any changes are saved.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the Energy Saver pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.



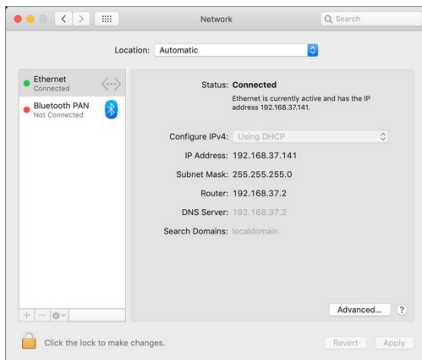
Using a policy to run as root is not necessary for local admin users.

Network Preference Pane

Standard User - System Defaults

For standard users when Network is not managed by a policy,

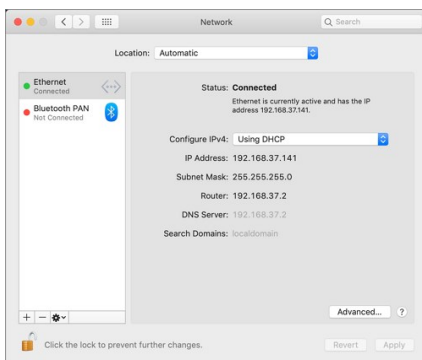
- all controls except for Location and Advanced are disabled and the padlock icon is closed.
- Clicking the Advanced... button opens a sheet depending on the network interface selected. Based on the selected interface, some elements may be enabled.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

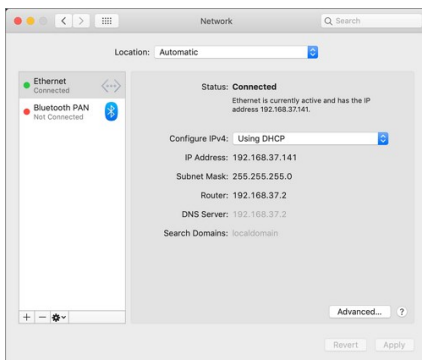
For standard users when Network is managed by a policy to run as root,

- all controls are enabled and changes are saved.
- Clicking the Advanced... button opens a sheet depending on the network interface selected. Based on the selected interface, elements are enabled.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the Network pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.



Using a policy to run as root is not necessary for local admin users.

Preference Pane macOS

A Preference Pane (abbreviated as `prefpane`) is a dynamically loaded plugin in Mac OS X. Introduced in Mac OS X v10.0, the purpose of a Preference Pane is to allow the user to set preferences for a specific application or the system by means of a graphical user interface.

Targeting Preference Panes

How do you target Preference Panes on macOS endpoints? On versions of Privilege Manager (10.3 and lower), you need to specify Preference Pane actions via filepath or file name. A chart is listed below for reference to some of the most common Preference Pane targets:

App Store	<code>com.apple.preferences.appstore.remoteservice</code>	<code>/System/Library/PreferencePanes/AppStore.prefPane/Contents/XPCServices/com.apple.preferences.appstore.remoteservice.xpc/Contents/MacOS/</code>
Date & Time	<code>com.apple.preference.datetime.remoteservice</code>	<code>/System/Library/PreferencePanes/DateAndTime.prefPane/Contents/XPCServices/com.apple.preference.datetime.remoteservice.xpc/Contents/MacOS/</code>
Energy Saver	<code>com.apple.preference.energysaver.remoteservice</code>	<code>/System/Library/PreferencePanes/EnergySaver.prefPane/Contents/XPCServices/com.apple.preference.energysaver.remoteservice.xpc/Contents/MacOS/</code>
Network	<code>com.apple.preference.network.remoteservice</code>	<code>/System/Library/PreferencePanes/Network.prefPane/Contents/XPCServices/com.apple.preference.network.remoteservice.xpc/Contents/MacOS/</code>
Parental Controls	<code>com.apple.preferences.parentalcontrols.remoteservice</code>	<code>/System/Library/PreferencePanes/ParentalControls.prefPane/Contents/XPCServices/com.apple.preferences.parentalcontrols.remoteservice.xpc/Contents/MacOS/</code>
Printers and Scanners	<code>com.apple.preference.printfax.remoteservice</code>	<code>/System/Library/PreferencePanes/PrintAndScan.prefPane/Contents/XPCServices/com.apple.preference.printfax.remoteservice.xpc/Contents/MacOS/</code>
Security & Privacy	<code>com.apple.preference.security.remoteservice</code>	<code>/System/Library/PreferencePanes/Security.prefPane/Contents/XPCServices/com.apple.preference.security.remoteservice.xpc/Contents/MacOS/</code>
Sharing	<code>com.apple.preferences.sharing.remoteservice</code>	<code>/System/Library/PreferencePanes/SharingPref.prefPane/Contents/XPCServices/com.apple.preferences.sharing.remoteservice.xpc/Contents/MacOS/</code>
Time Machine	<code>com.apple.prefs.backup.remoteservice</code>	<code>/System/Library/PreferencePanes/TimeMachine.prefPane/Contents/XPCServices/com.apple.prefs.backup.remoteservice.xpc/Contents/MacOS/</code>
User & Groups	<code>com.apple.preferences.users.remoteservice</code>	<code>/System/Library/PreferencePanes/Accounts.prefPane/Contents/XPCServices/com.apple.preferences.users.remoteservice.xpc/Contents/MacOS/</code>

Catalina Preference Pane Behavior

Refer to [Best Practices System Preferences](#) for details.

Introduced with Catalina and fully implemented with Big Sur, Apple announced the deprecation of kernel extensions and replaced them with system extensions that leverage the Endpoint Security framework

Kernel Extension (KEXT) vs. System Extension (SYSEX)

The Privilege Manager macOS agent is composed of several components and at the core of it are the KEXT and ThycoticACSvc daemon. These two work together to allow, deny, and elevate applications according to policy. With the deprecation of KEXTs in macOS Catalina, we are combining the functionality of these two components into the **com.thycotic.acsd** system extension that is hosted by **Privilege Manager.app**. In the KEXT version of the macOS agent, we relied on the KEXT to adjust processes so that they could run elevated. With the SYSEX version, we are no longer able to do that. We now leverage a sudo plugin to provide similar functionality.

Refer to [Using an MDM Profile for your Agent](#) for details on creating MDM profiles for your macOS agents.

Leveraging the AuthorizationDB

Many privileged operations are governed by rules in the authorizationdb and these rules determine what credentials are required to perform certain tasks depending on the right being authorized. To address restrictions placed on the macOS agent because we no longer have the fine-grained access and control provided by our KEXT, we're extending how we leverage the authorizationdb to provide least privilege for users on macOS endpoints. In addition, we'll be expanding upon this to provide coverage for more privileged operations.

Using a Privacy Preference Policy Control Configuration Profile Payload

The concept of [ICC](#) introduces Privacy Preference Policy Control (PPPC) configuration profile payload, which allow for enterprises to manage and ease, through Mobile Device Management (MDM), the installation process of products that leverage KEXTs and SYSEXs for their end-users. When properly configured, this eliminates the need for the user to deal with all of the dialogs below.

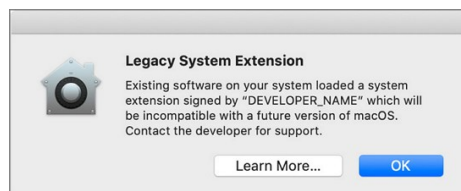
Thycotic can provide the necessary configuration payloads that can be loaded into or leveraged with your MDM solution.

Legacy Extensions (KEXT)

Effect on Privilege Manager Customers by Apple Deprecating Kernel Extensions In macOS

In 2019, Apple announced the deprecation of kernel extensions (KEXTS) in a future OS upgrade and that System Extensions should be used instead. Beginning in macOS 10.15.4, the use of kernel extensions will trigger a notification that software using this type of extension includes a deprecated API and an alternative should be provided by the vendor.

You may see this popup:



How is this Going to Affect Privilege Manager?

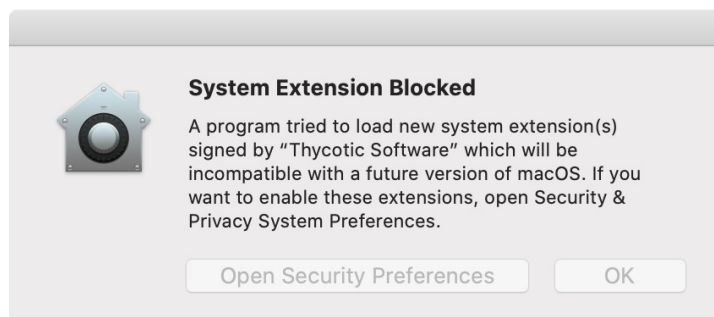
Thycotic plans to support Endpoint Security via system extension in Privilege Manager version 10.8.x to be delivered to support the Big Sur release. In the meantime, Privilege Manager will continue to function normally and no immediate action is required.

You can read more about legacy system extensions on [Apple's website](#).

Privilege Manager will continue to support kernel extensions for macOS versions that require them for the product to function.

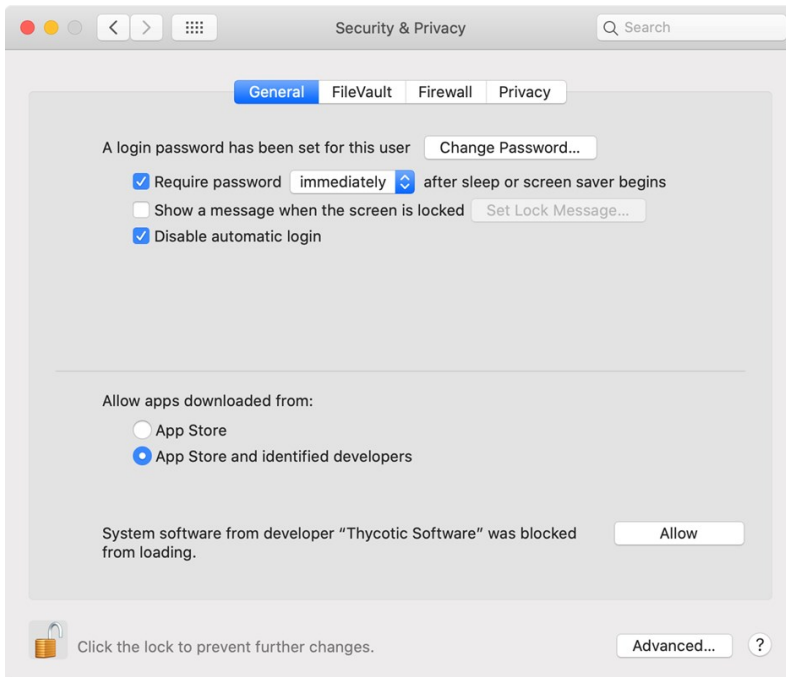
Catalina KEXT Warning

A user is informed that some product is trying to install a component that is trying to load a system extension and that their consent is required to allow it. Once Privilege Manager is installed, the user must allow it to satisfy this [Transparency, Consent, and Control \(TCC\) requirement](#). This means that an end-user approval is required for the product to be fully functional.



This dialog and the need to grant Full Disk Access to the SYSEX on Catalina and Big Sur can be remediated by Privacy Preference Policy Control (PPPC) configuration profile payloads.

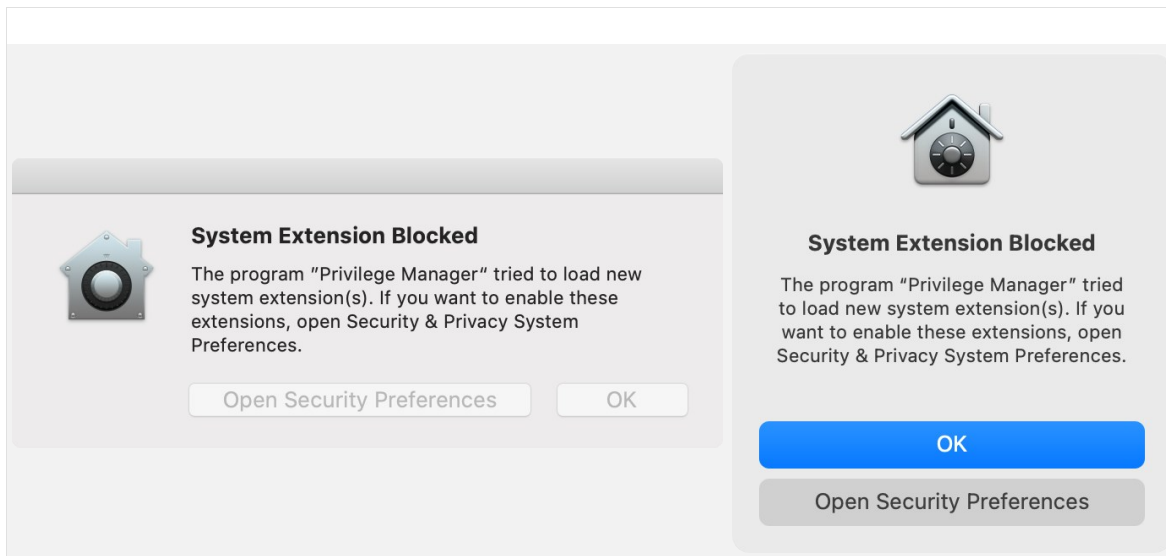
Here the user opens the **Security & Privacy** pane and clicks **Allow** for the Thycotic Software to run.



No further action is required by the user. [File and Folder access](#) may need to be enabled on the endpoint.

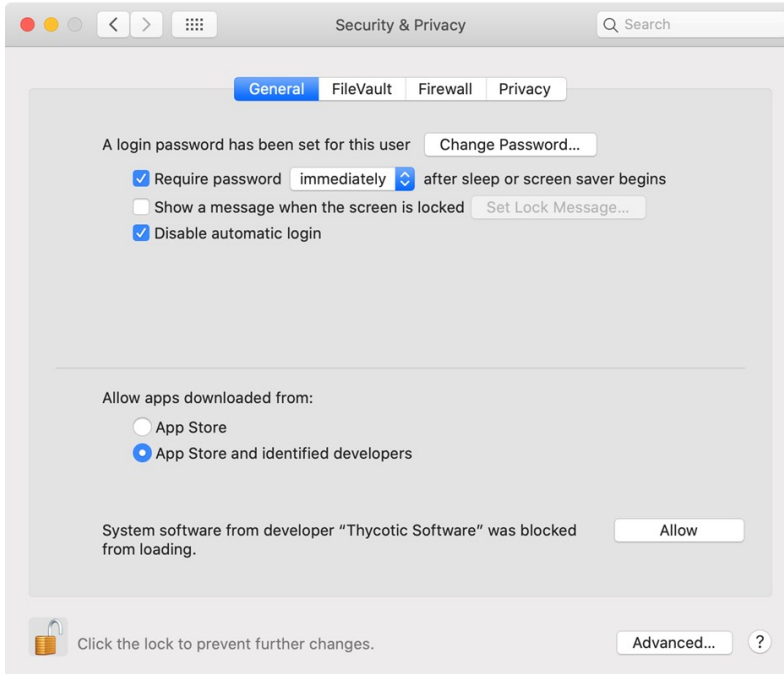
System Extensions (SYSEX)

With system extensions, the process is similar as outlined for the KEXT above.

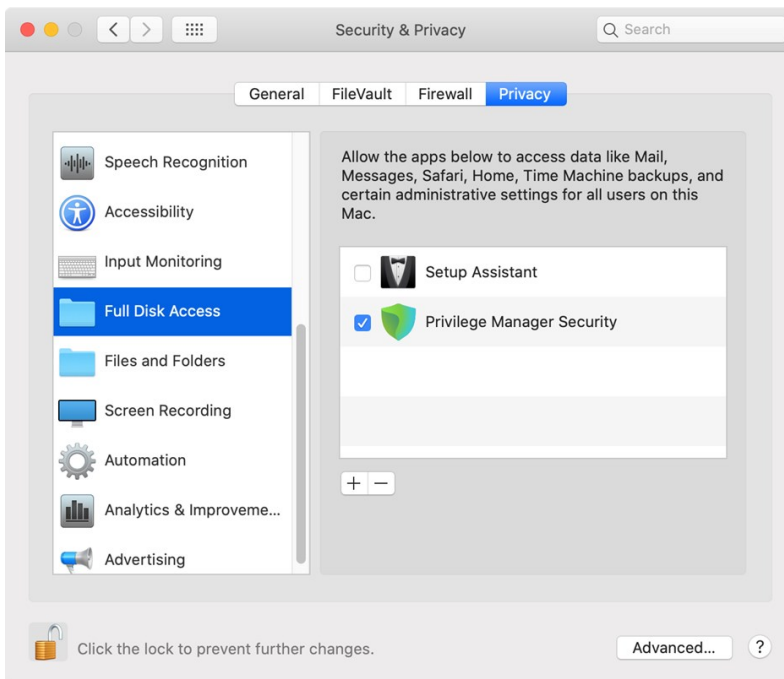


Catalina

Here the user opens the **Security & Privacy** pane and clicks **Allow** for the Privilege Manager system extension to run.

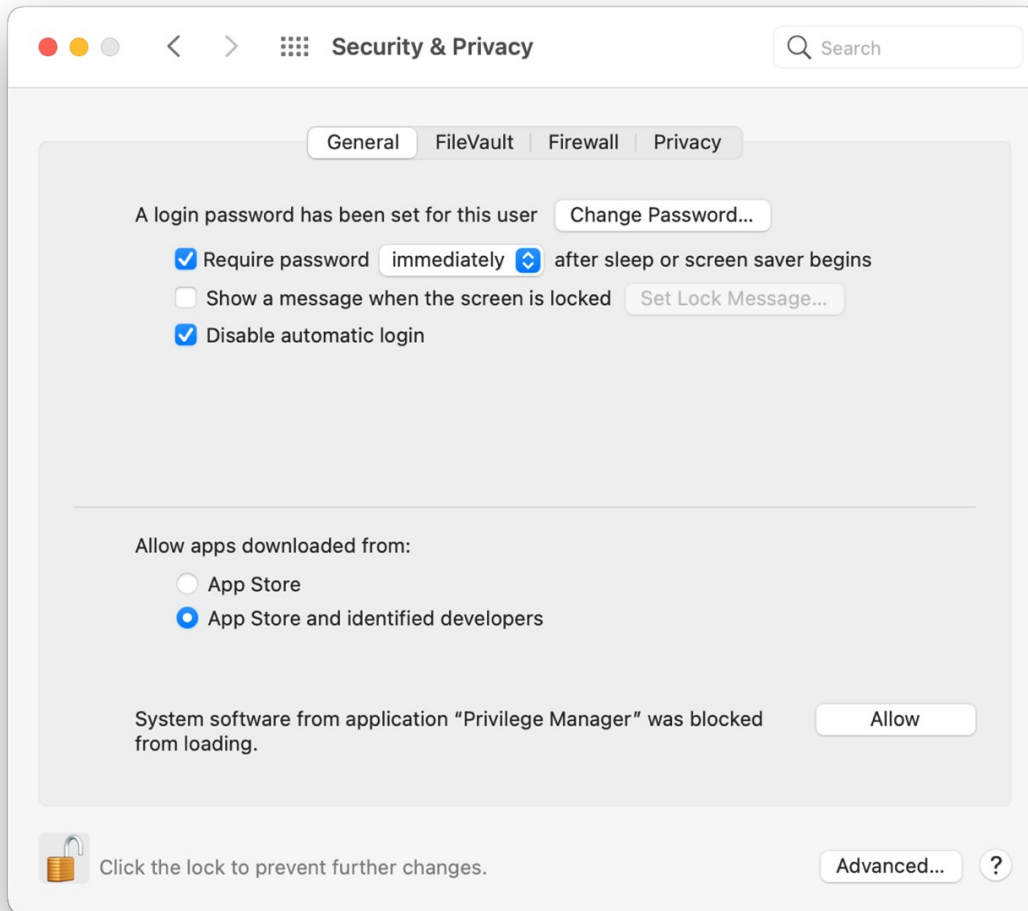


If you're not delivering a PPPC configuration profile via MDM to manage this, users will need to give Privilege Manager Security Full Disk Access.

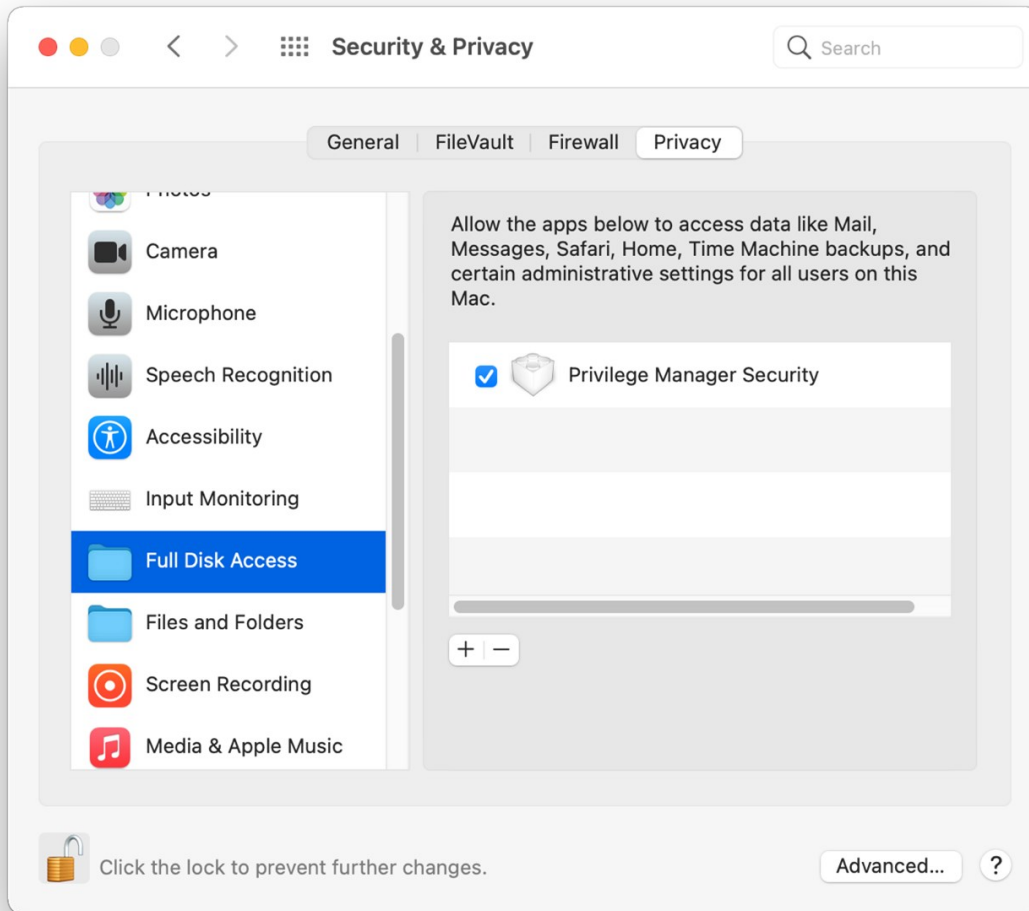


Big Sur

Here the user opens the **Security & Privacy** pane and clicks **Allow** for the Privilege Manager system extension to run.

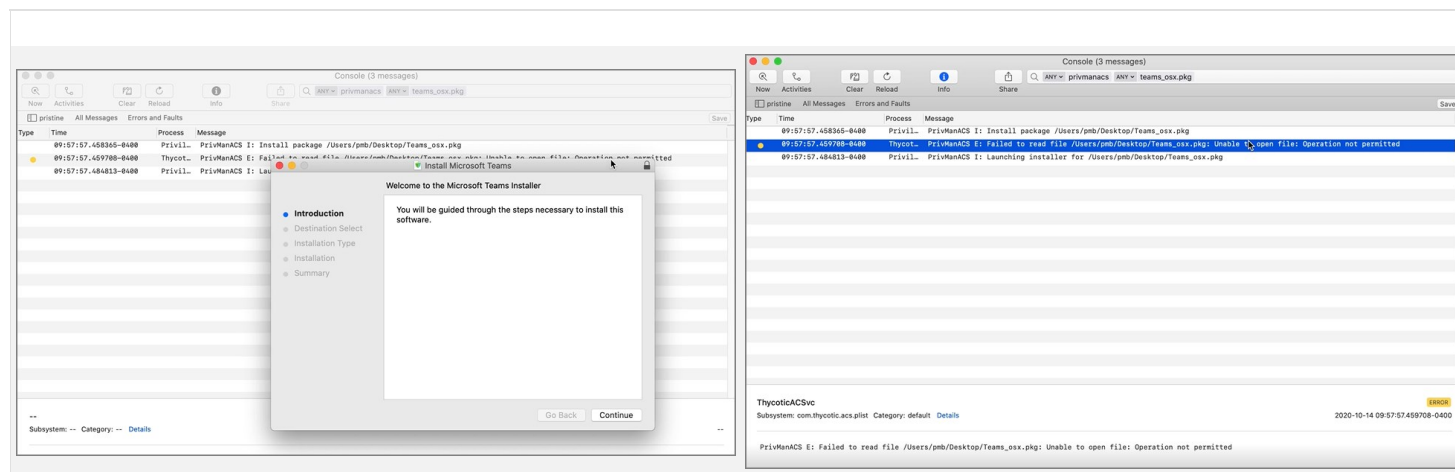


If you're not delivering a PPPC configuration profile via MDM to manage this, users will need to give Privilege Manager Security Full Disk Access.



Permissions determine who or what can access (view or alter) files on a computer. With the release of macOS Mojave (10.14), Apple introduced Transparency Consent and Control (TCC) to further limit the permissions and access granted to applications as they relate to user data and devices. With macOS Catalina (10.15), Apple extended this to prevent third-party daemons from accessing user data within certain folders. These include a user's Desktop, Documents, and Downloads folders. The user's Public folder is exempt from this restriction.

For example, on Catalina, when package (.pkg) installers are downloaded to a user's Desktop and there is a Privilege Manager policy governing them, an error like the following will be written to the [Unified Log](#).



In order to read files in these protected locations, third-party daemons need to be given the Full Disk Access (FDA) entitlement. On macOS Catalina, the FDA entitlement can't be granted manually to the daemon by a user. It must be provisioned by a TCC profile via a Mobile Device Management (MDM) solution.

macOS versions prior to Catalina do not experience this restriction.

Workaround via MDM Solution

If an MDM solution is in place, a TCC profile can be used to alleviate the problem. The below example can be used as a starting point. The example was specifically created for full disk access for a mobile configuration.

Either create a TCC profile based on this example for your environment or copy and paste the contents into a file and edit to meet your requirements.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0/EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Allows Privilege Manager to access all files on Catalina and higher</string>
<key>PayloadDisplayName</key>
<string>Privilege Manager ThycticACSvc Profile</string>
<key>PayloadIdentifier</key>
<string>com.thyctic.privilegemanager.thycticacsvc.01BF42EA-574B-47A3-8B06-CBA3731973EE</string>
<key>PayloadOrganization</key>
<string>Thyctic Software, LLC</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadUUID</key>
<string>01BF42EA-574B-47A3-8B06-CBA3731973EE</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
<array>
<dict>
<key>Allowed</key>
<true/>
<key>CodeRequirement</key>
<string>anchor apple generic and identifier "com.thyctic.ThycticACS" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = UJDHBB2D6Q)</string>
<key>Comment</key>
<string>Allow SystemPolicyAllFiles control for Privilege Manager ThycticACSvc</string>
<key>Identifier</key>
<string>com.thyctic.ThycticACS</string>
<key>IdentifierType</key>
<string>bundleID</string>
</dict>
</array>
</dict>
</dict>
</array>
<key>PayloadDescription</key>
<string>Allows Privilege Manager to access all files on Catalina and higher</string>
<key>PayloadDisplayName</key>
<string>Privilege Manager ThycticACSvc Profile</string>
<key>PayloadIdentifier</key>
<string>com.thyctic.privilegemanager.thycticacsvc</string>
<key>PayloadOrganization</key>
<string>Thyctic Software, LLC</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadScope</key>
<string>system</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>01BF42EA-574B-47A3-8B06-CBA3731973EE</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Secure Token is a macOS High Sierra or later account attribute, that is required to be added to a user account before that account can be enabled for FileVault on an encrypted Apple File System (APFS) volume. To help make sure that at least one account has a Secure Token attribute associated with it, a Secure Token attribute is automatically added to the first account to log into the OS login window on a particular Mac. Once an account has a Secure Token associated with it, it can create other accounts which will in turn automatically be granted their own Secure Token.

In order for Privilege Manager to support Secure Token during account creation and for password management, a local account with Secure Token enabled must be created on each macOS endpoint. The credentials for this account must be set as the Secure Token Management Credential.

When the Secure Token Management Credential is configured in the MacOS Agent Configuration, Privilege Manager will use this credential to create a local account on each macOS endpoint. The resulting managed local account will be used during account provisioning and password management to ensure that managed accounts are Secure Token enabled.

If the Secure Token Management Credential is removed in the MacOS Agent Configuration, the agent will use the non-Secure Token enabled method of password management and any new users created/managed will not be Secure Token enabled. Any existing users that are Secure Token enabled will fail to have their password managed because without a Secure Token Management Credential macOS will not allow the agent to manage the password of a Secure Token enabled user.

Note: The agent will ignore attempts to manage the service account. This includes provisioning and password management of the service account via LSS. You should not modify the service account, this includes changing its local password. Doing so may invalidate its configuration and cause the agent to fail password management.

Agent Configuration

To use the secure token with macOS Agents, the user credential needs to be established and linked to the macOS Agent configuration.

1. Navigate to **Admin | Configuration**, select the **Credentials** tab.
2. Click **Create**.

New User Credential

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Details

Name

Description

Settings

Account Name

Password [Edit](#)

3. Under Details enter a Name and Description.
4. Under Settings enter the **Account Name** and **Password** for the macOS user account with Secure Token access.
5. Click **Save Changes**.
6. Navigate to your macOS computer group and select **Agent Configuration**.

Application Control Agent Configuration Policy (MacOS)

General Change History Active Refresh More

Details

This configuration defines the default behavior for the Privilege Manager agent.

Name Application Control Agent Configuration Policy (MacOS)

Description This policy provides global configuration settings for the Mac OS Application Control Agent.

Platform Mac OS

Self-Elevation

This configuration setting enables the Request Elevation option in the right-click context menu. An application policy will need to be enabled to define what action is applied when a user requests an elevation.

Allow Self-Elevate No

Menu Text Request run as administrator

Intervals

Send Application Action Events 5 Minute(s)

Task Polling Interval 5 Minute(s)

Application Action Defaults

Quarantine Path /usr/local/thycotic/quarantine/

Secure Token (macOS)

Secure Token Enabled Management Credential

- In the **Secure Token Enabled Management Credential** field enter the macOS user credential you created in **step 2**.
- Click **Save Changes**.

Apple's Endpoint Security framework prevents Privilege Manager from performing process elevation of command-line binaries like done in the past. Privilege Manager's previous KEXT support for command line filtering in order to block, elevate, restrict, or allow commands is being replaced with a `sudo` plugin for Apple's newer OS versions starting with Catalina and newer.

Going forward, the `sudo` plugin supports a modular framework that allows third-party policy evaluation to govern whether a command is allowed to run. This architecture allows Privilege Manager to extend `sudo` functionality without replacing it and without introducing too much change to established workflows.

For **existing customers**, if privileged commands are already running via `sudo` and a Privilege Manager policy to elevate it, then there is nothing that needs to be changed. However, if some commands are elevated, specifically via policy and filters, those need to be re-evaluated and modified to utilize `sudo` to perform those commands.

Refer to the [macOS Application Approval Process via Sudo Plugin](#) topic. This topic explains the workflow for an approval policy elevating applications executed from a specific folder location.

Sudo Plugin Installation

In support of Big Sur and system extensions, the macOS agent install also installs the macOS `sudo` plugin at `/usr/local/libexec/sudo`. The plugin is owned by root and its configuration is located at `/etc/sudo.conf`.

Once Privilege Manager is added to a company's infrastructure, it discovers all accounts that exist on endpoints and allows Privilege Manager Administrators to control the exact membership of every local group via its Local Security features. This ensures the correct admin and root accounts are permanently set. Additionally, credentials will be controlled by enforcing password rotation on those accounts.





Privilege Manager's Application Control allows administrators to manage application activity on endpoint machines. Applications that require admin rights or root access can be automatically elevated, allowed applications are allow listed, and malicious applications are blocked.

Specific to the Windows Operating systems are the management of:

- [Client System Settings](#)
- [Adjust Process Rights Action](#)

The Client System Settings are common settings for standard Windows endpoint systems ranging from allowing installation of drivers to printers. These settings are deployed to Agents the same as any Policy.

By default each setting targets the default "Windows Computers" Computer Group.

8 Items		COMPUTER GROUP TARGET
DESCRIPTION		
<input checked="" type="checkbox"/> Add Devices Allow users to add drivers, installing drivers as necessary		Windows Computers 
<input checked="" type="checkbox"/> Add Printers Allow users to add printers, installing drivers as necessary		Windows Computers 
<input type="checkbox"/> Backup the System Allow users to perform system backup operations		
<input type="checkbox"/> Change the Date and Time Allow users to change the date, time and timezone		
<input type="checkbox"/> Change Network Adapter Settings Allow users to change the network adapter settings		
<input checked="" type="checkbox"/> Defragment the Disk Allow users to perform disk defragmentation operations		Windows Computers 
<input type="checkbox"/> Install Language Packs Allow users to install operating system display languages		
<input checked="" type="checkbox"/> Monitor Performance Allow users to run the Windows Performance Monitor utility		Windows Computers 

Changes to client system settings do not take effect until Policies have been cached and deployed to the agent. Review the agent status reports to see which agents have which Policies.

Add Devices

If active, users on Windows endpoints are allowed to add and install device drivers.

Add Printers

If active, users on Windows endpoints are allowed to add and install printer drivers.

Backup the Systems

If active, users on Windows endpoints are allowed to perform system backup operations.

Change the Date and Time

If active, users on Windows endpoints are allowed to change date, time, and timezone settings.

Change Network Adapter Settings

If active, users on Windows endpoints are allowed to change network adapter settings.

On Windows 7 endpoints with **Change Network Adapter Settings** active, do NOT enable high integrity when using the Administrative Rights action in policies.

Defragment the Disk

If active, users on Windows endpoints are allowed to perform disk defragmentation operations.

Install Language Packs

If active, users on Windows endpoints are allowed to install operating system display language packs.

Monitor Performance

If active, users on Windows endpoints are allowed to run the Windows Performance Monitor Utility.

The Privilege Manager UI

The Privilege Manager user interface, also referred to as the console, is launched in a browser. The URL has the following form:

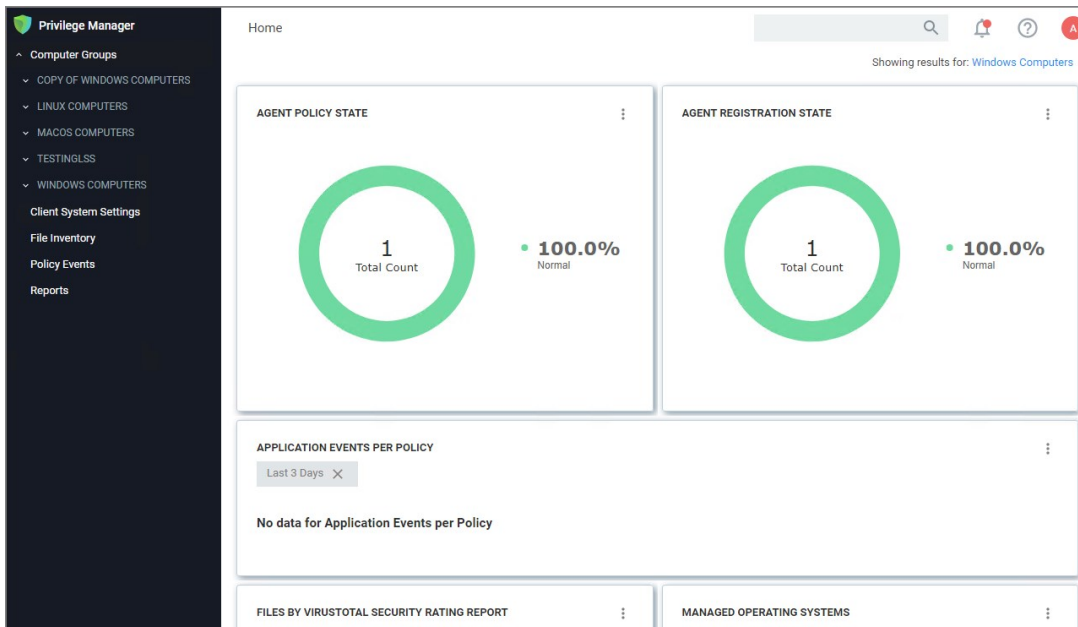
`https://[server-domain]/TMS/PrivilegeManager`

Where:

- server-domain, indicates the customer specific domain name, for example
 - <https://mydomain.com/TMS/PrivilegeManager> for On-premises installations and
 - <https://myassignedname.privilegemanagercloud.com/Tms> for Cloud instances.

The User Interface (UI) seen by all Privilege Manager roles is the same (whether Administrator or other). However, most of the interface is enabled only when you login in as a Privilege Manager Administrator; the other roles are able to perform very few activities.

The screenshot below shows the the Privilege Manager home page, with the main page scrollable.



The home page includes actionable dashboard elements as well as the gateway to the two major components of Privilege Manager, Local Security and Application Control. These are available from their respective tiles.

Much of the text and other content on the page is clickable. The link under it will help you drill down to more detail. (Although some links, here and on other UI pages, are shown in blue, you should not assume that the absence of blue font implies there is no link. The best way to discover links is to hover over the content to find out if it is clickable.)

The set of three little vertical dots, in the upper right corner of each tile, provide options to manipulate the tile.

The ? seen near the right corner of the main menu bar, is used throughout the UI to provide help messages or other access to guidance.

Many aspects Privilege Manager can be customized. The gauges displayed on the home page of the Privilege Manager console and at many other pages can be remove and others can be added. The same with the Reports Options on the Reports page.

What is a Gauge?

Gauges are used in Privilege Manager to display the results of periodic configuration checks of the server and endpoints. Gauges allow reports and graphs to keep historical trend data, and speed up access in the console.

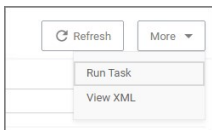
Privilege Manager currently has gauges published to track when an agent last communicated with the server, agents that have received all of their policies, agents that have a random password set, etc.

You can click the following gauges to drill down for more information:

- Agent Policy State
- Agent Registration State
- Application Event Counts by Publisher
- Application Events Per Policy
- Event Summary
- Files by VirusTotal Security Rating Report
- Managed Operating Systems
- Pending Approval
- Top Applications
- Top Applications Needing Elevation
- Top Applications Not Elevated or Denied
- Top Denied Applications
- Top Users
- Top Users Attempting to Run Denied Applications

In Privilege Manager navigation and controls are aligned with Thycotic's standard user experience. The main navigation menu is situated along the left side of your browser window and controls on each page are standardized.

The button for a **page refresh** and the **More** drop-down options are available at the top-right of your page.

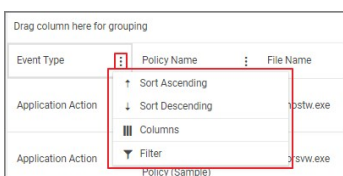


Whenever you are in editing mode on a page, you find a **Save or Cancel** banner on the top of your page.

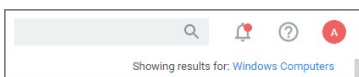


Breadcrumb navigation is provided on the top left of your page.

Table column sorting and filtering is available via the ellipsis on each table column:

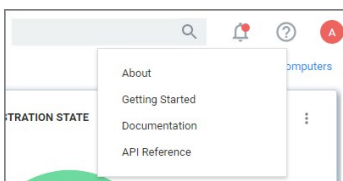


Search, Notification, Help, User Menus

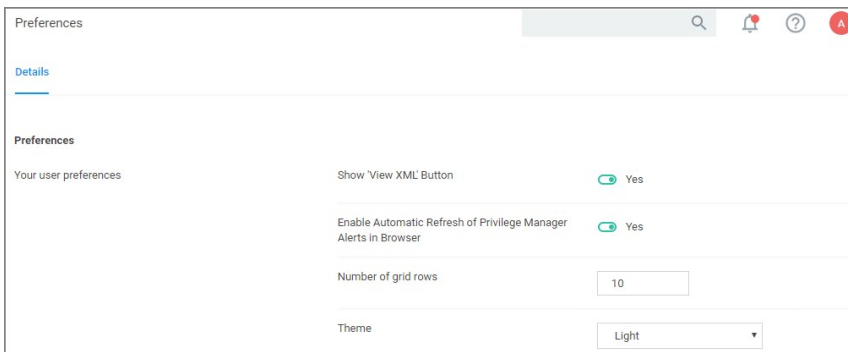


Next to the search menu is the **Notification/Alerts** icon. Click the icon to Manage Approvals and to view Notifications.

The help menu provides access to About, Getting Started, Documentation, and the API Reference.



The user icon provides access to information about the system name, Preferences, and it has the Logout button.



Controls to enable or disable a setting are unified across the user interface via on/off type switches. Users preferences like number of grid rows and color theme can be specified, these will be applied through the console one edited and saved.

Pin to Navigation Tree

When computer groups are created, they can be pinned to the navigation tree on the left. Click the bookmark type icon next to the computer group name or on the Computer Groups page to toggle if a group is shown in the side menu.

NAME	COMPUTERS	USERS	USER GROUPS	SHOW IN SIDE MENU
MacOS Computers	0	0	0	<input type="checkbox"/>
MacOS Test Computer Group Scoped to Mac Computers	0	0	0	<input type="checkbox"/>
Windows Computers	1	12	28	<input type="checkbox"/>

Table Grid Contents

On any table grid the user has an option to filter on what is displayed in the grid and what not.

Computer Groups

- In Side Menu
- All
- In Side Menu
- Not In Side Menu

Application Policies

- Type: All
- Ends Processing: All
- Active: All
- All
- Block
- Elevate
- Allow
- Client System Settings
- Monitor
- Restrict
- All
- Ends Processing
- Continues Processing
- All
- Active
- Inactive

User Policies

- Built-In: All
- Managed: All
- All
- Built-In
- User Defined
- All
- Managed
- Not Managed

Group Policies Same options as for User Policies

Scheduled Jobs All, Active, Inactive

Switches

The UI offers many areas where items or states can be switched from off to on or inactive to active and vice versa.



Main Menu

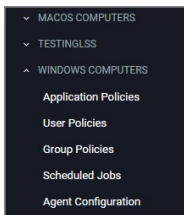
The main navigation menu on the left is organized into

- [Computer Groups](#)
- [Client System Settings](#)
- [File Inventory](#)
- [Policy Events](#)
- [Reports](#)
- [Admin](#)



Chevrons

A menu item with a chevron indicates the menu can be opened or closed, depending on chevron direction. For example in the image below the chevron pointing down for macOS computers indicates the item is collapsed.



The chevron pointing up for Windows computers indicates the item is expanded.

Computer Groups

The listed computer groups all have subitems organized by

- [Application Policies](#)
- [User Policies](#)
- [Group Policies](#)
- [Scheduled Jobs](#)
- [Agent Configuration](#)

Admin Menu

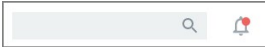
The Admin menu provides access to **Tools**, like

- [Disclose Password](#)
- [Manage Approvals](#)
- [Offline Approvals](#)

The other available **Admin** subitems are:

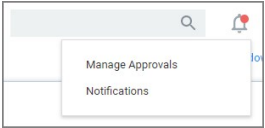
- [Actions](#)
- [Agents](#)
- [Config Feeds](#)
- [Configuration](#)
- [Diagnostics](#)
- [File Upload](#)
- [Filters](#)
- [Folders](#)
- [Import Items](#)
- [Licenses](#)
- [Personas](#)
- [Resources](#)
- [Roles](#)
- Secret Server - only available if integrated via Foreign Systems
- [Server Logs](#)
- [Setup](#) - only available for On-premises instances
- [Tasks](#)
- [Users](#)

Notifications can be accessed via the icon next to the search bar in the top right corner of the Privilege Manager console.



The notification icon displays an indicator when alerts are pending, such as:

- Manage Approvals
- Notifications



To access Alerts, click the icon and select Notifications from the menu options.

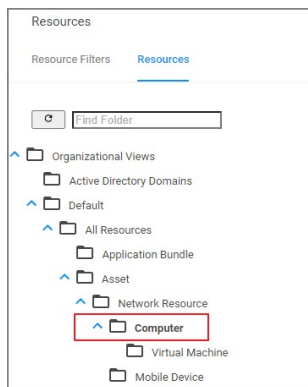
Alerts are listed by priority and category such as Unacknowledged Events, Pending Approvals Count, Number of Application Events, Install Agents, etc.

NAME	DESCRIPTION	PRIORITY
Unacknowledged Events	The number of unacknowledged events There are at least 619086 unacknowledged events, consider acknowledging or purging those events.	High
Pending Approvals Count	The number of pending approvals There are 501 pending approvals.	High
Number of Application Events	The size of the application events table The total number of application events is greater than 26239 consider purging old events.	High
Getting Started	Show Getting Started checklist.	Medium
Number of Old Computers	The number of old computers The total number of old computers greater than 11 consider deleting old computers.	Medium

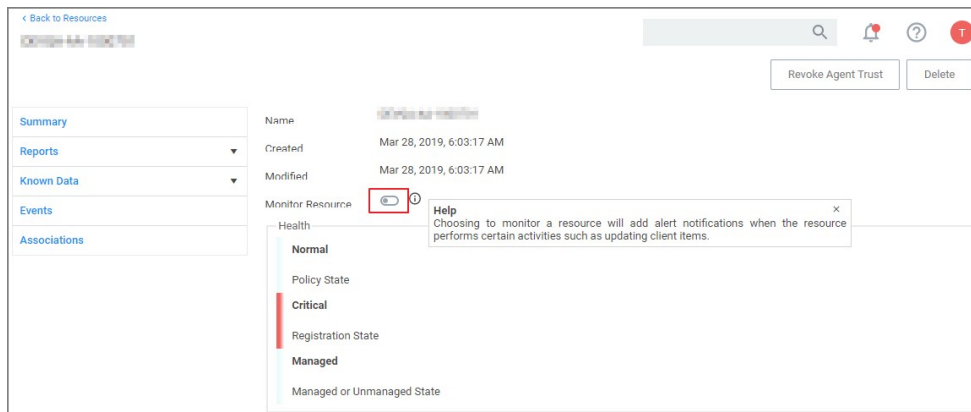
Endpoint Specific Alerts

Alert Notifications can also be triggered for a specific endpoint agent, if the computer resource was configured for monitoring.

1. Navigate to **Admin | Resources**.
2. On the **Resources** tab, open the **Computers** folder.



3. From the list select the endpoint you wish to monitor and open the Resource Explorer for that endpoint.
4. Set the **Monitor Resource** switch to active.



Once monitoring is enabled, alert notifications for the agent end point are available. These type of alerts inform about the agent registration, resource discovery, and update retrieval times.

The Manage Approvals page can be accessed in two ways, via:

- the Alerts icon and selecting Manage Approvals or
- **Admin | Manage Approvals** menu selection.

The screenshot shows the 'Manage Approvals' interface. At the top, there are 'Refresh', 'Approve', and 'Deny' buttons. Below is a table with 400 items. The table has columns for 'POLICY', 'USER', 'USER REASON', and 'REQUESTED'. One row is expanded to show details: 'User Reason' (This is not for work, but I want it.), 'File Path' (\\NetworkShare\Share\Sygic Assistant.exe), and 'Computer'. Below the details are 'Approve' and 'Deny' buttons. Another row is partially visible below.

<input type="checkbox"/>	POLICY	USER	USER REASON	REQUESTED +
<input type="checkbox"/>	User Access Control (UAC) Override Policy (Sample)		This is not for work, but I want it.	5/1/19, 5:33 PM
User Reason This is not for work, but I want it.				
File Path \\NetworkShare\Share\Sygic Assistant.exe				
Computer				
<input type="button" value="Approve"/> <input type="button" value="Deny"/>				
<input type="checkbox"/>	User Access Control (UAC) Override Policy (Sample)		I need this.	5/2/19, 5:46 AM

Use the expand/collapse icon (up/down chevron) to view and approve or deny requests.

Getting Started Overview - On-premises

The following topics provide a guided path through the on-premises installation and setup steps that are part of the initial stand-up of an on-premises Privilege Manager deployment. For cloud specific getting started instructions refer to [Getting Started Overview - Cloud](#).

Preliminary Configuration

Refer to these topics to learn more about the initial installation and setup steps:

1. [System Requirements](#)
2. [Antivirus Exclusions](#)
3. [Privilege Manager Installation](#)
4. [Agents Installation](#)
 - [Setting the Server Address for Privilege Manager Agents](#), if the address provided during the agent installation requires updates.
5. [Login](#)
6. [Licenses](#)

Familiarize yourself with the [Least Privilege](#) concept. Thycotic recommends a phased roll-out between the Application Control and Local Security, for example:

1. **Application Control:** Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines ([Event Discovery](#))
2. **Local Security:** Begin [managing your local user accounts](#) (only) and defining local group membership (Local Security | Manage Local Users)
3. **Application Control:** Tailor your policies so that they won't disrupt employee work ([Creating Policies](#)) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. **Application Control:** Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. ([Creating Policies](#) (Workflow))
5. **Local Security:** Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Refer to the Local Security documentation pages to learn more about:

- [Create & Manage Computer Groups, Local Groups, and Users](#)

Refer to the Application Control documentation pages to learn more about:

- [Application Control - Policy & Config Overview / Collecting File Data](#)
- [Sending Policies to Endpoints - View Deployment Status / Update Using Powershell / Agent Event Log Viewer](#)
- [Event Discovery - Learning Mode Policies & Examples / View Policy Results](#)
- [Creating Policies - Allowlisting, Denylisting, Quarantine, Elevation, Greylisting, & Reputation Checking Examples](#)
- [Policy Priority Overview & Example](#)

Refer to the Integration documentation pages to learn more about:

- [Integration & Foreign Systems](#)

Refer to these documentation pages to learn more about:

- [Reports](#)
- [Troubleshooting](#)

Refer to these documentation pages to learn more about:

- [Policies Catalog](#)
- [Filters Catalog](#)
- [Actions Catalog](#)
- [Privilege Manager Glossary](#)

The following topics provide a guided path through the instance setup and subsequent initial sign-in steps of a cloud Privilege Manager instance.

- [Cloud Quickstart Guide](#)
- [Cloud Login](#)
- [Agents Installation](#)
 - [Setting the Server Address for Privilege Manager Agents](#), if the address provided during the agent installation requires updates.

Cloud Specific vs. On-prem

The new Privilege Manager Application Programming Interface is by default available on all cloud instances upgraded to 10.8 or newly created.

The following features and options are different from On-premises or previous Privilege Manager Cloud (10.7.x) releases:

- The ServiceNow connector is automatically installed for all new cloud instances.
- The SMTP server is automatically configured during the cloud instance setup.
- The setup is managed by Thycotic and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection options to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Thycotic during maintenance periods.
- All license key management is done via Thycotic and license keys are not visible on the licensing page. There are presently no options for customers to add additional licenses directly.

The following features and options are **not** available in Privilege Manager Cloud:

- Access to the Security Manager console (Silverlight version) is not available.
- Server-side Powershell scripts not signed by Thycotic are not allowed. Custom server-side work can be done via Professional Services engagements.

All other features and functionality of Privilege Manager On-premises and Cloud are the same unless otherwise specified.

Rollout Recommendation

Familiarize yourself with the [Least Privilege](#) concept. Thycotic recommends a phased roll-out between the Application Control and Local Security, for example:

1. **Application Control:** Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines ([Event Discovery](#))
2. **Local Security:** Begin [managing your local user accounts](#) (only) and defining local group membership (Local Security | Manage Local Users)
3. **Application Control:** Tailor your policies so that they won't disrupt employee work ([Creating Policies](#)) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. **Application Control:** Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. ([Creating Policies](#) (Workflow))
5. **Local Security:** Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Local Security

Refer to the Local Security documentation pages to learn more about:

- [Create & Manage Computer Groups, Local Groups, and Users](#)

Application Control

Refer to the Application Control documentation pages to learn more about:

- [Application Control - Policy & Config Overview / Collecting File Data](#)
- [Sending Policies to Endpoints - View Deployment Status / Update Using Powershell / Agent Event Log Viewer](#)
- [Event Discovery - Learning Mode Policies & Examples / View Policy Results](#)
- [Creating Policies - Allowlisting, Denylisting, Quarantine, Elevation, Greylisting, & Reputation Checking Examples](#)
- [Policy Priority Overview & Example](#)

Integrations

Refer to the Integration documentation pages to learn more about:

- [Integration & Foreign Systems](#)

Reports & Troubleshooting

Refer to these documentation pages to learn more about:

- [Reports](#)
- [Troubleshooting](#)

Catalogs & Reference Guides

Refer to these documentation pages to learn more about:

- [Policies Catalog](#)
- [Filters Catalog](#)
- [Actions Catalog](#)
- [Privilege Manager Glossary](#)

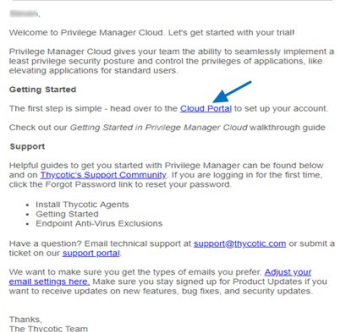
Privilege Manager Cloud is a scalable cloud platform, where all backend services, databases, and redundancy are securely managed by Thycotic and hosted on the Microsoft Azure platform. Customers do not have direct access to the databases or application file system.

This guide will walk you through an initial configuration of your cloud instance.

Initial Setup

After you've signed up for a Privilege Manager Cloud trial, you will receive 2 emails. The first one is from Customer Support and will ask you to create a password to log into the customer support portal.

The second email you will receive is from Thycotic Sales titled Privilege Manager Cloud Trial. This email directs you to the **Cloud Portal** to begin your instance setup.



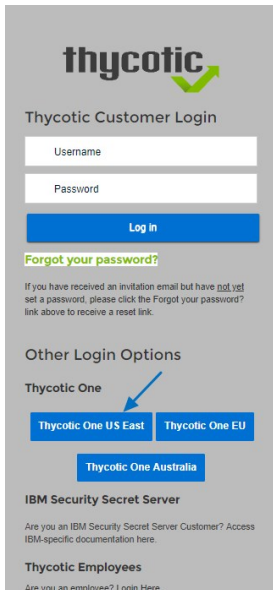
Select the Cloud Portal link. On the Setup page, choose your Cloud Environment location from the dropdown menu. Then click **Continue**.

Setup

You will be directed to the **Thycotic One** portal to create the password for your first user account with Administrator credentials. This account will be assigned to the email address you entered to request the trial. After confirming the password, click **Set Password and Login**.

Important: Thycotic recommends that you store the password in a secured physical location such as a safe or locked file cabinet. You can reset the password using an email reset, but **if this password is forgotten or you no longer have access to the email account, Thycotic will not be able to reset this password.**

On the Thycotic Login page, click the blue button that corresponds to your new Cloud's Thycotic One location (chosen above).



thycotic

Thycotic Customer Login

Username

Password

Log in

Forgot your password?

If you have received an invitation email but have not yet set a password, please click the Forgot your password? link above to receive a reset link.

Other Login Options

Thycotic One

Thycotic One US East Thycotic One EU

Thycotic One Australia

IBM Security Secret Server

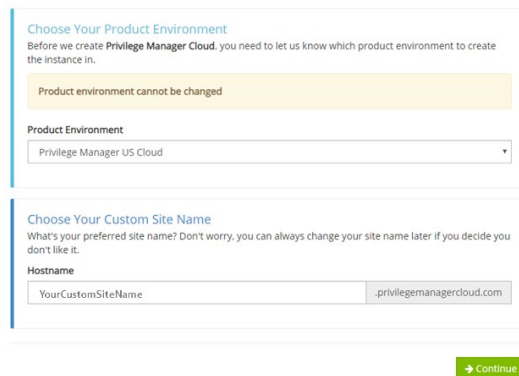
Are you an IBM Security Secret Server Customer? Access IBM-specific documentation here.

Thycotic Employees

Are you an employee? Login Here.

Next, on the Setup page choose the location of your cloud environment and enter the **Name** for your subdomain. Do not use special characters or spaces.

Setup



Choose Your Product Environment

Before we create **Privilege Manager Cloud**, you need to let us know which product environment to create the instance in.

Product environment cannot be changed

Product Environment

Privilege Manager US Cloud

Choose Your Custom Site Name

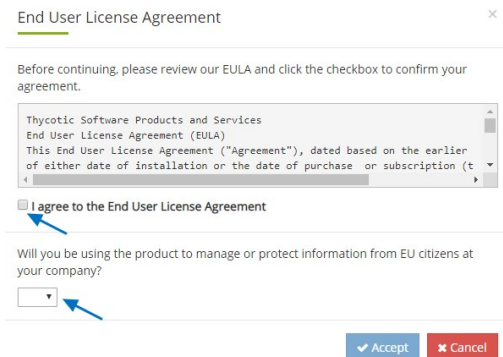
What's your preferred site name? Don't worry, you can always change your site name later if you decide you don't like it.

Hostname

YourCustomSiteName .privilegemanagercloud.com

Continue

Read the End User License Agreement and click the box to signify agreement. From the dropdown, select Yes or No to signify your organization's oversight of EU information. Click **Accept**.



End User License Agreement

Before continuing, please review our EULA and click the checkbox to confirm your agreement.

Thycotic Software Products and Services
End User License Agreement (EULA)
This End User License Agreement ("Agreement"), dated based on the earlier of either date of installation or the date of purchase or subscription (t

I agree to the End User License Agreement

Will you be using the product to manage or protect information from EU citizens at your company?

Yes

Accept Cancel

It will take approximately **20 minutes** for your new Privilege Manager Cloud to spin up.

Working

Please wait while we build your product. The process may take up to 20 minutes to complete.



When complete, click **Go to your Privilege Manager Cloud** instance and **Login with Thycotic One**.



Help Manage [privman246@mallinator.com](#)

Ready

Your product is ready

[Go to your product](#)

You will be automatically redirected to your new Privilege Manager home page.

The screenshot shows the Privilege Manager home page. On the left is a dark sidebar with navigation options: Privilege Manager, Computer Groups (with sub-items for 32-bit Windows, 64-bit Windows, and Mac OS), Client System Settings, File Inventory, Policy Events, and Reports. The main content area is titled 'Home' and shows 'Showing results for: Windows Computers'. It features two large donut charts: 'AGENT POLICY STATE' with a green ring, '3 Total Count', and '100.0% Normal'; and 'AGENT REGISTRATION STATE' with a green ring (66.7%) and a red ring (33.3%), '3 Total Count', and '66.7% Normal' and '33.3% Critical'. Below these are sections for 'APPLICATION EVENTS PER POLICY' (Last 3 Days, No data) and 'FILES BY VIRUSTOTAL SECURITY RATING REPORT' and 'MANAGED OPERATING SYSTEMS'.

Getting Started Screen

Follow the steps on the Getting Started screen. Start with step 1 to allow other users to access Privilege Manager and make sure all 5 steps are completed or reviewed before continuing.

Getting Started

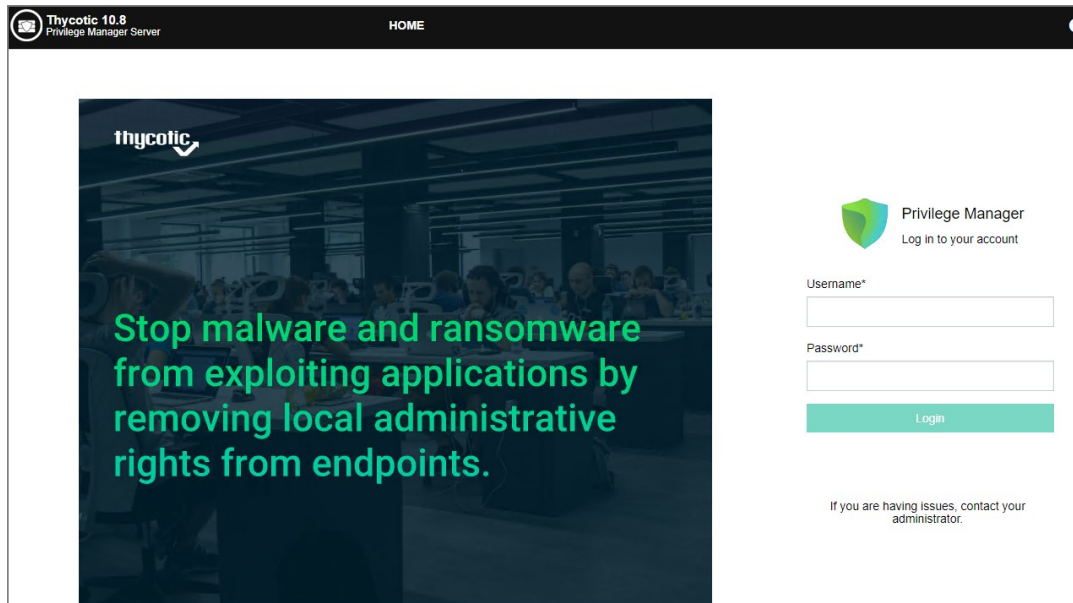
- 1 Choose an authentication provider that will be used to sign into Privilege Manager.
 - Configure with Azure AD: <https://thy.center/privman/link/AzureADCreateApplication?version=10.8.0>
 - Or continue using Thycotic One. Optionally you can create additional users.
 - 2 Setup SMTP Server
<https://thy.center/privman/link/PrivilegeManagerConnectSMTPServer?version=10.8.0>
 - 3 Install Agents
<https://thy.center/privman/link/TMSAgentSoftwareDownloads?version=10.8.0>
 - 4 Review our getting started guide to begin configuring policies
<https://thy.center/privman/link/PrivilegeManager?version=10.8.0>
 - 5 Implement anti-virus exclusions to allow Thycotic to run on the endpoint
<https://thy.center/privman/link/PrivilegeManagerAVExclusions?version=10.8.0>
- Do not show Getting Started banner

Close

To login to a Privilege Manager Cloud instance, use the URL and credentials provided to you. The URL is in the format of:

<https://myassignedname.privilegemanagercloud.com/Tms>

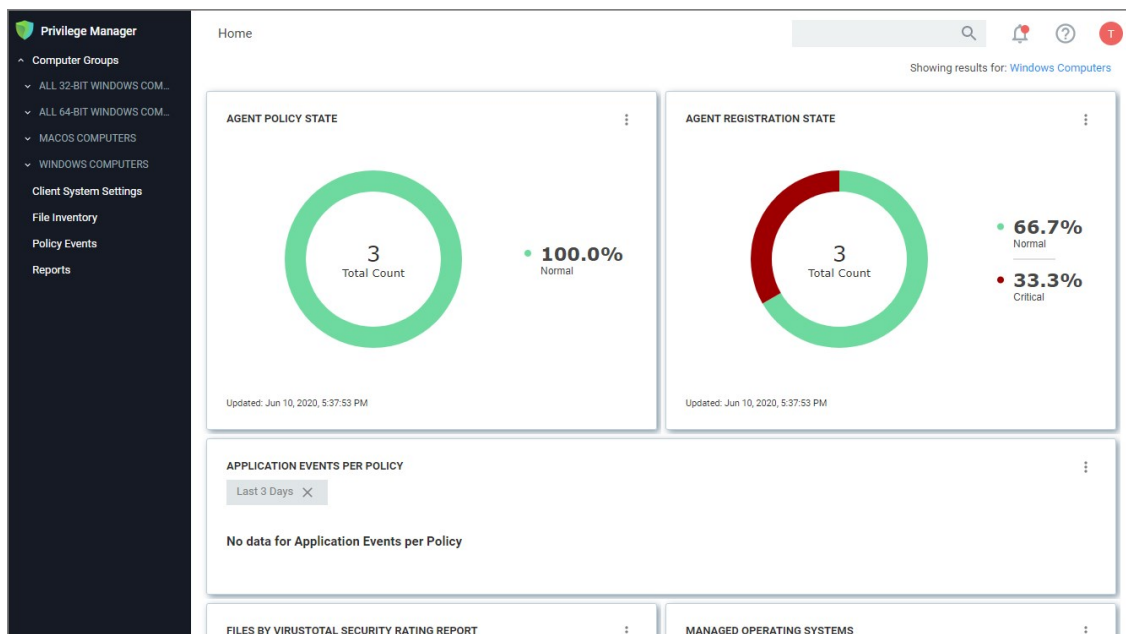
1. Navigate to your assigned login URL.



Depending on the authentication provider setup, users are presented with different login choices.

2. Click the Login button. This usually opens the Sign In dialog:
 1. Enter your username or Email address and click **Next**.
 2. Enter your password and click **Login**.

The Privilege Manager cloud console home page opens:



Note: To import and synchronize Azure Active Directory Groups and Users, refer to the following topic: [Setting Up Azure Active Directory Integration in Privilege Manager](#).

To add Thycotic One Users manually refer to the following topic: [How to Add Thycotic One Users Manually](#). That topic does also cover how to create Standard and API Client users.

Initial Login

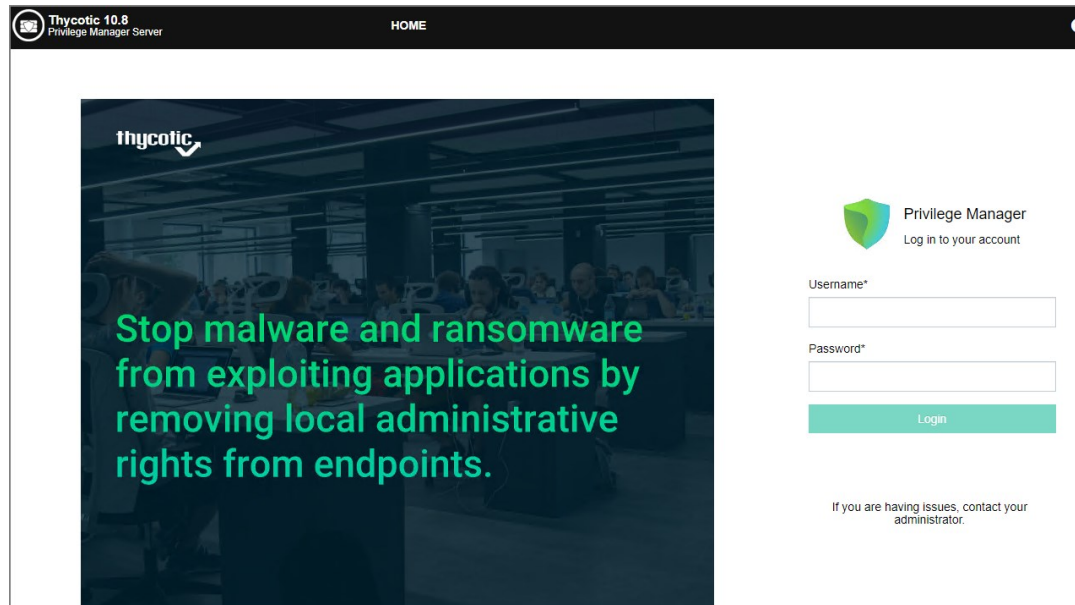
Using the credentials configured in the Create User section of the on-premises installation, validate that you can login to Privilege Manager and view the home screen.

The login URL for an on-premises Privilege Manager instance has this form:

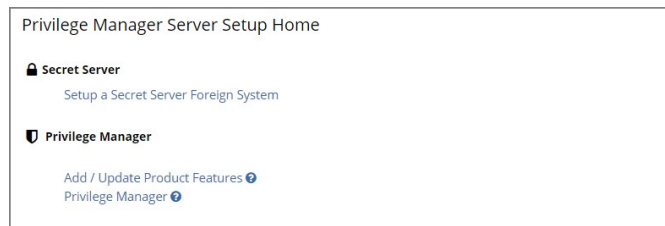
`https://[server-domain]/TMS/PrivilegeManager`

Note: On combined Secret Server/Privilege Manager installations you are initially logged in through Secret Server. If this is the case, you can find Privilege Manager by navigating to **Tools | Privilege Manager**.

The initial login for on-prem happens via NTLM:



After logging in the Privilege Manager Server Setup Home page opens.



Use the Privilege Manager link to login to the product. If you need to add or update product features, such as connectors for foreign systems, use the **Add / Update Product Features** link.

The **Setup a Secret Server Foreign System** link can be used to set-up an integration with Secret Server. This will also allow you to use Secret Server as an authentication provider. Also refer to [Setting up Integration between Privilege Manager and Secret Server](#)

At initial login the Getting Started Banner displays with help tips and next steps:

- Choose an authentication provider that will be used going forward to sign in to Privilege Manager.
- Setup the SMTP Server.
- Install Agents.
- Review the documentation to begin configuring policies.
- Implement anti-virus exclusions to allow Thycotic to run on the endpoint.

You may choose to not show the Getting Started Banner on subsequent logins.

Getting Started

- 1 Choose an authentication provider that will be used to sign into Privilege Manager.
 - Configure with Azure AD:
 - Or continue using NTLM
- 2 Sync local Active Directory in order to configure policies to target users, groups and OUs
- 3 Setup SMTP Server
- 4 Install Agents
- 5 Review our getting started guide to begin configuring policies
- 6 Implement anti-virus exclusions to allow Thycotic to run on the endpoint

Do not show Getting Started banner

Close

The Home screen of Privilege Manager can be found by clicking Home in the top banner of any page inside of Privilege Manager. From this dashboard you can jump into either Application Control or Local Security, depending on what you want to do. You also will be given different snapshots of various important information about your environment. Once you have agents installed and policies setup, you'll have a lot going on from the Home Dashboard:

Home

Showing results for: Windows Computers

AGENT POLICY STATE	AGENT REGISTRATION STATE
1 Total Count	1 Total Count
100.0% Normal	100.0% Normal

APPLICATION EVENTS PER POLICY

Last 3 Days X

No data for Application Events per Policy

FILES BY VIRUSTOTAL SECURITY RATING REPORT

MANAGED OPERATING SYSTEMS

If you previously had evaluation licenses and recently purchased, you will need to install your new license keys for production via the same steps as above. Normal trial licenses offer 50 endpoint agents and expire 30 days after issue.

When your Privilege Manager licenses expire or have exceeded the licensed count, Privilege Manager will stop processing new inventory and application control events. Endpoints will continue to enforce policies.

In your Installed Licenses list use the **Delete** option to remove expired or old licenses that are not in use anymore.



- **Client License:** This license provides coverage for endpoints that are workstations, such as Windows 10, windows 7, etc.
- **Server License:** This license provides coverage for endpoints that are server machines, Windows Server 2019, Windows 2016, etc.
- **Support License:** Without having a support license you will not be able to complete upgrades and will not be able to receive support or maintenance.

License Expired or Exceeded License Count

The Server will stop accepting data sent from agents that are in violation of the licensing. New endpoints will register, but will not be recorded, which means the endpoint:

- Will not get added to the resource targets and will not collect application or user inventories
- No password changes will occur, etc.
- Policies will run on the endpoint, but the server will completely discard the data, and it won't be stored.
- Tasks will not run - all automation will stop and event Discovery will not inventory users or applications, new endpoints won't be discoverable.

If you need to reset licenses for your Privilege Manager instance refer to the [Reset Licensing](#) topic.

Installation and Upgrades

This section contains all you need to know about installation and upgrading Privilege Manager and all its components.

The following topics are available:

- [System Requirements](#)
- [Recommended Anti Virus Exclusions](#)
- [Software Downloads](#)
- [Installation](#) - recommended installation procedure
 - [Manual Installation Instructions](#)
 - [Item Encryption](#)
- [Agent Installation](#)
 - [Agent System Requirements](#)
 - [Install Codes](#)
 - [Windows Bundled Agent Install](#)
 - [Windows](#)
 - [macOS](#)
 - [Directory Services Agent \(AD\)](#)
 - [Bundled Core and Directory Services Agents](#)
 - [Uninstall via Command Line](#)
 - [Agent Hardening](#)
- [Upgrades](#)
 - [Upgrading from 8.2 to Privilege Manager 10.4 and up](#)
 - [Offline Upgrades Privilege Manager](#)
 - [Offline Upgrades - Combined Secret Server and Privilege Manager](#)

Privilege Manager System Requirements

These are requirement for an on-premises integration.

Note: Verify that the .NET version between the Privilege Manager and Database Server in use are matching, especially if installed on different Windows Server versions.

4 CPU Cores	4 CPU Cores
8 GB RAM	16 GB RAM
40 GB Disk Space	150 GB Disk Space
Windows Server 2012 R2 or newer	Windows Server 2012 R2 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 3.0 or newer	

Note: Environments with over 25,000 Endpoints require a scoping call with a Thycotic engineer.

8 CPU Cores	8 CPU Cores
32 GB RAM	64 GB RAM
40 GB Disk Space	500 GB Disk Space
Windows Server 2016 or newer	Windows Server 2016 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 5.0 or newer	

- RAM, CPU, and Disk Space - negligible
- Windows 7 or newer. Thycotic performs validation on the latest Windows OS that is available via the Microsoft Insider Program to ensure any required changes are made prior to a new OS version release.
- MacOS 10.11 (El Capitan) or newer.

Also refer to [Agent System Requirements](#).

- System Requirements apply to both physical and virtual machines.
- For best performance, we recommend using dedicated (clean) servers for Thycotic products.
- PowerShell must be allowed to execute and cannot be blocked on the server or the endpoint by other products.
- If .NET and/or IIS features are not already installed on the web server, the Thycotic Installer will add and configure them automatically.
- If SQL is not already installed on a database server, the Thycotic Installer can setup SQL Express on the web server, however SQL Express is intended for Trials and Sandbox environments ONLY. Though Thycotic will support SQL Express, users will likely experience performance issues due to the memory and product limitations. If experiencing performance issues while using SQL Express, it is highly recommended to upgrade to SQL Server prior to contacting Thycotic Support.
- A link to Microsoft documentation on the use and limitations of SQL Express can be found at: <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017>
- Web Servers that are NOT supported: Small Business Server (SBS), The Essentials Edition, Domain Controllers, Sharepoint Servers.

- **Outbound (port 443 - HTTPS):** This is the default access port through which the agent connects to the server. You may specify a different port based on your environment.
- **Inbound (port 5593):** This is the default and only port that the agent listens on. This port is not required and you can block port 5593. If you block the port, the agents pull updates from the server based on a set schedule.
- **SQL (port 1433):** This is the default SQL DB port. The SQL port can be customized.

Anti Virus Exclusions

For Privilege Manager users we recommend several antivirus exclusions to maintain application performance and integrity. These guidelines apply to both real time and on-demand antivirus scanning.

Exclude these two directories from your antivirus filters to ensure Privilege Manager processes will not be blocked (or for a more granular approach to these exclusions, see the Client Item Database and Privilege Manager Application Control Agent Services sections at the end of this article):

```
%ProgramData%\Arellia\  
%ProgramFiles%\Thycotic\
```

Exclude the following antivirus programs for Privilege Manager's web server, also sometimes called Thycotic Management Server (TMS):

Temporary ASP.NET Files

Exclude the following directory to prevent degradation in performance and possible unexpected restarts of the Tms and TmsWorker IIS application pools:

```
%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
```

Exclude the following antivirus programs for databases.

SQL Server Data Files

These files contain data and typically have the following extensions:

- .mdf - primary data filegroups
- .ndf - secondary data filegroups
- .ldf - transaction log filegroups

SQL Server Backup Files

These files contain the backup files and typically have the following extensions:

- .bak - database backup files
- .trn - transaction log backup files

By default the directories that contain the Data and Backup files are located under C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL.

SQL profiler trace files

These files contain SQL Profiler Trace log data and can be contained in any folder.

They usually have the file extension .trc.

Exclude the following antivirus programs for managed endpoints.

Request Run As Administrator Registry Key

Privilege Manager Application Control installs a context menu item that allows executables to be "Request Run as Administrator."

This context menu is added under the following registry key which some antivirus programs incorrectly flag as malware:

```
HKLM\SOFTWARE\Classes\exe\Shell
```

Client Item Database

This directory contains the Thycotic Agent client item database and should be excluded from antivirus to prevent corruption:

```
%ProgramData%\Arellia\ClientItems
```

If required you can further limit this exclusion to all files with the .db and .db-* extensions under this location

Privilege Manager Application Control Agent Service

Some antivirus products require that the Privilege Manager Application Control service be excluded from tamper protection rules because Application Control manipulates other applications which antivirus products may mistake as malicious.

```
C:\Program Files\Thycotic\Agents\ApplicationControl\ArelliaACSvc.exe
```


Software Downloads

This page provides links to Thycotic Privilege Manager product and agents software downloads.

10.8.2	Combined Secret Server and Privilege Manager Installer - Authentication required!
	Privilege Manager Application Files - Authentication required!

Windows Endpoints

10.8.1150	Bundled Privilege Manager Agent Installer - Windows
10.8.1150	Core Thycotic Agent (x64)
10.8.1150	Core Thycotic Agent (x86)
10.8.2185	Application Control Agent (x64)
10.8.2185	Application Control Agent (x86)
10.8.2183	Local Security Solution Agent (x64)
10.8.2183	Local Security Solution Agent (x86)
10.8.1150	Bundled Privilege Manager Core and Directory Services Agent - Windows
10.8.1164	Directory Services Agent (x64)

macOS Endpoints

10.8.1019	Privilege Manager macOS Agent	Catalina and later using System Extensions (SYSEX)
10.8.27	Privilege Manager macOS Agent	Catalina and previous using Kernel Extensions (KEXT)

Prerequisites

ASP.NET Website

Privilege Manager is installed as an ASP.NET website. The setup.exe file will set up the website with the correct permissions and create the settings in IIS.

SQL Server Database

Thycotic products require an instance of SQL Server for the database backend and an instance of SQL Express will be installed by the setup.exe file if missing. The SQL Server database will require a SQL account with db_owner permission to complete the installation. SQL Express edition is intended for Sandbox and trial environments, Thycotic recommends purchasing SQL licensing for use in production environments.

Administrative Access

Throughout the installation process, you will be required to be an administrator to perform most actions. Please ensure that you are logged onto your system with a Windows account that has administrative rights before beginning your install.

Additional Recommendations

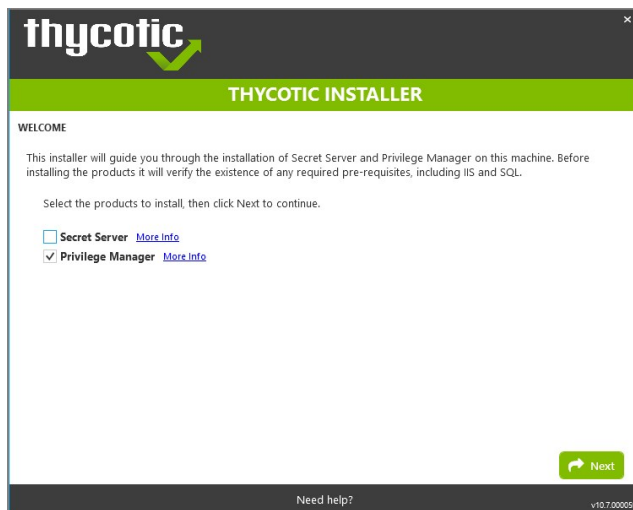
1. Use an SSL certificate for Privilege Manager.
2. Run Microsoft Update on your server to make sure all components are up to date.

Download the Latest Version of PM Installer

The latest version of Privilege Manager is available for download under the [Software Downloads](#) topic. It is recommended to run the downloaded setup.exe file as an administrator.

Running the Installer

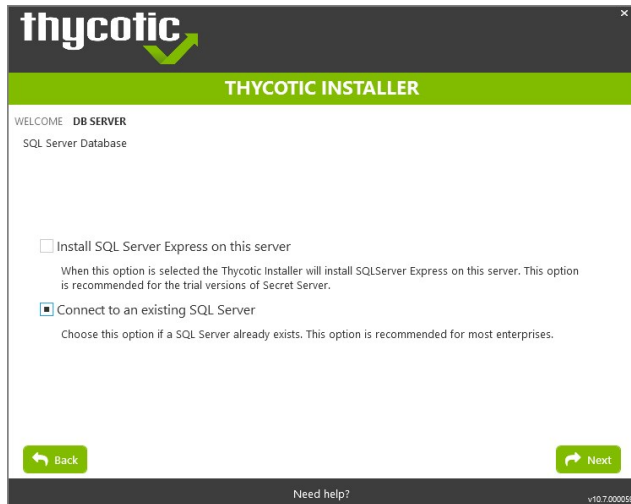
1. Double-click the downloaded setup.exe to run the installer. The installer opens on the **Welcome** tab:



2. Verify that the Privilege Manager box is checked.

Note: Privilege Manager as a standalone product comes with three roles Administrator, Basic User, and Help Desk User roles. Please refer to [Application Roles](#).

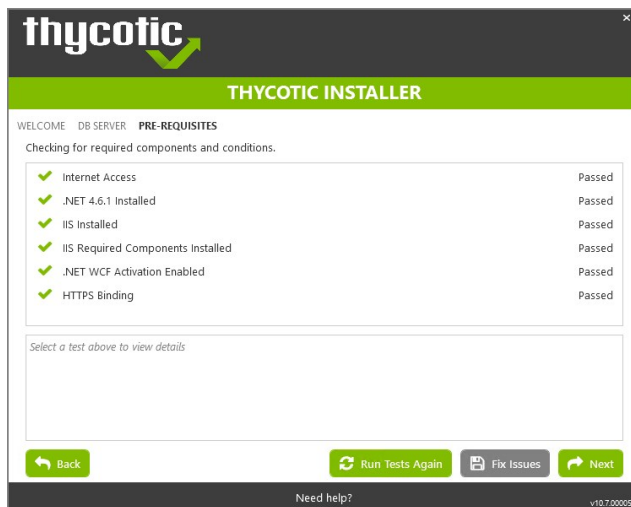
3. On the **Database** tab you can choose to either install SQL Express or connect to an existing SQL Server. SQL Express requires a internet access for the installer to download the installation package for SQL Express.



Note: For production environments Thycotic recommends installing a licensed edition of SQL before installing Thycotic products. The Express edition is only recommended for trial and sandbox environments.

- o If Internet access is not available a link to download SQL Server Express will be presented to the user. At that point, they are expected to install SQL Server Express and then restart the installer.
- o If Internet Access is available SQL Server Express will be installed.
- o After SQL is installed select Connect to an existing SQL Server.

4. The **Pre-Requisites** tab makes sure everything that is required to install Privilege Manager is setup correctly. Everything on this page can be installed outside of the installer, but if not, the installer will install and configure them for the user. Think of this page as the non-Thycotic configuration. If there are issues with this page it is very likely that the Internet will be able to help as these are not installation features that are specific to Thycotic. Click Fix Issues to automatically install the necessary pre-requisites. When Successful, click Next.



5. If you chose the "Connect to an existing SQL Server" option on the Database page, the **Database Connection** tab will now prompt you for the connection information that Privilege Manager will use. The Test Connection button must be run successfully before installation can continue. Once connection is established, click **Next**.

Note: If you are not using a default InstanceName on the SQL Server for the Privilege Manager database, provide the SQLServerName\InstanceName for **ServerName** or **IP**.

thycotic

THYCOTIC INSTALLER

WELCOME DB SERVER PRE-REQUISITES **DB CONNECTION** ACCOUNT

SQL Server Location

Server name or IP

Database name

SQL Authentication

SQL Server Authentication (SQL Server authentication requires Mixed Mode)

User name

Password

Windows Authentication using Service Account

Advanced (not required)

Back Next

Need help? v10.7.000059

thycotic

THYCOTIC INSTALLER

WELCOME DB SERVER PRE-REQUISITES DB CONNECTION **ACCOUNT**

User Account for Web Applications and Database Access

This account will be used for the web application(s) and will also need to have access to the SQL Server database with at least "db_creator" privileges. You may specify individual web application accounts on the upcoming review page if required.

User Name

Password

Validate Credentials Success

Back Next

Need help? v10.7.000059

1. If you choose SQL Server Authentication, next the Account tab will prompt for the server location where your SQL database is currently installed. Provide the Server Name or IP address for your Database server and Authenticate with Administrator SQL credentials. If your Secret Server database does not yet exist when you click "Test Connection" the Installer will create it. When the connection has been tested successfully, click Next.

6. The **Email Server** tab opens, here the connection information for the email server can be entered. This is also optional and can be skipped to be configured later in the application by clicking Skip Email. This page will configure email for Privilege Manager.

thycotic

THYCOTIC INSTALLER

WELCOME DATABASE PRE-REQUISITES DATABASE CONNECTION CREATE USER **EMAIL SERVER**

Please enter the connection information for the Email Server that will be used to send outgoing notifications from Secret Server.

Email Server

From Address

Use SSL

Use Custom Port

Port 25 ?

Authentication required

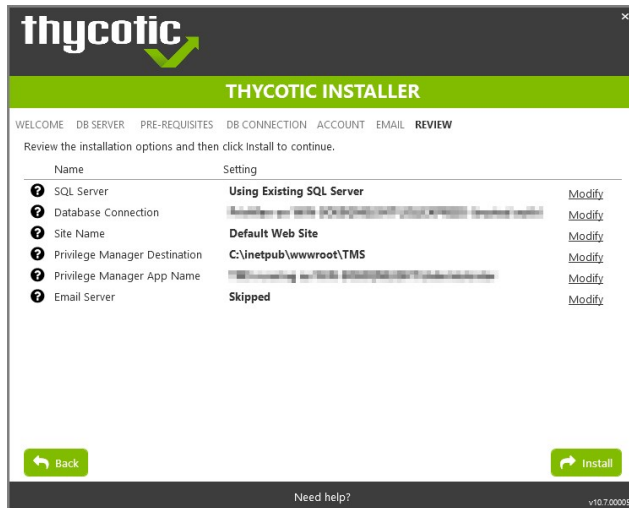
User name

Domain ?

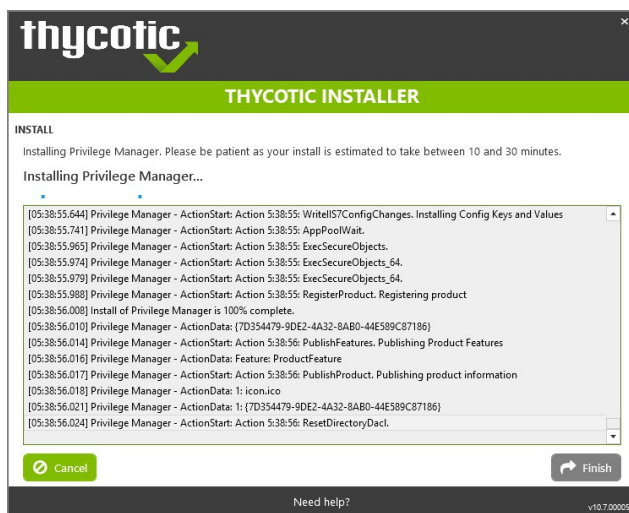
Password

Back Skip Email Send Test Email Next

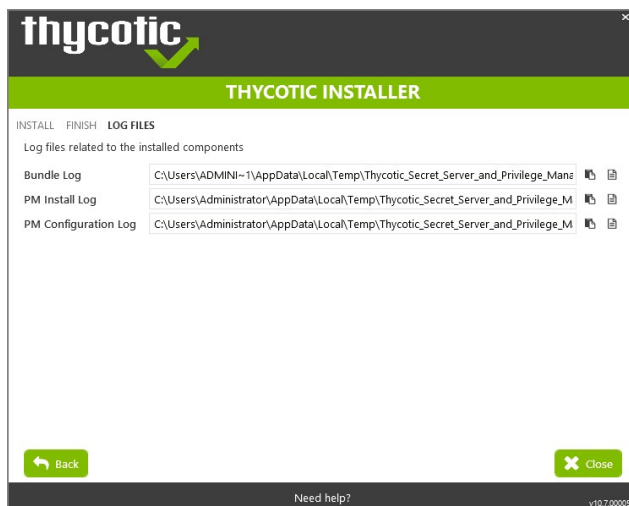
7. On the **Review** tab, most settings are defaulted for a user and they can choose to modify settings at this step. Certain validations will occur on these settings before the install can begin. Click Install to proceed.



8. The Install page will show the status from log files as Secret Server and/or Privilege Manager are installed. Installs vary depending on your environment, most installs last between 20-60 minutes.

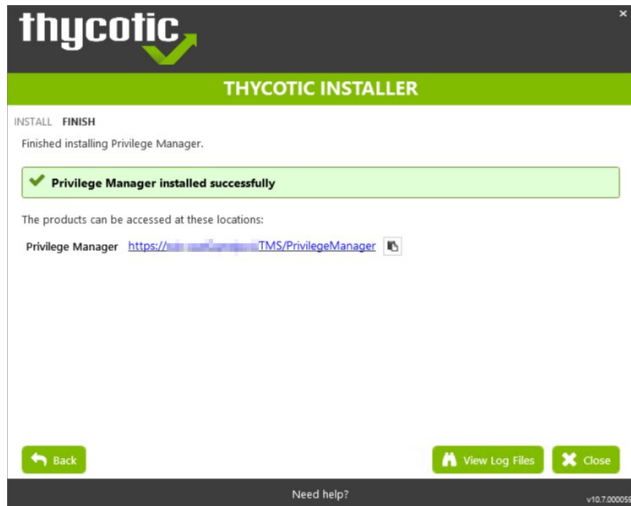


9. The **Log Files** tab is available after the applications are installed. The installer provides the link to open a web browser to the product login page. At this point, everything is installed and ready for you to begin using your new Thycotic product. If the installation failed or you wish you view the logs from the installation you can click the View Log Files button.



10. On the **Finish** tab, when the install has successfully completed, click the provided Privilege Manager URL to navigate directly to your setup landing page or open a browser and navigate to where your Privilege Manager is located, for

example: <http://localhost/TMS/PrivilegeManager>.



Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Installing Connectors or the API

Privilege Manager installs the core packages. Once your instance is up and running, use Setup to add connectors for foreign systems or the **Privilege Manager Application Programming Interface**.

Refer to [Upgrades](#) for details about how to access Setup and use the **Add / Upgrade Privilege Manager Features** option.

If you need to manually install Privilege Manager on a system and you already have an existing server installation, refer to the installation instructions described under the [High Availability Set-up for Privilege Manager](#). Otherwise follow the steps below.

Note: Thycotic recommends to always use the setup.exe installer to verify that your system meets the pre-requisites.

Download Privilege Manager Application Files

Make sure you have the prerequisites (IIS, .NET Framework, and SQL Server) installed before following the steps listed below.

After clicking the download link on the [Software Downloads](#) page, you will be able to download a .zip file that contains both Privilege Manager and Privilege Manager files.

Zip File Extraction Tool

You will also need to install a zip application like winzip or 7-zip to extract files for this install. 7-zip is used in the instructions below and can be downloaded for [free here](#).

Manual Installation (no setup.exe)

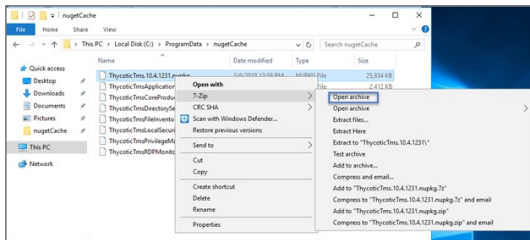
Clicking the download link above will take you to a portal page where you can choose to download a .zip file that contains the application files. Use this .zip file for the instructions below. Privilege Manger can be installed in a few different ways, as a:

- Virtual Directory
- Website

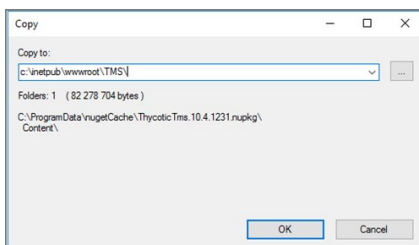
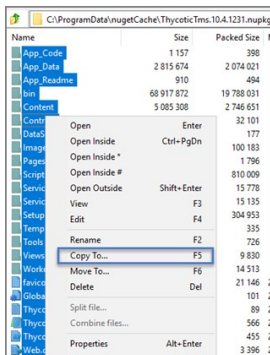
Installing as a Virtual Directory

1. Extract the contents of the .zip file and select the nugetCache folder. Move the contents of that folder to a temporary location like C:\ProgramData\ (Recommended)
2. Create a folder called TMS in the location C:\inetpub\wwwroot\
3. Navigate back to c:\ProgramData\nugetCache\ and using any zip application (ex: 7-zip, winzip, winrar, etc), open ThycoticTms.xx.x.xxx.nupkg

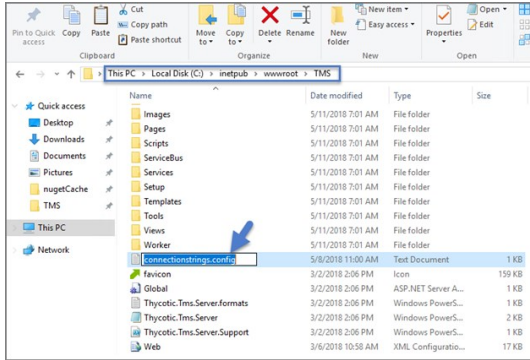
To do this with 7-zip: right-click ThycoticTms.xx.x.xxx.nupkg | 7-zip | Open Archive.



4. Open the Content directory and ctrl-A to select all of its contents. Copy these to the location C:\inetpub\wwwroot\TMS\



5. In C:\inetpub\wwwroot\TMS\ where you have extracted the TMS Site files, create a new file right-click **New | Text Document** called connectionstrings.config



6. Next, decide what mode you want to use to access your SQL database and follow the corresponding steps:

- **Mixed Mode/Integrated Security=False*** (for easiest configuration): Mixed Mode is required if you intend on using a SQL Server account to authenticate Privilege Manager to your SQL Server instance. If you are doing an evaluation and using the Privilege Manager setup.exe installer, we recommend using Mixed Mode with a SQL authentication account. This option will also require you to set a password for the SQL Server system administrator (sa) account. See the Integrated Security=False section below to use Mixed Mode.
- **Windows Authentication Mode/Integrated Security=True*** (recommended for best security): This will prevent SQL Server account authentication and requires a Windows Service account to run the Privilege Manager website. This will also require additional configuration in IIS once Privilege Manager is installed. Follow the steps under the Integrated Security=True section below to use Windows Authentication.

Integrated Security=False

Open in Notepad the connectionstrings.config file created in step 5 and copy in the following text; replacing the SQL Server Name, Database Name, User Name, and Password (highlighted in bold below) with values for your environment. Save changes.

```
<connectionStrings>
<add name="ApplicationServerWorkflowInstanceStoreConnectionString"
connectionString="Data Source=SQLServerAddress;Initial Catalog=DatabaseName;Integrated Security=False;User ID=myUserName;Password=myPassword;Application Name='Arellia Management Server - WF'" />
<add name="AmsConnectionString"
connectionString="Data Source=SQLServerAddress;Initial Catalog=DatabaseName;Integrated Security=False;User ID=myUserName;Password=myPassword;Application Name='Arellia Management Server'" />
</connectionStrings>
```

Integrated Security=True

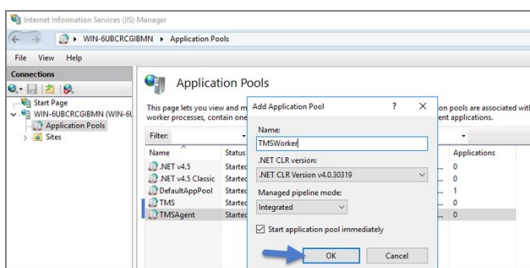
If you choose to set Integrated Security to True, you will need to ensure that the application pool service accounts have access to the database server in a later step.

Open in Notepad the connectionstrings.config file created in step 54 and copy in the following text; replacing the SQL Server Name and Database Name (highlighted in bold below) with values for your environment. Save changes.

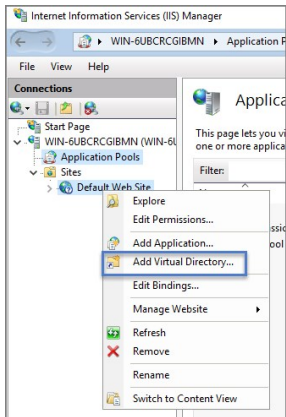
```
<connectionStrings>
<add name="ApplicationServerWorkflowInstanceStoreConnectionString"
connectionString="Data Source= SQLServerAddress;Initial Catalog= DatabaseName;Integrated Security=True;Application Name='Arellia Management Server - WF'" />
<add name="AmsConnectionString"
connectionString="Data Source= SQLServerAddress;Initial Catalog= DatabaseName;Integrated Security=True;Application Name='Arellia Management Server'" />
</connectionStrings>
```

Continue: Installing as a Virtual Directory

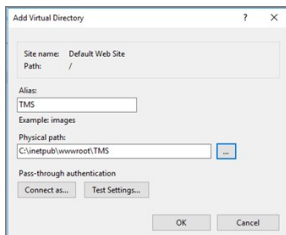
1. Open Internet Information Services Manager (inetmgr.exe).
2. Under your local server, right-click Application Pools and select **Add Application Pool..** Add three new application pools. Name one TMS, name another TMSAgent, and name the third TMSWorker.



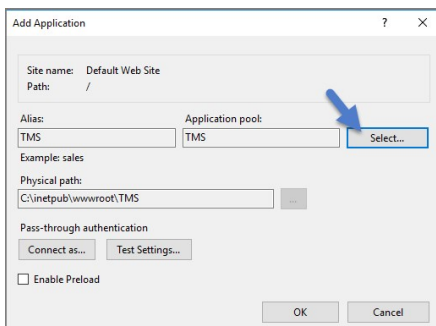
3. When creating your connection string, if you selected Integrated Security=True in step 6, change the Identity for your application pools to a service account that has DBOwner rights on the SQL database & make sure that the Identity for the three app pools have Modify rights to the folder that you put the Privilege Manager files into. To setup the service account correctly and set folder permissions and the Identities for these app pools, follow all of the steps in [Using a Service Account to run the IIS App pool](#) now.
4. Right-click Default Web Site in IIS and select Add Virtual Directory..



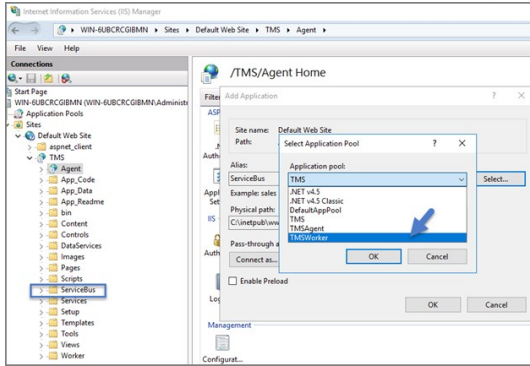
5. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in `http://myserver/TMS`.
6. Next, enter the physical directory where you unzipped Privilege Manager `C:\inetpub\wwwroot\TMS`.
7. Click **OK**.



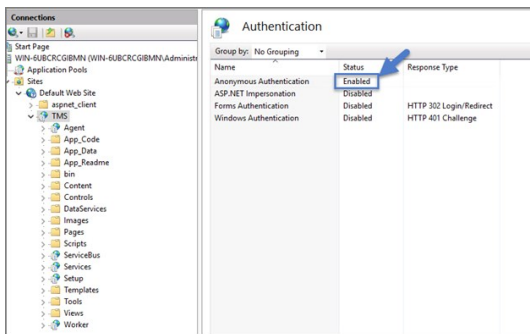
8. In the tree, right-click the new virtual directory and select **Convert to Application**.
9. Set the Application Pool to the one called TMS. Click **OK**.



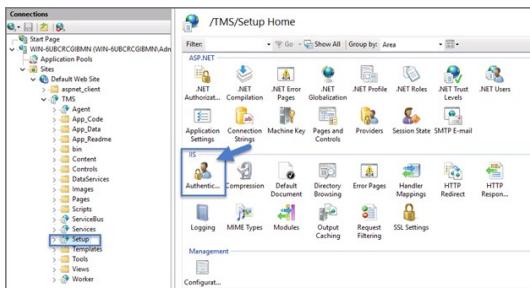
10. In the virtual directory expand the new TMS site, right click the Agent Subfolder and select **Convert to Application**.
11. Set the Application Pool to the one called TMSAgent and click **OK**.
12. Next, in the virtual directory navigate to the ServiceBus Subfolder. Right-click and select **Convert to Application**.
13. Set the Application Pool to the one called TMSWorker. Click **OK**.



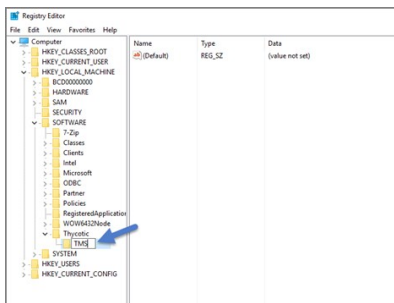
14. In the virtual directory select the Services Subfolder, right-click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called TMS. Click **OK**
15. In the virtual directory select the Setup Subfolder, right-click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called TMS. Click **OK**
16. In the virtual directory select the Worker Subfolder, right-click the new virtual directory and select **Convert to Application**. Set the Application Pool to the one called TMSWorker. Click **OK**
17. Select your TMS virtual directory, double click **Authentication** in the features pane and make sure that only *Anonymous Authentication* is set to **Enabled**. Everything else should be set to disabled.



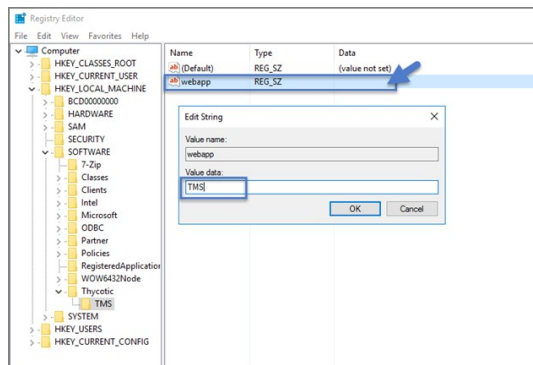
18. Select the Setup directory, double click **Authentication** in the features pane and make sure that Anonymous Authentication and Windows Authentication are both set to **Enabled** and everything else is disabled.



19. Select the Worker, double click **Authentication** in the features pane and make sure that Anonymous Authentication and Windows Authentication are both set to **Enabled** and everything else is disabled.
20. In **Regedit.exe**, create a new Registry key (HKEY_LOCAL_MACHINE) right-click on **Software** | **New** | **Key**, name the new key Thycotic. Next right-click on **Thycotic** | **New** | **Key**, name the new key TMS.



1. Create a new string value in the TMS folder right-click **TMS** | **New** | **String Value** with a name of webapp and a value of TMS (double click to assign value)



2. Create a 2nd new string value with a name of website and a value of the url to the root of the site you will be using (ex: "testlab" for a website of https://testlab/TMS)
 3. Create a new string value with a name of Webdir and a value of the path you put your Privilege Manager files in (i.e. C:\inetpub\wwwroot\TMS)
21. Ensure that the Privilege Manager folder has the proper permissions by checking that the account running the application pool in IIS has Modify permissions on the folder where Privilege Manager is installed. (i.e. C:\inetpub\wwwroot\ right-click **TMS** | **Properties** | **Security** tab, if the service account created in [Using a Service Account to run the IIS App pool](#) is not listed, Edit... | Add... | find account via Check Names | **OK**. Click on the account, check **Modify** | **Apply**.)
 22. If your server does not have internet access you will need to ensure that your **solutionCenter** is configured for the directory that you deposited the nupkg files into.

1. Go to the directory where you have installed the TMS site (i.e. C:\inetpub\wwwroot\TMS)
2. Open the **web.config** file with Notepad and find the line


```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com" /
```
3. Replace the value with the directory from step 1 (usually c:\ProgramData\NuGetCache). Save changes.

```
<add key="almah.mvc.requiresauthentication" value="false" />
<add key="almah.mvc.allowedRoles" value="" />
<add key="almah.mvc.routes" value="almah" />
<!--
<add key="nuget:source:DevSolutionCentre" value="http://localhost/TesDevNuGet/NuGet/" />
<add key="nuget:source:SolutionCentre" value="http://nuget-dev.ds.arelila.com/NuGet/" />
key="nuget:source:SolutionCentre" value="C:\ProgramData\NuGetCache" />
-->
<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NuGetCache" />
</appSettings>
<connectionStrings configSource="ConnectionStrings.config" />
<system.web>
```

Note: Make sure if using a local path to include the final slash.

Privilege Manager is now ready to be configured. Continue with [Completing Privilege Manager Installation from Website](#).

Installing as a Website

1. In IIS, right-click **Sites** and select **Add Website...**
2. Enter a Site name.
3. Click **Select...** and choose the application pool you created in the Manual Installation section from the drop-down menu. Click **OK**
4. Click the **_** beside the Physical path field and select the directory containing the unzipped Privilege Manager files (for example, C:\inetpub\wwwroot\TMS). Click **OK**
5. At the bottom of the Add Website window click **OK** to save your settings.

Completing Privilege Manager Installation from Website

Privilege Manager is now ready to complete installation. Open a browser and navigate to where your Privilege Manager Setup is located, for example: https://localhost/TMS/Setup. It will request windows credentials which must be the credentials for a local administrator on the web server.

The site will detect that it does not have the proper database configuration and walk you through installing the initial database objects.



After this initial step you will be presented with a list of Privilege Manager features you can choose to install.

1. Select **Add/Remove Product Features**
2. Select Application Control and Privilege Manager. This will automatically also select any prerequisites they require.

Each feature is delivered as a NuGet Package, the package will unzip, add files to the Privilege Manager website, and update the database with its required objects. Installing the database and features may take several minutes.
3. Click **Show Install Log** to reveal installation progress.

Once all features have been installed Privilege Manager is ready to use! Refer to the [Getting Started](#) section for setup and configuration advice.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

With version 10.5 and up, encryption of items no longer requires app pool permissions on the machine's certificate store.

What this means for Privilege Manager

New installations of Privilege Manager will no longer require that the application pool user has to have permission to access the certificate stores. Previously this permission was required in order to encrypt and decrypt items in the database.

Existing installs of Privilege Manager (10.4 and earlier) should not remove this permission and should not remove old certificates as they will still need them to decrypt old items which predate this change. Both the web setup page and the installers will create a local **encryption.config** file in the TMS directory to hold the keys to the key stored in the database. This file is highly sensitive and should be regarded with caution.

Agents are required on endpoint machines to carry out policies created in Privilege Manager. This section offers direct downloads and descriptions for all available agents.

Thycotic Agents can be deployed in various ways, via:

- software management systems,
- GPO,
- cloned (gold) images, and
- manually.

Instructions and links for agent installers are grouped as follows:

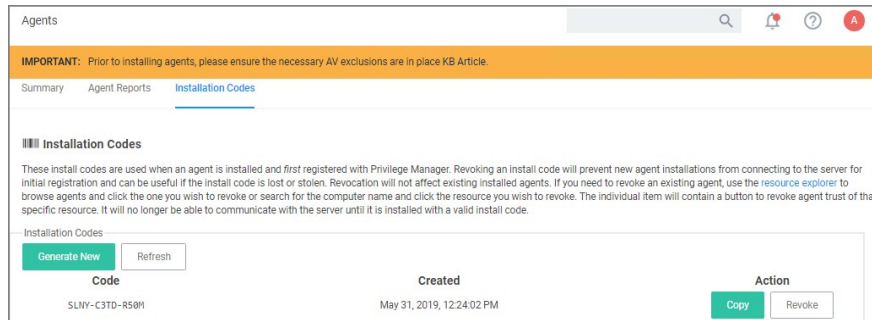
- [Bundled Agent Installer - Windows](#)
- Individual Agent Installers for Privilege Manager:
 - [64-bit Windows Operating Systems](#)
 - [32-bit Windows Operating Systems](#)
- [macOS Installer - 10.11 or Newer](#)
- [Directory Services Agent to support Local AD Synchronization with Cloud Instances](#)
- [Bundled Core and Directory Services Agents](#)

For details about Thycotic Agent System Requirements, see our [Agent System Requirements](#).

In version 10.5 and up, installation codes are required upon initial install to prove to the server that an agent install is authorized. Once an agent is installed, it deletes the install code and authenticates to the server via a certificate. See Agent Trust Revocation for certificate revocation.

The agent uses the install code to prove to the server that it is an authorized install. Once the agent is installed, the install code is deleted and the agent certificate is used to communicate with the server. The server needs either an install code or agent trust (a certificate) to accept communication from an agent. Multiple install codes can be created for bundling with different installers, if the last install code is revoked, a new one is generated automatically. Revoking an install code prevents new installations with that install code but does not affect previous installations since those agents now use their own certificates to authenticate.

1. Navigate to the agent settings under **Admin | Agents**.
2. On the Installation Codes tab you may Generate New codes, Refresh code information, Revoke, or Copy Codes to the clipboard to use in the installer.



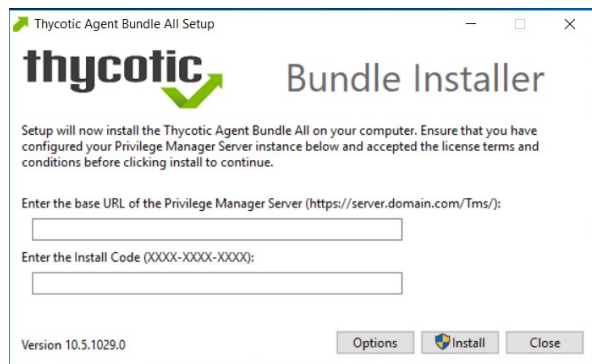
If deploying with msixexec, the following command shows an example for how to set the Install Code:

```
msixexec.exe /i ThycoticTmsSetup_x64.msi INSTALLCODE=1234XXXXABCD AMSURL=https://DOMAIN/Name/
```

Where:

- ThycoticTmsSetup_x64 is the install file used.
- INSTALLCODE is argument taking the install code value.
- AMSURL is the argument taking the base URL to the TMS installation.

If installing via a bundled installer, the install code is placed in the **Enter the Install Code** field (dashes in the install code are for readability and are optional).



Using the SetAMSServer.ps1 Script

If it becomes necessary to set the install code after the agent is installed, an install code can be set using a PowerShell script that must be run as an Administrator. This script, along with other useful agent scripts, will be located in the C:\Program Files\Thycotic\Powershell\Arelia.Agent folder on any machine with the Thycotic agent installed and it is called **SetAMSServer.ps1**.

The script will request parameters, as follows:

- The first parameter the script will request is the URL of the server you wish to connect to; its value should be `https://PrivilegeManagerURL/TMS/`.
- The second parameter it will ask for is the install code.

Agents can be installed without an install code, but they will be unable to register with the server until an install code is provided.

If older agents are used, the **Prevent Legacy Agent Registration (10.4 and older)** option might be checked in the **General** section under the **Admin | Configuration | Advanced** tab, which prevents older agents without install code from registering.

If an agent was previously installed and never revoked, the endpoint continues to have a valid certificate and a new agent can be installed with post-install registration.

For agents in an environment with a moderate policy configuration, the requirements for memory and disk space are as follows:

- Memory usage: 50Mb
- Disk usage:
 - Thycotic base agent: 10MB
 - Application Control Solution: 9MB
 - Local Security Solution: 3MB
 - Security Analysis Solution: 13 MB
- Average CPU over a week: 3%
- Impact to boot time: Negligible

Supported Windows Operating Systems (both 32- and 64-bit):

- Desktops: Windows 7, Windows 8, Windows 8.1, Windows 10
- Servers: Windows Server 2012 R2 and newer
- **Disable** the GPO security option "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing."

MacOS Agent

- MacOS 10.11 (El Capitan) or newer

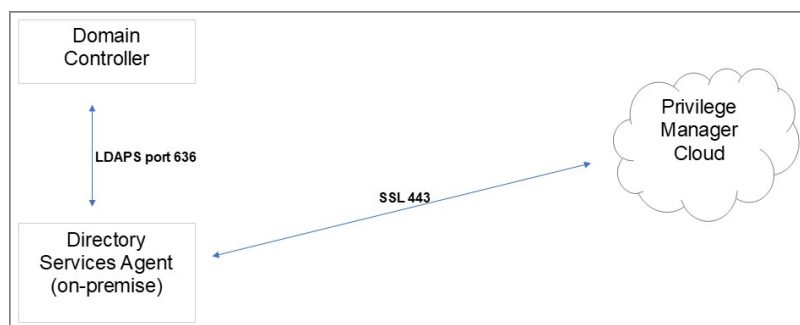
Note: Endpoints with Apple Silicon processor are not supported at this point.

Directory Services Agent

The Directory Services Agent needs to be installed on a well resourced system running either

- Windows 10 or above or
- Windows Server 2016 or above.
- Port requirements:
 - The agent needs to be able to communicate to the server on 443
 - AD Sync agent and Domain Controller over LDAPS

Note: The Directory Services Agent is available for x64-bit systems only.



Windows Management Framework download locations

Windows Management Framework 2.0 or newer

- Installed on Windows 7 and Windows Server 2012 R2 by default
- PowerShell 3.0 is installed on Windows 8 and Windows Server 2012 R2 by default
- Older operating systems require installation

Windows XP	http://download.microsoft.com/download/E/C/E/ECE99583-2003-455D-B681-68DB610B44A4/WindowsXP-KB968930-x86-ENG.exe
Windows Server 2008 (x86)	http://download.microsoft.com/download/F/9/E/F9EF6ACB-2BA8-4845-9C10-85FC4A69B207/Windows6.0-KB968930-x86.msu
Windows Server 2008 (x64)	http://download.microsoft.com/download/2/8/6/28686477-3242-4E96-9009-30B16BED89AF/Windows6.0-KB968930-x64.msu

.NET 4.0 Framework or newer

Windows 8 and newer and Windows Server 2012 and newer have 4.5 installed by default.

To download it, go to <http://www.microsoft.com/en-us/download/details.aspx?id=24872>.

.NET 2.0 Framework SP1

The .Net 2.0 SP1 update is required only for Windows XP. To download, go to http://download.microsoft.com/download/c/6/e/c6e88215-0178-4c6c-b5f3-158ff77b1f38/NetFx20SP2_x86.exe.

Ports/Agent Access Information

- **Outbound (port 443 - HTTPS):** This is the default access port through which the agent connects to the server. You may specify a different port based on your environment.
- **Inbound (port 5593):** This is the default and only port that the agent listens on. This port is not required and you can block port 5593. If you block the port, the agents pull updates from the server based on a set schedule.
- **SQL (port 1433):** This is the default SQL DB port. The SQL port can be customized.

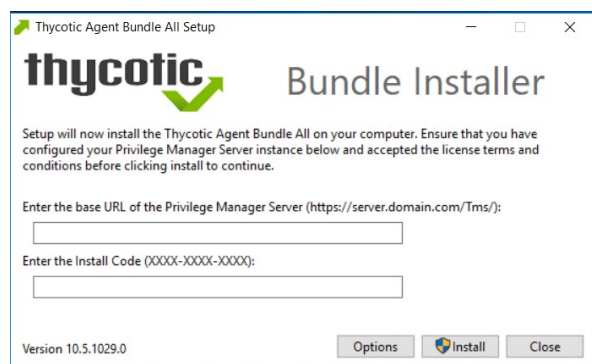
The bundled EXE installer is recommended when installing Privilege Manager on machines one at a time, for deployments through software delivery see the next section. This installer includes all Privilege Manager Agents for Windows machines (Core, ACS, LSS). You can use the bundled installer directly on individual endpoints for testing or for production environments in either 32-bit or 64-bit environments.

Important: To ensure you have installed all prerequisite software on your managed computers **before** you install the Thycotic agents, please see our [System Requirements for Privilege Manager](#) and [Agent System Requirements](#).

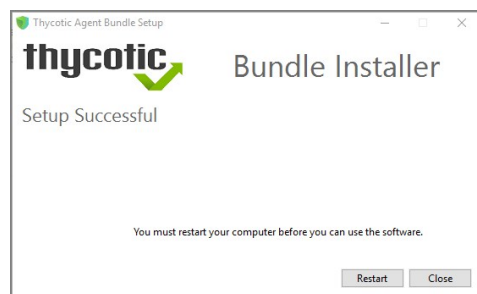
To install Thycotic agents **on a single testing machine**, follow these steps:

1. Download the [Bundled Agent Installer - Windows](#).
2. Run the Thycotic Bundled Installer on the computer you want to manage.
3. During the setup process, enter the Privilege Manager Server URL (or AZ Service Bus Queue URL) and the [Install Code](#) when prompted.

Note: The Install Code field can be left blank when using versions lower than 10.5.



4. After the installation you will be prompted to restart your endpoint.



Note: It may take 15-30 minutes for agents to receive new policies, to speed this up navigate to **Admin | Configuration | General** and click **Run Policy Targeting Update**, then open the Agent Utility on the endpoint and click the **Register** button.

Note: The bundled installer does require a restart in order to ensure the agent is completely ready to use.

Rollout to Multiple Systems

To install Thycotic agents **on multiple machines**, we recommend the following:

1. Download the [Agent standalone MSI](#) files based on specific systems.
2. Push them out through any software delivery system tool (e.g.: SCCM) using the recommended command lines.

Note: If you find that you've entered the wrong Privilege Manager Server address or want to change this settings, refer to the information under [Setting the Privilege Manager Server Address](#).

Silent Install

If the Bundled Agent Installer is run with the `/quiet` option for a silent install, the bundled installer will not accept the `installcode` or `baseurl` via the commandline. You have to set those values post install for the agent to be able to register with the server.

- [Agent Install Codes](#)
- [Setting the Privilege Manager Server Address](#)

Use the links below to download the agent installation software for Windows based endpoints.

There are three agents available for Windows endpoints:

- **Thycotic Agent:** The core agent is responsible for all reporting and monitoring communication on the endpoint. It can be considered the managing agent, while the Application Control and Local Security Agents are the worker agents.
- **Application Control Agent (ACS):** This agent is responsible for monitoring processes executing the Privilege Manager Application Control Functions on the endpoint.
- **Local Security Agent (LSS):** This agent is responsible for monitoring and executing Local Security functions.

Individual Agent Installers for Privilege Manager

Hardened Agents

If agent hardening was applied to user endpoints, the hardened agents need to be deleted via the `sc delete (agent name)` commandline command. This needs to be done under the context of the domain user prior to running the msi-based agent installation commands. When the agent is deleted successfully, a success message will be returned, for example:

```
C:\>sc delete arelliaagent
[SC] DeleteService SUCCESS
C:\>sc delete arelliaacsvc
[SC] DeleteService SUCCESS
```

Note: If the hardened agents are being deleted via software delivery script, the script needs to be delivered under the context of the domain user.

64-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools. For installing individual agents, begin with the Core Thycotic Agent:

- **Core Thycotic Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/ThycoticAgent_x64_10_8_1150.msi
- **Application Control Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_ApplicationControlAgent_x64_10_8_2185.msi
- **Local Security Solution Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_LocalSecurityAgent_x64_10_8_2183.msi

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

- **Core Thycotic Agent**

```
msiexec.exe /i "ThycoticAgent_x64_10_8_1150.msi" /norestart AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

- **Application Control Agent**

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x64_10_8_2185.msi" /norestart REBOOT=ReallySuppress /qn
```

- **Local Security Agent**

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x64_10_8_2183.msi" /norestart REBOOT=ReallySuppress /qn
```

32-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools. For installing individual agents, begin with the Core Thycotic Agent:

- **Core Thycotic Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/ThycoticAgent_x86_10_8_1150.msi
- **Application Control Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_ApplicationControlAgent_x86_10_8_2185.msi
- **Local Security Solution Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_LocalSecurityAgent_x86_10_8_2183.msi

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

- **Core Thycotic Agent**

```
msiexec.exe /i "ThycoticAgent_x86_10_8_1150.msi" /norestart AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

- **Application Control Agent**

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x86_10_8_2185.msi" /norestart REBOOT=ReallySuppress /qn
```

- **Local Security Agent**

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x86_10_8_2183.msi" /norestart REBOOT=ReallySuppress /qn
```

This agent supports the Active Directory synchronization between Privilege Manager Cloud instances and local directory services. This agent only needs to be installed on one system to perform the synchronization task. The local agent can be deployed into an AD environment instead of requiring direct connectivity from the server to the domain controllers. You will be able to configure the product in either method (direct or agent-based).

The agent method requires that the Directory Services Agent is installed on one computer connected to a domain controller. Once installed, the agent receives the Active Directory Sync (Agent) scheduled task along with other parameters such as the credential used, which AD objects, etc. to perform a synchronization between a Cloud instance and local AD.

Note: If the Directory Services Agent is installed on a system with an Application Control or a Local Security Agent, a license will be consumed. If a system has the Thycotic Agent (Core Agent) and Directory Services Agent installed ONLY, no license is consumed.

The Directory Services Agent for local AD synchronization with Privilege Manager Cloud instances is available for x64-bit systems only.

If the Directory Services Agent produces error messages about failed application control policy processing in the agent log, those messages can be ignored.

We recommend the following topics for details pertaining to the **Directory Services Agent** functionality:

- [Active Directory Synchronization](#), to learn how to setup and run the synchronization task on the **Synchronization** tab of the **Active Directory Domain** foreign system.
- [Agent System Requirements](#), to learn about the **Directory Services Agent** specific system requirements.

Prerequisites

The **Core Thycotic Agent** needs to be installed on the system that receives the **Directory Services Agent** installation. The other agents aren't required, but can be installed on the same system without issues.

Directory Services Agent Installation

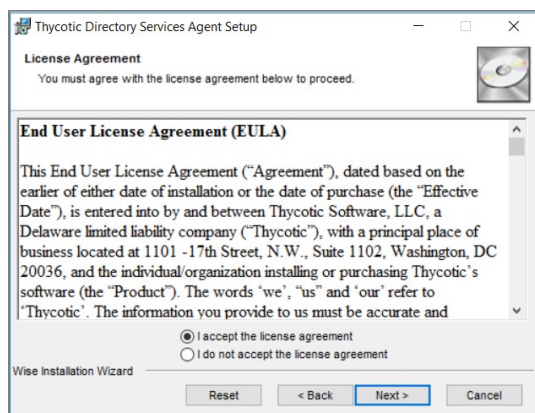
Download the latest version of the **Directory Services Agent** via the [Software Downloads](#) page.

1. Double-click the .msi file to start the installation wizard:



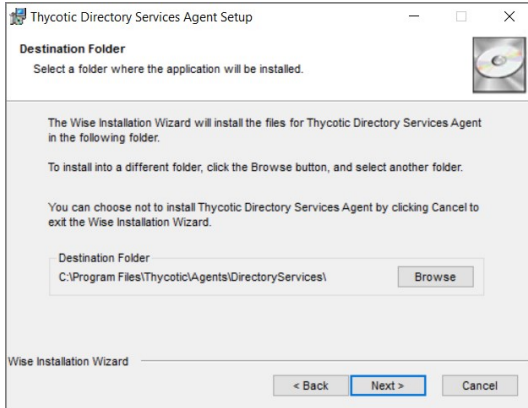
Close all other applications running on the system and click **Next**.

2. On the **EULA Agreement** screen, select **I accept the license agreement**.



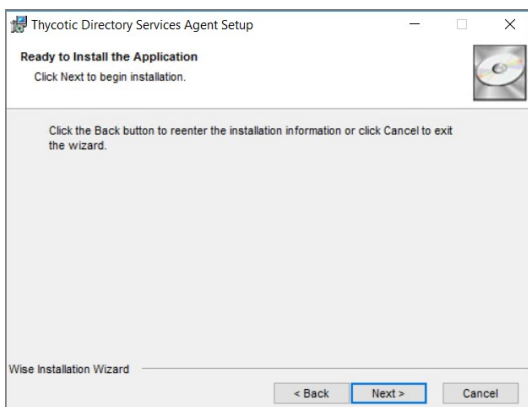
Click **Next**.

3. On the **Destination Folder** screen, keep the default installation destination or use **Browse** to select a different folder.



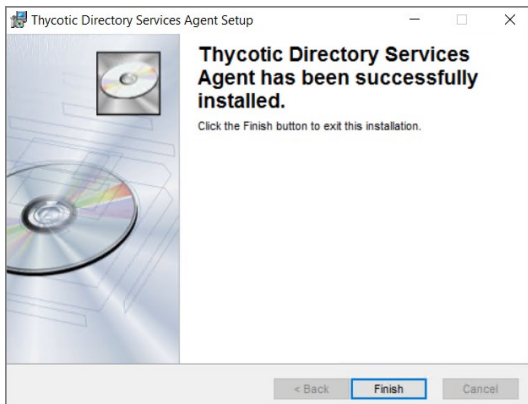
Click **Next**.

- On the **Ready to Install** screen, you have an option to go back to change your previous selection, otherwise click **Next** to proceed with the installation.



If you have any other Thycotic Agents already installed on the system, the installer may prompt you to stop the services before you can proceed.

- After a successful installation of the Directory Services Agent, you will see the following screen:



Click **Close**.

- Restart any previously stopped agent services.

The Bundled Mac Agent DMG + PKG installer is available for macOS systems. You can use this installer directly on individual endpoints for testing or for production environments.

Starting with 10.8.2 Thycotic provides two macOS Agent installers,

- one in support of **KEXT** based endpoint versions (10.8.xx) and
- the other in support of **SYSEX** based endpoint versions (10.8.xxxx).

For details about differences regarding KEXT and SYSEX, refer to [macOS Extensions](#).

Refer to the [Software Downloads](#) for the current versions available.

Installing macOS Agents

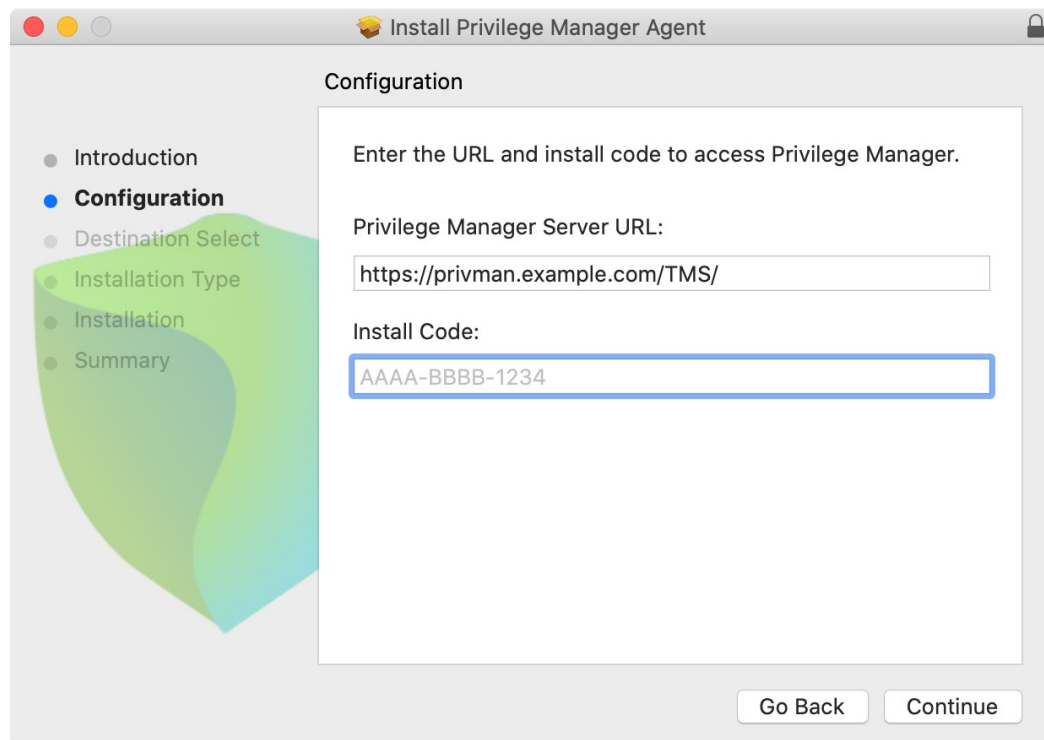
Note: If you enter the wrong install code or you need to update an install code for whatever reason, rerun the package installer to provide the correct/new install code. The Install Code field can be left blank when using versions lower than 10.5.

Directly

The Bundled macOS Agent is a DMG + PKG file. You can use this Mac agent installer directly on individual endpoints for testing or production environments.

To install the agent software on a single testing machine, follow these steps:

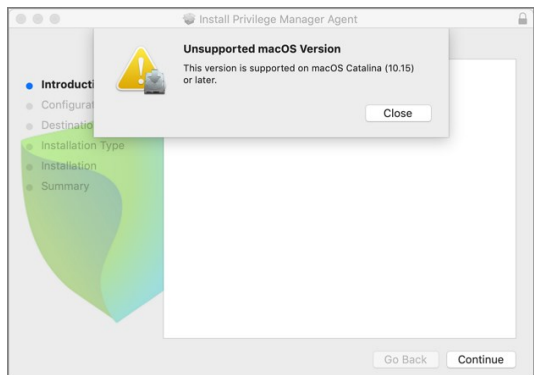
1. Go to
 - [Agent Downloads - KEXT](#) or
 - [Agent Downloads - SYSEX](#) to download the Privilege Manager Mac Agent.
2. Run the Bundled Mac Agent DMG + PKG Installer on the computer you want to manage.
3. During the setup process,
 1. enter the base URL and
 2. the Install Code when prompted.



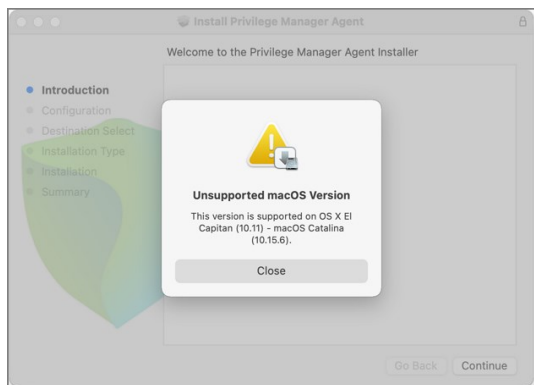
Note: The bundled installer does require a restart in order to ensure the agent is ready to use.

Unsupported Version Messages

If you attempt the to install the **SYSEX** agent bundle on an unsupported OS version, the following message is displayed:



If you attempt the to install the **KEXT** agent bundle on an unsupported OS version, the following message is displayed:



Using an Unattended Install Method

Begin by downloading the DMG + PKG package (See link for Privilege Manager Mac Agent listed above) on one of your Mac endpoints. Run the installer by double clicking the PKG file.

After installing this first agent, navigate to `/Library/Application Support/Thycotic/Agent/agentconfig.json`. The agentconfig.json file stores information such as your organization's URL and a few other custom settings like 'Task Polling Interval,' etc.

Open the file and add the "installCode" parameter after the "tmsBaseUrl" to that file as shown in the following code sample:

```
{
  "tmsBaseUrl": "https://servername/Tms",
  "installCode": "VALUEHERE"
}
```

There are two methods for deploying your remaining Mac agents in an unattended fashion:

- Network File Share
- Distribution Tool

Network File Share

If you want administrators to deploy agents onto individual macOS endpoints, save the PKG installer from the DMG side-by-side with the **agentconfig.json** file in a network share folder.

Due to new macOS security enhancements, users cannot run a PKG installer from a network share anymore. The administrator must then run the installer command-line tool from **Terminal.app** after mounting and cd'ing to the directory containing the PKG installer and **agentconfig.json** file:

KEXT

```
cd /Volumes/<network share>/<path to PKG installer>
sudo installer -pkg ThycoticManagementAgent-10.8.27.pkg -target /
```

SYSEX

```
cd /Volumes/<network share>/<path to PKG installer>
sudo installer -pkg ThycoticManagementAgent-10.8.1019.pkg -target /
```

The PKG will first look for an **agentconfig.json** file located in the same folder. When it finds this file, it will copy **agentconfig.json** into the `/Library/Application Support/Thycotic/Agent` folder during the unattended install on the Mac endpoint where the installer is running.

Distribution Tool

Using a Deployment Tool like Jamf or SCCM, include both the PKG installer and the **agentconfig.json** files in the distribution package together, then deploy the package onto your endpoint Macs by running a script using a tool or remotely by using ssh to install the PKG, for example:

KEXT

```
sudo installer -pkg ThycoticManagementAgent.10.8.27.pkg -target /
```

SYSEX

```
sudo installer -pkg ThycoticManagementAgent.10.8.1019.pkg -target /
```

As in the example using a Network Share, the PKG will first look for an **agentconfig.json** file located in the same folder. When it finds this file, it will copy **agentconfig.json** into the `/Library/Application Support/Thycotic/Agent` folder during

the unattended install on the endpoint Mac where the installer is running.

For more instructions on how to deploy in bulk using Microsoft Software System Center Configuration Manager (SCCM), Microsoft instructions for Macs are described [here](#).

After Initial Deployment

If the Mac already has an existing **agentconfig.json** file, it will NOT be overwritten because creating a file only occurs if the computer didn't already have an **agentconfig.json** installed. This means you can use the same distribution package for upgrades and new installs.

Note: It will take 15-30 minutes for newly installed agents to register in Privilege Manager. See the agent registration information in the [Terminal Commands](#) topic to speed the process up.

Uninstalling an Agent

When you need to uninstall the macOS Agent, use the **Uninstall.sh** shell command:

KEXT

```
sudo /Volumes/ThycoticManagementAgent-10.8.27/Uninstall.sh
```

SYSEX

```
sudo /Volumes/ThycoticManagementAgent-10.8.1019/Uninstall.sh
```

The **Thycotic Directory Services Installer** bundle delivers the Thycotic Agent (Core Agent) and the Thycotic Directory Services Agent in one package for installation on x64-bit systems.

We recommend to refer to the following topics before you proceed with the bundled installation:

- [Directory Services Agent \(AD\)](#), to learn more about the **Directory Services Agent** itself.
- [Active Directory Synchronization](#), to learn how to setup and run the synchronization task on the **Synchronization** tab of the **Active Directory Domain** foreign system.
- [Agent System Requirements](#), to learn about the **Directory Services Agent** specific system requirements.

Installing the Thycotic Directory Services Installer Bundle

To install this Thycotic agents bundle **on a single machine**, follow these steps:

1. Download the [Bundled Privilege Manager Core and Directory Services Agent - Windows](#).
2. Run the **ThycoticDirectoryServicesInstaller** on the computer you want to use for the active directory synchronization tasks.
3. During the setup process, enter the Privilege Manager Server URL (or AZ Service Bus Queue URL) and the [Install Code](#) when prompted.

Note: The Install Code field can be left blank when using versions lower than 10.5.



4. Click **Close** after the installation completes.

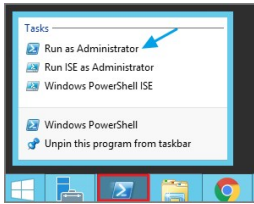
Note: It may take 15-30 minutes for agents to receive new policies, to speed this up navigate to **Admin | Configuration | General** and click **Run Policy Targeting Update**, then open the Agent Utility on the endpoint and click the **Register** button.

This topic explains how to uninstall the Agent through command line. If you're trying to uninstall an old agent in order to install a newer version of the agent, there is no need to do so. The installers will detect a previous version installed and uninstall the old version prior to installing the new agent.

Note: For hardened agents refer to information under [Windows Agents](#).

Manual Uninstall Steps

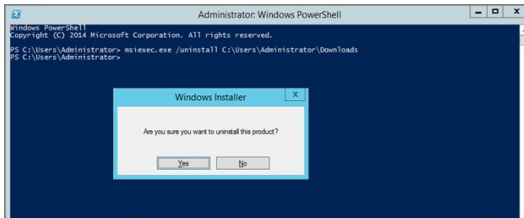
1. Navigate to the machine(s) where the agent is located.
2. Right-click on Windows Powershell and select **Run as Administrator**.



3. Run the following command:

```
msiexec.exe /uninstall <path to the msi installer>\ThycoiticAgent_x64_10_8_1155.msi
```

4. Select **Yes** on the Windows Installer prompt.



Privilege Manager software updates are made available via NuGet server packages. The upgrade process can be performed via **Add/Upgrade Features** link in the Privilege Manager Setup page.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

What's New in Privilege Manager 10.8

The 10.8 release of Privilege Manager introduces a new user interface, providing a redesigned user experience, simplifying many major areas and typical workflow processes when setting up application policies or local security.

To preview the enhancements made to the user interface, please view this [video](#).

Switching between the new and old UI post upgrade is not available.

Setting up the NuGet Source

Once Privilege Manager is installed on a server, updates can be performed by pointing the web.config file to the product NuGet source.

1. Navigate to C:\inetpub\wwwroot\TMS\ and right-click the web.config file.
2. Select Edit from the drop-down.
3. Verify the following line with correct NuGet source is present:

```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget" />
```

Updating Privilege Manager

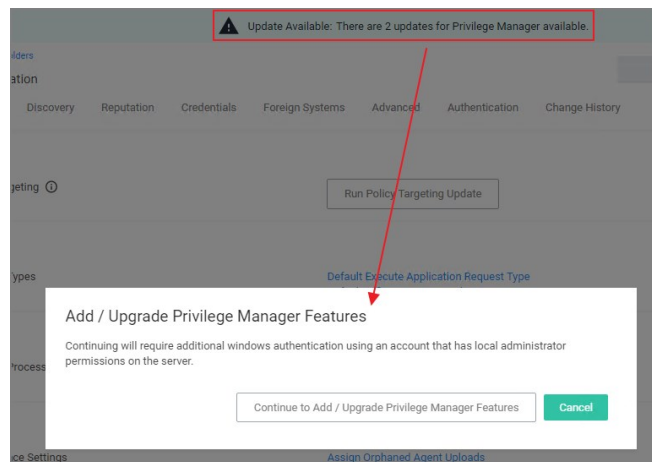
Note: Always make a backup of the Privilege Manager Database in SQL and the TMS web files before performing upgrades in a production environment. The default location of the web files on the Privilege Manager Server C:\inetpub\wwwroot\TMS.

On systems running Privilege Manager 10.5.1 or older with multiple Privilege Manager Server nodes, **stop** the TMS application pools on all secondary nodes before starting the upgrade. Restart the applications pools once the upgrade is completed. Newer Privilege Manager versions automatically initiate setup tasks when the primary node is being updated.

Primary Node

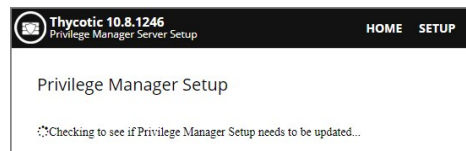
Privilege Manager provides an **Update Available** notification banner when updates are available. Users can also use the **Admin | Setup** menu to enter the check if an update is available.

1. Click the link in the banner to trigger the **Add / Upgrade Privilege Manager Features** modal:

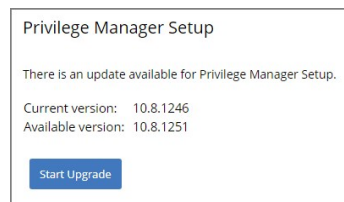


If you are not a local Administrator on the server, you will not be able to perform the upgrade. Based on your account role membership either click **Continue to Add / Upgrade Privilege Manager Features** or **Cancel** if your role permissions don't meet the requirement.

This starts the process to see if setup updates are available.



2. When updates are available, Privilege Manager will provide information about the current and available versions.



Click **Start Upgrade**.

3. A short *Install Complete* message is displayed before the setup process navigates to the **Currently Installed Products** page. The available product updates are listed by product name in alphabetical order.

Product Name	Installed	Available	Published	
Application Control Solution	10.8.1072	10.8.1078 New	8/3/2020 1:00 PM	Upgrade
Cylance Reputation Connector	10.8.1035	10.8.1078 New	8/3/2020 1:04 PM	Upgrade
Directory Services Connector	10.8.1121	10.8.1148 New	8/6/2020 1:20 AM	Upgrade
File Inventory Solution	10.8.1020	10.8.1021 New	7/21/2020 12:53 PM	Upgrade
Local Security Solution	10.8.1032	10.8.1033 New	7/21/2020 12:53 PM	Upgrade
Privilege Manager	10.8.1961	10.8.2032 New	8/11/2020 2:42 PM	Upgrade
Privilege Manager Application Programming Interface	10.8.1136	10.8.1139 New	8/11/2020 2:39 PM	Upgrade
Privilege Manager Mobile Console	10.8.1007	10.8.1008 New	7/21/2020 12:53 PM	Upgrade
Privilege Manager Server Core Maintenance	10.8.1396	10.8.1437 New	8/6/2020 10:05 PM	Upgrade
Privilege Manager Server Core Solution	10.8.1396	10.8.1437 New	8/6/2020 10:05 PM	Upgrade
Privilege Manager Silverlight Console	10.7.1447	10.7.1447	3/9/2020 6:41 PM	Repair
ServiceNow Connector	10.8.1006	10.8.2014 New	8/4/2020 4:51 PM	Upgrade
Symantec Management Platform Connector	10.7.1008	10.8.1003 New	7/21/2020 12:53 PM	Upgrade
SysLog Connector	10.8.1012	10.8.1013 New	7/21/2020 12:53 PM	Upgrade
System Center Configuration Manager Connector	10.8.1005	10.8.1012 New	7/21/2020 12:53 PM	Upgrade
VirusTotal Reputation Connector	10.8.1035	10.8.1078 New	8/3/2020 1:03 PM	Upgrade

[Install/Upgrade Products](#) [Refresh](#)

Use either of the following ways to upgrade your environment to the latest Privilege Manager version:

1. Click Upgrade next to individual packages, this will require to come back to the Installed Products page after each separate upgrade for most of the packages, **or**
2. Click **Install/Upgrade Products** at the bottom of the page.

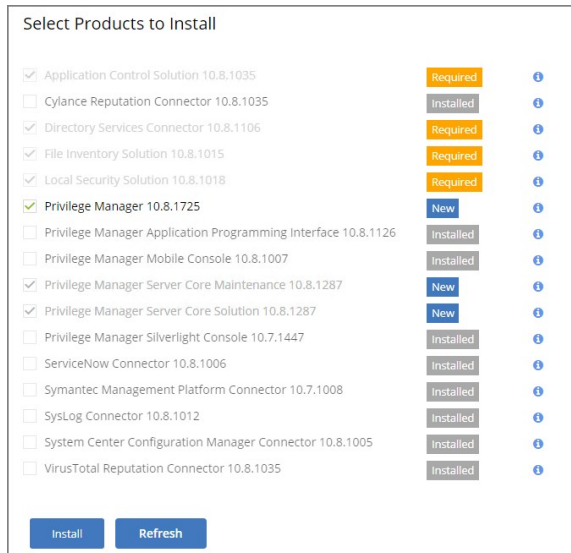
1. Select the products you want to install/upgrade.

Select Products to Install

- Application Control Solution 10.8.1078 [New](#) [i](#)
- Cylance Reputation Connector 10.8.1078 [New](#) [i](#)
- Directory Services Connector 10.8.1148 [New](#) [i](#)
- File Inventory Solution 10.8.1021 [New](#) [i](#)
- Local Security Solution 10.8.1033 [New](#) [i](#)
- Privilege Manager 10.8.2032 [New](#) [i](#)
- Privilege Manager Application Programming Interface 10.8.1139 [New](#) [i](#)
- Privilege Manager Mobile Console 10.8.1008 [New](#) [i](#)
- Privilege Manager Server Core Maintenance 10.8.1437 [New](#) [i](#)
- Privilege Manager Server Core Solution 10.8.1437 [New](#) [i](#)
- ServiceNow Connector 10.8.2014 [New](#) [i](#)
- Symantec Management Platform Connector 10.8.1003 [New](#) [i](#)
- SysLog Connector 10.8.1013 [New](#) [i](#)
- System Center Configuration Manager Connector 10.8.1012 [New](#) [i](#)
- VirusTotal Reputation Connector 10.8.1078 [New](#) [i](#)

[Install](#) [Refresh](#)

By default the products available for upgrade are listed. If you want to see all products currently installed, click **Show Installed products**.

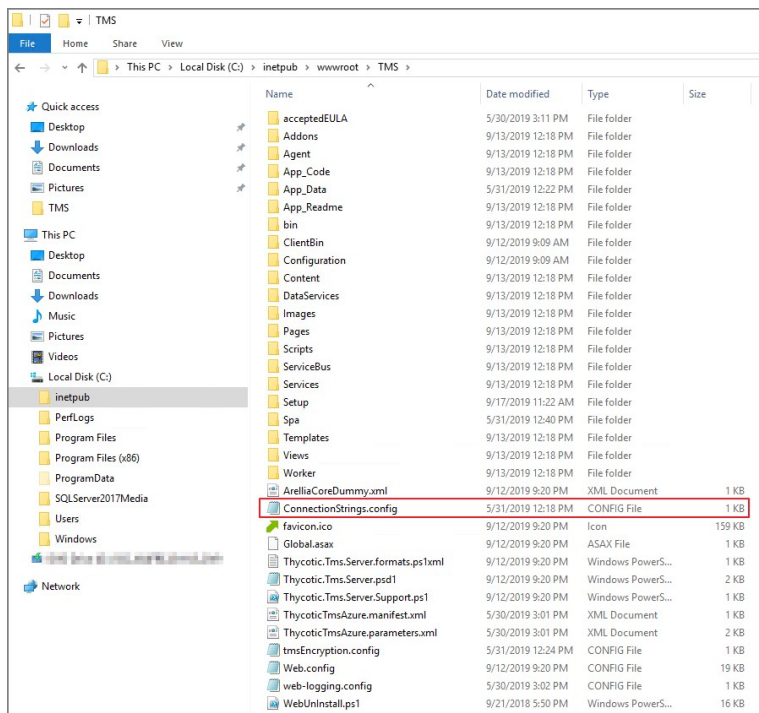


2. Click **Install**.

The installation/upgrade process starts and you can view the log while products are being installed.

Secondary Nodes

1. On the upgraded primary node navigate to TMS web files. The default location is: C:\inetpub\wwwroot\TMS.
2. Copy the TMS folder, except for the ConnectionStrings.config file.



3. On your secondary node navigate to the same folder location, most likely C:\inetpub\wwwroot\TMS and paste the copied files.
4. Repeat this the copy and paste for all other secondary Privilege Manager nodes in your environment.
5. Navigate to the IIS Manager and start all TMS Application pools on the secondary nodes.

Follow these steps to perform an offline upgrade for Privilege Manager. This article is ONLY applicable when upgrading from versions 10.2 and higher.

Note: Offline upgrades on **multiple** servers will need to be done manually.

1. Download the latest version for the Privilege Manager Offline Upgrade from [Software Downloads](#).
2. Extract the zip file.
3. From the unzipped folder, copy the contents of the nugetCache folder to this location on the web server: C:\ProgramData\NugetCache\.
4. Navigate to the TMS web folder (C:\inetpub\wwwroot\TMS), right-click and open with, e.g. **Notepad > Run as Administrator** the **web.config** file.
 1. Update the "value" field of this item <add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" /> to C:\ProgramData\NugetCache\, SUCH AS
<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NugetCache\" />
 2. Save the **web.config** file.
 3. Recycle the TMS app pools.
5. Navigate to <https://<webserver>/TMS/Setup/ProductOptions/ShowProducts>. This step will require windows authentication using an account that has local administrator permissions on the web server.
6. You should see new products available in the products list. Click the **Install/Upgrade Products** button.
7. Select the products you wish to upgrade or install, and follow the steps to finish the installation. If one of the products fails to install, please repeat these last two steps. You may encounter an issue with an error of "Version Store out of Memory" - this is transient and re-starting the upgrade will fix it. If you encounter any additional errors, please contact Thycotic Technical Support for assistance.

Note: An upgrade or repair to the product may rewrite the web.config with default settings. Always double-check that the web.config has the correct SolutionCentre path whenever you perform a manual upgrade. Also, the version numbers available should match the highest versions available in the C:\ProgramData\NugetCache\ folder on the web server.

Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Follow these steps to perform an offline upgrade for Privilege Manager and Secret Server. This topic is ONLY applicable when upgrading from products that are versions 10.2 and higher.

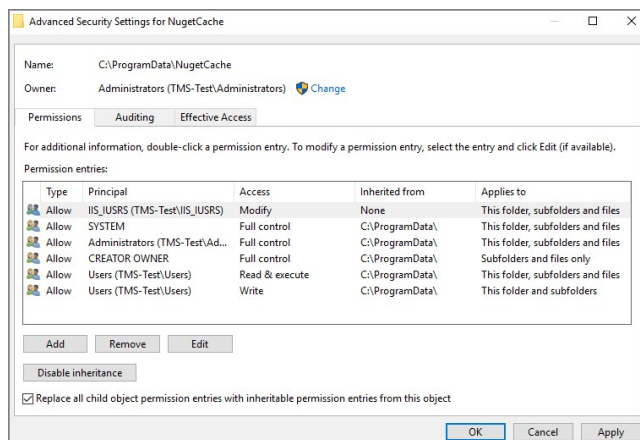
Note: Offline upgrades on **multiple** servers will need to be done manually.

1. Download the zip files for your offline upgrade [here](#). Copy/paste this zip file on your Privilege Manager Web server
2. Make a backup of the Secret Server and TMS web folders (Default path is C:\inetpub\wwwroot> SecretServer + TMS folders, copy/paste these into a backup folder)
3. Make a backup of the Database (In Secret Server navigate to Admin | Backup | Backup Now button)
4. On the web server, navigate to C:\ProgramData\NugetCache and delete all the files in the folder (*ProgramData folder may be hidden: View > check the Hidden items box to reveal)
5. Open Secret Server and navigate to: <https://<YourSecretServerURL>/Setup/Upgrade>
6. On the Secret Server Update page:

1. Select **Advanced (not required)** to open the advanced options.
2. Select **Choose File** and navigate to the location of the Secret Server Update zip package.
3. Select **Upload Upgrade File**.
4. When the new version is available select **Upgrade**.
Check <https://URL/TMS/Setup> to see if an install is already in progress (this is usually seen when the TMS Upgrade portion of SS shows successful)

7. Accept the License. Then allow the Secret Server upgrade to complete. Note: The Upgrade TMS step may say it was successful, or it may say it wasn't. Please ignore this message and continue to follow the steps below:
8. Open the C:\ProgramData\ folder:

1. Right-click on the NugetCache folder and select **Properties**.
2. Click on the **Security** tab.
3. Click the **Advanced** button.
4. Check the **Replace all child object permission entries with inheritable permission entries from this object** checkbox



5. Click the **OK** and **Yes**.
9. Navigate to the TMS web folder (C:\inetpub\wwwroot\TMS), right-click and open with, e.g. **Notepad > Run as Administrator** the **web.config** file.
 1. Update the "value" field of this item <add key="nuget.source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" /> to C:\ProgramData\NugetCache\, SUCH AS
<add key="nuget.source:SolutionCentre" value="C:\ProgramData\NugetCache\" />
 2. Save the **web.config** file.
 3. Recycle the TMS app pools.
10. Navigate to <https://<webserver>/TMS/Setup/ProductOptions/ShowProducts> The TMS setup page requires authentication with a Windows account that is a Local Administrator of the Web Server.
11. You should see new products available in the products list. Click the **Install/Upgrade Products** button.
12. Select the products you wish to upgrade or install, and follow the steps to finish the installation. If one of the products fails to install, please repeat these last two steps. You may encounter an issue with an error of "Version Store out of Memory" - this is transient and re-starting the upgrade will fix it. If you encounter any additional errors, please contact Thycotic Technical Support for assistance.

Note: An upgrade or repair to the product may rewrite the web.config with default settings. Always double-check that the web.config has the correct SolutionCentre path whenever you perform a manual upgrade. Also, the version numbers available should match the highest versions available in the C:\ProgramData\NugetCache\ folder on the web server.

Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Upgrading from our 8.2 version to Privilege Manager 10.4 and up can't be done from <https://servername/Ams/Setup/>. To upgrade, we recommend using the same database and removing the old application before installing the new version. This can be done automatically or manually.

Automatic Steps

1. Download http://tmsnuget.thycotic.com/Software/ThycoticTmsinstaller_10_0_1570.exe and run it on the web server where your existing Arellia Management Server 8.x version is installed.
2. Follow the prompts.
3. Once it completes, you'll access the server at <https://servername/Tms/> instead of <https://servername/Ams/>.
4. Go to <https://servername/Tms/Setup> to install the latest 10.x version.
5. Open **IIS Manager** and go to **Sites | Ams | Agent | Uploads**.
6. Click on the **BITS Uploads** and change the notification URL from <http://localhost/Ams/Services/BitsUpload.ashx> to <http://localhost/Tms/Services/BitsUpload.ashx>.
7. Download and install the latest agents. Please refer to the agent installation section [the latest agent installation](#).

Note: Old agents will continue to work because of the redirect created during the install that sends traffic from <https://servername/Ams/Agent> to <https://servername/Tms/Agent>. When upgrading the agents, we recommend that you set the **AMSURL** to the new <https://servername/Tms/> address.

Manual Steps

1. Remove the AMS website from the web server.
2. Download the latest bundled installer <http://thycotic.com/products/secret-server/resources/download-secret-server/>.
3. Follow the prompts to install Privilege Manager, setting the database connection to the existing database.
4. Download and deploy the latest agents that are [available here](#).

Note: Set the AMSURL to the new server address, <https://servername/Tms/>

DB Backup

Thycotic recommends that Privilege Manager databases are backed-up prior to an upgrade. For details regarding SQL database backups, refer to the vendor documentation of your SQL database, such as [Back Up and Restore of SQL Server Databases](#).

TMS Folder Backup

Other measures to take before any upgrade are to make a backup copy of your Privilege Manager TMS folder and all it's contents.

1. On your Privilege Manager host system navigate to C:\inetpub\wwwroot\TMS (default installation location).
2. Create a backup copy of the TMS folder contents at another location on your system or network.

Repair Solution

When running into an error condition during an upgrade, try the repair option for the specific solution that errored out.

Also refer to [Troubleshooting - Installation and Upgrade Issues](#).

Privilege Manager Agents

The [Privilege Manager Agents](#) are a critical component of Thycotic's application control and local security, giving you the ability to evaluate the health and status of endpoints in real time. Agents are required on endpoint machines to implement Privilege Manager policies.

Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and endpoint operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

Privilege Manager supports agents on:

- Windows
- macOS

endpoint operating systems.

For information about installing agents, refer to [Agent Installation](#) to review agent system requirements and the specific agent installation procedures. This section of our document is a general agent information section, containing details about how to use/interact with agents and to provide information about the agent processes.

To make sure that local Administrators do not tamper with Thycotic agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Thycotic Agent or Thycotic Application Control. Refer to [Agent Hardening](#).

When your agents are installed, you can verify the status of your Agents' health in terms of Registration State and Policy State from the Home page. You also can navigate to **Admin | Agents** for more information about installed agents.

The Agent Health dials describe how many Managed Operating Systems you have as well as your Agent(s) Registration State and Policy State. If you click on the Agent Registration State dial, you will see a report on a list of machines (the "MonitoredResource" column) where each registered agent is installed.

Clicking the Agent Policy State dial from the Home dashboard brings you to a report that links all of your agent-registered machines with the Number of Policies Missing from each agent. This page will become invaluable once you have multiple policies running over different computer groups in your network.

Agent Diagnostics

Once your agents are installed, verify that they have registered in Privilege Manager. Navigate to either:

- **Admin | Diagnostics** to access the **Diagnostics** page or

Diagnostics

This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.

Clear Descriptive Item Cache Clear Local Storage Cache Import Items Console Logs

Managed Operating Systems Agent Registration State Agent Policy State Password Age

System Health: **Normal**

- Remote Task Status: **Normal**
- Number of Old Computers: **Normal**
- Unacknowledged Events: **Normal**
- Pending Approvals Count: **Normal**
- Number of Application Events: **Normal**
- File Uploads Size: **Normal**
- Background Message Queue Size: **Normal**
- Background Message Queue Older than 1 Week: **Normal**

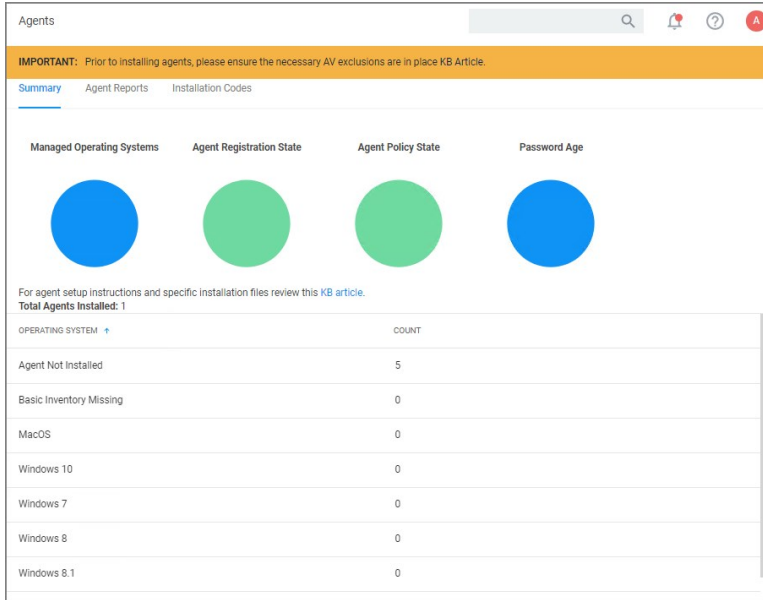
Licensing: **Normal**

- Client License Expiration: **Normal**
- Server License Expiration: **Normal**

Key Configuration Settings: **Properly Configured**

- Product Licenses Installed: **Normal**
- Server Activity Paused: **Information**
- Update Available: **Properly Configured**
- Configure Active Directory: **Properly Configured**
- Set Default User Credential: **Properly Configured**
- Install Agents: **Properly Configured**

- **ADMIN | Agents** to view your agent details.



After the initial policies are received, future updates will be based on the task schedules set in Update Applicable Policies and Scheduled Registration policies. Ensure to select the correct policies based on Windows or Mac operating systems. To edit these schedules, navigate to your computer group and select **Scheduled Jobs**. The **Triggers** can be customized under the **Job Schedule** section.

On the agent details page you will see the quantity of agents registered and what operating system is running on registered endpoints. Registered endpoints can also be viewed in the report **Agent Installation Summary** by navigating to the **Agent Reports** tab.

- Agent Installations**
Lists computers and their installed agent information.
- Agent Summary by OS**
List of Operating Systems discovered with or without the agent installed.
- Agent Registration State**
A chart showing the state of agent registration.
- Agents missing a policy**
Lists computers with the agent installed that are missing a Policy.
- All policies not received by agents**
Lists computers with the agent installed and which policies have not been received by each agent.
- Agent Policy State**
Chart showing the breakdown of agents missing policies. Normal means 0 policies are missing.

From the reports pages you can click into any of the **target machines** listed that have a Thycotic agent installed. Pictured below is a view from one of these resource pages where you can check the machine's System Health and configured policies.

Name	test-lab-docs
Created	May 31, 2019, 12:24:52 PM
Modified	May 31, 2019, 12:24:52 PM

Health

- Normal
 - Policy State
- Normal
 - Registration State
- Managed
 - Managed or Unmanaged State

The agent traffic is secured via SSL/TLS (1.2).

Starting with Privilege Manager version 10.8.2, the agent adds memory checks for all processes that are managed/elevated via Privilege Manager. Any processes not managed by Privilege Manager, should be checked for process hollowing

through means of products like Windows Defender ATP.

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents **independent** of the endpoint operating system.

The following topics are available:

- [Setting the Privilege Manager Server Address](#)
- [Connecting Agents to the Privilege Manager Server](#)
- [Agent Trust Revocation](#)
- [Uninstalling an Agent with Script](#)
- [How to prevent Backwards Compatibility for Agents v10.4 and earlier](#)
- [Configuring for a Test Environment](#)
- [VM Deployments](#)
- [Agent Tasks](#)

Agents require a Privilege Manager Server to communicate with. The recommended way to set the URL address is during the [installation of the Thycotic Agent](#). If an Azure Service Bus or Reverse Proxy is used, the URL can point at the URL of those components.

The URL address can be changed post-install via the registry or PowerShell.

Setting the Privilege Manager Server (TMS) Address via PowerShell

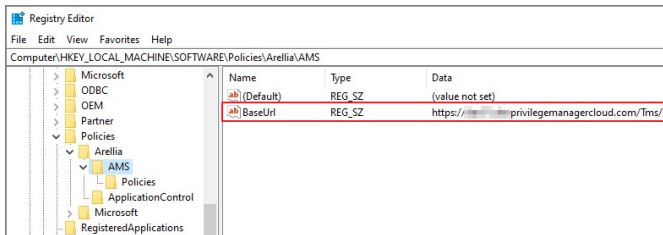
To set the Privilege Manager Server (TMS) address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\Powershell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server.

Changing the Privilege Manager Server (TMS) Address via the Registry Editor

1. Open the Registry Editor (regedit)
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**
3. Right click BaseUrl and select Modify.



4. In the Edit String dialog box, change the BaseURL to your TMS Address.
5. Close the registry.
6. Restart the Agent service.

Privilege Manager agents are installed on endpoint machines to implement policies which are defined by the user (the Privilege Manager administrator) in the Privilege Manager console (the user interface of the Privilege Manager Server).

This article is about agent deployment to endpoints in Virtual Desktop Infrastructure (VDI) or other similar environments. It describes the different cases and options for deploying Privilege Manager agents to VDIs and discusses the pros and cons where relevant. It is expected to be read by a user who is the Privilege Manager administrator for the customer.

Installing the Privilege Manager agent is supported as part of a VDI image build. There are a few different ways to accomplish this, based on the (Privilege Manager) customer's environment and preferences. Discussion of the relevant issues and options is grouped in this article as follows:

Identifying Agents to The Console

The pertinent question here is: Do you (the user) plan to use (or are using) persistent virtual machines (VMs) or dynamic VMs? There are different implications for each of these, discussed below.

Persistent VMs

In a persistent VM, machines images are created, spun up, and then persist indefinitely. This case is fairly simple. We can treat these machines the same as we would physical machines except for concerns around the universally unique identifier (UUID), which will be discussed further on (in the section, "Multiple VMs Collapsed to a Single Resource").

Dynamic VMs

In a dynamic VM, a golden image is spun up each time a user requests it with their profile and it is then applied on top. This case is more complicated.

The major concern is agent spamming, which would happen as follows: the Privilege Manager console sees each new image as a new computer and rapidly runs through the customer's licenses, leaving a large number of orphan machines. There are a few different ways to deal with this situation, discussed in the sub-sections below.

Multiple VMs Collapsed to a Single Resource

The easiest way to support dynamic VMs is for you to collapse all of your VMs to a single computer resource on the console. This can be accomplished as follows:

1. Add a registry entry in HKLM\Software\Arellia\Agent called "AgentIdOverride."
2. Install the agent on a physical computer and allow it to register.
3. Next, in the Privilege Manager console:
 1. Navigate to Admin > Agents.
 2. Click on one of the charts to view a list of registered computers.
 3. Find the computer in the report and click on it. This will take you to the Resource View of that computer. The ID for this computer is the UUID displayed as the last part of the URL (after "/item/view/") in the browser address bar.
 4. Copy this ID value (the last part of the browser URL).
4. Place the copied ID value in the AgentIdOverride registry entry.

Alternatively, if you want multiple VDI images to which differing policy sets are applied, you could have different values. The rollout computers in the console could then be assigned to the appropriate resource targets.

The benefits of this approach are:

- It is by far the simplest to implement.
- It results in the fewest licensing issues.
- Moreover, because the resources are created ahead of time they can be inventoried and assigned to the appropriate resource targets. Consequently, a machine would get the appropriate policies as soon as it spins up with no need to wait for processes to run either on the desktop or server.

The downside of this approach is:

- There would be some loss of fidelity in data on the console, specifically around which machine an event happened on. However, since virtual desktops are by nature transitory that may be less of a concern. Privilege Manager will still attach usernames to the event data so you will know "who" (the end user) if not necessarily "where" (the specific endpoint).

Pool of Values to Support Multiple VMs

If you wish to be more specific, the following technique could be used: create a pool of UUID values to be assigned to the AgentIdOverride and assign one from this pool when the machine spins up.

With this technique, as part of the VDI provisioning, Privilege Manager would trigger the basic inventory task to make sure that the server gets correct information on the machine name and details. You would want a pool of values rather than a random one to prevent spamming new agents. Reusing the values would keep that under control.

Managing Agent Trust and Certificates

This section discusses certificate management.

As of version 10.5, Privilege Manager validates agent certificates against the specific agent that was initially registered. There are two cases:

- All desktops using a single agentID: This case is fairly straightforward. A single certificate would be included as part of the desktop image which would match what was stored in the database for that ID and all of the communication would be accepted.
- A pool of IDs: In this case, there are two potential ways to do certificate management:
 - Method 1: Navigate to Admin > Configuration > Advanced; select the "Allow Agent Certificate Mismatch" option; turn on the option. (It is off by default.)
 - Method 2: Deploy the install code on machine imaging, as follows:
 - Add a registry entry in HKLM\Software\Arellia\Agent of type String and call it "InstallCode."
 - In the Privilege Manager console:
 - Navigate to Admin > Agents > "Installation Codes" tab.
 - Click "Copy" to copy the value displayed under Code.
 - Paste the copied value into the InstallCode registry entry.
 - Once this entry is set, then during the agent registration process, the agent sends this InstallCode up to the server along with whatever certificate it has. This overrides the database entry and allows that agent to communicate as long as it is up and running.

Minimizing Time Between VDI Deployment and Policy Enforcement

This section is about policy deployment.

In a non-VDI environment, when Privilege Manager deploys agents to desktops, there can be a significant delay between deployment and policy enforcement and it is not a concern because it is a one-time issue.

However, in the case of VDI, machines are created and recreated daily and this delay becomes a larger issue. In this case, you must make sure that the Client Items database, with the appropriate policies, is part of the initial desktop image. This file can be created in C:\ProgramData\Arellia\ClientItems and can be simply copied from a machine that has the agent deployed and all policies downloaded.

However, if any policy changes are made after image creation you would need to either update that file in the golden image or add a post-deployment step to run the Powershell script "C:\Program Files\Thycotic\Powershell\Arellia.Agent\UpdateClientItems.ps1" and trigger the virtual desktop to download the latest policy items.

Licensing Concerns with Windows 10 Amazon Workspaces

This section discusses licensing concerns, specifically with Windows 10 Amazon Workspaces.

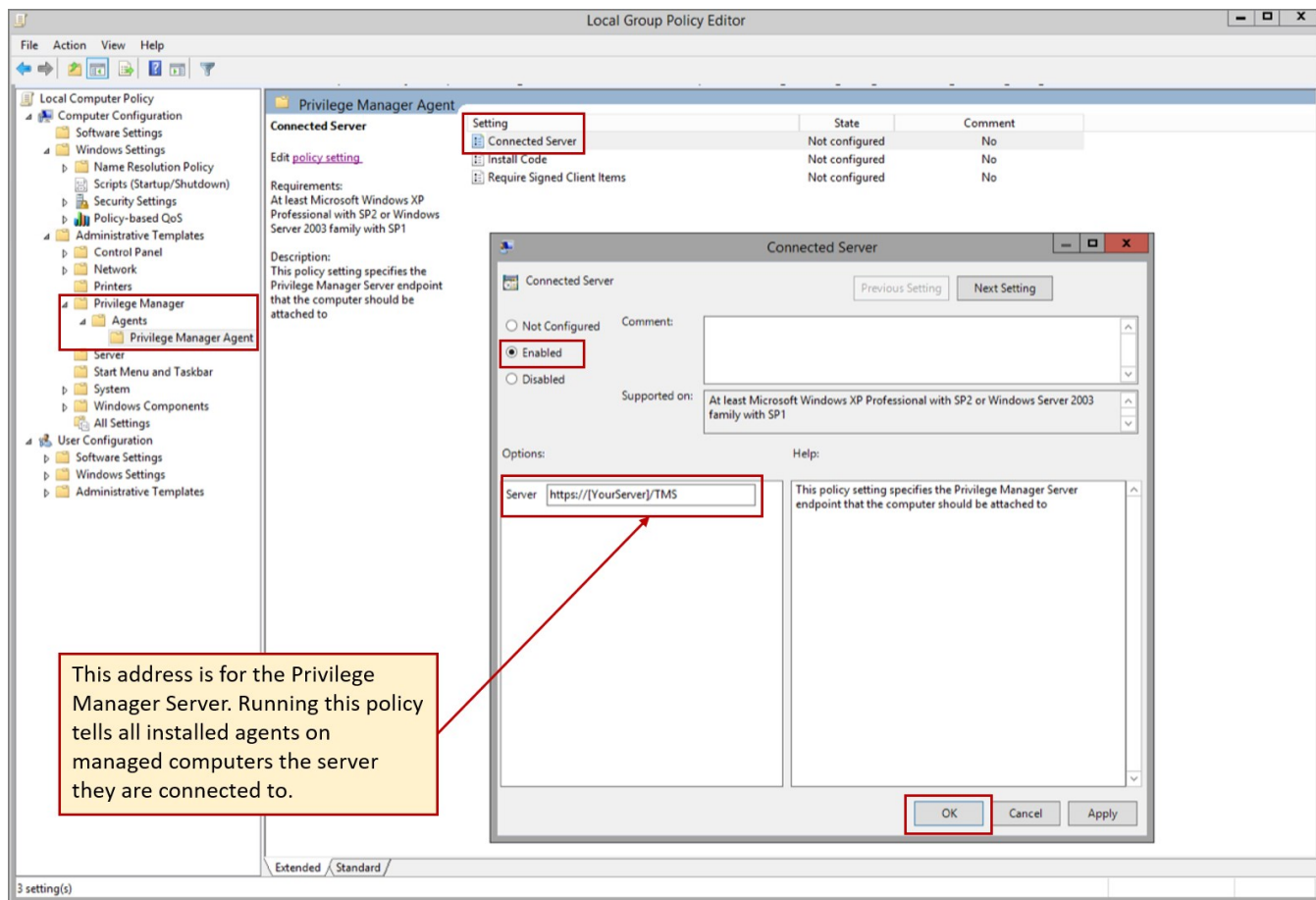
Although Amazon claims to offer a Windows 10 VDI environment, what they offer is not technically speaking Windows 10. Rather, what they provide is a Windows Server 2016 environment running what they call Windows 10 Experience.

This means that when Privilege Manager inventories it, the Privilege Manger agent believes that it is running on a server class OS. Therefore, from a licensing perspective, Amazon Workspaces need to be licensed as servers, rather than as clients.

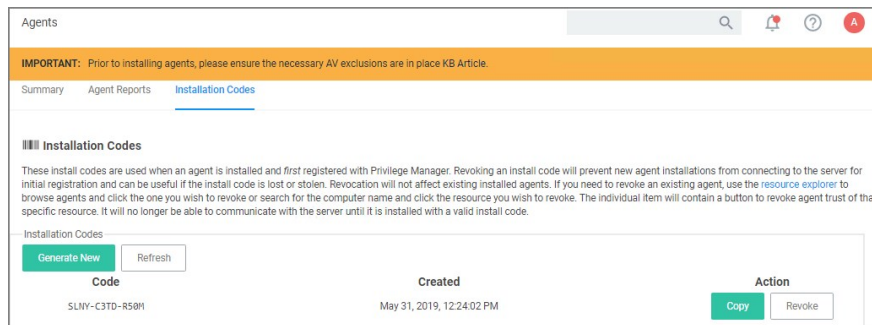
Regardless of how you installed agents or rolled agents out to your network, Privilege Manager has a method to link those agents with Servers. Privilege Manager has templates (files) that enable you to point agents back to the Privilege Manager Server.

To perform this task, do the following steps:

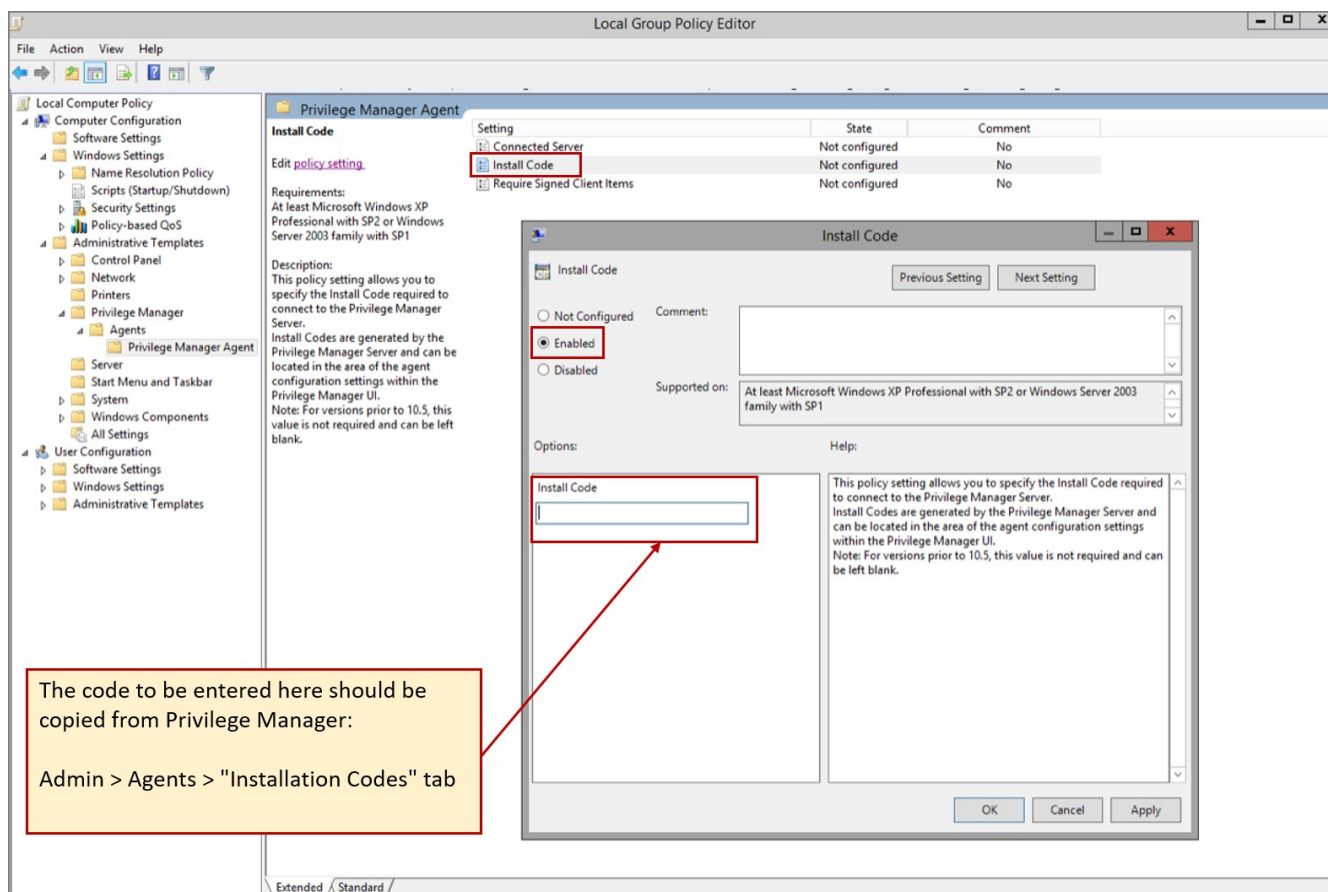
1. Download the attached [PrivilegeManagerAgent.admx](#) and [PrivilegeManagerAgent.adml](#) zip folders and extract the corresponding files (one file from each zip folder).
2. Install the downloaded and extracted custom Privilege Manager Group Policy files either on a single machine or on a domain controller.
 - o To install on a single machine:
 1. Copy PrivilegeManagerAgent.admx to %systemroot%\PolicyDefinitions
 2. Copy PrivilegeManagerAgent.adml to %systemroot%\PolicyDefinitions\en-US
 - o To install on a Domain Controller effectively making the custom GPO available to all Domain Administrators:
 1. Copy PrivilegeManagerAgent.admx to %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions
 2. Copy PrivilegeManagerAgent.adml to %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US
3. From the Group Policy Management Editor, navigate to Policies.
4. Go to Administrative Templates > Privilege Manager > Agents > Privilege Manager Agent and click Connected Server.



5. In the Connected Server window click **Enabled**.
6. In the Server field, **enter** the URL for your Privilege Manager Server, click **OK**.
7. Now you need to copy some data from Privilege Manager. In Privilege Manager, navigate to **Admin | Agents | Installation Codes** tab.



- Copy the **Code** value by clicking **Copy**.
- Switch back to the Group Policy Editor, in the Privilege Manager Agent window, click Install Code.



- In the Install Code window, click **Enabled**.
 - In the Install Code field, paste the Code value you copied from Installation Codes tab in Privilege Manager.
 - Click **OK**.
10. Set the Client Item Signature Validation. By default, Privilege Manager validates only client items that have a signature present. If you want to require that all client items have a valid signature, then configure the group policy settings to enforce the **Require Signed Client Items** setting.

Un-Installing Old Templates

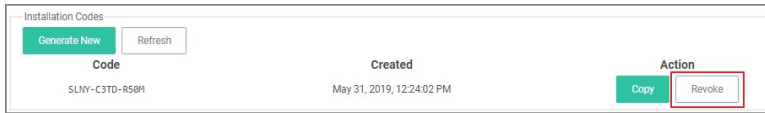
If you had previously downloaded and installed files which had the names "AMSAgent.admx" and "AMSAgent.adml", these should be removed. Do so as follows:

- To un-install from a single machine:
 - Delete AMSAgent.admx from %systemroot%\PolicyDefinitions
 - Delete AMSAgent.adml from %systemroot%\PolicyDefinitions\en-US
- To un-install from a Domain Controller:
 - Delete AMSAgent.admx from %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions
 - Delete AMSAgent.adml from %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US

With Privilege Manager 10.5 and up, you can revoke an agent trust relationship.

Revoking the Trust from the Server

1. Navigate to the Agent Install Code's page and click **Remove Agent Trust**.

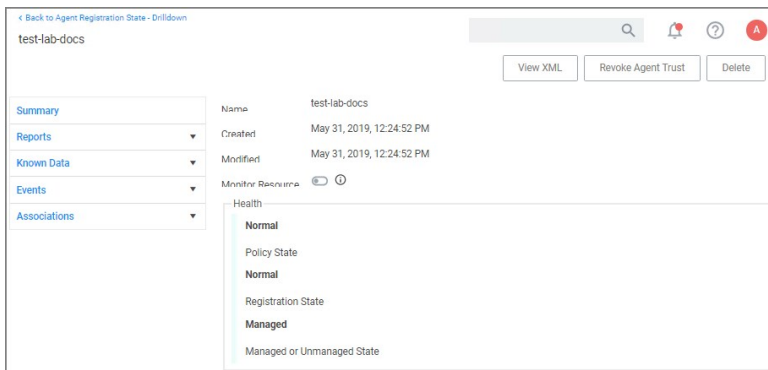


2. Click **OK** to confirm.

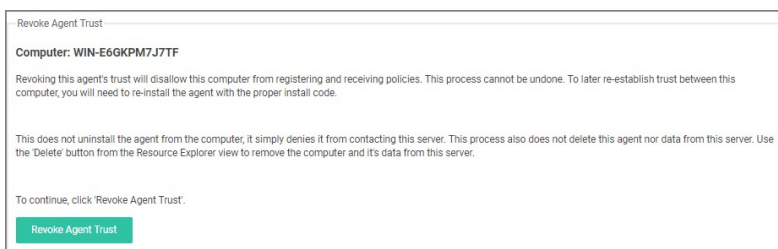


Revoking the Trust for the Computer Resource

1. Navigate to **Admin | Agents** to open the Agents Summary page.
2. Select an Operating System group from list.
3. On the Managed Computers by Operating System page, select one of the computer resources.



4. Click **Revoke Agent Trust**



5. Confirm by clicking **Revoke Agent Trust**

Message on the Revoke Agent Trust dialog:

"Revoking this agent's trust will disallow this computer from registering and receiving policies. This process cannot be undone. To later re-establish trust between this computer, you will need to re-install the agent with the proper install code.

This does not uninstall the agent from the computer, it simply denies it from contacting this server. This process also does not delete this agent nor its data from this server. Use the 'Delete' button from the Resource Explorer view to remove the computer and its data from this server."

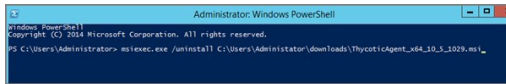
This topic covers uninstalling an agent when the endpoint is not going to be upgraded to a new version of Privilege Manager agents anymore.

If you're trying to uninstall an old agent in order to install a newer version of the agent, use the Upgrade Products/Feature link under the Setup page.

Using a PowerShell Script to Uninstall an Agent

1. Navigate to the machine(s) where the agent is located.
2. Right-click on **Windows Powershell** and **Run as administrator**.
3. Run the following command:

```
msiexec.exe /x ThycoticAgent_x64_VERSION.msi /qn
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The window shows the following text: "Windows PowerShell", "Copyright (c) 2016 Microsoft Corporation. All rights reserved.", and a command prompt where the command "msiexec.exe /uninstall C:\Users\Administrator\downloads\ThycoticAgent_x64_10.5_1029.msi_" has been entered. The cursor is at the end of the command.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (c) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> msiexec.exe /uninstall C:\Users\Administrator\downloads\ThycoticAgent_x64_10.5_1029.msi_
```

4. On the prompt, click **Yes**.

Starting in Privilege Manager version 10.5 and up, due to security updates you can now prevent services from using agents versions 10.4 and earlier from communicating with the Privilege Manager server.

Resolve

1. Launch Privilege Manager.
2. Navigate to **Admin | Configuration**.
3. Click the **Advanced** tab.
4. Set the **Prevent Legacy Agent Registration (10.4 and older)** to **Yes**.

The screenshot shows the 'Configuration' page for the 'Privilege Manager Server' in the 'Advanced' tab. The 'General' section contains several settings:

- Save performance counters * Yes No
- Load on Demand Flags
- Session Timeout minutes
- Allow Agent Certificate Mismatch * Yes No
- Maximum Application Event Count *
- Prevent Legacy Agent Registration (10.4 and older) *** Yes No
- Max time skew minutes

The 'Prevent Legacy Agent Registration (10.4 and older) *' setting is highlighted with a red box.

5. Click **Save Changes**.

You need to set Privilege Manager Agent configuration options to readily test configuration changes in a test environment. The agent configurations outlined in this page allow for accelerated feedback when testing use cases.

1. Under your Computer Group select **Agent Configuration**.

Application Control Agent Configuration Policy (Windows)

General Change History Active Refresh More

Details

This configuration defines the default behavior for the Privilege Manager agent.

Name: Application Control Agent Configuration Policy (Windows)

Description: This policy provides global configuration settings for the Windows Application Control Agent.

Self-Elevation

This configuration setting enables the Request Elevation option in the right-click context menu. An application policy will need to be enabled to define what action is applied when a user requests an elevation.

Allow Self-Elevate: No

Menu Text: Request run as administrator

Intervals

Send Application Action Events: 5 Minute(s)

Send ActiveX Events: 5 Minute(s)

Refresh Client Item Cache (Legacy): 1 Hour(s)

Application Action Defaults

Display Message Timeout: 5 Second(s)

Quarantine Path: C:\quarantined files

Show Advanced

2. Under Self-Elevation, set the Request Elevation option. For this an application policy needs to be enabled to define what action is applied when a user requests an elevation. Enter the text for the message in the text field.
3. Under Intervals, adjust the values to receive quicker turnarounds on any tests run on a test instance.
 1. Set Sent Application Action events every to 1 Minutes.
 2. Set Send ActiveX events every 5 Minutes.
 3. Set Refresh Client Items cache every 5 Minutes.
4. Set the **Application Action Defaults** like the Display Message Timeout and Quarantine Path.
5. Keep the advanced settings as is (Thycotic recommends to only change the advanced settings after consulting via Professional Service engagement.)
6. Click **Save Changes**.

Certain Privilege Manager tasks are directly related to agent processes and their operational loads.

Server side tasks, also known as Remote Client Scheduled Commands do not require a policy. Agent tasks require a policy. These types of tasks are with the exception of one, by default enabled and run on a scheduled basis. Most are read-only system tasks, that can be copied, renamed, and then customized.

The majority will run for the first time after system initialization.

Windows Remote Client Scheduled Commands

Restrict Account Permissions on Agent Services (Windows)	Instructs computers to only allow the specified users to start and stop the Thycotic services.	n/a	No
Basic Inventory (Initial, Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Basic Inventory (Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.	daily	Yes
Cleanup sent Privilege Manager Events (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Configure Privilege Manager Remove Programs	Configure the Privilege Manager Remove Programs behavior.	daily	Yes
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.	daily	Yes
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.	daily	Yes
Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.	daily	Yes
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.	daily	Yes
Scheduled Registration (Windows)	Initiate agent registration with server.	daily	Yes
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.	daily	Yes
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Applicable Policies (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Provisioned Resource Client Items (Windows)		daily	Yes
User Logon Inventory Policy	Updates user logon data on the given schedule.	weekly	Yes
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.	weekly	Yes

MacOS Remote Client Scheduled Commands

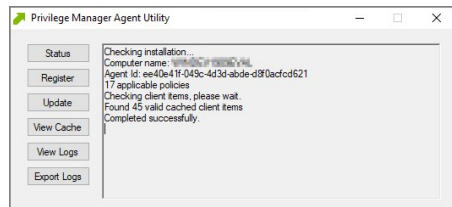
Basic Inventory (Initial, Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.	daily	Yes
Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.	daily	Yes
Cleanup sent Privilege Manager Events (Mac OS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Default File Inventory Policy (Mac OS)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes
Local User Inventory Policy (Mac OS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (Mac OS)	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Retry errored TMS Events (Mac OS)	Scan Agent queue for any events that require retransmission.	daily	Yes
Scheduled Registration (Mac OS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.	daily	Yes
Update Agent Commands (Mac OS)	When this policy is triggered the Agent will update agent command items.	daily	Yes
Update Applicable Policies (Mac OS)	When this policy is triggered the Agent will check the server for updated policies.	daily	Yes
Update Provisioned Resource Client Items (Mac OS)		daily	Yes

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on Windows systems.

The following topics are available:

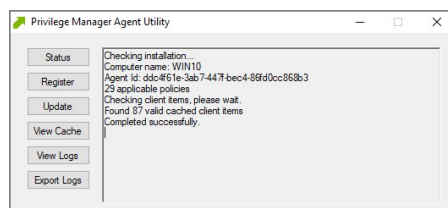
- [Windows Agent Utility](#)
- [Agent Hardening 10.7.1 and up](#)
- [Pre-10.7.1 Agent Hardening](#)
- [Troubleshooting](#)

Most endpoint troubleshooting will begin with the agent. There is an Agent Utility that is installed with the agent, used to troubleshoot issues from the endpoint. To open the utility, navigate to the C:\Program Files\Thycotic\Agents\Agent folder on the endpoint, and run the **Agent Utility.exe** application. That will launch the utility, and it will look like the screenshot below.



Status Button

The Status button will check that the endpoint can communicate with the server and will show you helpful information (such as the Agent ID and how many policies the machine has) and will validate the client items cache. It is also helpful in determining if there are any communication issues between the endpoint and the web server. Below is a screenshot of the information shown after clicking on the Status button.



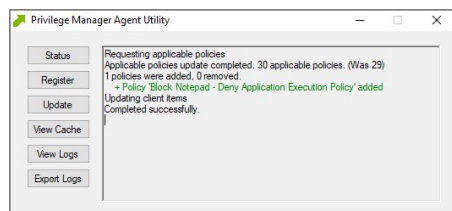
Register Button

The Register button will attempt to register the agent machine with the web console. It will show you the URL that the machine is using to communicate with the console. It will also give errors if there are issues with that communication. If you have just installed an agent on the machine, then it will also give information about the install code if there are any errors with that.



Update Button

The Update button will communicate back to the web server and update any new applicable policies or changes to current policies, filters, actions, etc. the endpoint already has on it.



View Cache Button

The View Cache button will open the Agent Cache Viewer in a separate window. It displays the Policies, Filters, and Actions the endpoint has cached currently.

Type	Name	Last Updated
Agent Policies	Retry errored TMS Events (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Local User Inventory Policy	10/18/2019 12:34:06 PM
Agent Policies	Cleanup Agent Inventory Transfers (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Scheduled Check Pending Client Tasks - Cloud (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Update Applicable Policies (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Perform Resource Discovery (Windows)	10/18/2019 12:34:06 PM

Starting with Privilege Manager version 10.7 the Client Item Cache is list also searchable. Enter a search term into the search bar and just review items that contain that term.

Type	Name	Last Updated
Agent Commands	Force Client Item Update Command	10/21/2019 5:56:17 AM

View Logs

Clicking on the View Logs button will open the Agent Log Viewer in a separate window. The screenshot below shows what the log viewer looks like.

TimeGenerated	Message	Source	Module
2018-09-14 09:44:26	No policies applies to process 5152 (C:\Windows\System32\audiodg.exe)	Source: CASMonitor Module: ArelbaAC3Svc.exe	CASMonitor Application Control
2018-09-14 09:44:26	DllProcessWork: Ignoring Process 6178 (C:\Windows\System32\cmd.exe) as it is a protected process.	Source: CASMon; C:\Windows\Process	Application Control
2018-09-14 09:44:25	No policies applies to process 6560 (C:\Windows\System32\backgroundtaskhost.exe)	Source: CASMonitor Module: Arel	CASMonitor Application Control
2018-09-14 09:44:24	No policies applies to process 4164 (C:\Program Files\Thyrotic\Agents\Agent\Thyrotic Agent User.exe)	Source: CASMo; CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Program Files\Thyrotic\Agents\Agent\Thyrotic Agent User.exe. Last updated: 2018-09-04 11	Source: CFilScanE; CFilScanEngine	Application Control
2018-09-14 09:44:24	Policy Block Notepad - Deny Application Execution Policy: &S:\Software\Kase439-18025f03b0-9f30c463\policy_2\applic1	Source: CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Windows\System32\notepad.exe. Last updated: 2018-09-06 12:07:54.	Source: CFilScanE; CFilScanEngine	Application Control
2018-09-14 09:44:24	No policies applies to process 6252 (C:\Windows\System32\amsmisr.exe)	Source: CASMonitor Module: ArelbaAC3Svc...	CASMonitor Application Control
2018-09-14 09:44:18	No policies applies to process 6209 (C:\Windows\System32\dlh.exe)	Source: CASMonitor Module: ArelbaAC3Svc.exe; E...	CASMonitor Application Control
2018-09-14 09:44:18	No policies applies to process 4332 (C:\Windows\System32\dlh.exe)	Source: CASMonitor Module: ArelbaAC3Svc.exe; E...	CASMonitor Application Control

Export Logs Button

Clicking on the Export Logs button will allow you to save the agent logs so that you can send them to someone if needed. They will be saved in the .evtx format so they can be opened with Event Viewer in Windows. Anytime there are issues with policies on endpoints and you need additional assistance, you will need to collect the agent logs first to help with determining what is causing the issue.

Agents Troubleshooting

The following topics for agents troubleshooting are available in this section:

- [Advanced Messages not working for child processes of Microsoft Edge](#)
- [Agent Registration Error Following an OS Upgrade](#)
- [Running updateclientitems.ps1 on an Agent triggers an error](#)
- [Client Item List Downloads](#)

The following topics about Endpoint Troubleshooting are available:

- [Endpoint Troubleshooting](#)
- [Catalina FileSystemWatcher Issue](#)
- [How to Recover an Unresponsive macOS Endpoint](#)

Agent updateclientitems.ps1 Error

While running the updateclientitems.ps1 powershell script on a machine, you receive the following error:

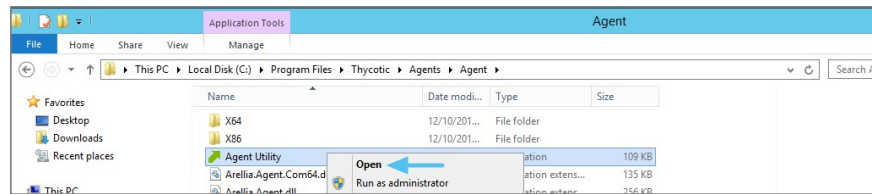
"KeySet does not exist"

```
PS C:\Program Files\Thycotic\PowerShell\Arellia.Agent> .\UpdateClientItems.ps1
-----
Client Items
-----
[FAILED] Downloading Windows Group Policies client item list
Keyset does not exist
```

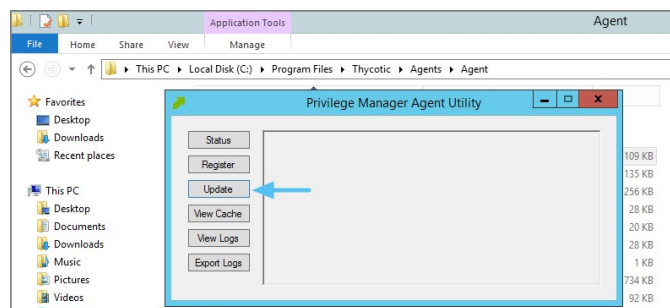
Note: The best practice to updating policies on machines would be to run the Agent Utility versus the PowerShell script. If you are still receiving the same error when using the Update button on the Agent Utility, open up a support case and include a screenshot of the error in the Agent Utility along with the agent logs.

1. Navigate to the Machine(s) where you want to update the policy and open the Agent Utility.

C:\Program Files\Thycotic\Agents\Agent

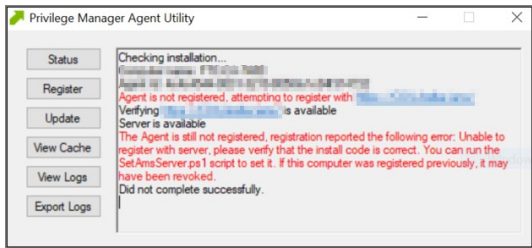


2. Select **Update**



Agent Registration Issue

After upgrading, you encounter the following issue with the Agent utility after selecting "Register".



This can be caused by a Windows OS upgrade due to either a new version or build. The certificate changes and the agent will need to be re-configured for the new certificate.

Detailed Information

A. Uninstall and reinstall the agent on the machine.

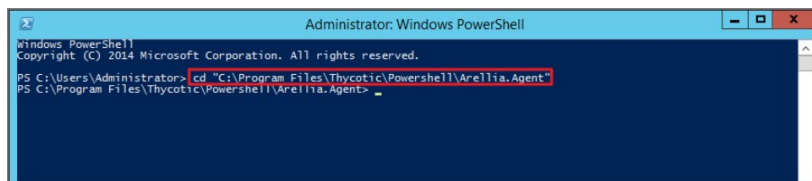
Or

B. Run the following PowerShell scripts to re-configure the agent.

Using a PowerShell Script

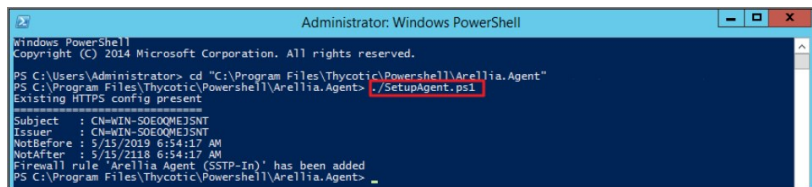
1. Right-click on **Windows PowerShell** and **Run as Administrator**.
2. Enter in the following command:

```
cd "C:\Program Files\Thycotic\PowerShell\Arellia.Agent"
```



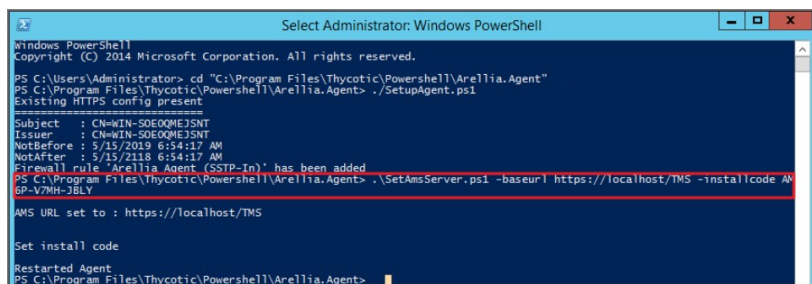
3. Enter in the following command:

```
.\SetupAgent.ps1
```



4. Enter in the following command:

```
.\SetAmsServer.ps1 -baseurl https://servername/TMS -installcode ?????-????-????
```



5. Enter in the following command:

```
.\UpdateClientItems.ps1
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> ./SetupAgent.ps1
Existing HTTPS config present
=====
Subject       : CN=WIN-S0E0QMEJ5NT
Issuer        : CN=WIN-S0E0QMEJ5NT
NotBefore     : 5/15/2019 6:54:17 AM
NotAfter      : 5/15/2118 6:54:17 AM
Firewall rule 'Arellia Agent (SSTP-In)' has been added
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\SetAmsServer.ps1 -baseurl https://localhost/TMS -installcode AM
6P-V7MH-JBLY
AMS URL set to : https://localhost/TMS

Set install code

Restarted Agent
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> ./UpdateClientItems.ps1
=====
Client Items
=====
Refreshing Agent Commands: 7/31 client items
Refreshing Agent Gauges: 0 client items
Refreshing Agent Policies: 17/61 client items
Refreshing Application Actions: 2/41 client items
Refreshing File Filters: 2/292 client items
Refreshing Provisioned Resources: 0/1 client items
Refreshing Scap Entities: 0 client items
Refreshing Windows Group Policies: 0/1 client items
Refreshing Windows Group Policy Settings: 0 client items

No client item updates required

Last client item update: Force Client Item Update Command - 2 minutes ago

=====
Policies
=====
Last added policy: Global Process Monitor - 3 hours ago
Last updated policy: Global Process Monitor - 2 hours ago
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent>
```

Client Item List Downloads

When you run the UpdateClientItems.ps1 PowerShell script to update policies on a machine you see errors below:

```
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1
*****
Client Items
*****

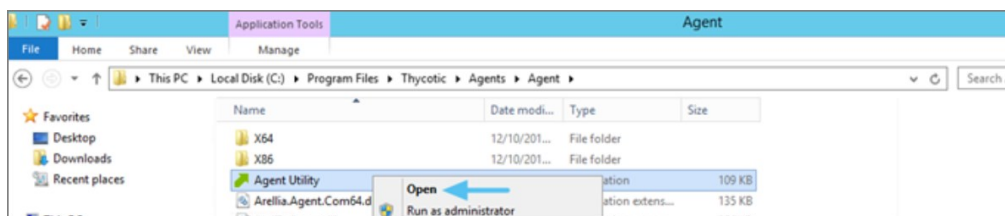
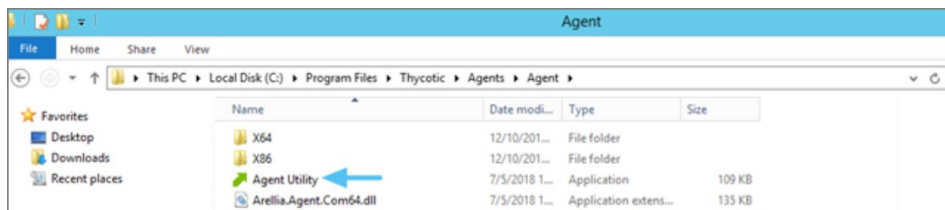
[FAILED] Downloading Windows Group Policies client item list
Keyset does not exist
```

Error: [FAILED] Downloading Windows Group Policies client item list - Keyset does not exist

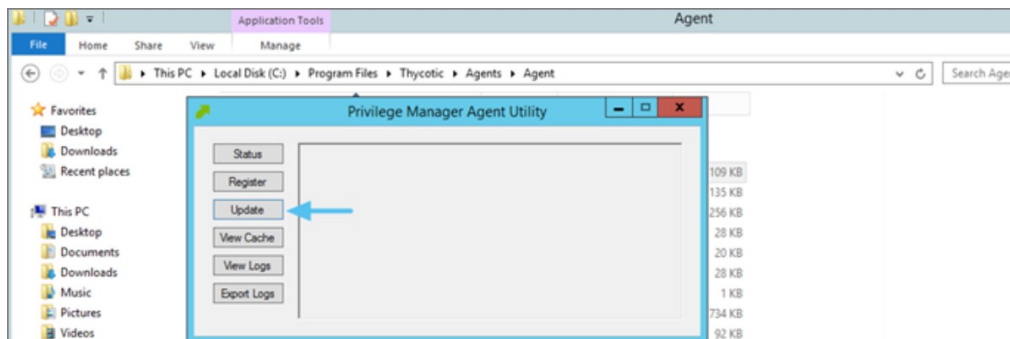
Note: This will only affect systems prior to Privilege Manager 10.7.

Resolve

1. Navigate to the Machine(s) where you want to update the policy.
2. Open the Agent Utility by going to C:\Program Files\Thycotic\Agents\Agent



3. Click **Update**.



Advanced Messages not Working for Child Processes of Microsoft Edge

When opting to Run an application from Microsoft Edge on Windows 10 version 1803, Advanced Messages for application justification or approval are not honored.

Detailed Information

If an application control policy targets an application such as the Google Chrome installer, the approval or justification messages will prevent the process from continuing until the message prompt is completed. However, when choosing the "Run" option when downloading an application in Microsoft Edge, the process will be created under the browser_broker.exe service and in Windows 10 version 1803 the process continues and does not wait for the Privilege Manager message to be completed.

Other versions of Windows 10 and Microsoft Edge do not appear to have this issue.

Workaround

An application control policy can be created to block browser_broker.exe and prevent users from using the "Run" option in Microsoft Edge.

Alternatively, upgrading Windows 10 will also fix the issue.

Endpoint Issues

This topic is intended to assist users in troubleshooting issues (such as policies not yielding expected results) from an endpoint machine that has the Thycotic agent installed on it.

Policy Troubleshooting

If there is an issue with policies not getting updated on the endpoint, or specific files or applications not being elevated or blocked, please use the information below to help determine what is causing the issue.

Policies Not Getting Updated

If policies are not getting updated on the endpoint, there could be a communication issue between the machine that has the agent installed on it and the web server. The best way to determine if there is a communication issue would be to open the Agent Utility on the endpoint as described in the previous section, and then do the following:

1. Click on the Status button and see if there are any errors shown.
2. Click on the Register button and check for errors shown there.
3. Click on the Update button and check for errors there as well.

If there is an issue with the endpoint communicating with the web server, there will be errors displayed in red after clicking on those buttons.

Specific Files or Applications Not Being Elevated or Blocked

If specific files or applications are not being elevated or blocked properly, then you will need to look in the Agent Logs on the endpoint. You can open the logs by first opening the Agent Utility on the machine. Once that is open, click on the View Logs button to bring up the Agent Log Viewer.

The Agent Log Viewer is very helpful for troubleshooting issues with policies not applying correctly. In the log, you can see if a policy applied to a certain process, and if so, what policy applied to that process. You can also see if there was no policy that applied to that specific process.

For example, in the screenshot below of the Agent Log Viewer, you will see a policy called "Block Notepad - Deny Application Execution Policy" that has been applied to the endpoint.

□

The highlighted entry on the screenshot above shows that the "Block Notepad - Deny Application Execution Policy" was triggered when notepad was opened. Double-click on the log entry to see further details as shown below. This shows the exact process that met the criteria of the policy and shows the priority number of that policy. The policy priority is useful information if the application continues processing through multiple policies.

□

With this information, you know that the policy applied to the Notepad process correctly. If there were other policies that applied to that same process, you would see them in the log viewer as well. There are certain situations in which clients will apply multiple policies to the same process. When troubleshooting issues with certain files or applications, the log viewer is a valuable tool to use.

If there is no policy that applies to a certain process, the Agent Log Viewer shows you that as well. In the screenshot of the log viewer, presented above in this section, you can notice entries showing that there are some processes to which no policies apply. Entries that begin with "No policies applies to process..." indicate that no policy was triggered when the application executed on the endpoint. If a client says that a specific file or application is not being blocked or elevated, then in the log viewer you can see what process is running when they launch the application and whether a policy is applying to that process.

If there are any Errors in the log viewer, they are shown in **Red**. Warnings are shown in **Blue**, and Informational messages are shown in **Black**.

Users on Privilege Manager 10.7.1 or up should use the new policy named **Restrict Account Permissions on Agent Services (Windows)**. Refer to [Agent Hardening 10.7.1 and up](#) for details on the policy used starting with Privilege Manager 10.7.1.

Editing the Agent Service Start / Stop Control (Windows) Policy

1. Navigate to **ADMIN | Policies**.
2. Click on the **General** Tab.
3. In the Name field enter **Agent Service Start / Stop Control**.

The screenshot shows the 'Policies' management interface. At the top left is a blue 'Add New Policy' button. Below it are navigation tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General' (which is selected and underlined). On the right side, it says '1 to 1 of'. Below the tabs is a table with columns 'ENABLED', 'NAME', and 'FOLDER'. The first row shows 'Any' in the 'ENABLED' column, 'agent service' in the 'NAME' column, and 'Windows' in the 'FOLDER' column. Below the table, the details for the selected policy are shown: 'Enabled' (checked), 'Agent Service Start / Stop Control (Windows)' in the name field, and 'Windows' in the folder field.

4. Click on the **Agent Service Start / Stop Control (Windows)** policy.

The screenshot shows the configuration page for the 'Agent Service Start / Stop Control (Windows)' policy. The breadcrumb is 'Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)'. There are tabs for 'General', 'Parameters', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment'. The 'General' tab is selected. The configuration shows: 'Enabled' (checked), 'Name' (Agent Service Start / Stop Control (Windows)), 'Description' (Instructs computers to only allow the specified users to start and stop the Thycotic services.), and 'Command' (Local Security Set Service Security Script with Account IDs). At the bottom are buttons for 'Back', 'Edit', 'Create a Copy', 'Delete', and 'Export'.

5. To customize the Agent Hardening policy navigate to the **Parameters tab**.
6. Click **Edit**.

The screenshot shows the 'Parameters' tab of the policy configuration page. The breadcrumb is 'Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)'. The 'Parameters' tab is selected. The text says 'Enter default parameter values for this task.' There are two sections: 'Services' and 'User Accounts'. Each has a '+ Add' button and a list of items. 'Services' includes 'ArelliaACSvc' and 'ArelliaAgent'. 'User Accounts' includes 'Administrators'. At the bottom are buttons for 'Save', 'Cancel', and 'Export'.

7. Under **User Services** click the + button and use the search field to select the Services to be targeted by the task
8. Under **User Accounts** click the + button and use the search field to find the specific user account that has permissions to make changes to the Agent services.
9. Click **Save**.

Note: If you require a rollback of the agent hardening due to upgrade issues, use the manual Restore Default Agent Permissions procedure following below.

Restore Default Agent Permissions

If you need to rollback agent hardening on your endpoints, follow these steps to restore the default agent permissions:

1. Navigate to **ADMIN | More...** and select **Config Feeds**.
2. Next to **Privilege Manager Product Configuration Feeds** click **Select Items**.
3. Next to **Thycotic Management Server Core** click **Select Items**.
4. Download the **Reset Agent Service Permissions** config feed.

Data Feeds > Thycotic Management Server Core

i The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	DOWNLOADED
Maintenance Resources	Contains maintenance gauges, tasks, etc. for optimal TMS performance	Nov 27, 2019, 12:58:05 PM	Download
Reset Agent Service Permissions	Contains a policy to restore the security descriptor on Thycotic Services	Jan 23, 2020, 4:13:21 PM	Download
SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.	Jul 24, 2019, 5:23:54 PM	Download

[Back](#)

5. Once the config feed is installed, navigate to **ADMIN | Policies** and select the General tab.
6. Search for the agent service policies and select to edit.

Policies

[Add New Policy](#)

Windows Mac OS Client System Settings ActiveX Firewall General

1 to 2 of 2

ENABLED	NAME	FOLDER
Any	agent service	
Enabled	Agent Service Start / Stop Control (Windows)	Windows
Not Enabled	Agent Service Clear Restrictions (Windows)	Windows

7. Disable the **Agent Service Start / Stop Control (Windows)** policy.

1. Click **Edit**.
2. Deselect **Enabled**.

Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Agent Service Start / Stop Control (Windows)

Description Instructs computers to only allow the specified users to start and stop the Thycotic services.

Command Local Security Set Service Security Script with Account IDs

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [View as XML](#) [Export](#)

1. Click **Save**.

8. Enable the **Agent Service Clear Restrictions (Windows)** policy.

1. Click **Edit**.
2. Select **Enabled**.

Remote Scheduled Client Command > Agent Service Clear Restrictions (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Agent Service Clear Restrictions (Windows)

Description Sets the Security Descriptor back to Default on Thycotic services.

Command Local Security Clear Restrictive Service Security Script

Back Edit Create a Copy Delete View as XML Export

1. On the Targets tab specify the computers that need to be targeted by this policy.
2. On the Triggers tab specify when to run and/or what events will trigger the policy to run.

9. Click **Save**.

Agent installations on endpoints can be secured, only allowing a specified user access to start or stop an agent service and denying any agent control access to a local Administrator or basic user account.

To make sure that local Administrators do not tamper with Thycotic agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Thycotic Agent or Thycotic Application Control.

A user or group needs to be available in Privilege Manager to be selected while setting up the task. This user or group will have rights to start and stop agent services running on endpoints once the **Restrict Account Permissions on Agent Services (Windows)** policy is enabled.

Note: If you implemented Agent Hardening prior to 10.7.1, **disable** and **delete** the following policies:

- Agent Service Start / Stop Control (Windows)
- Agent Service Clear Restrictions (Windows)

Editing the Restrict Account Permissions on Agent Services (Windows) Policy

1. Under your Computer Group, select **Scheduled Jobs**.
2. Search for **Restrict Account**

Search Results for Restrict

NAME	TYPE	MODIFIED	DESCRIPTION
DocTest - Restrict Account Permissions on Agent ...	Remote Scheduled Client Command	2/19/20, 4:15 PM	This policy restricts access on the selected servi...
Restrict Account Permissions on Agent Services (...)	Remote Scheduled Client Command	6/25/20, 7:12 AM	This policy restricts access on the selected servi...
Restrict Account Permissions on Services (Script) ...	Agent Executed Powershell Script	6/25/20, 7:12 AM	This powershell script will set the given security d...
Restrict Account Permissions on Services (Windo...	Remote Client Task	6/25/20, 7:12 AM	This task will restrict access on the selected serv...

3. Click on the **Restrict Account Permissions on Agent Services (Windows)** policy.

Restrict Account Permissions on Agent Services (Windows)

This item is read-only.

Details Change History Inactive Duplicate More

Scheduled Job Details

Name	Restrict Account Permissions on Agent Services (Windows)
Description	This policy restricts access on the selected services to only the system and selected accounts. No other ...
Computer Groups Targeted	1 (1 total endpoints) Windows Computers
Deployment	Not deployed (Policy is inactive)

Job Settings

Command	Restrict Account Permissions on Services (Script) (Windows)
Services *	ArelliaACSvc ArelliaAgent
User Accounts *	Administrators

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run.

Default: Upon task creation/modification
Default: Daily at 10:00:00 AM starting Wed Feb 12 2020 (repeating every 1 hour: for a duration of 24 hours)
Add Trigger

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not

Idle Conditions Start the task only if the computer is idle
And is idle for 10 minute(s)

4. To customize the policy click **Duplicate**.

Create a copy of Restrict Account Permissions on Agent Services (Windows)

Name

Copy of Restrict Account Permissions on Agent Services (Windows)

Cancel Create

5. Customize the name of the copied policy and click **Create**.

Test Restrict Account Permissions on Agent Services (Windows)

Details Change History Inactive Refresh More

Scheduled Job Details

Name: Test Restrict Account Permissions on Agent Services (Windows)

Description: This policy restricts access on the selected services to only the system and selected accounts. No other accounts (including Administrators) will be able to start/stop or modify the services.

Computer Groups Targeted: 1 (1 total endpoints) Windows Computers x Add

Deployment: Not deployed (Policy is inactive)

Job Settings

Command: Restrict Account Permissions on Services (Script) (Windows)

Services *: ArelliaACSvc, ArelliaAgent Edit

User Accounts *: Administrators Edit

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy to be run.

Upon task creation/modification x
Daily at 10:00:00 AM starting Wed Feb 12 2020 (repeating every 1 hour for a duration of 24 hours) x
Add Trigger

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions: Start the task only if the computer is idle

Power Conditions: Start the task only if the computer is on AC power
 Stop if the computer switches to battery power

Advanced Conditions: Allow task to be run on demand
 Run task as soon as possible after a scheduled start is missed
 If the task fails, attempt to restart
 Stop the task if it runs for longer than

If the task is already running, then the following rule applies: Default (Do not start a new instance)

6. Customize the policy's

- o Scheduled Job Details.
- o Job Settings.
- o Job Schedule.
- o Job Conditions.

1. Under **Services** the Arellia Application Control Service and Arellia Agent Service are present by default. Add any services you might also want to protect. Use the search field to find and specify other service names.
2. For **User Accounts** use **Edit** and use the search field to find specific user accounts that have permissions to make changes to the specified services. Administrators are present by default, if you wish to limit to only a subset of users with administrative rights, create a group and update accordingly.

7. Click **Save Changes**.

8. Set the policy to **Active**.

Note: If you wish to update a hardened agent, refer to information under the topic [Windows Agents](#).

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on macOS.

The following topics are available:

- [Modify Update Agent Commands \(MacOS\) Policy](#)
- [MacOS Agent Utility Preference Pane](#)
- [Terminal Commands](#)
- [Finding Logs without using the Agent Utility](#)
- [How to Recover an Unresponsive macOS Endpoint](#)
- [Using an MDM Profile for your Agent](#)

With the 10.8 release of Privilege Manager, Thycotic is introducing a UI based macOS Agent Utility implemented as a preference pane. The utility provides functionality previously only available via Terminal shell commands. The utility allows customers to easily troubleshoot by

- checking an endpoint status.
- view an endpoint cache.
- view logs in log viewer.
- export logs.

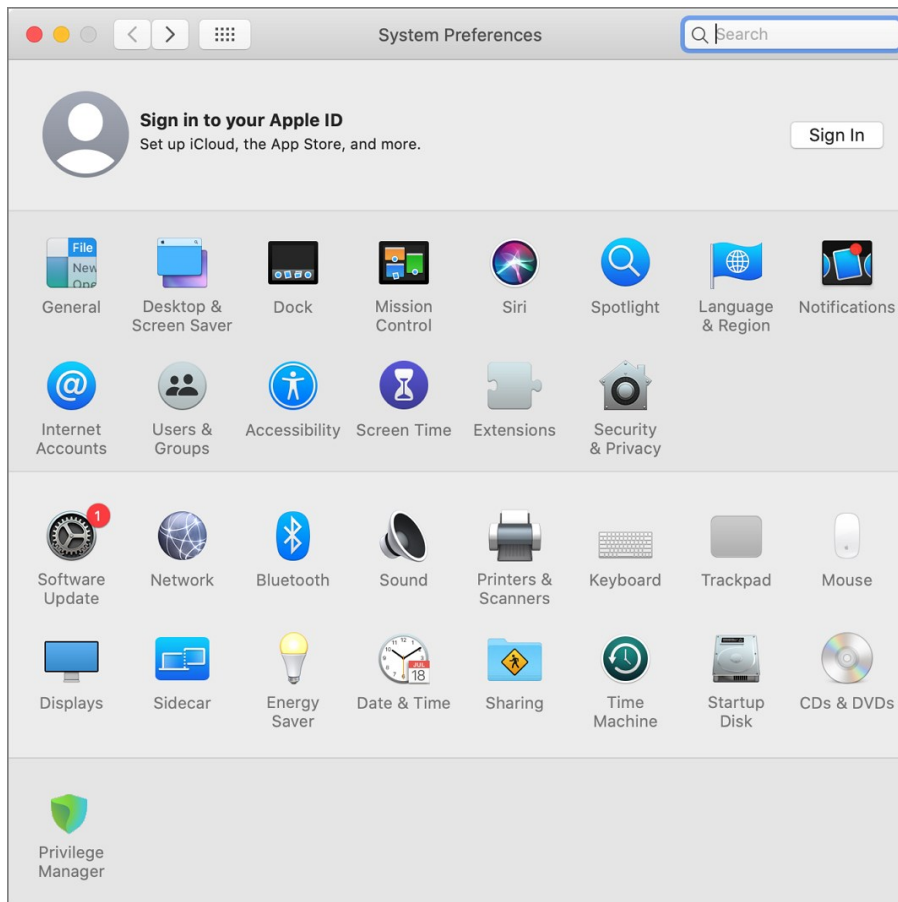
It also offers UI guided means to

- register the agent with the server.
- update the endpoint to retrieve latest policies.

Accessing the Agent Utility

To access the Privilege Manager macOS Agent Utility,

1. Open the System Preferences on your macOS endpoint.



2. Click **Privilege Manager** to open the preference pane.

General Tab

When a local admin user opens the utility, the controls to make changes are unlocked. For standard users they are locked, but can be unlocked by providing an administrator user name and password, just as possible with all other preference panes.

The screenshot shows the Privilege Manager interface with two tabs: 'General' and 'Client Items'. The 'General' tab is active and displays the following information:

- Agent Information:**
 - Computer Name: GarryColby
 - Agent Id: 0a6d7b20-d37e-4261-a1e7-9837a24a6592
 - Applicable Policies: 4
 - Cached Client Items: 27
 - Last Updated: April 24, 2020 at 3:37:04 PM EDT
- Server Information:**
 - Server URL: <https://PrivilegeManagerURL/TMS/>

At the bottom of the 'General' tab, there are buttons for 'Register' and 'Modify', and a lock icon with the text 'Click the lock to prevent further changes.' Below the lock icon are buttons for 'Open Log File' and 'Update Client Items'.

On the general tab the utility provides under **Agent Information** details like the Computer Name, Agent Id, the number of applicable policies and client items cached. It also provides the data/time stamp of the last update.

Under **Server Information** the Server URL for the current agent registration is listed. Here, administrator users can either Register a not yet registered agent, or modify an existing agent registration.

Use **Open Log File** to open the agent's log file.

The screenshot shows the 'agent.log' file with the following content:

```

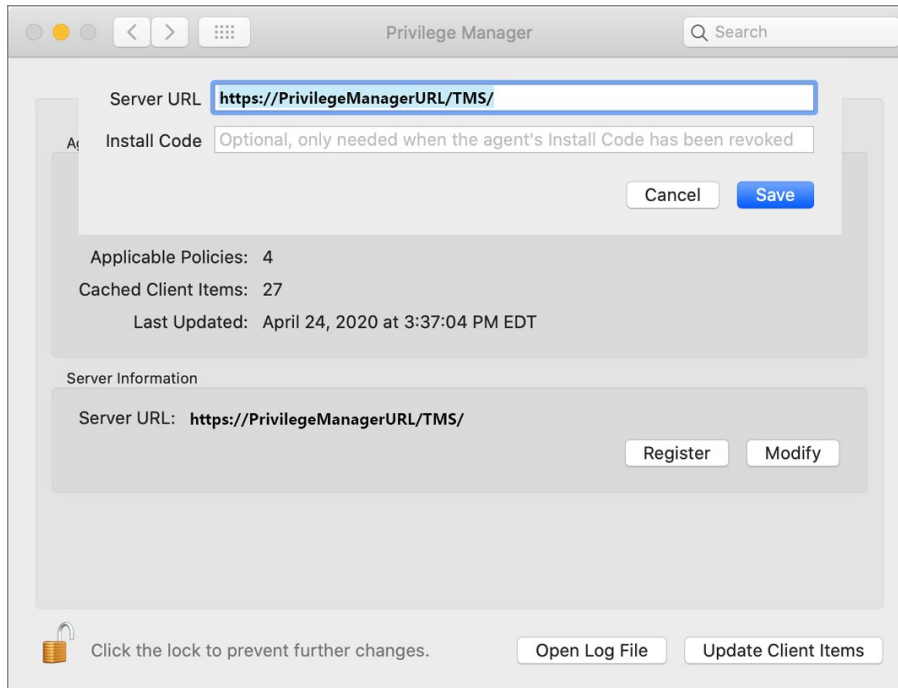
f18f-4c9d-92f8-42dc8ac94844
2020-04-28T18:51:04-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T18:51:04-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T18:51:04-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T18:51:04-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T18:51:04-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T18:51:04-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 18:53:04 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
2020-04-28T18:53:05-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T18:53:05-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T18:53:05-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T18:53:05-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T18:53:05-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T18:53:05-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 18:55:05 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
2020-04-28T18:55:06-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T18:55:06-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T18:55:06-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T18:55:06-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T18:55:06-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T18:55:06-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 18:57:06 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
2020-04-28T18:57:07-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T18:57:07-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T18:57:07-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T18:57:07-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T18:57:07-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T18:57:07-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 18:59:07 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
2020-04-28T18:59:08-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T18:59:08-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T18:59:08-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T18:59:08-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T18:59:08-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T18:59:08-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 11:01:08 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
2020-04-28T11:01:09-INFO] Running scheduled item "Retry errored TMS Events - Catalina (macOS)", (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844)
2020-04-28T11:01:09-INFO] Running client command 0ff26611-9382-43e8-9b8a-abfd1682076 for scheduled item Retry errored TMS Events - Catalina (macOS) (dcbcbca4-f18f-4c9d-92f8-42dc8ac94844).
2020-04-28T11:01:09-INFO] Attempting to run command 0ff26611-9382-43e8-9b8a-abfd1682076.
2020-04-28T11:01:09-INFO] Getting runner for type Arellia.Data.Contracts.Agent.ClientItems.AgentPowerShellCommandContract.
2020-04-28T11:01:09-INFO] Running client command Retry errored TMS Client Events (MacOS) (0ff26611-9382-43e8-9b8a-abfd1682076).
2020-04-28T11:01:09-INFO] Task "Retry errored TMS Events - Catalina (macOS)" is scheduled at "04/28/2020 11:03:09 -04:00" 1 minutes from now. dcbcbca4-f18f-4c9d-92f8-42dc8ac94844
  
```

Use **Update Client Items** to trigger a client item update. When **Update Client Items** is clicked and if there are updates to applicable policies or policies are added to the endpoint, the last updated timestamp will change to reflect when the last client items change on the endpoint happened. The date/time stamp does not reflect when the last update client items command ran, the date/time stamp only updates when there was an actual change on the endpoint.

Registering/Modifying an Agent

To register an agent or to modify an existing agent registration via agent utility, follow these steps:

1. Open the Privilege Manager agent utility.
2. On the General tab under Server Information click Register or Modify.



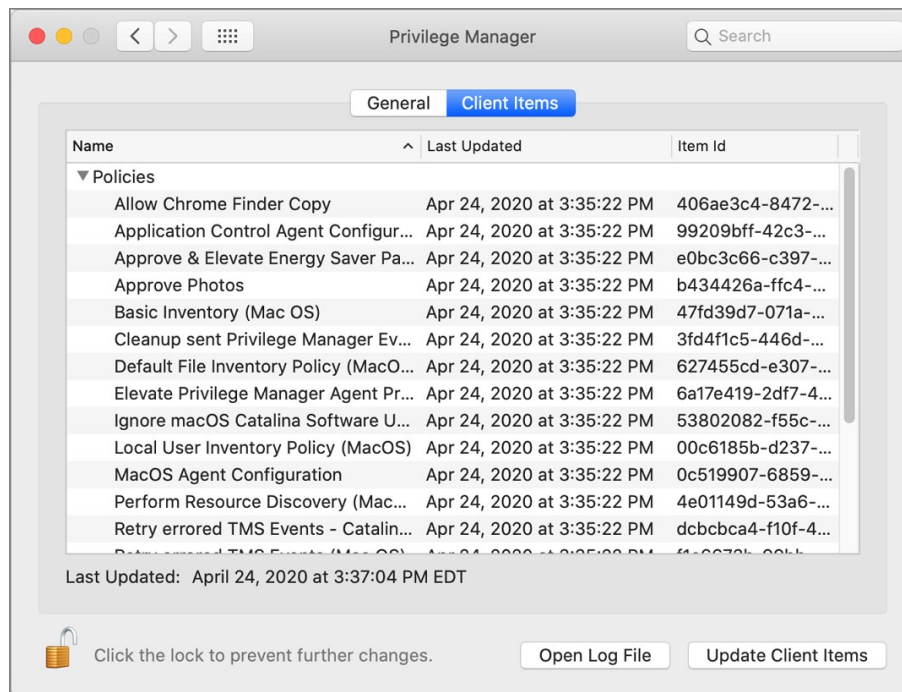
1. Enter the **Server URL** for the agent registration or modified registration.
2. If the agent has been installed without an install code or the agent's registration was revoked, provide an install code to register the agent.
3. Click **Save**.

Client Items Tab

The Client Items tab provides an overview of all client items on the endpoint. The client items are grouped into the following categories:

- Policies
- Actions
- Commands
- Filters

The following image shows the client items on the endpoint in an unlocked preference pane with policies expanded.



Use expand/collapse to better navigate through the list of applicable client items on the endpoint. The following image shows the client items on the endpoint in a locked preference pane with policies collapsed.

Privilege Manager

Search

General Client Items

Name	Last Updated	Item Id
▶ Policies		
▼ Actions		
Run as Root	Apr 24, 2020 at 3:35:25 PM	6a910f96-2459-44...
Application Approval Request Mess...	Apr 24, 2020 at 3:35:25 PM	bb5093a8-880c-4...
▼ Commands		
Local Security Inventory Command	Apr 24, 2020 at 3:35:25 PM	d1de4815-2874-4c...
Retry errored TMS Client Events (M...	Apr 24, 2020 at 3:37:01 PM	0ff26611-9382-43e...
▼ Filters		
Copy Install Application	Apr 24, 2020 at 3:35:25 PM	2acef6ae-9a32-44f...
Wizard Generated App Bundle Filte...	Apr 24, 2020 at 3:35:25 PM	34d045b5-6b81-4...
System Preferences	Apr 24, 2020 at 3:35:25 PM	c7ef59e4-6d1d-411...
Wizard Generated App Bundle Filte...	Apr 24, 2020 at 3:35:25 PM	a918136c-5b27-43...
Energy Saver Preference Pane (Ma...	Apr 24, 2020 at 3:35:25 PM	5691109d-a72f-4c...

Last Updated: April 24, 2020 at 3:37:04 PM EDT

Click the lock to make changes.

Open Log File Update Client Items

Agents receive new policies on a schedule which can be modified.

To check or change the schedule, follow these steps:

1. Go to **Admin | Resources**
2. Select for this macOS machine named the **Update Agent Commands (Mac OS) Policy**.
3. Edit the schedule on the **Triggers** tab.

In the Mac Terminal application you can perform the following commands directly to your Thycotic macOS agent.

Note: The sudo command may prompt for admin account password verification.

Find this list by entering the following into Terminal:

```
sudo /usr/local/thycotic/agent/agentUtil.sh
```

These are the commands returned for the utility:

```
runcschedule -scheduleId (id)
updateclientItems
clientItemsSummary
register
setmsserver -serverUri (https://servername.com/Tms/)
setmsserver -serverName (servername)
stop
start
restart
enableverboselogging
disableverboselogging
```

Command Usage

To perform a command, insert the name of the above command that you need to perform into this command string:

```
sudo /usr/local/thycotic/agent/agentUtil.sh [InsertCommandHere]
```

As one example, if you entered an incorrect server name path in the agent installer and Privilege Manager therefore cannot find and register your Mac agent, you can run the command:

```
sudo /usr/local/thycotic/agent/agentUtil.sh setmsserver -serverUri (https://servername.com/Tms/)
```

Which is using the correct server name URI to redirect your agent toward the correct server location.

Or, to register an agent immediately after updating the Privilege Manager server location, type:

```
sudo /usr/local/thycotic/agent/agentUtil.sh register
```

The complete command shell exchange looks like this:

```
macadmin-MacBook-Pro:~ madadmin$ sudo /usr/local/thycotic/agent/agentUtil.sh register
Password:
Initiated registration.
macadmin-MacBook-Pro:~ madadmin$
```

For troubleshooting your Mac agent, logs are found in the Console application. There are two places to check for logs in Console:

1. You can filter your machine's logs by clicking your machine's name under Devices and typing "Thycotic" into the top search bar.
2. Thycotic-specific logs are recorded in a Console folder that is titled thycotic (found in the left side bar: **Reports | /var/log | thycotic**).

If you utilize an MDM tool like JAMF, you can create configuration profiles to make management of the agent more silent on your macOS Catalina and Big Sur deployments.

You will need two different configuration profiles for each version of the agent (or two different payloads within the same profile):

- a KEXT or SYSEX Allow Profile
- a PPPC profile that gives Full Disk Access to ThycoticACSvc (KEXT) or com.thycotic.acsd (SYSEX). Refer to [macOS File/Folder Access](#)

SYSEX

SYSEX Allow Info

You can create a SYSEX Allow profile for ThycoticManagementAgent-10.8.nnnn.pkg and above using your MDM's profile creator and the following information:

- Team Identifier: UJDHBB2D6Q
- Allowed System Extensions: com.thycotic.acsd

SYSEX PPPC Profile Info

1. Install the agent on a test endpoint.
2. Use Jamf's **PPPC Utility** or another method to create a profile that gives Full Disk Access to the Privilege Manager Security system extension (**com.thycotic.acsd.systemextension**) found under Macintosh HD/Library/SystemExtensions.

Alternatively, make a custom configuration profile using the XML below:

```
<?xml version="1.0" encoding="UTF-8"?>
<DOCTYPE plist PUBLIC "-//Apple/DTD PLIST 1.0/EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Allows Privilege Manager SYSEX to access all files on Catalina and higher</string>
<key>PayloadDisplayName</key>
<string>Privilege Manager Security</string>
<key>PayloadEnabled</key>
<true/>
<key>PayloadIdentifier</key>
<string>F34A5382-C24E-42D8-970E-4D6C0A03A229</string>
<key>PayloadOrganization</key>
<string>Thycotic</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadUUID</key>
<string>41A7F168-58C5-4F98-BC37-5E762CF79595</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
<array>
<dict>
<key>Allowed</key>
<integer>1</integer>
<key>CodeRequirement</key>
<string>anchor apple generic and identifier "com.thycotic.acsd" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists /* or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists /* and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists /* and certificate leaf[subject.OU] = UJDHBB2D6Q)
</string>
<key>Identifier</key>
<string>com.thycotic.acsd</string>
<key>IdentifierType</key>
<string>bundleID</string>
<key>StaticCode</key>
<integer>0</integer>
</dict>
</array>
</dict>
</dict>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>Privilege Manager Security SYSEX PPPC FDA</string>
<key>PayloadEnabled</key>
<true/>
<key>PayloadIdentifier</key>
<string>749AFA6B-3B75-47CF-9A5B-89E909B785FD</string>
<key>PayloadOrganization</key>
<string>Thycotic LTD</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>749AFA6B-3B75-47CF-9A5B-89E909B785FD</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

KEXT

KEXT Allow Info

You can create a KEXT Allow profile for ThycoticManagementAgent-10.8.nn.pkg and below using your MDM's profile creator and the following information:

- Team ID: UJDHBB2D6Q
- Kernel Extension Bundle ID: com.thycotic.ThycoticACS

KEXT PPPC Profile Info

1. Install the agent on a test endpoint.
2. Use Jamf's **PPPC Utility** (free, no Jamf subscription needed) or another method to create a profile that gives Full Disk Access to the ThycoticACSvc daemon found under Macintosh HD/Library/Extensions/ThycoticACS.kext/Contents/MacOS/ThycoticACSvc

Alternatively, make a configuration profile with the XML below:

```
<?xml version="1.0" encoding="UTF-8"?>
<DOCTYPE plist PUBLIC "-//Apple/DTD PLIST 1.0/EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
```

```
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Allows Privilege Manager to access all files on Catalina and higher</string>
<key>PayloadDisplayName</key>
<string>Privilege Manager ThycoticACSVc Profile</string>
<key>PayloadIdentifier</key>
<string>com.thycotic.privilegemanager.thycoticacsvc</string>
<key>PayloadOrganization</key>
<string>Thycotic Software, LLC</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadUUID</key>
<string>A63BED50-BCDB-4F17-824A-54A897DDF4FF</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
<array>
<dict>
<key>Allowed</key>
<true>
<key>CodeRequirement</key>
<string>anchor apple generic and identifier "com.thycotic.ThycoticACS" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists /* or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists /* and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists /* and certificate leaf[subject.OU] = UJDHBB2D6Q</string>
<key>Comment</key>
<string></string>
<key>Identifier</key>
<string>com.thycotic.ThycoticACS</string>
<key>IdentifierType</key>
<string>bundleID</string>
</dict>
</array>
</dict>
</dict>
</array>
<key>PayloadDescription</key>
<string>Allows Privilege Manager KEXT to access all files on Catalina</string>
<key>PayloadDisplayName</key>
<string>Privilege Manager ThycoticACSVc Profile</string>
<key>PayloadIdentifier</key>
<string>com.thycotic.privilegemanager.thycoticacsvc</string>
<key>PayloadOrganization</key>
<string>Thycotic Software, LLC</string>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>40A30559-0558-4FA4-8B52-69472EFBD3D</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Troubleshooting on macOS Endpoints

The following topics offer troubleshooting help for macOS endpoints and agents:

- [macOS - FileSystemWatcher](#)
- [How to Recover an Unresponsive macOS Endpoint](#)

How to Recover an Unresponsive macOS Endpoint

In case a macOS endpoint ever becomes unresponsive due to conflicting policy configurations, the following steps allow a user to recover the endpoint without having to restore or rebuild the system.

Note: Applies to all macOS versions on which the KEXT is supported.

1. Turn off the macOS system.
2. Hold down the `⌘+S` keys and power the system back on. Keep holding those keys down until it shows that it is booting in single-user mode.
3. Follow the prompts to mount the root device as read-write. It will instruct you to enter the following:

```
/sbin/fsck -fy  
/sbin/mount -uw /
```

4. Rename the kernel extension so that you can get back to a functioning macOS:

```
cd /Library/Extensions  
mv ThycoticACS.kext ThycoticACS.kext.org  
exit
```

5. The system will restart.
6. Disable and/or delete policies that are causing the issue.
7. Update client items before renaming the kernel extension and having it start automatically. You can force client item updates by performing the following in Terminal.app:

```
sudo /usr/local/thycotic/agent/updateClientItems.sh
```

8. Restore the kernel extension in Terminal.app:

```
cd /Library/Extensions  
sudo mv ThycoticACS.kext.org ThycoticACS.kext  
exit
```


Catalina FileSystemWatcher Issue

There is a known issue on macOS Catalina and later versions, preventing the the agent from receiving notification of events that need to be sent to the server. To workaround this, the **Retry errored TMS Events - Catalina and Big Sur (macOS)** policy can be enabled to ensure all events get sent to the server.

The defaults for this new Remote Scheduled Client Command are as follows:

The screenshot shows the configuration page for a policy named "Retry errored TMS Events - Catalina and Big Sur (macOS)". The page is titled "Retry errored TMS Events - Catalina and Big Sur (macOS)" and includes a search bar, a notification bell, a help icon, and a user profile icon. Below the title, there are tabs for "Details" and "Change History", and a status indicator "Inactive" with a refresh button and a "More" dropdown menu.

Scheduled Job Details

- Name:** Retry errored TMS Events - Catalina and Big Sur (macOS)
- Description:** Scan Agent queue for any events that require retransmission.
- Platform:** Mac OS
- Computer Groups Targeted:** 1 (0 total endpoints)
[All macOS Catalina and Big Sur Computers with Application Control Agent Installed \(Target\)](#) [Add](#)
- Deployment:** Not deployed (Policy is inactive)

Job Settings

- Command:** Retry errored TMS Client Events (MacOS)
- No parameters**

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run.

Default: Daily at 2:00:02 AM starting Mon Oct 01 2018 (repeating every 5 minutes for a duration of 24 hours)

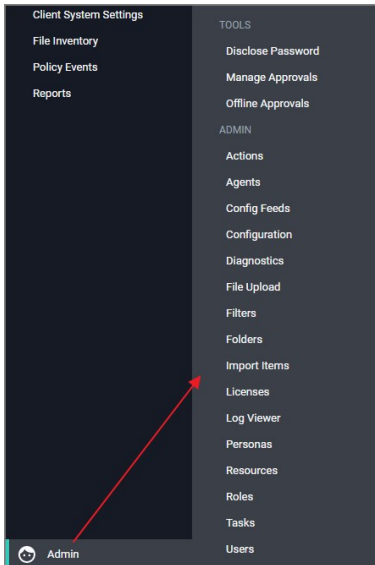
[Add Trigger](#)

- Customize the schedule if necessary to best suit your particular implementation.
- The default resource targets required are specified by default as **All macOS Catalina and Big Sur Computers with Application Control Agent Installed (Target)**. The results of the computer group include any macOS Catalina computers that have the agent installed and are properly configured for Application Control.

Once the policy is enabled on an endpoint, the agent will perform the **Retry errored TMS Client Events (MacOS)** command and send any events that have not been sent.

Privilege Manager Administration

Access to many system administration tasks happens via the **Admin** menu at the bottom of the left navigation menu.



This section of the Privilege Manager documentation covers how to setup and configure resources listed under the Admin Menu. There are other common tasks an Administrator will do like create, edit, and delete policies, local groups and users, those are detailed further under their respective sections and are not addressed here under Admin procedures.

In Privilege Manager, taking action is the name of the Application Control game. Once you know how to accurately identify events via filters, the next crucial step in policy creation is to make stuff happen by applying specific actions to your filtered targets. This begs the question: what actions are possible to perform in Privilege Manager?

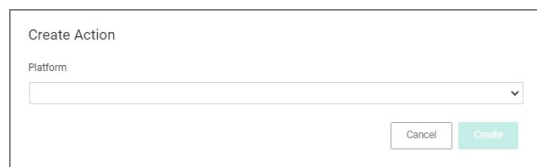
The most popular and well-known action categories in Application Control include:

- **Blocking Actions** - Blocking an application simply means: deny it, or prevent it from running.
- **Monitoring Actions** - This is a category of actions that can be applied to unknown applications that attempt to run. Sandboxing is another term often linked to monitoring, because you can create policies that link to reputation checking tools (like VirusTotal) to perform smart actions once an unknown file's reputation has been verified.
- **Elevation Actions** - Allowing an application to run (allow listing) is good and well for trusted programs, but many trusted applications also require a higher credential set than your end users normally have access to. The elevation action category will allow an application to run with elevated permissions so any user can, for example, install that trusted HP printer on your network without taking time out of a HelpDesk employee's day. Implementing elevation policies allow "Least Privilege" to be implemented by your organization, eliminating the need for local users to have full administrator access on their computer.
- **Workflow Actions** - Some actions explicitly enforce an organization's workflow system. The big example here is the "Request Access" action that will prompt a user for the reason they are trying to access an application for verification purposes and auditing.
- **Display Message Actions** - Display messages are paired with one of the action types listed above. Display Message Actions are customizable and serve to tell the end user what is happening and why.

For a more complete (and more specific) list of all out-of-the-box Privilege Manager actions and types of actions, see the [List of Default Actions](#) topic.

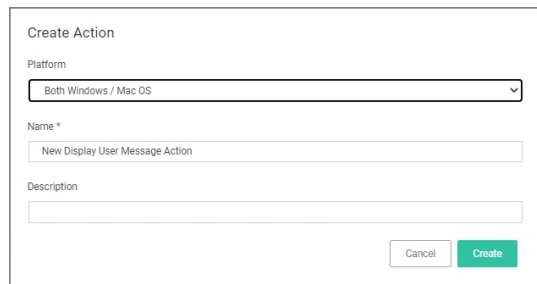
Creating a New Action Manually

Navigate to **Admin | Actions** in Privilege Manager and click **Create Action**. Under Action Details, select a platform type and then choose an action type from the dropdowns (see our Actions' Catalog for descriptions of action types).



The screenshot shows the 'Create Action' form. The 'Platform' dropdown menu is open, showing a list of options. The 'Cancel' and 'Create' buttons are visible at the bottom right of the form.

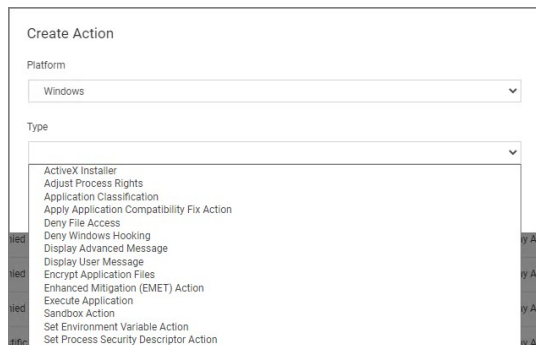
Select a specific platform or choose both:



The screenshot shows the 'Create Action' form with 'Both Windows / Mac OS' selected in the Platform dropdown. The Name and Description fields are empty. The 'Cancel' and 'Create' buttons are visible at the bottom right.

If **Both Windows / Mac OS** is selected, enter a name/description and click **Create**. Otherwise select a type from the drop-down based on selected platform:

- Windows:



The screenshot shows the 'Create Action' form for Windows. The Platform dropdown is set to 'Windows'. The Type dropdown is open, showing a list of action types including: ActiveX Installer, Adjust Process Rights, Application Classification, Apply Application Compatibility Fix Action, Deny File Access, Deny Windows Hooking, Display Advanced Message, Display User Message, Encrypt Application Files, Enhanced Mitigation (EMET) Action, Execute Application, Sandbox Action, Set Environment Variable Action, and Set Process Security Descriptor Action.

- macOS:



The screenshot shows the 'Create Action' form for macOS. The Platform dropdown is set to 'Mac OS'. The Type dropdown is open, showing a list of action types including: Allow Copy Action (MacOS), Display Advanced User Message (MacOS), and Display User Message.

Name your new action and type a Description, then click **Create**.

Editing options for this action will depend on the type of was action selected from the drop-down.

Windows Specific Actions

The following are Windows specific topics on actions:

- [ActiveX Installer Action](#)
- [Application Classification Action](#)
- [Apply Application Compatibility Fix Action](#)
- [Deny File Access Action](#)
- [Deny Windows Hooking Action](#)
- [Encrypt Application Files Action](#)
- [Endpoint Group Member Approval Action](#)
- [Set Environment Variable Action](#)
- [Execute Application Action](#)
- [Group Member Approval Action](#)
- [Sandbox Action](#)
- [Set Process Security Descriptor Action](#)
- [Adjust Process Rights Action](#)

Adjust Process Rights Action

This topic explains the Adjust Process Rights Action and Unrestricted Tokens in Privilege Manager.

When elevating process rights with Application Control Solution (ACS) on Windows, there are times when the rights given by ACS appear to be insufficient. The process still doesn't work as it does when the user is logged in as Administrator, accepts the UAC box, or the process is run with the right-click Run As Administrator option. Sometimes an error is returned stating insufficient rights to access.

Microsoft with the release of Windows Vista introduced changes to security which included creating two tokens for users when they log in. For more information refer to the [Microsoft Documentation on Restricted Tokens](#).

The lower privilege token is the one always used unless the user goes through UAC or other processes. ACS allows administrators to choose which token should be used to elevate certain processes. The lower privilege token, if it works, is the better option as it has fewer privileges and thus protects the system better. But if necessary, the higher-privilege token can be used by ACS when manipulating the process's security configuration.

The following are the Privilege Manager default Adjust Process Rights Actions. As with all actions delivered with Privilege Manager, these actions cannot be modified. They can be copied and then customized and as many actions as necessary can be created for a custom implementation:

- Add Administrative Rights
- Add Administrative Rights - Unrestricted
- Adjust Process Rights for Resource Monitor
- Remove Administrative Rights
- Remove Advanced Privileges Action

Each of those actions has by default Related Items associated, which need to be considered when customizing an action.

Note: The **Suppress UAC** action should only be used with Agent versions 10.4 and older.

Adjust Process Rights Action Settings Explained

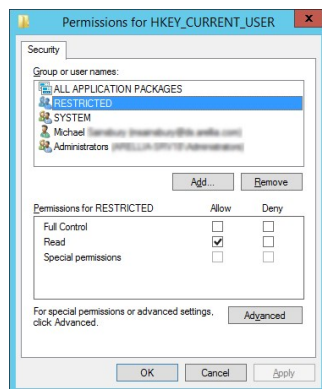
The application action elevates or restricts the permissions and/or privileges held by a process security token. By default, each process inherits the user's security token.

The four main areas to customize are:

- Selecting an **Action Type**, which can either Elevate Rights or Restrict Rights. When the adjustment is a rights restriction, there is an advanced feature that allows you to apply restricted Security Identifiers (SIDs), which further restricts access to securable objects. More about this under the [What is a Restricted SID](#) topic.
- Adding or Removing **Windows Privileges**, these come pre-populated with a set of default recommendations for each out of the box Action. To learn more about these Windows Privileges visit [Microsoft's Documentation about User Rights Assignment](#).
- Adding or Removing **Build-in Roles**, these are the roles that provide file level access to a system and they are based on group membership.
- Adding or Removing **Well-known Accounts**, these are specifying the integrity levels at which processes can run. Also refer to [Microsoft's Documentation about Mandatory Integrity Control](#).

What is a Restricted SID?

A restricted ID is an access token that modifies a user's access to securable objects and controls a user's ability to perform various system-related operations on the local computer.



When a restricted process or thread tries to access a securable object, the system performs two access checks, using the

- token's enabled SIDs, and
- the list of restricted SIDs.

Access is granted only if both access checks allow the requested access rights.

When to use restricted ID

Use a restricted SID to further restrict the applications in the sandbox, which you can use as another method of monitoring. In other words, this is a way to protect yourself against unknown applications if you don't want to implement a blocking policy.

The restricted SID will allow only Read access to the user registry but not to the local machine registry. Also, restricted processes do not have rights to open any network-based resource, such as file servers. As a result, the restricted SID will be able to do very little and apps may not work correctly under this model. Ultimately, apps in the sandbox that have restricted SID applied to them will be severely locked down.

Using Apply Restricted SID

When you select Restrict Rights and then Apply Restricted SID, you add the Restricted SID to the process. When evaluating security for any operation, when there is any Restricted SID specified then not only does the Security Descriptor need to allow access to the user, but explicitly to the Restricted SID.

How to Add Windows Permissions

Windows permissions are specific OS based permissions to perform actions, like changing system time or taking ownership of a files vs. accessing securable resources. To learn more about these Windows Privileges visit [Microsoft's Documentation about User Rights Assignment](#).

How to Use Well-known Accounts

In this area you will most likely specify either of the following:

- High Mandatory Level
- Low Integrity Level
- Medium Integrity Level
- Medium Plus Integrity Level
- Restricted Code Well Known Group
- System Integrity Level
- Untrusted Mandatory Level

These integrity levels determine who else can use a specific process. Processes launched by a standard user are by default medium integrity. Any process that gets launched via an elevated policy has a high integrity level assigned by default.

Processes need to have level parity to be able to utilize each other. This means, if a process is running at a high integrity level and wants to inject code into another process, it can do so if that other process is running at high, medium, or low integrity levels, but it cannot inject code into system level processes. Processes that run at low integrity levels can be utilized by pretty much any other process, but they cannot reach out to other processes.

New processes are always created with the minimum of the user integrity and file integrity levels. This guarantees that a new process never executes with higher integrity than the executable file.

Example Scenario

In Privilege Manager we can use these Well-known Accounts to set or remove level integrity independent of or in combination with any assigned elevation or blocking policies.

For example, Adobe applications are generally part of elevation policies in an organization. As mentioned before an elevation policy defaults to a high integrity level. Due to Adobe interoperability requirements within their product suites and with processes launched by standard users, it requires medium integrity levels for all Adobe products.

Any elevation policy pertaining to Adobe products, needs an **Adjust Process Rights Action** that sets the **Well-known Accounts** setting to **Medium Integrity Level**.

Additional Options Explained

Under Additional Options customers can select to **Use User's Unrestricted Token** and **Disallow changes to the process rights after applying changes**.

The use of the unrestricted token option is another level of available customization beyond what can be enabled or disabled via the Adjust Process Rights Settings. Enabling this token presents the user with extra levels of access rights over the process. If changes to the process rights are disallowed, the user's unrestricted token is valid as long as the pertaining process is running.

For example if you have a standard user policy for a certain process to run at medium integrity level, but you want to enable more rights without fully elevating and granting the process a high integrity level, you can use the unrestricted access token to fine tune.

Enabling Unrestricted Token Use

To set the unrestricted token, follow these steps:

1. Select the action of type **Adjust Process Rights Action** that best fits your specific business need.
2. Create a copy of that action.
3. Select the **Use User's Unrestricted Token** checkbox on the copied action and save the action with a new name (for example "Unrestricted Token - Add Admin Rights").
4. Add the new action to new policies or change existing policies and remove the old action.
5. Add the new action and save the changes.
6. Then update the agent client policies.
7. The ACS agent must retrieve the details of the new action from the server via the ACS web service.
8. The change may take a few minutes to reach the client machine after the client policies have updated depending on how busy the server is.

Adjust Process Right for Resource Monitor

The following image shows the default action. To customize make a copy to change any of the default items.

The screenshot displays the configuration interface for the 'Adjust Process Rights for Resource Monitor' action. It is divided into several sections:

- Action Details:**
 - Name:** Adjust Process Rights for Resource Monitor
 - Description:** This actions will adjust process rights necessary to run Resource Monitor.
 - Platform:** Windows
- Adjust Process Rights Settings:**
 - Action Type:** Elevate Rights (selected), Restrict Rights
 - Windows Privileges:** Act as part of the operating system, Bypass traverse checking, Change the system time, Create a pagefile, Create a token object, Create Global Objects, Debug programs, Impersonate a client after authentication, Load and unload device drivers, Profile system performance, +2 more. Includes an 'Edit' link.
 - Built-in Roles:** Administrators. Includes an 'Edit' link.
 - Well-known Accounts:** Add Well-known Accounts
- Additional Options:**
 - Use user's unrestricted token
 - Disallow changes to the process rights after applying changes

Related Item - Policy

The following image shows the default related item policy for the above action. To customize make a copy to change any of the default items.

Client Option - Elevate Resource and Performance Monitoring

This item is read-only.

General Policy Events Change History Inactive Duplicate More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers
Deployment	Not deployed (Policy is inactive)
Last Modified	Jul 6, 2020, 1:58:06 PM by Trusted Installer
Priority *	60
Description	Elevates privileges of users to allow them to run Windows Resource and Performance Monitor ut...

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
[Filters](#)

Applications Targeted	Performance Monitor Utility (perfmon.exe) Resource Monitor (resmon.exe)
Inclusions	No options selected
Exclusions	No options selected

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy
[Actions](#)

Actions	Adjust Process Rights for Resource Monitor
Child Actions	No options selected
Audit Policy Events	<input type="checkbox"/> Record all activity detected by this policy in Policy Events

ActiveX Installer Action

This type of action is a specific use-case for older Windows systems (Windows XP and Windows Server 2003). The ActiveX installer action allows or denies an application to enable standard users to install approved ActiveX components. If you don't know what ActiveX means, you won't need to use this type of action.

New ActiveX Installer

[Details](#) [Related Items](#) [Change History](#) [Refresh](#) [More](#)

Action Details

This action is only supported on Windows XP and Windows Server 2003 Operating Systems. To elevate ActiveX controls on new Windows Operating Systems, create and deploy an ActiveX Group Policy via Privilege Manager.

Name	New ActiveX Installer
Description	<input type="text"/>
Platform	Windows

ActiveX Installer Settings

To see available ActiveX components, enable the [COM Inventory Policy](#)

Deny ActiveX Components	Add Deny ActiveX Components
Elevated Installation	Add Elevated Installation
Silent Elevated Installation	Add Silent Elevated Installation

Parameters

The following details can be set on the ActiveX action:

- Deny ActiveX Components, or
- Elevated Installation, or
- Silent Elevated Installation

For those actions for ActiveX, these parameters can be specified:

- Scope by Organization Group
- Search text
- Maximum rows returned
- Resources (use the column filter function to locate a resource and click **Add**)

Application Classification Action

This type of action will restrict applications from modifying certain items and will enforce standard Windows ACLs when the targeted application accesses restricted files, folders, registry keys, or services on a computer.

New Application Classification Action

[Details](#) [Related Items](#) [Change History](#) Refresh More

Action Details

Name	<input type="text" value="New Application Classification Action"/>
Description	<input type="text"/>
Platform	Windows

Application Classification Settings

Application Classification	<input type="text" value="Classification"/>
----------------------------	---

Apply Application Compatibility Fix Action

This type of action will allow old applications that must be run via compatibility mode to execute without manual compatibility adjustments.

The screenshot shows a web interface for configuring a 'New Application Compatibility Fix'. At the top, there are tabs for 'Details', 'Related Items', and 'Change History', along with 'Refresh' and 'More' buttons. The 'Action Details' section includes a 'Name' field with the value 'New Application Compatibility Fix', a 'Description' field with the text 'This action will apply the specified application compatibility fix', and a 'Platform' dropdown set to 'Windows'. The 'Compatibility Layer Settings' section has two radio buttons: 'Standard Layer' (unselected) and 'Custom Layer' (selected). Below this is a 'Layer Name' text input field. There are two sub-sections, 'Shims' and 'Flags', with 'Shims' being the active tab. The 'Shims' section shows '0 Items' and an 'Add Shim' button.

Parameters

The following Compatibility Layer Settings can be set on the Apply Application Compatibility Fix action:

- Custom vs. Standard Layer, which lets users select a layer either x86 and x64, x86 only, or x64 only.
- Shims
- Flags

Deny File Access Action

As the name suggests, this type of action will prevent applications from reading or writing (or both) to certain directories or to certain file types.

The screenshot shows a configuration window titled "New Deny File Access Action". It has tabs for "Details", "Related Items", and "Change History". There are "Refresh" and "More" buttons in the top right. The "Action Details" section includes a "Name" field with the value "New Deny File Access Action", a "Description" text area, and a "Platform" dropdown set to "Windows". The "Deny File Access Settings" section includes "Deny Access" with radio buttons for "Deny Read" and "Deny Write", a "Path" field with an "Include subdirectories" checkbox, "File Extensions" with a link "Add File Extensions", and "MIME Types" with a link "Add MIME Types".

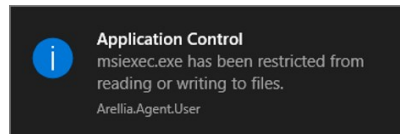
Parameters

The following Deny File Access Settings can be specified:

- Deny Access to read and/or write operations.
- Path and possibly subdirectory locations.
- Specific file extensions.
- MIME types.

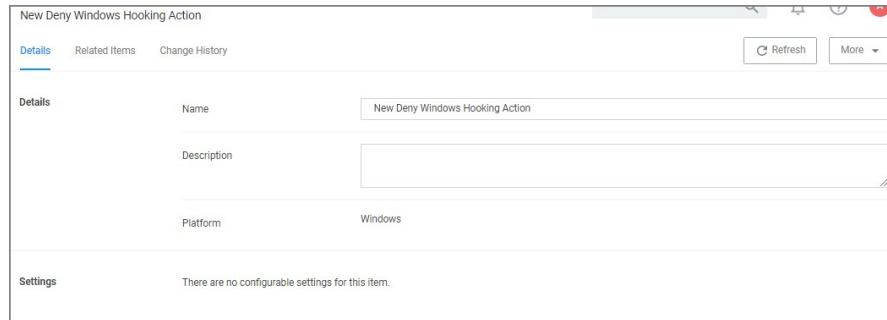
Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.



Deny Windows Hooking Action

This type of action will limit specified applications from interacting in malicious ways with other applications.

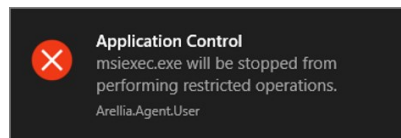


The screenshot shows a configuration window titled "New Deny Windows Hooking Action". It has three tabs: "Details", "Related Items", and "Change History". The "Details" tab is active. At the top right of the details section, there are "Refresh" and "More" buttons. The "Details" section contains three fields: "Name" with the value "New Deny Windows Hooking Action", "Description" which is empty, and "Platform" with the value "Windows". Below the details section is a "Settings" section with the text "There are no configurable settings for this item."

This action does not have any configurable parameters.

Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



Encrypt Application Files Action

This type of action will force applications to use Microsoft encryption when saving a file.

New Encrypt Application Files Action

Details Related Items Change History Refresh More

Action Details

Name: New Encrypt Application Files Action

Description:

Platform: Windows

Encrypt File Settings

Path:

Include subdirectories

File Extensions: [Add File Extensions](#)

MIME Types: [Add MIME Types](#)

Parameters

The following Encrypt Application Files Settings can be specified:

- Path and the option to include subdirectories.
- File Extensions.
- MIME Types.

Endpoint Group Member Approval Action

This action can be used for *over the shoulder* approvals, whether systems are on- or offline. The supervisor approves access by authentication on the user's endpoint system.

1. Navigate to **Admin | Actions**.
2. Click **Create**.
 1. On the **Create Action** modal from the **Platform** drop-down select **Windows**.
 2. From **Type** drop-down select **Endpoint Group Member Authenticated Approval Action**.
 3. Enter a meaningful **Name** and **Description**.
 4. From the **Approval Group** drop-down, select the group membership of the approver.

Create Action

Platform
Windows

Type
Endpoint Group Member Authenticated Approval Action

Name *
New Endpoint Group Member Authenticated Approval Action

Description

Approval Group *
Web Admin

5. Click **Create**.

[Back to Actions](#)

New Endpoint Group Member Authenticated Approval Action

Details Related Items Change History Refresh More

Action Details

Name: New Endpoint Group Member Authenticated Approval Action


Description:

Platform: Windows

Settings

Require approval by a member of the group: [Web Admin](#)

Window Design

Message prompt logo: 

Application label: Application:

Approval status label: Approval status:

Approval status section: A previous request for this application has been submitted for review.

Cancel button text: Cancel

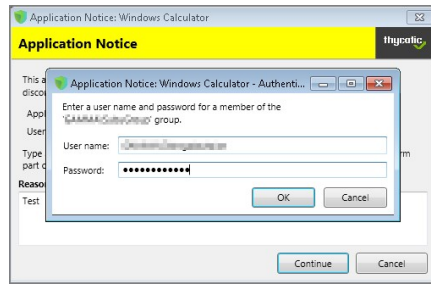
Continue button text: Continue

Information section: This application has not been approved for use according to corporate policy. Please discontinue use or enter

3. Under Settings verify the **Require approval by a member of the group**: contains the correct group. If you ever need to change it, come back to this page and click the group name to access the change modal.
4. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for these approvals.
5. Under the **Actions** section, search for and add the action you previously created.
6. Click **Save Changes**.
7. Click the **I** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your endpoint agents.

Policies also automatically update according to a schedule.

Sample Group Member approval notice with approval overlay:



Refer to the **Endpoint Group Member Authenticated Approvals** report to view a history of "over the shoulder" approvals:

Endpoint Group Member Authenticated Approvals

Filter Report Refresh CSV PDF Search

Drag column here for grouping

User	File Path	Time	Policy	Agent	Approver	Command Line	Reason
...	C:\Windows\sys...	9/22/2020 11:57 PM	Test Service Now Application Control Policy	*C:\Windows\sys...	Test
...	C:\Windows\sys...	9/22/2020 10:36 PM	Test Service Now Application Control Policy	*C:\Windows\sys...	Test
		9/22/2020 10:12 PM		...			
		9/22/2020 9:37 PM		...			
		9/22/2020 4:50 PM		...			
		9/22/2020 4:45 PM		...			

10 items per page 1 - 10 of 10 items

Related Topics

- [Group Member Authenticated Message Action](#), which guides you through setting up approvals based on the group membership of the approver.
- [Using an Endpoint Group Member Authenticated Message Action](#), which guides you through setting up *over the shoulder* approvals that can be used on- and offline with a ServiceNow system integration.

Execute Application Action

This type of action will execute another application and (optionally) wait on that process to complete before the original process can execute.

New Execute Application Action

Details Related Items Change History Refresh More

Action Details

Name: New Execute Application Action

Description: This action will execute the specified application.

Platform: Windows

Execute Application Settings

Executable:

Command Line:

Wait for executable to complete before allowing process to run

Terminate process if exit code:

Parameters

The following Execute Application Settings can be specified:

- an executable
- command line arguments

Group Member Approval Action

This action can be used for approvals that are based on a group membership authentication of the approver.

1. Navigate to **Admin | Actions**.
2. Search and select **Group Member Authenticated Message Action**.
3. Click **Duplicate**.
4. Name your new action and click **Create**.

← Back to Group Member Authenticated Message Action

New Group Member Authenticated Message Action

Details Related Items Change History Refresh More

Action Details

Name: New Group Member Authenticated Message Action

Description: This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member.

Settings


This feature is not supported for Azure Active Directory joined computers. Only Domain joined computers will work.

Require authentication:

- By the interactive end-user
- By a member of the group: Administrators

Wait for message prompt to complete before running application

Window Design

Message prompt logo:  Choose File | No file chosen

Application label: Application:

Authorization information section: Please have a member of this group authorize this request to continue.

Cancel button text: Cancel

Continue button text: Continue

5. Customize the Action based on your specific business requirements.
6. Verify the **By the member of the group:** is active and a group is listed below the button. If you ever need to change it, come back to this page and click the group name to access the change modal.
7. Click **Save Changes**.
8. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for these approvals.
9. Under the **Actions** section, search for and add the action you previously created.
10. Click **Save Changes**.
11. Click the **I** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your endpoint agents.

Policies also automatically update according to a schedule.

Related topics:

- [Endpoint Group Member Authenticated Message Action](#), which guides you through setting up *over the shoulder* approvals that can be used on- and offline.
- [Using an Endpoint Group Member Authenticated Message Action](#), which guides you through setting up *over the shoulder* approvals that can be used on- and offline with a ServiceNow system integration.

Sandbox Action

This type of action will limit the environments in which certain code can execute. The sandbox runs a process in a job object that limits its ability to interact with other processes, as well as limiting some specific types of interactions with the operating system.

New Sandbox Action

Details Related Items Change History Refresh More

Action Details

Name: New Sandbox Action

Description: [Text Area]

Platform: Windows

Sandbox Action Settings

Restrictions:

- Limit Desktop
- Limit Global Atoms
- Limit Display Settings
- Limit System Parameters
- Limit Write Clipboard
- Limit Handles
- Limit Exit Windows
- Limit Read Clipboard

Parameter

The following Sandbox Action Settings can be enabled:

- Limit Desktop
- Limit Global Atoms
- Limit Display Settings
- Limit System Parameters
- Limit Write Clipboard
- Limit Handles
- Limit Exit Windows
- Limit Read Clipboard

Set Environment Variable Action

This type of action sets an environment variable for processes that could change the behavior of an application, or be caught by an Environment Variable filter in another policy.

The screenshot shows a configuration window titled "New Set Environment Variable Action". At the top, there are tabs for "Details", "Related Items", and "Change History". To the right of the tabs are "Refresh" and "More" buttons. The main content is divided into two sections: "Action Details" and "Environment Variable Settings".

Action Details	
Name	<input type="text" value="New Set Environment Variable Action"/>
Description	<input type="text" value="This action will set the specified environment variable."/>
Platform	Windows

Environment Variable Settings	
Name	<input type="text"/>
Value	<input type="text"/>

Parameters

The parameters for the Set Environment Variable action are setting the name and value of the environment variable.

Set Process Security Descriptor Action

Adjusting Process Security allows a process to be protected from most tampering by users. For example, adjusting process security can restrict who can stop a process from the task manager.

The screenshot shows a configuration window titled "New Set Process Security Descriptor". At the top, there are tabs for "Details", "Related Items", and "Change History". To the right of the tabs are "Refresh" and "More" buttons. The main content area is divided into two sections: "Action Details" and "Process Security Details".

Action Details

Name	<input type="text" value="New Set Process Security Descriptor"/>
Description	<input type="text" value="This action will apply the specified security descriptor to the process"/>
Platform	Windows

Process Security Details

Alters the process security using the specified Security Descriptor

Process Security Descriptor	<input type="text" value=""/>
-----------------------------	-------------------------------

Parameters

The parameters for the Set Process Security Descriptor action are done via resource selection from a list of available security descriptors.

macOS Specific Actions

The following are macOS specific topics on actions:

- [Display Advanced User Message Action \(MacOS\)](#)
- [Allow Copy Action \(MacOS\)](#)
- [Just-in-Time Group Membership Action](#)

Allow Copy Action (MacOS)

Action to allow copying of application on macOS systems.

New Allow Copy Action (MacOS)

Details Related Items Change History Refresh More

Action Details	Name	New Allow Copy Action (MacOS)
	Description	
	Platform	Mac OS

Allow Copy Settings	Path	
---------------------	------	--

Parameters

The following Allow Copy Action Settings can be specified:

- Path

Display Advanced User Message Action (MacOS)

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

New Display Advanced User Message Action (MacOS)

deny

Details Related Items Change History Refresh More

Action Details

Name New Display Advanced User Message Action (MacOS)

Description

Platform Mac OS

Settings

Title

Message Type Deny Application Message

Approval type

Message 1

Parameters

The following Display Advanced Message Settings can be specified:

- Title
- Message Type, such as
 - Deny Application Message
 - Warning Message
 - Justify Application Usage
 - Deny Application with Justification
 - Approval Request Message
- Message, which is the actual text of the message displayed to the user.

Just-in-Time Group Membership Action

This action will add a user to the specified group for a specified time. This action can then be added to a controlling policy to give Just-in-Time elevation to a user. The action is a read-only action by default. To customize this macOS action for your endpoints, use the **Duplicate** option.

1. Navigate to **Admin | Actions**.
2. Search for and select **Just-in-Time Group Membership** from the list of available macOS actions.
3. Click **Duplicate**.
4. Enter a name for your newly created action and click **Create**.

The screenshot shows the configuration page for the 'macOS Just-in-Time Group Membership' action. The page has a breadcrumb trail: '< Back to Just-in-Time Group Membership'. Below the title, there are tabs for 'Details', 'Related Items', and 'Change History'. A 'Refresh' button and a 'More' dropdown menu are also present. The 'Action Details' section includes a text description: 'This action will add a user to the admin group for a specified time.' The 'Name' field is filled with 'macOS Just-in-Time Group Membership', and the 'Description' field contains the same text. The 'Platform' is set to 'Mac OS'. The 'Settings' section includes a note: 'Enter the name of the group as it will appear on the endpoint. Consider that authorization is checked when the application is started when you set your duration, you may only need a few seconds.' The 'Group Name' field is filled with 'admin'. The 'Duration' section has two radio buttons: 'Specific length of time' (unselected) and 'As long as application is active' (selected). The 'Specific length of time' option has a value of '5' and a unit dropdown set to 'Minute(s)'.

5. Under **Settings** specify
 1. the **Group Name** as created on the endpoint.
 2. the **Duration** either
 - set a specific length of time, here you need to consider that authorization is started when the application starts, or
 - use the default *as long as application is active*.
6. Click **Save Changes**.

Message Actions

Messages are the most common application action used in Privilege Manager. These messages are presented for end users on their endpoints. There are two kinds of messages:

- Basic, these display as smaller pop-ups directly from the taskbar area. They display and fade automatically. From the Action Type drop-down these are the [Display User Message](#) actions for both Windows and macOS.
- Advanced, these messages display as a user dialog, requiring users to justify access to a certain application or to warn the user. Most of these messages require user interaction, but some can be set to fade in and out for the end user. From the Action Type drop down these are the [Display Advanced Message](#) for Windows and [Display Advanced User Message \(MacOS\)](#) for macOS endpoints.

Both basic and advanced messages are useful for providing feedback to users that an application is being blocked, usage of the application is being logged, or any message that the end user should see.

Basic vs. Advanced Messages

Basic messages briefly pop up from the end user's task bar. They display like other Windows notifications, are shown on the screen, and then disappear without any user interaction required.

Basic messages do not include custom branding or logos. It is easiest to edit basic messages via Privilege Manager's UI. However, the default message may suffice for some use. Basic messages only display a message. These messages do not perform an action. For example, the basic Deny Execute Message should be used in conjunction with the Deny Execute action.

Advanced messages display as a new dialog, typically in the center of the screen, and usually require an interactive action from the end user - entering a justification, enter credentials, waiting for approval, selecting a continue or cancel button, etc.

Advanced message actions are used for justification and approval policies. The 'Application Denied Notification Action' is the only default advanced message that does not require an interactive action from the end user. While this message has a cancel button to remove the message, this message will fade from the user's screen after a short period of time.

Advanced messages include branding, which can be customized. Some fields are recommended to edit in the XML instead of the UI. These details are expanded in the section on Customizing Advanced Messages.

Types of Advanced Message Actions

There are three categories of advanced messages:

- Advanced Feedback Messages - require information from the end user.
- Approval Request Messages - require information from the end user and approval from the application support team.
- No Required Input Messages - display information to the end user, but do not require information from the end user. May require a button push to clear the message.

Advanced Feedback Messages

Advanced feedback messages require users to justify their need to use an application.

Authentication Justification Message Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.

The screenshot shows a dialog box titled 'Application Notice' with a yellow header and a 'thycotic' logo. The main text reads: 'This application has **not been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue.' Below this, it says 'Application: msiexec' and 'Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.' There is a text input field labeled 'Reason (required):'. At the bottom, there are fields for 'User name:' (containing 'MPT-WINPC01\Administrator') and 'Password (required):', along with 'Continue' and 'Cancel' buttons.

Group Member Authenticated Message Action

This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member. This process is also known as an over-the-shoulder request, meaning that the end-user will have to get their boss or a member of a specific domain user group to approve the request.

The screenshot shows a dialog box titled 'Application Notice' with a yellow header and a 'thycotic' logo. The main text reads: 'This application has **not been approved** for use according to [corporate policy](#).' Below this, it says 'Application: msiexec' and 'Date: 11/4/2019 4:22:53 PM'. A blue information box contains the text: 'This process requires authentication by a member of the following group. Group name: Please have a member of this group authorize this request to continue.' Below this, there are fields for 'User name:' (containing 'MPT-WINPC01\Administrator') and 'Password (required):', along with 'Continue' and 'Cancel' buttons.

Justify Application Elevation Action

This action will display a justification prompt to the user before allowing the application to run. The Justify Application Elevation Action is to be used with the User Requested Run As Administrator filter in an application control policy. This action collects information from users and creates reports on the server for approval requests.

Application Elevation: msixec

Application Elevation

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Continue Cancel

Justify Application Message Action

This action will display a justification prompt to the user before allowing the application to run. It is used to collect information from users and create reports on the server with reasons why a user was running an application that hasn't been approved or denied yet.

Application Elevation: msixec

Application Elevation

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Continue Cancel

Approval Request Messages

The approval request messages are similar to the justification messages because they both gather feedback from end users and report it in the Privilege Manager console. Approval request messages also allow for end-users to see a waiting screen until their request has been either approved or denied.

Approval Request Form Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.

Application Notice: msixec

Application Notice

This application has **not been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

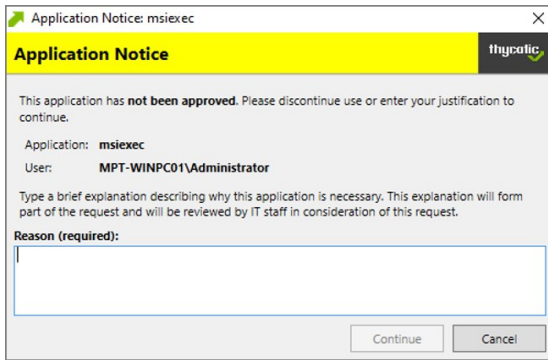
Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.

Reason (required):

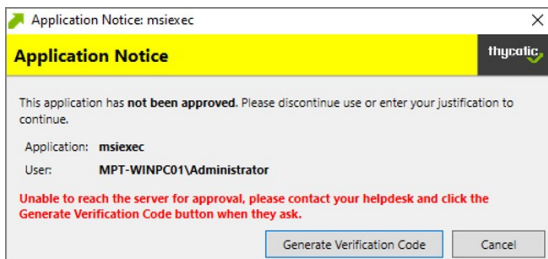
Continue Cancel

Approval Request (with Offline Fallback) Form Action

This action displays an approval request form before allowing the application to run. These messages will then show a waiting screen until the request is either approved or denied by the appropriate Privilege Manager user/admin. With this advanced message, the same dialogue box as the Approval Request Form Action will appear:



If the machine is offline or can't connect to Privilege Manager to upload the request, another dialogue box will then appear to prompt the end user to contact the helpdesk and generate a verification code:

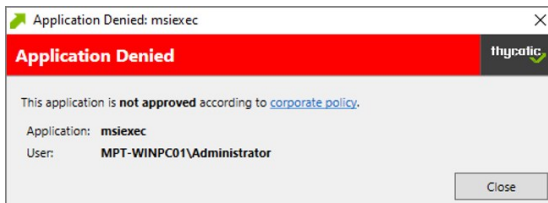


No Required Input Messages

No required input messages differ from the advanced feedback message actions because they do not require a justification to continue. End users need only acknowledge the displayed message. This feature requires that the Microsoft .Net Framework is installed on client machines.

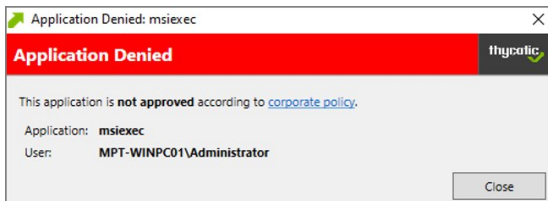
Application Denied Message Action

This action stops an application from being launched and will display a notification of denial to the user attempting to run a process controlled by a policy.



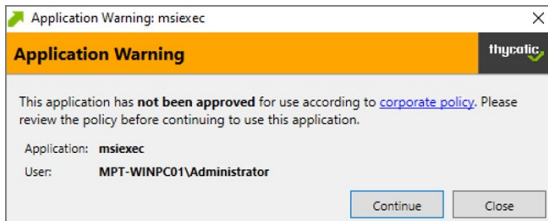
Application Denied Notification Action

This action will display a notification to the user that the process has been denied by a policy. The notification window fades in and out automatically and will close after a defined period of time.



Application Warning Message Action

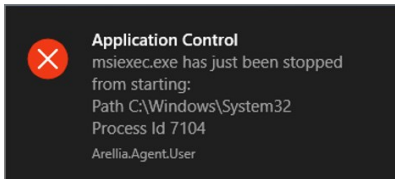
This action will display a warning to the user before allowing the application to run.



Types of Basic Messages

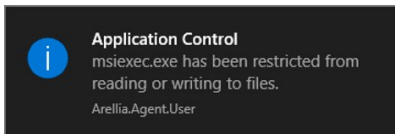
Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



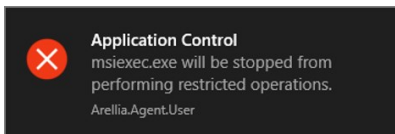
Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.



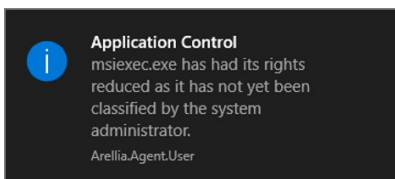
Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



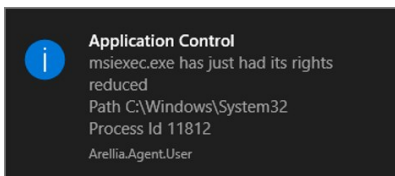
Limit Process Rights for New Applications Message

This action displays a message to the user informing that an application has had its rights reduced. The Remove Administrator Rights or Remove Advanced Privileges Action needs to be used with this message.



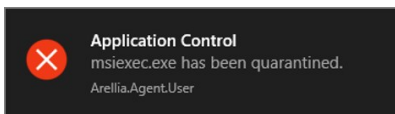
Remove Rights Message

This action displays a message to the user informing them of an associated action. The Remove Administrative Rights Action or Remove Advanced Privileges Action should be used with this message.



Quarantine Message

This action displays a message to the user informing that an application has been quarantined. The File Quarantine Action should be used with this message.

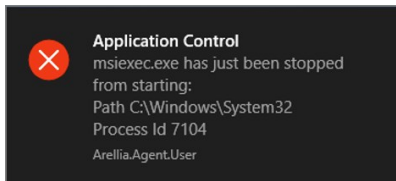


Deny Execute Action

This action stops specific application from executing. It is a default action without any configurable settings. It is a read-only item.

Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



Deny Execute Message

The Deny Execute Message does not include company branding and is easy to edit in the Privilege Manager console. The default of this basic user message action is displayed like this:

Deny Execute Message

This item is read-only.

Details | Related Items | Change History

Duplicate | More

Action Details

Name	Deny Execute Message
Description	This action displays a message to the user informing them that an application has been denied execution.
Platform	Windows, Mac OS

Display User Message Settings

Title	Application Control
Message	{0} has just been stopped from starting: Path (1) Process Id (3)
Icon type	Error
Display Timeout	3 second(s)

Customization

1. In Privilege Manager, search for the default message that will be customized. In this example, we search for the default **Deny Execute Message**.
2. Select the item from the search results.

Search Results for Deny Execute Message

deny execute message

2 Items | Type: All

NAME	TYPE	MODIFIED	DESCRIPTION
Company - Deny Execute Message	Display User Message Action	12/3/19, 6:43 AM	This action displays a message to the user informing the...
Deny Execute Message	Display User Message Action	7/6/20, 1:58 PM	This action displays a message to the user informing the...

3. This is a read-only action, to customize the default message, users need to click **Duplicate**.

Deny Execute Message

This item is read-only.

Details | Related Items | Change History

Duplicate | More

Action Details

Name	Deny Execute Message
Description	This action displays a message to the user informing them that an application has been denied execution.
Platform	Windows, Mac OS

Display User Message Settings

Title	Application Control
Message	{0} has just been stopped from starting: Path (1) Process Id (3)
Icon type	Error
Display Timeout	3 second(s)

4. Enter a name for the new message action. It is recommended to use standard naming conventions with your custom items, e.g. beginning custom names with your company name is a great way to differentiate between the default items and your custom items.
5. Click **Create**.
6. Customize the Title and Message, use the Icon Type drop-down to specify the type, and set the Display Timeout.

Company - Deny Execute Message

Details Related Items Change History Refresh More

Action Details

Name: Company - Deny Execute Message

Description: This action displays a message to the user informing them that an application has been denied execution.

Platform: Windows, Mac OS

Display User Message Settings

Title: Application Control

Message: (0) has just been stopped from starting.
Path (1)
Process Id (3)

Icon type: Error

Display Timeout: 3 Second(s)

7. Click **Save Changes**.

Display Advanced Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

Parameters

The following Display Advanced Message Settings can be specified:

- Require authentication.
 - By the interactive end-user
 - By a member of the group
 - Wait for message prompt to complete before running application

Further the Window Design parameters can be set. Those settings include customization of company logo for branding, label, status, button, instruction, prompt, and reason texts just to name a view.

Examples

- [Create Custom Notifications](#)

Display User Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

Test Display User Message Action

Details Related Items Change History Refresh More

Action Details

Name: Test Display User Message Action

Description: Testing Display User Message action

Platform: Windows

Display User Message Settings

Title:

Message:

Icon type: Information

Display Timeout: 3 Second(s)

This action is available for both Windows and macOS systems.

Parameters

The following Display User Message Settings can be specified:

- Title
- Message
- Icon type, which can be specified as Information, Warning, Error, Thycotic, or Program.
- Display timeout setting, which can be specified in Seconds, Minutes, Hours, Days, or Weeks.

Examples

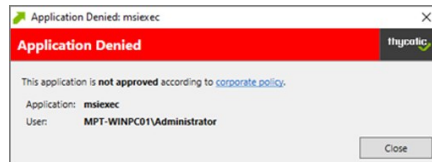
- [Deny Execute Message](#)

[priority]: # (3)

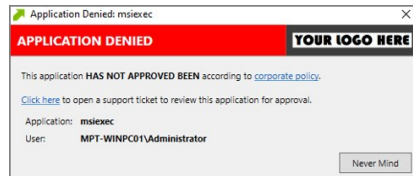
Create Custom Notifications

The default Application Denied Notification Action can be edited/replaced by a customized notification action to better suite a specific customer need.

Example of Default Notification:



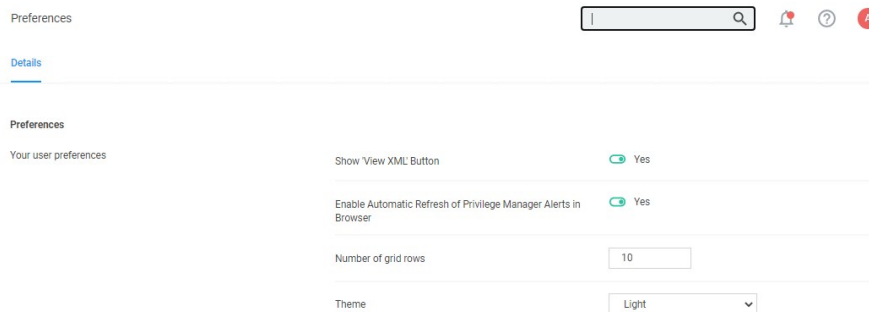
Example of Custom Notification:



Enable View as XML

To edit the message text the **View as XML** button has to be enabled in your console.

1. Navigate to and click your user icon, select **Preferences**.
2. Verify **Show 'View XML' Button** is set to **Yes**, if set to No change the switch.

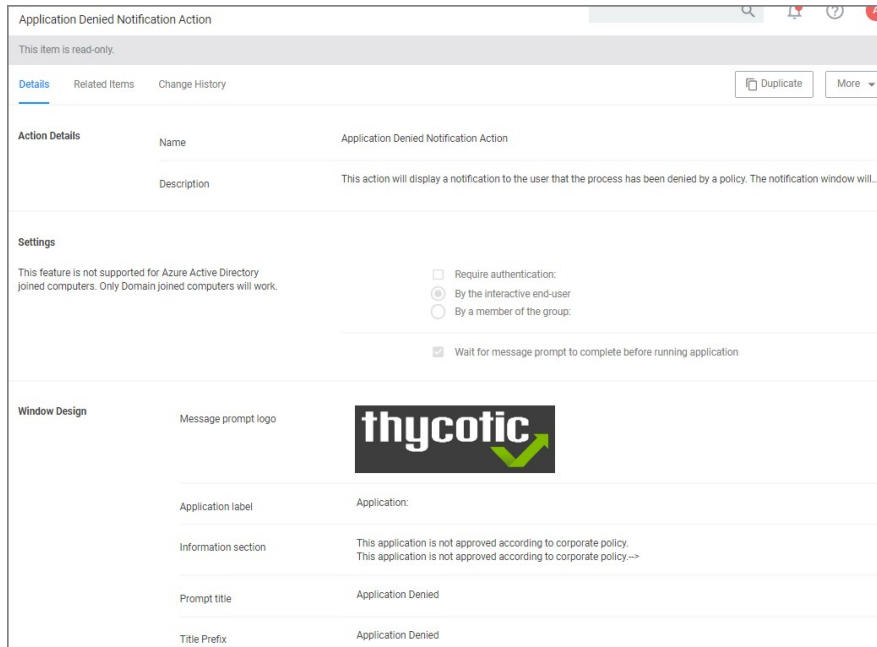


3. Click **Save Changes**.

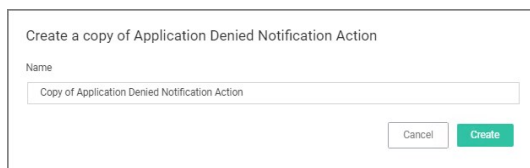
Customizing the Application Denied Notification Action

Default Actions shouldn't be edited directly, however Privilege Manager default items can be copied for customization purposes.

1. In the top Search box enter Application Denied Notification Action.
2. Click on the name of the Action **Application Denied Notification Action**.



3. Click **Duplicate**.
4. Enter a customized and meaningful name for the action. It is recommended to use standard naming conventions with your custom items. Beginning custom names with your company name is a great way to differentiate between the default items and your custom items.

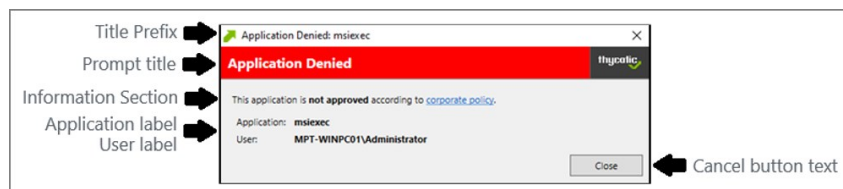


5. Click **Create**. Once you click Create, the new action page opens.
6. To upload a custom image file click **Choose File**. You can upload a custom logo, the file size should be under 128 KB and the width should be 500 pixels or less with a maximum height of 34 pixels.
The logo that is uploaded should NOT be a high-resolution image. This image will be delivered to every endpoint with every message in which it's used. The smaller the image, the better, for sending the message to the endpoints and for the endpoint to load the message.

7. Click **Save**.

Editing the Text in the UI


Privilege Manager makes it very easy to edit the text of a message. The fields are listed in alphabetical order on the item's view page. Compare each field to this overview image:



Most of the lines do not include individualized stylings per line. Editing the text in the UI will simply edit the text as required. The **Information Section** field includes html formatting for the hyperlink to the corporate policy. That hyperlink will be removed if the text is edited on the message's edit page.

Window Design

Message prompt logo



Choose File | No file chosen

Application label: Application

Information section: This application is not approved according to corporate policy
This application is not approved according to corporate policy-->

Prompt title: Application Denied

Title Prefix: Application Denied

User label: User:

Note: It is **NOT** recommended to edit the Information Section directly on the message's edit page. Instead, editing the Information Section via XML retains the html formatting for this line. If no changes are made to the Information Section, the html formatting is retained. All other fields can be changed except the Information Section and the html formatting for the Information Section is retained.

Editing the Text via XML

1. Select **More** and click **View as XML**

```

Test of Application Denied Notification Action
Test of Application Denied Notification Action
1 <CustomXamlExecutionActionContract xmlns:adc="http://schemas.orellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="
2 <adc:AttributesNoReplication System/adc:Attributes>
3 <adc:Description>This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in an
4 <adc:FolderId>f92777a-86b3-4459-b5af-1dcbee252871</adc:FolderId>
5 <adc:ItemId>ad9817fe-4224-46f9-96a9-bc4b5c8383a5</adc:ItemId>
6 <adc:Name>Test of Application Denied Notification Action</adc:Name>
7 <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
8 <adc:State i:type="adc:ItemState">
9 <adc:CreatedById>2de66e6e-5098-44ac-ad36-6a1ae8fefe7</adc:CreatedById>
10 <adc:CreatedDate>
11 <dc:DateTime>2020-07-07T00:24:06.6387625Z</dc:DateTime>
12 <dc:OffsetMinutes>-240</dc:OffsetMinutes>
13 </adc:CreatedDate>
14 <adc:EffectiveSecuredId>8117848-22d5-4e76-8989-19470b7a3a64</adc:EffectiveSecuredId>
15 <adc:EffectiveSecuredInheritedId>77c2974-8c40-4ae6-931e-fe60d87781a9</adc:EffectiveSecuredInheritedId>
16 <adc:IsCreated>true</adc:IsCreated>
17 <adc:ModifiedById>e3644cb-8d76-4e7e-8399-9288dc88b951</adc:ModifiedById>
18 <adc:ModifiedDate>
19 <dc:DateTime>2020-07-07T00:24:06.6387625Z</dc:DateTime>
20 <dc:OffsetMinutes>-240</dc:OffsetMinutes>
21 </adc:ModifiedDate>
22 <adc:VisualStateId>785143a9-13f8-5332-ad68-281ea027f96a</adc:VisualStateId>
23 </adc:State>
24 <adc:Strings />
25 <adc:Tags />
26 <AdjustSession>false</AdjustSession>
27 <CommandLine />
28 <Executable>.\ArelliaDisplayXamlAction.exe</Executable>
29 <TerminateExitCode>0</TerminateExitCode>
30 <WaitOnApplication>true</WaitOnApplication>
31 <ChildAssociations />
32 <OfflineApprovalType>OfflineNotAllowed</OfflineApprovalType>
33 <OwnsItemId />
34 <RequireLogon>false</RequireLogon>
35 <UserGroupId i:nil="true" />
36 <Xaml>:![CDATA[<div
37 xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"

```

2. Change the notification text in the XML viewer:

Line 82 has the following:

```
<Paragraph><Run>This application is </Run><Bold><Run>not approved</Run></Bold><Run> according to </Run><Hyperlink TargetName="" blank" NavigateUri="http://www.example.com/policy"><Run>corporate policy</Run></Hyperlink></Run></Paragraph>
```

Edit this space with the URL and the name of the Hyperlink you would like for your pop up Window.

```
<Paragraph><Run>This application HAS NOT BEEN APPROVED according to </Run><Hyperlink TargetName="" blank" NavigateUri="http://www.example.com/policy"><Run>corporate policy.</Run><Run><Click here, </Run><Hyperlink TargetName="" blank" NavigateUri="http://www.thycotic.com/helpdesk"><Run>to open a support ticket for review this application for approval.</Run></Hyperlink></Run></Paragraph>
```

3. Change the default timeout:

If you wish to change the default time out for how long the Deny Notification stays up (default is 6 seconds), edit Line 299:

```
<:Interaction.Triggers>
<:EventTrigger EventName="Loaded">
<adc:InvokeCommandWithDelayAction x:Name="CloseAction" Command="{BindingCloseCommand}" Delay="00:00:06" />
</:EventTrigger>
</:Interaction.Triggers>
```

To change it to 15 seconds, edit this elements delay parameter to 15:

```
<adc:InvokeCommandWithDelayAction x:Name="CloseAction" Command="{BindingCloseCommand}" Delay="00:00:15" />
```

4. Click **Import**. If you get an error, please address your changes. Errors are indicated with a red dot. Save any edits when resolving errors.

Updating the Policy with the new Action

After creating a custom notification action, the policy using the default notification needs to be updated.

1. Navigate to **Application Policies** and locate the policy that uses the notification you wish to update.
2. Go to the **Actions** section.

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy
[Actions](#)

Actions: [Deny Execute](#), [Deny Execute Message](#) Edit

Child Actions: [Add Child Actions](#)

Audit Policy Events: Record all activity detected by this policy in [Policy Events](#)

3. Click **Edit**.
4. Search for the action you just duplicated and modified.

16 Items

Application Compatibility Testing	Add
Test ActiveX Installer	Add
Test Adjust Process Rights Action	Add
Test Adjust Process Rights Action	Add
Test Application Classification Action	Add
Test Application Compatibility Fix	Add
Test Deny File Access Action	Add
Test Deny Windows Hooking Action	Add
Test Display Advanced Message Action	Add
Test Display User Message Action	Add
Test Encrypt Application Files Action	Add

2 Items

Deny Execute	Remove
Deny Execute Message	Remove

1. Click **Add** to add the action to the right pane of the dialog.
 2. Click **Remove** for the old action used previously.
5. Click **Update**.

Test Deny Application Execution Policy

Save changes? If you press cancel, all your changes will be lost.

Deployment: Not deployed (Policy is inactive)

Last Modified: May 15, 2020, 2:38:01 PM by Principal Self Well Known Group

Priority: 3

Description: Test security rating policy prevents processes from running.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
[Filters](#)

Applications Targeted: [Add Applications Targeted](#)

Inclusions: [Add Inclusions](#)

Exclusions: Present in Signed Security Catalog Edit

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy
[Actions](#)

Actions: [Test Display Advanced Message Action](#) Edit

Child Actions: [Add Child Actions](#)

Audit Policy Events: Record all activity detected by this policy in [Policy Events](#)

6. Click **Save Changes**.

Policy changes are automatically propagated to the endpoints. Note, that this might not be instantaneous based on the refresh cycle.

Action messages can be localized for user interaction on endpoints. For this to work, create a duplicate the **Approval Request Form Action** and then view and modify the XML of that duplicated item.

If you look at the xml example code below, you will see the `<axc:LocaleResourceCollection x:Key="LocaleResources">` element with one child `<axc:LocaleResourceSet>`. This child is the default language for the approval request, which is English.

To add a localization such as Spanish:

1. Copy the `<axc:LocaleResourceSet>` element block including the `</axc:LocaleResourceSet>` element.
2. Paste it underneath `</axc:LocaleResourceSet>`.
3. Add `Language="es"`, as in `<axc:LocaleResourceSet Language="es">`.
4. Modify the elements with string values to the correct translation for that language.

For a list of valid language code values, refer to https://docs.microsoft.com/en-us/openspecs/office_standards/ms-oe376/6c085406-a698-4e12-9d4d-c3b0ee3dbc4a (the more specific language is used first, such as 'es-ES' for Spanish - Spain and then the broader 'es' will be used if a specific language translation is not found, the last resort is the invariant translation).

Example for Spanish

Open this [link](#) to access, copy, or download the example xml.

This topic describes the out-of-the-box actions that are available in Privilege Manager and can be used to make your policy configuration process easy.

Actions Catalog

Here is the complete list of Actions that come with Privilege Manager out-of-the-box, according to OS and category type.

macOS

Adjust Effective Process Rights Action	Run as Root	Adjust the process rights of the application to run as the root user (MacOS)
Allow Copy Action	Allow Copy to Applications Directory	This action is used by policies that allow users to copy applications to the root Applications directory as standard users.
	Allow Package Installation	This action is used by policies that allow users to run the package installer elevated.
Display Advanced Message Action	Application Approval Request (with Offline Fallback) Message Action	Application Approval Request Message Action for Mac OS
	Application Approval Request (with ServiceNow Request Item Number) Message Action	This action will display an approval request form for ServiceNow integrations for approval before allowing application to run on macOS endpoints.
	Application Approval Request Message Action	Application Approval Request Message Action for Mac OS
	Application Denied Message Action	This action will display a modal denial notification message to the user and prevent application execution on MacOS.
	Application Justification Message Action	Application Justification Message Action for Mac OS
	Application Warning Message Action	Application Warning Message Action for Mac OS
Just in Time Group Membership Action	Just In Time Group Membership Action	This action will add a user to a specified group for a specified time.
Display User Message Action	Deny Execute Message	This action displays a message to the user informing them that an application has been denied execution
Deny Execute Action	Deny Execute	This action stops specified applications from executing
Quarantine File Action	File Quarantine	This action can be used to quarantine a file by moving it to the default agent quarantine path

Windows

Adjust Process Rights Action	Add Administrative Rights	This action adds basic administrative rights needed to install and run specified applications
	Add Administrator Rights - Unrestricted	This action adds administrative rights at a higher integrity level for specified applications. Usually you will only need to use this type of action if an application or installer needs to create a global object, such as a service, or if system changes require unrestricted administrator rights
	Remove Administrator Rights	This action removes administrative rights for specified applications
	Remove Advanced Privileges Action	This action removes advanced privileges for specified applications from the process token
Application Verifier Action	Application Compatibility Testing	This action triggers application compatibility testing while the process runs and sends the results to the server
Create Children Processes as User	De-elevate Child Processes	Ensures that all child processes are created without administrator rights. Forces all new processes created by the targeted application to be launched by a de-elevated token.
Deny Execute Action	Deny Execute	This action stops specified applications from executing
Deny File Access Action	Deny Read/Write Access to Microsoft Office Document Files	This action can be used to deny read and write access to Microsoft Office documents
	Deny Write Access to Executable Files	This action can be used to deny write access to common executable files
Deny Windows Hooking Action	Deny Windows Hooking	This action limits specified applications from interacting in malicious ways with other applications
Display Advanced (Xaml) Windows Message	Application Denied Message Action	This action will display a modal denial notification message to the user and prevent application execution on Windows
	Application Denied Notification Action	This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in and out and automatically close after a period of time
	Application Warning Message Action	Application Warning Message Action for Windows.
	Approval Request (with Offline Fallback) Form Action	This action will display an approval request form for approval before allowing application to run.
	Approval Request (with ServiceNow Request Item Number) Form Action	This action will display an approval request form for ServiceNow integrations for approval before allowing application to run.
	Approval Request Form Action	This action will display an approval request form for approval before allowing application to run

	Authenticated Justification Message Action	This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application
	Group Member Authenticated Message Action	This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member
	Justify Application Elevation Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy
	Justify Application Message Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy
	Mobile Approval Request Form Action	This action will display a approval request form for approval before allowing application to run.
Display User Message Action	Deny Execute Message	This action displays a message to the user informing them that an application has been denied execution
	Deny Files Read and Write Access Message	This action displays a message to the user informing them that an application will be restricted from certain file access
	Limit Process Rights for New Applications Message	This action displays a message to the user informing them that an application has had its rights reduced
	Quarantine Message	This action displays a message to the user informing them that an application has been quarantined
	Remove Rights Message	This action displays a message to the user informing them of an associated action
	SWV Global Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV global layer
	SWV Isolation Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV isolation layer
	Windows Hooking Message	This action displays a message to the user informing them that an application will be stopped from interacting with other applications
Encrypt Application Files	Encrypt Common Application Documents	This action can be used to automatically encrypt common application documents using Windows EFS.
	Encrypt Microsoft Office Documents	This action can be used to automatically encrypt Microsoft Office documents using Windows EFS.
Execute Application Action	Immediate File Inventory	This action will inventory the file being executed
GenericDetourAction	Enable UAC Virtualization	This action will turn on UAC virtualization for the target process.
Meter Application Action	Meter Application Usage	This action meters the usage of the specified applications
Quarantine File Action	File Quarantine	This action can be used to quarantine a file by moving it to the default agent quarantine path
Restrict File Dialogs	Restrict File Dialogs	This action prevents users from abusing the elevated rights of the application via the file open and save dialogs. This is a recommended action that customers should add to their elevation policies.
Set Environment Variable Action	Suppress User Account Control Consent Dialog	This action will prevent the UAC consent dialog from being displayed.
Set Process Security Descriptor Action	Locked down Service Process Security Descriptor	This action applies a restrictive security descriptor disallowing Administrators the right to terminate the process.
Apply SVS Layer Action	Workspace Virtualization Global Layer	This action places specified applications in a common Workspace Virtualization global layer
	Workspace Virtualization Isolation Layer	This action places specified applications in a common Workspace Virtualization isolation layer

Configuration Feeds are extensions to Privilege Manager. They can be found by navigating to **Admin | More** and then selecting the **Config Feed** link. Configuration feeds allow Thycotic to deliver new components/items to Privilege Manager. Simply click through the options in the Config Feeds page starting with the Select Items button and download anything that might be useful in your environment. Once the item is downloaded, it is immediately available in your Privilege Manager instance.

The main product areas covered are:

- Application Control Solution
- Local Security Solution
- Thycotic Management Server Core

Application Control Solution	Ignoring macOS Updates	Contains the policy to ignore macOS Catalina in the Software Update preference pane.
	Reset ignored macOS Software Updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane.
	Secondary File Hash Exclusion Policy	Policy template to exclude non-executable files from the hash process.
	UNC Allow Policy Template	Contains the UNC Share Allow Policy Template to scan a network share and automatically allow files in MSI, ISO, ZIP files.
	UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files.
	Visual Studio Installer Elevation	This configuration feed imports example filters and a policy for elevating Visual Studio Installers. After the installation the policy needs to be activated. Note: For enhanced security, the policy should include a certificate filter when rolled out into a production environment.
Local Security Solution	Disclose Password HelpDesk Tab	Adds the helpdesk tab to the Security Manager console.
Thycotic Management Server Core	Maintenance Resources	Contains maintenance gauges, tasks, etc. for optimal TMS performance.
	Reset Agent Service Permissions	Contains a policy to restore the security descriptor on Thycotic Services for Privilege Manager versions prior to 10.7.1.
	SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.
	Privileged Behavior Analytics Integration	Contains tasks for sending data to Privileged Behavior Analytics (PBA) - requires a SysLog Foreign System to be configured.

The Thycotic Application Control Agent collects the file hash of a new process and also the hashes of the child processes it runs. Sometimes non-executable file types cause execution issues during the hashing process. Via the downloadable Configuration Feeds, Thycotic offers a policy template that provides the ability to exclude certain file extensions from the hash process.

If non-executable files like xlsx, xls, mdb, and accdb for example cause execution issues, download the **Secondary Hash Exclusions** policy template. By default .mdb and .accdb are excluded from the file hashing procedure in Privilege Manager. To not overwrite default behavior, make them a part of your exclude list at all times.

Always manually test a new policy deployment on a single endpoint, and only push the solution to all desired endpoints after a successful verification on the test environment.

Note: This feature requires a Thycotic Control Agent version of 10.5 or greater.

Create File Exclusion through Config Feed

1. Navigate to **Admin | Config Feeds** link.
2. Next to **Privilege Manager Configuration Feeds** click **Select Items**.
3. Next to **Application Control Solution** click **Select Items**.
4. Locate the **Application Control - Secondary Hash Exclusions** and click **Download**.

Name	Description	Last Updated	Downloaded	
Application Control - Ignore macOS Catalina software update	Contains the policy to ignore macOS Catalina in the Software Update preference pane	Jul 9, 2020, 1:28:18 PM	Jul 13, 2020, 12:59:19 PM	Download
Application Control - Reset ignored macOS software updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane	Jul 9, 2020, 1:28:18 PM	Jul 13, 2020, 12:59:31 PM	Download
Application Control - Secondary Hash Exclusions	Contains the policies for the excluding specific extensions from the secondary hash calculations	Jul 9, 2020, 1:28:18 PM	Jul 13, 2020, 2:34:31 PM	Installed
Application Control - UNC Allow Policy Template	Contains the UNC Share Allow Policy Template to scan a network share and automatically allow files in MSI, ISO, ZIP files	Jul 9, 2020, 1:28:18 PM		Download
Application Control - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files	Jul 9, 2020, 1:28:18 PM	Aug 7, 2019, 10:44:28 AM	Download

The policy template is being downloaded and installed.

5. Use **Search** and type **Secondary Hash Exclusion**.
6. From the results list select the new policy **Deploy File Hash Exclusion Setting (Windows)**.

NAME	TYPE	MODIFIED	DESCRIPTION
Deploy File Hash Exclusion Setting (Windows)	Remote Scheduled Client Command	9/8/20, 8:31 PM	Deploy Secondary File Hash exclusion list to registry.

7. Under **Job Settings | File Extensions not to Hash** you can add to the list of extensions, for example xlsx, xls. By default .mdb and .accdb extensions are already listed.

Deploy File Hash Exclusion Setting (Windows)

🔔
?
M

Details Change History
Inactive
Refresh
More

Scheduled Job Details

Name

Description

Computer Groups Targeted Add

1 (1 total endpoints)
Windows Computers

Deployment ⓘ Not deployed (Policy is inactive)

Job Settings

Command

File Extensions not to Hash ⓘ

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run.

[Default: Daily at 8:00:00 PM starting Tue Jul 31 2018 \(repeating every 2 hours for a duration of 24 hours\) ✕](#)
[Default: Upon task creation/modification ✕](#)
[Add Trigger](#)

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions Start the task only if the computer is idle

8. Click **Save Changes**.

Manually Test on Endpoint

To create manual secondary extension exceptions to file hash collection, add a registry key to the endpoint.

1. Open Registry Editor (regedit.exe) and navigate to HKLM:\Software\Policies\Arellia\AMS.
2. Create **New I String Value**
 1. Name: **SecondaryExtensionExclusions**
 2. Value: enter a comma-separated list of extensions to include, i.e. xls,xls,mdb,accdb.
3. Restart the Thycotic services on this machine.

Open a file matching an extension from your inclusion list and test if it works on this endpoint. If it works, create a Policy to push this registry key creation to all desired endpoints.

Important: This does not apply to macOS systems based on Big Sur (macOS 11.0) or later. The --ignore option is not supported on Big Sur system.

MacOS has a command-line utility that can be used to ignore specific software updates in the Software Update preference pane. To provide a way in Privilege Manager to ignore or reset ignored OS updates, the following policies are available via configuration feeds.

Name	Description	Last Updated	Downloaded	
Application Control - Ignore macOS Catalina software update	Contains the policy to ignore macOS Catalina in the Software Update preference pane	Jul 9, 2020, 1:28:18 PM		Download
Application Control - Reset ignored macOS software updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane	Jul 9, 2020, 1:28:18 PM		Download
Application Control - Secondary Hash Exclusions	Contains the policies for the excluding specific extensions from the secondary hash calculations.	Jul 9, 2020, 1:28:18 PM	Sep 13, 2019, 12:26:55 PM	Download
Application Control - UNC Allow Policy Template	Contains the UNC Share Allow Policy Template to scan a network share and automatically allow files in MSI, ISO, ZIP files	Jul 9, 2020, 1:28:18 PM		Download
Application Control - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files	Jul 9, 2020, 1:28:18 PM	Aug 7, 2019, 10:44:28 AM	Download

- The Ignore macOS Catalina Software Update (Mac OS) - The Ignore macOS Catalina Software Update (Mac OS) policy uses the Run Shell Script (Mac OS) command. By default, it is triggered to run Daily at 5:00:00 AM starting Fri Dec 20 2019, with default Targets specified as MacOS Computers.
- The Reset ignored macOS Softwares Update (Mac OS) - The Reset ignored macOS Softwares Update (Mac OS). uses the Run Shell Script (Mac OS) command. By default, it is triggered to run Daily at 5:30:00 AM starting Fri Dec 20 2019, with default Targets specified as MacOS Computers.

Configuration Feeds

1. Navigate to **Admin | Config Feeds**.
2. Click on **Select Items** for **Privilege Manager Product Configurations**.
3. Click on **Select Items** for Application Control Solution.
4. Download both configuration feeds **Ignore macOS Catalina software update** and **Reset Ignored macOS software updates**.

Enabling the Policies

Following the config feeds install, you need to enable the policy to ignore the update.

1. Navigate to your macOS Computer Group and click **Scheduled Jobs**.
2. Click on **Ignore macOS Catalina Software Update (Mac OS)**.

ENABLED	NAME	DESCRIPTION
Enabled	Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.
Enabled	Cleanup sent Privilege Manager Events (Mac OS)	Purges Agent events that have been successfully transmitted from managed endpoint...
Not Enabled	Copy of Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.
Enabled	Default File Inventory Policy (MacOS)	The purpose of this policy is to inventory software programs running on the managed ...
Not Enabled	Ignore macOS Catalina Software Update (Mac OS)	This will ignore the macOS Catalina software update and cause it to be removed from ...
Enabled	Local User Inventory Policy (MacOS)	The purpose of this policy is to inventory Local User account, groups and group memb...
Enabled	Perform Resource Discovery (Mac OS)	Schedule on which agents will check with server to determine if any local resources re...
Not Enabled	Reset ignored macOS Software Updates (Mac OS)	This will reset ignored macOS software updates and cause them to be available in the ...
Enabled	Retry errored TMS Events (Mac OS)	Scan Agent queue for any events that require retransmission.
Enabled	Update Agent Commands (Mac OS)	When this policy is triggered the Agent will update agent command items.
Enabled	Update Provisioned Resource Client Items (MacOS)	

3. Set the **Inactive** switch to **Active**.
4. Click **Save Changes**.

Resetting the Policy

1. To reset the changes, set the ignore updates policy to inactive and save the changes.
2. Navigate to the **Reset ignored macOS Software Updates (Mac OS)** policy.
3. Set the **Inactive** switch to **Active**.
4. Click **Save Changes**.

Scheduling

You can edit when the policy runs by scrolling down to the Job Schedule and Job Conditions section on the policy page.

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy to be run.

Default: Daily at 5:00:00 AM starting Fri Dec 20 2019 ×
[Add Trigger](#)

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions Start the task only if the computer is idle

Power Conditions Start the task only if the computer is on AC power
 Stop if the computer switches to battery power

Advanced Conditions Allow task to be run on demand
 Run task as soon as possible after a scheduled start is missed
 If the task fails, attempt to restart
 Stop the task, if it runs for longer than

If the task is already running, then the following rule applies:

Note: Once the policies are enabled they do not run immediately. If you would like the policies to run right way you will need to click on the information icon next to Deployment and select the **Resource and Collection Targeting Update** task.

The Configuration area in Privilege Manager allows users with Privilege Manager Administrator roles to setup new or change existing configurations for areas like user credentials, foreign systems integrations, or authentication. It lets administrators specify settings that control Privilege Manager Server and Console behavior via the Advanced tab.

The Change History tab under Configuration provides users an overview of changes made to configuration items.

When clicking the ? to the top right, the Configuration page gives the user an overview of the Key Configuration settings and System Health.

The configuration page is tabulated and offers configuration or review options under the following tabs:

- [General](#)
- [Discovery](#)
- [Reputation](#)
- [Credentials](#)
- [Foreign Systems](#)
- [Roles](#)
- [Advanced](#)
- [Authentication](#)
- [Change History](#)

Advanced Tab

The Advanced tab lets you configure settings:

- File Inventory Solution such as
 - [Collectors](#)
- [Privilege Manager Application Programming Interface](#)
- Privilege Manager Server
 - [Monitor](#)
 - [General](#)
 - [ServiceBus](#)
 - [Proxy](#)
- [Privilege Manager Solution](#)
- [Thycotic Mobile Console Solution](#)






To edit any of the advanced settings, make changes and then click **Save Changes**.

File Inventory Solution

Under the File Inventory Solution the file extensions used for inclusions and exclusions are specified.

- ISO contents filters with default extensions of .exe, .cat, and .zip.
- MSI contents filters with default extensions of .exe and .cat.
- Package contents filters with default extensions of .exe, .iso, .msi, .cat, .vhd, .vmdk, and .zip.
- VHD contents filters with default extensions of .exe, .cat, and .zip.
- ZIP contents filters with default extensions of .exe, .cat, .msi, and .zip.

When you click Edit at the bottom of the page, you can change any of the listed file extensions.

File Inventory Solution	
Collectors	
Package contents filter 	<input type="text" value="*.exe;*.iso;*.msi;*.cat;*.vhd;*.vmdk;*.zip"/>
ISO contents filter 	<input type="text" value="*.exe;*.cat;*.zip"/>
Zip contents filter 	<input type="text" value="*.exe;*.cat;*.msi;*.zip"/>
MSI contents filter 	<input type="text" value="*.exe;*.cat"/>
VHD contents filter 	<input type="text" value="*.exe;*.cat;*.zip"/>

Monitor Settings

Under the Privilege Manager Server category, the second section is Monitor settings. The Monitor setting is designed to monitor the Worker Role to ensure it is healthy and active. When enabled, the process checks the health at each Ping Interval and waits until the Timeout value before considering it unhealthy.

Privilege Manager Server	
Monitor	Monitor Worker Role * <input type="checkbox"/> Yes
Ping interval <input type="checkbox"/>	<input type="text" value="15"/> seconds
Base local address <input type="checkbox"/>	<input type="text" value="https://localhost/"/>
Timeout <input type="checkbox"/>	<input type="text" value="32"/> seconds

Monitor Worker Role

When this setting is enabled the health of the monitor process will be polled.

Ping Interval

Specifies how often the server will attempt to contact the Monitor process to query its health. The default is set to 15 Seconds.

Base Local Address

This setting specifies the base URL of the Monitor process.

Timeout

Specifies how long the server process will wait to hear back from a ping request to the Monitor process. The default is set to 30 Seconds.

Privilege Manager Application Programming Interface

Enabling this setting will allow authorized calls to the public facing application programming interface.

1. Set the switch to Yes to enable the API.

Privilege Manager Application Programming Interface	
General	Enable API * ⓘ <input checked="" type="checkbox"/> Yes

You will need to create an [API Client User](#) and assign a role to this user.

General System Settings

Under the Privilege Manager Server category, the first section is General settings.

General	Save performance counters *	<input type="checkbox"/> No
	Load on Demand Flags	<input type="text" value="31"/>
	Session Timeout	<input type="text" value="720"/> minutes
	Allow Agent Certificate Mismatch *	<input type="checkbox"/> No
	Maximum Application Event Count *	<input type="text" value="1000000"/>
	Prevent Legacy Agent Registration (10.4 and older) *	<input type="checkbox"/> No
	Max time skew	<input type="text" value="5"/> minutes
	Inactivity Timeout	<input type="text" value="360"/> minutes
	Encryption provider *	<input type="text" value=""/>
	Command Timeout	<input type="text" value="180"/> seconds
	System Secret Vault	Configure
	Validate agent event signatures *	<input checked="" type="checkbox"/> Yes

Save Performance Counters

If this setting is selected, the performance counter data will be recorded in the database. Also refer to [Delete Old Performance Counter Events](#).

Load On Demand Flags

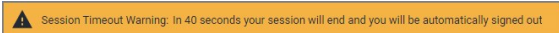
The value is a flag set specifying what item values are allowed to be on-demand loaded. 0 none, 1 strings, 2 tags, 4 security, 8 associations, 16 data class states, 31 all.

Session Timeout

This setting specifies the maximum time in **minutes** for a login session to be active without having to negotiate another token. The default is set to 720 Minutes (12 Hours).

Session Timeout Warning

Two minutes before the set session timeout window expires, Privilege Manager displays a yellow warning with countdown timer to inform users about the pending session timeout.



Allow Agent Certificate Mismatch

This is a checkbox that when selected allows agents to communicate with the server even if there is a certificate mismatch.

Maximum Application Event Count

This settings specifies the Maximum number of application action events that will be kept in the database. The default setting is 1,000,000. Also refer to [Purge Maintenance - Application Control Events](#).

Prevent Legacy Agent Registration (10.4 and older)

Enabling this setting prevents older agents (prior to 10.5) from registering, allowing only agents with valid agent Install Codes. Only enable this option if you are certain your managed computers have all been upgraded to 10.5 or newer agents.

Max Time Skew

This setting specifies the maximum time difference (in minutes) to allow client system clocks to be out of sync with the server.

Inactivity Timeout

This settings specifies the maximum allowed time for inactivity when logged into the Privilege Manager console. The default is set to 30 Minutes. The session token remains active and does not need to be renegotiated when the inactivity timeout happens within the specified session timeout window.

Encryption Provider

This setting specified the Encryption Provider used to encrypt sensitive data.

Command Timeout

This settings specifies the SQL command timeout. The default is 180 Seconds.

System Secret Vault

This link lets you configure the foreign system used to store secrets.

Password Complexity for Standard Users

This setting is set to yes by default, meaning the password complexity rules are enforced when creating or editing a Privilege Manager user resource.

Refer to [Password Complexity Enforcement](#) for further details.

Validate Agent Event Signatures

Enabling this setting will verify the signature contained within agent events that are sent to the server. Any events with invalid signatures are discarded.

ServiceBus Settings

Under the Privilege Manager Server category, the fourth section is ServiceBus settings.

ServiceBus	Connectivity Mode * ⓘ	HTTPS
------------	-----------------------	-------

Connectivity Mode

This setting specifies the connectivity mode for Service Bus. The default is HTTPS, which is also recommended.

Proxy Settings

Under the Privilege Manager Server category, the third section is Proxy settings.

Proxy	Proxy server credential ⓘ	<input type="text"/>
	Port ⓘ	<input type="text" value="8080"/>
	Use proxy server * ⓘ	<input checked="" type="checkbox"/> Yes
	Proxy server ⓘ	<input type="text"/>

Proxy Server

This setting specifies the name or IP address of the proxy server.

Proxy Server Credential

This link lets you configure the credential used to authenticate with the proxy server.

Port

This setting specifies the port used for communications to the proxy server.

Use Proxy Server

If set, communications will be done via the proxy server specified.

Privilege Manager Solution

If selected then the acknowledge events button will be visible in Policy Events.

1. Set the switch to Yes to enable the acknowledge events button.

Privilege Manager Solution

General Show Acknowledge Events Yes

Once you save the changes, you will see an Acknowledge All button on the Policy Events grid after selecting an unacknowledged event.

New Loaded Resource 9/11/202... ×

Policy
[New Monitor Applications Run with Administrator Rights Policy](#)

Policy Description
Monitors the execution of applications that are run with Administrator Rights.

Total Events
3089

Pending Events
3089

Acknowledge All

Create Filter

View File

Authentication Tab

The Authentication tab is used for setting up the Authentication Provider used with Privilege Manager. Different authentication providers can be setup based on configured Foreign Systems. The user logs in based on the active authentication provider. Only one authentication provider can be active at any given time.

Configuration

General Discovery Reputation Credentials Foreign Systems Advanced **Authentication** Change History

Authentication

Select the authentication providers you want to use.

Azure Active Directory Domain	<input type="checkbox"/>
Azure Active Directory Domain 2	<input checked="" type="checkbox"/>
Azure Active Directory Domain 3	<input type="checkbox"/>
Azure Active Directory Domain 4	<input type="checkbox"/>

Note: If you are trying to change your Authentication Provider specifically to NTLM, Privilege Manager runs a verification to make sure the local built-in Administrators Group is in the Privilege Manager Administrators Role.

Credentials Tab

The Credentials tab lets you configure and add new credentials required for configured Foreign Systems.

The screenshot shows the 'Credentials' tab within a configuration window. At the top, there are navigation tabs: General, Discovery, Reputation, **Credentials**, Foreign Systems, Advanced, Authentication, and Change History. Below the tabs, there is a search bar with '7 Items' and a 'Create' button. A table lists existing credentials with columns for NAME, DESCRIPTION, LAST MODIFIED BY, and LAST MODIFIED ON.

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED ON
Azure Service Bus Credential	Service Bus credential for Mobile app integration.	Administrator	4/16/20, 9:25 AM
Default Proxy Server User Credential	Proxy Server User Credential	Trusted Installer	7/6/20, 11:27 PM
Default User Credential	Default User Credential	Trusted Installer	7/6/20, 11:27 PM
New User Credential	New User Credential	Administrator	4/16/20, 9:12 AM
PM-Test Admin	test admin account	Administrator	8/22/19, 10:21 AM
	New User Credential	Administrator	10/24/19, 7:45 PM
SCCM Account	New User Credential	Administrator	11/5/19, 5:45 AM

1. Navigate to **Admin | Configuration** and select the **Credentials** tab.
2. Click **Create** to add a new credential.

The screenshot shows the 'New User Credential' configuration form. It has two main sections: 'Details' and 'Settings'. The 'Details' section contains 'Name' and 'Description' fields, both with the value 'New User Credential'. The 'Settings' section contains a 'Password' field with the value 'Account Name' and a 'Password' label. Below the password field, it says 'No password is set' with an 'Edit' link.

Details

Name: New User Credential

Description: New User Credential

Settings

Account Name: [Field]

Password: No password is set [Edit](#)

User Credentials and Roles

As described for the Roles Tab, Privilege Manager comes with a set of default user roles. Those roles can be edited or new ones can be added to the system.

The role for the Privilege Manager Administrator gives permissions to manage all aspects of the Privilege Manager implementation. As a best practice, it is recommended to set-up roles that limit administrative access to tasks directly related with a users job role.

For integrations with Secret Server keep in mind that Privilege Manger has the ability to use Secret Server as its storage container for credentials. This includes credentials for connecting to integrated systems such as Service Now, as well as credentials for local accounts that are managed by Local Security in Privilege Manager. Customers can choose to integrate with Secret Server only (no Vault setup) or Secret Server and Vault. Either option requires Authentication Data setup for Foreign Systems in Privilege Manager. Refer to the [Setting up Integration between Privilege Manager and Secret Server](#) topic.

If you are integrating with Active Directory synchronization please refer to [Active Directory Synchronization](#).

Note: If you synced with Azure AD, and then added that user to the Privilege Manager Administrators Role, that Azure AD user has admin rights only, if Azure AD is used as the auth provider. If users login via Thycotic One, use **Admin I Users** to create a new user and then add that new user to the Privilege Manager Administrators Role, refer to [How to Add Thycotic One Users Manually](#).

Create User during Installation

During the installation process the Create User page is where you enter information for the initial Privilege Manager Administrator user. Please remember these credentials as they are necessary to login to the web application after you complete the installation.

Discovery Tab

This tab is for resource discovery. After a resource is initially discovered by the server, the name is set to **New Loaded Resource...** After discovery runs the names of those resources are updated.

Resource Discoverers are selectable under the **Advanced** section. Resource Discoverers are categorized by Agent and Server Discoverers. Most are selected by default and can be disabled via switch.

The screenshot shows the Configuration page with the Discovery tab selected. The page title is "Configuration" and the navigation tabs are General, Discovery, Reputation, Credentials, Foreign Systems, Advanced, Authentication, and Change History. The Discovery tab is active. Below the navigation, there is a "Resource Discovery" section. It contains a paragraph: "After a resource is initially discovered by the server, the name is set to 'New Loaded Resource...'. After the following discovery has run the names of those resources will be updated." To the right of this paragraph are two links: "Review Server Resource Discovery Schedule" and "Review Endpoint Resource Discovery Schedule". Below these links is a toggle switch for "Default File Inventory Policy (Windows)" which is currently turned on. A "Hide Advanced" link is visible on the right side of this section. Below the "Resource Discovery" section is a section titled "Enable or Disable Resource Discoverers". This section is divided into two categories: "Agent Discoverers" and "Server Discoverers". Under "Agent Discoverers", there are ten items, each with a toggle switch that is currently turned on: App Bundle Agent Discoverer, COM Component Agent Discoverer, COM Application Agent Discoverer, DCOM Agent Discoverer, File Agent Discoverer, File Agent Discoverer (File Location), File Agent Discoverer (Services), File Discoverer from ACS Events, File Discoverer from Approval Events, and Security Descriptor Agent Discoverer. Under "Server Discoverers", there are five items, each with a toggle switch that is currently turned on: Digital Certificate Server Resource Discoverer, Domain User Group Server Resource Discoverer, File Digital Signature Resource Discoverer, Security Descriptor Server Resource Discoverer, and User Server Resource Discoverer.

Refer to [Best Practices](#) in the Policy Events section for further details.

Foreign Systems

Foreign Systems in Privilege Manager are any systems for which a connections or an integration has to be set-up, providing a system URL (network address) and authentication information. Foreign Systems can be Thycotic or third-party products and their basic integration set-up in Privilege Manager is alike.

Foreign Systems Tab

Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD.

In order to use Secret Server as the password vault please review [Setting up Integration between Privilege Manager and Secret Server](#)

Configuration	
General	Discovery
Reputation	Credentials
Foreign Systems	Advanced
Authentication	Change History
Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD.	
11 Items	
NAME	COUNT
Active Directory Domains	2
Azure Active Directory Domains	1
Azure Service Bus	2
Privilege Manager Server	1
Secret Server	1
ServiceNow	1
SMTP Server	1
Symantec Management Platform	1
SysLog	8
System Center Configuration Manager	0
Thycotic One	1

Integrations

Thycotic Foreign Systems

- [Integration between Privilege Manager and Secret Server](#)
- [Integration between Privilege Manager and Privileged Behavior Analytics](#)

AD Integration

- [Setting Up Azure Active Directory Integration in Privilege Manager](#)

Third-Party Foreign Systems Integration

- [Set-up an SMTP Server Connection](#)
- [Set-up a Cyance Connection](#)
- [Set-up a ServiceNow Ticketing Connection](#)
- [Set-up VirusTotal](#)
- [Set-up an SCCM Connection](#)
- [Set-up Syslog](#)

Thycotic Products Integrations

The following topics on integrating Privilege Manager with other Thycotic products are available:

- [Integration between Privilege Manager and Secret Server](#)
- [Integration between Privilege Manager and Privileged Behavior Analytics](#)

Setting up Integration between Privilege Manager and Secret Server

Privilege Manager has the ability to use Secret Server as its storage container for credentials. This includes credentials for connecting to integrated systems such as Service Now, as well as credentials for local accounts that are managed by Local Security in Privilege Manager. Customers can choose to integrate with Secret Server only (no Vault setup) or Secret Server and Vault. Either option requires Authentication Data setup for Foreign Systems in Privilege Manager.

The Secret Server Vault integration for 10.7.1 and newer does not require Secret Server to be setup as the authentication provider. Any supported authentication provider can be used, independent from using Secret Server as a Password Vault.

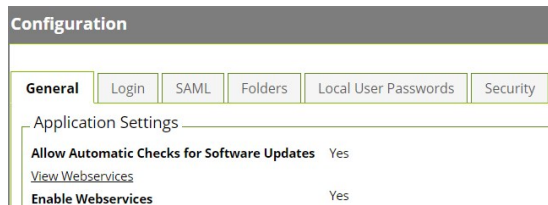
In Secret Server, Privilege Manager credentials are stored as Secrets, and Privilege Manager uses the Secret Server REST API to communicate with Secret Server.

For this the proper license types need to be set-up, as Secret Server Express (free) does not support the integration with Privilege Manager.

Verify Web Services are Enabled in Secret Server

As a prerequisite, you need to make sure that your Secret Server instance has Web Services Enabled.

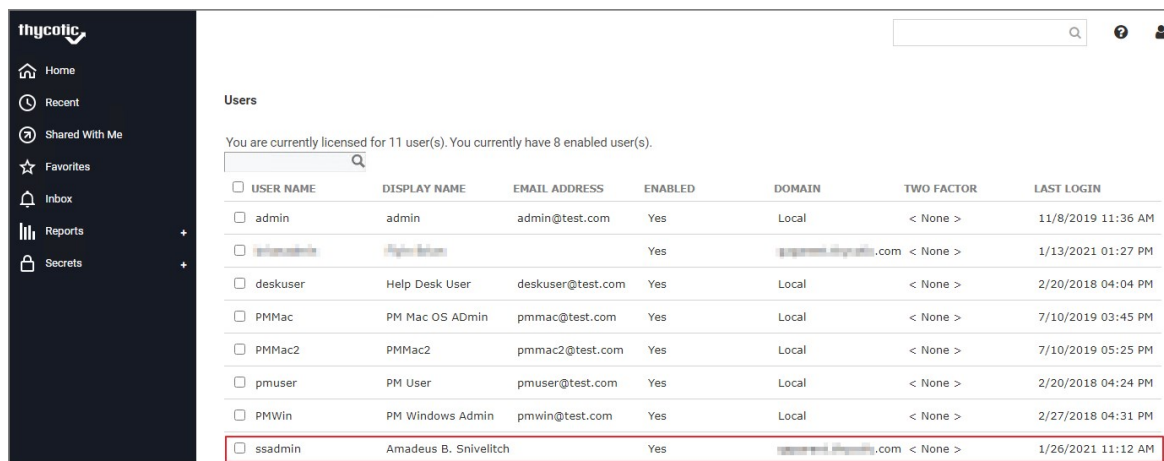
1. Navigate to **Admin | Configuration | Application Settings**.
2. Verify that under View Webservices the **Enable Webservices** option is reflecting **Yes**.



3. Navigate to **Admin | Users** and verify you have a user configured to be used for the credential setup in Privilege Manager. This can be a regular Secret Server user or a Secret Server Application account.

Note: The account needs to have a role with ALL of the following Secret Server permissions.

Add Secret
Administer Configuration
Administer Folders
Administer Licenses
Assign Secret Policy
Create Root Folders
Delete Secret
Edit Secret
Own Secret
View Secret



4. In your Privilege Manager instance, enter the credentials for that user at **Admin | Configuration | Credentials**. Create/Edit the default Secret Server credential account to specify which account will be used by Privilege Manager to connect to Secret Server. Depending on your setup, this can be the "Default User Credential" in Privilege Manager.

Setup Authentication Data in Privilege Manager

1. Navigate to **Admin | Configuration**.
2. Click the **Foreign Systems** tab.

3. Select **Secret Server** from the list.
4. In the Name column click on **Default Secret Server**.

5. Under Settings, update the following:
 1. **Credential**: This is a Secret Server user (preferably an application account). Refer to required permissions above.
 2. **Secret Server Url**: This is the url that end users use to access Secret Server. **HTTPS** is required. Also the validation on this field will reach out to Secret Server using the url provided. If it can't be reached, or if the Secret Server version is lower than 10.6, there will be a 404 not found validation error. The URL needs to be fully qualified ending with a */*.
 3. **TMS Url**: This is the url to access TMS itself. It is the url that end users use to access Privilege Manager, minus the PrivilegeManager/ part at the end of the path. This URL also needs to be well formed and fully qualified ending with a */*.
6. Click **Save**.
7. Scroll down to **Integration Features | Authentication** and enable Secret Server as the authentication provider by clicking the **Setup Secret Server Integrated Authentication** link.
8. Set the switch for Secret Server to enabled.

9. Click **Save Changes**.

After these steps the Secret Server Foreign System is ready for use. If you need to enable or disable features for this integration, the Integration Feature list is below the Settings area on the page. Follow any of the links to turn features on and off.

Configure Privilege Manager Credential Vault (optional)

1. Scroll down to **Integration Features | Secret Server Vault** and setup Secret Server as the vault by clicking the **Secret Server Vault** link.
2. Set the switch for the Vault to enabled.

On the Password Vault Settings configuration page:

1. Set the switch **Use Secret Server** in order to use Secret Server's vault to store credentials.
2. Enter the username and password for the account that will be used to access Secret Server.

Note: These are the same credentials that will be stored as the Secret Server Default Credential (located at the **Admin | Configuration | Credentials** tab). If a user already has been entered here, the same account will be auto populated into the configuration page.

3. Back on the **Password Vault Settings** configuration page click **Save Changes**.

Password Migration

After the vault and authentication set-up, all passwords are migrated from Privilege Manager to Secret Server. This migration process may take time.

Important Notes

The migration will create a root folder in Secret Server named Privilege Manager Secrets. Do NOT delete this folder. The folder, by default only has the sync account user as an owner, with no other permissions. The permissions on this folder can be modified to allow helpdesk users or administrators access to the Secrets. Do NOT remove the sync account user's permissions from the folder.

If desired the folder can be moved or renamed within Secret Server.

Templates

There are two Templates that Privilege Manager uses to store Secrets in Secret Server. These templates must exist with the proper fields and be marked as active.

- **Password (Template Id: 2)**: The following fields need to exist on the template:
 - Username
 - Password

Do NOT mark any other fields in that template as required!

- **Windows Account (Template Id: 6003)**: The following fields need to exist on the template:
 - Machine
 - Username
 - Password

Do NOT mark any other fields in that template as required!

Note: To troubleshoot or remove the integrated configuration, navigate to the **Admin | Configuration | Advanced** tab in Privilege Manager. Locate the **System Secret Vault** setting and click the **Select Resource** link. Here, a user can manually add and remove the Secret Server vault. If you choose to remove the Secret Server vault, a migration of passwords from Secret Server's vault to Privilege Manager automatically happens.

- Verify that your Protocol, Host, and Port match your SysLog server details (SysLog URL and SysLog Port from the PBA System Settings details).

The screenshot shows the configuration page for a PBA SysLog Server. It has a 'Details' tab selected and 'Change History' link. There are 'Refresh' and 'More' buttons. The 'Foreign System Details' section includes a 'Name' field with 'PBA SysLog Server' and a 'Description' field with 'New SysLog Server'. The 'Settings' section includes a 'Protocol' dropdown set to 'TCP + TLS', a 'Host' field with a long URL, and a 'Port' field with '5140'. A 'Show Advanced' link is at the bottom right.

Using the PBA Send Tasks

- Navigate to **Admin | Tasks** and from the folder tree select **Server Tasks | Foreign Systems**.
- Click **PBA - SysLog**

The screenshot shows the 'Tasks' page with the 'Automation' tab. A search bar contains 'Find Folder'. The folder tree on the left is expanded to 'Foreign Systems > PBA - SysLog'. The main area shows a list of 5 items: 'Send AD Group Data to PBA', 'Send Endpoint Data to PBA', 'Send File Data to PBA', 'Send Policy Data to PBA', and 'Send User Data to PBA'. There are 'Create' and 'Export' buttons at the top right of the list.

- For Privilege Manager to send data based on any of these task, the PBA SysLog server you created as a Foreign System above, needs to be added as the SysLog System ID. This can either be done

- o **On Demand** when running the task:

- Select a PBA Data Send tasks and click **Run**.
- Specify the SysLog System ID.

The screenshot shows a 'Run Task' dialog box. It has a 'Task Name' field with 'Interactive run on Tue Aug 11 2020'. The 'Data source' dropdown is set to 'PBA Policy Metadata'. There is a 'Replace Spaces with underscore' checkbox which is unchecked. The 'SysLog System ID' dropdown is set to 'PBA SysLog Server'. There are 'Cancel' and 'Run Task' buttons at the bottom.

- Click **Run Task**

- o **By setting up a schedule:**

- Select a PBA Data Send tasks and click **View**.
- Under **Parameters** specify the SysLog System ID.
- Define a **Schedule**, by clicking **New Schedule**

4. Click **Save Changes**.

Repeat for each of the data sets you want to use in PBA.

Enable Send Application Events to PBA

The config feeds installation also add a remote scheduled client command for PBA to Privilege Manager. The **Send Application Events to PBA** policy is by default disabled.

1. Under your computer Group navigate to **Scheduled Jobs**.
2. On the **Scheduled Jobs** page search for PBA and select **Send Application Events to PBA**

Send Application Events to PBA
Inactive Refresh More

Scheduled Job Details

Name: Send Application Events to PBA

Description: Send Application Events to PBA

Computer Groups Targeted: 1 (1 total endpoints)
Windows Computers Add

Deployment: Not deployed (Policy is inactive)

Job Settings

Command: Send Application Events to PBA

PBA API Endpoint *

PBA API Key *

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run.

Default: Daily at 12:00:00 AM starting Fri Oct 25 2019 (repeating every 15 minutes for a duration of 24 hours) Add Trigger

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions Start the task only if the computer is idle

Power Conditions Start the task only if the computer is on AC power
 Stop if the computer switches to battery power

Advanced Conditions Allow task to be run on demand
 Run task as soon as possible after a scheduled start is missed
 If the task fails, attempt to restart
 Stop the task if it runs for longer than
 If the task is already running, then the following rule applies: Default (Do not start a new instance)

- o Under Job Settings enter the PBA **Event Post URL** and **X-API-Key** details from the PBA system settings information.
- o Modify the Job Schedule if customization is required.
- o Customize any of the Job Conditions to better fit your implementation.

3. Click **Save Changes**.

4. Set the **Inactive** switch to **Active**.

5. Next to Deployment click the **i** icon and select the **Resource and Collection Targeting Update** task to run.

Active Directory Integration

By adding an Active Directory Domain the system can synchronize users, groups, and computers. Once configured a directory synchronization task will need to be started to actually import AD information. Default User Credentials need to be created as well for the system to be able to connect.

The following topics are available in the Active Directory (AD) integration section:

- [Setting Up Local Active Directory Synchronization](#)
- [Setting Up Azure Active Directory Integration in Privilege Manager - 10.6 and up](#)

Active Directory Synchronization

The following procedures show the steps necessary to set-up Active Directory synchronization in Privilege Manager.

If you already configured the AD Default User Credential skip to the Foreign Systems set-up procedure.

Note: For local AD synchronization with Privilege Manager cloud the Directory Services Agent has to be installed. We recommend [installing the Directory Services Agent](#) on a system that already has the Thycotic Agent (Core Agent) installed; however you may also use a domain connected system and newly install both the Core and Directory Services Agent by using the [bundled installer](#).

Set-up AD Default User Credential

1. Select **Admin | Configuration**.
2. Select the **Credentials** tab.
3. Edit the **Default User Credential** or use **Create** to add a new user. Set a domain credential with an Account Name and Password that has can read from the Active Directory domain(s).

4. Click **Save Changes** and continue with step 2 in the Foreign Systems set-up procedure.

Setup Foreign Systems

1. Select **Admin | Configuration**.
2. Select the **Foreign Systems** tab.
3. Select Active Directory Domains.

NAME	COUNT
Active Directory Domains	1
Azure Active Directory Domains	0

4. On the Active Directory Domains page, select **Create**.
5. Enter a fully qualified domain name and a friendly name.

6. Under the required Credential click **Select...**

Select Resource

Name	Description	Last Modified By	Last Modified
Azure Service Bus Credential	Service Bus credential for Mobile app integration.	Administrator	Thu Apr 16 2020 09:25:28 GMT-0400 (Eastern Daylight Time)
Default Proxy Server User Credential	Proxy Server User Credential	Trusted Installer	Tue Jul 07 2020 15:38:33 GMT-0400 (Eastern Daylight Time)
Default User Credential	Default User Credential	Trusted Installer	Tue Jul 07 2020 15:38:33 GMT-0400 (Eastern Daylight Time)
New User Credential	New User Credential	Administrator	Thu Apr 16 2020 09:12:33 GMT-0400 (Eastern Daylight Time)
New User Credential	New User Credential	Administrator	Tue Jul 07 2020 09:10:10 GMT-0400 (Eastern Daylight Time)
PM -Test Admin	test admin account		Thu Aug 22 2019 10:21:08 GMT-0400 (Eastern Daylight Time)
qa parent	New User Credential	Administrator	Thu Oct 24 2019 19:45:36 GMT-0400 (Eastern Daylight Time)
SCCM Account	New User Credential	Administrator	Tue Nov 05 2019 05:45:08 GMT-0500 (Eastern Standard Time)

10 items per page 1 - 8 of 8 Items

Cancel

7. From the Resources page select a credential.

New

Fully Qualified Domain Name *

Friendly Name *

Credential *

[Default User Credential](#)

Cancel Create

8. Click **Create**.

New Active Directory Domain

General Synchronization Change History Refresh More

Active Directory Details

Once Active Directory is configured a Directory Synchronization task will need to run to import the appropriate data. These tasks can be scheduled and synchronization can be coordinated through one or multiple tasks as needed by each specific environment. As an example, one task may synchronize users once a week, another task could synchronize computers daily, and perhaps a third could synchronize a specific LDAP query for specific Organizational Units (OUs) from Active Directory.
[Read more about configuring Active Directory](#)

Name

Description

Settings

The credential used to access Active Directory needs read access to the Active Directory (does not need Domain Administrator access)

Credential

Fully Qualified Name

Use LDAPS No

9. Verify the **URL** (Fully Qualified Name) is correct.

10. If the domain uses LDAPS, set the switch to enable.

11. Click **Save Changes**.

12. Once Active Directory is configured a Directory Synchronization task needs to run to import the appropriate data. Select the **Synchronization** tab.

13. Select the task(s) you want to perform:

1. Import:

- Users
- Groups
- Computers
- Custom LDAP Query

2. Connectivity, via either

- **Privilege Manager server** that can reach a domain controller on your network:

1. Synchronization Task Config:

- Schedule - Schedules help keeping your system in sync with your domain updates.
- Domain Partner (optional)

2. Click **Save Changes**.

3. Click **Run**, to manually run the task on demand.

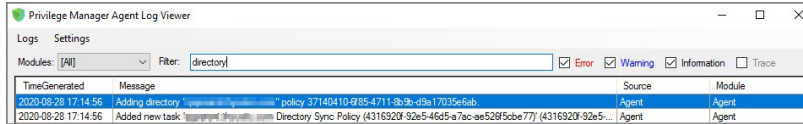
- **Directory Services Agent** that is installed on one of your domain connected on-premises computers designated to perform the sync. Cloud hosted customers likely need to choose this option.

1. Under **Agent Policy Config**:

- Schedule: Schedules help keeping your system in sync with your domain updates.
- Agent Computer: Select the computer that has the Thycotic Core and Directory Services Agents installed.
- Domain Partner (optional)

2. Click **Save Changes**.

By setting this up via Directory Services Agent, the directory policy and the Directory Sync Policy task are applied to the agent, which based on the task schedule kicks off the local active directory synchronization. You can verify this by checking your Agent logs.

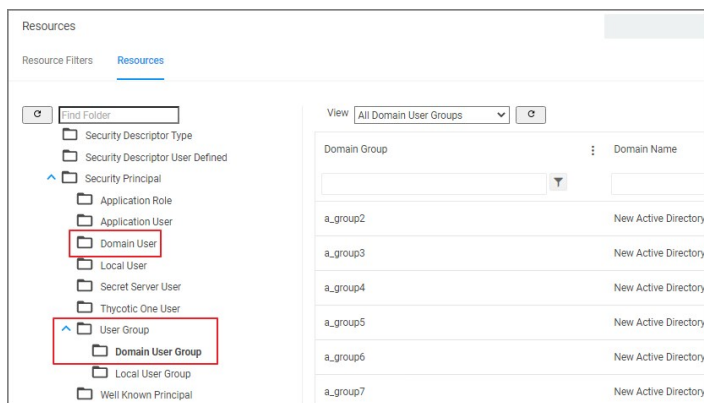


Tasks can be scheduled and synchronization can be coordinated through one or multiple tasks as needed by each specific environment. As an example, one task may synchronize users once a week, another task could synchronize computers daily, and perhaps a third could synchronize a specific LDAP query for a specific group from Active Directory.

Viewing Imported Users and Groups

You may verify and browse the users and groups that are expected to be imported from Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.
 1. Select **Domain User**. You should see a list that contains imported Active Directory users.
 2. Select **User Group**. You should see a list that contains imported Active Directory groups (other groups may exist in the list as well).



Setting Up Azure Active Directory Integration In Privilege Manager

Setting up Azure AD integration with Privilege Manager requires steps in your Azure tenant and in Privilege Manager.

In Privilege Manager the Azure Active Directory Domain Foreign System requires the following from the Azure Portal:

- Tenant (this is the unique identifier of the Azure Active Directory instance)
- Application ID (an application registration in the directory instance)
- Client Secret (this is found in Certificates & Secrets in the Azure portal for the previously created application registration)

Setting up Azure AD Integration in Privilege Manager requires these components independent of On-premises or Cloud:

- User Credential
- An Azure Active Directory Domain Foreign System
- Executing a Privilege Manager Task (Import Users and Groups)
- Creating a Scheduled Task to synchronize the users and groups on a regular basis

Note: You do not need to have an active directory domain before you can sync with an Azure Active Directory. However, there are benefits for synchronizing on-premises Active Directory to Azure AD.

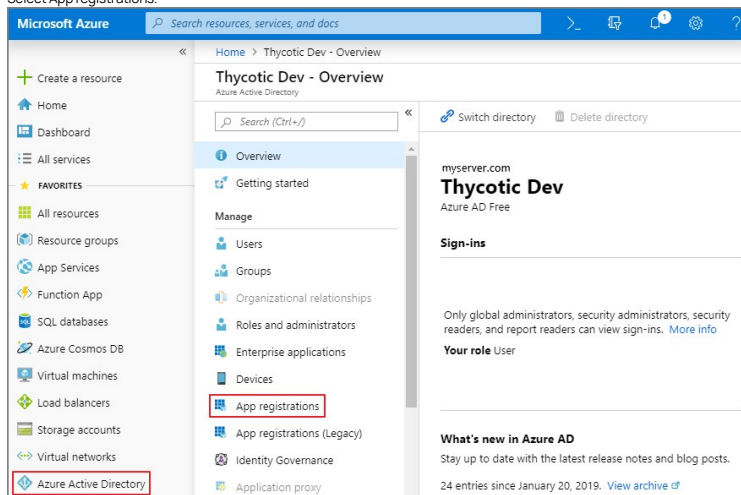
Prerequisites

Assign Azure user(s) to the **Privilege Manager Administrators** Role. In order for users to authenticate via Azure AD, they need to be members of various roles. There must be at least one member from your Azure Directory to be allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

Setting up Azure AD with Privilege Manager

Steps In the Azure Portal

1. Navigate to your <https://portal.azure.com>
2. In your Azure portal, navigate to and open Azure Active Directory.
3. Verify you are in the right tenant or use the filter to switch.
4. Select App registrations.



5. Select **+ New registration**.
6. Under Register an application, enter
 1. an application **Name**.
 2. select **Supported account types** based on your business requirements
 3. specify the following Redirect URI values using the URI of your Privilege Manager server: <https://myserver.example.com/TMS/>

Note: This URI does not need to be a publicly visible address. It is only used in redirecting the browser back to the Privilege Manager web application after authentication. For Privilege Manager Cloud subscriptions, the URI should be pointed to the URI that was set up for you, for example: <https://myassignedname.privilegemanagercloud.com/Tms/>

Home > Thycotic Dev | App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

doc-example-1 ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Thycotic Dev only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://myserver.example.com/Tms/ ✓

By proceeding, you agree to the [Microsoft Platform Policies](#) ☒

Register

1. Click the **Register** button.

7. Navigate to your newly created application registration.

8. Select the **Authentication** option.

1. Enter these additional URIs in the Redirect URI field:

- <https://myserver.example.com/Tms/Account/Signout/>
- <https://myserver.example.com/Tms/Account/SignoutCallback/>

2. In the **Implicit Grants** area, check the box labeled **ID tokens**.

doc-example-1 | Authentication

Search (Ctrl+) | Save | Discard | Got feedback?

Overview
Quickstart
Integration assistant (preview)

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Owners
Roles and administrators (Preview)
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web Quickstart Docs ☒

Redirect URIs
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#) ☒

https://myserver.example.com/Tms/ ☒

Add URI

Logout URL
This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.
e.g. https://myapp.com/logout ✓

Implicit grant
Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

Access tokens

ID tokens

9. Select the **API Permissions** option.

10. Click the **+ Add a permission** option to add the Microsoft Graph API.

Request API permissions

PREVIEW

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Visual Studio Team Services
Integrate with Visual Studio Team

11. Select the **Application permissions** option for the type of permissions.
12. Open the **Directory category** and select the **Directory.Read.All** permission.

Request API permissions

PREVIEW

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
AccessReview	
Application	
AuditLog	
Calendars	
Calls	
ChannelMessage	
Chat	
Contacts	
Device	
Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All Read directory data	Yes
<input type="checkbox"/> Directory.ReadWrite.All Read and write directory data	Yes

Domain

13. Click the **Add permissions** button at the bottom to finish this step.
14. Click the **+ Add a permission** option to add the **Azure Active Directory Graph API**.

Request API permissions

PREVIEW

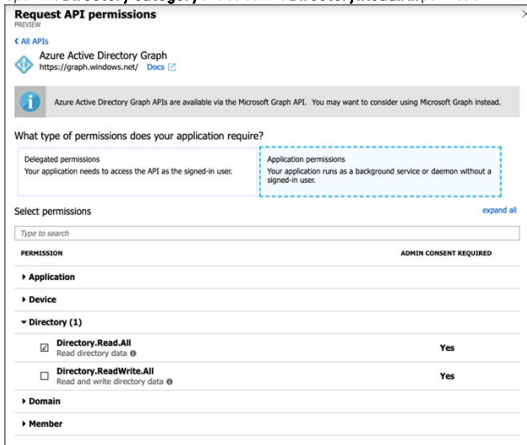
Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
Azure Data Explorer (with Multifactor Authentication) Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Azure Data Lake Access to storage and compute for big data analytic scenarios	Azure Import/Export Programmatic control of import/export jobs
Azure Rights Management Services Allow validated users to read and write protected content	Customer Insights Create profile and interaction models for your products	Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination
Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central	Dynamics CRM Access the capabilities of CRM business software and ERP systems	Dynamics ERP Programmatic access to Dynamics ERP data
Flow Service Embed flow templates and manage flows	Intune Programmatic access to Intune data	OneNote Create and manage notes, lists, pictures, files, and more in OneNote notebooks
Power BI Service Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI	PowerApps Runtime Service Powerful data storage, modeling, security and integration capabilities	SharePoint Interact remotely with SharePoint data
Skype for Business Integrate real-time presence, secure messaging, calling, and conference capabilities	Speech Create powerful speech-enabled features using speech to text and text to speech conversion	Yammer Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

Supported legacy APIs

Azure Active Directory Graph Programmatic access to directory data and objects	Exchange A powerful, easy-to-use way to access and manipulate Exchange data
--	---

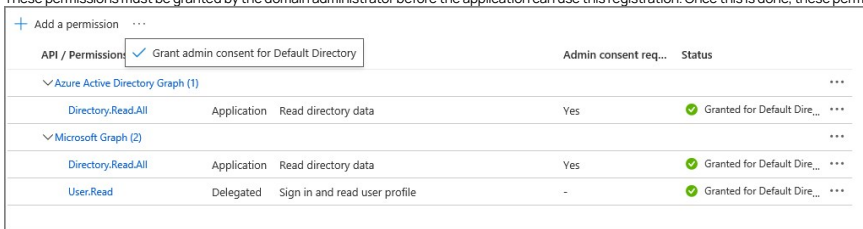
15. Select the **Application permissions** option for the type of permissions

16. Open the **Directory category** and select the **Directory.Read.All** permission.

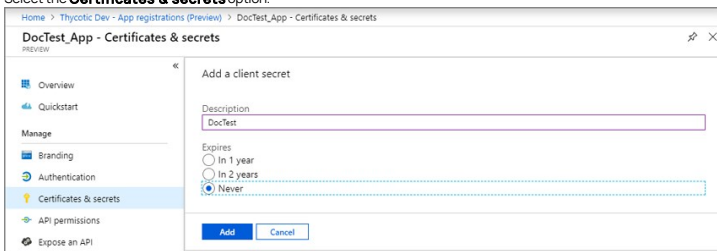


17. Click the **Add permissions** button at the bottom to finish this step.

18. These permissions must be granted by the domain administrator before the application can use this registration. Once this is done, these permissions will show a green check box next to them as shown here.



19. Select the **Certificates & secrets** option.



20. Click **+ New client secret**.

21. Add a **Description** and chose an **Expires** setting based on your business requirements.

22. Click **Add** to create the secret.

23. Use the **Click to copy** icon to copy the newly created secret to the clipboard.

You will need the Application Id and the Client Secret you copied to the clipboard in Privilege Manager to complete the setup.

Steps In your Privilege Manager Instance

Set-up Foreign Systems

1. Select **Admin I Configuration**.
2. Select the **Foreign Systems** tab.
3. Select **Azure Active Directory Domains**.
4. Click **Create**.

New

Name *

Description

Domain *

5. Enter a Name, Description, and Domain, which is the DNS name of the Tenant from the Azure Portal identified at the beginning of this document.

6. Click the **Create**.

Thycotic QA Azure AD (do not change)

[Configuration](#) [Change History](#)

Azure AD Domain Details
 For more information, see topic on [setting up your Azure AD connection](#).

Name *

Description

DNS Name *

Sign-On URL *

Azure Applications (client) ID *

Azure Client Secret *

Next Steps

① Import Users & Groups

② Assign Azure Users to Administrator Role

admin

Administrators

afred@mailinator.com

API Teting1

API User Created On Apr 17, 2020,dbes

Thycotic One (Thycotic One)

③ Enable as Authentication Provider

Yes

7. Verify the **Sign-on URL** is correct. This value should match what was specified in the Redirect URI option when setting up the Application Registration.

8. Enter the **Azure Application (client) ID**. This is the Application ID that was created when registering your application in the Azure Portal.

9. Click **Save Changes**.

10. Continue to the Azure AD Authentication Provider section and click **Edit**.

11. Complete the three steps:

1. Import Users & Groups from Azure AD. This process may take a few minutes to complete, depending on the size of the directory. Privilege Manager offers two tasks for this import:

- **Default Import AzureAD Users/Groups.** imports ALL users and groups.
- **Import Specific Azure AD Users and Groups.** imports only the specified users and/or groups.

Refer to setup and scheduling of these tasks under the "Import Users and Groups via Privilege Manager Task" and "Create Scheduled Task for Users/Groups Synchronization" topics below.

2. Assign Azure user(s) to the Privilege Manager Administrators Role. In order for users to authenticate via Azure AD, they will need to be added as members of various roles. There must be at least one member from this Azure Directory allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

3. Set as Authentication Provider.

12. Click **Save Changes**.

Viewing Imported Users and Groups

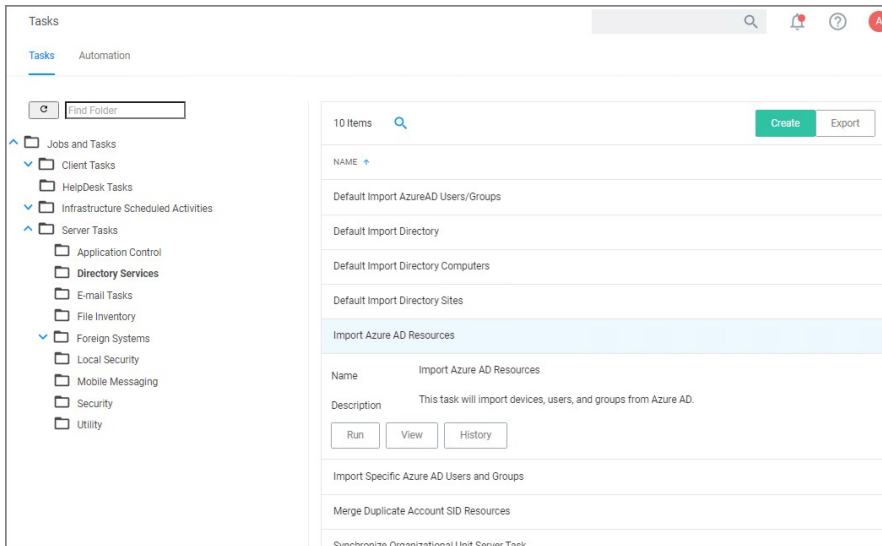
You may verify and browse the users and groups that are expected to be imported from Azure Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.
6. Select **Domain Users**. You should see a list that contains imported Azure AD users.
7. Select **User Group**. You should see a list that contains imported Azure AD groups (other groups may exist in the list as well).

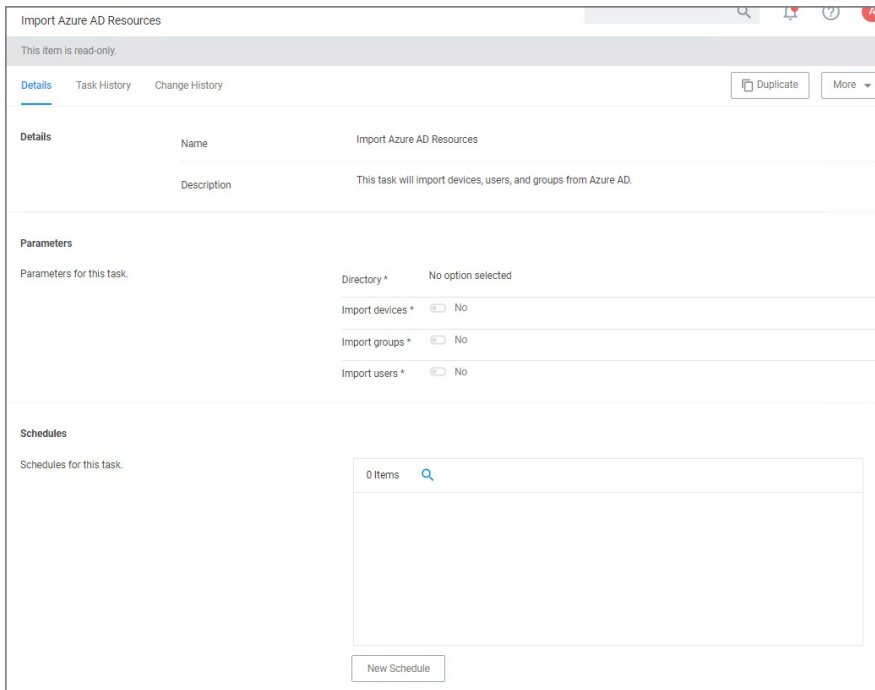
Import Users and Groups via Privilege Manager Task

This step was performed initially as part of setting up the Azure AD directory. To re-import users and groups, you can perform that operation again to pick up changes that may have occurred in the directory, such as new users that have been added or group membership changes. To run this manually:

1. Navigate to **Privilege Manager | Admin | Tasks**.
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.



5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **Run**, then **Select Resource** and select from the available resources.



7. Select the Azure Active Directory Domain you previously created.
 1. Enable **Import Devices**.
 2. Enable **Import Groups**.
 3. Enable **Import Users**.

8. Click **Run Task**.

If you only want a subset of the directory to be imported, enable select and enable only the resources you wish to import at this point.

Create Scheduled Task for Users/Groups Synchronization

To schedule this operation to happen on a regular schedule:

1. Navigate to **Privilege Manager | Admin | Tasks**.
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.
5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **View**.
7. In the Schedules tab, click **New Schedule** to create a new schedule.
 1. On the **Schedule** tab, define the desired schedule.
 2. On the **Parameters** tab, select the **Azure Active Directory** resource that you created earlier and make selections for importing devices, users, and groups.
8. Click **Save Changes**.

Third-Party Foreign Systems Integration

- [Set-up an SMTP Server Connection](#)
- [Set-up a Cyance Connection](#)
- [Set-up a ServiceNow Ticketing Connection](#)
- [Set-up VirusTotal](#)
- [Set-up an SCCM Connection](#)
- [Set-up the SMP Integration](#)
- [Set-up Syslog](#)

Set-up Cylance Integration

Cylance is an Artificial Intelligence Based Advanced Threat Prevention Solution for enterprise environments. Privilege Manager (v10.5+) integrates with Cylance to help you proactively act on any unknown applications that run in your environment to prevent potential malware attacks. The steps below walk through how to setup a Cylance Integration in Privilege Manager and then create an example policy to begin using Cylance intelligence in action across your environment.

Keep in mind that while the Cylance integration provides insight into threat analysis, ultimately you can use Privilege Manager policies to act or react in whatever way makes most sense to your organization.

Cylance Connector Installation Steps (On-prem only)

1. Open a browser on your Privilege Manager Web Server, browse to [https://\[YourInstanceName\]/TMS/Setup/](https://[YourInstanceName]/TMS/Setup/)
2. On the Currently Installed Products screen, choose Install/Upgrade Products.
3. Select option Thycotic Cylance Reputation Connector.
4. Click on **Install** and Accept the End User License Agreement. You will see your Installation Progress. Click on "Show install Logs" link to check for any errors

Note: If the installation of Cylance initially fails, redirect to [https://\[YourInstanceName\]/TMS/Setup/](https://[YourInstanceName]/TMS/Setup/) and click the Repair button next to the Cylance Product.

5. Once the Installation is successful, click on the **Home** button.

Configuring the Cylance Connector

1. Navigate to **Admin | Configuration** and select the **Reputation** tab.
2. From the Select Rating Provider drop-down, select **Cylance Rating Provider**.

The screenshot shows the 'Configuration' page for the Cylance Reputation connector. The 'Reputation' tab is selected. The 'Select Rating Provider' dropdown is set to 'Cylance Rating Provider'. Below this, there are 'Refresh' and 'More' buttons. A note states: 'Cylance administrators should add the Thycotic agent to the Cylance safe list. Review [Privilege Manager's documentation](#) on antivirus exclusions.' The 'Credentials' section includes 'Application Secret *' (masked with dots and a 'Show' button) and 'Application ID *' (masked with a dot and a 'Show' button'). The 'Settings' section includes 'Tenant ID *' (set to '5') and 'Region' (set to 'North America').

3. Enter the required **Credentials** and **Settings** details. These details can be found in your Cylance account (login at protect.cylance.com).

1. In our Cylance account, navigate to **Settings** and select **Integrations**. You find the **Tenant Id** on the right side of the Custom Applications area.

Settings

Application User Management Device Policy Global List Update Certificates **Integrations**

Custom Applications (4)

[+ ADD APPLICATION](#) Tenant ID: ba14bf04-b634-4129-8f40-f60bf253e05 [Copy](#)

EdB.PrivMan.Integration	Read 6	Write 4	Modify 5	Delete 0	Edit Delete Dropdown
test another one	Read 9	Write 6	Modify 0	Delete 0	Edit Delete Dropdown
Demo Test	Read 6	Write 4	Modify 5	Delete 0	Edit Delete Dropdown
PrivilegeManager.AppControl	Read 6	Write 4	Modify 5	Delete 0	Edit Delete Dropdown

2. Select your Privilege Manager integration from the Custom Application list. You find the required **Application ID** and **Application Secret** on the left side of the page.

PrivilegeManager.AppControl Read | 6 Write | 4 Modify | 5 Delete | 0 [Edit](#) [Delete](#) [Dropdown](#)

Application ID: 314689f2-3afe-4182-bf25 [Copy](#) Application Secret: ***** [Copy](#) [Regenerate Credentials](#)

PRIVILEGE	READ	WRITE	MODIFY	DELETE
Devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Global Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packages Configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packages Deployment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Threats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zones	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Focus Views	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS InstaQueries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Rule Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Commands	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Exceptions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Rules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Detections	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Once the Cylance details are entered in Privilege Manger, click **Save Changes**.

Create a Cylance Security Rating Filter

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the **Platform** drop-down select either Windows or macOS.
4. From the **Filter Type** drop-down select **Security Rating Filter**.
5. Name the policy and add a Description.
6. From the **Security Rating System** drop-down, select **Cylance Rating System**.

Create Filter

Platform
Windows

Type
Security Rating Filter

Name *
New Security Rating Filter

Description

Security rating system *
Cylance Rating System

7. Click **Create**.

New Security Rating Filter

Details Related Items Change History Refresh More

Filter Details

Name: New Security Rating Filter

Description:

Platform: Windows

Settings

Security Rating System: Cylance Rating System

Rating Level: Unknown

Timeout: 1 Second(s)

Error Handling

On timeout, consider the result: Error Condition

On failure, consider the result: Error Condition

8. Click **Create**.

9. Select the **Rating Level** you wish to apply. You can also specify a **Timeout** value and **Error Handling** conditions on timeout and/or on failure, the options are:

- o Matched
- o Not Matched

10. Click **Save Changes**.

Create a Cylance Policy

Use the Application Policies wizard to create a policy that uses the Cylance Security Rating filter created in the steps above.

Set-up Microsoft System Center Configuration Manager (SCCM) Integration

Privilege Manager integrates with Microsoft System Center Configuration Manager (SCCM) to allow the

- [import of computers](#) for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- [import of existing Device Collections](#) from SCCM and use them for Privilege Manager computer groups.
- [inventory of SCCM Software Packages](#) to use the package contents in Privilege Manager Application Control policies.

Create a Credential

Privilege Manager needs a username and password to access SCCM. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | Credentials**.
2. Click **Create**, to create user credentials to access SCCM.
3. After entering the user credentials information for SCCM, click **Save Changes**.

Connecting to SCCM

Before you can import data from SCCM you need to setup a foreign systems connection in Privilege Manager for the SCCM integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **System Center Configuration Manager**. If this is not listed, make sure the connector is installed by verifying via the **Privilege Manager Add/Upgrade Features** page.
3. Click **Create**.

4. Enter the name of the SCCM Server and provide the **WMI Namespace of the SCCM Site**.
5. Click **Create**.
6. Under Settings from the **Credential** drop-down, select the SCCM account created in the previous procedure.
7. Click **Save Changes**.

Import Computers

Before you can import collection data from SCCM, Privilege Manager needs to know about computers in your SCCM.

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Computers**.

4. Click **Run**.
5. Select your SCCM system via the **Select...** option.

1. Under Scope by Organizational Group type the name of your sccm system in the search text or use the search option.

6. Click **Run Task**

Verify the Computers have been Imported (optional)

1. Navigate to **Admin | Resources**.
2. Open the **Resources** tab.
3. In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
4. Select a computer from that list.
5. Select the Known Data tab in the computer resource explorer view.
6. In the tree under **Foreign Systems**, you should have the Foreign System Id and SCCM Platform Id data.

Create a Collection

After computers have been imported, you can create a collection to mirror an SCCM collection.

1. Navigate to **Admin | Resources**, open the **Resource Filters** tab.
2. In the folder tree under **Resource Filters** open **Collections | System Center Configuration Manager**.
3. Click **Create**
4. Enter a Name and Description, and specify the SCCM instance to connect to.

5. Click **Create**.

6. Select the Filter Definition tab and under **Foreign Collection** select the Collection target.

7. Click **Save Changes**.

8. Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.

9. Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Packages**.

4. Click **Run**.
5. Select your SCCM system via the **Select...** option.
 1. Under Scope by Organizational Group type the name of your sccm system in the search text or use the search option.

6. Click **Run Task**

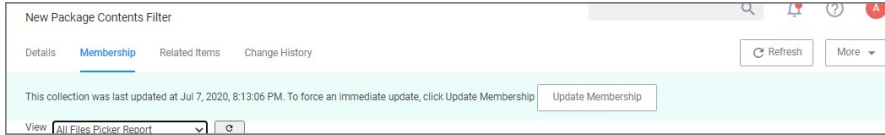
Alternatively the **SCCM Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

Create a SCCM Package Content Filter

After the Package Synchronization completes the SCCM Packages can be used in application control policies via package content filters.

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. From the Platform drop-down select Windows.
4. From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
5. Set the Name and Description of the filter.
6. Click **Create**.
7. Under **Collection Settings**
 1. from the **Data Source** drop-down select a resource.
 2. Click the package link to specify the SCCM that will be targeted.
 3. Set the switch **Results will be to Included**.

8. Navigate to the **Membership** tab.
9. If no items are listed in the membership table, click **Update Membership**.



Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Thycotic recommends to use the *Inventory Packages Referenced in Allowlists* task instead.

10. Click **Save Changes**.

This filter can then be referenced in Application Control policies.

Set-up ServiceNow Integration

Foreign System Configuration

Here are the steps to integrate Workflow between your ServiceNow Ticketing System and Privilege Manager.

1. Verify which ServiceNow User account you will use for your integration with Privilege Manager. If you decide to create a new user account to manage your approval requests, make sure that it includes the required roles for your environment:
 - o Web Service Admin (`web_service_admin`) and
 - o Approval Admin (`approval_admin`).
 - o For ServiceNow MID Server environments, the `mid_server` role permission also needs to be added to the account.
 - o The task **Create ServiceNow Request Items** requires temporary **admin** credentials for the ServiceNow instance. Once those items are created, the user does not need admin access anymore.

Refer to [ServiceNow product documentation, specifically Base System Roles](#).

2. Verify that the ServiceNow connector is installed for your Privilege Manager Cloud instance:
 1. In the Privilege Manager console navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
 2. If the connector is installed, **ServiceNow** is listed under Foreign System.

NAME	COUNT
Active Directory Domains	2
Azure Active Directory Domains	0
Azure Service Bus	1
Privilege Manager Server	1
Secret Server	1
ServiceNow	0
SMTP Server	0

3. Select the **Credentials** tab.
4. Click **Create**.
5. Under Details, enter a Name and Description for your ServiceNow credentials.
6. Under Settings, enter the information from your ServiceNow User account that was referenced in step 1 above, click **Save Changes**.
7. Select the **Foreign Systems** tab.
8. Select the **ServiceNow** link from the list of foreign systems displayed.
9. Click **Create**.
10. Enter a Name for your ServiceNow Server.
11. Enter the Base URL from your ServiceNow instance `https://[InstanceName].service-now.com/`.
12. Click **Create**.
13. Assign the credentials you created previously to link to your instance.

Foreign System Details

Name: New ServiceNow Server

Description: New ServiceNow Server

Settings

Credential: [Dropdown menu open]

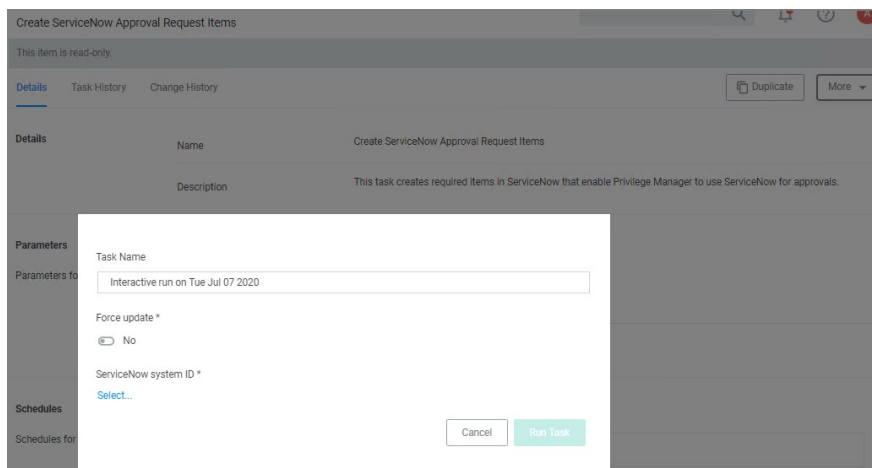
URL: [Text input field]

Available Credentials:

- Azure Service Bus Credential
- Default Proxy Server User Credential
- Default User Credential
- New User Credential
- New User Credential
- New User Credential
- PM -Test Admin

14. Next, in **Search** at the top of your Privilege Manager console, search for *Create ServiceNow Approval Request Items*.

15. In your search results, **click on this task** and then select from the **More** drop-down **Run Task**



16. Under ServiceNow System ID, click **Select...** and select the resource and add the ServiceNow Server that you created as a Foreign System earlier.

1. From the Scope by Organizational Group drop-down, select your resource.
2. Enter a Search text.
3. Click **Search**.
4. Select from the list of returned results.
5. Click **Select**.

17. Click **Run Task**

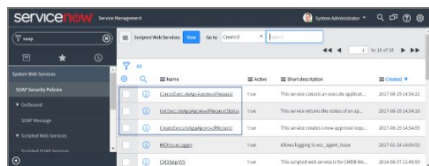
Note: Clients with robust ServiceNow installations are welcome (and in fact encouraged) to alter their ServiceNow scripted web services for use with their own ServiceNow items and workflow rather than relying on this importing task.

The task you just ran creates several new items in your ServiceNow dashboard.

ServiceNow Steps

Open ServiceNow and navigate to **Scripted Web Services | Scripted SOAP Services** to verify that these three new options are listed:

- CancelExecuteAppApprovalRequest,
- CreateExecuteAppApprovalRequest,
- GetExecuteAppApprovalRequestStatus



Now you've successfully defined a SOAP endpoint that Privilege Manager knows how to call to initiate a ServiceNow request for approval.

Define Policy and Actions

You need to create an action and attach it to a policy to manage what events you want sent to ServiceNow for approvals.

1. In the Privilege Manager console, navigate to **Admin | Tasks**
2. Click the **Automation** tab.
3. In the tree navigate to **Automation | Approvals | Approval Processes**, click **Create**.

New

Template

ServiceNow Approval Process

Name *

New ServiceNow Approval Process

Description

Cancel Create

4. Enter a name and description, click **Create**.

New ServiceNow Approval Process

Details Change History Refresh More

Service Now Approval Process Details

Name: New ServiceNow Approval Process

Description: [Empty]

Settings

ServiceNow Server: Test ServiceNow Server

Check request status every: 20 Second(s)

Timeout after: 20 Minute(s)

Show Advanced

5. Under **Settings** specify your ServiceNow Server, click **Save Changes**.

6. Back in the Automation tree, select **Approval Types**, click **Default Execute Application Request Type**.

Tasks

Tasks Automation

Find Folder

Automation

- Approvals
 - Approval Processes
 - Approval Types**
- Powershell Commands
- Privilege Manager Solutions
- Workflow

3 Items Create Export

NAME

Default Execute Application Request Type

Name: Default Execute Application Request Type

View

Duplicate and customize the Automation Task.

7. Select your **ServiceNow Approval Process**.

Default Execute Application Request Type

Details Change History Refresh More

Approval Process Details

Name: Default Execute Application Request Type

Description: [Empty]

Settings

Characteristics

Policy Specific: No

File Specific: Yes

Options

Security Rating System(s): VirusTotal Rating System Edit

Process Handler: New ServiceNow Approval Process

8. Click **Save Changes**.

Using an Approval Request (with ServiceNow Request ItemNumber) Form Action

1. Navigate to **Admin | Actions**.

2. Search and select **Approval Request (with ServiceNow Request Item Number) Form Action**.

Approval Request (with ServiceNow Request Item Number) Form Action

This item is read-only.

Details | Related Items | Change History

Duplicate | More

Action Details

Name: Approval Request (with ServiceNow Request Item Number) Form Action

Description: This action will display a approval request form for approval before allowing application to run.

Settings

This feature is not supported for Azure Active Directory joined computers. Only Domain joined computers will work.

Require authentication:

- Require authentication:
- By the interactive end-user
- By a member of the group:

Approval Type: Default Execute Application Request Type

Window Design

Message prompt logo:

Application label: Application:

3. Click **Duplicate**.

4. Name your new action and click **Create**.

5. Customize the Action based on your specific business requirements.

6. Click **Save Changes**.

7. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for ServiceNow Approvals.

8. Under the **Actions** section, search for and add the action you previously created, *ServiceNow Approval Request Form Action*.

9. Click **Save Changes**.

10. Click the **I** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your endpoint agents.

Policies also automatically update according to a schedule.

Using an Endpoint Group Member Authenticated Message Action

This action can be used for *over the shoulder* approvals whether systems are on- or offline. The supervisor approves access by authentication on the user's endpoint system.

1. Navigate to **Admin I Actions**.

2. Click **Create**

1. On the **Create Action** modal from the **Platform** drop-down select **Windows**.

2. From **Type** drop-down select **Endpoint Group Member Authenticated Approval Action**.

3. Enter a meaningful **Name** and **Description**.

4. From the **Approval Group** drop-down, select the group membership of the approver.

Create Action

Platform: Windows

Type: Endpoint Group Member Authenticated Approval Action

Name *: New Endpoint Group Member Authenticated Approval Action

Description:

Approval Group *: Web Admin

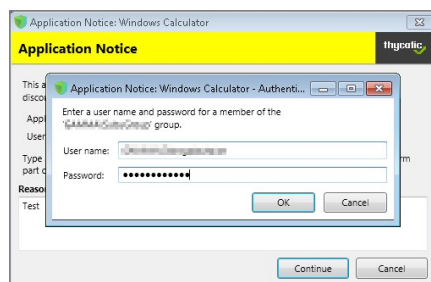
Cancel | Create

5. Click **Create**.

3. Under Settings verify the **Require approval by a member of the group**: contains the correct group. If you ever need to change it, come back to this page and click the group name to access the change modal.
4. Navigate to your computer group's **Application Policies**, click **Create Policy** or find an existing policy that you want to use for ServiceNow Approvals.
5. Under the **Actions** section, search for and add the action you previously created.
6. Click **Save Changes**.
7. Click the **I** next to **Deployment** and select **Resource and Collection Targeting Update** to immediately send the policy to your endpoint agents.

Policies also automatically update according to a schedule.

Sample Group Member approval notice with approval overlay:



Refer to the **Endpoint Group Member Authenticated Approvals** report in Privilege Manager or your ServiceNow instance to view a history of "over the shoulder" approvals:

< Back to Reports

Endpoint Group Member Authenticated Approvals

Filter Report Refresh CSV PDF Search

Drag column here for grouping

User	File Path	Time	Policy	Agent	Approver	Command Line	Reason
	C:\Windows\sys...	9/22/2020 11:57 PM	Test Service Now Application Control Policy			"C:\Windows\sys...	Test
	C:\Windows\sys...	9/22/2020 10:36 PM	Test Service Now Application Control Policy			"C:\Windows\sys...	Test
		9/22/2020 10:12 PM					
		9/22/2020 9:37 PM					
		9/22/2020 4:50 PM					
		9/22/2020 4:45 PM					

10 items per page 1 - 10 of 10 items

Integration Workflow

Now that you have a policy attached to your ServiceNow integrated Action, the requests from your policy will be sent through ServiceNow for approval.

1. On your endpoint, perform the action that your policy targets for ServiceNow Approval. You will be prompted with a justification window to explain your request. To approve these requests, open your ServiceNow Dashboard.
2. Go to **My Requests** in ServiceNow and you will see your new requests.
3. Click Requested for details.
4. In the Request page you will be able to view details of what action is being requested, and you can Accept the action.
5. On your endpoint, the pending justification window will update to an Approved status, and the user will be able to access their requested application.

Create Approval Request Items Task

Privilege Manager integrates with ServiceNow to manage approvals for user-requested application execution and elevation. For this integration to work there are several items that must be created in your ServiceNow instance. You can create these items manually or run the Create ServiceNow Approval Request Items task in Privilege Manager to create them automatically.

Most of the items created automatically by the Create ServiceNow Approval Request Items task are generic, and you are encouraged to replace these items with their own, and use your own workflows, forms, etc. This document describes what default items this task creates, and what is required for the integration to work so that you can adjust according to your own ServiceNow system.

How to create ServiceNow Approval Request Items Task

When you run the Create ServiceNow Approval Request Items task, Privilege Manager creates the necessary items in ServiceNow so that it can use ServiceNow to manage requests to approve execution or elevation of applications. This section describes each item and their functions:

Thycotic:

The task creates a service catalog category named "Thycotic" within your ServiceNow UI.

Execute Application Request:

The task creates a service catalog item named "Execute Application Request" and associates it with the Thycotic service catalog category.

Variables

PMApprovalId	The Privilege Manager internal identifier for the approval request
PMInitiatorId	The Privilege Manager internal identifier for the user that initiated the request
PMInitiatorName	The name of the user that initiated the request
PMPolicyId	The Privilege Manager internal identifier for the policy associated with the approval request
PMPolicyName	The name of the policy associated with the approval request
PMAgentId	The Privilege Manager internal identifier for the endpoint on which the request was initiated
PMAgentName	The name of the endpoint on which the request was initiated
PMProcessId	The Privilege Manager internal identifier for the process configuration item associated with the approval request
PMProcessName	The name of the process configuration item associated with the approval request
PMFilePath	The path to the application the user is attempting to run
PMUserReason	The reason given by the user requesting the approval

CreateExecuteAppApprovalRequest

The task creates a scripted SOAP service named "CreateExecuteAppApprovalRequest." When a user initiates an approval request, Privilege Manager will call this service with input data about the request. The default script will create a new Execute Application Request service catalog item, fill out the variable data from the inputs, and submit the item. The service returns the ID of the item to Privilege Manager so that it can periodically check or update the status of the item.

Script Input

The task creates inputs with the same names as the Variables in Execute Application Request listed above

Script Output

The task creates an output named "PMRequestId." Privilege Manager looks for this output by name and records it so can be used in future service calls to check or update the request status.

GetExecuteAppApprovalRequestStatus

The task creates scripted SOAP service named "GetExecuteAppApprovalRequestStatus." When an approval is in progress, Privilege Manager will periodically call this service to determine if the request has been approved or rejected.

Script Input

The task creates an input named "PMGetRequestId." Privilege Manager supplies this input using the value from PMRequestId that was output from the CreateExecuteAppApprovalRequest service.

Script Output

PMApprovalStatus	Privilege Manager expects this service to return PMApprovalStatus with one of the following values:
	approved: The request has been approved
	rejected: The request has been rejected
	pending: The request is still pending approval or rejection
	invalid: PMGetRequestId is not a valid ID, or the approval request is in an otherwise invalid state and will be rejected by Privilege Manager.
PMComment	If there is a comment by the worker that approved or rejected the request, it can optionally be returned in the output named PMComment. If this output is present Privilege Manager will record it with the status of the request in its database

CancelExecuteAppApprovalRequest

The task creates a scripted SOAP service named "CancelExecuteAppApprovalRequest." If a request times out from within Privilege Manager, Privilege Manager will call this service to cancel the corresponding item in ServiceNow.

NOTE: Privilege Manager expects this service to be defined in ServiceNow, but the product does not invoke this except when a request times out from Privilege Manager.

Inputs

PMCancelRequestId	Privilege Manager call this service with PMCancelRequestId set to the value from PMRequestId returned from the CreateExecuteAppApprovalRequest service.
PMCancelComment	Privilege Manager calls this service with PMCancelComment set to a comment about why the request is being canceled.

Outputs

The task creates the output named **TmsCancelResult**. Privilege Manager expects an output with this name, but currently ignores the value.

Required Integration Points

What Can Change vs. What Must Remain

Most of the ServiceNow back end can be changed to accommodate your own items and workflows. Privilege Manager only requires the three scripted SOAP web services described above. You are welcome to change the script within the services to do whatever is necessary for your environment.

While the inputs that Privilege Manager sends to the services are fixed, once they reach ServiceNow you are free to do (or not do) what you want with the values.

Privilege Manager expects the outputs from the services as described above. PMRequestId is by default the ServiceNow sys_id of the requested service catalog item instance, but can be any string up to 256 characters used to identify the request. It's up to you to ensure that the status and cancel services can interpret that value.

You can change the names of the services if you update the names in the ServiceNow Approval Process configuration in Privilege Manager. You can also create multiple ServiceNow Approval Process items within Privilege Manager, and each can reference their own set of services.

Set-up Symantec Management Platform (SMP) Integration

Privilege Manager integrates with the Symantec Management Platform (SMP) to allow the

- [import of computers](#) for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- [import of existing Resource Collections](#) from SMP and use them for Privilege Manager policy targets.
- [inventory of SMP Software Packages](#) to use the package contents in Privilege Manager Application Control policies.

Create a Credential

Privilege Manager needs a username and password to access SMP. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | Credentials**.
2. Click **Create** to create user credentials to access SMP.
3. After entering the user credentials information for SMP, click **Save Changes**.

Connecting to SMP

Before you can import data from SMP you need to setup a foreign systems connection in Privilege Manager for the SMP integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **Symantec Management Platform**. If this is not listed, make sure the connector is installed by verifying via the Privilege Manager Add/Upgrade Features page.
3. Click **Create**.

4. **Name** the Symantec Management Platform and provide the **URL of the Altiris console**.
5. Click **Create**.
6. Select the newly created SMP foreign system and click **Edit**.
7. Under Settings select the SMP user credential that you created in the previous procedure.
8. Click Save.

Import Computers

Before you can import collection data from SMP, Privilege Manager needs to know about computers in your SMP.

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
3. Click **SMP Sync Computers**.

4. Click **Run**.

- Select your SMP system via the **Select...** option.

- Click **Run Task**

Verify the Computers have been Imported (optional)

- Navigate to **Admin | Resources**.
- Open the **Resources** tab.
- In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
- Select a computer from that list.
- Select the Known Data tab in the computer resource explorer view.
- In the tree under **Foreign Systems**, you should have the Foreign System Id and SMP Platform Id data.

Create a Collection

After computers have been imported, you can create a collection to mirror an SMP collection.

- Navigate to Resources, open the **Resource Filters** tab.
- In the folder tree under **Resource Filters** open **Collections | Symantec Management Platform**.
- Click **Create**
- Enter a Name and Description, and specify the SMP instance to connect to.

- Click **Create**.
- Select the Filter Definition tab and under **Foreign Collection** select the Collection target.

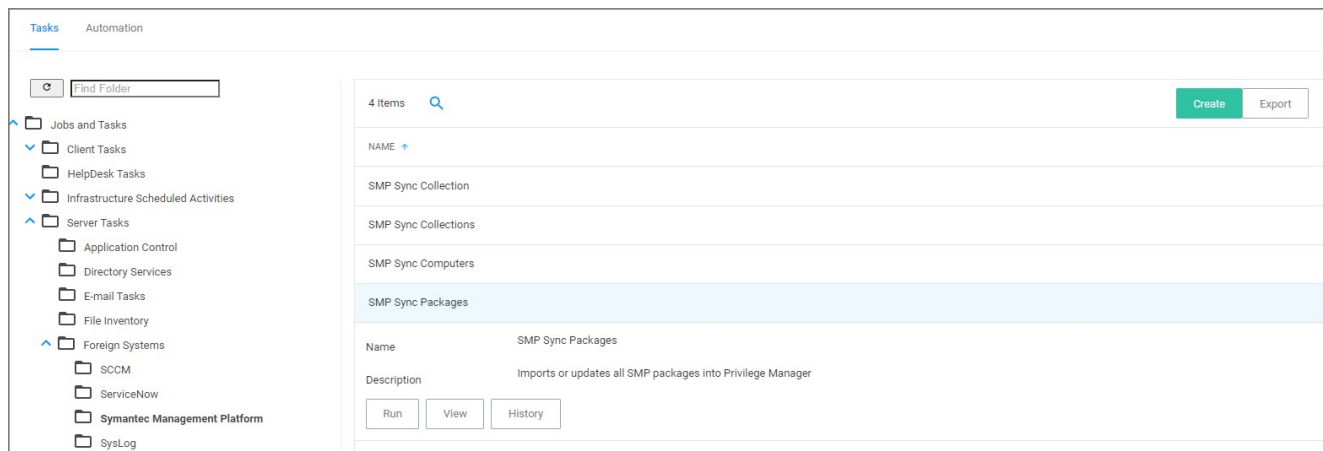
- Click **Save Changes**.

- Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.
- Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

- Navigate to **Admin | Tasks**.
- On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
- Click **SMP Sync Packages**.



- Click **Run**.
- Select your SMP system via the **Select...** option.



- Click **Run Task**

Alternatively the **SMP Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

Create a SMP Package Content Filter

After the Package Synchronization completes the SMP Packages can be used in application control policies via package content filters.

- Navigate to **Admin | Filters**.
- Click the **Create Filter** button.
- From the Platform drop-down select **Windows**.
- From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
- Set the Name and Description of the filter.
- Click **Create**.
- Next to Package, click **Select resource...**
- Select the package from SMP that will be targeted.
- Set the switch **Results will be to Included**.

The screenshot shows the 'New Package Contents Filter' configuration page in the 'Details' tab. The page has a top navigation bar with 'Details', 'Membership', 'Related Items', and 'Change History' tabs. There are 'Refresh' and 'More' buttons in the top right. The 'Filter Details' section contains: Name: 'New Package Contents Filter'; Description: 'Filters files contained in the specified package'; Platform: 'Windows'. The 'Collection Settings' section contains: Data Source: 'Package Contents Query'; Package *: '00000000-0000-0000-0000-000000000000'; Results will be: 'Excluded'.

10. Navigate to the **Membership** tab.
11. If no items are listed in the membership table, click the **Sync Package** button.

The screenshot shows the 'New Package Contents Filter' configuration page in the 'Membership' tab. The 'Membership' tab is selected. A message states: 'This collection was last updated at Jul 7, 2020, 8:13:06 PM. To force an immediate update, click Update Membership'. There is an 'Update Membership' button. At the bottom, there is a 'View' dropdown menu set to 'All Files Picker Report' and a refresh icon.

Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Thycotic recommends to use the *Inventory Packages Referenced in Allow Lists* task instead.

12. Click **Save Changes**.

This filter can then be referenced in Application Control policies.

Set-up SMTP Connection

Simple Mail Transfer Protocol (SMTP) is the Internet standard for email transmission. Often organizations use an SMTP Server – or a server that is specifically dedicated to transmitting email messages via TCP Port 25 – and in order to send email alerts with Privilege Manager policies, you must ensure that your email server is connected to Privilege Manager.

SMTP In Cloud Environments

Starting with version 10.7.1 of Privilege Manager Cloud, the SMTP foreign system is automatically configured with the email server information as provided during the cloud instance set-up. The information can be added/changed following the initial set-up.

Configuring the SMTP Connection

To set up the connection, follow these steps:

1. Navigate to **Admin | Configuration | Foreign Systems** (tab).
2. Click SMTP Server, then **Create**.
3. Add the Name of your SMTP Server and the base Uri (ex: smtp://[hostname]:[port]), then **Create**.

Next, in order to begin email alert notifications for a policy, you will need to assign a Task for the job. The **Setting Up Email Alerts** information below is just one example of tasks that can be configured for automated email notifications.

Setting up Email Alerts

Email alerts can be created in **Admin | Tasks > Server Tasks > E-mail Tasks**, then **Create**.

Approval Requests

1. Navigate to **Admin | Tasks | Automation** tab, then expand **Approvals** and select **Approval Processes**.
2. In the center section you will see options including Manual Approval Process with E-mail Alerts (If this option does not exist, click **Create** to add it). Click this option and then **Edit**.
3. Enter the requested information.
 1. For the Start Activity, type Send E-mail for New Approval Task.
 2. For the SMTP Server, select the resource for the SMTP connection you created above.
4. Click **Save Changes**.

Note: For cloud environments the SMTP server settings are pulled from an existing configuration and **can't** be edited via the parameters tab.

Set-up SysLog Connection

Privilege Manager can push out SysLog formatted messages on a set schedule. Note that this does not happen immediately upon events occurring. Listed below are steps for configuration and task creation for scheduling the action of sending Discovery Event logs to a SysLog server.

Note: The Send policy feedback option needs to be enabled on all policies that are supposed to send SysLog formatted events.

Configuring SysLog Connection

To configure SysLog messages in Privilege Manager:

1. Navigate to **Admin | Configuration** and select the Foreign Systems tab.
2. Click on SysLog and **Create**. Set a Name and the SysLog Server Address (either tcp or udp). The default is udp on port 514.

3. Once the server is created, you can use **Edit** to change any of the configuration settings.

The protocol drop-down options are UDP, TCP, and HTTPS. HTTPS supports integrations with DEVO.

Setting up SysLog Server Tasks

1. After adding a new Syslog connection, to manually send logs to your Syslog Server go to **Admin | Tasks**.
2. Expand the **Server Tasks** folder, then **Foreign Systems**, select SysLog and click **Create**.
3. From the **Template** drop-down, for example select **Send SysLog Application Events**.
4. Add a Name for this task, an Event Name (e.g. "Privilege Manager Application Events"), and Event Severity.
5. From the **SysLog System** drop-down select your SysLog server foreign system (configured above).
6. Optionally also enter a **Security Ratings Provider**, depending on your other integrations.

7. Click **Create**.

Once created, you'll be taken to the new Scheduled Task's page where you can run the task on demand and/or specify how often you want events received by Privilege Manager (i.e. all events viewed in Admin I Event Discovery) to be pushed out to the SysLog server. The schedule can be hourly, every 30 minutes, daily, or whatever time period is preferred.

After this task runs and successfully completes, verify that Event Discovery events appear in your SysLog system.

Template Options

The following template options are available:



Template

- Send SysLog Application Action Events
- Send SysLog Application Action Events**
- Send SysLog Application Justification Events
- Send SysLog Bad Rated Application Action Events
- Send SysLog Events
- Send SysLog Newly Discovered File Events
- Send SysLog Password Disclosure Events

Event Name *

- **Send SysLog Application Action Events** - Use this template to send application action events to your SysLog system. Application Action Events contain generic information about the application that run, which policy was triggered, the date/time stamp, computer, and user for example.
- **Send SysLog Application Justification Events** - Use this template to send application justification events to your SysLog system. For example, if a user runs an application requiring a justification workflow.
- **Send SysLog Bad Rated Application Action Events** - Use this template to send an event to your SysLog system, when an application is being installed or executed, that is identified with a bad security rating.
- **Send SysLog Events** - Use this template to send all SysLog events to your SysLog system. These events are based on the different options you selected on the SysLog server during setup.
- **Send SysLog Newly Discovered File Events** - Use this template to send newly discovered file events to your SysLog system. For this to produce any events the Default File Inventory Policy needs to be enabled and resource discovery schedules need to be customized.
- **Send SysLog Password Disclosure Events** - Use this template to send all password disclosure events to your SysLog system.

Data Sources

The following five data sources can be used with the respective templates above:

- **Application Control Justification Events** (7d6bdbf0-8f2a-4e9c-9c7e-fa6b75803c45)
- **Application Control Policy Feedback** (eeb7aa6-f675-4586-a7e3-3eb54b59ba4d)
- **Recently Discovered Applications Query** (b875d3a6-433c-42cc-8332-05350343e498)
- **Local Security Password Disclosure Events** (13d6cf4d-0132-4401-88ab-80b55301c60c)
- **Application Control Policy Feedback Restricted to Security Level** (4eb4ec69-d7a9-4797-972a-41855d3e7799)

If custom data sources are used, they need to specify the following fields:

- externalId
- Facility
- Severity
- EventTime
- Host
- DeviceVendor
- DeviceProduct
- DeviceVersion
- Name
- CEFSecurity

Troubleshooting If SysLog Option Is Missing under Foreign Systems

If you are a Privilege Manager Cloud customer, contact Thycotic support to have it added to your instance.

On-premises customers, navigate to [https://\[YourOrganizationURL\]/TMS/Setup/ProductOptions/SelectProducts](https://[YourOrganizationURL]/TMS/Setup/ProductOptions/SelectProducts) and check the Thycotic SysLog Connector option. Install the SysLog Connector and accept the License Terms and Conditions.

Set-up VirusTotal Connection

Privilege Manager can perform real-time reputation checks for any unknown applications by integrating with analysis tools like VirusTotal. This article shows how to set up the integration between Privilege Manager and VirusTotal and then create a monitoring policy in Privilege Manager for reputation checking.

VirusTotal API Key

As a first step the VirusTotal Ratings Provider has to be configured. For this,

1. Sign up for a Free VirusTotal account at <https://www.virustotal.com/>.
2. Sign in to VirusTotal and find your API key under your **Username | Settings | API Key**.

Install VirusTotal

As a second step VirusTotal needs to be installed in Privilege Manager.

Note: You need outbound access on your server for that installation.

1. Open a browser on your Privilege Manager Web Server.
2. Browse to <https://YourInstanceName/TMS/Setup/>.
3. On the Currently Installed Products screen, choose Install/Upgrade Products.
4. Check the Thycotic VirusTotal Reputation Connector, click **Install**. Then **Accept** the End User License Agreement. You will see your Installation Progress.

Note: If the installation of VirusTotal initially fails, redirect to <https://YourInstanceName/TMS/Setup/> and click the **Repair** button next to the VirusTotal Product.

5. Navigate to **Thycotic Privilege Manager | Admin | Configuration | Reputation** tab.
6. Select **VirusTotal Rating Provider** from the Select Rating Provider drop down menu.

The screenshot shows the 'Configuration' page for the 'Reputation' section. The 'Details' tab is active, showing the following configuration:

- Name:** VirusTotal Rating Provider
- Description:** Application Control VirusTotal based provider for resource security ratings.
- VirusTotal API Key:** A masked field with 'Show API Key' and 'Change' buttons.
- Classify as 'Suspect':**
 - When 1 or more positive indicators are found by leading scan engines.
 - When the total number of positive indicators reaches 10 or more across all contributors.
- Classify as 'Bad':**
 - When 2 or more positive indicators are found by leading scan engines.
 - When the total number of positive indicators reaches 50 or more across all contributors.

7. Enter the **VirusTotal API Key**, click **Update**.

8. Enter information under Details and specify settings for Suspect and Bad classifications.

9. Click **Save Changes**.

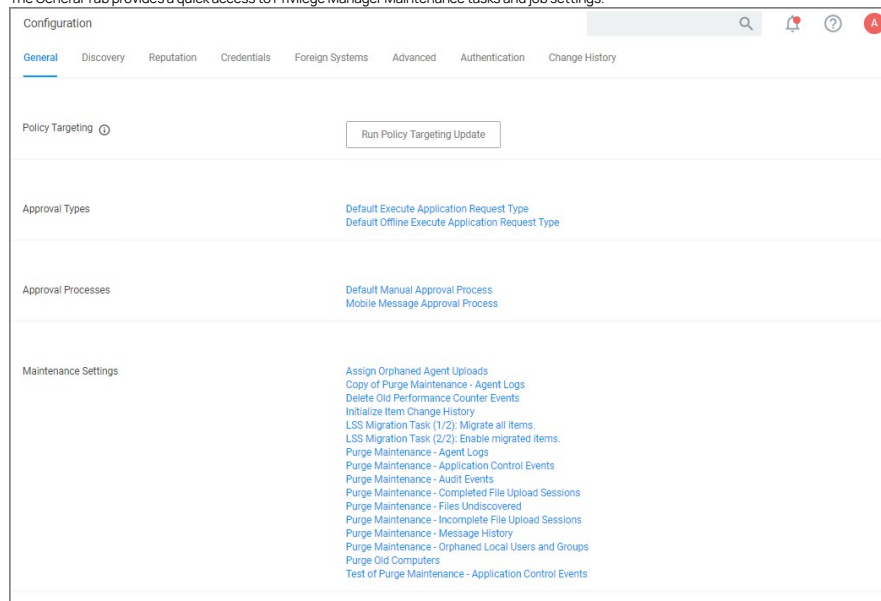
Note: VirusTotal can be used without API Key. If the free version is used, reputation checks are limited to 4 per Minute. Thycotic does not recommend this for a production environment.

For the implementation example below, we are creating two filters, using one default filter, and creating a policy. One filter is the standard Security Rating Filter the other filter controls, that we only send applications to VirusTotal for a reputation check that are in the user's Downloads and Temp directories.

Further details about creating a Security Rating Filter and other needed filters to work with reputation checking policies refer to the [Reputation Checking](#) topic.

General Tab

The General Tab provides a quick access to Privilege Manager Maintenance tasks and job settings.



Policy Targeting

The Policy Targeting Update automatically caches the list of policies applicable to each agent by updating the collections and resource targets.

Approval Types

For approval types can be specified as policy or file specific, a Security Rating System can be added, and a Process Handler can be entered. The following default approval types are available:

- Default Execute Application Request Type
- Default Offline Execute Application Request Type

Approval Processes

These are read-only items and by default Administrators are always allowed to approve any requests and an optionally activity can be started as part of the approval.

- Default Manual Approval Process
- Default Offline Approval Process
- Mobile Message Approval Process

Markdig.Syntax.Inlines.LinkInLine

- [Assign Orphaned Agent Uploads](#)
- [Delete Old Performance Counter Events](#)
- [Initialize Item Change History](#)
- [Purge Maintenance - Agent Logs](#)
- [Purge Maintenance - Application Events](#)
- [Purge Maintenance - Audit Events](#)
- [Purge Maintenance - Completed File Upload Sessions](#)
- [Purge Maintenance - Files Undiscovered](#)
- [Purge Maintenance - Incomplete File Upload Sessions](#)
- [Purge Maintenance - Message History](#)
- [Purge Old Computers](#)

History Tab

The Change History tab is accessible via:

- **Admin | Configuration** – listing all changes made to Advanced, Authentication Provider, Foreign Systems, Discovery, and Reputation item configuration settings.
- **Admin | Policies** – listing all changes made to policies.
- Admin | More and then (for the default menu, might differ if customized)
 - **Filters** – listing all changes made to a specific filter.
 - **Actions** – listing all changes made to a specific action.
 - **Resources** – listing all changes made to a specific user editable resource. Meaning resources that are not user editable, like a file extension, do not have a history change tab.
 - **Tasks** – listing all changes made to a specific task.

Once the tab is selected, it opens a two-column page. On the left all recorded changes are listed with the newest record on top. This left column data provides a summary of the changes:

- who made the change,
- what was changed,
- the type of change,
- item changed, and
- date/time of the change.

For any changes made to the Authentication Provider for Foreign Systems, like changing from NTLM to Azure Active Directory for example, the Change History provides details about the active and staged states with true and false indicators.

Looking at Details

The following image shows an example of the change history for a foreign system entry. The change shows that the foreign system was initially pointed at the local host URL, with a Credential and Client Secret pertaining to that localhost instance. An update was made to configure a real Secret Server instance URL with accompanying changes of Client Secret and Credential to be able to authenticate against that new URL.

The screenshot shows the 'Change History' tab for a 'Default Secret Server' configuration. The interface includes a 'Refresh' button and a list of 7 items. The items are grouped by date:

- Wednesday July 1, 2020**: Imported item: State \ NewSecretFolderid : 5, Default Secret Server, 6:04 PM.
- Friday June 19, 2020**: test1 Saved item: Credential : Default User Credential, Default Secret Server, 4:36 PM.
- Thursday June 18, 2020**: Saved item: State \ PingPath : healthcheck.aspx, Default Secret Server, 2:59 PM.
- Thursday June 18, 2020**: Saved item: Credential : [redacted], Default Secret Server, 6:40 PM.
- test1**: Saved item: State \ CurrentlyConnected : True, Default Secret Server, 11:18 AM.

The right-hand pane shows details for the selected item, including a 'Credential' section with a 'primary.local' button and a 'Default-User-Credential' button.

Drilling Down

To look at details of any given change, select one of the change entries in the left column. For the example we created a policy to deny the installation of iTunes on Windows endpoints.

The screenshot shows the 'Change History' tab for a 'Deny iTunes Installation' policy. The interface includes a 'General' tab, 'Policy Events', and 'Change History' tabs, along with an 'Active' toggle switch. The items are grouped by date:

- Tuesday July 7, 2020**: test1 Created item from template, Deny iTunes Installation, 9:46 AM.
- test1 1**: Created item from template: Created item from tem..., Deny iTunes Installation, 9:46 AM.
- test1 2**: Deny iTunes Installation, 9:46 AM.

The right-hand pane shows details for the selected item, including a 'Created item from template' section and a 'Deny iTunes Installation' section.

What we see:

1. Information about the system and user initiating the change, here test1 and information about the type of change, here Created from template.
2. The name of the item that was created from template, the date and time when the change occurred.
3. Details on the summary information from the left, such as a link to view the user details and what change was done to which item.

The next screen shows a state change due to the policy being saved. The State\ResourceTargetids are being saved for the first time for this policy.

Deny iTunes Installation

General Policy Events **Change History**

2 Items

Tuesday July 7, 2020	test1 Tuesday, July 7, 2020, 9:46:29 AM Saved item Deny iTunes Installation
test1 Saved item: ApplyToResourcesSettings \ AllowedTargetRoleTypeId ... Deny iTunes Installation 9:46 AM	ApplyToResourcesSettings \ AllowedTargetRoleTypeId Computer 00000000-0000-0000-0000-000000000000
test1 Created item from template: Created item from template Deny iTunes Installation 9:46 AM	State \ ResourceTargetIds Windows Computers
	Enabled True

The last entry in the Change History list provides all the details about the change to the policy after initial creation and save.

Item Change History Report

The [Item Change History Report](#) is part of the **Diagnostic** group on the Reports page. You can also search for "change history" and the report will be listed on the search results page. Click the link to access the report.

The report lists the history of item changes.

Item Change History

Filter Report Refresh CSV PDF Search

Drag column here for grouping

Name	Operation	User	Date	Correlation ID
New User Credential	CreateFromTemplate	Administrator	7/7/2020 9:10 AM	ed74b28d-399d-4a79-9141-3e691122b2a8
Create inbound TCP firewall rule for Elevate Adding Inbound TCP Firewall Rule Privilege	CreateFromTemplate	Administrator	7/6/2020 11:00 PM	368940d4-94d9-4cee-8a8f-971f1808882c
New Display Advanced User Message Action (MacOS)	Save	Administrator	7/6/2020 9:00 PM	3ca93080-bfa0-4e02-8cfa-277e2fd6bab6
New Display Advanced User Message Action (MacOS)	CreateFromTemplate	Administrator	7/6/2020 9:00 PM	6e1841e1-f2af-4c4d-af1f-fee089e3088b
Test of Application Denied Notification Action	Clone	Administrator	7/6/2020 8:24 PM	f96f463e-1c58-4058-b10f-2c81f3b24f09
Copy of Deny Execute Message	Clone	Administrator	7/6/2020 8:07 PM	2b3ecc9f-5e52-4644-a488-854a07c1682b
New Adjust Process Rights Action	Save	Administrator	7/6/2020 7:42 PM	c9675353-5e6e-4185-8e8f-18f9fa2956b
New Adjust Process Rights Action	CreateFromTemplate	Administrator	7/6/2020 7:42 PM	c73da2d0-8fe5-4001-bae9-7ebe7c42b9d8
New Set Process Security Descriptor	Save	Administrator	7/6/2020 7:24 PM	ec86ef31-4df0-4692-b2dd-3aa633d69f84
New Set Process Security Descriptor	CreateFromTemplate	Administrator	7/6/2020 7:24 PM	1b41a4cc-1651-4089-ab16-446c7b133ab4

For further investigation, you can access the item that was changed by clicking the entries in the Name column.

Reputation Tab

Here you select the Rating Provider from drop-down. Current options are Cylance and VirusTotal rating providers.

The configuration details required are different for the two rating providers as shown in the following sample images.

Cylance Rating Provider

The screenshot shows the configuration page for the Cylance Rating Provider. The page is titled "Configuration" and has a navigation menu with tabs: General, Discovery, Reputation (selected), Credentials, Foreign Systems, Advanced, Authentication, and Change History. A search bar and notification icons are in the top right. Below the navigation, there is a "Select Rating Provider" dropdown menu set to "Cylance Rating Provider". A "Refresh" button and a "More" dropdown are on the right. A note states: "Cylance administrators should add the Thycotic agent to the Cylance safe list. Review [Privilege Manager's documentation](#) on antivirus exclusions." The "Credentials" section includes "Application Secret" (masked with dots and a "Show" button) and "Application ID" (masked with a dot and a "Show" button"). The "Settings" section includes "Tenant ID" (value: 5) and "Region" (value: North America).

VirusTotal Rating Provider

The screenshot shows the configuration page for the VirusTotal Rating Provider. The page is titled "Configuration" and has a navigation menu with tabs: General, Discovery, Reputation (selected), Credentials, Foreign Systems, Advanced, Authentication, and Change History. A search bar and notification icons are in the top right. Below the navigation, there is a "Details" section with a "Refresh" button. The "Details" section includes "Name" (value: VirusTotal Rating Provider), "Description" (value: Application Control VirusTotal based provider for resource security ratings.), and "VirusTotal API Key" (masked with asterisks, with "Show API Key" and "Change" buttons). The "Classify as 'Suspect'" section has two rows, each with a toggle switch and a condition: "When 1 or more positive indicators are found by leading scan engines." and "When the total number of positive indicators reaches 10 or more across all contributors." The "Classify as 'Bad'" section has two rows, each with a toggle switch and a condition: "When 2 or more positive indicators are found by leading scan engines." and "When the total number of positive indicators reaches 50 or more across all contributors."


Navigate to the **Admin | Diagnostics** page to view more comprehensive agent details. The Diagnostics page is also the go-to stop for full system health. Go there to find Server Console Logs and other system level warnings or tips.

Diagnostics deny 🔍 🔔 ? ⚠️

This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.

[Clear Descriptive Item Cache](#) [Clear Local Storage Cache](#) [Import Items](#) [Console Logs](#)

Managed Operating Systems **Agent Registration State** **Agent Policy State** **Password Age**



System Health

- Normal**
- Remote Task Status
- Normal**
- Number of Old Computers
- Warning**
- Unacknowledged Events
- Normal**
- Pending Approvals Count
- Normal**
- Number of Application Events
- Normal**
- File Uploads Size
- Normal**
- Background Message Queue Size
- Normal**
- Background Message Queue Older than 1 Week

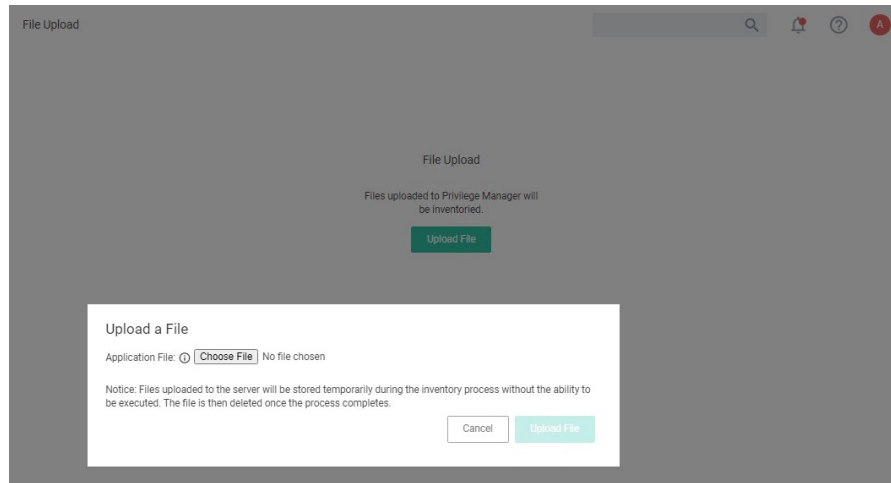
Key Configuration Settings

- Properly Configured**
- Product Licenses Installed
- Normal**
- Server Activity Paused
- Information**
- Update Available
- Properly Configured**
- Configure Active Directory
- Properly Configured**
- Set Default User Credential
- Properly Configured**
- Install Agents

Licensing

- Normal**
- Client License Expiration

The File Upload options allows existing file uploads via the standard Choose File dialog.



The file upload functionality is available during imports of items, for diagnostics, and for inventory purposes.

In Privilege Manager, using a robust filtering system is the key to creating accurate and effective Policies.

A filter is made up of specific criteria that Privilege Manager uses to target important file data (or Events) that occur across your environment. You can think of Filters as the core identifiers in your Privilege Manager system. They are used to identify various levels of activity across your organization's computers, including processes (applications) that are launched on computers, who is executing an application, or the state of the computer that the process is being executed on.

An Event in Privilege Manager is any piece of file data or executable on a computer that is targeted by a policy.

There are different methods for Filter-creation and usage, but if you take the time to familiarize yourself with our out-of-the-box filters they can help make your policy-creation process easy. This article will provide details and descriptions for Windows Filters in Privilege Manager and how you can begin using out-of-the-box Filters, or create your own.

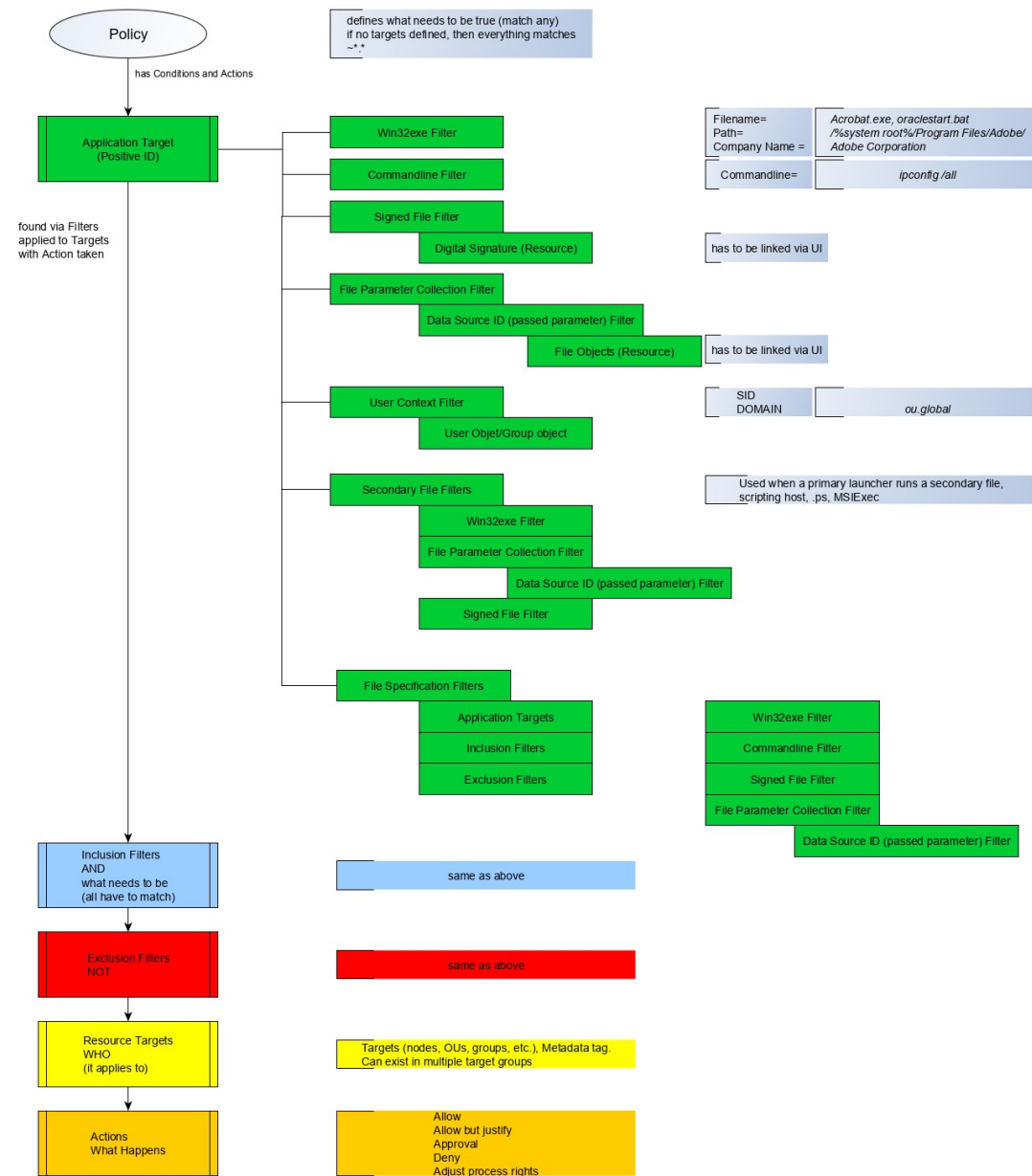
Types of Filters

We recommend leveraging Privilege Manager's out-of-the-box filters to get your policies up and running fast! For a complete list of out-of-the-box filters according to category type, review our Filters' Catalog for Privilege Manager here.

You can search your full list of available filters by navigating to **Admin | Filters** in Privilege Manager. If you already know what you want to target, simply try typing keywords in the search bar to check whether a filter exists that fits your target goal.

Note: If using the default filters provided with Privilege Manager, always verify existing targeting information.

Review the [Filters Catalog for Privilege Manager](#) for details about all out-of-the-box filters shipped with the product.



Create A Copy - How to Use Filter Templates

Out-of-the-Box filters are designed to be used as templates, meaning when you open these filters you will see a **Duplicate** option rather than the option to immediately Edit. These filter templates are protected to provide a jumping off point whenever creating new filters. They are formed by specific criteria that you can tailor according to your specific use case after copying.

Keep in mind that every filter in Privilege Manager - whether or not it is a template - can be leveraged by the Copying feature.

Creating a New Filter Manually

The following are basic steps to create a filter. Based on platform and type the end result shown in this example can be different.

1. In the Privilege Manager console, navigate to **Admin | Filters**.

2. Click **Create Filter**.

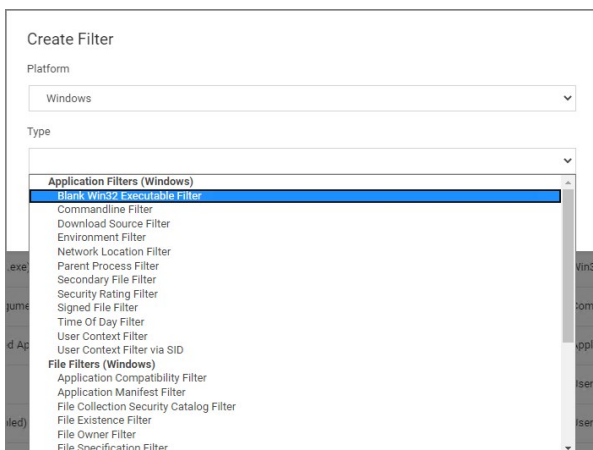
3. On the **Create Filter** modal,

1. select a Platform from the drop-down.



The screenshot shows the 'Create Filter' modal with the 'Platform' dropdown menu open. The dropdown is currently empty, and there are 'Cancel' and 'Create' buttons at the bottom right.

2. select the Type from the drop-down.



The screenshot shows the 'Create Filter' modal with the 'Type' dropdown menu open. The dropdown is currently empty, and there are 'Cancel' and 'Create' buttons at the bottom right.

3. enter a **Name** and **Description**.



The screenshot shows the 'Create Filter' modal with the 'Platform' dropdown set to 'Windows' and the 'Type' dropdown set to 'Blank Win32 Executable Filter'. The 'Name' field contains 'New Win32 Executable Filter' and the 'Description' field is empty. There are 'Cancel' and 'Create' buttons at the bottom right.

4. Click **Create**.

Once the filter is created, the new filter page opens and information under the Details, File Specifications, and File Details sections can be edited. The Save and Cancel buttons appear once you make the first change on the page.

[← Back to Filters](#)

Test 1 Win32 Executable Filter

Details Related items Change History

Refresh More ▾

Filter Details

Name: Test 1 Win32 Executable Filter

Description: doc test filter

Platform: Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name:

File Path:

Include subdirectories

First Discovered: Anytime In the last 0 minute(s)

File Details

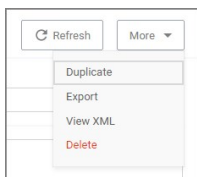
To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character (*) is allowed only at the end. All values specified must match the file detail for the file to be included in the set.

Internal name:

Original filename:

More Options Menu for Filters

The **More** options menu offers users entry points to duplicate, export, view xml, and delete filters that are already on the system.



Creating New Filters using Event Discovery

One way to begin creating new Filters that identify specific files or applications on your network is to set up a Learning Mode Policy and use the events pulled in by Privilege Manager from actions performed on a test machine. Refer to [Event Discovery](#) for more information on setting up a Learning Mode Policy.

1. In Privilege Manager, navigate to **File Inventory**.

The screenshot shows the 'File Inventory' section of the Privilege Manager console. The left-hand navigation pane has 'File Inventory' selected. The main content area shows a table with columns: FILE NAME, ORIGINAL FILE NAME, PRODUCT NAME, PRODUCT VERSION, and FIRST DISC. The first row is highlighted in blue and has a red box around it with the number '2'. To the right, a modal window titled 'New Loaded Resource - 2jmj715...' is open, showing a 'Create Filter' button with a red box around it and the number '3' next to it.

2. Select a recognized event.
3. Click **Create Filter**.

This brings you to the **Manage Application** modal with the known identifiers needed for targeting this specific event auto-populated, for this example chrome.exe.

The 'Manage Application' modal contains the following fields:

- File Name
- File Path
- Internal Name
- Original File Name
- Product Name
- Company Name
- File Version
- Product Version

Buttons at the bottom: , ,

The modal has options to **Create and Add to Policy** or to just **Create Filter**.

Note: If you are NOT directed to such a dialog, this means Privilege Manager doesn't have enough information to target this event yet. In these cases you may need to create Filters manually.

The dialog reveals the available list of building blocks, attributes, or criteria used for creating a filter. In other words, the following list of criteria are possible data fields that Privilege Manager can look and sift through for on any given event that your policies target for Windows machines. Note that criteria can vary depending on the type of filter you are creating:

- File Name
- Path
- Internal Name
- Original File Name
- File Version
- Product Name

- Product Version
- Company Name
- File Signature (File must be signed by)

You can choose which criteria to use by checking or un-checking any of the available check boxes on the dialog. If you are new to the filter creation process, we recommend experimenting with these different identifiers in your test environment to ensure that you are using a comprehensive list of identifiers in your filter, enough to target the application or file intended but not too specific that variations to your target will fall through the filter's criteria hooks.

A Resource Target in Privilege Manager is a specified set of computers that meet certain criteria (e.g., type of operating system or location of the computers), meant to be used as targets for policies or scheduled tasks. To make a policy apply to a certain set of computers, you need a resource target comprising that set of computers and assign that resource target to the policy (or, to state it differently, assign the policy to the resource target).

There are several built-in resource targets (for example, "All 64-bit Windows Computers with Application Control Agent Installed") that can be used when defining policies so that users generally do not need to create custom resource targets. However, there are cases when the latter is needed and, toward that end, this article focuses on user defined resource targets.

This topic also briefly touches upon collections, a concept related to resource targets.

Resource targets are not the only kind of targets that can be assigned to policies; one could also assign an application filter to a policy to make the policy apply to the application file included in the filter.

User Defined Resource Targets

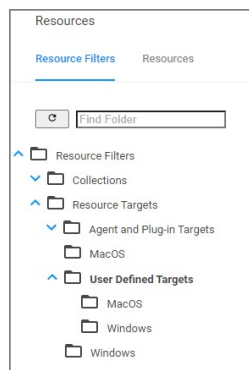
Targets are defined by starting with all known computers and then adding filters to narrow down the set (and after an initial narrowing down, if needed, expand it in some way).

You could create unique targets for all your policies, but if you want to create a target to be reused across multiple policies, it will be more practical to follow these steps.

Interface to View or Create/Modify User Defined Targets

In the Privilege Manager console, navigate to **Admin | Resources**. On the Resources page select the **Resource Filters** tab, then in the tree go to **Resource Filters | Resource Targets | User Defined Targets**, and select either MacOS or Windows.

If you already created user defined targets, you see them listed here and can modify any of them by clicking the name and then editing the definition.



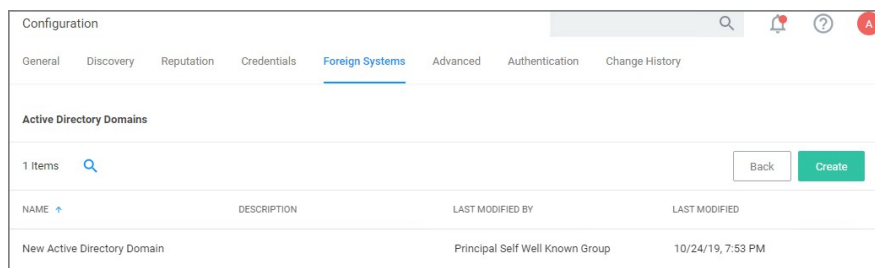
Performance Considerations

Resource Targets are reevaluated when the scheduled task "Collection and Resource Targeting Update" runs. This operation is expensive for large numbers of computers. To keep performance high we suggest that you keep the overall number of targets to a minimum. Also note that targets with simpler definitions are generally less expensive.

Active Directory as Related to Resource Targets

After you have created an Active Directory (AD) instance in Privilege Manager, you need to import computers (computer records, to be more precise).

1. Navigate to **Admin | Configuration | Foreign Systems**.



2. Select your AD instance and navigate to the **Synchronization** tab.

- Under **Import** select which objects you want to import from your AD instance.
 - If you select **Computers**, the default import task also imports the Organization Units (OU) to which the computers belong.
 - If you select **LDAP query**, enter the query in the text field.
- Under **Connectivity** select your import path. Import either directly from the server (as long as a domain controller can be reached on the network) or by using an on-premises computer running the [AD Sync agent](#).
- Click **Save**.

After the task completes, navigate to **Admin | Resources**, select the **Resource** tab. In the tree under **Organizational Views | Active Directory Domains | (your AD name)**, you should be able to see your OUs and computers.

These OUs are what you can select using the "Group" option, for "List Type", when building a target.

Note: Changes made in AD are not immediately reflected in Privilege Manager. Setup scheduled tasks to periodically import changes. The operation can be long-running for large domains, so be careful about the frequency with which you schedule the import.

Assigning Policies to Targets

To assign a policy to your target or better to add your target to a policy, find the policy on the Policies page and edit the **Policy Details**. Use the **Add** and **Edit** options to modify your policy.

< Back to Application Policies

Elevate Privilege Manager Remove Programs Utility Policy

This item is read-only.

General Policy Events Change History Inactive Duplicate More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers
Deployment	Not deployed (Policy is inactive)
Last Modified	Jun 9, 2020, 5:59:38 PM by Trusted Installer
Priority *	2
Description	This policy elevates the security rights for the Privilege Manager Remove Programs ...

Conditions

Refer to the [Policies](#) section to review details about Policy Administration.

Collections

A collection is a predefined list of computers. A collection is often meant to act as a filter and hence is also sometimes referred to as a filter.

Collections are typically defined by an SQL query that returns a list of computer IDs or other resource IDs.

Built-in collections are available in Privilege Manager, for example, "All x64 Windows Computers" and "Domain Controllers."

User defined collections are possible but typically expected to be created by Privilege Manager professional services, on behalf of a user, rather than directly by a user. Users are encouraged to define custom targets using existing (built-in) collections, groups, and fixed lists rather than creating new collections.

When using RegEx in Filters instead of a single file name or file specification, make sure to verify the syntax and test your filter before using it in production.

Examples of program names with versions in file names:

```
(flashutil[ a-zA-Z0-9\.\.]+.exe)
```

```
Winamp58_3660_beta_full_en*us
```

```
(winamp[ a-zA-Z0-9\.\.]+.exe)
```

```
Wiresharkwin642.6.6.exe
```

```
(wireshark*win64[ a-zA-Z0-9\.\.]+.exe)
```

This topic provides the Privilege Manager filters catalog for all out-of-the-box filters that are baked into Privilege Manager and can be used to make your policy configuration process easy.

Win32 Executable Filters

Add Hardware Utility (hdwwwiz.exe)	Filter used to identify the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
AOL Instant Messenger	Filter used to detect AOL Messenger
AppCmd for App Pool Recycling (appcmd.exe)	Filter used to identify the AppCmd executable
Backup and Restore Utility (sdclt.exe)	Filter used to identify the Windows Backup and Restore utility
Chrome	Filter used to detect Google Chrome web browsers
COM Elevation Host Utility (COMElevateHost.exe)	Filter to detect the COMElevateHost. This is used to detect when COM components are being elevated, such as the Network Adapter Properties
Command Processor (cmd.exe)	Filter used to identify the Windows command shell processor
Control Panel Utility (control.exe)	Filter used to identify the process used to launch Control Panel applets
Defragment GUI Utility (dfrgui.exe)	Filter used to identify the disk defragment utility within Windows
Device Pairing Wizard	Filter used to identify the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
Eudora	Filter used to detect Eudora email client
Firefox	Filter used to detect Firefox web browsers
Google Talk	Filter used to detect Google Talk
IIS Manager Executable Filter (inetmgr.exe)	Filter used to identify the IIS Manager executable
IIS Reset Executable Filter (iisreset.exe)	Filter used to identify the IIS Reset executable
Internet Explorer	Filter used to detect Internet Explorer web browsers
ISCSI Executable Filter (iscsipl.exe)	Filter used to identify the ISCSI executable
iTunes	Filter used to detect iTunes
Library Loader Utility (rundll32.exe)	Filter used to identify the dynamic library loader utility used by Windows to launch various system configuration applets
Microsoft Installer File Filter	Filter used to detect the Microsoft Installer. This filter can be used in policies with secondary file filters targeting specific MSI files
Microsoft Management Console (mmc.exe)	Filter used to identify the Microsoft Management Console Utility
Microsoft Windows Media Player	Filter used to detect Windows Media Player
MS Access	Filter used to detect Microsoft Access
MS Excel	Filter used to detect Microsoft Excel
MS FrontPage	Filter used to detect Microsoft FrontPage
MS InfoPath	Filter used to detect Microsoft InfoPath
MS Lync	Filter used to detect Microsoft Lync
MS OIS	Filter used to identify the Office Picture Manager Image Viewer
MS Outlook	Filter used to detect Microsoft Outlook
MS Powerpoint	Filter used to detect Microsoft PowerPoint
MS PPTVIEW	Filter used to detect Microsoft PowerPoint Viewer
MS Publisher	Filter used to detect Microsoft Publisher
MS Visio	Filter used to detect Microsoft Visio
MS VPreview	Filter used to detect Microsoft VPreview
MS Word	Filter used to detect Microsoft Word
MSN Messenger	Filter used to detect MSN Messenger
NLB executable Filter (nlbmgr.exe)	Filter used to identify the NLB Manager executable
ODBC Executable Filter (odbcad32.exe)	Filter used to identify the ODBC executable
Opera	Filter used to detect the Opera Browser
Outlook Express	Filter used to detect Microsoft Outlook Express

Performance Monitor Utility (perfmon.exe)	Filter used to identify the Performance Monitor launcher stub utility within Windows
Powershell (powershell.exe)	Filter used to identify the Windows Powershell command processor
Printer Control Utility (printui.exe)	Filter used to identify the printer management applet launcher within Windows
QuickTime	Filter used to detect QuickTime
RealPlayer	Filter used to detect RealPlayer
Resource Monitor (resmon.exe)	Filter used to identify the Windows Resource Monitor application
Safari	Filter used to detect Apple Safari on Windows
Scripting Host (cscript.exe)	Filter used to identify the Windows Scripting Host command-line utility
Scripting Host (wscript.exe)	Filter used to identify the Windows Scripting Host commandline utility
Setup Display Languages Utility (lpksetup.exe)	Filter used to identify the Install/Uninstall of Display Languages setup utility for Windows
ShareX	This filter targets the ShareX application
Skype	Filter used to detect Skype
Trillian	Filter used to detect the Trillian application
User's Temp Directory Win32 Executable Filter	Filter used to target any executable (exe) in a user's temp directory
Win32 Executables Discovered in the Last Week	This filter is limited to applications discovered on the endpoint within the last week
Winamp	Filter used to detect Winamp application
Windows Firewall (netsh.exe)	Filter used to identify the Windows Firewall netsh.exe
Windows Messenger	Filter used to detect Windows Messenger
Yahoo! Messenger	Filter used to detect Yahoo Messenger

Commandline Filters

Filter | Description | ----- | Add Printer Commandline Arguments | Filter used to identify the Add Printer UI applet | Azman.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Authorization Manager | Backup and Restore Commandline Arguments | Filter used to identify the Backup and Restore component, used as a commandline argument to a process | Certmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Certificate Manager | Ciadv.msc Commandline Filter for MMC Snap-In | Filter used to detect Indexing Service Management | Compmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Computer Management | Dfragmgt.msc Commandline Filter for MMC Snap-In | Filter used to detect the MMC Snap-in used to defragment disks in Windows XP | Devmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Device Manager | Dhcpmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect DHCP Management | Diskmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Disk Management | Dnsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect DNS Management | Eventvwr.msc Commandline Filter for MMC Snap-In | Filter used to detect Event Viewer | Fsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Shared Folders Management | Fsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect File Resource Manager | Gpedit.msc Commandline Filter for MMC Snap-In | Filter used to detect Group Policy Editor | Hardware Wizard Applet | Filter used to identify a commandline argument referring to the Control Panel applet used to add new hardware | Lusrmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Local User and Group Management | Napclfcfg.msc Commandline Filter for MMC Snap-In | Filter used to detect NAP Client Configuration | Network Adapter Elevate Attempt | Filter used to detect when a user right-clicks on a network adapter and selects Properties | Ntmsmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Removable Storage Manager | Performance Monitor Component (perfmon.msc) | Filter used to detect Performance Monitor | Printmanagement.msc Commandline Filter for MMC Snap-In | Filter used to detect Print Management | Recycle App Pool Commandline | Filter used to identify the recycle command for application pools | Rsop.msc Commandline Filter for MMC Snap-In | Filter used to detect Resultant Set of Policy | Secpol.msc Commandline Filter for MMC Snap-In | Filter used to detect Local Security Settings Manager | Services.msc Commandline Filter for MMC Snap-In | Filter used to detect Services Manager | Sqlservermanager12.msc Commandline Filter for MMC Snap-In | Filter used to detect SQL Server Manager | System Control Panel Applet | Filter used to identify a commandline argument referring to the Control Panel applet used to change the system time and date settings | Tpm.msc Commandline Filter for MMC Snap-In | Filter used to detect Trusted Platform Module Management | Wbadmin.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Server Backup | Wf.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Firewall Management | Wmiingmt.msc Commandline Filter for MMC Snap-In | Filter used to detect WMI Management |

Environment Filters

Manual Application Compatibility Setting	Detects whether an application is being run with manual override options
User Access Control Consent Dialog Detected	This filter will match when an application that requires User Access Control consent is launched
User Requested Run As Administrator	Detects whether a user has right-clicked on an application and used Thycotic's custom 'Request Run as Administrator' option

Network Location Filters

Disconnected from Network	Filter used to detect when the computer is not attached to a network
Domain Network Location Filter	Filter used to detect when the computer is attached to a network classified as domain
Private Network Location Filter	Filter used to detect when the computer is attached to a network classified as private
Public Network Location Filter	Filter used to detect when the computer is attached to a network classified as public

Parent Process Filters

Thycotic Copy/Installer Helper Parent Process Filter	Filter used to detect when a user attempts to copy a file using the Privilege Manager copy helper
---	---

--

Secondary File Filters

Target MSI and Scripts executed from the User's Temp Directory Filter used to target MSI and Scripts executed from the User's Temp Directory

Security Rating Filters

VirusTotal This filter will target VirusTotal for Reputation Checking
VirusTotal-Bad Rating This filter will target VirusTotal for Reputation Checking
VirusTotal-Clean Rating This filter will target VirusTotal for Reputation Checking
VirusTotal-Suspect Rating This filter will target VirusTotal for Reputation Checking

VirusTotal Filters based on configuring VirusTotal integration in Privilege Manager. For steps to do this, see our [VirusTotal Integration Guide here](#)

Time of Day Filters

Business Hours (8:30AM to 5:30PM) This filter is limited to 8AM to 6PM weekdays
Business Hours (8AM to 6PM) This filter is limited to 8AM to 6PM weekdays
Business Hours (9AM to 5PM) This filter is limited to 9AM to 5PM weekdays
Weekends This filter is limited to weekends

User Context Filters

Administrators Detects when an application is running with elevated (administrator) permissions
Administrators (Include Disabled) Detects when an application has an administrator user token

File Filters

Application Compatibility File Filters

Administrative Rights Required Application Compatibility Filter This filter tests whether Windows has detected that this executable requires administrative rights
Generic Installer Detection Filter This filter indicates that Windows has detected that an executable is an Application Setup
Highest Available Application Compatibility Filter This filter tests whether Windows has detected that this executable required highest available rights
Specific Installer Detection Filter This filter indicates that Windows has detected that an executable is an Application Setup
Specific Non Installer Detection Filter This filter indicates that an executable has been flagged as not being an Application Setup

Manifest Filters

Require Administrator Rights Manifest Filter This filter tests whether an executable is marked as requiring Administrative rights
Require Highest Available Rights Manifest Filter This filter tests whether an executable is marked as requiring highest available rights
Manifest Present Filter This filter tests whether an executable has a security manifest

File Owner Filters

System (Wheel) File Owner Files that are owned by the Wheel Group (Unix)
System File Owner Filter Filter used to detect files owned by the System account
Trusted Installer File Owner Filter Filter used to detect files owned by the Trusted File Owner account

File Specification Filters

--

Any Package (MacOS)	Target .pkg and .mpkg files
App Store Preference Pane (MacOS)	Filter used to detect App Store Preference Pane in Mac
Common Executable Folders	Filter used to detect files in common executable directories, such as C:\Windows, C:\Program Files, and C:\Program Files(x86)
Date and Time Preference Pane (MacOS)	Date and Time Preference Pane (MacOS)
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS
Default File Specification (All executable types)	Specifies all executable file types in Windows and Program files
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS
Default File Specification (Windows)	This specifies executables in Windows and Program files
Documents and Settings	Filter used to detect files in the Downloaded Program Files directory
Drivers	Filter used to detect files in the C:\Windows\System32\drivers directory
Energy Saver Preference Pane (MacOS)	Filter used to detect the Energy Saver Preference Pane in Mac
Executables in Windows Directories	This specifies executables in Windows directories
Executables in Windows Directories (All executable types)	Specifies all executable file types in Windows directories that are not present in a signed security catalog
Mac OS/Users/File Specification	The default filter for files in the /Users/ directory on MacOS
Network Drive Filter	Specifies files present on network file systems
Optical Drive Filter (CD/DVD)	Specifies files present on optical drives (CD/DVD)
Parental Controls Preference Pane (MacOS)	Filter used to detect the Parental Controls Preference Pane in Mac
Printers and Scanners Preference Pane (MacOS)	Filter used to detect the Printers and Scanners Preference Pane in Mac
Program Data	Filter used to detect files in the C:\ProgramData\ directory
Program Files	Filter used to detect files in the C:\Program Files\ directory
Program Files (x64 on Win32)	Filter used to detect files in the C:\Program Files\ directory
Program Files (x86)	Filter used to detect files in the C:\Program Files(x86)\ directory
Removable Drive Filter	Filters files present on removable drives such as Floppy Drives and USB devices
Security and Privacy Preference Pane (MacOS)	Filter used to detect Security and Privacy Preference Pane in Mac
Sharing Preference Pane (MacOS)	Filter used to detect the Sharing Preference Pane in Mac
System Catalog Folder	Filter used to detect files in the CatRoot directory
System Preferences (MacOS)	Filter used to detect the System Preferences Preference Pane in Mac
Temporary ASP.NET 1.0 Files	Filter used to detect files in the .NET 1.0 Temp directory
Temporary ASP.NET 1.1 Files	Filter used to detect files in the .NET 1.1 Temp directory
Temporary ASP.NET 2.0 Files	Filter used to detect files in the .NET 2.0 Temp directory
Temporary Files	Filter used to detect files in the C:\Windows\Temp directory
Thycotic Copy/Installer Helper Application	Filter used to detect usage of the Privilege Manager copy helper
Time Machine Preference Pane (MacOS)	Filter used to detect the Time Machine Preference Pane in Mac
Uncommon Executables Folders	Filter used to detect files in the Uncommon directories
Users and Groups Preference Pane (MacOS)	Filter used to detect the Users and Groups Preference Pane in Mac
User's Directory Collection File Specification Filter	Used to target any file in the user's temp directory
User's Downloads Directory File Specification Filter	Used to target any file in the user's temp directory
User's Temp Directory File Specification Filter	Used to target any file in the user's temp directory
Windows Directory	Filter used to detect files in the C:\Windows directory
Windows Directory (Include Subdirectories)	Filter used to detect files in the C:\Windows\ directory
Windows Dll Cache	Filter used to detect files in the C:\Windows\System32\dlldata directory
Windows Side By Side	Filter used to detect files in the C:\Windows\WinSxS\ directory
Windows Software Distribution	Filter used to detect files in the Windows Software Distribution directory
Windows\System32	Filter used to detect files in the C:\Windows\System32 directory

Windows\System32 (Include Subdirectories)	Filter used to detect files in the C:\Windows\System32\ directory
Windows\SysWOW64	Filter used to detect files in the SysWOW64 directory
Windows\SysWOW64 (Include Subdirectories)	Filter used to detect files in the SysWOW64\ directory

Security Catalog Filters

Present In Signed Security Catalog	Filter used to detect Operating System Files and other trusted files dynamically on each system by using that machine's Signed Security Catalog. This filter does not need to be modified on the server
---	---

Miscellaneous Filters

App Bundle Filters

All Application Bundles Filter (MacOS)	Filter used to detect All Applications Bundles
---	--

Coff Header Filters

32-bit Executables	Filter used to detect files with the 32-bit executable machine type header set
All Executable Types	This filter includes all executable types
Commandline Executables	Filter used to detect files with the Windows console subsystem header set
GUI Executables	Filter used to detect files with the GUI header set
Native Executables	Filter used to detect files with the executable header set
Windows CE Executables	Filter used to detect files with the Windows CE Subtype header set
Program File Executables	Filter used to detect files with the executable or DLL header set
Posix Executables	Filter used to detect files with the POSIX header set
X64 Executables	Filter used to detect files with x64 machine type header set

File Parameter Collections

All Deny List Security Rated Applications	This collection contains all applications that have been denylisted by applying a security rating
All Executables Discovered in Last 2 Weeks	Filter used to detect files that have been discovered by the server in the past 2 weeks
All Executables Discovered in Last Day	Filter used to detect files that have been discovered by the server in the past day
All Executables Discovered in Last Week	Filter used to detect files that have been discovered by the server in the past week
All Executables Discovered in Last Month	Filter used to detect files that have been discovered by the server in the past month
All Greylist Security Rated Applications	This collection contains all applications that are being monitored.
All Unclassified Applications	This collection contains all applications that have not been classified by a security rating
All Allow Listed Security Rated Applications	This collection contains all applications that have been allowed by applying a security rating

Mach-O Header Filters

macOS DyLib	Identifies dynamic library (dylib) files according to their embedded Mach-O header (not specifically according to file name)
macOS Executables	Identifies files marked as executables according to their Mach-O header (not file mode changes via chmod)

Filter Types and Descriptions

There are different types of filters. When creating a new filter for Windows or macOS, the "Filter Type" drop-down gives you a list of options that include the categories:

- [Application Filters](#)
- [File Filters](#)
- [Inventory Filters](#)
- [macOS Specific Filters](#)

These are loose groupings that signify a few different approaches to the filtering method or targets.

Common Filter Characteristics

Each filter has a Details area that contains the filter name, description, and platform association. These details are usually specified when you create the filter, either by choosing **Create Filter**, editing an existing filter, or duplicating an existing filter.

Those characteristics are used for searches or filtering and allow users to easily find existing filters.

Filter Change History

Each filter has a **Change History** tab, where audit information can be reviewed from the time the filter was created in the system.

Details	Membership	Related Items	Change History
3 Items			Select an item to view details
Wednesday June 24, 2020			
TEST-System1\JohnDoe Saved item: Uses DataSource : Hash Based Query , made 3 other... DocTest File Collection of Hashes Filter			2:04 PM

Refer to [Change History](#) to learn more about drilling down into the change history of resources and the report.

How to Search for Filters

All out-of-the-box filters can be searched, duplicated, and then customized to be used in policies.

1. Navigate to **Admin | Filters**.

NAME	DESCRIPTION	TYPE	SUPPORTED
.bat file filter	filter for batch files	Secondary File Filter	Windows

The list of all filters is sortable by Name (default), Description, Type, and OS Support.

You may limit your list output, by changing from the default **All** or Supported selection for macOS or Windows to Not Supported.

<input checked="" type="checkbox"/> All	
<input type="checkbox"/> Supported	ter
<input type="checkbox"/> Not Supported	ter

2. Using the search option next to the OS drop-down, lets you search the list contents based on the column the contents is sorted by. So if your list is sorted by **Name**, but you are looking for all commandline filter types you have in the system, sort your list by **Type** first.
3. Then click **Search** and enter a search term, for this example *commandline*.

NAME	DESCRIPTION	TYPE
Commandline Executables	Filter used to detect files with the Windows console subsystem head...	Coff Header Filter
Add Printer Commandline Arguments	Filter used to identify the Add Printer UI applet.	Commandline Filter
azman.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Authorization Manager	Commandline Filter
Backup and Restore Commandline Arguments	Filter used to identify the Backup and Restore component, used as a ...	Commandline Filter

You can also use the search option on the top-right from any page of your Privilege Manager console and get the a list of commandline filters returned. If you use this search option, the search field does not retain your search term. The results are based on the search term matching the Name and/or Type, so the list will contain more items than searching based on column selection.

Search Results for Commandline Filter

32 Items Type: All

NAME	TYPE	MODIFIED	DESCRIPTION
azman.msc Commandline Filter for MMC Snap-in	Commandline Filter	6/15/20, 6:53 AM	Filter used to detect Windows Authorization Manager
certmgr.msc Commandline Filter for MMC Snap-in	Commandline Filter	6/15/20, 6:53 AM	Filter used to detect Windows Certificate Manager
ciadv.msc Commandline Filter for MMC Snap-in	Commandline Filter	6/15/20, 6:53 AM	Filter used to detect Indexing Service Management
Commandline Filter	Xml Item Template	6/15/20, 6:53 AM	

The columns returned for this search are sorted by Name (default), Type, Modified Date, and Description.

Application Filters

These generally target specific executables or things about the environment. These types of filters can be used to limit policies to a certain time of day, the parent process of an application, the security rating of an application, or the user or group running the process.

The following Application Filter type filter topics are available:

- [Blank Win32 Executable Filter](#)
- [Commandline Filter](#)
- [Download Source Filter](#)
- [Environment Filter](#)
- [Network Location Filter](#)
- [Parent Process Filter](#)
- [Secondary File Filter](#)
- [Security Rating Filter](#)
- [Signed File Filter](#)
- [Time Of Day Filter](#)
- [User Context Filter / User Context Filter via SID](#)

Blank Win32 Executable Filter

Identifies specific application files by specifications like name, path, and when first discovered.

← Back to Filters

🔍
🔔
?
A

Test 1 Win32 Executable Filter

Refresh
More ▾

Filter Details

Name	<input type="text" value="Test 1 Win32 Executable Filter"/>
Description	<input type="text" value="doc test filter"/>
Platform	Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name	<input type="text"/>
File Path	<input type="text"/>
	<input type="checkbox"/> Include subdirectories
First Discovered	<input checked="" type="radio"/> Anytime <input type="radio"/> In the last 0 minute(s)

File Details

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character (*) is allowed only at the end. All values specified must match the file detail for the file to be included in the set.

Internal name	<input type="text"/>
Original filename	<input type="text"/>

Parameters

Win32 Executable filters have two sets of parameters:

- **File Specifications**, such as
 - File Name
 - File Path with option to include subdirectories
 - First Discovered, which can be specified as "Anytime" or "In the last" either Minutes, Hours, Days, or Weeks.
- **File Details** (common attributes), such as
 - Internal name
 - Original filename
 - File version
 - Product name
 - Product version
 - Company name
 - Copyright (version 10.7 and up)

Examples

Used to target specific applications, for example allowing `acrobat.exe` or `notepad++.msi` to be used on endpoints.

Commandline Filter

These filters will perform an exact, partial or regex match on the commandline of the process. Privilege Manager comes with default commandline filter types, which are all read-only, but can be copied to be customized.

This filter is available for both Windows and macOS systems.

Search for Commandline Filters

1. Navigate to **Admin | Filters**.
2. In the search field for the **Type** column enter commandline.

NAME	DESCRIPTION	TYPE
Commandline Executables	Filter used to detect files with the Windows console subsystem head...	Coff Header Filter
Add Printer Commandline Arguments	Filter used to identify the Add Printer UI applet.	Commandline Filter
azman.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Authorization Manager	Commandline Filter
Backup and Restore Commandline Arguments	Filter used to identify the Backup and Restore component, used as a ...	Commandline Filter

3. Select a filter to view its details and/or use **Duplicate** to customize the filter.

eventvwr.msc Commandline Filter for MMC Snap-in

This item is read-only.

Details | Related Items | Change History | Duplicate

Filter Details	Name	Value
	Name	eventvwr.msc Commandline Filter for MMC Snap-in
	Description	Filter used to detect Event Viewer

Settings	Match Type	Value
	Match Type	Partial Match
	Command Line	eventvwr.msc

If you Duplicate (make a copy of an existing) filter, "rename" the filter and click **Create**.

Create a copy of eventvwr.msc Commandline Filter for MMC Snap-in

Name

Copy of eventvwr.msc Commandline Filter for MMC Snap-in

Cancel Create

Create a new Commandline Type Filter

1. Navigate to **Admin | Filters**.
2. Click **Create Filter**.
3. On the New Filter page, select the platform. For this example, select **Windows**.
4. From the **Filter Type** drop-down select **Commandline Filter**.
5. Enter a name and description and click **Create**.

Create Filter

Platform

Type

Name *

Description

6. Customize the newly created filter.

[Back to Filters](#)

New Commandline Filter

[Details](#)
[Related Items](#)
[Change History](#)

Filter Details	Name	<input type="text" value="New Commandline Filter"/>
	Description	<input type="text"/>
	Platform	Windows
Settings	Match Type	<input type="text" value="Exact Match"/> <ul style="list-style-type: none"> Exact Match <li style="background-color: #007bff; color: white;">Exact Match Partial Match Regular Expression
	Command Line	<input type="text"/>

1. Under **Settings**.

1. Set the **Match Type**. This can be either an exact or partial match or specified as a regular expression.
2. Enter the commandline to match.

7. Click **Save Changes**.

Parameters

Commandline Filters have one section to set the parameters for the filter.

The **Match Type** gives you the options:

- Exact Match
- Partial Match
- Regular expression

Command Line:

- This is the section where you enter in the given command parameters to pull up the file or action.

Examples

A commandline filter examines the commandline (excluding the primary executable) and applies a pattern match (Exact, Partial or Regular Expression).

For example allowing /FlushDNS as a command for IPConfig.

Download Source Filter

The filter checks where a file is being downloaded from. This filter allows you to identify specific download sources, and allows the ability to allow list sources you trust or block sources you don't. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Both Windows / Mac OS

Type
Download Source Filter
Security Rating Filter
Signed File Filter
Time Of Day Filter

This filter is available for both Windows and macOS systems.

< Back to Filters

New Download Source

Details Related Items Change History Refresh More

Filter Details

Name New Download Source

Description

Platform Windows, Mac OS

Settings

This filter checks for the existence of download source information associated with a file.

Include files that contain any download source information
 Include files that contain specific download source information

Match Type Exact Match

Host

Parameters

The filter checks for the existence of download source information associated with a file.

Settings:

- Include files that contain any download source information
- Include files that contain specific download source information
- Match type
- Host

Examples

This filter would allow you to control what download sources should be allowed or blocked.

Environment Variable Filter

This type of filter can target environment variables of a process that is started.

[← Back to Filters](#)

New Environment Variable Filter

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Filter Details	Name	<input type="text" value="New User Requested Run As Administrator"/>
	Description	<input type="text" value="Detects whether a user has right-clicked on an application and used Privilege Manager's custom 'Request Run as Administrator' option."/>
	Platform	<input type="text" value="Windows"/>

Settings	Name	<input type="text" value="ACSRUNASADMIN"/>
	Value	<input type="text"/>
	Match Type	<input type="text" value="Partial Match"/>

Parameters

- Name
- Value
- Match Type:
 - Exact Match
 - Partial Match
 - Regular expression

Examples

A environment variable filter type detects whether a user has right clicked on an application and used Privilege Manager's custom *Request Run as Administrator* option.

Network Location Filter

This type of filter identifies a computer's connection to specific networks like public, private, or unclassified networks.

[Back to Filters](#)

🔔
?
A

New Network Location Filter

Details
Related Items
Change History

Refresh

More ▾

Filter Details

Name	<input type="text" value="New Network Location Filter"/>
Description	<div style="border: 1px solid #ccc; height: 20px;"></div>
Platform	Windows

Settings

Only allow network connections of type No Public ▾

Network Connectivity

Include connections where

<input checked="" type="radio"/> IPv4 Internet	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv4 Local Network	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv4 Subnet	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv4 No Traffic	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv6 Internet	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv6 Local Network	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv6 Subnet	<input type="text" value="undetected"/>
<input checked="" type="radio"/> IPv6 No Traffic	<input type="text" value="undetected"/>
Results should be	<input type="text" value="included"/>

Parameters

You can adjust the following setting options for Network Location filters:

- **Only allow network connections of type:**

- Public
- Private
- Domain

- **Network Connectivity:**

- IPv4 and IPv6 options for connectivity

- **Results should be:**

- Included or excluded

Examples

Some examples of this filter can be set to detect:

- when the computer is not attached to a network
- when the computer is attached to a network classified as public
- when the computer is attached to a network classified as domain

Parent Process Filter

This type of filter can identify parent processes of certain executables.

[Back to Filters](#)

New Parent Process Filter

Search [] Notifications [] Help [] Profile [A]

[Details](#) [Related Items](#) [Change History](#) [Refresh](#) [More](#)

Filter Details

Name:

Description:

Platform:

Settings

Applications: [Add Applications](#)

Conditional (optional)

Include Only Filters ⓘ [Add Include Only Filters](#)

Exclude Any Filters ⓘ [Add Exclude Any Filters](#)

This filter is available for both Windows and macOS systems.

Parameters

- Applications
- Conditions
- Include only filters
- Exclude any filters

Examples

This filter is used to detect when a user attempts to copy a file using the Privilege Manager copy helper.

Using Secondary File Filters

This topic explains how to create policies for applications that trigger file executions. Implementing a policy to filter on a file type, which is used by another executable, is done by setting a **Secondary File Filter**. The Secondary File Filter is available for both Windows and macOS systems.

The following topics show the steps to create policies and include filters that enforce actions on endpoints when batch files, PowerShell scripts, or Microsoft Installer files execute. Any type of executer can be specified and policed this way.

In general, the steps are similar for the different file types to be policed.

Via File Inventory

- With Learning Mode enabled, you use the File Inventory to discover new resources.
- Select a discovered resource and use **Create Filter**.
- On the Manage Application modal select which specifications to match.
- Use **Create and Add to Policy** option.

Via Policy Wizard

- You create a controlling policy via the Wizard.
- On the **What do you want to target step?** you can select an existing filter, upload a file (recommended for .msi/.exe applications), or use an already inventoried file.
- Policy Wizard builds the policy and after you name and create it, you can further customize all the details. The Policy wizard automatically adds the correct application targets, inclusions an/or exclusions.

Examples

- [Best Practices](#)
- [Targeting script file execution, like .bat and .ps1](#)
- [Targeting installer/executables execution, like .msi and .exe](#)

Best Practice Using a Secondary File Filter

Using File Inventory

As a best practice you create an elevate policy with a priority of X (for example 85) to elevate or allow specific scripts or files to run. Then you add a policy with a priority of X+1 to deny any other execution of the command processor, PowerShell, or Microsoft installer files. For this example, .msi is used.

1. In the Privilege Manager Console under **Computer Groups** navigate to **File Inventory**.
2. From the list of discovered resources, we are selecting our example TortoiseGit.

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCO
updater.exe	updater.exe	Firefox	76.0.1.7432	6/29/20,9
firefox.exe	firefox.exe	Firefox	76.0.1.0	6/29/20,9
CompatTelRunner.exe	CompatTelRunner.exe	Microsoft® Windows® Operating System	10.0.18362.1035	6/29/20,9
DeviceCensus.exe	DeviceCensus.exe	Microsoft® Windows® Operating System	10.0.18362.1035	6/29/20,9
TortoiseGit-2.8.0.0-64bit.msi				6/26/20,7
New Loaded Resource 6/26/2020 7:06:17 PM				
test.ps1				6/26/20,5
test.bat				6/26/20,5
chrome.exe	chrome.exe	Google Chrome	83.0.4103.116	6/25/20,1
ChromeSetup.exe	GoogleUpdateSetup.exe	Google Update	1.3.34.3	6/25/20,1
RExD3E6.exe	RestartExplorer.exe	RestartExplorer	2.8.0.0	6/25/20,1
opera_autoupdate.exe		Opera auto-updater	68.0.3618.173	6/25/20,1
assistant_installer.exe		Opera Browser Assistant Installer	69.0.3686.36	6/25/20,1
installer.exe	Opera Installer		68.0.3618.173	6/25/20,1

3. Click **Create Filter**.

4. On the Manage Application page, check the **File Name** and **Signed By** checkboxes.

Manage Application

File Name

File Path

Signed By [Edit](#)

Hash

5. Click **Create Filter**.

Back to File Inventory

TortoiseGit-2.8.0.0-64bit.msi Secondary Filter

Details Related Items Change History

Filter Details

Name

Description

Platform Windows

Settings

The selected filters will be applied to the target application. The target file is taken from the command-line of the application.

Filters [Wizard Generated File Specification Filter for 'TortoiseGit-2.8.0.0-64bit.msi'](#) [Edit](#)

6. Navigate to **Computer Groups | Windows Computers**.

7. Select **Application Policies**.
8. Click **Create Policy**.
9. In the policy wizard select **Controlling**, click **Next Step**.
10. In the policy wizard select **Allow**, click **Next Step**.
11. In the policy wizard select **Specific Applications**, click **Next Step**.
12. In the policy wizard select **Existing Filter**, click **Next Step**.
 1. Search for and add the secondary file filter created from the file inventory above.
 2. Click **Update**.
13. On the policy wizard page that now lists the existing filter, click **Next Step**.

What do you want to target?

Existing Filter
Add existing filters to this new policy

File Upload
Upload a file to create a filter that targets it

Inventoried File

Selected Filters

Existing Filter

TortoiseGit-2.8.0.0-64bit.msi Secondary ... [Remove](#)

14. Name the policy and click **Create Policy**.

Finalize this Policy

Name *

Description

Priority *

[Create Policy](#)

The policy wizard added based on the selected filter the application target to allow the TortoiseGit application.

Allow TortoiseGit Application Policy

General Policy Events Change History

Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) [Windows Computers](#) [Add](#)

Deployment Not deployed (Policy is inactive)

Last Modified Jun 30, 2020, 7:01:12 PM by test-lab-docs\Administrator

Priority *

Description

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted [TortoiseGit-2.8.0.0-64bit.msi](#) [Secondary Filter](#) [Edit](#)

Inclusions [Add Inclusions](#)

Exclusions [Add Exclusions](#)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.

Actions [Add Actions](#)

Child Actions [Add Child Actions](#)

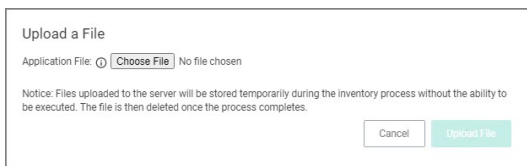
Executables File Example

In this example we are creating a policy to deny running .msi files.

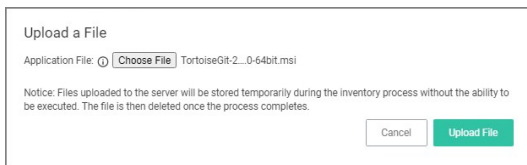
Creating the Policy

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Block**, click **Next Step**.
6. In the policy wizard select **Notify and Block**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **File Upload**.


1. On the Upload a File modal, Click **Choose File**.



2. Select the file(s) you wish to be targeted. For this example we are selecting a TortoiseGit installer package.



3. Click **Upload File**.
4. On the Manage Application dialog, check **File Name**.



Select more details like the File Path or the Hash, if you want to make this policy more specific.

5. Click **Create Filter**.

The screenshot shows a web interface for selecting filters. The main area is titled "What do you want to target?" and contains three selectable options: "Existing Filter" (Add existing filters to this new policy), "File Upload" (Upload a file to create a filter that targets it), and "Inventoried File" (Create a new filter from a file that was discovered during File Inventory). A "Next Step" button is located at the bottom right. On the right side, a "Selected Filters" sidebar is visible, showing the "Existing Filter" section with a "Wizard Generated File Specification Filter for Tortol..." and a "Remove" link.

6. Click **Next Step**.

9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 10, since it is a deny and notify policy.

The screenshot shows the "Finalize this Policy" page. The main area contains three input fields: "Name *" with the value "deny [tortoise] msi execution", "Description" with the value "This policy blocks the specified executables from running", and "Priority *" with the value "10". At the bottom left is a "Previous Step" button and at the bottom right is a "Create Policy" button. On the right side, a sidebar provides instructions for the "Name", "Description", and "Priority" fields. The "Name" field instruction says "Name this policy so you can recognize it among your list of other policies". The "Description" field instruction says "Explain what this policy is doing, what processes it targets, and its effect on end users." The "Priority" field instruction says "Policies are evaluated in numerical order, where 1 is first (highest priority) and larger numbers are last (lowest priority). When choosing a priority number, you must be aware of all other policies that are defined and the order in which they are called by the agent."

10. Click **Create Policy**.

< Back to Packages for 'deny tortoisegit.msi execution'

deny tortoisegit.msi execution

General Policy Events Change History

Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted ¹ (1 total endpoints)
Windows Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jun 30, 2020, 4:18:31 PM by WIN-E6GKPM7J77F\Administrator

Priority *

Description

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
[Filters](#)

Applications Targeted Microsoft Installer File Filter Edit

Inclusions Packages for 'deny tortoisegit.msi execution' Edit

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy
[Actions](#)

Actions Application Denied Message Action Edit

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

Show Advanced

The policy wizard added based on the selected file upload and the file inventory that was executed and application target of Microsoft Installer Files.

A secondary file filter was added under Inclusions, identifying a specific file filter for the tortoisegit.msi execution.

Script Execution File Example

In this example we are creating a policy to deny running a batch or ps1 file, which the policy targets through a secondary file filter.

This example is for a Windows endpoint, but the policy can be created in the same way for a macOS system.

Creating the Policy

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Block**, click **Next Step**.
6. In the policy wizard select **Notify and Block**, click **Next Step**.
7. In the policy wizard select **Script**, click **Next Step**.
8. In the policy wizard select **File Upload**.

1. On the Upload a File modal, Click **Choose File**.

Upload a File

Application File: No file chosen

Notice: Files uploaded to the server will be stored temporarily during the inventory process without the ability to be executed. The file is then deleted once the process completes.

2. Select the file(s) you wish to be targeted. For this example we are first uploading a test.bat and then test.ps1 file. You need to run through the upload and manage application steps twice, once for each file you are uploading.

Upload a File

Application File: test.ps1

Notice: Files uploaded to the server will be stored temporarily during the inventory process without the ability to be executed. The file is then deleted once the process completes.

3. Click **Upload File**.
4. On the Manage Application dialog, check **File Name**.

Manage Application

File Name

File Path

Hash

Select more details like the File Path or the Hash, if you want to make this policy more specific.

5. Click **Create Filter**.

Policies

What do you want to target?

Existing Filter
Add existing filters to this new policy

File Upload
Upload a file to create a filter that targets it

Inventoried File
Create a new filter from a file that was discovered during File Inventory

Selected Filters

Existing Filter

File Upload
Wizard Generated File Specification Filter for 'test.bat' [Remove](#)
Wizard Generated File Specification Filter for 'test.ps1' [Remove](#)

Inventoried File

6. Click **Next Step**.

9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 10, since it is a deny and notify policy.

Finalize this Policy

Name *

Description

Priority *

[Create Policy](#)

Name
Name this policy so you can recognize it among your list of other policies

Description
Explain what this policy is doing, what processes it targets, and its effect on end users.

Priority
Policies are evaluated in numerical order, where 1 is first (highest priority) and larger numbers are last (lowest priority). When choosing a priority number, you must be aware of all other policies that are defined and the order in which they are called by the agent.

10. Click **Create Policy**.

deny and notify about test.bat and test.ps1 script file

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) Windows Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jun 30, 2020, 3:47:34 PM by WIN-E6GKPM7J7TF\Administrator

Priority * 10

Description This policy blocks the specified executables from running

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

Applications Targeted Command Processor (cmd.exe) Edit
PowerShell (powershell.exe)
Scripting Host (cscript.exe)
Scripting Host (wscript.exe)

Inclusions Scripts for 'deny and notify about test.bat and test.ps1 script file' Edit

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. Actions

Actions Deny Execute Edit
Deny Execute Message

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

Show Advanced

The policy wizard added based on the selected file uploads and the file inventory that was executed 4 types of application targets:

- Command Processor (cmd.exe)
- Powershell (powershell.exe)
- Scripting Host (cscript.exe)
- Scripting Host (wscript.exe)

A secondary file filter was added under Inclusions, identifying two specific file filters for the test.bat and test.ps1 files.

Verifying the Policy Works

1. Add a test.bat file with a simple Hello World command to your system.

1. Create a new text file and add

```
ECHO OFF
ECHO Hello World
PAUSE
```

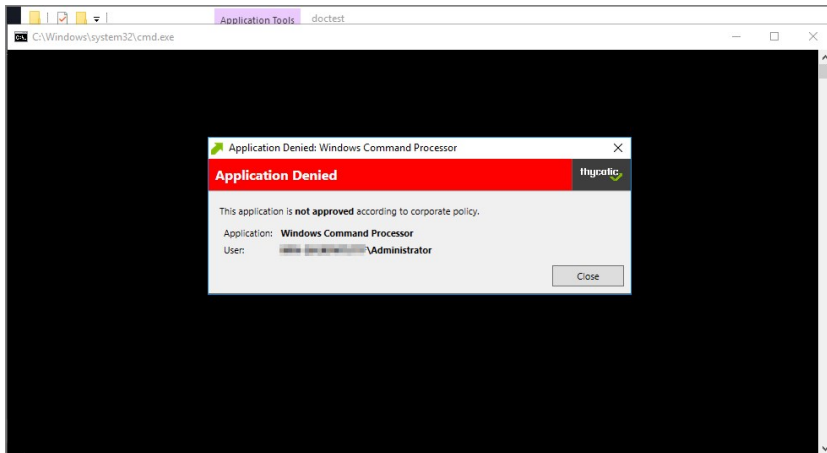
2. Save the file as test.bat.

2. With your policy set to **active**, double-click the test.bat file.

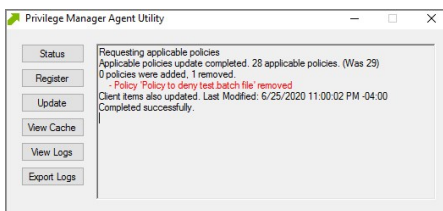
Block ^

Policy to deny test.batch file	Priority 10	Active
--------------------------------	-------------	--------

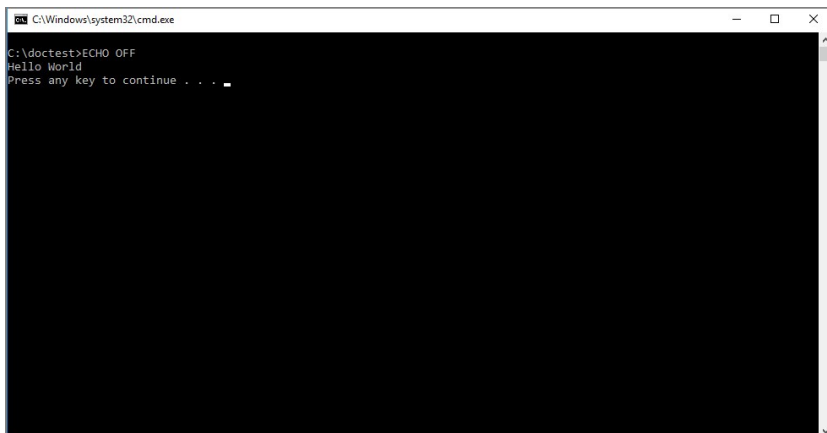
The policy triggers the specified message action:



3. With your policy set to **Inactive**, verify via Agent Utility that the update was received and the policy was removed:



4. Double-click the test.bat file.



The batch file is executed and Hello World is printed to the cmd.exe output window.

Security Rating Filter

If you have integrated Privilege Manager with a Reputation Checking provider like VirusTotal, these filters allow you to look up a rating for a file or application (is it good, bad, suspect/suspicious, or unknown).

Create Filter

Platform

Type

Name *

Description

Security rating system *

This filter is available for both Windows and macOS systems.

Parameters

[Back to Filters](#)

New Security Rating Filter

Details | Related Items | Change History

Filter Details

Name:

Description:

Platform:

Settings

Security Rating System:

Rating Level:

Timeout:

Error Handling

On timeout, consider the result:

On failure, consider the result:

The parameters for the Security Rating Filter would include the following:

- Security Rating System
 - Application Control Rating System
 - Cylance Rating System
 - VirusTotal Rating System
- Rating level
 - Unknown
 - Clean
 - Suspect
 - Bad
- Timeout, can be specified in seconds or milliseconds
- Error Handling
 - On timeout, consider the result
 - Matched
 - Note Matched
 - Error Condition
 - On Failure, consider the result
 - Matched
 - Note Matched
 - Error Condition

Example

The example above displays how to create a security rating filter after integrating Privilege Manager with VirusTotal.

Signed File Filter

This filter allows you to associate one or more Digital Certificate(s) that are trusted and verify that an application or file is signed by one of those certificates. *No out-of-box filters exist in Privilege Manager for this type.*

The screenshot shows the 'New Signed File Filter' configuration interface. At the top, there is a navigation bar with a back arrow, search icon, notification bell, help icon, and user profile icon. Below the navigation bar, the title 'New Signed File Filter' is displayed. There are three tabs: 'Details' (selected), 'Related Items', and 'Change History'. To the right of the tabs are 'Refresh' and 'More' buttons. The main content area is divided into two sections: 'Filter Details' and 'Settings'. In the 'Filter Details' section, there are three rows: 'Name' with the value 'New Signed File Filter', 'Description' with the text 'Includes only files that are signed by the specified digital certificates.', and 'Platform' with the value 'Windows'. The 'Settings' section contains a descriptive text: 'This filter will match any application that is signed by one of the chosen digital certificates or subject name.' Below this text are two fields: 'Digital Certificates' with a plus icon and a link 'Add Digital Certificates', and 'Subject Name' with a plus icon and an empty text input field.

These filters can be used in several of the following ways:

- A target for ACS policies
- A parameter to prevent spoofing

Signed Application filters identify applications based on their digital certificates.

This filter is available for both Windows and macOS systems.

Parameters

Under Settings users:

- add one or more digital certificates, which are discovered via inventory.
- enter a Subject Name (version **10.7 and up**). If Subject Name is specified, the digital certificates above will be ignored. The following three match types are supported:
 - The * character can be pre- or post- appended to a string to perform a begins with or ends with match (i.e. `Microsoft*`).
 - Lower-case RegEx is also supported and must be surrounded with parenthesis. (i.e. `(micro*)`)
 - Setting the subject name to * will match any file signed with a valid certificate. (**Not recommended by Thycotic**)

Examples

Adobe (TM) requires several certificates that are used to sign applications.

Because of this, you may want all applications signed by Adobe to allow listed, so that a signed application filter targeting Adobe Certificates allows all applications signed by Adobe to run.

Targeting the latest Adobe Flash Installer via a Win32 Executable filter and then using the signed application filter ensures that the application really is the adobe flash installer. The Signed Application Filter works as a validation filter for applications.

Time of Day Filter

This type of filter exists to create policy parameters for specific time frames.

[← Back to Filters](#)

New Time Of Day Filter

Search [] | [] | [] | []

[Details](#) | [Related Items](#) | [Change History](#) | [Refresh](#) | [More](#) ▾

Filter Details

Time of day filters can be used as application targets, inclusion, or exclusion filters in policies to limit when a policy applies or does not apply based upon the current time on the agent. For example, if you wanted to block Spotify during business hours.

Name:

Description:

Platform: Windows

Time of Day Filter Settings

Time of day filters can target the same time every day or different periods on different days.

Different Periods on Different Days

<input checked="" type="radio"/> Sunday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Monday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Tuesday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Wednesday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Thursday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Friday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>
<input checked="" type="radio"/> Saturday	<input type="text" value="12:00 A"/>	to	<input type="text" value="12:00 A"/>

This filter is available for both Windows and macOS systems.

Parameters

The time of day filter has two different settings to allow you to set time and day allowances.

- Same period everyday from
- Different Periods on Different Days

Examples

You can use the time of day filter in a policy to only pickup specific times or days of the week.

Using User Context Filters

User Context Filters are used in a policy as either an

- inclusion filter, to specify that the policy only applies to users in a specific AD Group
- exclusion filter, to specify that the policy applies to everyone except the users in a specific AD Group.

The User Context Filters are part of the Application Filter templates listed for Windows:

doctest User Context Filter

Details Related Items Change History Refresh More

Filter Details

Name: doctest User Context Filter

Description:

Platform: Windows

Include only files with the owner set to any of the following accounts

Built-in Accounts: [Add Built-in Accounts](#)

Well-known Accounts: [Add Well-known Accounts](#)

Domain User Groups: [Add Domain User Groups](#)

Specific Users: [Add Specific Users](#)

All specified conditions must be met. Uncheck to match any of the specified conditions. No

Require accounts to be enabled. No

This filter is available for both Windows and macOS systems.

On-Premise

For Privilege Manager on-premises the **User Context Filter** can be used after the Active Directory synchronization completes. When creating and editing the filter, add any

- Build-in Accounts,
- Well-known Accounts, and/or
- Domain User Groups, or
- Specific Users.

to specifically select user context.

Then select if **ALL** conditions must be met. Leave the box unchecked to match **ANY**. You can also specify, if accounts must be enabled to be targeted. This is an important checkbox to set if specific users have been added.

Cloud

For Privilege Manager cloud the **User Context Filter via SID** can be used if (Azure) AD synchronization has not been set up but the SID of the group is known. When creating the filter, enter the

- Group SID, and
- Group Name, to name the group if it does not exist.

Create Filter

Platform: Windows

Type: User Context Filter via SID

Filter Name *: New User Context Filter

Group SID *:

Group Name *: DOMAIN\GROUPNAME

Cancel Create

File Filters

These target specific file information. File Filters can be used to target the file owner of the application, the type of file, the application manifest of the file, or whether the application is present in the signed security catalog (Operating System Files).

The following File Filter type filter topics are available:

- [Application Compatibility Filter](#)
- [Application Manifest Filter](#)
- [File Collection Security Catalog Filter](#)
- [File Existence Filter](#)
- [File Owner Filter](#)
- [File Specification Filter](#)
- [File Type Filter](#)
- [Internet Zone Filter](#)
- [Security Catalog Filter](#)

Application Compatibility Filter

This type of filter identifies the rights or permissions that an application requires to run.

[Back to Filters](#)

New Application Compatibility Filter

Details Related Items Change History Refresh More

Filter Details

Name: New Application Compatibility Filter

Description:

Platform: Windows

Settings

Perform execution level test: No
None Specified

Perform installer detection test: No

Generic Installer: not set

Specific Installer: not set

Specific Non Installer: not set

Results should be: included

Parameters

By default **Perform execution level test** is set to no, if you change this to Yes, you can specify:

- As Invoker
- Highest Available
- Require Administrator

By default **Perform installer detection test** is set to no, if you change this to Yes, you can specify:

- Generic Installer to be set or not set.
- Specific Installer to be set or not set.
- Specific Non Installer to be set or not set.
- if the Results should be included or excluded.

Remember to **Save Changes** after any customization.

Application Manifest Filter (*Manifest Filter*)

Applications that declare specific rights required via a manifest, such as applications that need administrative privileges.

[← Back to Filters](#)

New Application Manifest Filter

Details Related Items Change History Refresh More

Filter Details	Name	New Application Manifest Filter
	Description	
	Platform	Windows
Settings	Only perform presence check	<input checked="" type="checkbox"/> Yes
	Execution Level	None Specified

Parameters

By default **Only perform presence check** is set to Yes, if you change this to No, you can specify the **Execution Level** as either:

- As Invoker
- Highest Available
- Require Administrator

Remember to **Save Changes** after any customization.

File Collection Security Catalog Filter

This is a special collection of files allow or deny list. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type.*

You can use these filters to target executables found in security catalogs. The built-in filter targets the Signed Security Catalog (Windows\System32\catroot) and is typically used to automatically allow list applications from Microsoft.

Create Filter

Platform
Windows

Type
File Collection Security Catalog Filter

Name *
New File Collection Security Catalog Filter

Description

File collection

Catalog signing certificate
[Select...](#)

Timestamp server

Parameters

- File collection, this is the specific catalog you want to use.
- Catalog signing certificate, select the specific certificate from a list.
- Timestamp server, specifies a particular version to be used.

[Back to Filters](#)

New File Collection Security Catalog Filter

Details Related Items Change History

Filter Details

Name: New File Collection Security Catalog Filter

Description:

Platform: Windows

Settings

File Collection: Security Descriptor

Catalog Signing Certificate: E="release+certificates@mozilla.com", CN=Mozilla Corporation

Catalog Signing Timestamp Server:

File Existence Filter

This type of filter identifies whether a file exists. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
File Existence Filter

Name *
New File Existence Filter

Description

File Path

Cancel Create

This filter is available for both Windows and macOS systems.

Parameters

- Path, this must be an exact file path. Windows Environment Variables are supported though, %ProgramFiles% for example.

[Back to Filters](#)

New File Existence Filter

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Filter Details

Name	New File Existence Filter
Description	
Platform	Windows

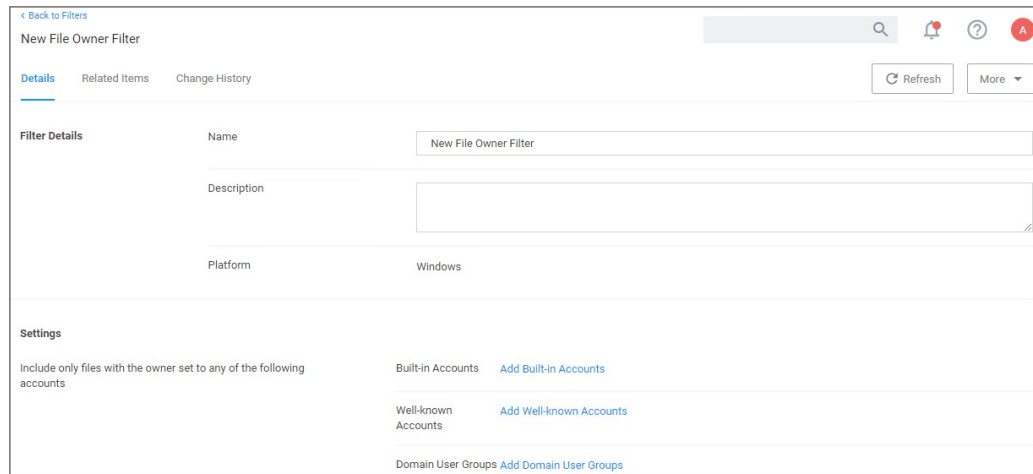
Settings

This filter will check for the existence of a file at a defined path on the managed computer.

File Path C:\Program Files (x86)\Windows Photo Viewer\ImagineDevices.exe

File Owner Filter

This filter identifies files based on ownership.

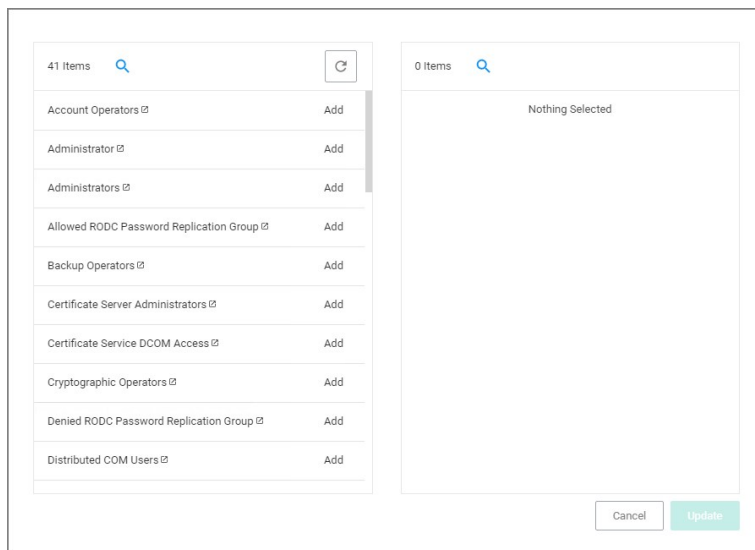


This filter is available for both Windows and macOS systems.

Parameters

Under settings you specify to include only those files with an owner having certain accounts or being part of certain domain user groups.

- Build-in Accounts



- Well-known Accounts

48 Items	
All Application Packages	Add
Anonymous Logon Well Known Group	Add
Application Class/Classification	Add
Authenticated Users Well Known Group	Add
Batch Logon Well Known Group	Add
Creator Group Well Known Group	Add
Creator Owner Server ID	Add
Creator Owner Well Known Group	Add
Dialup Well Known Group	Add
DWM-1	Add

1 Items	
Creator Group Server ID	Remove

- Domain User Groups

2,211 Items	
A	Add
a_group	Add
a_group1	Add
a_group11	Add
a_group12	Add
a_group2	Add
a_group3	Add
a_group4	Add
a_group5	Add
a_group6	Add
a_group7	Add

1 Items	
a_group10	Remove

Remember to click **Update** and **Save Changes** following any customization.

File Specification Filter

This filter identifies files based on their file name, extension, path, or location on a computer.

[← Back to Filters](#)

New File Specification Filter

🔍
🔔
?
Ⓜ

[Details](#) [Related Items](#) [Change History](#)

Filter Details	Name	<input type="text" value="New File Specification Filter"/>
	Description	<input type="text"/>
	Platform	Windows

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters [Add File filters](#)

Include only filters [Add Include only filters](#)

Exclude any filters [Add Exclude any filters](#)

This filter is available for both Windows and macOS systems. Use this filter for macOS endpoints only to target known scripts or command-line tools; otherwise use the [Default File Specification \(macOS\)](#) filter.

Parameters

- File Names
- Path
- Drive Types
- Attributes, include reparse points is the only default enabled attributes

Additional Filters

Additional Filters can be added optionally.

- File filters, at least one of the filters added here must match.
- Include only filters, all of the filters added here have to match.
- Exclude any filters, any matching filters added here will be excluded.

File Type Filter

This filter identifies files based on what type of file it is. *No out-of-box filters exist in Privilege Manager for this type.*

< Back to Filters

New File Type Filter

Details Related Items Change History Refresh More

Filter Details

Name New File Type Filter

Description

Platform Windows

Settings

File Extensions Add File Extensions

MIME Types Add MIME Types

Parameters

• File Extensions

< Back to Filters

New File Type Filter

Details Related Items Change History Refresh More

Filter Details

Name New File Type Filter

Description

Platform Windows

Settings

File Extensions Add File Extensions

MIME Types Add MIME Types

• MIME Types

435 Items

0 Items

Nothing Selected

AIFF/Amiga/Mac audio Add

Amiga SoundTracker audio Add

ANIM animation Add

application log Add

Applix Graphics image Add

Applix Spreadsheets spreadsheet Add

Applix Words document Add

AR archive Add

ARJ archive Add

ASF video Add

Cancel Update

Add the parameters, click **Update** and **Save Changes**.

Internet Zone Filter

This filter identifies what internet zone a computer is connected to on your network, such as Trusted Sites and Local Intranet. *No out-of-box filters exist in Privilege Manager for this type.*

The screenshot shows the 'New Internet Zone Filter' configuration interface. At the top, there is a navigation bar with a search icon, a notification bell, a help icon, and a user profile icon. Below the navigation bar, there are tabs for 'Details', 'Related Items', and 'Change History'. A 'Refresh' button and a 'More' dropdown menu are also present. The main content area is divided into two sections: 'Filter Details' and 'Settings'. In the 'Filter Details' section, the 'Name' field contains 'New Internet Zone Filter', the 'Description' field is empty, and the 'Platform' is set to 'Windows'. In the 'Settings' section, there are three radio buttons: 'Existence of any zone information' (unselected), 'Standard zone:' (selected), and 'Custom zone ID' (unselected). The 'Standard zone:' radio button has a dropdown menu open, showing four options: 'Local Intranet', 'Trusted Sites' (highlighted in blue), 'Internet', and 'Restricted Sites'.

Parameters

- Existence of any zone information
- Standard zone:
 - Local Intranet
 - Trusted Sites
 - Internet
 - Restricted Sites
- Custom Zone IDs

Security Catalog Filter

This is a special collection of files to allow or deny list. For example, the Microsoft Security Catalog is often allow listed as a trusted catalog.

The screenshot shows the 'New Security Catalog Filter' configuration page. At the top, there is a navigation bar with a search icon, a notification bell, a help icon, and a user profile icon. Below the navigation bar, there are tabs for 'Details', 'Related Items', and 'Change History'. A 'Refresh' button and a 'More' dropdown menu are also present. The main content area is titled 'Filter Details' and contains the following fields:

- Name:** New Security Catalog Filter
- Description:** (Empty text area)
- Platform:** Windows

At the bottom of the page, there is a 'Settings' section with a 'Digital Certificates' link and an 'Add Digital Certificates' button.

Parameters

- Digital Certificates

The screenshot shows a dialog box for selecting digital certificates. It is divided into two panes. The left pane, titled '69 Items', contains a list of certificates with their names and an 'Add' button next to each. The right pane, titled '0 Items', shows 'Nothing Selected'. At the bottom of the dialog, there are 'Cancel' and 'Update' buttons.

Certificate Name	Action
CN="Cisco Systems, Inc.", OU=Endpoint Security, ...	Add
CN="OpenVPN Technologies, Inc.", O="OpenVPN ...	Add
CN="OpenVPN Technologies, Inc.", O="OpenVPN ...	Add
CN="Zoom Video Communications, Inc.", O="Zoo...	Add
CN=DigiCert Timestamp Responder, O=DigiCert, ...	Add
CN=DOTPDN LLC, O=DOTPDN LLC, STREET=392...	Add
CN=GlobalSign TSA for MS Authenticode - G2, O...	Add
CN=Google Inc, O=Google Inc, L=Mountain View, ...	Add
CN=Google LLC, O=Google LLC, L=Mountain Vie...	Add
CN=Google LLC, O=Google LLC, L=Mountain Vie...	Add

Unable to Access Cortana and Search for Windows 10

This issue might be due to the **Present In Signed Security Catalog** not being added to the **Exclusion Filters** section in a policy.

How to Resolve

1. Launch **Privilege Manager** and navigate to your **Application Policies**.
2. Click on a previously created policy.
3. Under **Conditions**, next to Exclusions select **Add Exclusion Filter**.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.

Applications Targeted (Filters) 🔗	\\path-to\share\ - File Scan Filter	Edit
Inclusions	Add Inclusions	
Exclusions	Add Exclusions	

4. Search for **Present In Signed Security Catalog**.

1 Items [✕](#) [🔄](#)

Present in Signed Security Catalog 🔗	Add
--	---------------------

0 Items [🔍](#)

Nothing Selected

[Cancel](#) [Update](#)

5. Click **Add** next to the **Present In Signed Security** filter.

6. Click **Update**.

7. Click **Save Changes** on the policy page.

Note: Once the agents check back into the web console which by default occurs every 30 minutes, the machines will get the new policy changes. However if you would like to test the policy update on a specific machine, please continue.

8. Go to the Machine(s) where you want to update the policy and open the Agent Utility.

e.g., C:\Program Files\Thycotic\Agents\Agent

9. Click **Update**.

Inventory Filters

These depend on file inventory data, meaning they generally apply to already discovered applications or files pulled in by Privilege Manager tasks. For example, after running an inventory task on a specific computer or group of computers, Privilege Manager can glean through the list of file inventory that is reported and target those files.

Note: No out-of-box filters exist in Privilege Manager for this type of filter category. Most Filters of this type are associated with a data source during their creation. That data source is not to be changed. The exception is the Security Catalog File Filter where the data source needs to be added after the filter has been created.

The following Inventory Filter type filter topics are available:

- [File Collection from List of Sha1 Hashes Filter](#)
- [File Scan Results Filter - Computer](#)
- [File Scan Results Filter - Policy](#)
- [MSI File Contents Filter](#)
- [MSI Package Contents Filter](#)
- [Package Contents Filter](#)
- [Security Catalog Contents Filter](#)
- [Virtual Disk File Contents Filter](#)
- [Virtual Disk Package Contents Filter](#)

File Collection from List of Sha1 Hashes Filter

This type of filter identifies file inventory based on Secure Hash Algorithms. *No out-of-box filters exist in Privilege Manager for this type.*

When creating this filter the target hashes need to be entered as a comma-separated list:

Create Filter

Platform
Windows

Type
File Collection from List of SHA1 Hashes Filter

Name *
DocTest File Collection of Hashes Filter

Description

Comma-separated SHA1 Hashes *
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12_da39a3ee5e6b4b0d3255bfe95601890afd80709

This filter is available for both Windows and macOS systems.

Parameters

Once the filter is created, the following settings can be viewed and/or edited:

- Data Source:
 - Hash Based Query (**do not change the data source**)
- Results will be:
 - Included (default)
 - Excluded

[Back to Filters](#)

DocTest File Collection of Hashes Filter

Details | Membership | Related Items | Change History

Filter Details

Name	DocTest File Collection of Hashes Filter
Description	<input type="text"/>
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	Hash Based Query
Results will be	<input checked="" type="checkbox"/> Included

Under the **Membership** tab various reports can be viewed:

- All Files Picker Report
- Win32 File Picker Report
- Default Resource Picker Report

Details **Membership** Related Items Change History Refresh More

This collection was last updated at Jun 24, 2020, 2:02:13 PM. To force an immediate update, click Update Membership Update Membership

View All Files Picker Report 🔄

File Name	Product Name	Version	Header Type
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
New Loaded Resource - 2mj7l5rSw0yVb/vlWAYKK/YBwk= - Created via Sha1 Filter			Unknown
New Loaded Resource - L9ThxnotKpzhJ7hu3bnORuT6xt= - Created via Sha1 Filter			Unknown

Under the **Related Items** tab items will be listed if the filter is used in a policy or as a secondary filter.

File Scan Results Filter (Computer)

This type of filter identifies file inventory based on another computer's file scan results. This allows for one computer that has been setup properly to be used as a source for this filter. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
File Scan Results Filter (Computer)

Name *
New File Scan Results (Computer) File Filter

Description
Specifies files reported by the specified file scan reporting filters by the specified computers

This filter is available for both Windows and macOS systems.

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, this **should not be edited**. The information here is specific to the task of the File Scan Results Filter for computers.
- Computer, this is the actual computer resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.

Details | Membership | Related Items | Change History

Filter Details

Name	New File Scan Results (Computer) File Filter
Description	Specifies files reported by the specified file scan reporting filters by the specified computers
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	File Scan Results Query - Computer
Computer *	00000000-0000-0000-0000-000000000000
Reporting Filter *	
Results will be	<input checked="" type="radio"/> Excluded

File Scan Results Filter (Policy)

This type of filter identifies file inventory based on Privilege Manager Policies. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
File Scan Results Filter (Policy)

Name *
New File Scan Results File Filter

Description
Specifies files reported by the specific file scan reporting filter based on policy

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, this **should not be edited** it is the File Scan Policy Results Query.
- Specifies the File Scan Policy, this is the actual Policy resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.

New File Scan Results File Filter

Details Membership Related Items Change History

Filter Details

Name	New File Scan Results File Filter
Description	Specifies files reported by the specific file scan reporting filter based on policy
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	File Scan Policy Results Query
Specifies the File Scan policy *	
Reporting Filter *	
Results will be	<input checked="" type="radio"/> Excluded

MSI File Contents Filter

This type of filter identifies file inventory based on .MSI file contents, i.e. specific Windows package installers. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
MSI File Contents Filter

Name *
New MSI File Contents Filter

Description
Filters executable files contained in the specified MSI file

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the MSI File Contents Query.
- File:
 - Parameters (these are required)
 - Win32 Executable
 - Product Name
 - Select Resource, this is the actual MSI file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.

Details | Membership | Related Items | Change History

Filter Details

Name	New MSI File Contents Filter
Description	Filters executable files contained in the specified MSI file
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	MSI File Contents Query
File *	
Results will be	<input checked="" type="radio"/> Excluded

Viewing, Editing, and Saving the Parameters

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Filter Details

Name:

Description:

Platform:

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source:

File *

Results will be

-
- nlascv.dll
- nlascv.dll
- notepad.exe
- notepad++.exe**
- nsisvc.dll
- nsisvc.dll
- omni.ja
- openvpn.exe

MSI Package Contents Filter

This type of filter identifies file inventory based on MSI package contents. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
MSI Package Contents Filter

Name *
New MSI Package Contents Filter

Description
Filters executable files contained in the specified MSI package

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the MSI Package Contents Query.
- Package:
 - Parameters:
 - Scope by Organizational Group
 - Search text
 - Maximum rows returned, this is a required parameter and the default is 10000.
 - Select Resource, this is the actual MSI package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

Details | Membership | Related Items | Change History

Filter Details

Name	New MSI Package Contents Filter
Description	Filters executable files contained in the specified MSI package
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	MSI Package Contents Query
Package *	00000000-0000-0000-0000-00000000-0000 Click here to select the package parameters.
Results will be	<input checked="" type="radio"/> Excluded

Viewing and Editing the Package Parameters

Select Resource

Resource type
Package

Scope by Organizational Group
All Resources

Search text ⓘ

Maximum rows returned *
10000

Viewing and Adding the Resource(s)

Select Resource

Name	Resource Type	Description	CreatedDate
UNC File Inventory Package for \\filesystem\TPI\	Package		Wed Aug 07 2019 15:39:36 GMT-0400 (Eastern Daylight Time)
UNC File Inventory Package for \\path-to\share\	Package		Thu Aug 08 2019 09:47:26 GMT-0400 (Eastern Daylight Time)

« ‹ 1 › » 10 items per page 1 - 2 of 2 Items

Cancel Change Search

Package Contents Filter

This type of filter identifies file inventory based on package contents. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
Package Contents Filter

Name *
New Package Contents Filter

Description
Filters files contained in the specified package

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, (**do not edit**) this is the Package Contents Query.
- Package:
 - Parameters:
 - Scope by Organizational Group
 - Search text
 - Maximum rows returned, this is a required parameter and the default is 10000.
 - Select Resource, this is the actual package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

Details | Membership | Related Items | Change History

Filter Details

Name	New Package Contents Filter
Description	Filters files contained in the specified package
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	Package Contents Query
Package *	00000000-0000-0000-0000-000000000000 Click here
Results will be	<input checked="" type="radio"/> Excluded

Viewing and Editing the Package Parameters

Select Resource

Resource type
Package

Scope by Organizational Group
All Resources

Search text ⓘ

Maximum rows returned *
10000

Adding the Resource(s)

Select Resource

Name	Resource Type	Description	CreatedDate
UNC File Inventory Package for \\filesystem\TPI\	Package		Wed Aug 07 2019 15:39:36 GMT-0400 (Eastern Daylight Time)
UNC File Inventory Package for \\path-to\share\	Package		Thu Aug 08 2019 09:47:26 GMT-0400 (Eastern Daylight Time)

« < 1 > » 10 items per page 1 - 2 of 2 Items

Cancel Change Search

Security Catalog Contents Filter

This is a special collection of files to allow or deny list. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
Security Catalog Contents Filter

Name *
New Security Catalog File Filter

Description
Filters a list of files contained in Security Catalogs that were inventoried by the specified file scan reporting

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source
- Computer Filter
- Computers
- Reporting Filter
- Resource Targets
- Results will be either excluded (default) or included.

Details | Membership | Related Items | Change History

Filter Details

Name	New Security Catalog File Filter
Description	Filters a list of files contained in Security Catalogs that were inventoried by the specified file scan reporting filters by the specified computers.
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	
Computer Filter *	00000000-0000-0000-0000-000000000000
Computers *	00000000-0000-0000-0000-000000000000
Reporting Filter *	00000000-0000-0000-0000-000000000000
Resource Targets *	00000000-0000-0000-0000-000000000000
Results will be	<input checked="" type="radio"/> Excluded

Virtual Disk File Contents Filter

The Virtual Disk File Contents Filter filters files contained in the specified virtual disk file. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
Virtual Disk File Contents Filter

Name *
New Virtual Disk File Contents Filter

Description
Filters files contained in the specified virtual disk file

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source, **(do not edit)** this is the Virtual Disk File Contents Query.
- File, this is the actual virtual disk file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.

[Details](#) | [Membership](#) | [Related Items](#) | [Change History](#)

Filter Details

Name	New Virtual Disk File Contents Filter
Description	Filters files contained in the specified virtual disk file
Platform	Windows

Collection Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	Virtual Disk File Contents Query
File *	
Results will be	<input checked="" type="radio"/> Excluded

Virtual Disk Package Contents Filter

Filters files contained in the specified virtual disk package. *No out-of-box filters exist in Privilege Manager for this type.*

Create Filter

Platform
Windows

Type
Virtual Disk Package Contents Filter

Name *
New Virtual Disk Package Contents Filter

Description
Filters files contained in the specified virtual disk package

Parameters

Once the filter is created the following settings can be viewed and/or edited:

- Data Source. (do not edit) this is the Virtual Disk Package Contents Query.
- Package. select the actual package resource that is required for the query.
- Results will be either excluded (default) or included.

Details Membership Related Items Change History

Filter Details

Name	New Virtual Disk Package Contents Filter
Description	Filters files contained in the specified virtual disk package
Platform	Windows

Collection Settings

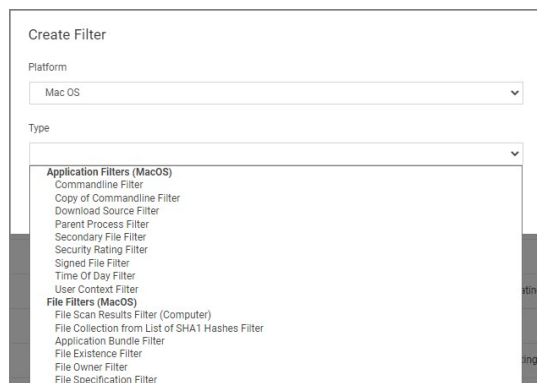
This filter will check for the existence of a file that is a member of the following collection.

Data Source	Virtual Disk Package Contents Query
Package *	
Results will be	<input checked="" type="radio"/> Excluded

MacOS Specific Filters

Most of the Application and File type filters apply to Windows as much as macOS platforms. There are some macOS specific filters that are covered in this section.

This is the default drop-down list when adding a new filter for macOS:



Creating macOS Filters Manually

In cases when Privilege Manager does not have enough information from the discovery process on a macOS endpoint, filters have to be created manually.

To manually find granular information required for targeting applications in Privilege Manager on a macOS endpoint,

1. Right-click the target application and select **Show Package Contents**.
2. Navigate to **Contents Info.plist**, this gives you a coded list of items that you can match into the details page of your Filter.

For example, the highlighted section below can be entered into the **Bundled Identifier** line item when creating a Firefox filter.

```

<array>
  <string>video/webm/string
</array>
<key>CFBundleTypeIdentifier</key>
<string>MIME.Video.WebM/string
<key>CFBundleTypeRole</key>
<string>Viewer/string
</dict>
</array>
<key>CFBundleExecutable</key>
<string>firefox</string>
<key>CFBundleIdentifier</key>
<string>org.mozilla.firefox
<key>CFBundleIconFile</key>
<string>Icon.icns
<key>CFBundleInfoDictionaryVersion</key>
<string>1.0
<key>CFBundleName</key>
<string>Firefox
<key>CFBundlePackageType</key>
<string>APPL</string>
<key>CFBundleShortVersionString</key>
<string>68.0.1
<key>CFBundleSignature</key>
<string>00000000
<key>CFBundleURLTypes</key>
<array>
  <dict>
    <key>CFBundleURLIconFile</key>
    <string>Documents/Icons/string
    <key>CFBundleURLName</key>
    <string>http://www.mozilla.org
    <key>CFBundleURLSchemes</key>
    <array>
      <string>http/string
    </array>
  </dict>
</array>
</dict>
</array>
<key>CFBundleURLIconFile</key>
<string>Documents/Icons/string
<key>CFBundleURLName</key>
<string>http://www.mozilla.org
<key>CFBundleURLSchemes</key>
<array>
  <string>http/string
</array>

```

List of MacOS Filters

The following filters are available based on type from a quick select drop-down menu, after choosing macOS as the platform.

Application Filter Types

- [Commandline Filter](#)
- [Download Source Filter](#)
- [Parent Process Filter](#)
- [Secondary File Filter](#)
- [Security Rating Filter](#)
- [Signed File Filter](#)
- [Time Of Day Filter](#)
- [User Context Filter](#)

File Filter Types

- [Application Bundle Filter](#)
- [File Collection from List of SHA1 Hashes Filter](#)
- [File Existence Filter](#)
- [File Owner Filter](#)
- [File Scan Results Filter \(Computer\)](#)
- [File Specification Filter](#)

List of Default Filters for Event Discovery

The following filters are the default filters used during inventory event discovery on macOS endpoints:

- [Default File Specification \(MacOS\)](#)
 - [Default Applications Folder \(MacOS\)](#)

- [System Applications Folder \(MacOS\)](#)
- [Default App Bundles File Specification Filter](#)
- [Default Application Bundles Filter \(MacOS\)](#)
- [System Application Bundles Filter \(MacOS\)](#)

Available Preference Pane Filters

- [Date and Time Preference Pane filter](#)
- [Energy Saver Preference Pane filter](#)
- [Network Preference Pane filter](#)

Application Bundle Filter

This type of filter identifies application bundles for macOS systems.

Create Filter

Platform
Mac OS

Type
Application Bundle Filter

Name *
New Application Bundle Filter (MacOS)

Description

Prior to Privilege Manager 10.7.1, the value of the Bundle Name field required the inclusion of the .app extension (e.g. Console.app). The Bundle Name field should have an entry like **console.app** or **photos.app** to correctly apply the filter. If it is not present, the filter will fail to properly match. With Privilege Manager 10.7.1, the presence of the .app extension is properly calculated during policy processing.

Pre-10.7.1 Example

The bundle name should appear when creating the filter.

Settings

Bundle Name Console.app

Bundle Path

Include subdirectories

Parameters

- Bundle Name
- Bundle Path
 - Include subdirectories

The following bundle properties can be used to identify an application bundle in an Application Bundle filter. These properties are found in the info.plist for the application on macOS systems.

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Info String
- Min System Version

Note: The **Bundle Name** field is separate from the Bundle Name in the property list. If you have the Bundle Name field populated and it doesn't match the binary being executed, the filter will fail to match and not process the property list values in the Info.plist file. If an app is discovered as a new loaded resource and assigned to a policy, a filter is created and pre-populated based on the information pulled from the info.plist file.

Details Related Items Change History

Filter Details

Name

Description

Platform

Settings

Bundle Name

Bundle Path

Include subdirectories

Match the following property list values

<input checked="" type="checkbox"/> App Category	is equal to	<input type="text" value="public.app-category.photography"/>
<input checked="" type="checkbox"/> Bundle Identifier	is equal to	<input type="text" value="com.apple.Photos"/>
<input checked="" type="checkbox"/> Bundle Name	is equal to	<input type="text" value="Photos"/>
<input type="checkbox"/> Bundle Version		
<input type="checkbox"/> Bundle Version (short)		
<input checked="" type="checkbox"/> Executable File	is equal to	<input type="text" value="Photos"/>
<input type="checkbox"/> Info String		
<input type="checkbox"/> Min System Version		

Info.plist Example for Photos

```
<key>CFBundleExecutable</key>
<string>Photos</string>
<key>CFBundleHelpBookFolder</key>
<string>Photos.help</string>
<key>CFBundleHelpBookName</key>
<string>com.apple.Photos.help</string>
<key>CFBundleIconFile</key>
<string>AppIcon</string>
<key>CFBundleIconName</key>
<key>CFBundleIdentifier</key>
<string>com.apple.Photos</string>
<key>CFBundleInfoDictionaryVersion</key>
<string>6.0</string>
```

Default App Bundles File Specification Filter

This type of filter identifies application bundles for macOS systems. With this application bundles filter in place, macOS application bundles are inventoried regardless of their installation path in either /Applications or /System/Applications) on all versions of macOS.

Default App Bundles File Specification Filter

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	Default App Bundles File Specification Filter
Description	The default filter for discovering app bundles on MacOS.
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters [Default Application Bundles Filter \(MacOS\)](#) [System Application Bundles Filter \(MacOS\)](#)

Include only filters No options selected

Exclude any filters No options selected



By default this is a read-only filter which uses the following Additional Filters:

- File filters:
 - [Default Application Bundles Filter \(MacOS\)](#)
 - [System Application Bundles Filter \(MacOS\)](#)

The option to include subdirectories is enabled by default.

Example

1. Navigate to **Admin | Filters**.
2. In the search field next to the supported/not supported OS drop-downs, search for *default app*.

NAME	DESCRIPTION	TYPE	SUPPORTED
Copy of Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS.	File Specification Filter	
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS.	File Specification Filter	

3. Select the **Default App Bundles File Specification Filter** filter to view its details and/or create a copy to customize the filter.
4. Click **Duplicate**.
5. Set the needed parameters.
6. Click **Save Changes**.

Default File Specification (MacOS)

This filter identifies files based on their file path or location on a computer.

Default File Specification (MacOS)

This item is read-only.

Details
Related Items
Change History

Filter Details

Name	Default File Specification (MacOS)
Description	The default filter for discovering executable files on MacOS.
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names ⊙

Path ⊙

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters ⊙

- [Default Applications Folder \(MacOS\)](#)
- [System Applications Folder \(MacOS\)](#)

Include only filters ⊙

- [macOS Executables](#)

Exclude any filters ⊙

No options selected

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

- File filters:
 - [System Applications Folder \(MacOS\)](#)
 - [Default Applications Folder \(MacOS\)](#)
- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

Example

1. Navigate to **Admin | Filters**.
2. In the search field next to the supported/not supported OS drop-downs, search for *default file*.

Filters

2 Items MacOS: All ▾ Not Supported ▾ 🔍 ✕

NAME ↑	DESCRIPTION
Copy of Default File Specification (MacOS)	The default filter for discovering executable files on MacOS.
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS.

3. Select the **Default File Specification Filter (MacOS)** filter to view its details and/or create a copy to customize the filter.
4. Click **Duplicate**.
5. Set the needed parameters.
6. Click **Save Changes**.

Preference Pane Filters

The following Preference Pane Filters are supported for targeting in run as root type policies triggering justification and approval type interactive user dialogs:

- [Date and Time Preference Pane filter](#)
- [Energy Saver Preference Pane filter](#)
- [Network Preference Pane filter](#)

For the following list of default preference pane filters, Thycotic recommends to only target the preference pane in basic deny access policies:

- App Store Preference Pane
- Parental Controls Preference Pane
- Printers and Scanners Preference Pane
- Security and Privacy Preference Pane
- Sharing Preference Pane
- Time Machine Preference Pane
- Users and Groups Preference Pane

Date and Time Preference Pane Filter

The Date and Time Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Date and Time Preference Pane (MacOS)

NOTICE: This filter definition is known not to work on macOS 10.15 (Catalina) at this time. However, it will work on earlier versions of macOS. For more information, see this KB Article.

This item is read-only.

Details Related Items Change History Duplicate More

Filter Details

Name	Date and Time Preference Pane (MacOS)
Description	Date and Time Preference Pane (MacOS)
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names	com.apple.preference.datetime.remoteservice
Path	/System/Library/PreferencePanes/DateAndTime.prefPane/Contents/XPCServices/com.apple.preference.datetime.remoteservice.xpc/Contents/MacOS/
Drive Types	<input type="checkbox"/> Unknown Type <input type="checkbox"/> No Root Directory <input type="checkbox"/> Removable Drive (Floppy/USB) <input type="checkbox"/> Fixed Disk <input type="checkbox"/> Network Drive <input type="checkbox"/> Optical Disk (CD/DVD) <input type="checkbox"/> RAM Disk
Attributes	<input type="checkbox"/> Include subdirectories <input type="checkbox"/> Include system files <input type="checkbox"/> Include hidden files <input type="checkbox"/> Include reparse points <input type="checkbox"/> Include system reparse points

Additional Filters (optional)

File filters	No options selected
Include only filters	No options selected
Exclude any filters	No options selected

Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Energy Saver Preference Pane Filter

The Energy Saver Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Energy Saver Preference Pane (MacOS)

NOTICE: This filter definition is known not to work on macOS 10.15 (Catalina) at this time. However, it will work on earlier versions of macOS. For more information, see this KB Article.

This item is read-only.

[Details](#) [Related Items](#) [Change History](#) Duplicate More

Filter Details

Name	Energy Saver Preference Pane (MacOS)
Description	Energy Saver Preference Pane (MacOS)
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names	com.apple.preference.energysaver.remoteservice
Path	/System/Library/PreferencePanes/EnergySaver.prefPane/Contents/XPCServices/com.apple.preference.energysaver.remoteservice.xpc/Contents/MacOS/
Drive Types	<input type="checkbox"/> Unknown Type <input type="checkbox"/> No Root Directory <input type="checkbox"/> Removable Drive (Floppy/USB) <input type="checkbox"/> Fixed Disk <input type="checkbox"/> Network Drive <input type="checkbox"/> Optical Disk (CD/DVD) <input type="checkbox"/> RAM Disk
Attributes	<input type="checkbox"/> Include subdirectories <input type="checkbox"/> Include system files <input type="checkbox"/> Include hidden files <input type="checkbox"/> Include reparse points <input type="checkbox"/> Include system reparse points

Additional Filters (optional)

File filters	No options selected
Include only filters	No options selected
Exclude any filters	No options selected

Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Network Preference Pane Filter

The Network Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Network Preference Pane (MacOS)

NOTICE: This filter definition is known not to work on macOS 10.15 (Catalina) at this time. However, it will work on earlier versions of macOS. For more information, see this KB Article.

This item is read-only.

[Details](#)
[Related Items](#)
[Change History](#)

Filter Details

Name	Network Preference Pane (MacOS)
Description	Network Preference Pane (MacOS)
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names	com.apple.preference.network.remoteservice
Path	/System/Library/PreferencePanes/Network.prefPane/Contents/XPCServices/com.apple.preference.network.remoteservice.xpc/Contents/MacOS/
Drive Types	<input type="checkbox"/> Unknown Type <input type="checkbox"/> No Root Directory <input type="checkbox"/> Removable Drive (Floppy/USB) <input type="checkbox"/> Fixed Disk <input type="checkbox"/> Network Drive <input type="checkbox"/> Optical Disk (CD/DVD) <input type="checkbox"/> RAM Disk
Attributes	<input type="checkbox"/> Include subdirectories <input type="checkbox"/> Include system files <input type="checkbox"/> Include hidden files <input type="checkbox"/> Include reparse points <input type="checkbox"/> Include system reparse points

Additional Filters (optional)

File filters	No options selected
Include only filters	No options selected
Exclude any filters	No options selected

Once you create a duplicate, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Default Applications Folder (MacOS)

The default filter for discovering executable files in /Applications on macOS.

Default Applications Folder (MacOS)

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	Default Applications Folder (MacOS)
Description	The default filter for discovering executable files in /Applications on MacOS.
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters

Exclude any filters

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

System Applications Folder (MacOS)

The default filter for discovering executable files in /System/Applications on macOS endpoints.

System Applications Folder (MacOS)

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	System Applications Folder (MacOS)
Description	The default filter for discovering executable files in /System/Applications on MacOS.
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters

Exclude any filters

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

Default Applications Bundle Filter (MacOS)

The default filter for discovering application bundles in /Applications on macOS endpoints.

Default Application Bundles Filter (MacOS)

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	Default Application Bundles Filter (MacOS)
Description	Default Application Bundles Filter (MacOS)
Platform	Mac OS

Settings

Bundle Name	
Bundle Path	/Applications/ <input checked="" type="checkbox"/> Include subdirectories
Match the following property list values	<input type="checkbox"/> App Category <input type="checkbox"/> Bundle Identifier <input type="checkbox"/> Bundle Name <input type="checkbox"/> Bundle Version <input type="checkbox"/> Bundle Version (short) <input type="checkbox"/> Executable File <input type="checkbox"/> Info String <input type="checkbox"/> Min System Version

This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

macOS Executables

The default filter for executable Mach-O files. This filter is available for macOS systems.

Include only files with a Mach-O header marked with attributes set via the filter Settings:

macOS Executables

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	macOS Executables
Description	The default filter for executable Mach-O files.
Platform	Mac OS

Settings

Include only files with a Mach-O header marked with the following attributes.

Cpu Type	All Cpu Types
File Type	Demand Paged Executable File
Flags	<ul style="list-style-type: none"> <input type="checkbox"/> No Undefined References not set ▼ <input type="checkbox"/> Incremental Link Output not set ▼ <input type="checkbox"/> Dynamic Linker Input not set ▼ <input type="checkbox"/> Dynamic Linker Bound Undefined References not set ▼ <input type="checkbox"/> Prebound Dynamic Undefined References not set ▼ <input type="checkbox"/> Split RO And RW Segments not set ▼ <input type="checkbox"/> Run Lazy Init Routine not set ▼ <input type="checkbox"/> Two-Level Name Space Bindings not set ▼ <input type="checkbox"/> Force Flat Name Space Bindings not set ▼ <input type="checkbox"/> Guarantee No Multiple Definitions not set ▼ <input type="checkbox"/> No Dyld Notify not set ▼ <input type="checkbox"/> Prebinding Can Be Redone not set ▼ <input type="checkbox"/> Binds All Modules not set ▼ <input type="checkbox"/> Can Divide Sections not set ▼ <input type="checkbox"/> Canonicalized Binary not set ▼ <input type="checkbox"/> Contains External Weak Symbols not set ▼ <input type="checkbox"/> Uses Weak Symbols not set ▼ <input type="checkbox"/> Stacks Have Stack Execution Privilege not set ▼ <input type="checkbox"/> Safe For Root Use not set ▼ <input type="checkbox"/> Safe For issetguld() Processes not set ▼ <input type="checkbox"/> Do Not Need Examine Dependent Dyllbs not set ▼ <input type="checkbox"/> Load Random Address not set ▼ <input type="checkbox"/> Dead Strippable DYLIB not set ▼ <input type="checkbox"/> Has TLV Descriptors not set ▼ <input type="checkbox"/> No Heap Execution not set ▼ <input type="checkbox"/> App Extension Safe not set ▼
Results should be	excluded ▼

System Application Bundles Filter (MacOS)

The default filter for app bundles files in /System/Applications on macOS endpoints.

System Application Bundles Filter (MacOS)

This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Filter Details

Name	System Application Bundles Filter (MacOS)
Description	System Application Bundles Filter (MacOS)
Platform	Mac OS

Settings

Bundle Name	
Bundle Path	/System/Applications/ <input checked="" type="checkbox"/> Include subdirectories
Match the following property list values	<input type="checkbox"/> App Category <input type="checkbox"/> Bundle Identifier <input type="checkbox"/> Bundle Name <input type="checkbox"/> Bundle Version <input type="checkbox"/> Bundle Version (short) <input type="checkbox"/> Executable File <input type="checkbox"/> Info String <input type="checkbox"/> Min System Version

This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

The Folders area contains all the resource items available by default and custom created in Privilege Manager. It provides an overview for each major items group.

Policies Folder Overview

The screenshot shows the 'Policies' folder overview. On the left, a tree view shows the hierarchy: Policies > General > Group Policy > Privilege Manager Solutions > Application Control > Directory Services > File Inventory > Local Security > Policies > Windows > Managed Users and Groups > Resources. The main pane shows a search bar with 'Find Folder' and a list of 6 items. The items are:

- Group Membership for 'doc-test' in 'Windows Computers' - v. 1
- Password Management Policy for user 'Test Disclosure' on computers in 'Windows Computers'
- Password Management Policy for user 'Test Password Disclosure' on computers in 'Windows Computers'
- User Account Policy for 'Test Disclosure' in 'Windows Computers' - v. 1
- User Account Policy for 'Test Password Disclosure' in 'Windows Computers' - v. 1
- User Account Policy for 'Willson' in 'Windows Computers' - v. 1

Tasks Folder Overview

The screenshot shows the 'Tasks' folder overview. On the left, a tree view shows the hierarchy: Jobs and Tasks > Client Tasks > Client Item Updates > Directory Services > Event Maintenance > File Inventory > Local Security > HelpDesk Tasks > Infrastructure Scheduled Activities > Server Tasks. The main pane shows a search bar with 'Find Folder' and a list of 6 items. The items are:

- Perform Active-X Download Inventory
- Update Application Actions Client Items
- Update Client Commands Client Items
- Update File Filter Resource Client Items
- Update Policy Client Items
- Update Provisioned Resource Client Items

Reports Folder Overview

The screenshot shows the 'Reports' folder overview. On the left, a tree view shows the hierarchy: Reports > Helpdesk Reports > Infrastructure > Privilege Manager Solutions > Resource Reports > Data Class Reports > Related Resource Reports > Resource List Reports > Application Control > Data Class Reports > List Reports > Core > Directory Services > File Inventory > Local Security > Resource Summary Reports. The main pane shows a search bar with 'Find Folder' and a message: '0 Items' and 'No items'. There is an 'Export' button.

Resources Folder Overview



In Privilege Manager Administrators need the ability to export complete policies, including dependent filters, actions, resource targets and any related items. They also need the ability to then import those policies into another instance.

The export and import feature can be used for production environments with multiple instances and for troubleshooting purposes when assistance is needed.

The feature provides the ability

- to export single policies for specific troubleshooting purposes.
- to bulk export via policies folders at any given folder level, except on root folders, depending on specific needs.
- to choose to overwrite or leave in place what's already there.
- to select specific objects or bulk select

This feature supports the bulk migration and creation of policies, including all of their dependencies.

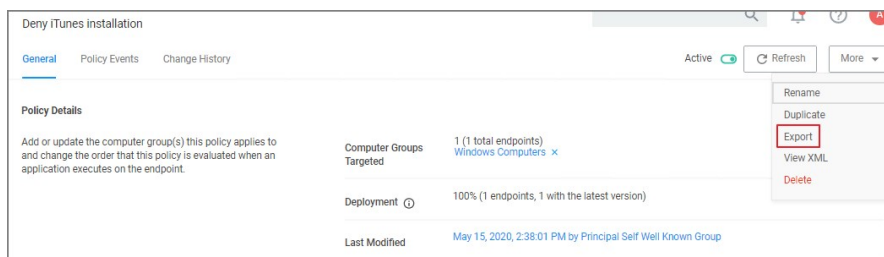
Exporting Items

Items at various levels of complexity can be exported. The UI offers several access points for an export operation.

Specific Policy Export

To export a specific policy with dependent filters and actions:

1. Navigate to the specific Policy and select it.
2. From the top-right **More** menu select **Export**.



3. A modal opens asking the user to confirm the download of the specific policy.



Click **Download**.

The policy is downloaded to your system's default download location as a .zip file

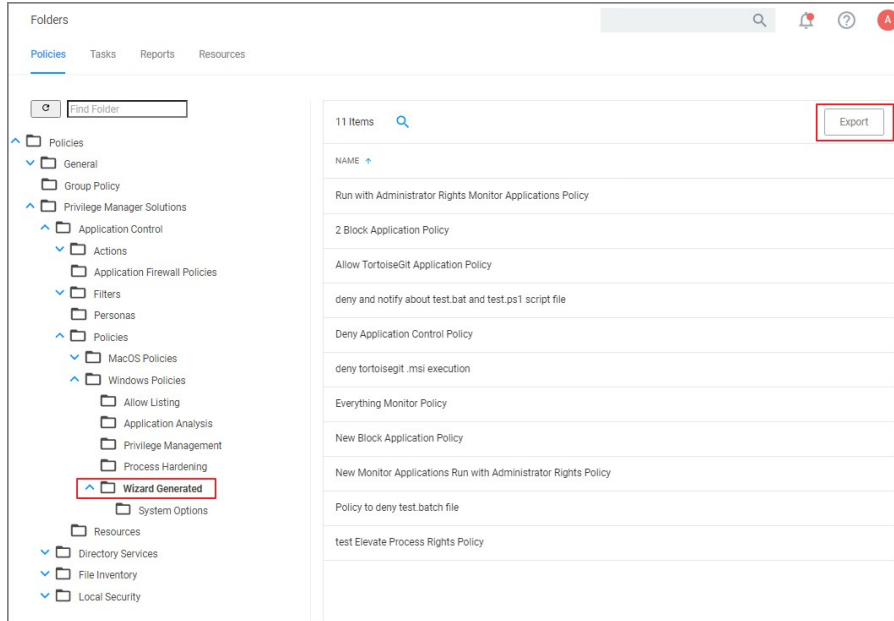
The policy details are downloaded in a zip file named after the policy name that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

The export of filters, tasks, or reports is done in a similar way, by navigating to the specific item, locating the Export button and proceeding through the export process steps.

Folder Exports

Bulk export of items is possible via the Folders page.

1. Navigate to **Admin | Folders**. The export of folders is available on the Policies, Tasks, and Reports. On the Resources tab, the export is only possible for Resource Filters.
2. From the folders tree select any of the available folders.



Click **Export**.

3. A modal opens asking the user to confirm the download of the specific policy.

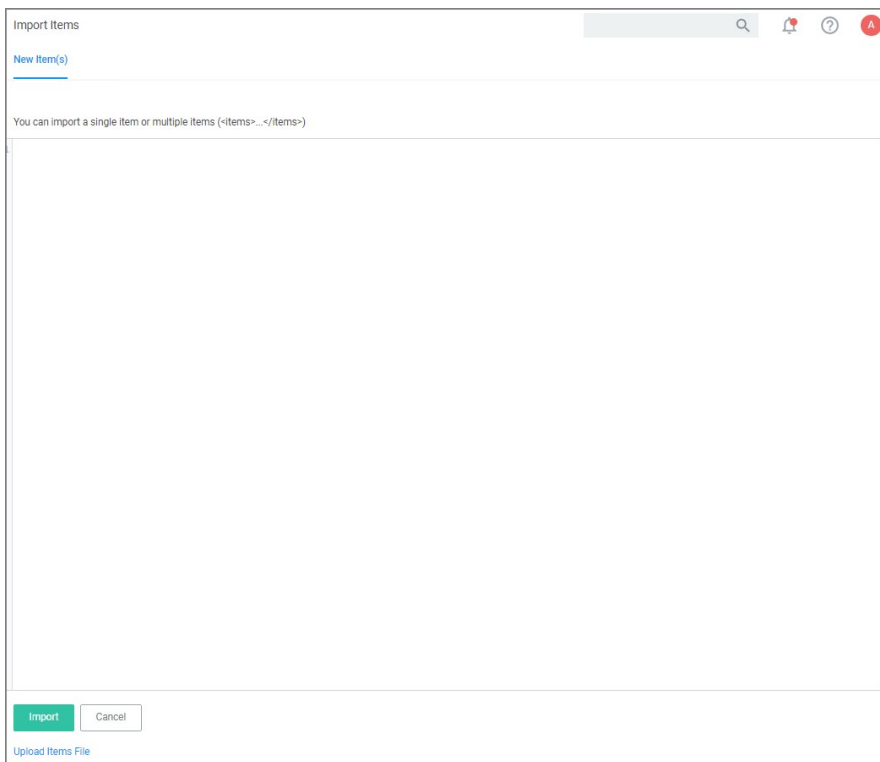


Click **Download**.

The items are downloaded in a zip file named after the folder that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

Note: Prior to importing any data into your environment, Thycotic recommends to create a backup of the current Privilege Manager Database.

Items can be imported in different ways, which are further detailed below.



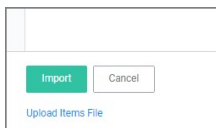
Using Import Items

1. Navigate to **Admin | Import Items**.
2. The xml viewer opens and you may copy xml item data here to import. Or use the **Upload Items File** option as described under [Using Diagnostics Upload Items File](#).

Using Diagnostics Upload Items File

To import items via file upload follow these steps:

1. Navigate to **Admin | Diagnostics** and select **Import Items**.
2. Scroll to the bottom of the page and select the **Upload Items File** link.



3. The **Import Items** dialog opens, browse to your file location and select the file containing the data to import.



Supported file types for the import are .xslt, .xbl, .xsl, .xml, and .zip.

By default the **Overwrite Existing Items** checkbox is selected. If you want to skip items that already exist, un-check the box.

4. Click the **Upload** button.

You can verify the uploaded data by navigating to **Admin | Folders**. Depending on your import, the data is listed under Policies, Tasks, or Resource Filters.

For details about License setup etc., refer to [Getting Started](#).

On-Premises

For On-prem instances licenses can be added and deleted by users with Privilege Manager Administrators' roles.

Licenses							
Utilization Summary							
PRODUCT	OS TYPE	STATUS	TOTAL LICENSES	IN USE	START DATE	AUP RENEWAL	EXPIRES
Privilege Manager Suite	Client	OK	100	0	11/16/2017, 5:28:41 PM		
Privilege Manager Suite	Server	OK	100	1	11/16/2017, 5:28:42 PM		
Installed Licenses							
2 Items							Add License
NAME	LICENSE KEY	EXPIRES	TYPE				
FOR DEVELOPMENT PURPOSES ONLY	2DQ0G-JDNAR-RHZWB-ODAVW-GC544	Does not expire.	Client Delete				
FOR DEVELOPMENT PURPOSES ONLY	TNQ1C-DVY31-U40BF-3LG07-89HS0	Does not expire.	Server Delete				

Cloud

For Cloud instances, licenses can be deleted by users with Privilege Manager Administrators' roles.

Licenses							
Please ensure you only remove superfluous licenses and that valid licenses are not removed. You will be unable to add a new license without the assistance of a Thycotic support member.							
Utilization Summary							
PRODUCT	OS TYPE	STATUS	TOTAL LICENSES	IN USE	START DATE	AUP RENEWAL	EXPIRES
Privilege Manager Suite	Client	OK	100	13	11/16/2017, 12:28:41 PM		
Privilege Manager Suite	Server	OK	100	1	11/16/2017, 12:28:42 PM		
Installed Licenses							
3 Items							
NAME	LICENSE KEY	EXPIRES	TYPE				
FOR DEVELOPMENT PURPOSES ONLY	*****-*****-*****-IC544	Does not expire.	Client Delete				
FOR DEVELOPMENT PURPOSES ONLY	*****-*****-*****-19HS0	Does not expire.	Server Delete				
FOR DEVELOPMENT PURPOSES ONLY (3 Year Ter...	*****-*****-*****-AMZ0	November 15th 2020, 12:28:42 pm	Support Delete				

Cloud licenses can only be added by Thycotic support members.

The Server Logs provide insight into the Privilege Manager Server Logs.

TIMESTAMP	SEVERITY	MESSAGE	PROCESS	SERVER
10/15/20, 4:30 PM	Information	Dispatching tasks for schedule 'Resource Targeting Update' (79983944-adfb-4632-ad37-192b0...	/TMS/Worker	demo-server
10/15/20, 4:30 PM	Information	Got message to update client item 30e52018-c4dc-497a-898f-2af5fe84b9ef.	/TMS/Agent	demo-server
10/15/20, 4:30 PM	Information	Got message to update client item 7588fc50-9ff9-41dd-8922-44e47c4a587c.	/TMS/Agent	demo-server
10/15/20, 4:30 PM	Information	Got message to update client item cd280aa5-14af-47af-be3f-622081433578.	/TMS/Agent	demo-server
10/15/20, 4:30 PM	Information	Got message to update client item da915de8-94dd-4d75-a849-c0540552aee7.	/TMS/Agent	demo-server
10/15/20, 4:30 PM	Information	Got message to update client item b88e93ee-67ec-4dbb-baa5-dca1a5ee017e.	/TMS/Agent	demo-server
10/15/20, 4:30 PM	Information	Work complete for 'Collection and Resource Targeting Update Worker' (e84608f0-f656-48c7-8...	/TMS/Worker	demo-server
10/15/20, 4:30 PM	Information	Starting work for 'Collection and Resource Targeting Update Worker' (e84608f0-f656-48c7-891...	/TMS/Worker	demo-server
10/15/20, 4:30 PM	Information	Dispatching tasks for schedule 'Collection Update' (e8c63fa0-9e99-4cd9-b67b-19dbd69ad91).	/TMS/Worker	demo-server
10/15/20, 4:30 PM	Warning	Ignoring save for change tracking item b95536ae-05fe-472c-ab89-a90491dd28b2 because ther...	/TMS/Worker	demo-server
10/15/20, 4:30 PM	Information	Dispatching tasks for schedule 'Client Item Update' (87e415f2-29e2-4584-947a-d0a06d8fc521).	/TMS/Worker	demo-server

By default the Server Logs are shown for the last 30 minutes and with the Severity and Application set to All. These change be changed via the available drop-down options:

Duration

Last 30 Minutes ▾

- All
- ✓ Last 30 Minutes
- Last Hour
- Last 4 Hours
- Last 12 Hours
- Last 24 Hours
- Last 7 Days
- Custom

Severity

Severity: All ▾

- ✓ All
- Verbose
- Information
- Warning
- Error
- Critical

Application

Application: All ▾

- ✓ All
- Core
- Agent
- Worker
- Services
- ServiceBus
- Setup

Details

Details for a log entry can be viewed by clicking on the row containing the log entry.

Server Log Detail

Time: Nov 3, 2020
 Severity: Warning
 Process: /TMS/Worker
 Server: [REDACTED]

```

1 Ignoring save for change tracking item b95536ae-05fe-472c-ab89-a90491dd28b2 because there is no item operation
2 at Thycotic.Platform.BaseItem.ItemImplementationManager.ConstructSaveCommands(IItem item, AmsSqlCommandColle
3 at Thycotic.Tms.Item.BaseItem`2.ConstructSaveCommand(AmsSqlCommandCollection commands)
4 at Thycotic.Tms.Item.BaseItem`2.AttemptSaveInternal()
5 at Thycotic.Utilis.RetryHelper.Retry(Int32 retries, Action action, Predicate`1 canRetry)
6 at Thycotic.Tms.Item.BaseItem`2.Save()
7 at Thycotic.Platform.Managers.CredentialManager.SetPasswordWithChangeTracking(Guid resourceId, SecureString
8 at Thycotic.Platform.DataClass.PasswordChangeDataClassDataLoaderImplementationProvider.SaveDataClassData(IDa
9 at Thycotic.Platform.Resource.ResourceDataLoader.Save(IPerformanceCounterContextProvider pcc, String pccName
10 at Thycotic.Platform.Resource.DataLoader.CommitResources()
11 at Thycotic.Platform.Resource.DataLoader.OnProcessClientMessageResources(XmlReader dataReader)
12 at Thycotic.Platform.Resource.DataLoader.Process(XmlReader dataReader)
13 at Thycotic.Tms.Item.Resource.BaseDataLoadingItem`2.OnProcessInventoryMessageXml(XElement elem, Inventory
14 at Thycotic.Tms.Item.Resource.BaseDataLoadingItem`2.OnProcessInventoryMessage(InventoryMessage invMsg, DateT
15 at Thycotic.Tms.Item.Resource.BaseDataLoadingItem`2.ProcessMessage(IMessage message)
16 at Thycotic.Platform.Messaging.DefaultReliableMessageProcessor.Process(IReliableMessageReference messageRef)
  
```

[Close](#)

Search by CorrelationID

The Server Logs are searchable via CorrelationID for better troubleshooting support. If you are looking for log details about an error that occurred in the UI, copy the CorrelationID from the error message and enter it in the table grid search field.

- Error providing CorrelationID:

- Search Server Logs for CorrelationID:

TIMESTAMP	SEVERITY	MESSAGE	PROCESS	SERVER
11/3/20, 6:31 PM	Error	Service request "POST" to "https://127.0.0.1/TMS/Services/api/Item/Import?folderid=null&productid=null&impor...	/TMS/Services	[REDACTED]

- Details for error based on CorrelationID search:

Server Log Detail

Time: Nov 3, 2020

Severity: Error

Process: /TMS/Services

Server: XXXXXXXXXX

```
1 Service request "POST" to "https://127.0.0.1/TMS/Services/api/item/Import?folderId=null&productId=null&importFl
2
3 ( Exception Details: System.InvalidOperationException: Uploaded file of unknown type "application/octet-stream"
4 at Thycotic.Tms.ServiceRole.Services.Json.ItemManagementService.ImportItems2(Nullable`1 folderId, Nullable`1
5 at lambda_method(Closure , Object , Object[] )
6 at System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ActionExecutor.<>c__DisplayClass.<GetExecutor>
7 at System.Web.Http.Controllers.ReflectedHttpActionDescriptor.ExecuteAsync(HttpControllerContext controllerCo
8 --- End of stack trace from previous location where exception was thrown ---
9 at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
10 at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
11 at System.Web.Http.Controllers.ApiControllerActionInvoker.<InvokeActionAsyncCore>d__0.MoveNext()
12 --- End of stack trace from previous location where exception was thrown ---
13 at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
14 at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
15 at System.Web.Http.Filters.ActionFilterAttribute.<CallOnActionExecutedAsync>d__5.MoveNext()
16 --- End of stack trace from previous location where exception was thrown ---
17
```

Close

In Privilege Manager, Personas are collections of privileges for specific roles at an organization. You can assign Personas to users on a specific Computer Group to elevate their identity to perform specific tasks.

For example: A "SQL Administrator" Persona might be created that assigns rights to launch Certificate Manager and SQL Server Configuration Manager. Only users under this Persona would be allowed to execute these applications on your network.

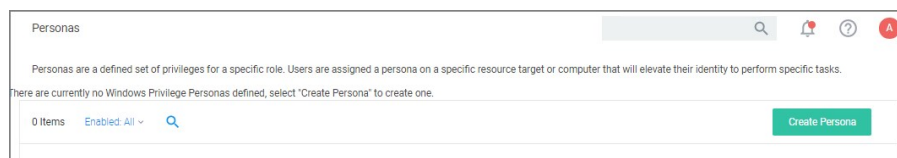
Note: It is recommended to setup Active Directory Synchronization first and run the synchronization task to then easily assign Personas to domain user groups.

Viewing your Personas

To see all your Personas navigate to **Admin | Personas**. From the Windows Privilege Personas page, you can create new Personas and manage existing Personas.

Creating a Persona

To create a Persona, click **Create Persona**. You will be presented with a dropdown list of Persona Templates to choose from.



Custom Persona	An empty Persona template for the users to customize based on their needs.
Network Administrators Persona	Automatically elevates applications that are commonly needed to manage network configurations. Elevate DHCP, DNS, and NLB Configuration
Security Administrators Persona	Automatically elevates applications that are commonly needed to manage local users and security settings. Elevate Local User and Groups and Group Policy Object Editor
SQL Administrators Persona	Automatically elevates applications that are commonly needed to manage SQL servers. Elevate Certificate Manager, ODBC Configuration, and SQL Server Configuration Manager
Storage Administrators Persona	Automatically elevates applications that are commonly needed to manage file storage settings. Elevate Disk Defragmentation, Disk Management, iSCSI Connection Configuration, Quota Management, Shared Folders, and Windows Backup
Web Administrators Persona	Automatically elevates applications that are commonly needed to manage web servers. Elevate App Pool Recycling, Certificate Manager, IISReset, and adding TCP Firewall Rules

Select a Persona Template and then provide a Name and Description. Once you are ready to proceed, click Create. If you selected any Persona Template other than Custom Persona then you will have pre-populated Behaviors that you can choose to delete or keep. Otherwise, you will start with a blank Persona.



For Persona Settings, you can change the name, description, and whether the Persona will be enabled. For Persona Behaviors, you can click Add Behavior and choose which privilege(s) you want to allow for this Persona. Finally, for Persona Targets you can choose which Active Directory Domain User Groups this Persona will affect and on which Active Directory Organizational Units this Persona will apply.

New Web Administrators Persona

Details Refresh More

Details

Name

Description

Enabled No

Behaviors Add Behavior

NAME	PARAMETERS	
Elevate App Pool Recycling via AppCmd Recycle	No additional parameters	<input type="button" value="x"/>
Elevate IIS Manager (inetmgr.exe) Privilege	No additional parameters	<input type="button" value="x"/>
Elevate IISReset Privilege	No additional parameters	<input type="button" value="x"/>

Targets

This Persona does not have any targets. To add targets click the "Add Target" button below.

Add Target

Set the persona to **Enabled** and click **Save Changes** to finish creating your Persona.

The Resource Explorer provides information about any type of resource item in Privilege Manager.

The Resource Explorer provides:

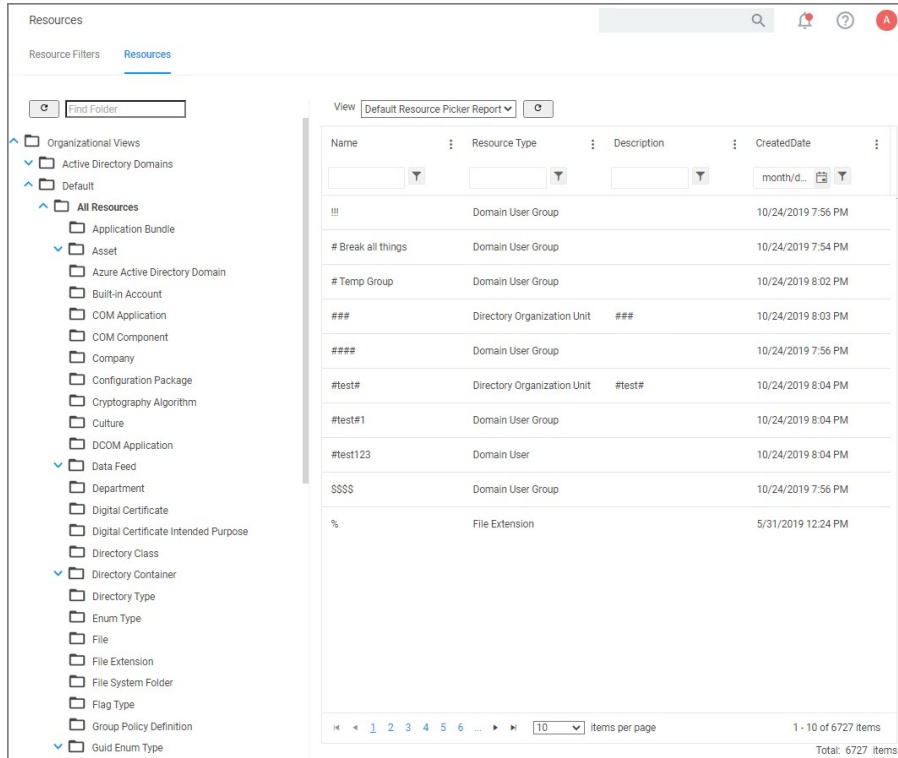
- **Summary**, which contains general information, such as name, description, and modified date for any resource accessed.
- **Known Data**, such as any data known that relates to the resource. This data is different from resource type to resource type. For example, a domain has Global Domain Details and no account details, and a file will have all sorts of information pertaining to the file.
- **Events** are log-style data entries that are directly related to the resource. For example for discovered files, those are the events that are reported from an endpoint.
- **Associations**, are any associated/related items.

Resources can be deleted from the Resource Explorer page.

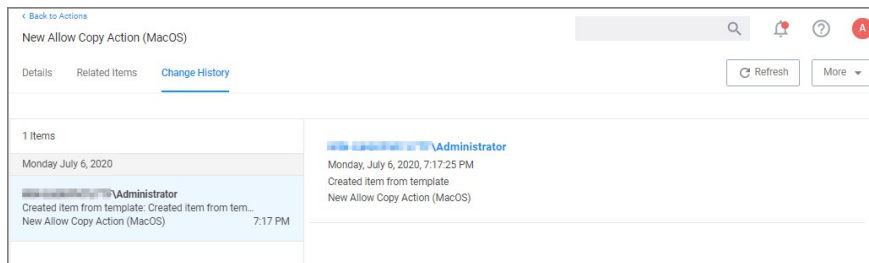
Note: Only use Delete when you are absolutely sure that you want to delete that resource. Clicking on Delete will delete the current resource record you are viewing.

The Resource Explorer is accessible by either navigating to

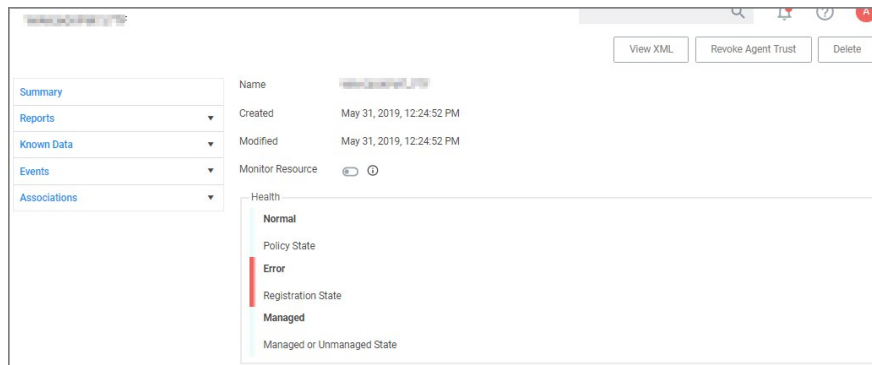
- **Admin | Resources** and expanding the Resources tree drilling down to a named resource to further explore and/or edit.



- **Change History** tab of a named resource.



- any named item, such as a report, in the Privilege Manager console and selecting a named resource. Example navigation for the following image, *Admin | Agents | select one system from the list | select one computer from "Managed Computers by Operating System" list:*

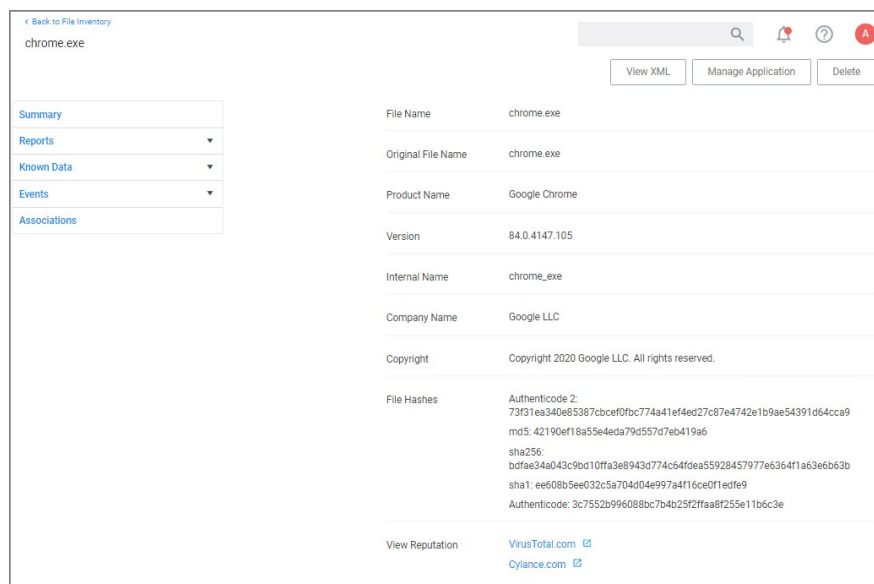


Example for Discovered Files

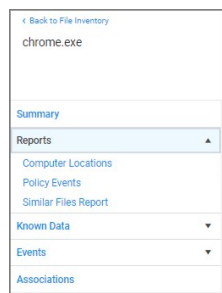
You enter the Resource Explorer for discovered file through **File Inventory** on the main navigation tree. On the Events page, click any of the discovered files and use **View File** to drill down to the files resources.

The following image shows all discovered information about the chrome.exe file, such as:

- File Name
- Original File Name
- Product Name
- Version
- Internal Name
- Company Name
- Copyright information
- File Hashes
- View Reputation, if a reputation provider is integrated with your Privilege Manager instance.



Under the **Reports** drop-down you can look at further details on the **Computer Locations**, **Policy Events**, and **Similar Files Report** tabs.



The **Computer Locations** tab provides details about the discovery locations where the file was discovered.

The **Policy Events** tab provides details about the policy events that triggered by the file if executed.

The **Similar Files Report** tab provides a list of and links to similar files that have been discovered by Privilege Manager.

chrome.exe

View XML Manage Application Delete

Summary

Reports

- Computer Locations
- Policy Events
- Similar Files Report
- Known Data
- Events
- Associations

Drag column here for grouping

Product Name	Win32 Executa...	Internal Name	Company Name	Product Version	File Version
Google Chrome	elevation_service...	elevation_service...	Google Inc.	74.0.3729.169	74.0.3729.169
Google Chrome	chrome.exe	chrome_exe	Google LLC	75.0.3770.100	75.0.3770.100
Google Chrome	elevation_service...	elevation_service...	Google LLC	75.0.3770.100	75.0.3770.100
Google Chrome	elevation_service...	elevation_service...	Google LLC	75.0.3770.142	75.0.3770.142
Google Chrome	chrome.exe	chrome_exe	Google LLC	75.0.3770.142	75.0.3770.142
Google Chrome	chrome.exe	chrome_exe	Google LLC	76.0.3809.100	76.0.3809.100
Google Chrome	elevation_service...	elevation_service...	Google LLC	76.0.3809.100	76.0.3809.100
Google Chrome	elevation_service...	elevation_service...	Google LLC	76.0.3809.132	76.0.3809.132
Google Chrome	chrome.exe	chrome_exe	Google LLC	76.0.3809.132	76.0.3809.132
Google Chrome	elevation_service...	elevation_service...	Google LLC	77.0.3865.90	77.0.3865.90

The Known Data for a discovered file includes details like the

- File Inventory, which provides COFF Header and File Digital Signature data in raw form.

chrome.exe

View XML Manage Application Delete

Summary

Reports

- Computer Locations
- Policy Events
- Similar Files Report
- Known Data
- File Details
- File Digital Signature
- File Inventory
- COFF Header
- File Digital Signature Raw
- File Header Raw
- macOS Package Summary
- Hash
- Software Management
- Events
- Associations

View Default Viewer

NAME	VALUE
Characteristics	34
Checksum	1864253
Machine	34404
Magic	523
MajorImageVersion	0
MajorOperatingSystemVersion	5
MajorSubsystemVersion	5
MinorImageVersion	0
MinorOperatingSystemVersion	2
MinorSubsystemVersion	2
NumberOfSections	10
NumberOfSymbols	0
Subsystem	2
TimeDateStamp	2020-07-24T19:32:43-04:00
Win32VersionValue	0

- Software Management, which provides the files Manifest, Version Info in raw form, and Win32 Executables details.

NAME	VALUE
CompanyName	Google LLC
Copyright	Copyright 2020 Google LLC. All rights reserved.
FileSubType	0
FileType	1
FileVersion	84.0.4147.105
InternalName	chrome_exe
Language	English (United States)
OriginalFileName	chrome.exe
ProductName	Google Chrome
ProductVersion	84.0.4147.105

- File Details, such as name, file extension, file size, and if protected or not.
- File Digital Signature, which provided information on the Signer, Countersigner if available, and the signature date/time stamp.
- Hash, provides details on the name, the hash, and hex hash.

Under Events, Infrastructure offers a view into the Resource Discovery events that discovered the file, in this example the File Agent Discoverer and File Agent Discoverer (File Location) events.

NAME	VALUE
AgentDiscovererResourceId	5410f92f-5abe-482e-957f-b989738c00b8
Discovered	2020-07-28T11:17:44-04:00
ResourceDiscovererId	ee05db41-a444-40e9-910e-aa2682dba8fa

This discovered file resource has no related items associated and thus the Associations area of the Resource Explorer is empty.

Example for User Resource

When you are looking at change history for any item and click the view user link, you access the **Resource Explorer** for that specific user resource. The Summary information for that specific user resources shows:

- Name – this is the user account that made the change.
- Created – indicates when the item was created.
- Modified – indicates when the item was last modified.

MacOS Catch-all Monitor Policy

General Policy Events **Change History**

Inactive Refresh More

2 Items

Thursday August 6, 2020

Thursday, August 6, 2020, 4:06:20 PM

Saved item
MacOS Catch-all Monitor Policy

Administrator
Saved item: Stage 2 processing : True , made 7 othe...
MacOS Catch-all Monitor Policy 4:06 PM

Administrator
Created item from template: Created item from tem...
MacOS Catch-all Monitor Policy 1:33 PM

Stage 2 processing True False

Continue enforcing policies for child processes after enforcing this policy False True

Continue enforcing policies after enforcing this policy False True

Exclusion filters
Default App Bundles File Specification Filter

Application targets
Mac OS /Users/ File Specification

ApplyToResourcesSettings \ AllowedTargetRoleTypeId
Computer 00000000-0000-0000-0000-000000000000

State \ ResourceTargetids
MacOS Test Computer Group Scoped to Mac Computers

Enabled False

The resource explorer is providing information about the current state of that user resource.

Administrator

View XML Delete

Summary	Name	Administrator
Reports	Created	Sep 12, 2019, 6:00:40 PM
Known Data	Modified	Sep 12, 2019, 6:00:40 PM
Events		
Associations		

Under **Known Data** we can explore the information for **Security Management | Global Account Details**.

Administrator

View XML Delete

View: Default Viewer

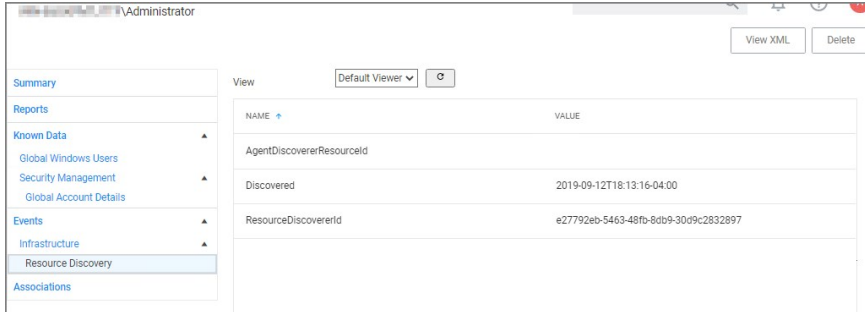
NAME	VALUE
AccountDomain	...
Description	
IsBuiltin	false
Name	ADMINISTRATOR
Rid	500
SID	...

Users can select the View from the drop-down and see information on the type of the resource. User resources provide details about:

- AccountDomain – identifies the domain for the user account.
- Description
- IsBuiltin – can be true false to indicate if the account is built-in or not.
- Name – Name associated with the user account.
- Rid
- SID

Selecting the Global Windows Users information shows Name, Domain, and Userid.

Under **Events**, you can view **Infrastructure | Resource Discovery** information:



Under **Associations** you can see related items, such as **Group Membership**, which is based on the users credentials.

Error Message after Deleting a User Resource

In case a resource was deleted, an error message like the following will be shown the next time the resource view link is accessed.

InvalidItemIdException

The server could not find an item required for this request. Please check the server logs for additional information.
The specified Guid '9c0f4d76-5557-4aab-941d-3d13bc30cf81' is not a valid item.

The following Privilege Manager roles are available by default and it is possible to add to or remove members from these roles. Privilege Manager also allows the creation of new roles, if a customer environment requires more role support.

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED
Privilege Manager Administrators	Privilege Manager Administrators	Trusted Installer	6/23/20, 8:48 PM
Privilege Manager Field Engineering		Trusted Installer	6/23/20, 8:48 PM
Privilege Manager Helpdesk Users	Privilege Manager Helpdesk Users	Trusted Installer	6/23/20, 8:48 PM
Privilege Manager MacOS Administrators	Privilege Manager MacOS Administrator	Trusted Installer	6/23/20, 8:48 PM
Privilege Manager Users	Privilege Manager Users	Trusted Installer	6/23/20, 8:48 PM
Privilege Manager Windows Administrators	Privilege Manager Windows Administrators	Trusted Installer	6/23/20, 8:48 PM

< **Note:** Privilege Manager's Roles logic prevents the removal of a user account with an Administrator Role, if that user account is the last with those Administrator Role privileges. Privilege Manager does not allow current users to delete their own account.

Note: Privilege Manager manages the roles of users accessing the console, unless Privilege Manager is connected to Secret Server. When connected to Secret Server, role membership is controlled by Secret Server.

Also refer to the following topic: [User Credentials and Roles](#).

All these roles are considered application role permissions.

Privilege Manager Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console.

Privilege Manager Field Engineering

This role is reserved for future use.

Privilege Manager Helpdesk Users

This role allows the user to have approve or deny escalation requests access. The helpdesk role can also disclose passwords.

Privilege Manager MacOS Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to macOS systems. This role can view but not edit Windows policies.

Privilege Manager Users

This role allows the user to have read permissions to most items, but no rights to modify security permissions. This role can disclose passwords.

Privilege Manager Windows Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to Windows systems. This role can view but not edit macOS policies.

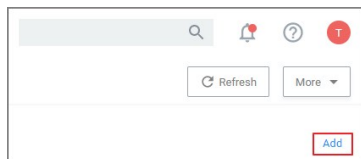
Creating/Deleting Roles

To create a new role,

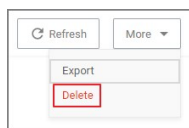
1. On the top of the Roles page, click **Create**.
2. Enter a name for the role, a description, and an account name.
3. Click **Create**.

Once has been added, the new role's page opens and you can

1. Add Users to or edit the role, via **Add**.



2. Delete the role, via **More | Delete** and then confirm on the Delete Item modal by clicking **Delete Item**.



Delete Item

Item to be deleted: [Doctest - Privilege Manager New Users](#)

Cancel

Delete Item

The following table provides an overview of Privilege Manager Application Roles:

Privilege Manager Administrators	Can do anything.	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	
Privilege Manager Field Engineering	Cannot do anything out of the box. Reserved for future use.												
Privilege Manager Helpdesk Users	This role has the least permissions. It can disclose passwords and manage approvals only.				yes		yes						
Privilege Manager MacOS Administrators	Can do anything an administrator can, but only for macOS policies and resource targets.	yes (macOS)	yes	yes	yes		yes	yes		yes (macOS)	yes	yes	yes
Privilege Manager Users	This is a read only role that can view all items, disclose passwords, and manage approvals.		yes		yes		yes				yes		
Privilege Manager Windows Administrators	Can do anything an administrator can, but only for Windows policies and resource targets.	yes (Win)	yes	yes	yes		yes	yes		yes (Win)	yes	yes	yes

Refer to the [Upgrade](#) to learn more about Privilege Manager's setup feature for updates.

In Privilege Manager tasks are activities that can be run on demand or regularly scheduled. If they are regularly scheduled, the schedule triggers the execution of a task instance, which performs specific actions based on set parameters.

Remote Scheduled Client Command type tasks that are considered agent-side require policies to be applied on the agent endpoints, the ones that are considered server-side do not require policies to be executed.

Tasks are set-up via **Admin I More** and then selecting the Tasks link. They are categorized as following:

- [Client Tasks](#)
- [Server Tasks](#)
- [HelpDesk Tasks](#)
- [Infrastructure Scheduled Activities](#)

The following general task topics are available:

- [Agent Hardening](#)
- [Maintenance tasks details](#)
- [Other tasks to schedule](#)
 - [Emailing Reports](#)
- [Reset Licensing](#)
- [Tasks Launching Executables without User Context](#)

Note: Upgrading to Privilege Manager 10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **MacOS Computers**.

If you want to prevent this automatic merge, modify the XML of this item:

```
PrivilegeManager/Item/xml/b2e02684-d154-48ca-9987-12b1759df822
```

Add on line 2 <adc:Attributes>NoModify</adc:Attributes>.

Client Tasks

Client Tasks are used to run or schedule activities at the endpoints, like:

- Basic Inventory, which triggers the agent to immediately report basic inventory back to the server. The information can be viewed for a computer under Known Data. Data sets are different based on endpoint operating system.
- Resource Discovery Client Task, which populates agent-side data for any resources that have been discovered but lack detailed information.
- Update Applicable Policies, which triggers policy updates at the endpoints.

Note: All default enabled client tasks are **read-only items** and if any customization to the schedule is required, create a copy to add, save, and apply changes. Schedule changes can be added on the Triggers page when clicking the existing schedule and then **Show Advanced**.

Details for each task are provided under the following topics:

- [Basic Inventory](#)
- [Cleanup Agent Inventory Transfer](#)
- [COM Inventory Policy](#)
- [Cleanup Sent Privilege Manager Event](#)
- [Configure PM Remove Programs](#)
- [Default File Inventory Policy](#)
- [Ensure UAC Override Setting](#)
- [Local User Inventory Policy](#)
- [Perform Resource Discovery](#)
- [Retry Errored TMS Events](#)
- [Set Agent Log Size](#)
- [Scheduled Check for Pending Tasks](#)
- [Shared Folder Inventory Policy](#)
- [Scheduled Registration](#)
- [Update Agent Commands](#)
- [Update Applicable Policies](#)
- [User Logon Inventory Policy](#)
- [Update Provisioned Resource Client Items](#)
- [Windows Server Inventory Policy](#)

Basic Inventory

Basic Inventory (Initial, Windows) and (Initial, Mac OS) are scheduled to run at a client's initial start-up after the agent is installed. The cause of the policy's trigger is the task creation.

The common Basic Inventory is scheduled to run daily at 8 am.

For Windows systems the policies instruct the agent on the client system to report the following WMI classes to the server:

- Win32_ComputerSystem,
- Win32_ComputerSystemProduct
- Win32_OperatingSystem WMI

Basic Inventory (Initial, Windows)

Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: ROOT\CIMV2:WIN32_ComputerSystemProduct, ROOT\CIMV2:Win32_ComputerSystem, ROOT\CIMV2:Win32_OperatingSystem
Triggers	Daily at 10:00:00 AM Upon task creation/modification
Targets	All Windows Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	250 KB
Agent Received Size	n/a
Restrictions	none

Basic Inventory (Windows)

Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: ROOT\CIMV2:WIN32_ComputerSystemProduct, ROOT\CIMV2:Win32_ComputerSystem, ROOT\CIMV2:Win32_OperatingSystem
Triggers	Daily at 8:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Initial, Mac OS)

Default Active	Yes
Command	Perform Basic Inventory (MacOS)
Triggers	Daily at 10:00:00 AM

	Upon task creation/modification
Targets	All MacOS Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Mac OS)

Default Active	Yes
Command	Perform Basic Inventory (MacOS)
Triggers	Daily at 10:00:00 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Cleanup Agent Inventory Transfer

Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.

Cleanup Agent Inventory Transfers (Windows)

Default Active	Yes
Command	Cleanup Agent Inventory Transfers
Triggers	Daily at 2:00:02 AM
Targets	10.8: Windows Computers Legacy: All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of failed file transfers
Agent Received Size	n/a
Restrictions	none

Cleanup Sent Privilege Manager Events

Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.

Cleanup sent Privilege Manager Events (Windows)

Default Active	Yes
Command	Remove sent TMSClient Events (Windows)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

Cleanup sent Privilege Manager Events (Mac OS)

Default Active	Yes
Command	Remove sent TMSClient Events (MacOS)
Triggers	Daily at 2:30:02 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

COM Inventory Policy

The purpose of this policy is to inventory COM+ and DCOM packages installed on the client. The inventory of these package

COM+ (Component Object Model) and DCOM (Distributed Component Object Model) utilize RPC calls for component communication and access to the object's methods and data. Running an inventory on those packages on a client is beneficial, if apps using those packages require elevation or should be denied.

Default Active	No
Command	Local Security COM Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of COM+ and DCOM packages
Agent Received Size	n/a
Restrictions	none

Configure Privilege Manager Remove Programs

Configure the [Privilege Manager Remove Programs](#) behavior.

For standard users the utility by default,

- adds all programs to the Control Panel.
- hides repair options for all installers.
- shows the blocked installer list.
- prevents Thycotic software from being uninstalled.

Default Active	Yes
Command	Configure Remove Programs Application
Parameters	selected: Add to Control Panel, Hide Repair for All Installers, Show Blocked Installers in List, Vendor software that can't be Uninstalled: Thycotic.
Triggers	Daily at 10:00:00 PM (repeating every 2 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

Default File Inventory Policy

The purpose of this policy is to inventory software programs running on the managed computer.

These policies use their respective OS based File Specification filters, which in turn have a set of optional additional filters to identify the programs to be inventoried.

Default File Inventory Policy (Windows)

Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (Windows)
Triggers	Weekly on Sun at 3:00:00 AM
Targets	All Windows Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	none

Default File Inventory Policy (MacOS)

Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (MacOS), Default App Bundles File Specification Filter
Triggers	Weekly on Sun at 3:00:00 AM
Targets	All Mac OS Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	none

Ensure UAC Override Setting (Windows)

Ensures that the UAC Override Registry Key is set.

Default Active	Yes
Command	Ensure UAC Override Registry Key
Parameters	Default File Specification (Windows)
Triggers	Daily at 12:00:00 AM At startup
Targets	10.8- Windows Computers Legacy: All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 15 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

Local User Inventory Policy

The purpose of this policy is to inventory Local User accounts, groups and group membership on the client. This policy can also be used to inventory specific account privileges.

Local User Inventory Policy

Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of users and groups
Agent Received Size	n/a
Restrictions	GPO - Audit Account Management enabled does not use Security Event Log

Local User Inventory Policy (MacOS)

Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of users and groups
Agent Received Size	n/a
Restrictions	none

Perform Resource Discovery

Schedule on which agents check with server to determine, if any local resources require discovery.

After any type of resource discovery, it might be possible that the server does not have all the details required to correctly identify what was initially provided by the agent. The agent periodically checks in with the server, if any additional information needs to be discovered. The sever then sends information back to the agent about any pending item clarifications.

Perform Resource Discovery (Windows)

Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 12:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on server request
Agent Received Size	depends on request volume and the number of items pending on server for clarification
Restrictions	none

Perform Resource Discovery (Mac OS)

Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 3:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	MacOS Computers
Conditions	Idle: None specified by default
	Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on server request
Agent Received Size	depends on request volume and the number of items pending on server for clarification
Restrictions	none

Retry Errored TMS Events

Scan Agent queue for any events that require retransmission.

Retry errored TMS Events (Windows)

Default Active	Yes
Command	Retry errored TMS Client Events (Windows)
Parameters	Force Resending (incl. transient errors)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	none

Retry errored TMS Events (Mac OS)

Default Active	Yes
Command	Retry errored TMS Client Events (MacOS)
Triggers	Daily at 2:00:02 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	none

Scheduled Check for Pending Tasks

Scheduled Check Pending Client Tasks - Internet Clients (Windows)

Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.

Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	depends on number of pending items
Restrictions	none

Scheduled Registration

Scheduled Registration (Windows)

Initiate agent registration with server.

Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Scheduled Registration - Internet Clients (Windows)

Initiate agent registration with server less frequently than internal clients.

Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Scheduled Registration (Mac OS)

When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.

Default Active	Yes
Command	Start TMS Registration
Triggers	Daily at 2:00:00 AM (repeating every 1 hour for a duration of 24 hours)
Targets	All MacOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).

(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Set Agent Log Size

Configures the size of the Agent Event Log. By default this is set to 1 MB. For most environments it is recommended to increase the Agent Event Log size. This task can be used to override the default setting.

Default Active	No
Command	Set Agent Log Size (Windows)
Parameters	Log Size: 20 MB
Triggers	Daily at 6:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

Shared Folder Inventory Policy

The purpose of this policy is to inventory shared folders on the client.

Default Active	No
Command	Local Security Shared Folder Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of shared folders on the endpoint
Agent Received Size	n/a
Restrictions	none

Update Agent Commands

Task sends up request for hashes of specific client item types. With Privilege Manager version 10.7 and up returned items are filters based on the last time run the task ran.

Update Agent Commands (Windows)

Instructs Agent to update any agent commands if required.

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Agent Commands (Mac OS)

When this policy is triggered the Agent will update agent command items.

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	depends on the number of updated commands
Restrictions	none

Update Applicable Policies

Update Applicable Policies (Windows)

Instructs Agent to check with server for policy changes.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Applicable Policies - Internet Clients (Windows)

Instructs Agent to check with server for policy changes less frequently than internal clients.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 2 hours for a duration of 24 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Applicable Policies (Mac OS)

When this policy is triggered the Agent will check the server for updated policies.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All MacOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).

(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	depends on the number of updated policies
Restrictions	none

Update Provisioned Resource Client Items

These policies trigger the Agent to force a Client Item Update for provisioned resources on the specific client system.

Update Provisioned Resource Client Items (Windows)

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on the number of provisioned items
Agent Received Size	n/a
Restrictions	none

Update Provisioned Resource Client Items (MacOS)

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All MacOS Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on the number of provisioned items
Agent Received Size	n/a
Restrictions	none

User Logon Inventory Policy

Updates user logon data based on a given schedule to provide primary user information.

Default Active	Yes
Command	Windows Logon Event Processor
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of user sessions
Agent Received Size	n/a
Restrictions	none

Windows Server Inventory Policy

The purpose of this policy is to inventory Windows Services on the client.

Default Active	Yes
Command	Local Security Service Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it ran for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of installed windows services
Agent Received Size	n/a
Restrictions	none

Server Tasks

Component Based List of Default Tasks

Application Control	Get Security Rating for File	Get/update the security rating for the given file.
	Get Security Ratings for Files	Get/update the security ratings for the given files.
	Refresh Security Rating Reports	Refreshes old security rating reports for resources rated by the given provider.
Application Control Cylance		
Directory Services	Default Import AzureAD Users/Groups	Run this task to import/update Azure AD users and groups.
	Default Import Directory	Run this task to import/update directory OUs, users, and containers.
	Default Import Directory Computers	Run this task to import/update directory computer resources.
	Default Import Directory Sites	Run this task to import/update directory sites.
	Import Specific Azure AD Users and Groups	Import specific users and groups from Azure Active Directory.
	Merge Duplicate Account SID Resources	Run this task to merge resources that have a duplicate account SID.
	Synchronize Organizational Unit Server Task	Synchronize Organizational Unit Server Task.
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
Email Tasks	Send Gauge Summary E-mail Task	Send a specific report on a schedule.
File Inventory	Inventory File	Run this task to collect detailed information on the selected file for reports, filters, etc.
	Inventory File Resource	Run this task to update information on an existing file resource for reports, filters, etc.
	Inventory Package	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Package with Exclusions	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages	Run this task to scan the contents of a list of packages and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages Referenced in Allow Lists	Run this task to collect detailed information for files contained in packages referenced in one or more allow lists.
	Inventory Uploaded File	This task is used internally to collect detailed information from files uploaded remotely to the server. It is visible only for status information and troubleshooting.
Foreign Systems		
	SCCM	Tasks here let you synchronize users, computers, and specific SCCM collection.
	ServiceNow	Creates ServiceNow Approval Request items.
	Symantec Management Platform	Tasks here let you synchronize SMP collections and package(s).
	Syslog	Creates tasks to send events to the configured syslog server based on specific templates.
Local Security	Update Primary User	Updates the primary user for the given computer resource.
	Update Primary User for Collection	Updates the primary user for each computer in the given collection.
Thycotic One Users	Sync users with Thycotic One	Run this task to synchronize PM users with a Thycotic One instance.
Security	Rebuild Item Security Cache	Run this task to mark all entries in the item security cache as invalid, forcing a rebuild.
	Refresh Agent Secrets	Run this task to refresh the agent secrets that were generated before the given max age.
	Revoke Agent Secrets	Run this task to revoke the secrets from one or more agents.
	Revoke Secrets from All Agents	Run this task to revoke the secrets from all agents.
	Set Security Rating	Run this task to manually set the security rating (used in filters) for the selected files.
	Update Security Ratings for Resource	Run this task to update the security ratings (used in filters) for the given resources using the given rating system.
Utility	Delete Item	This task will delete an item, and optionally dependent children.
	Reset Licensing	This task will reset licensing, deleting all installed license keys.
	Update Server Gauge State	This task will update the state of a server gauge.

Helpdesk Tasks

By default this folder is empty. Administrators can use it to copy tasks for HelpDesk users to run them. The HelpDesk folder provides security settings on those folders that would grant permissions if someone puts tasks in that area.

Infrastructure Scheduled Activities

These are tasks that pertain to either core functions or to components and subcomponents of Privilege Manager.

Core, no folder at root level	Client Items Update OBSOLETE WITH v 10.7 and higher	Updates client items required by agents.
	Collection and Resource Targeting Update	Updates collections and resource targets.
	Collection Update	Update collections.
	Import Local Group Policy Definitions	Loads Group Policy Definitions from the local machine.
	Import Secret Server Licenses	A scheduled import of licenses from Secret Server.
	Licensing Update	Updates licensing product counts.
	Resource Discovery	Run this task to populate data for resources that have been discovered but lack detailed information.
	Resource Target Update	Use this task to updates resource targeting.
Application Control		
App Control Cylance	Refresh Cylance Security Rating Report	Refreshes Cylance security rating reports on a schedule.
App Control VirusTotal	Recalculate Ratings for VirusTotal Provider	Recalculates security rating levels for resource rated by the given provider.
	Refresh VirusTotal Security Rating Reports	Refreshes VirusTotal security rating reports on a schedule.
Approval	ServiceNow Approval	Initiates a ServiceNow approval process and waits for the result.
Configuration	Reconfigure for System Secret Vault Change	This task is run by the system when the configured system secret vault setting has changed.
Data Feed	Content Tasks	Download Data Feed Entry - Download Data Feed Entity.
		Import Data Feed Entry - Imports data feed entities and their corresponding data feeds, primarily designed to be used by the Setup component.
		Import Product Configuration Package - Download Data Feed Entity.
	Update Tasks	Clear Data Feed Entity Updated - Clear Data Feed Entity.
		Update Data Feed - Updates the Privilege Manager Configuration Feed List
		Update TMS Configuration List Data Feed - Updates the Privilege Manager Configuration Feed List.
Directory Services	Active Directory Merge Computers	Merges computers created by Directory Services.
	Active Directory Merge Single Computer	Merges a single computer during agent registration. Needed if AD Sync has occurred before agent registration.
	Import Secret Server Domains	A scheduled import of AD domains from Secret Server.
	OU Directory Scope Collection Update	This task updates the membership of Directory Services OU scope collections.
	Promote Windows Domains	Promotes any Windows domains to Active Directory domains.
	Update Active Directory Details	Updates Active directory domain details including domain controllers.
File Inventory	Update File Filter Security Catalogs	Updates security catalogs associated with File Collection Security Catalog Filter items.
Import Activities	Import Packages	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Import Packages v3	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Install Products V4	This task installs product NuGet packages.
	Install Products V4 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
	Install Products V5	This task installs product NuGet packages.
	Install Products V5 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
Local Security	Primary User Update	Updates the primary user for each computer in the given collection.
	User Credentials Data Update	This task ensures that resource credentials match the source user data.
Maintenance Tasks	Assign Orphaned Agent Uploads	This task assigns agent event uploads that have been orphaned.
	Delete Old Performance Counter Events	This task deletes internal performance counter events last updated before the specified time.
	Purge Maintenance - Agent Logs	This server task removes all Agent Log data that is older than the time period specified.

	Purge Maintenance - Application Control Events	Purges the selected Application Control Event types from the database based on the time range specified.
	Purge Maintenance - Audit Events	This task removes audit event records older than the specified time period.
	Purge Maintenance - Completed File Upload Sessions	This task removes completed file upload sessions older than the specified time period.
	Purge Maintenance - Files Undiscovered	Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.
	Purge Maintenance - Incomplete File Upload Sessions	This task removes incomplete file upload sessions older than the specified time period.
	Purge Maintenance - Message History	This server task removes all Message History data that is older than the number of seconds/minutes/hours/days/weeks specified. Message History data tracks all events received by the Privilege Manager Server and is used for information purposes.
	Purge Old Computers	Remove old computers and gauge data for those old computers.
Monitoring	Check for Available Product Updates	Checks the configured <code>nuget:source:SolutionCentre</code> for available product updates.

Scheduled Tasks

In addition to maintenance tasks, there are other tasks that should be scheduled to run regularly by Privilege Manager administrators. It's recommended to run these tasks to determine how long they take to complete in each environment, then schedule appropriately to cover task completion and needs.

AD Import and Synchronization Tasks

Import Active Directory users and groups on demand and based on a set schedule.

Note: Depending on AD structure and size, the tasks should be planned to avoid bulk imports and synchronization of too large of a number of accounts.

Task Parameter Conflicts

When task parameters are set at the task level, they can't be changed when a schedule is created for that task. However, in some circumstances, if you have already defined parameters at the task schedule level and then go back to the task to set the values, you may end up with task schedule parameter conflicts. When there are conflicts with the version currently on the server, the Privilege Manager console shows a modal to resolve the existing conflicts before any schedule modifications can be saved.

Schedule Parameter Conflicts

The following schedules for this task have conflicting parameters.
Please review the conflicting parameters and choose if you would like to either

- Keep all conflicting parameters on the schedules
- Remove all conflicting parameters from the schedules

[New Task Schedule](#)

- groupNames
- azureId

The user can review the task that introduced the conflict by clicking the linked item, which is opened in a new browser tab.

The options to resolve are

- Keep all conflicting parameters on the schedule - click the **Keep** button.
- Remove all conflicting parameter from the schedule - click the **Remove** button.

Or cancel if you wish to clean up the conflicts by manually editing task parameters on the conflicting items. However, something indicated as a conflict isn't necessarily a problem. The functionality is implemented so that users have the ability to stop changes on the schedule level by setting something other than default on the task level. If a parameter on the task is a default value, then that parameter will not be in conflict, if it does not match on the schedule.

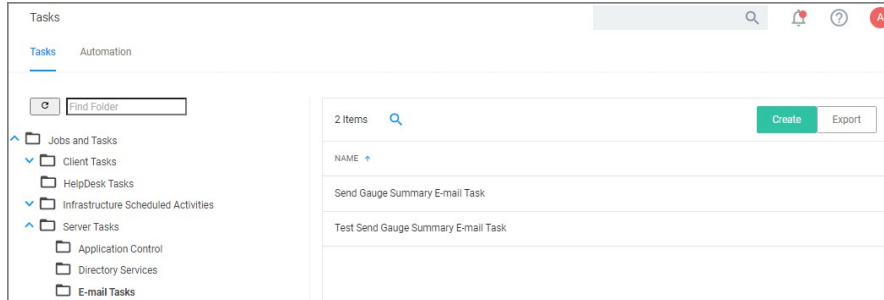
Whenever there is a deviation from the default value on the task level, even with the parameter on the schedule matching, users are asked to resolve the conflict by keeping the current values.

E-mail Reports Task

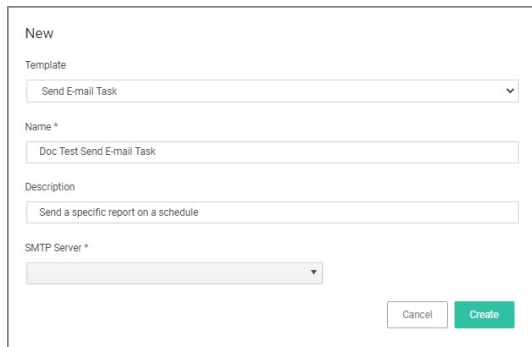
Any report created in Privilege Manager can be sent to a group of recipients based on a scheduled task.

To set this up, create a new Server task to send emails.

1. Navigate to **Admin | Tasks**.
2. In the folder tree open **Server Tasks | E-mail Tasks**.



3. Click **Create**. For on-prem instances the modal has an SMTP Server selection option, for cloud instances the server defaults to a pre-configured value and does not have the SMTP Server field.

The 'New' modal form contains the following fields: a 'Template' dropdown menu with 'Send E-mail Task' selected; a 'Name *' text input field containing 'Doc Test Send E-mail Task'; a 'Description' text input field containing 'Send a specific report on a schedule'; and an 'SMTP Server *' dropdown menu. At the bottom right of the form are 'Cancel' and 'Create' buttons.

4. From the Template drop-down select **Send E-mail Task**.
5. Enter the task name and description.
6. If this is for an on-premises instance, for **SMTP Server**, search for your SMTP server that is already configured as a foreign system for your instance.
7. Click **Create**.

Doc Test Send E-mail Task
Refresh More

Details
Task History
Change History

Details

This task can be scheduled to run periodically on the web server or be run immediately by using the Run Task option from the More menu.

Name:

Description:

Command:

Parameters

Parameters for this task.

Report To Run *

From Address *

To Address *

Schedules

Schedules for this task.

0 items

Note: For cloud environments the SMTP server settings are pulled from an existing configuration and can't be edited via the parameters tab.

Under **Details** and **Parameters** you can change/edit any of the task specific information:

1. From the **Command** drop-down, select what command you wish to execute, e.g. Email Report Results.
2. From the **Report to Run** drop-down, search for and select the report you wish to send.
3. In the **From Address** field enter the sender information you wish to be provided.
4. In the **To Address** field specify the recipient(s) (this can be a comma-separated list of addresses).
5. Click **Save Changes**.

Under the **Schedules** section of the page you can specify a schedule for this specific task.

1. Click **New Schedule**

Tasks
Cancel Save Changes

Save changes? If you press cancel, all your changes will be lost.

Schedule Details

Task to run: Doc Test Send E-mail Task

Schedule Name:

Schedule

Schedule Type:

Once
 Daily
 Weekly
 Monthly

Starting UTC

Recur every day(s)

[Show Advanced](#)

Parameters

Report To Run *

From Address *

To Address *

Set up the schedule specifics for this task.

2. Click **Save Changes**.

When a task is used to launch executables, but the task does not have an associated user context, the appropriate user token cannot be assigned. This applies to systems with 10.7 and above agents.

Example Scenario

A scheduled task launches an executable, which requires elevation, for example running the performance monitor process. That task is then set to run with elevated permissions, however not as a specific user, but rather as a local user group. Such task used in a policy will cause the executable to fail, since a specific user token cannot be associated.

Workaround

If you don't have a user context to assign to a task for launching an executable, you can use a PowerShell script in combination with the task and policy.

1. Create a PowerShell script to launch the executable.
2. Set the task to launch powershell.exe.
3. Pass in the name of the script.
4. Set the your policy to target that script.

Privilege Manager has many tasks that can be run to ensure that the data in the database is up-to-date and to purge old or unwanted information. This section provides an overview of the maintenance tasks and other schedulable tasks in Privilege Manager.

Determining how often to schedule maintenance tasks depends on the associated items, like events, files, computers, etc. and their build up. These tasks have default **parameters** assigned but are not scheduled to run. Privilege Manager administrators should schedule these tasks based on their needs and system performance.

The primary maintenance tasks that will need to be scheduled to ensure Privilege Manager databases do not grow too excessively are the

- Purge Maintenance - Application Control Events and
- Purge Maintenance - Files Undiscovered tasks and,
- in pre-10.5 systems, the
 - Purge Maintenance - Completed File Upload Sessions and
 - Purge Maintenance - Incomplete File Upload Sessions tasks.

Maintenance Tasks

These maintenance tasks can be found at

- **Admin | Configuration | General (tab)** or
- **Admin | Tasks | Jobs** and
- **Tasks | Infrastructure Scheduled Activities | Maintenance Tasks**

Assign Orphaned Agent Uploads

This task will assign agent event uploads that have been orphaned.

Parameters: Max records [default setting = 2500]

Delete Old Performance Counter Events

This task will delete internal performance counter events last updated before the specified time.

Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Day.

This maintenance task should be used if [Save Performance Counters](#) is enabled in the general section of the advanced configuration settings.

Initialize Item Change History

This task is run after installs to ensure items with change tracking enabled have initial history entries. This is an automated task to populate initial states of items across updates.

LSS Migration Tasks

For information on the LSS Migration tasks refer to [Migrate Local Security Policies](#).

Purge Agent and Gauge Data for Deleted Computers

This task will delete orphaned data from AgentActivity, AgentRegistration, and GaugeInstanceState.

Notes: This can be helpful to run, to remove unwanted data for computers that have been deleted from Privilege Manager.

Purge Duplicate Computers

Remove duplicate computers.

Notes: When AD sync occurs, Privilege Manager creates a new object in the database for each computer object. When the agent is installed, it references this same object. If the agent is installed before AD sync occurs, there can be 2 different objects in the database for the same machine. This task merges the duplicate objects and is usually only needed when agents are installed before a computer comes in from AD sync.

Purge Maintenance - Agent Logs

This server task will remove all Agent Log data that is older than the time period specified.

Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Week.

Purge Maintenance - Application Control Events

Purges the selected Application Control Event types from the database either

- manually based on a specified range of time, or
- automatically after reaching a set threshold. Refer to [Maximum Application Event Count](#) time range specified.

Parameters: Event Types to Purge (Application Action Events, Application Justification Events, Application Metering Events, Application Verifier Events). All of these Application Control Events are populated in the various Application Action reports.

Notes: Only Purge Events that belong to specific policies

Purge Application Control Events older than

Notes: Depending on policy settings, Application Control Events can pull a large amount of data into the database. Privilege Manager administrators must setup schedules for this task, as needed, to purge old or excessive data from Application Control policies.

Purge Maintenance - Audit Events

This task will remove audit event records older than the specified time period.

Parameters: Purge events older than [default setting = 30 day(s)]

Notes: The Audit events mainly pertain to and are used in Change History tracking. This task should not need to be scheduled.

Purge Maintenance - Completed File Upload Sessions

This task will remove completed file upload sessions older than the specified time period.

Parameters: Purge completed sessions older than [default setting = 1 day(s)]

Notes: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Files Undiscovered

Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.

Parameters: Delete Files that have been undiscoverable for longer than [default setting = 1 week(s)]

Notes: This task clears up files with the name "New Loaded Resource" that are older than X days. This can be a helpful task to schedule to remove undiscoverable files from the Event Discovery results (for example, temp files that an installer creates and then deletes).

Purge Maintenance - Incomplete File Upload Sessions

This task will remove incomplete file upload sessions older than the specified time period.

Parameters: Purge incomplete sessions older than [default setting = 2 day(s)]

Notes: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Message History

This server task will remove all Message History data that is older than the time period specified. Message History data tracks all events received by the Privilege Manager Server and is used for informational purposes.

Parameters: Delete Message History older than [default setting = 30 day(s)]

Notes: This task clears the [Ams.Resource].[MessageHistory] table. Use this task to purge that table, if it is excessively large.

Purge Maintenance - Orphaned Local Users and Groups

This task will delete local users and groups that reference a computer as their parent domain (which will block deletes), but are not part of that computers users and groups.

Purge Old Computers

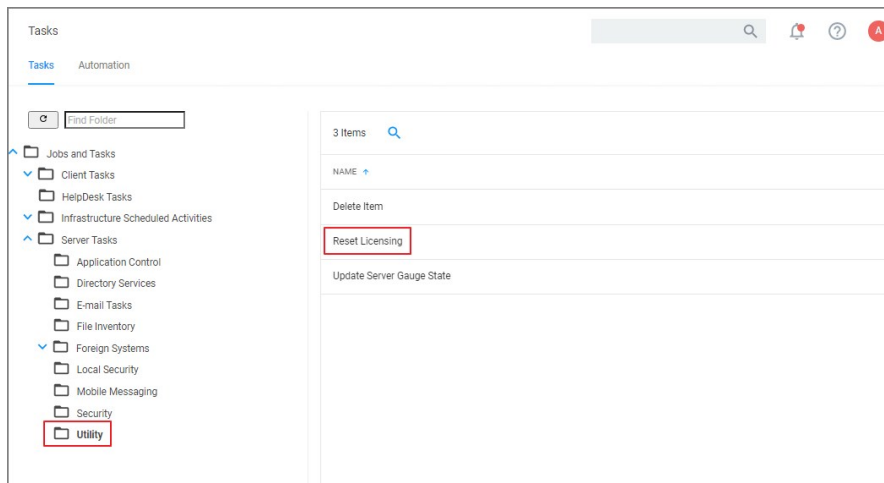
Remove old computers and gauge data for old computers. Remove any agents that have not communicated with the server in a set number of days (default 90), resulting in a critical Agent state.

With Privilege Manager 10.7 and up license registrations can be reset. The Reset Licensing task allows upgrading users to remove outdated licenses.

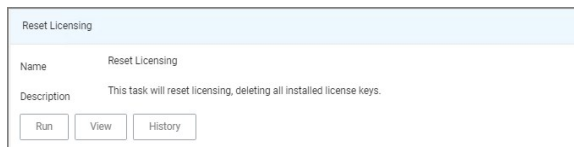
After acknowledging the license reset, all licenses are removed from the Privilege Manager instance. When no licenses can be found, the no product licenses warning banner displays on the top of the console.

Using the Reset Licensing Task

1. Navigate to the **Admin | Tasks**.
2. From the Tasks folder tree, select **Server Tasks | Utility**.
3. From the options on the right, select **Reset Licensing**.

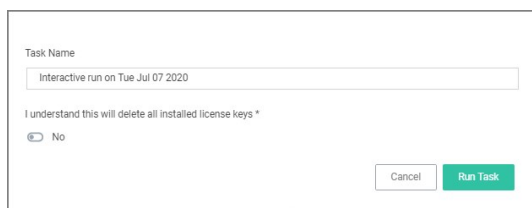


Reset Licensing is a read-only task.



4. Click **Run**.

To run the task, the user needs to acknowledge the removal of all installed license key.



The task does not run without that acknowledgement and an error is generated.

Note: Do not use the scheduling functionality on this task. After a license reset, new licenses should be applied ASAP.

To re-apply licenses refer to the information under [Licensing](#) in the Getting Started section.

Administrator users can create and edit Privilege Manager users and assign and remove roles for these users.

There are three types of users:

- Thycotic One users - these are only available in cloud environments and are manually added.
- API Users - these are available for the public API implementation.
- Standard Users - these are users manually added by an administrator after the initial installation of Privilege Manager.

How to Manually Add Thycotic One Users

To manually add users to your Privilege Manager cloud instance, follow these steps:

1. Navigate to **Admin | Users**.

The screenshot shows the 'Users' management page. At the top, there is a search bar and navigation icons. Below the header, there is a paragraph explaining that users created here will be assigned to Privilege Manager roles and will be sent to Thycotic One for login. A note states that brand new Thycotic One users will receive a verification email that expires in 30 minutes. Below this is a table with 44 items, a search icon, and a 'Create' button. The table has columns for NAME, DESCRIPTION, LAST MODIFIED BY, LAST MODIFIED, and TYPE. Two rows are visible: one for 'admin' (Standard User) and one for 'jdoe@mycloudinstance.com' (Thycotic One user).

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED	TYPE
admin		admin@mycloudinstance.com	5/27/20, 2:06 PM	Standard User
jdoe@mycloudinstance.com		Principal Self Well Known Group	6/1/20, 4:45 PM	Thycotic One

2. Click **Create**.

The dialog box is titled 'Select a User Type'. It contains a 'User Type' dropdown menu with 'Thycotic One' selected. There are 'Cancel' and 'Create' buttons at the bottom.

3. From the **User Type** drop-down, select **Thycotic One** and click **Create**.

The form is titled 'New'. It has a 'Thycotic One Instance' dropdown menu. Below it are three required fields: 'Email', 'Name', and 'New Thycotic One User'. There are 'Cancel' and 'Create' buttons at the bottom.

4. From the **Thycotic One Instance** drop-down, search for and select your instance for the new user.
5. Enter the **Email** and **Name** of the new Thycotic One user in the respective fields.
6. Click **Create**.

How to Manually Add Standard Users

Standard users can view and edit their own accounts, such as password updates, but can't create new users or delete their own user.

1. Navigate to **Admin | User**.

Users

You may create users to synchronize with Thycotic One here. This will allow them to be assigned to Privilege Manager roles. When the user goes to log in, they will be sent to Thycotic One and asked to provide a username and password. If they have not created a password, they will need to create a new account at that time. For more information on Thycotic One user creation, see our [documentation page on user creation](#).

Brand new Thycotic One users will receive a verification email that expires in 30 minutes.

44 Items

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED	TYPE
admin		admin@mycloudinstance.com	5/27/20, 2:06 PM	Standard User
jdoe@mycloudinstance.com		Principal Self Well Known Group	6/1/20, 4:45 PM	Thycotic One

On-prem instances see a note that Thycotic One users can only be created if a Thycotic One Foreign System is configured.

2. Click **Create**.

3. From the **User Type** drop-down, select **Standard User** and click **Create**.

Select a User Type

User Type

Thycotic One

API Client

Standard User

Thycotic One

4. On the **Enter User Details** modal, enter

Enter User Details

User Name

Display Name

1. the **User Name**.
2. the **Display Name**.

5. Click **Create**.

6. On the newly created User's details page, add

Save changes? If you press cancel, all your changes will be lost.

User Details

Add roles to a user [here](#).

This user does not have a password set.

User Name

Display Name

Email Address

Password

Include Number, Symbol, Upper case in password field for valid password

Confirm Password

Field is required, Passwords don't match

Locked Out

- o the user's **email address**
- o a **password**
- o **roles** to the user by clicking the **Add roles to a user here** link. You can create users without assigning roles. To go through the steps of assigning roles, refer to the **Add Roles to a User** topic below.

7. Click **Save Changes**.

The user is now active in the system and you may edit the user details.

Details | Related Items | Change History | Active | Refresh | More ▾

User Details

Add roles to a user [here](#).

User Name: John Doe

Display Name: jdoe

Email Address: jdoe@mycompany.com

Password:

Confirm Password:

Locked Out:

How to Manually Add API Client Users

API Client users can view and edit their own accounts, such as password updates, but can't create new users or delete their own user.

1. Navigate to **Admin | User**.
2. Click **Create**.
3. From the **User Type** drop-down select **API Client** and click **Create**.

< Back to Users | API User Created On Jun 10, 2020 | Search | Notifications | Help | 1

Details | Related Items | Change History | Active | Refresh | More ▾

User Details

Add roles to a user [here](#).

Generating a new API secret will replace and revoke the previous one.

[Reset Secret](#)

Display Name: API User Created On Jun 10, 2020

Client ID: 19e4ccca-0285-49ae-84eb-ab33f48fca1c

Secret: JTD0eJIRuC6Cc7N5zECJMVDwDQZRUrcV

Expires: Never

Locked Out:

Please copy this secret before navigating away from this page. You will not be able to see it after leaving this page.

API Client users are by default created with a date and time reference when the user was added. If you wish, you can modify the display name. The newly create user is automatically set to active on creation. Prior to navigating away from the page, make sure to take note of the **Client ID** and copy the **Secret** into your vault.

Make sure the API user is a member of a role, the role depends on what you need the API to do.

Use **Reset Secret** to generate a new secret for this user, it invalidates the old secret you copied to the vault. Once you click **Reset Secret** you need to confirm the action. The new secret will be shown until you navigate away from the page. All changes need to be saved to take effect.

Add Roles to a User

1. On the **User Details** page, from the **Add roles to user here** click [here](#).

< Back to jdoe

Roles

10 Items New

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED
PM - Test Admin		1c20f4c76-5557-4a4b-9413-3d112bc20c30 (Unnam...	8/22/19, 10:19 AM
Privilege Manager Administrators	Privilege Manager Administrators	Trusted Installer	4/30/20, 1:07 PM
Privilege Manager Field Engineering		Trusted Installer	4/30/20, 1:07 PM
Privilege Manager Helpdesk Users	Privilege Manager Helpdesk Users	Trusted Installer	4/30/20, 1:07 PM
Privilege Manager MacOS Administrators	Privilege Manager MacOS Administrator	Trusted Installer	4/30/20, 1:07 PM
Privilege Manager MacOS Administrators	Privilege Manager MacOS Administrator	Trusted Installer	1/2/20, 6:02 AM
Privilege Manager Users	Privilege Manager Users	Trusted Installer	4/30/20, 1:07 PM
Privilege Manager Windows Administrators	Privilege Manager Windows Administrators	Trusted Installer	4/30/20, 1:07 PM
Privilege Manager Windows Administrators	Privilege Manager Windows Administrators	Trusted Installer	1/2/20, 6:02 AM
Test Privilege Manager New Users		W1M2S08PMTJ0TTF Administrator	11/8/19, 2:26 PM

2. From the roles page select the role you want to add to the user, for example *Privilege Manager Windows Administrators*.

< Back to Roles

Privilege Manager Windows Administrators

Membership Change History Refresh More

Membership Windows Administrators Administrators Role Members Edit

1. Click **Edit**.

1

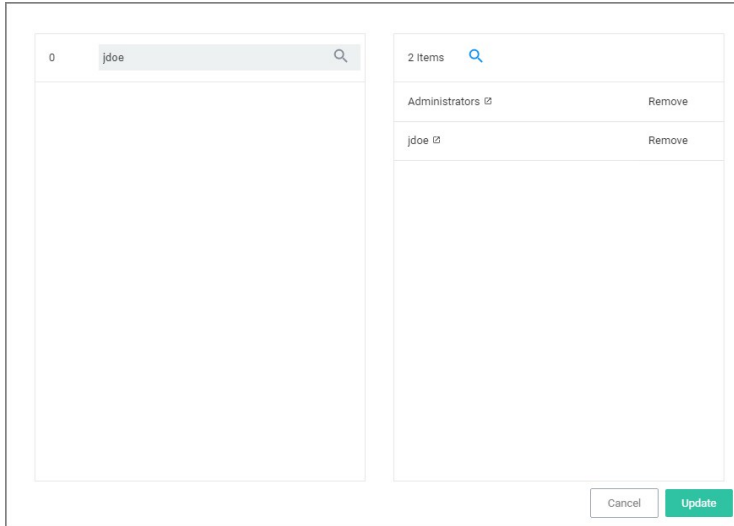
jdoe Remove Add

1 Items

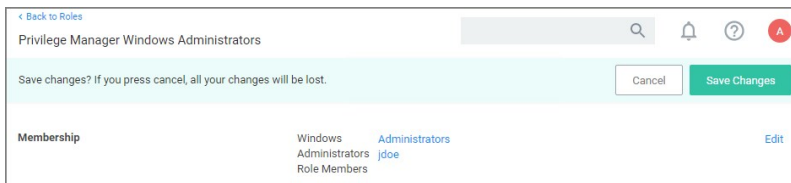
Administrators Remove

Cancel Update

1. Click the **name** or **Add** to add the user to the role.



2. Click **Update**.



3. Click **Save Changes** to save the role update.

Privilege Manager Administrators can turn complex password policy rules on and off for Privilege Manager users. This can be set via the [advanced configuration](#) page. Password complexity is turned on by default.

Policy rules:

- minimum of 8 characters
- minimum 1 symbol
- minimum 1 uppercase
- minimum 1 lowercase

The screenshot shows a web browser window with the title 'WWonka'. At the top, a light green banner contains the text 'Save changes? If you press cancel, all your changes will be lost.' and two buttons: 'Cancel' and 'Save Changes'. Below this is the 'User Details' section. On the left, there is a link 'Add roles to a user here.' and a message 'This user does not have a password set.'. On the right, there are input fields for 'User Name' (containing 'Willy Wonka'), 'Display Name' (containing 'WWonka'), and 'Email Address'. Below these is a 'Password' field containing two asterisks. A red text note below the password field reads 'Include Number, Symbol, Upper case in password field for valid password'. At the bottom of the password section are 'Cancel' and 'Save Password' buttons. At the very bottom of the form is a 'Locked Out' toggle switch.

The password policy applies to UI and API Client users.

The enforcement takes effect when a new Privilege Manager user is created or an existing user resource is edited.

The Tools menu in Privilege Managers offers access to

- [Disclose Password](#)
- [File Upload](#)
- [Manage Approvals](#)
- [Offline Approvals](#)
- Secret Server, if integrated.

The Password Disclosure tool lets users based on role permissions disclose passwords and look a password rotation history.

The password rotation history is helpful when systems are being restored to a time prior to the current password.

Using the Disclose Password Tool

1. Navigate to **Admin | Tools: Disclose Password**.
2. The Computer page opens.

Select Computer

Computer name

Computer domain

OS name *

Select a computer from the list.

Select Computer

Computer Name	Computer Domain	OS Name	IP Address	Count
my-computer	WORKGROUP	Microsoft Windows Server 2016 Standard	-1	2

10 items per page 1 - 1 of 1 items

3. The Password Disclosure page opens, it list the managed users and also provides links to view the current password and to password history.

Disclose Password

Computer [my-computer](#)

Managed Users

2 Items

USER NAME	COMPUTER	DOMAIN	LAST CHANGED	
my-computer\Test Disclosure	my-computer	WORKGROUP	7/7/20, 8:41 AM	View Historical Password Show
my-computer\Wilson	my-computer	WORKGROUP	6/25/20, 12:06 PM	View Historical Password Show

4. Click on **Show** to view the current password.

Password

Password at June 25, 2020 at 12:06:08 PM GMT-4

Phonetic

! CHARLIE alpha sierra tango alpha whiskey
alpha yankee TWO ZERO TWO ZERO

5. Click on **View Historical Password** to view the password history.

Historical Passwords	
CHANGED ▾	
6/25/20, 12:06 PM	View Password
6/12/20, 7:49 AM	View Password
4/29/20, 3:58 PM	View Password

[Close](#)

Select a link on the **Historical Password** modal to view any of the rotated passwords.

Password

Password at June 25, 2020 at 12:06:08 PM GMT-4

!Castaway2020

Phonetic

**! CHARLIE alpha sierra tango alpha whiskey
alpha yankee TWO ZERO TWO ZERO**

[Close](#)

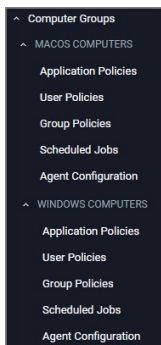
Note: Any password disclosure is audited and can be viewed in the **Password Disclosure History** report (requires Administrator role membership).

Computer Groups

Privilege Manager's user interface provides a logical categorization via Computer Groups. The basic categorization is by operating system. Based on size of organization different business units can be targeted by separate Computer Groups established in Privilege Manager.

Each Computer Group has the following areas to specifically address

- Application Policies, which are used for [Application Control](#) policies that can be created by using the Policy Wizard.
- [User Policies](#), which are used as part of [local security](#) and pertain to specific users.
- [Group Policies](#), which are also part of [local security](#), but pertain to a group of users.
- Scheduled Jobs, these are also known as client tasks. Many are by default active.
- Agent Configuration, these are agent configuration policies allowing a global configuration of agent behavior.



If you have agents already installed and registered, you will see Computer Group numbers listed, divided by Privilege Manager's two out-of-the-box computer groups:

- Windows Computers and
- MacOS Computers

NAME	COMPUTERS	USERS	USER GROUPS	SHOW IN SIDE MENU
MacOS Computers	0	0	0	
Windows Computers	2	30	35	

For example, in the screenshot above only 2 agent are registered with Privilege Manager. Local Security tells us that the agents are installed on a Windows computer (thus categorized in the Windows Computers group), that there are 30 local Users and 35 User Groups on the two machines. Local Security automatically discovers this information upon every agent's registration with Privilege Manager.

If you have Computer Groups (also called Resource Targets) already configured for Application Control in Privilege Manager, keep in mind that those groups also appear as Group Policies for a given Computer Group in the left navigation tree.

Local Security in Privilege Manager allows customers to

- discover all local accounts and groups that exist on endpoints.
- provide membership control of those accounts on endpoints.
- allows to take complete ownership of the local credentials by enforcing password rotation for all accounts on those endpoints.
- use best practices when it comes to locking down the network from malicious endpoint attacks that exploit unsecured administrative access.

Local Security is made up of

- Computer Groups
- Local Groups
- Local Users

Under Reports various Local Security reports and summaries are available.

Computer Groups

These so called resource targets (as configured in Application Control) are specified sets of computers that meet certain criteria, that are targeted by certain policies and scheduled tasks.

Each computer group contains all local groups and local users on endpoints with a local security agent installed. When the agent registers, Local Security automatically discovers the local groups that exist on each machine.

Local Groups

Each local group has a list of local users that exist in that specific local group. From that list you can see

- how many groups each user account is a member of.
- whether the user account is built-in or user-defined.
- whether or not the account itself is managed.

Local Users

Setting up a local user account with password rotation means that the account is a managed account within Privilege Manager.

To add new computer groups tailored to your organization's environment.

1. Click **Create Computer Group**.
2. From the **Platform** drop-down, select either macOS or Windows.
3. Enter a Name and Description for your new group.

10.8 UI Computer Group Scoped to Windows Computers

Details Results Related Policies

Refresh More

Details

Name: 10.8 UI Computer Group Scoped to Windows Computers

Description:

Platform: Windows

Filter Rules

All filtering rules start with "All Computers". Each consecutive rule removes resources from that list in order.

Add Rule

1 Items

ORDER	OPERATION	LIST TYPE	SELECTED ITEMS
0	Only Keep Computers in	Collection	All Windows Computers

4. To select the machines you want to include within this group, you must add Filter Rules that will target the appropriate machines on your organization's network. The default filter rule begins with a rule that targets computers within the main OS Computer Group that was selected when you created the group, meaning it will target either all Windows or all Mac computers with registered agents.

To narrow your group, click **Add Rule**.

Filter Rules

All filtering rules start with "All Computers". Each consecutive rule removes resources from that list in order.

Add Rule

1 Items

ORDER	OPERATION	LIST TYPE	SELECTED ITEMS
0	Only Keep Computers in	Collection	All Windows Computers

Multiple rules can be added per computer group. To change already established Computer Groups use add rules or change the resources already targeted.

1. Specify the **Operation** behavior, which can be:
 - Only Keep Computers in (default)
 - Include Computers in
 - Remove Computers in
2. In the **List Type** column select from the following options:
 - Computer List: Under **Selected Items**, use **Add** if nothing is selected yet. Search for and select specific computers from the provided list of registered machines.
 - Collection: Under **Selected Items**, enter a collection name, e.g. collections can be "All Windows Computers" or "All Managed Computers". You may also choose from the options in the drop-down
 - OU (Organizational Unit): Under **Selected Items**, click **Select** and pick the OU from the populated domain tree.



- Security Group: Under **Selected Items**, search for and select a security group filter.

5. Click **Save Changes**.

Every Computer Group is divided into Groups and Users. Both **Groups** and **Users** in this context refer to local accounts on the machines that are included in the Computer Group.

The Computer Group page lists all local groups on this set of computers, and provide a high-level overview of the selected computer group based on Local Users, Local Groups, and the number of computers in the group.

Remember: when an agent registers, Local Security will automatically discover the local groups that exist on each machine.

Create New Local Group

To create a new Group,

1. Under your Computer Group, select Group Policies.
2. Click **Create Group**.
3. Enter a Name for your new group.
4. Click **Create**.

10.8 Editing Group

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Group Details

Manage this group by selecting edit. Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static and will no longer be able to be updated directly on the endpoint.

Manage Group Yes

Group Name 10.8 Editing Group

Description

No Members Add Member

The Manage Group switch is by default set to Yes.

5. Click **Add Member**.
6. From the **Type** drop-down, select either
 - o Domain User
 - o Domain Group
 - o Local User
7. On the **Add Member** dialog, select from the available resource items by setting the switch.

Add Members

Select which member(s) to add to this group. Once in the members grid, choose what action is taken on the account by selecting from the options in the "Operation" column.

Type

User Account

12 Items

USER NAME +	BUILT-IN	MANAGED
<input type="checkbox"/> TestAdmin	User Defined	Not Managed
<input type="checkbox"/> treebeard	User Defined	Not Managed
<input checked="" type="checkbox"/> Wilson	User Defined	Managed

Cancel Add Member

8. Click **Add Member**.

Manage Local Groups

Managing a local group means that you determine which user accounts are in the group. In other words, if a group is being managed, the group membership will remain static and will no longer be able to be updated directly on the endpoint. Before adding users to any group, make sure you really want all those users in that particular group. Any exact group membership setting is rolled out to ALL endpoints in that computer group.

If a local group is not managed the Manage Group checkbox is not selected. To Manage the group, click Edit from the Details tab and then check the Manage Group box. Click Save Changes, and Yes to Confirm Navigation. Changes to these settings may take up to 15 minutes to update on your endpoints.

When managing a group, existing members and any that have been added to the policy will appear in the Members table. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. From the drop-down choose which operation to perform if an account (user) is found on the endpoint. The following options can be selected:

- Ignore if found
- Add if missing
- Remove if found

Using **Remove if found** for **All Other Users and Groups** instates exact group membership and **Ignore if found** cannot be used on individual accounts that are part of that group. Note that, if **exact group membership** is used, an account that is initially listed as **Ignore if found** switches to **Remove if found** as part of the group membership. Individually specified accounts can be set to **Add if missing** in those groups.

Note: Once saved, group membership is permanently defined. Updates made directly on the endpoint that break this policy will be immediately reverted.

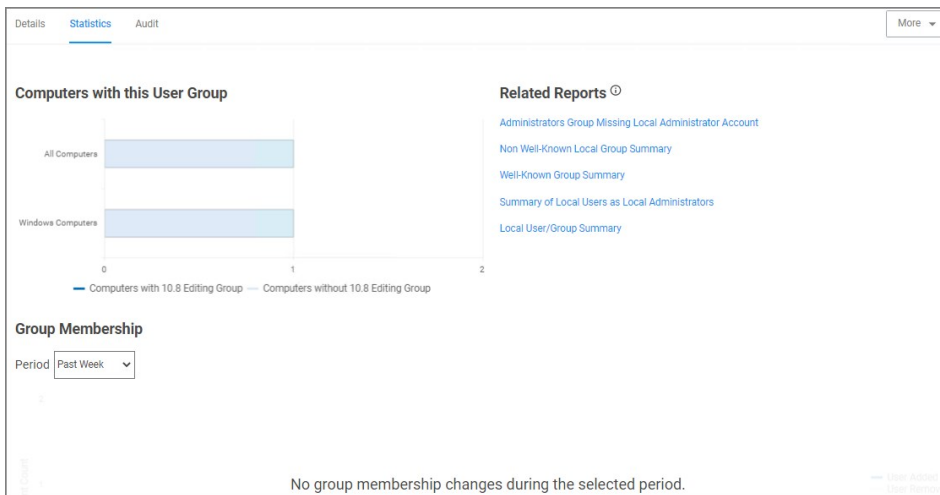
MEMBER	TYPE	COUNT	OPERATION
Wilson	Managed User	0	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px; margin-right: 5px;"> Add if missing Ignore if found Add if missing Remove if found </div> <div style="border: 1px solid #ccc; padding: 2px; margin-left: 5px;"> Remove </div> </div>
All Other Users and Groups			<div style="border: 1px solid #ccc; padding: 2px; width: 100px; text-align: center;"> Remove </div>

The last row defines what action to take **on all other users and groups**. This ensures exact membership can be defined and any other users or groups can be automatically removed.

Statistics

The **Statistics tab** for a local group highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network are included in this group and whether there have been changes made to the Group's Membership within the specified period. Click on these graphs to drill down into more details.

Note: The reports in the "Related Reports" sections are scoped to only include endpoints in the current computer group. To view reports across all computers, go to the Reports section of the product.



Audit

The **Audit tab** is where you will find an audit record of all membership additions and deletions that have been made to your local groups.

The Users page listed under your Computer Group shows a list of local users that exist within this Computer Group. The information highlighted by this table includes

1. how many groups each user account is a member of,
2. whether the user account was built-in or user-defined, and
3. whether or not the account itself is managed.

Managing local users in Local Security means that you are setting a password for the account and can rotate the password as desired.

USER NAME	GROUP COUNT	BUILT-IN	MANAGED
Administrator	1	Built-In	Not Managed
ciscoacvpnuser	0	User Defined	Not Managed
DefaultAccount	1	Built-In	Not Managed
gollum	2	User Defined	Not Managed
Guest	1	Built-In	Not Managed
LSSAdmin	1	User Defined	Not Managed
radagast	2	User Defined	Not Managed
Tauriel Mirkwood	0	User Defined	Managed
Test Disclosure	0	User Defined	Managed
Test Password Disclosure	0	User Defined	Managed
TestAdmin	3	User Defined	Not Managed
treebeard	2	User Defined	Not Managed
Wilson	1	User Defined	Managed

Create New Local User

To create a new local user,

1. Navigate to your Computer Group for this new user and select User Policies.
2. On the User Policies page, click **Create User**.
3. Enter the new User Name.
4. Click **Create**.
5. This takes you to the Account Details tab of your new user's account. To create a user through Local Security, it must be a managed user.

Tauriel Mirkwood

[Account Details](#) | [Account Password](#) | [Groups](#) | [Statistics](#)

User Details

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manager.

User Managed Not Configured

User Name Tauriel Mirkwood

Full Name Tauriel Mirkwood

Description

6. Set the **User Managed** switch to **Yes**.

In Local Security, the most important thing to know about your user accounts is whether or not each is being managed. Managing a local user account means that you are able to rotate the account's password from Local Security's console in Privilege Manager.

Tauriel Mirkwood

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

User Details

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manager.

User Managed Yes

User Name Tauriel Mirkwood

Full Name

Description

Account is Disabled No

Initial Password No password is set [View Password](#)
[Edit](#)

User Must Change Password At Next Logon Off

User Cannot Change Password Off

Password Never Expires Off

Note: The following settings are all specific to Windows endpoints and will not be displayed for macOS based Computer Groups:

- Account is Disabled
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires

7. Set the rules pertaining to the user's password. Managed user accounts require an initial password when created.

8. Click **Save Changes**.

While editing a user you can change the account User Name, add details like the full name of the user, you may disable the account or update the schedule that pushes out modifications to endpoints.

The most important part of managing a user is setting a one-time password for the account. This means that any user of the account is no longer able to access the account with the former password, effectively locking a user out of the account unless they contact the Privilege Manager Local Security Helpdesk.

The **Groups tab** for a Local Account tells you how many groups and computers the account is on. Clicking on a Group Name from this page directs you back to the details of that local group.

The **Statistics tab** for a local user account highlights some quick visual statistics and links to relevant reports based on key factors, like how many computers from your network have this user account and whether there have been changes made to the user's membership within the specified period. Click on the graphs to drill down into more details.

Password Management: Randomize Local Account Passwords

Local Security allows administrators to manage users and also to manage passwords and password rotation. Managing users, passwords, and rotation scheduled often go hand-in-hand, but not every managed user account also requires password rotation. For example, service accounts are managed, but usually do not have password rotation setup.

Password rotation can also be setup for existing users without having to provision user accounts.

Note: Password rotation is an option that is not required for all accounts, especially not for service accounts.

1. On the **Account Password** tab, set the **Password Managed** switch to **Yes**.

2. Edit password length and strength rules. The password on this account will be rotated based on the Update Schedule details, click on the schedule link.

Tauriel Mirkwood

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Password Management

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

[View Password History](#)

Password Managed Yes

Characters Uppercase
 Numbers
 Lowercase
 Symbols

Password Length Characters

Log Password Before Change Yes

Schedule Every 30 days at 12:34:00 PM (UTC) starting Tue Jul 21 2020

The password for the account on each endpoint in the Computer Group will be unique.

3. Click **Save Changes**.

If the password is being managed, the update schedule determines when the new password is applied.

Note: The Account Details of the user do NOT need to be managed in order to manage the password on a local account.

Reports Relating to Managed Accounts

- **All Computers with Managed Passwords:** Lists all computers that have at least one local user with a managed password.
- **Password Disclosure History:** Lists all local and provisioned user's passwords that have been disclosed in a given time frame.
- **Disclosure Summary (Local User):** Lists all local users whose managed password has been disclosed in the given time frame.

To inventory shared folders on computers that have the local security agent installed, enable the shared folder inventory policy. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

Enable the Policy

1. Under your **Computer Group**, navigate to **Shared Folder Inventory Policy**.

Shared Folder Inventory Policy

Details Change History Inactive Refresh More

Scheduled Job Details

Name: Shared Folder Inventory Policy

Description: The purpose of this policy is to inventory shared folders on the client.

Computer Groups Targeted: 1 (1 total endpoints) Windows Computers Add

Deployment: Not deployed (Policy is inactive)

Job Settings

Command: Local Security Shared Folder Inventory Command

No parameters

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run.

Default: Weekly on Sun at 2:00:00 AM starting Tue Jan 01 2013 Add Trigger

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions: Start the task only if the computer is idle

Power Conditions: Start the task only if the computer is on AC power; Stop if the computer switches to battery power

Advanced Conditions: Allow task to be run on demand; Run task as soon as possible after a scheduled start is missed; If the task fails, attempt to restart; Stop the task if it runs for longer than

If the task is already running, then the following rule applies: Do not start a new instance

2. Set the **Inactive** switch to **Active**.

To disable the guest account on computers that have the Local Security Agent installed, enable the **Disable Local Guest Accounts** remote scheduled client command. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

To enable the policy:

1. Under your **Computer Group**, navigate to **Disable Local Guest Accounts**.

The screenshot displays the configuration interface for the 'Disable Local Guest Accounts' policy. It is currently in an 'Inactive' state. The 'Scheduled Job Details' section includes the job name, a description, the target computer groups (Windows Computers), and the deployment status. The 'Job Settings' section shows the command 'Local Security Provision Command', the provisioned users 'Disabled Guest Account', and an option to add provisioned groups. The 'Job Schedule' section is set to a default daily trigger at 8:00:00 AM. The 'Job Conditions' section allows for configuring when the task should run based on idle status, power source (AC or battery), and advanced options like running on demand.

2. Set the **Inactive** switch to **Active**.

If you wish to customize any aspects of the default behavior, create a copy and edit the copied policy.

The Disable Local Guest Accounts policy uses the Local Security task Disable Guest Accounts. If you wish to run the task on demand follow these steps:

1. Navigate to **Admin | Tasks**.
2. On the Tasks tab open the folder tree to **Client Tasks | Local Security**.
3. Select the **Disable Guest Account** task.

The screenshot shows the 'Tasks' management interface. On the left, a folder tree is expanded to 'Local Security'. The main pane displays a list of tasks, with 'Disable Guest Account' selected. The task details pane shows the name 'Disable Guest Account' and provides buttons to 'Run', 'View', or 'History' the task.

4. Click **Run**.

The Thycotic Local Security Agent collects logon and logoff events from Windows on a schedule configured via the User Logon Inventory policy. The Agent collects logon and logoff events and reports them as inventory data. The **Update Primary User for Collection** task calculates the primary user and the primary user and associated inventory data can then be viewed in the Resource Explorer.

The **User Logon Inventory Policy** is by default active.

The screenshot shows the configuration page for the 'User Logon Inventory Policy'. It is currently active, as indicated by a green toggle switch. The page is divided into several sections:

- Scheduled Job Details:**
 - Name:** User Logon Inventory Policy
 - Description:** Updates user logon data on the given schedule.
 - Computer Groups Targeted:** 1 (1 total endpoints) Windows Computers
 - Deployment:** 100% (1 endpoints, 1 with the latest version)
- Job Settings:**
 - Command:** Windows Logon Event Processor
 - No parameters:** No parameters
- Job Schedule:**
 - Default:** Weekly on Sun at 2:00:00 AM starting Tue Jan 01 2013
- Job Conditions:**
 - Idle Conditions:** Start the task only if the computer is idle (disabled)
 - Power Conditions:** Start the task only if the computer is on AC power (disabled); Stop if the computer switches to battery power (disabled)
 - Advanced Conditions:**
 - Allow task to be run on demand (checked)
 - Run task as soon as possible after a scheduled start is missed (checked)
 - If the task fails, attempt to restart (disabled)
 - Stop the task if it runs for longer than (disabled)

If you wish to customize the schedule or any other policy specification, create a copy of the default policy (More > Duplicate) and edit the settings.

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **Admin I Tasks**.
2. In the folder tree open **Server Tasks | Local Security** and search for **Update Primary User for Collection**.
3. Click **View**.
4. Customize the settings and schedule by editing the task.

The screenshot shows the configuration page for the 'Update Primary User for Collection' task. It is currently inactive, as indicated by a grey toggle switch. The page is divided into several sections:

- Details:**
 - Name:** Update Primary User for Collection
 - Description:** Updates the primary user for each computer in the given collection.
- Parameters:**
 - Collection:** [Dropdown menu]
 - Days to evaluate *:** 90
 - Include local logons *:** Yes (checked)
 - Include remote desktop logons *:** No (disabled)
- Schedules:**
 - Schedules for this task:** 0 Items

5. Click **Save Changes**.

You can run the **Update Primary User for Collection** task at any time to immediately recalculate the primary user for all computers in the selected collection.

Viewing the Resource

The Windows Logon Session events can be viewed by opening the **Local User/Group Summary** report and selecting a computer resource from the list. Then select Events | Local Security | Windows Logon Sessions.

WINDOWS10PRO

Revoke Agent Trust Delete

View Windows Logon Sessions Data Class Report CSV PDF

User	Logon Time	Logoff Time	Minutes	Type	Remote Addr...	Logon ID	Logon Event ID	Logoff Event ID	User SID
MYDC\Administ...	6/4/2020 4:30 PM			Incomplete Remote Interactive	192.168.1.29:0	a84b59f8-a18a-7f6d-3834-097729db55af	62948		S-1-5-21-3398682143-3951403953-3019020845-500

The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.

Note: Thycotic recommends to use a Professional Services engagement when migrating local security to Privilege Manager 10.7 or newer.

Before any migration is performed, make sure to backup your Privilege Manager database.

Migration Steps

Starting with Privilege Manager 10.7 the LLS Migration Readiness Report is available. The report is generated after an upgrade to 10.7 or higher from any previous Privilege Manager version.

To access the LLS Migration Readiness Report, follow these steps:

1. From anywhere in the Privilege Manager console search for LSS Migration.

NAME	TYPE	MODIFIED	DESCRIPTION
LSS Migration Readiness Drilldown DataSource	DataSource Item	7/10/20, 7:49 AM	
LSS Migration Readiness Report	Report	7/10/20, 7:49 AM	Displays all the policies that will be affected by the LSS Migr...
LSS Migration Readiness Report - Drilldown	Report	7/10/20, 7:49 AM	Displays all the changes that will occur relating to this policy ...
LSS Migration Script (1/2): Migrate all items.	Powershell Script	7/10/20, 7:49 AM	Powershell Script
LSS Migration Script (2/2): Enable the migrated items.	Powershell Script	7/10/20, 7:49 AM	Powershell Script
LSS Migration Task (1/2): Migrate all items.	Powershell Task	7/10/20, 7:49 AM	
LSS Migration Task (2/2): Enable migrated items.	Powershell Task	7/10/20, 7:49 AM	

The search does show all LSS Migration labeled results found in Privilege Manager. As the image shows, there are two related reports and tasks.

2. Select **LSS Migration Readiness Report**.
3. The report shows a table containing Policy IDs, their Name, and the current migration status.

PolicyId	Policy Name	State
3fd4f1c5-446d-4f3c-ab36-fc1fa44e94a7	Cleanup sent Privilege Manager Events (Mac OS)	Skipped: Is not using a Local Security Command.
5018b338-3415-4868-bfbb-062d10543c88	DocTest - Restrict Account Permissions on Agent Services (Windows)	Skipped: Policy should have at least one target.
693b1bdb-f683-40af-b3c6-036573f75511	User Account Policy for 'Test Disclosure' in 'Windows Computers' - v. 1	Skipped: Task has already been migrated.
5c603f9b-4201-4905-bba8-18d750ec0ca8	Password Management Policy for user 'Test Password Disclosure' on computers in 'Windows Computers'	Skipped: Task has already been migrated.
d68f8120-8a6e-4a08-bb2b-7840ded212c5	Password Management Policy for user 'Tauriel Mirkwood' on computers in 'Windows Computers'	Skipped: Task has already been migrated.
8bdd1879-0a5b-4fca-815e-7e9a4900949a	Group Membership for '10.8 Editing Group' in 'Windows Computers' - v. 1	Skipped: Task has already been migrated.
e8f8ae67-3031-49f1-9b5e-84969dab1e55	Password Management Policy for user 'Test Disclosure' on computers in 'Windows Computers'	Skipped: Task has already been migrated.
aae5e485-6c7f-49ec-91c9-8efc63f2954d	User Account Policy for 'Wilson' in 'Windows Computers' - v. 1	Skipped: Task has already been migrated.
b541f5c1-c205-4969-9b23-a608323f51c6	User Account Policy for 'Tauriel Mirkwood' in 'Windows Computers' - v. 1	Skipped: Task has already been migrated.
0709ee0b-bc4b-4d3a-8674-bbad5f277053	User Account Policy for 'Test Password Disclosure' in 'Windows Computers' - v. 1	Skipped: Task has already been migrated.

The migration state can be:

- o Ready for migration.
- o Skipped: Is not using a Local Security Command.
- o Skipped: Task has already been migrated.

4. To learn more about items that are listed as *Ready for migration* click on the item in the table. This opens up the **LSS Migration Readiness Report - Drilldown** report.

LSS Migration Readiness Report - Drilldown

Filter Report Refresh CSV PDF Search

Drag column here for grouping

Action	Resource Type	Resource Name	Resource RID	For Computer Group	From Resource Id
Will Create	User	Guest	501	Windows Computers	00000000-0000-0000-0000-000000000000
Will Create	Password Randomization Policy	Password Management Policy for user 'Guest' on computers 'Windows Computers'	N/A	Windows Computers	8a8d473b-3624-4ba4-84dc-3c2508b3bf1d

The drilldown report shows the Action to be performed for that particular item during the migration.

For example: The data shown in the image above indicates that two items will be created in Privilege Manager's Local Security. One item is a *User* the other a *Password Randomization* entry. For the user the item is created with **Resource Name** of *Administrator* and the **Resource RID** will be *500*. It further shows that the action will be done **For Computer Group** and **From ResourceID** as indicated.

During the report creating, Privilege Manager will find and resolve conflicts that might be caused by many policies targeting the same computer group with the same user/group, or multiple password rotation policies for the same user. The LSS migration script resolves these conflicts in a way that respects the logic of the initial policy set-up, and comply with the new model for the data.

5. If there aren't any conflicts and all items found can be migrated, use the LSS Migration tasks to migrate and then enable to items pertaining to Local Security. This is a two step process, first migrate then enable.

1. Search for LSS Migration Task (1/2): Migrate all items.

LSS Migration Task (1/2): Migrate all items.

Details Task History Change History Refresh More

Details

This task can be scheduled to run periodically on the web server or be run immediately by using the Run Task option from the More menu.

Name: LSS Migration Task (1/2): Migrate all items.

Description:

Command: LSS Migration Script (1/2): Migrate all items.

Parameters

Parameters for this task. No parameters

Schedules

Schedules for this task.

0 Items

New Schedule

2. After all items are migrated, run the LSS Migration Task (2/2): Enable migrated items.

LSS Migration Task (2/2): Enable migrated items. 🔍 🔔 ? D

[Details](#) [Task History](#) [Change History](#) Refresh More

Details

This task can be scheduled to run periodically on the web server or be run immediately by using the Run Task option from the More menu.

Name: LSS Migration Task (2/2): Enable migrated items.

Description:

Command: LSS Migration Script (2/2): Enable the migrated items. ▾

Parameters

Parameters for this task. No parameters

Schedules

Schedules for this task.

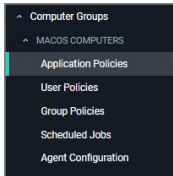
0 Items 🔍

--

New Schedule

Either of these tasks can be edited, to have parameters or schedules defined.

Default macOS Computer Group.



This is the navigation entry point into the macOS Computer Group. The sub nodes are in feature parity with other OS computer groups. All policies or resources underneath **MACOS COMPUTERS** pertain to that specific default computer group.

Refer to the [Policy Wizard](#) section for details on decision points for:

- [Creating a Monitoring Policy](#)
- [Creating a Controlling Elevation Policy for macOS](#)
- [Creating a Controlling Allow Policy for macOS](#)
- [Creating a Controlling Block Policy for macOS](#)

macOS Specific Policies

Once your macOS agent is registered, creating policies for your macOS machines follows a very similar process to creating policies for Windows machines in Privilege Manager. The main approach should be via the use of the Policy Wizard aided by the following:

1. Collect File Data – This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed via **File Inventory**.
2. Create Filters – This step sorts important file data (Events) according to different criteria.
3. Create Policies – This step defines what
 1. Actions to perform on applications and
 2. Targets (Locations) for those actions.
4. Assign Filters to Policies – This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be set to active.
5. Order your Policies based on priority level—Once your policies are created, the order they execute across your network matters. See the [Policy Priority](#) topic for more details.

In macOS, roles are bifurcated into two groups: Admins, and Users rather than by Group Policy Objects (GPO) found in Windows environments.

Actions Supported by macOS Agents (Kernel vs System Extensions)

The following actions are supported by macOS agents:

Allow Copy to /Applications Directory	supported	n/a
Allow Package Installation	elevate via UI	via sudo plugin
Application Approval Request (with Offline Fallback) Message Action	elevate via UI	via sudo plugin
Application Approval Request (with ServiceNow Request Item Number) Message Action	elevate via UI	via sudo plugin
Application Approval Request Message Action (workflow request)	elevate via UI	via sudo plugin
Application Denied Message Action	no difference	no difference
Application Justification Message Action	elevate via UI	via sudo plugin
Application Warning Message Action	no difference	no difference
Deny Execute / Deny Execute Message	no difference	no difference
File Quarantine	no difference	no difference
Quarantine Message	no difference	no difference
Run as Root (Elevate)	no difference	via sudo plugin
Just In Time (Elevate)	n/a	via sudo plugin

Agent Behavior with Actions

When a policy is used to manage .pkg installations on macOS endpoints with the Privilege Manager agent installed, you can expect the following behaviors:

Installation of a .pkg happens without prompting for credentials when

- the only action configured in the policy is **Allow Package Installation** or
- if any of the following are configured along with **Allow Package Installation**:
 - Application Approval Request Message Action
 - Application Approval Request (with Offline Fallback) Message Action
 - Approval Request (with ServiceNow Request Item Number) Form Action
 - Application Justification Message Action
 - Application Warning Message Action

A .pkg will NOT be installed if the only action is either of the following:

- Deny Execute
- Deny Execute + Deny Execute Message
- Application Denied Message Action

Any .pkg not managed by a Privilege Manager policy will be installed via the normal macOS workflow requiring admin credentials when prompted.

Allow Copy to Install Applications

Note: This is the procedure for the kernel extension.

A policy can be created to allow or deny standard users to install specific applications by copying/pulling the application into the /Applications folder. Follow this example to create a policy that will enable this functionality for your macOS user.

1. Navigate to your macOS Computer Group and select **Application Policies**.
2. Click **Create Policy**.
3. Select **Controlling** and click **Next Step**.
4. Select **Allow** and click **Next Step**.
5. Select what exactly you want the policy to target. This can be based on an **Existing Filter**, a **File Upload**, and/or **Inventoried File(s)**. Multiple targets can be selected.
6. Click **Next Step**.
7. Enter a Name and description for your policy, click **Create Policy**.

Allow Copy to Install Application Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (0 total endpoints) MacOS Computers x	Add
Deployment	Not deployed (Policy is inactive)	
Last Modified	Aug 5, 2020, 4:23:26 PM by Administrator	
Priority *	<input type="text" value="85"/>	
Description	<input type="text" value="This policy allows the specified applications."/>	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted	Wizard Generated App Bundle Filter	Edit
Inclusions	Add Inclusions	
Exclusions	Add Exclusions	

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. [Actions](#)

Actions	Add Actions
Child Actions	Add Child Actions
Audit Policy Events	<input type="checkbox"/> Record all activity detected by this policy in Policy Events

8. Click **Add Inclusions**.
9. Search for and add the **Copy Install Application** filter.
10. Click **Update**.

Allow Copy to Install Application Policy

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted: 1 (0 total endpoints) Add
MacOS Computers x

Deployment: Not deployed (Policy is inactive)

Last Modified: Aug 5, 2020, 4:23:26 PM by [User] Administrator

Priority:

Description:

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted: Wizard Generated App Bundle Filter Edit

Inclusions: Copy Install Application Edit

Exclusions: [Add Exclusions](#)

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. [Actions](#)

Actions: [Add Actions](#)

Child Actions: [Add Child Actions](#)

Audit Policy Events: Record all activity detected by this policy in [Policy Events](#)

11. Click **Save Changes**.

12. Set the **Inactive** switch to **Active** for policy updates at the endpoint.

Note: The new Copy Install Application Filter should not be used with the existing Privilege Manager Copy/Installer Helper Parent Process Filter, which should be removed from any policy before adding the new Copy Install Application Filter to the policy.

Updating Existing Policies to Use the Copy Install Application Filter

If you have policies that currently use the Privilege Manager Copy/Installer Helper Parent Process Filter use the following steps to update them to use the Copy Install Application Filter in the Privilege Manager UI:

1. Navigate to the macOS Computers Group and select **Application Policies**.
2. For each application that currently uses the **Privilege manager copy/installer helper parent process filter** as an inclusion filter, remove that filter and add the **Copy Install Application** filter instead.
3. Click **Update**.
4. Under Actions remove **Allow copy to /Applications Directory** and add the **Application Approval Request Message Action** in its place.
5. Click **Update**.
6. Click **Show Advanced** and set these two option to active:
 - o Continue Enforcing.
 - o Enforce Child Processes.

Policy Enforcement

Continue Enforcing After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.

Applies To All Processes Policy will apply to system based processes. If setting is not enabled, policy will only apply to interactive users.

Enforce Child Processes Include child processes in the policy enforcement

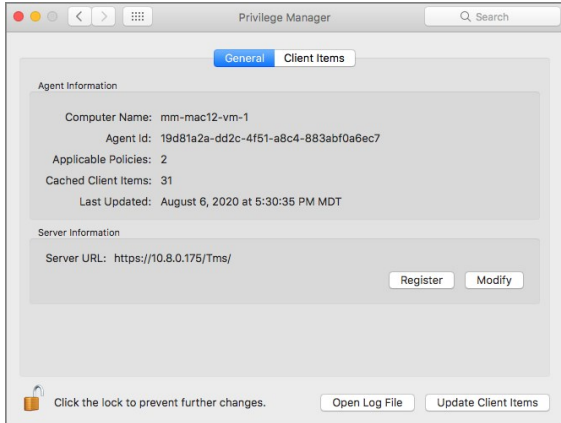
Stage 2 Processing Only needed for catch-all deny policies to ensure that the policy only applies to applications NOT allowed directly or indirectly by a policy that applies to the parent process.

7. Click **Save Changes**.

Updating the Endpoint

On the macOS endpoint,

1. Open **System Preferences | Privilege Manager**.

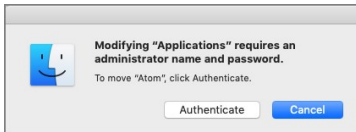


2. Click **Update Client Items**

The agent updates with new and updated policies and synchronizes.

Expected User Experience

After the policies are updated, users can open a DMG or just drag and drop an application bundle to /Applications. They'll see the authenticate message and click **Authenticate**.



Deny Zoom Application

Note: This is the procedure for the kernel extension.

With your monitoring policies properly set up, anything you do on your Mac test machine will be discovered by Privilege Manager. For this example we will create a policy that blocks the Zoom applications.

File Inventory

Open the Zoom applications on an macOS test endpoint. When these applications are opened, Privilege Manager discovers these as an *Application Action from Event Discovery Testing Computers Audit Policy (MacOS)*.

1. In the Privilege Manager Console, navigate to **File Inventory**.
2. Verify new items have been registered by your Event Discovery Testing Computers (MacOS) policy. These may be listed as **New Loaded Resources**.

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	7/19/2020 9:49:55 AM			7/19/20, 5:49 AM
New Loaded Resource	81oSbXBhVsvDEa/MI3KTZ...			7/14/20, 1:46 PM

3. Select a **New Loaded Resource** link.
4. On the loaded Resource Explorer page, click the **Discover Now** button. It still may take time to properly load details about these new events, usually indicated by a **Discovery Status** of **New**.

The screenshot shows the 'New Loaded Resource 7/19/2020 9:49:55 AM' page. It includes a navigation bar with 'Back to File Inventory', a search bar, and notification icons. Below the navigation are buttons for 'Discover Now', 'Manage Application', and 'Delete'. The main content area is divided into a left sidebar with tabs for 'Summary', 'Reports', 'Known Data', 'Events', and 'Associations'. The right pane displays details for the resource:

- File Name: New Loaded Resource 7/19/2020 9:49:55 AM
- File Hashes: sha1: 505647a61a3843df4d13153c35cdd4ee9490cf64
- View Reputation: VirusTotal.com
- Discovery Status: New

Clicking the Discover Now button creates and executes a **Manual client-side resource discovery** task. If you click the status link the task page opens (not shown in this example sequence).

On the Resource Explorer page of a fully discovered resource, you can click **Manage Application** to select the details you want to use to either create a filter or create and add to a policy options.

The screenshot shows the 'Manage Application' dialog box overlaid on the Resource Explorer page for 'Zoomusinstaller.pkg'. The dialog has three sections:

- File Name**: Zoomusinstaller.pkg
- File Path**: (empty field)
- Hash**: 798f3039172a1202130adcfbc41fe0927b7af87f

At the bottom of the dialog are three buttons: 'Cancel', 'Create and Add to Policy', and 'Create Filter'.

When a resource is fully discovered it is displayed with full name on the discovery events page:

File Inventory

30 Items Past month 🔍

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
Zoomusinstaller.pkg				7/28/20, 5:37 PM

From the File Inventory page you can also use the **View File** or **Create Filter** options to create specific filters for the discovered applications and assign those to existing policies.

File Inventory

30 Items Past month 🔍

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
Zoomusinstaller.pkg				7/28/20, 5:37 PM
ISSSetup.exe	ThycoticSetup.exe	IBM Security Secret Server Installer	10.7.59.7	7/28/20, 5:07 PM
New Loaded Resource eEU6RTTib2nz6/90...				7/21/20, 7:34 PM
New Loaded Resource lYTQfpGcjB0tgsZVDPQSh...				7/20/20, 4:03 PM
New Loaded Resource Swe/viwCwZj/9Pnc0xrqAh...				7/20/20, 4:03 PM
New Loaded Resource 5jggaqq1QE+HDTow/jec...				7/20/20, 4:03 PM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 7/19/2020 9:49:55 AM				7/19/20, 5:49 AM
New Loaded Resource 81oSbXBhvSvDEa/MI3KTZ...				7/14/20, 1:46 PM
New Loaded Resource xj3n49yr3TYfO/Fo3mH1+E...				7/13/20, 5:59 PM
New Loaded Resource 61egISzn90Zj/6is3HEriuhe...				7/13/20, 5:59 PM
New Loaded Resource 2F0MioaPzo4WTH1/IH6M...				7/13/20, 5:58 PM

Zoomusinstaller.pkg ✕

Create Filter

View File

Assign to Policy

Once the resources have been fully discovered, the fastest way to either create a new policy or add to an existing one is via the Assign to Policy link on the Events page.

1. Click **Create Filter**.
2. The **Manage Application** page opens for the selected resource.

Manage Application

File Name ⓘ

Zoomusinstaller.pkg

File Path ⓘ

Hash ⓘ

798f3039172a1202130adcfbc41fe0927b7af87f

Cancel Create and Add to Policy Create Filter

3. Click **Create and Add To Policy**.

Manage Application

Policy

Cancel Update Policy

4. On the **Manage Application** page select your existing deny application execution policy from the drop-down and click **Update Policy**.

Test Deny Application Execution Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (0 total endpoints) MacOS Computers Add

Deployment Not deployed (Policy is inactive)

Last Modified Aug 5, 2020, 6:53:43 PM by [user]

Priority * 3

Description This policy prevents processes from running.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

Applications Targeted Wizard Generated File Specification Filter for Zoomusinstaller.pkg Edit

Inclusions Add Inclusions

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user.

Actions Deny Execute Deny Execute Message Edit

5. Set the **Inactive** switch to **Active**.

Updating the Endpoint

On the macOS endpoint,

1. Open **System Preferences | Privilege Manager**.

Privilege Manager Search

General Client Items

Agent Information

Computer Name: mm-mac12-vm-1
Agent Id: 19d81a2a-dd2c-4f51-a8c4-883abf0a6ec7
Applicable Policies: 2
Cached Client Items: 31
Last Updated: August 6, 2020 at 5:30:35 PM MDT

Server Information

Server URL: https://10.8.0.175/Tms/ Register Modify

Click the lock to prevent further changes. Open Log File Update Client Items

2. Click **Update Client Items**.

Policy Verification

Once this Deny-policy is updated on your endpoint, when you click Zoom, you will see a message like this:

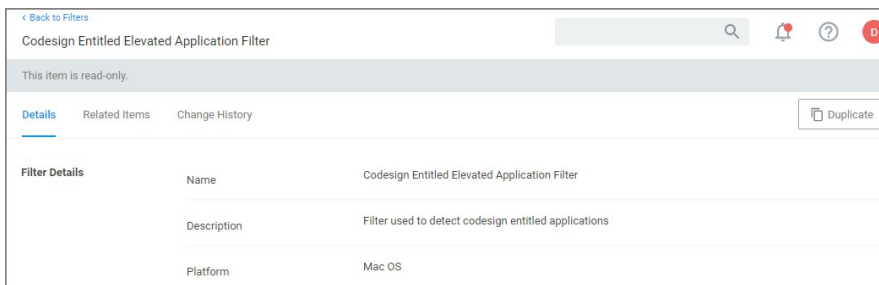
The application "Zoom" can't be opened.

OK

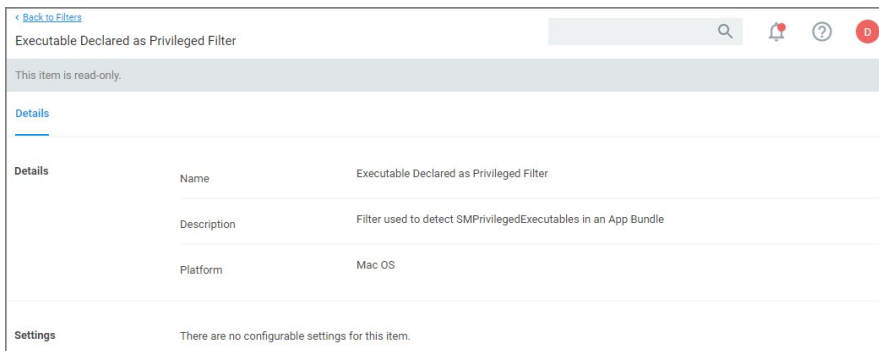
Determine Admin Requirement

Use discovery with event notification to determine if an application requests or requires administrative privileges to perform tasks or run on a macOS endpoint.

1. Use the **Codesign Entitled Elevated Application Filter**. This filter creates events for application bundles that have a specific entitlement that might prompt for administrative permissions if launched.



2. Use the **Executable Declared as Privileged Filter**. This filter creates events for application bundles that list a privileged helper in their info.plist files.



3. Add both filters as the application target to a new policy and enable the **Send Policy Feedback** action for that policy.

Creating the Policy

1. Using the Policy Wizard, create a monitoring policy for specific applications.
2. Choose your targets. You can specify several different targets, for this example select **Existing Filter**.
3. Search for and add the two duplicated filters you created above.
4. Click **Update**.
5. Click **Next Step**.
6. Name your policy and click **Create Policy**.
7. Under Actions, set the **Audit Policy Events** switch to active.

Determine Admin Requirement Monitor Policy

General Policy Events Change History

Inactive Refresh More

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (0 total endpoints) [MacOS Computers](#) [Add](#)

Deployment Not deployed (Policy is inactive)

Last Modified Aug 5, 2020, 7:41:04 PM by [\[User\]](#)

Priority *

Description

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted [Codesign Entitled Elevated Application Filter](#) [Executable Declared as Privileged Filter](#) [Edit](#)

Inclusions [Add Inclusions](#)

Exclusions [Add Exclusions](#)

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy [Actions](#)

Actions [Add Actions](#)

Child Actions [Add Child Actions](#)

Audit Policy Events Record all activity detected by this policy in [Policy Events](#)

8. Click **Save Changes**.

9. Set the **Inactive** switch to **Active**.

10. Next to **Deployment** click the **I** icon and run the **Resource and Collection Targeting Update** task.

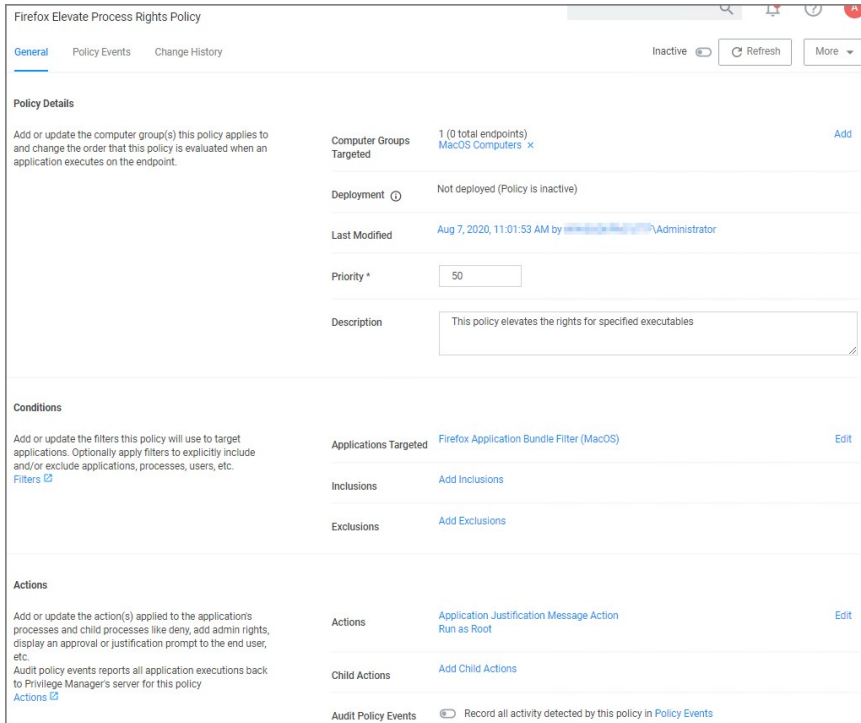
Note: There is currently no option to determine if command-line tools require admin privileges.

Require Justification - FireFox

The following example provides information on setting up a justification required policy for FireFox on a macOS endpoint.

Create a filter for Firefox either from discovery or manually. Use that filter in the steps below.

1. Using the Policy Wizard, create a controlling policy that elevates application execution on endpoints.
2. Select **Require Justification**, and click **Next Step**.
3. Select what file type to target, for this example select **Executable**, and click **Next Step**.
4. Choose your target, for this example **Existing Filter**.
5. Search for and add your Firefox filter.
6. Click **Updated**.
7. Click **Next Step**.
8. Name your policy and add a description, click **Create Policy**.

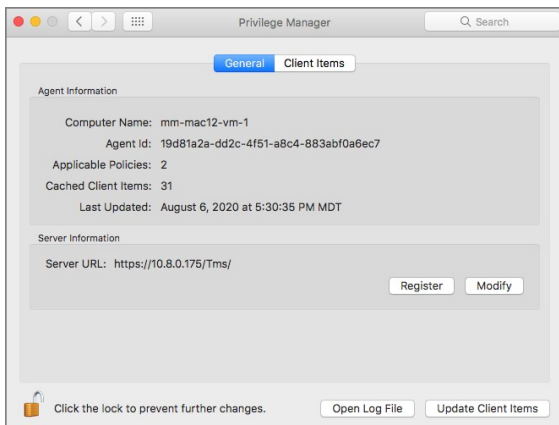


9. Set the **Inactive** switch to **Active**.

Updating the Endpoint

On the macOS endpoint,

1. Open **System Preferences | Privilege Manager**.




2. Click **Update Client Items**.

The agent updates with new and updated policies and synchronizes.

Expected User Experience

Once the justification policy is updated on an endpoint, when users click Firefox they will see a prompt to enter their justification reason for accessing Firefox.

Application Notice 

Please provide a reason as to why you require this application to be run with elevated rights.

Application Firefox
User standard1

Type a brief explanation describing why this application is necessary. This explanation will be recorded and may be reviewed by the IT staff for consideration into [corporate policy](#).

Reason (required)

Cancel Publisher Info Continue

macOS Approval Process

To accommodate the new macOS Endpoint Security system extensions, the approval workflow of the macOS agent now terminates any justification or approval process and presents the user with an applicable message action.

The following workflows are impacted by this change:

- Application Approval Request Message Action
- Deny Execute
- Deny Execute and Deny Execute Message Action
- Deny Execute and Application Denied Message Action
- Application Justification Message Action
- Application Warning Message Action

Refer to the [Actions](#) topic.

Application Approval Request Message Action

Workflow **prior to** Privilege Manager 10.8:

Action waits for the user to either click **Cancel** or enter an **Approval Request Message** and click **Request Approval**.

Workflow **starting with** Privilege Manager 10.8:

Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.

- If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
- If the user clicks **Request Approval**, the Approval is submitted and the user is presented with a modal dialog informing them that the approval request has been submitted and that they will be notified via Notification Center.
 - If successfully submitted, the request is queued and monitored by Privilege Manager.app.
 - If denied, a notification is pushed to the Notification Center indicating the app was denied. Clicking the notification or clicking the button to dismiss the notification causes the notification to be removed from the Notification Center.
 - If the request is approved, a notification is pushed to the Notification Center indicating the request was approved. Behavior for:
 - **application bundles**: Clicking the notification causes the app to be launched and the notification to be removed from the Notification Center.
 - **command-line utilities**: Clicking the notification causes the notification to be removed from the Notification Center. The user will have to manually run the command-line utility from a terminal window. If the user chooses to dismiss the notification, the notification is removed from the Notification Center and no further action is taken.
 - If the approval request fails to be submitted, **Request Approval** is disabled on the Request Approval dialog and an error message displayed.

Deny Execute

This action immediately denies the execution of the application and no interaction with Privilege Manager.app is required. The workflow is:

- MacOS will display a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- No further user interaction is provided or necessary.

Deny Execute and Deny Execute Message Action

This action immediately denies the execution of the application. The workflow is:

- MacOS will display a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- A user notification is posted to the Notification Center that indicates the process was denied.
 - Clicking the notification or clicking the button to dismiss the notification causes the notification to be removed from the Notification Center.
- No further user interaction is necessary.

Deny Execute and Application Denied Message Action

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
- The custom **Application Denied Message** is shown. **Cancel** and **Publisher Info** are the only buttons enabled.
 - Clicking **Cancel** closes the window.
 - Clicking **Publisher Info** displays certificate information for the application that was denied.
- No further user interaction is necessary.

Application Justification Message Action

This action waits for the user to either **Cancel** or enter a **Justification Message** and click **Continue**. The workflow is:

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
 - If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
 - If the user clicks **Continue**, the **Justification** will be submitted and the app bundle will be launched.

Application Warning Message Action

This action waits for the user to either click **Cancel** or **Continue**. The workflow is:

- Privilege Manager immediately denies the execution with macOS displaying a dialog indicating the application can't be opened. If the user has granted Privilege Manager.app the necessary *SendEvents* right, Privilege Manager closes the dialog.
 - If the user clicks **Cancel**, the dialog is dismissed and no further action taken.
 - If the user clicks **Continue**, the app bundle will be launched.

Move to Trash Bin Policy

When a standard user deletes an application bundle via **-delete** or **drag-n-drop** from /Applications, the following actions are taken based on policy evaluation:

- Allow - Is allowed without prompting user for credentials
- Present appropriate Advanced Message Dialog:
 - Approval - Approval process is invoked before it is allowed to complete
 - Cancelled - It is denied.
 - Denied - Denied dialog is invoked and user can not delete the application bundle
 - Justification - Justification process is invoked before it is allowed to complete
 - Cancelled - It is denied.
 - Offline-Approval - Offline-approval process is invoked before it is allowed to complete
 - Cancelled - It is denied.
 - Warning - Warning dialog is invoked before it is allowed to complete
 - Cancelled - It is denied.

To allow a standard user to delete application bundles from the /Applications directory, create an elevation policy that uses the **Copy Install Application** filter under Inclusions. We recommend to also add a justification message action.

1. Navigate to your macOS Computer Group and select **Application Policies**.
2. Click **Create Policy**.
3. Select **Controlling** and click **Next Step**.
4. Select **Elevate** and click **Next Step**.
5. Select **Require Justification** and click **Next Step**.
6. Select what types to target. This can be based of an **Executables**, a **Installer Packages**, and/or **Scripts**. Multiple targets can be selected.
7. Click **Next Step**.
8. Select what exactly you want the policy to target. This can be based of an **Existing Filter**, a **File Upload**, and/or **Inventoried File(s)**. Multiple targets can be selected.
9. Click **Next Step**.
10. Enter a Name and description for your policy, click **Create Policy**.
11. Click **Add Inclusions**.
12. Search for and add the **Copy Install Application** filter.
13. Click **Update**.
14. Click **Save Changes**.
15. Set the **Inactive** switch to **Active** for policy updates at the endpoint.

Conditions	
Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters	Applications Targeted Add Applications Targeted
	Inclusions Copy Install Application
	Exclusions Add Exclusions
Actions	
Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy Actions	Actions Application Justification Message Action
	Child Actions Add Child Actions
	Audit Policy Events <input type="checkbox"/> Record all activity detected by this policy in Policy Events

Application Self-elevation

Finder Sync Extensions allow application control on macOS endpoints. Just as on Windows endpoints, users can request application self-elevation via right-click mouse action. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.

Note: This feature is only available with the KEXT based Privilege Manager Agent. Self-elevation in this form is not possible with the system extension.

Configuring Application Self-elevation

Your Privilege Manager needs to be configured to allow self-elevation of applications on an endpoint. Follow these server configuration steps:

1. Navigate to your **MacOS Computers** computer group and select **Agent Configuration**.
2. Under **Self-Elevation** set the **Allow Self-Elevate** switch to **Yes**.
3. In the **Menu text** entry field you may customize the default **Request run as administrator** text.

The screenshot shows the 'Application Control Agent Configuration Policy (MacOS)' interface. The 'Self-Elevation' section is highlighted with a red box. It contains the following fields:

- Allow Self-Elevate:** A toggle switch currently set to 'No'.
- Menu Text:** A text input field containing 'Request run as administrator'.

Other sections visible include 'Details' (Name: Application Control Agent Configuration Policy (MacOS), Description: This policy provides global configuration settings for the Mac OS Application Control Agent, Platform: Mac OS), 'Intervals' (Send Application Action Events: 5 Minute(s), Task Polling Interval: 5 Minute(s)), 'Application Action Defaults' (Quarantine Path: /usr/local/tycolic/quarantine/), and 'Secure Token (macOS)' (Secure Token Enabled Management Credential).

4. Click **Save Changes**.

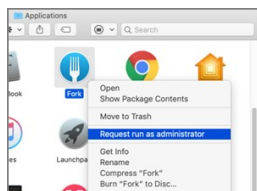
Note: When Self-Elevation options are modified in the **MacOS Agent Configuration**, client items on a macOS system must be updated and on older versions of macOS the user must logout and login for the changes to take effect.

After enabling Self-Elevation of applications in the **MacOS Agent Configuration**, you can create policies to target the **User Requested Run As Administrator Filter (macOS)** and specify which action you want taken. If you choose Approval Request, users will have to request and gain approval before having the application elevated.

How to Request an Application Run as Administrator

Note: This is the procedure for kernel extension. On endpoints using system extension, the [Unexpected Link Text](#) needs to be used instead.

To request to run an application as Administrator, the user at the macOS endpoint navigates to and selects the applications in Finder and uses either right-click or Control+Click to invoke Finder's context menu:



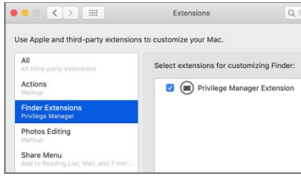
Here the user selects the Request run as administrator menu option.

Depending on the policy in place, this will either be granted immediately or trigger an approval request.

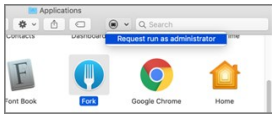
Troubleshooting: Verify the Finder Extension Is Installed

The Finder Privilege Manager extension installs by default during an agent install or upgrade. The extension is enabled/disabled based on the **MacOS Agent Configuration** policy on the Privilege Manager Server. If the extension is not enabled, check with your system administrator.

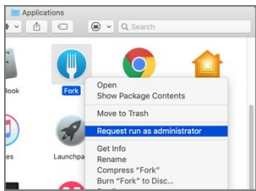
1. Open **System Preferences | Extensions**.
2. Select **Finder Extensions**.
3. Verify that Privilege Manager Extension is listed and enabled for customizing Finder.



Once the Privilege Manager Extension is enabled, the extension icon is visible in Finder.



The extension is also present as a menu item when you right-click or control+click an application in Finder.



Finder Extension and Drive Type Extensions

On endpoints that are also using OneDrive, GoogleDrive, DropBox, or similar extensions, when enabling the Finder Extension the endpoint will take about 2 min to correctly initialize.

For systems prior to Privilege Manager 10.8, if a finder sync extension does not work correctly. Execute the following steps in sequence:

1. Disable the Privilege Manager Finder Extension.
2. Install/Enable other third-party Finder Extension.
3. Enable the Privilege Manager Finder Extension.

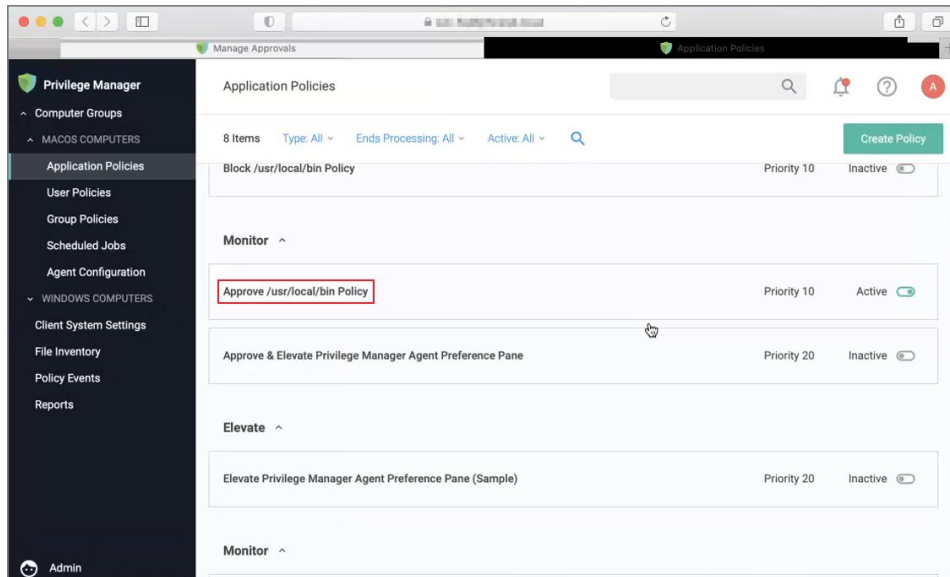
macOS Application Approval Process via Sudo Plugin

The macOS sudo plugin provides the means to run an application elevated via Terminal.app on macOS systems running Catalina and Big Sur. The sudo plugin also provides user feedback via Terminal when the request is approved or denied.

When an application policy requires approval, the user will be presented with a message in Terminal "Waiting for approval... (Ctrl+C to cancel)". The application execution is blocked until the approval comes in. If the request is approved, the application runs. If it is denied, the process exits.

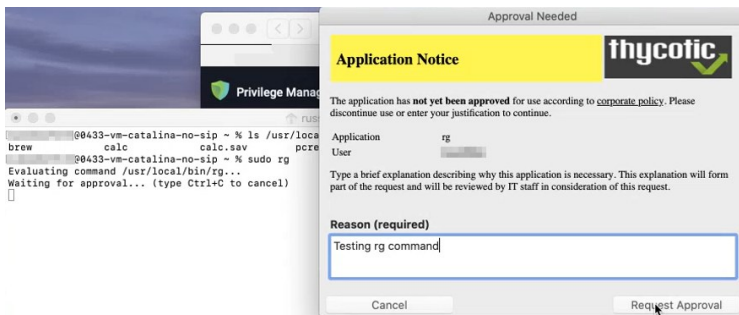
Example: Elevate Applications Executed from Folder

The following monitor policy is configured to elevate applications located within `/usr/local/bin` after an approval when run via sudo.



Endpoint Interaction

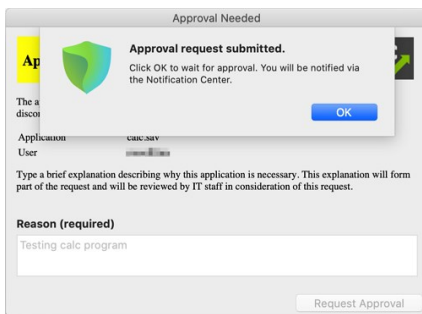
1. At the macOS endpoint, open Terminal.app and run an application via sudo. The **Approval Needed** message opens:



2. Enter the approval reason and click **Request Approval**

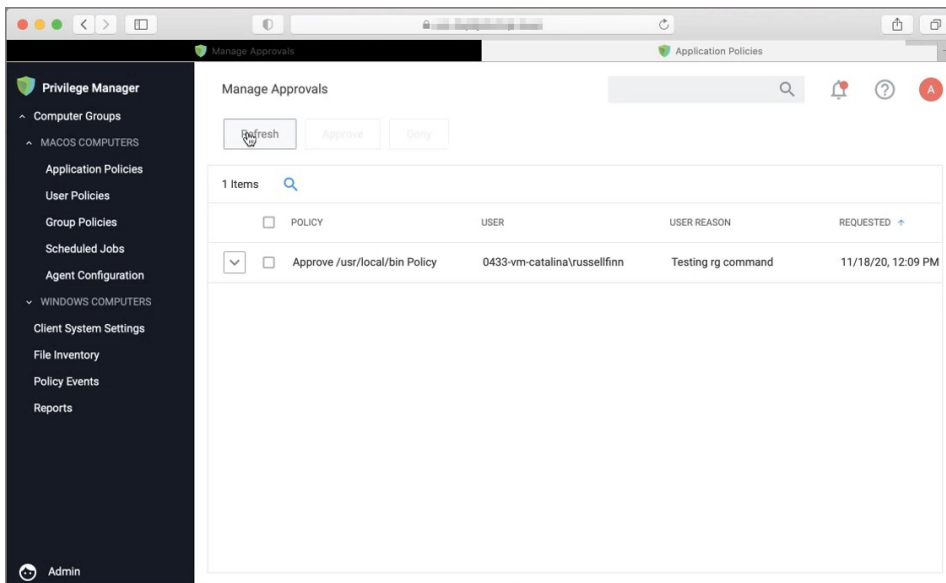
In the Terminal, **Waiting for approval... (Ctrl+C to cancel)** is displayed and the **Approval request submitted.** dialog opens.

3. You will be notified of any status change via the notification center. Click **OK** to wait for the approval.



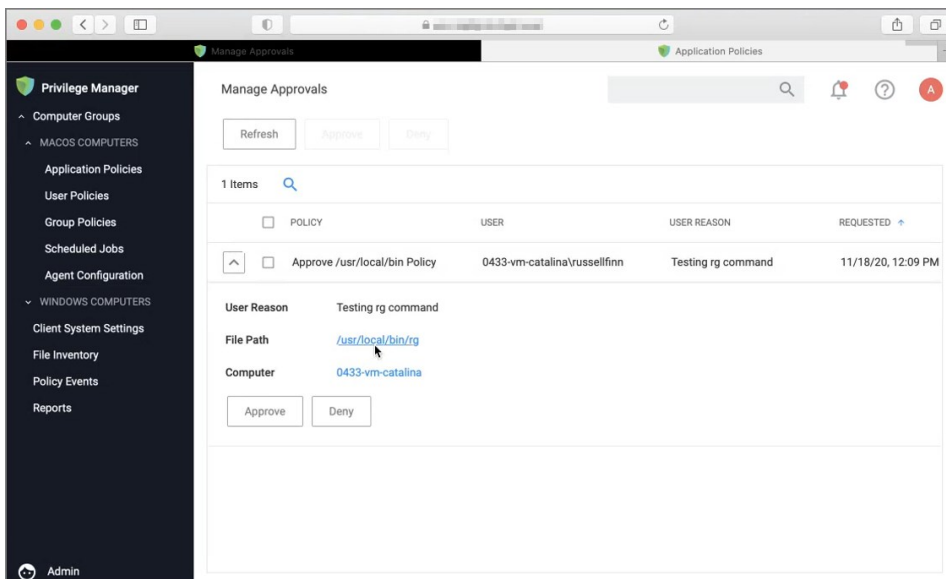
Privilege Manager Console Interaction

1. As an approval supervisor, navigate to **Admin | Manage Approvals**.

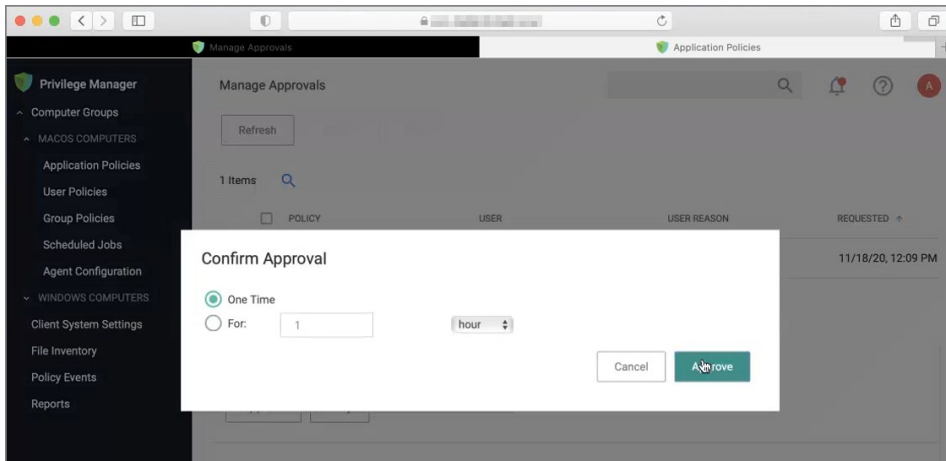


2. If no approval requests are listed, click **Refresh**.

3. **Expand** the approval you want to either approve or deny.



4. Click **Approve**.



- On the **Confirm Approval** modal, choose to either issue a **One Time** or a **timed** approval. The default opens to **One Time**.
- Click **Approve**

Endpoint Interaction

Following Approval

Following an approval, Terminal writes **Running command elevated** and shows other process messages.

```
Terminal --zsh -- #2
@0433-vm-catalina-no-sip ~ % sudo rg interface /etc/postfix
Evaluating command /usr/local/bin/rg...
Waiting for approval... (type Ctrl+C to cancel)
Running command elevated
/etc/postfix/generic
90:# or when it is listed in $inet_interfaces or
91:# $proxy_interfaces.
197:# inet_interfaces
198:# The network interface addresses that this system
202:# proxy_interfaces
203:# Other interfaces that this machine receives mail on
/etc/postfix/virtual
97:# tination, or when it is listed in $inet_interfaces
100:# or $proxy_interfaces.
254:# inet_interfaces
255:# The network interface addresses that this system
271:# proxy_interfaces
272:# Other interfaces that this machine receives mail on
/etc/postfix/main.cf
122:# The inet_interfaces parameter specifies the network interface
124:# the software claims all active interfaces on the machine. The
127:# See also the proxy_interfaces parameter, for network addresses that
```

Following Denial

Following a denial, Terminal writes **Approval request was denied** and shows other process messages.

```
Terminal --zsh -- #2
@0433-vm-catalina-no-sip ~ % sudo rg interface /etc/postfix
Evaluating command /usr/local/bin/rg...
Waiting for approval... (type Ctrl+C to cancel)
Approval request was denied
@0433-vm-catalina-no-sip ~ %
```

Adding macOS Agents to a Computer Testing Group

The Policy Configuration examples in the following section will use a Learning Mode Policy that enables us to perform actions (i.e. run applications) on a test computer that Privilege Manager will then pick up. This makes targeting specific applications during policy creation easy.

Creating a MacOS Test Computer Group

To create a Monitoring (or Learning Mode Policy) on your Mac, begin by

1. Creating a macOS based test computer group:
 1. Navigate to **Computer Groups**.
 2. Click **Create Computer Group**.
 3. From the **Platform** drop-down select MacOS.
 4. Enter a name and description for your new group.
 5. Click **Create**.

MacOS Test Computer Group Scoped to Mac Computers

Details Results Related Policies Refresh More

Details

Name MacOS Test Computer Group Scoped to Mac Computers

Description

Platform Mac OS

Filter Rules

All filtering rules start with "All Computers". Each consecutive rule removes resources from that list in order. Add Rule

1 Items

ORDER	OPERATION	LIST TYPE	SELECTED ITEMS
0	Only Keep Computers In	Collection	All MacOS Computers

6. Add the macOS endpoints you want to be part of the computer group.
7. Click **Save Changes**.
8. Pin your computer group to the left navigation menu for quick access. Click the bookmark icon next to the computer group name.

Setting Up Monitoring Policies for macOS

1. Under your MacOS Test Computers Computer Group select **Application Policies** and click **Create Application Policy**.
2. From the Policy Wizard select **Monitoring** and click **Next Step**.
3. Select **Everything** and click **Next Step**.
4. Enter a name, for example *MacOS Catch-all Monitor Policy*.
5. Click **Create Policy**.

MacOS Catch-all Monitor Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (0 total endpoints) MacOS Test Computer Group Scoped to Mac Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Aug 6, 2020, 1:33:34 PM by Administrator

Priority * 200

Description This policy monitors the execution of all applications. Not recommend on more than a handful of machines.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

Applications Targeted Add Applications Targeted

Inclusions Add Inclusions

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy Actions

Actions Add Actions

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

6. Customize the policies Conditions, Actions, and Policy Enforcement, for example:

- Under Applications Targeted, click **Add Application Target** and search for and add **Mac OS /Users/ File Specification**.
- Under Exclusions, click **Edit** and add **Default App Bundles File Specification Filter** to the exclusion list.
- Under **Show Advanced | Policy Enforcement** set the switch for **Stage 2 Processing** to active an all others to inactive.

MacOS Catch-all Monitor Policy

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Description This policy monitors the execution of all applications. Not recommend on more than a handful of machines.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

1 Applications Targeted Mac OS /Users/ File Specification Edit

Inclusions Add Inclusions

2 Exclusions Default App Bundles File Specification Filter Edit

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy Actions

Actions Add Actions

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

Policy Enforcement

Continue Enforcing After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.

Applies To All Processes Policy will apply to system based processes. If setting is not enabled, policy will only apply to interactive users.

Enforce Child Processes Include child processes in the policy enforcement

3 Stage 2 Processing Only needed for catch-all deny policies to ensure that the policy only applies to applications NOT allowed directly or indirectly by a policy that applies to the parent process.

Hide Advanced

7. Click **Save Changes**

8. Set the **Inactive** switch to **Active**.

This "Testing Computers" group should only be used for testing specific machines and configuration purposes. It should not be assigned to large groups of computers in your production environment.

Verify that under **Actions** the **Audit Policy Events** switch is active.

Inventoring .pkg Files

Privilege Manager allows the inventory of macOS .pkg files. With the ability to upload and extract the contents within the .pkg files Privilege Manager inventories the applications that are bundled in any given .pkg.

1. Use **Admin | File Upload** to start the inventory process.
2. Choose a file to upload and click **Upload File**.

Upload a File

Application File: ThycoticMana_10.8.15.pkg

Notice: Files uploaded to the server will be stored temporarily during the inventory process without the ability to be executed. The file is then deleted once the process completes.

3. After uploading a .pkg file select the **Go to File Details** button.

Upload a File

The file was successfully uploaded. Click the button below to view the file inventory details and optionally create filters or assign it to a policy.

In the Resource Explorer an Administrator can now look at all the details from the inventory.

- Showing the list of applications:

The screenshot shows a web interface for viewing application details. The title bar reads "ThycoticManagementAgent-10.8.15.pkg". At the top right, there are buttons for "View XML", "Manage Application", and "Delete". Below the title bar, there is a "View" section with a dropdown menu set to "macOS Package Contents" and buttons for "CSV" and "PDF". The main content area is divided into two columns. The left column contains a navigation menu with items: "Summary", "Reports", "Known Data", "File Inventory", "File Header Raw", "macOS Package Contents" (highlighted), "macOS Package Summary", "Hash", "Events", and "Associations". The right column displays a list of applications under the heading "Privilege Manager". The applications listed are: "AgentUtil", "dotnet", "Thycotic.Agent.Service", "ThycoticACS", "ThycoticACSvc", "ACSAgent", "ACSAuthPlugin", and "ACSFinderSyncExtension".

- Click on the main application **Privilege Manager** to see those details:

Privilege Manager

View XML Manage Application Delete

File Name	Privilege Manager
Bundle Identifier	com.thycotic.privilegemanagergui
Bundle Name	Privilege Manager
Display Name	
Version	10.8.15
Short Version	10.8.15
Type	APPL
Region	
Bundle Executable	Privilege Manager
Min System Version	10.11
Application Category	
Copyright	Copyright 2018, Thycotic Software, LLC
File Hashes	md5: 31af37af0829f3696e3d9938dc9a19f7 sha256: 4fffa14b6dea2ba7dc9569888be77759b7d90233fd2afba95a969891e605a75 sha1: 6233612c4438c9148ea08d25678925232fc54b7a
View Reputation	VirusTotal.com Cylance.com

- Click on Known Data and open **Software Management | MacOS Bundle** to see the information specified in the macOS bundle:

Privilege Manager

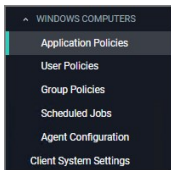
View XML Manage Application Delete

View: Default Viewer

NAME	VALUE
ApplicationCategoryType	
BundleExecutable	Privilege Manager
BundleName	Privilege Manager
Copyright	Copyright 2018, Thycotic Software, LLC
DisplayName	
Identifier	com.thycotic.privilegemanagergui
MinSystemVersion	10.11
PackageType	APPL
Region	
ShortVersion	10.8.15
Version	10.8.15

Note: Any packages that deviate from the standard configuration and layout might not have their contents inventoried correctly. If that is the case, unpack the .pkg and upload each contents file individually for inventory purposes.

Default Windows Computer Group.



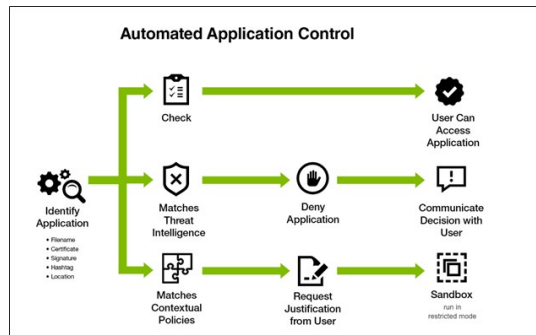
This is the navigation entry point into the Windows Computer Group. The sub nodes are in feature parity with other OS computer groups. All policies or resources underneath **WINDOWS COMPUTERS** pertain to that specific default computer group.

Refer to the [Policy Wizard](#) section for details on decision points for:

- [Creating a Monitoring Policy](#)
- [Creating a Controlling Elevation Policy for macOS](#)
- [Creating a Controlling Allow Policy for macOS](#)
- [Creating a Controlling Block Policy for macOS](#)
- [Creating a Controlling Restrict Policy for Windows](#)

Application Control in Privilege Manager allows administrators to manage all application activity on endpoints. Applications requiring admin rights or root access can be automatically elevated if trusted, applications can be allowed, and malicious applications can be blocked.

In other words, the key to keeping your organization's employees working both securely and effectively without notable disruptions to their work is by tailoring a robust, role-based Application Control system. On the other hand, managing local administrator and root accounts through Local Security is the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.



Dashboard

From Privilege Manager's Home navigate to your computer groups in the left navigation tree and select Application Policies.

The screenshot shows the Privilege Manager interface. On the left is a navigation menu with categories like Computer Groups, Application Policies, User Policies, and Group Policies. The main area displays 'Application Policies' with 36 items. It features filters for Type, Ends Processing, and Active status, along with a search bar and a 'Create Policy' button. The policies are grouped into sections: 'Elevate' (one policy: 'Elevate Privilege Manager Remove Programs Utility Policy', Priority 2, Inactive), 'Deny / Blacklist' (four policies: 'New Deny Application Execution Policy' (Priority 3, Inactive), 'Deny iTunes installation' (Priority 3, Active), 'Test Deny Application Execution Policy' (Priority 3, Inactive), and 'iTune - Deny installation' (Priority 3, Active)), and another 'Elevate' section.

At the most basic level, a Monitoring policy is a policy that takes no action, it exists only to gather data and you can use the data it gathers for audits or for assigning actions to application events retrospectively. For trials and Proof of Concept (PoC) environments these can be pointed at specific endpoints in order to learn about events that are already happening, or in order to test-run specific applications that you want to quickly introduce into Privilege Manager.

Any Monitoring policy will have the **Audit Policy Events** set to active under the Actions section.

Note: Audit Policy Events is generally inactive in production environments outside of specific auditing or data-collecting initiatives due to the large amount of data these policies can gather.

Creating a Monitoring Policy

Use the policy wizard to create a monitoring policy for the learning mode phase on your instance.

1. Under your Computer Group navigate to Application Policies, click **Create Policy**.
2. On the **What type of policy?** page select Monitoring and click **Next Step**.
3. On the **What processes do you want this policy to monitor in this computer group?** page select **Everything** and click **Next Step**.
4. Enter a new name for the policy and click **Create Policy**.

The screenshot displays the configuration page for a monitoring policy named 'Everything Monitor Policy'. The interface includes a search bar, navigation tabs for 'General', 'Policy Events', and 'Change History', and a status indicator 'Inactive'. The 'Policy Details' section contains fields for 'Computer Groups Targeted' (Windows Computers), 'Deployment' (Not deployed), 'Last Modified' (Jul 1, 2020), 'Priority' (200), and a 'Description' field. The 'Conditions' section includes 'Applications Targeted', 'Inclusions', and 'Exclusions'. The 'Actions' section lists 'Actions', 'Child Actions', and 'Audit Policy Events' (Record all activity detected by this policy in Policy Events).

Note: It is not recommended to run be active on more than a handful of machines.

Discover Applications that Require Administrator Rights

The most influential applications are those that require administrator credentials to run. For setting up endpoints that are organized by Least Privilege, you can use a monitoring policy to discover all events requiring Administrator rights.

Use the policy wizard to create a monitoring policy for the learning mode phase on your instance.

1. Under your Computer Group navigate to Application Policies, click **Create Policy**.
2. On the **What type of policy?** page select Monitoring and click **Next Step**.
3. On the **What processes do you want this policy to monitor in this computer group?** page select **Applications Run as Admin** and click **Next Step**.
4. Enter a new name for the policy and click **Create Policy**.

Run with Administrator Rights Monitor Applications Policy

General Policy Events Change History

Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) Windows Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jul 1, 2020, 3:07:57 PM by Administrator

Priority * 190

Description Monitors the execution of applications that are run with Administrator Rights.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

Applications Targeted Administrators Edit

Inclusions Add Inclusions

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. Actions

Actions Add Actions

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

View Policy Results

To view all feedback, or event, sent from your existing policies with the Send Policy Feedback activity checked, navigate to **Policy Events**. Events will be listed in the main section and on the left sidebar you can scope results for certain policies, computers, time frame, etc. You can use this view to assign any events to policies by clicking Assign to Policy under the event listing.

Privilege Manager

Computer Groups

- COPY OF WINDOWS COMPUTERS
- LINUX COMPUTERS
- MACOS COMPUTERS

Application Policies

User Policies

Group Policies

Scheduled Jobs

Agent Configuration

TESTINGLSS

WINDOWS COMPUTERS

- Application Policies
- User Policies
- Group Policies
- Scheduled Jobs
- Agent Configuration
- Client System Settings
- File Inventory
- Policy Events

Policy Events

14 Items Policy: All

FILE NAME	# OF EVENTS	POLICY	LAST EVENT
Arellia.Agent.InventoryHelper.exe	102	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 2:41 PM
taskhostw.exe	36	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 12:07 PM
conhost.exe	20	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 8:07 AM
slui.exe	20	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 9:01 AM
chrome.exe	16	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 1:16 PM
opera_autoupdate.exe	14	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 8:07 AM
InstallAgent.exe	13	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 8:07 AM
msfeedssync.exe	10	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 2:41 PM
installer.exe	7	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 8:07 AM
launcher.exe	7	New Monitor Applications Run with Administrator Rights Policy	7/1/20, 8:07 AM

Discover All Events on Test Endpoints

Another type of monitoring policy will discover all events on targeted machines regardless of whether the application requires Administrator Rights. This policy is used in test environments to quickly target policies at untrusted/unwanted applications, but is not recommended for production settings.

- Under your Computer Group navigate to Application Policies, click **Create Policy**.
- On the **What type of policy?** page select **Monitoring** and click **Next Step**.
- On the **What processes do you want this policy to monitor in this computer group?** page select **Everything** and click **Next Step**.
- Enter a new name for the policy and click **Create Policy**.
- Under **Computer Groups Targeted** add the **Application Compatibility Testing Windows Computers (Target)** collection and remove the **Windows Computer** target.

Test Computer Monitor Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (0 total endpoints)
Application Compatibility Testing Windows Computers (Target) x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jul 23, 2020, 5:24:20 PM by [redacted]

Priority * 200

Description This policy monitors the execution of all applications. Not recommend on more than a handful of machines.

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
[Filters](#)

Applications Targeted Add Applications Targeted

Inclusions Add Inclusions

Exclusions Present in Signed Security Catalog Edit

6. Click **Save Changes**.

After setting up your first policies, keep in mind that even after you enable them, new policies are not immediately sent to target endpoints. Instead, policies are updated on endpoints via the schedule defined by the Update Applicable Policies task. By default this task runs once daily.

1. Search for the *Update Applicable Policies* task:

NAME	TYPE	MODIFIED	DESCRIPTION
Update Applicable Policies	Remote Client Task	6/16/20, 7:11 AM	
Update Applicable Policies	Agent Executed Powershell Command	6/16/20, 7:11 AM	Requests applicable policies from the Privilege Manager ...
Update Applicable Policies - Internet Clients (Windows)	Remote Scheduled Client Command	6/16/20, 7:12 AM	Instructs Agent to check with server for policy changes le...
Update Applicable Policies (Mac OS)	Remote Scheduled Client Command	6/16/20, 7:12 AM	When this policy is triggered the Agent will check the ser...
Update Applicable Policies (Windows)	Remote Scheduled Client Command	6/16/20, 7:12 AM	Instructs Agent to check with server for policy changes.

2. Select the **Update Applicable Policies (Windows)** for example.
3. To edit the time scheduled that sets off this task, under Job schedule click **Add Trigger**.

Update Applicable Policies (Windows)

This item is read-only.

Details Change History Active Duplicate More

Description Instructs Agent to check with server for policy changes.

Computer Groups Targeted 1 (1 total endpoints)
Windows Computers - Internal Network (Target)

Deployment 0% (1 endpoints, 0 with the latest version)

Job Settings

Command Update Applicable Policies

No parameters

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run. Default: Daily at 12:00:00 AM starting Mon Oct 01 2018 (repeating every 30 minutes for a duration of 24 hours)
Add Trigger

1. Select to run this schedule **Once** on demand and make sure the time indicated is in the future. Clicking **Show Advanced** give you more options for the modification.

Update Schedule

Begin On a schedule

Once Daily Weekly Monthly

Starting 6/17/2020 12:05 PM UTC

Hide Advanced

Delay task for up to (random delay) 0 second(s)

Repeat every 0 minute(s) for a duration of 0 minute(s)

Expire month/day/year

Cancel Save

In production environments having a delayed deployment schedule prevents performance issues when adjusting policies and rolling them out across a large number of agents on your network. However, when setting up new policies you may want to immediately activate them on testing endpoints and verify your configurations are working correctly.

4. Click **Save**. The data under **Job Schedule** indicates to run once.

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run. Once at 12:05:00 PM (UTC) starting Wed Jun 17 2020
Add Trigger

5. Click **Save Changes** for the modification to take effect.

View Deployment Status

Within a Policy's Detail View, verify the deployment status. This will tell you how many computers the policy is already deployed on:

The screenshot shows the 'Policy Details' page for 'iTune - Deny installation'. The policy is active and has a deployment status of 100% (1 endpoint, 1 with the latest version). The targeted computer group is 'Windows Computers'. The last modified date is May 15, 2020, 2:38:02 PM by Principal Self Well Known Group. The priority is set to 3.

Property	Value
Computer Groups Targeted	1 (1 total endpoints) Windows Computers x
Deployment	100% (1 endpoints, 1 with the latest version)
Last Modified	May 15, 2020, 2:38:02 PM by Principal Self Well Known Group
Priority *	3

Note: If the deployment status number is 0 or incorrect, it is possible that the *Resource and Collection Targeting Update* task needs to run.

Update Policies on an Endpoint using Powershell (prior version 10.7)

On Privilege Manager version prior to 10.7, the fastest way to deploy or update your policies on a specific testing endpoint is by running a simple Powershell script directly on your test machine where a Thycotic Agent is installed.

1. On your endpoint machine, right-click on the Windows Powershell application and select Run as Administrator.
2. Navigate to the Agent directory by entering the following command and then enter:
`cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"`
3. Next type
`UpdateClientItems.ps1`
4. Hit enter.

Note: If your policies are not immediately updated, wait a few minutes and try running the script again.

After you've updated your test endpoints, you can try running applications that are targeted by your policies to make sure the policies are configured correctly. You will also see the policy's Deployment status information updated if refreshed.

Agent Event Log Viewer

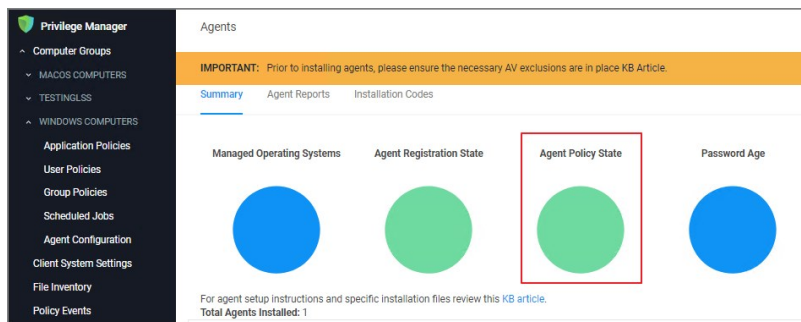
Another helpful place to look when setting up new policies is your Agent's Event Log Viewer. On your endpoint machine,

1. Navigate to your Thycotic Agent files. This is usually located in C:\Program Files\Thycotic\Powershell\Arellia.Agent.
2. Right-click on **AgentLogViewer** and select the Log Viewer button. This opens your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server. For remote access, Agent logs are also viewable through the Windows Event Viewer.
3. Scroll all the way to the top of the page to see the most recent activity from your Thycotic Agent.
4. Deselect the Information box on the upper right-hand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.

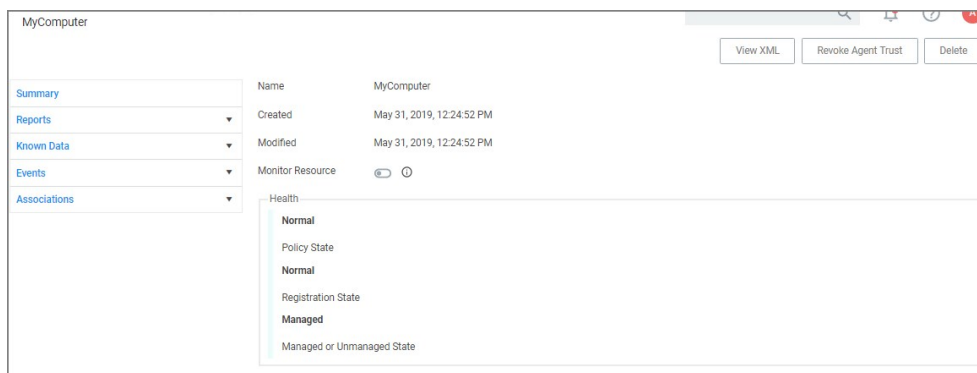
Now that you know how to update your endpoints and check to make sure your policies are working, it's time to start building new policies!

These are the steps for verifying which policies were received by an agent:

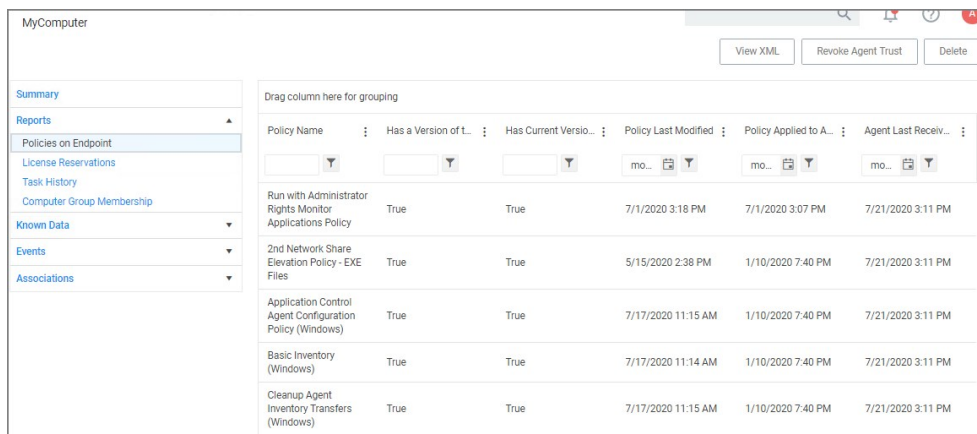
1. Navigate to **Admin | Agents** and click on **Agent Policy State**.



2. On the **Agent Policy State - Drilldown** page select the computer, whose policy state you wish to examine.
3. This opens the Resource Explorer for the selected endpoint.



4. Open the **Reports** section and select **Policies on Endpoint**.



View the policies that the agent on the endpoint has received. The Filter on the **Policy Name** column allows you to search for specific policies.

The column details are:

- **Has a Version of the Policy** and **Has Current Version of the Policy** provide information about the version of the policy.
- **Policy Last Modified** informs when a policy was last changed.
- **Policy Applied to Agent** specifies when the policy was first received by the agent.
- **Agent Last Received Policies** informs when the agent last contacted the server to request updates.

Various Privilege Manager policies and filters use Regular Expressions (RegEx) to specify application or file names to match against.

For Privilege Manager all RegEx strings need to be in lowercase. A good resource for testing RegEx is <https://regexr.com>

Special RegEx Characters

The following characters have special meaning in RegEx, and should be used with an escape character when there is a need to represent a literal character.

To perform the escape a \ (backslash) needs to precede the following characters: + * ? ^ \$. [] { } () \ | /

A Privilege Manager Win32 file filters path name does not use the ending directory slash \. RegEx for path names should also not include the ending \.

Escape Example

For the literal (x86)\.netC++ the RegEx is \\\(x86)\\.netC++.

Wildcard Example

In RegEx: . * is a wildcard

File Name Examples

Match with Wildcard before the File Name

Matching anything before the file name and ending with a file type, use a wildcard before the file name.

File Name=""eetechcode.exe" use this in Privilege Manager (*.eetechcode\exe\$)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match File Name Containing String and File Type

To match a filename that contains a character string on both sides of the actual file name and that must end with a specific file type:

File Name=""eetechcode*.exe" use this in Privilege Manager (*.eetechcode.*\exe\$)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match with Wildcard at end of File Name and before File Type

Matching a file name with a string that contains anything between the string and the file type.

File Name=""eetechcode*.exe" use this in Privilege Manager (^eetechcode.*\exe\$) this is a

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard in the Middle of Two Strings

Matching a file name beginning with a string, followed by a wildcard and another string with the last string that includes the file type at the end.

File Name=""eetech*code.exe" use this in Privilege Manager (^eetech.*code\exe\$)

Results:

- Match eetechcode.exe
- Match eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard at End of File Type

Matching a file name with the wildcard at the end of the file name after the file type, when the filename begins with a string that includes the file type and matches anything after the file type.

File Name=""eetechcode.exe*" use this (*.eetechcode\exe.*)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

File Path Examples

Wildcard at the End of the Path

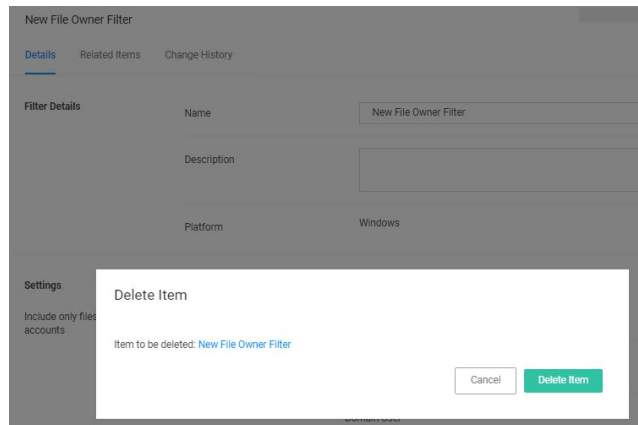
To match when a wildcard is at the end of the File Path like:

When deleting items there might be dependencies, like a filter is used in a policy. If that filter is then deleted without modifying or also deleting the policy, the policy will stop working without anyone realizing that the filter has been deleted.

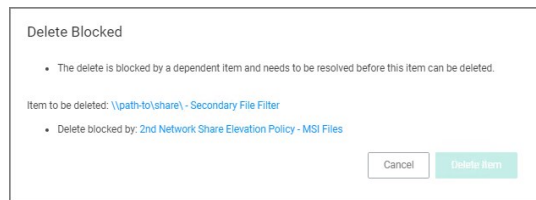
Privilege Manager detects dependencies when items are deleted and alerts the user to

- any dependent items, which block the deletion.
- any child items, which will also be deleted.

When a the **Delete** button is clicked on a filter, in this example the filter is called **allow notepad++ any version secondary file filter** and no dependencies are detected, a **Delete Item** modal opens. The user can proceed by clicking the **Delete Item** button.

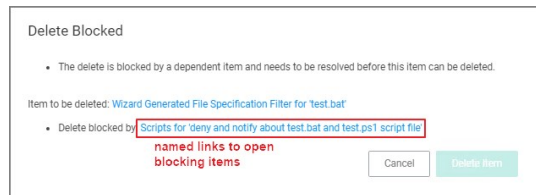


If that filter is part of a policy and the **Delete** button is clicked, the **Item Dependency: Delete Blocked** modal opens.



From the modal the user can see that the delete is blocked by a dependent item. A tool tip is shown when hovering the mouse pointer over the icons.

The trash can icon informs about which item was selected to be deleted. The blocked icon informs which items are blocking the deletion.



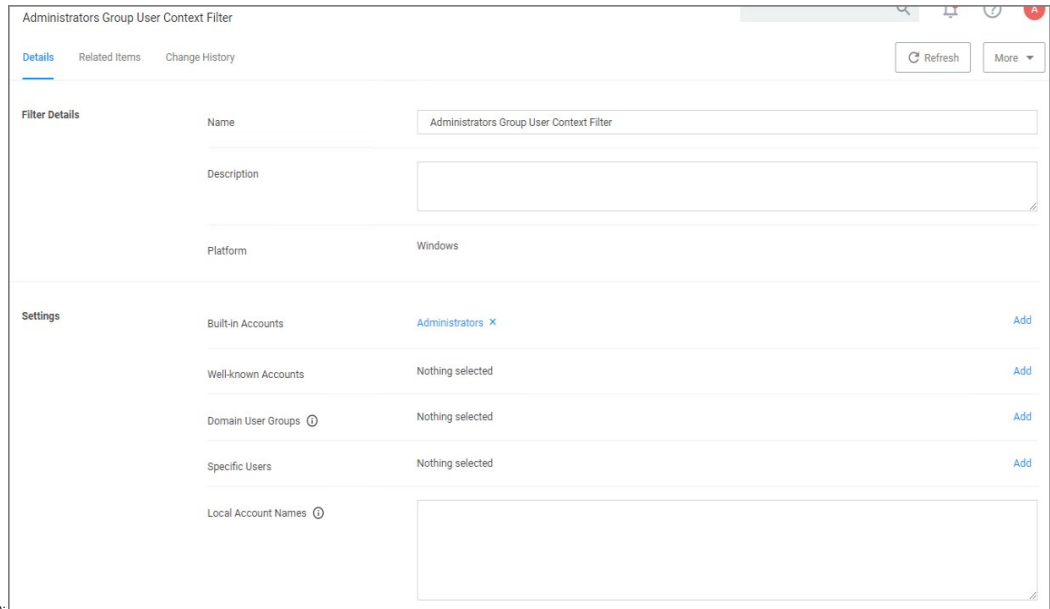
While there are blocking items, the **Delete Item** or **Delete Item and Children** buttons are disabled. The delete button is dynamic and will only display **Delete Item and Children** if both of those are dependencies, otherwise it will only display **Delete Item**.

Blocking dependent items can be accessed and deleted by clicking on the named item link. This opens the dependent item in another browser tab, where it can be viewed and deleted.

If you wish to exclude certain users via filter from an application policy, follow these general guidelines.

Targeting Administrators with the Exclusion

To target the Administrators group, you need to use a User Context filter and select under **Built-in Accounts** options the **Administrators**. The out of the box **Administrators (Include Disabled)** filter (item f9569529-62d4-49ba-aa21-b9362e1f4de6) accomplishes the same. The include disabled text just means the user is a member of the group, but the process may or may not be elevated.

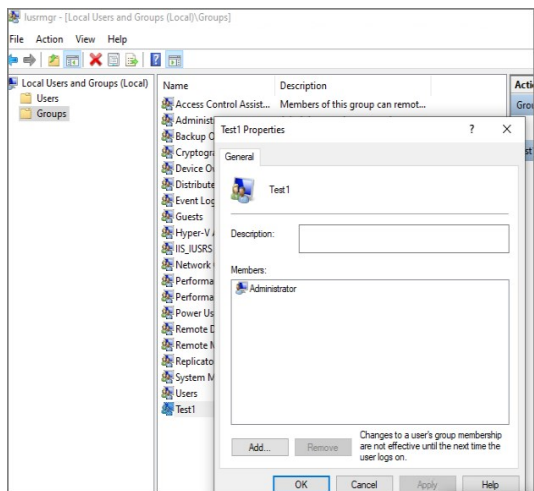


Screenshot of a working filter for the Administrators Group:

Targeting new Local Groups (not built-in)

The Local Group Names option can be used to target new local groups. New local groups are user groups that are not considered built-in system or out of the box Windows groups, such as Users, Administrators, Power Users, Backup Users, etc.

For example, create a new local group on a local computer and call the group "Test1". Then add a user to it that you wish to exclude.



If you then configure a filter like the following the policy should correctly exclude users in the group.

Test1 Group User Context Filter

Details Related Items Change History Refresh More

Filter Details

Name: Test1 Group User Context Filter

Description: [Empty text area]

Platform: Windows

Settings

Built-in Accounts	Nothing selected	Add
Well-known Accounts	Nothing selected	Add
Domain User Groups ⓘ	Nothing selected	Add
Specific Users	Nothing selected	Add
Local Account Names ⓘ	[Empty text area]	
Local Group Names ⓘ	Test1	

Policies

In Application Control, layered Policies create the backbone or parameters, that dictate precisely how privileges are accessed across your network. They define what a user can run, and where. A policy is made up of customizable filters that apply an action to specific Computer Groups. In other words, each policy is defined by:

- Filters - What criteria needs to be met to apply this policy?
- Targets - Where should this policy be applied?
- Actions - What should happen to the applications this policy applies to? (i.e. blocked, allowed, etc.)

During the creation of a Policy you will specify Actions and Targets, but Filters are created separately and then assigned to Policies.

The **Privilege Manager Policy Wizard**, guides users through the policy creation process, with step-by-step decision making guidance.

Using Policy Templates

Privilege Manager ships with most commonly used policy templates. These are utilized by the policy wizard when creating a new policy.

Thycotic also provides templates that do not ship with the product, but that can be downloaded via **Config Feeds** from within the Privilege Manager Console. Once downloaded and installed, customers can access those policy templates via **Admin I Folders**. Here a new policy can be created based on a template from a drop-down list. This policy will have associated targets, filters, and actions set, which can be further customized to cover an organization's specific needs. Also refer to [Configuration Feeds](#).

Overview of the Configuration Process

While there are many different types of policies, the setup process must follow these basic steps:

1. Collect File Data - This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed under **File Inventory**.
2. Create Filters - This step sorts important file data (Events) according to different criteria.
3. Create Policies - This step defines what
 1. Actions to perform on applications and the
 2. Targets (Locations) for those actions.
4. Assign Filters to Policies - This step directs a Policy's actions to the appropriate Events happening on your network.
5. Order your Policies based on priority level - Once your policies are created, the order they execute across your network matters. See the Policy Priority section in this guide for more details.

Collecting File Data

Before Privilege Manager can do anything else for Application Control, it must be able to recognize files or file types in your environment like applications or executables that run. File data can be collected in several ways:

- Event Discovery - Discover active applications on your network by setting up Learning Mode Policies
- File Upload - Directly upload a specific file that you want to target
- Remote File Inventory Task (Windows/macOS) - Scans endpoints directly and imports all file data (both active and inactive files) that exist on the targeted machine(s).

Points to Consider

If you configure Privilege Manager policies incorrectly they could prevent services or programs from starting or running with the proper rights.

Policies are evaluated in order based on the Policy Priority value on the Policy. If a blocking policy that denies applications is too broad and is set with too high a priority, it can unintentionally prevent other applications from running or letting the user request approval to run.

You can avoid conflicts resulting from incorrectly configured Privilege Manager policies by using the following best practices:

- Always test policies on machines which mirror the production environment before rolling out to production.
- Assign policies that allow processes a lower policy priority number than policies that deny processes.
- Make sure your other policy enforcement settings check boxes are selected or cleared, depending on the aims of your policy.
- Policies that deny processes always exclude the following application filters:
 - LocalSystem and Service
 - Signed Security Catalog
- You should (almost) never use wildcards in deny policies. Wildcards should be considered only after performing extensive testing.

Policy Enforcement

Each policy has advanced settings to address any non default Policy Enforcement options. Some of those pertain to parent-child processes and how policies are processed when they are supposed to work together in such parent-child or stage 2 processing scenarios.

Policy Enforcement		
Continue Enforcing Policies	<input type="checkbox"/>	Once an application meets the criteria of this policy, subsequent policies will not be evaluated.
Continue Enforcing Policies for Child Processes ⓪	<input checked="" type="checkbox"/>	Subsequent policies will be evaluated for child processes.
Stage 2 Processing	<input type="checkbox"/>	This policy will be applied before policies are evaluated for child processes.
Applies To All Processes	<input type="checkbox"/>	Policy will only apply to interactive users.
Skip Policy Analysis at Start-up	<input type="checkbox"/>	Pause policy analysis during boot-up (use only on filter heavy policies)

Continue Enforcing

After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.

This setting has to be active for **Stage 2 Processing** to work as intended.

Continue Enforcing Policies for Child Processes

Include child processes in the policy enforcement, meaning subsequent policies will be evaluated.

In certain situations this needs to be disabled, if for example you want to allow and application if it is launched by a specific process, but deny it if it's executed directly. Refer to the **Stage 2 Processing** description.

Stage 2 Processing

Policies are initially evaluated for the primary process. If no matches are found, policies are evaluated for a parent of that process. If active, the policy is applied before policies are evaluated for child processes.

For example, if you want to allow regedit.exe when launched by cmd.exe but block it if launched directly, you need to create

1. a policy to target and allow cmd.exe with an inactive "Enforce Child Processes" and
2. a policy that targets regedit.exe with a deny action and "Stage 2 processing" enabled.

The priority on the policy that targets regedit.exe directly needs to be higher than the priority on the allow cmd.exe policy.

Applies to All Processes

Policy will apply to system based processes. If this setting is not active, the policy will only apply to interactive users.

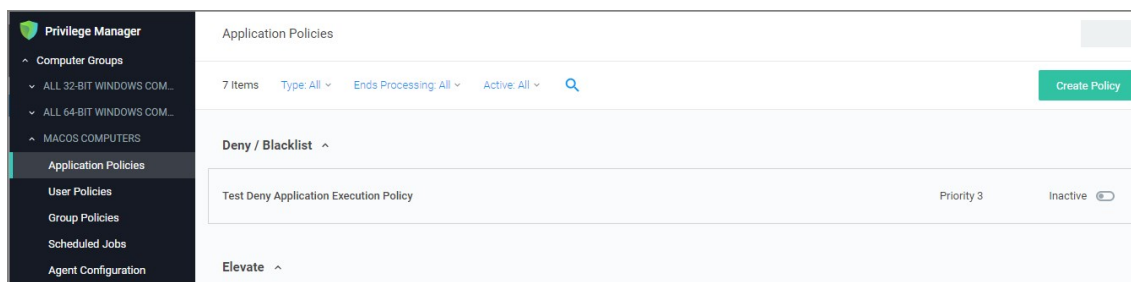
Skip Policy Analysis at Start-up

This setting can be used to pause policy analysis during boot-up, refer to [Increase Boot-up Performance](#) for details.

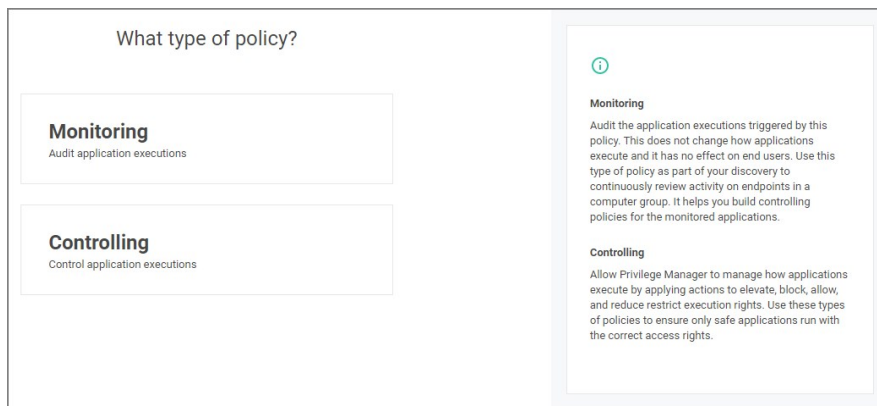
Using the Policy Wizard

Privilege Manager 10.8 is introducing the Policy Wizard for an easy and guided creation of new policies.

1. For any of your Computer Groups navigate to **Application Policies**.



2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points references per OS:

- o [Monitoring Policy Diagram](#)
- o macOS:
 - [Controlling Allow Diagram](#)
 - [Controlling Block Diagram](#)
 - [Controlling Elevate Diagram](#)
- o Windows
 - [Controlling Allow Diagram](#)
 - [Controlling Block Diagram](#)
 - [Controlling Elevate Diagram](#)
 - [Controlling Restrict Diagram](#)

3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

Using a Blank Policy

It is possible to create a new policy based on a blank template. On the first page of the Policy Wizard, you can find a link to **Skip the wizard** at the bottom of the page.



Click the link to open a blank policy and build the policy out manually.

[← Back to Application Policies](#)

Policies

Search [] Notifications [] Help [] Profile [A]

Name this policy

Name *

Description

Priority *

[Previous Step](#) [Create Policy](#)

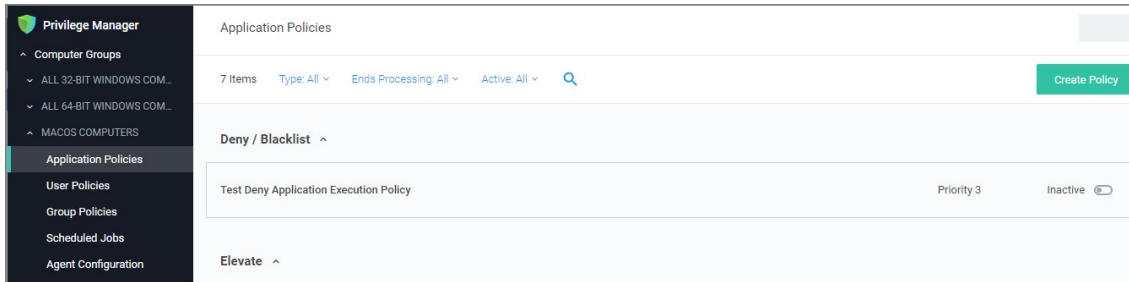
Name
Tips on how to name your policy

Description
Helper text

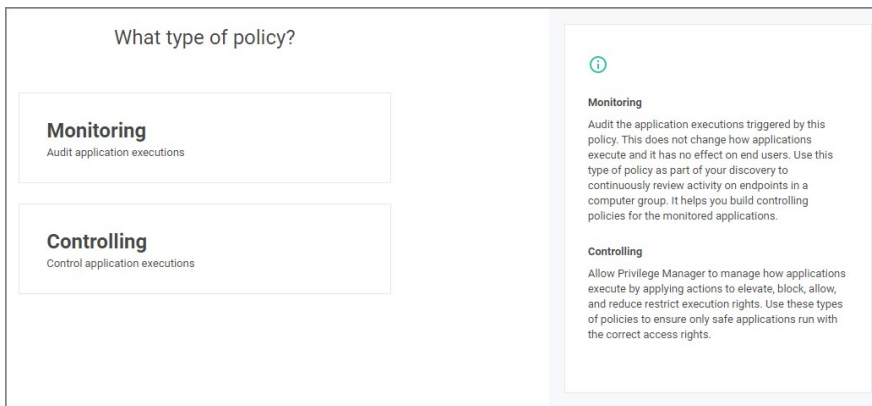
Priority
Helper text

Creating a Monitoring Policy

1. For any of your Computer Groups navigate to **Application Policies**.



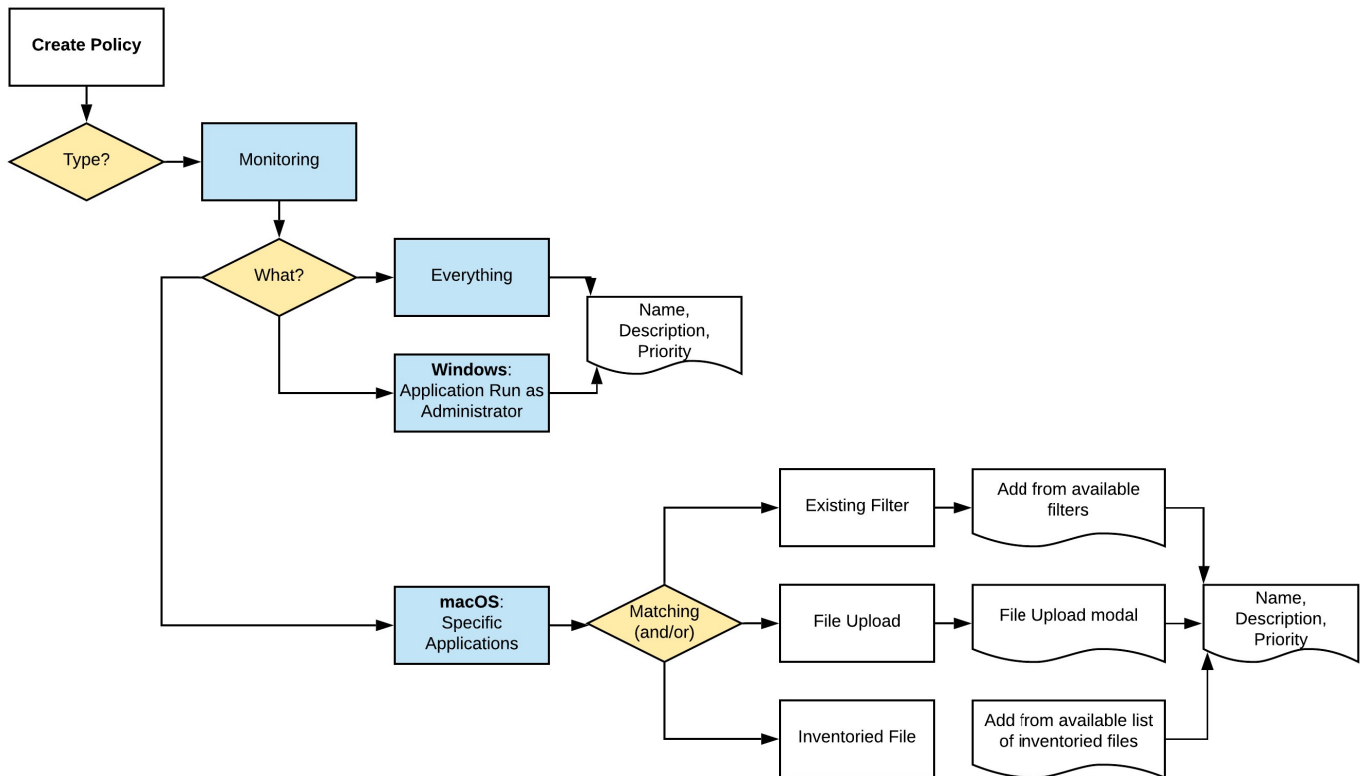
2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:

Monitoring Policies



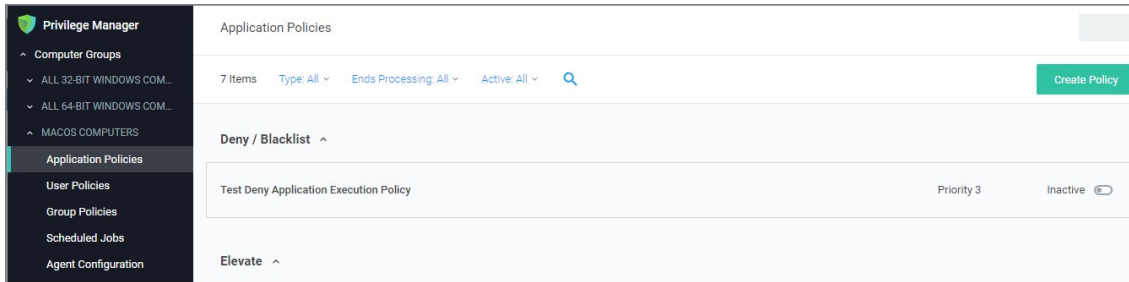
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

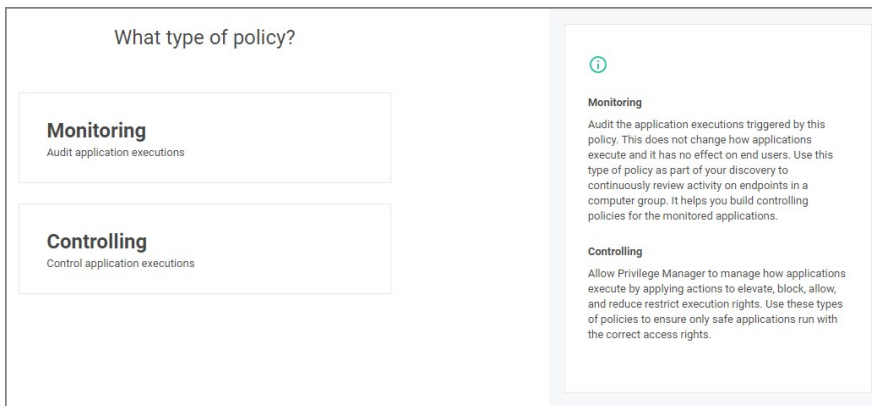
Creating a Controlling Allow Policy for macOS

1. For any of your Computer Groups navigate to **Application Policies**.



The screenshot shows the Privilege Manager interface. On the left is a dark sidebar with a navigation menu: Privilege Manager, Computer Groups, ALL 32-BIT WINDOWS COM..., ALL 64-BIT WINDOWS COM..., MACOS COMPUTERS, Application Policies (highlighted), User Policies, Group Policies, Scheduled Jobs, and Agent Configuration. The main content area is titled 'Application Policies' and shows 7 items. There are filters for Type, Ends Processing, and Active, and a search icon. A green 'Create Policy' button is in the top right. Below the filters, there is a 'Deny / Blacklist' section with a dropdown arrow. Underneath, a policy named 'Test Deny Application Execution Policy' is listed with 'Priority 3' and an 'Inactive' toggle switch. At the bottom, there is an 'Elevate' dropdown arrow.

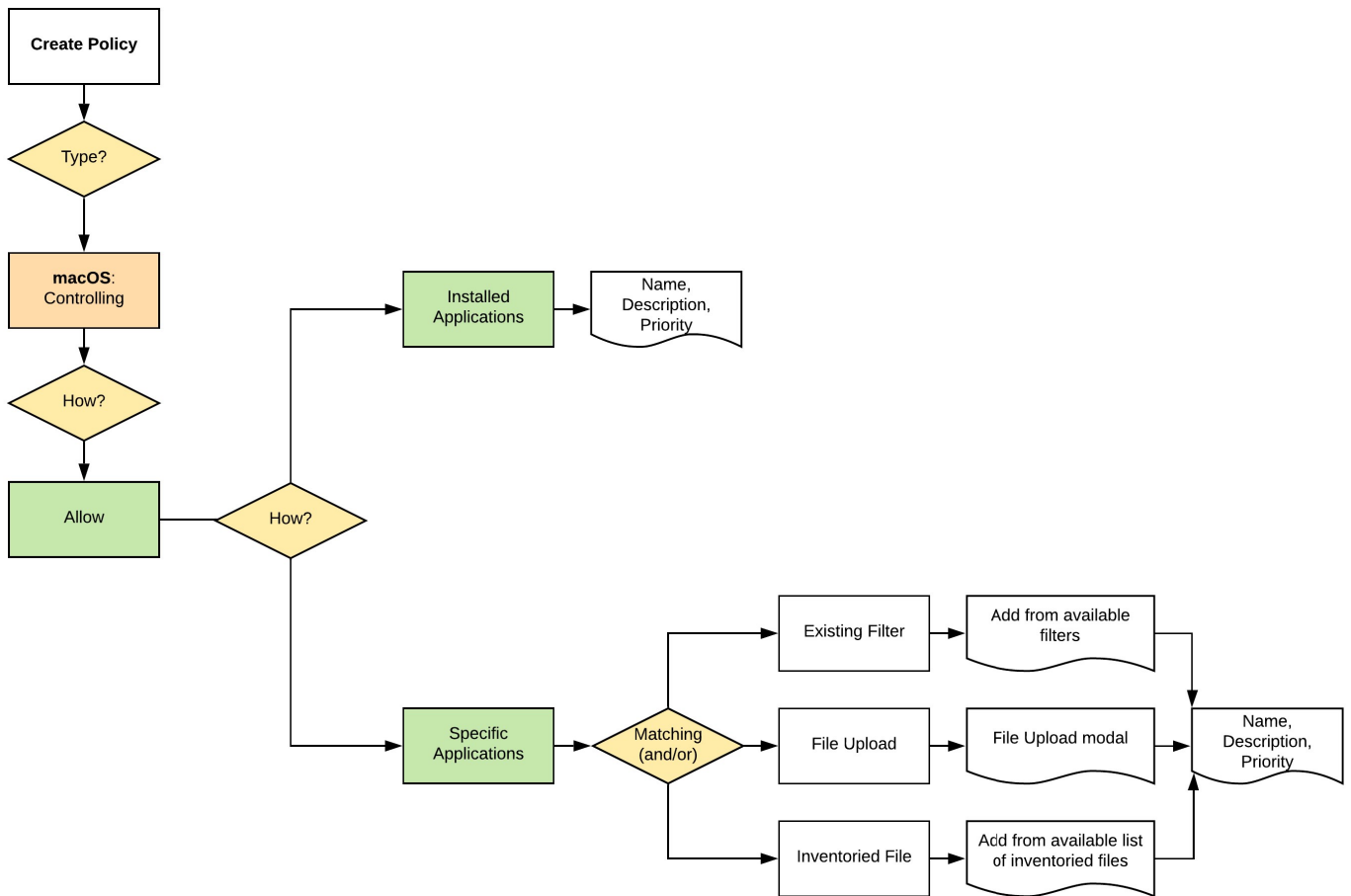
2. Click **Create Policy**.



The screenshot shows a wizard screen titled 'What type of policy?'. On the left, there are two selection boxes: 'Monitoring' (Audit application executions) and 'Controlling' (Control application executions). On the right, there is an information panel with an 'i' icon. It contains two sections: 'Monitoring' (Audit the application executions triggered by this policy. This does not change how applications execute and it has no effect on end users. Use this type of policy as part of your discovery to continuously review activity on endpoints in a computer group. It helps you build controlling policies for the monitored applications.) and 'Controlling' (Allow Privilege Manager to manage how applications execute by applying actions to elevate, block, allow, and reduce restrict execution rights. Use these types of policies to ensure only safe applications run with the correct access rights.)

Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



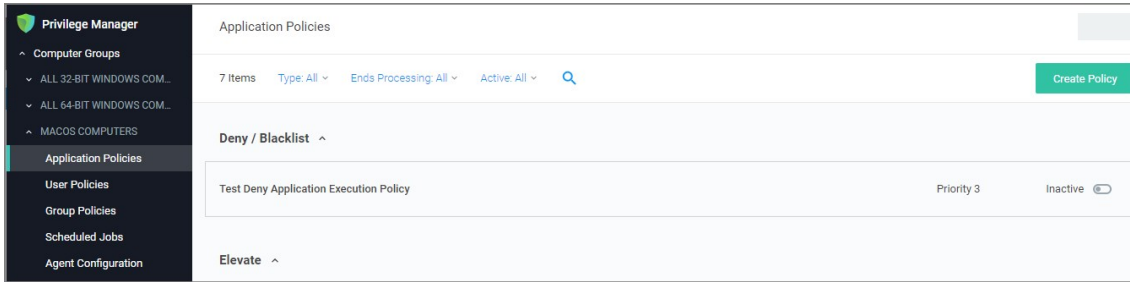
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

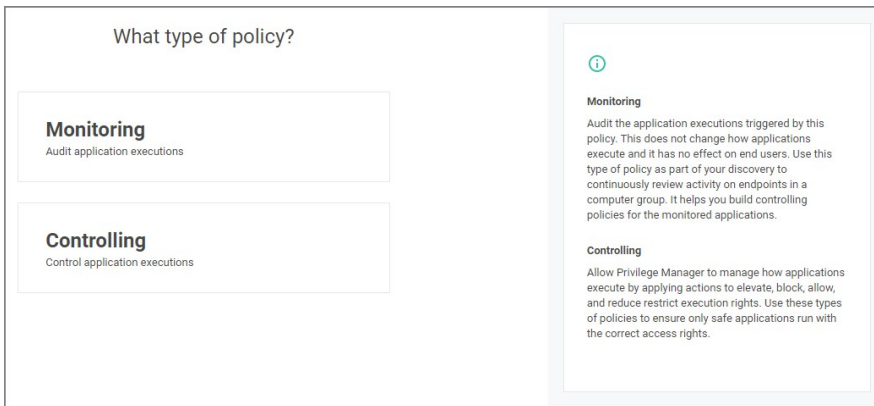
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Block Policy for macOS

1. For any of your Computer Groups navigate to **Application Policies**.

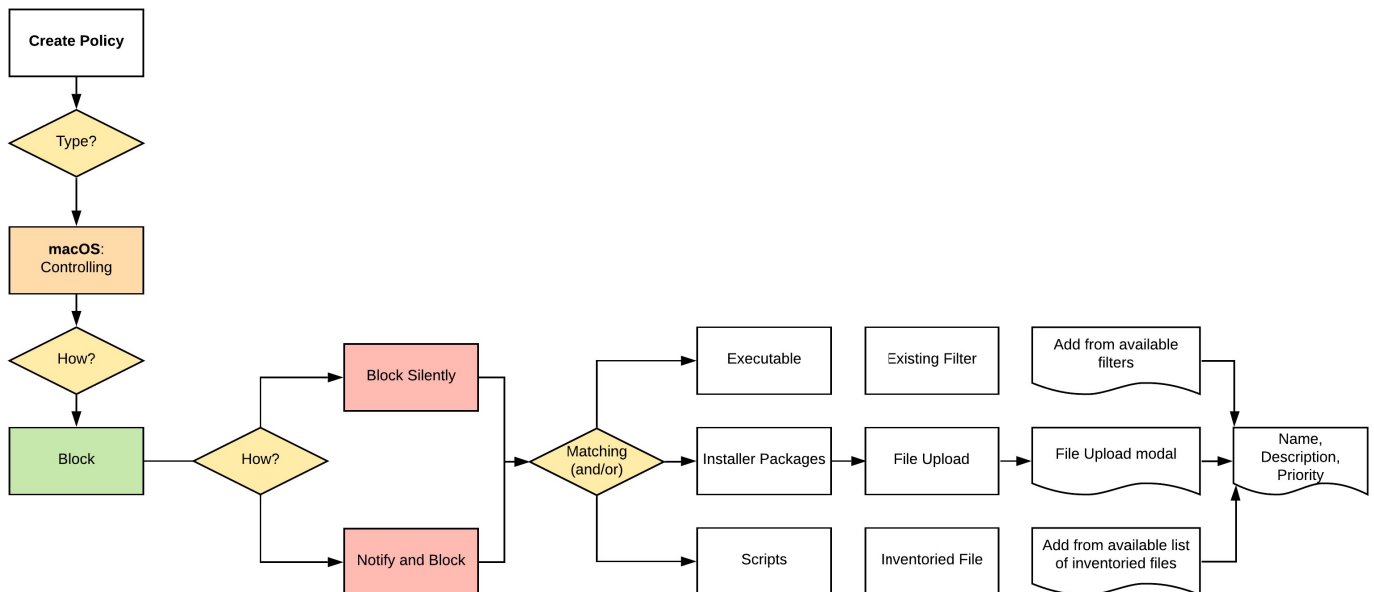


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



3. After assigning a name, description and verifying the priority number, click **Create Policy**.

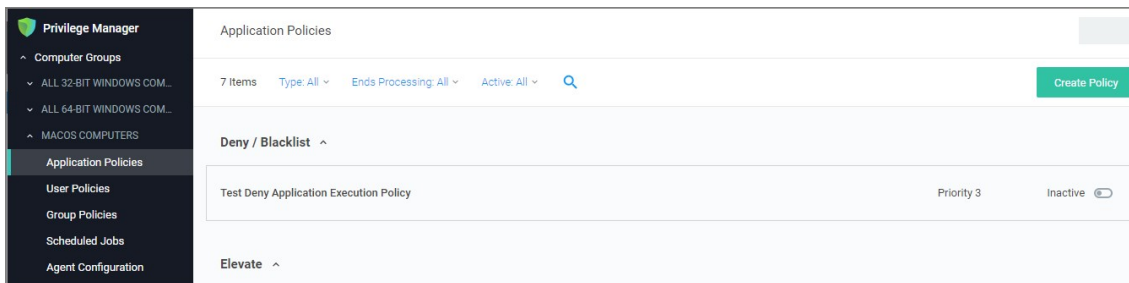
While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

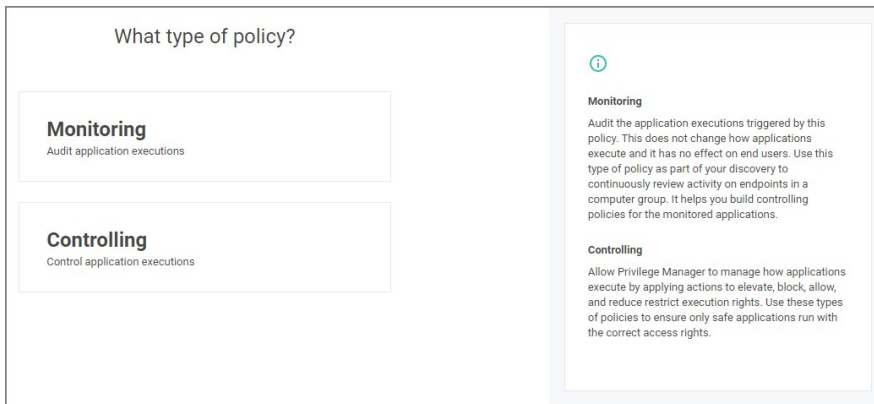
Creating a Controlling Elevation Policy for macOS

Note: The diagram shows actions "Run as Root" and "Just in Time" which will only work with the system extension based agent introduced with Privilege Manager 10.8.2.

1. For any of your Computer Groups navigate to **Application Policies**.

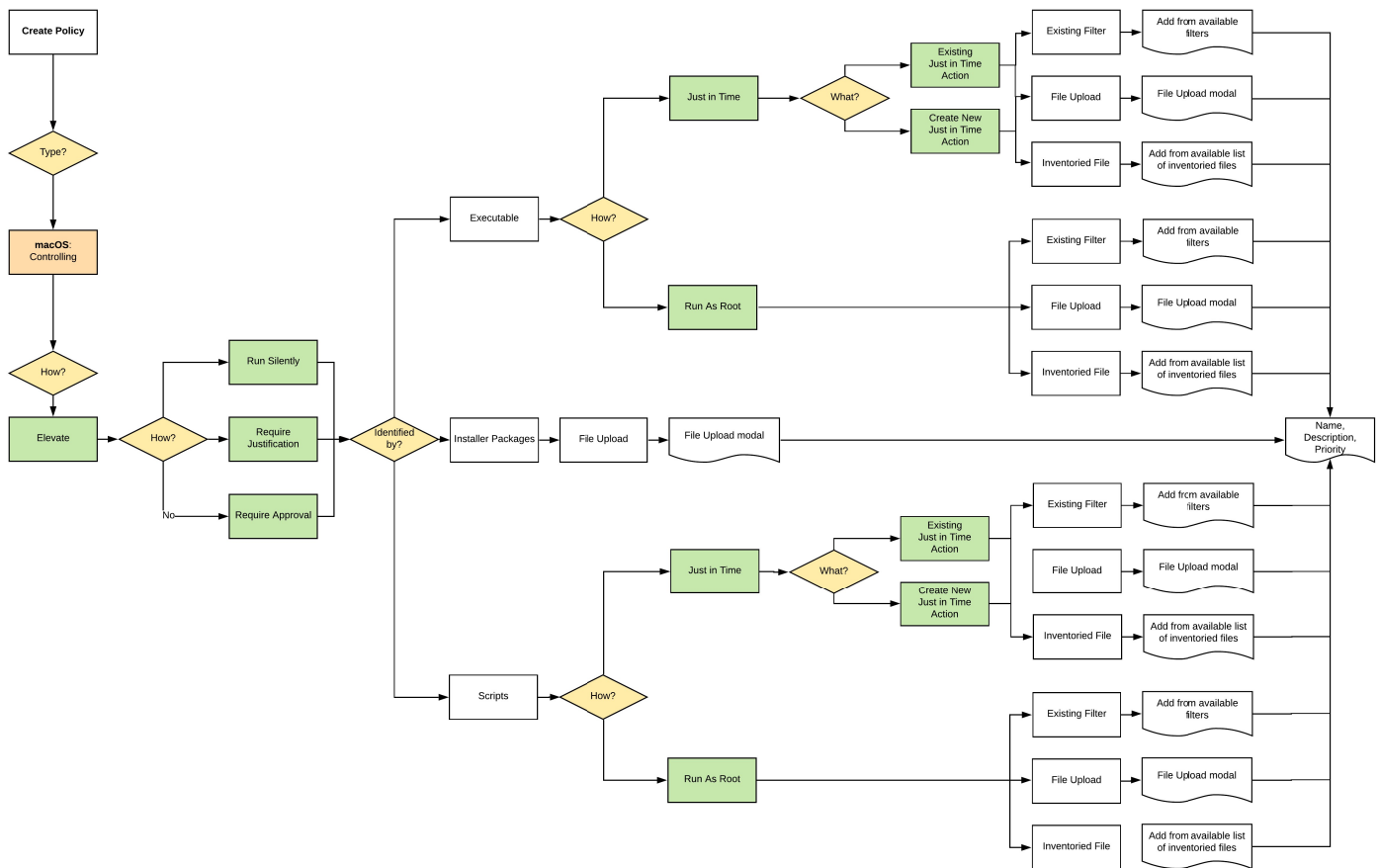


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Allow Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

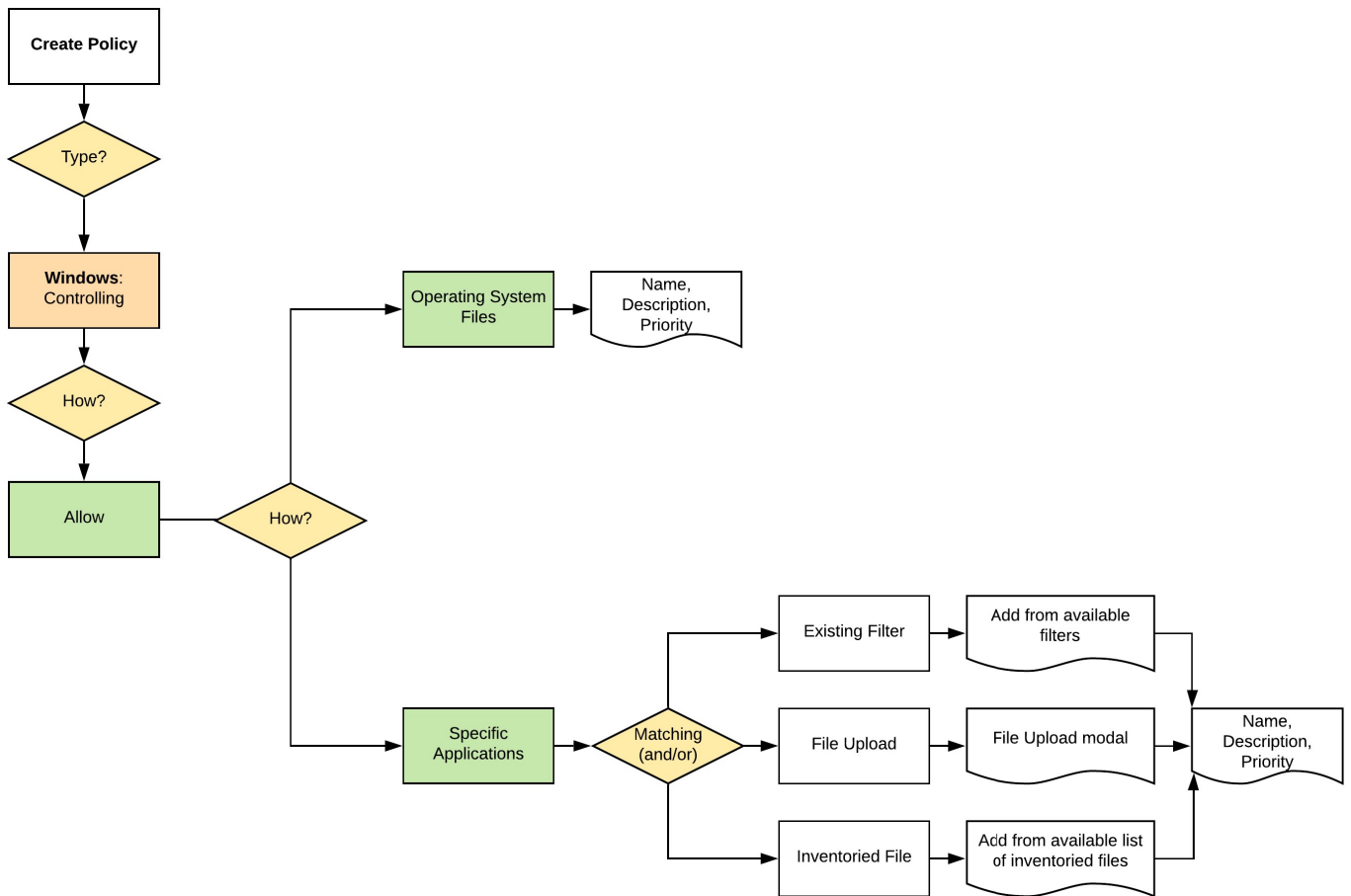
The screenshot shows the 'Privilege Manager' interface. On the left is a dark sidebar with a navigation menu: 'Privilege Manager', 'Computer Groups', 'ALL 32-BIT WINDOWS COM...', 'ALL 64-BIT WINDOWS COM...', 'MACOS COMPUTERS', 'Application Policies' (highlighted), 'User Policies', 'Group Policies', 'Scheduled Jobs', and 'Agent Configuration'. The main content area is titled 'Application Policies' and shows '7 Items'. There are filters for 'Type: All', 'Ends Processing: All', and 'Active: All', along with a search icon and a 'Create Policy' button. Below the filters, there are two expandable sections: 'Deny / Blacklist' and 'Elevate'. The 'Deny / Blacklist' section is currently expanded, showing a table with one row: 'Test Deny Application Execution Policy' with 'Priority 3' and an 'Inactive' toggle switch.

2. Click **Create Policy**.

The screenshot shows a wizard screen titled 'What type of policy?'. On the left, there are two selectable options: 'Monitoring' (Audit application executions) and 'Controlling' (Control application executions). On the right, there is an information panel with an 'i' icon. It contains two sections: 'Monitoring' and 'Controlling'. The 'Monitoring' section explains that it audits application executions but does not change how they execute. The 'Controlling' section explains that it allows Privilege Manager to manage application execution by applying actions like elevate, block, allow, and restrict.

Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



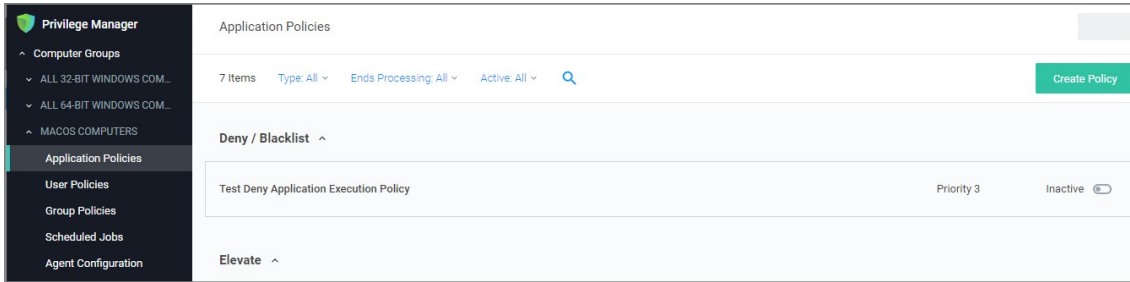
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

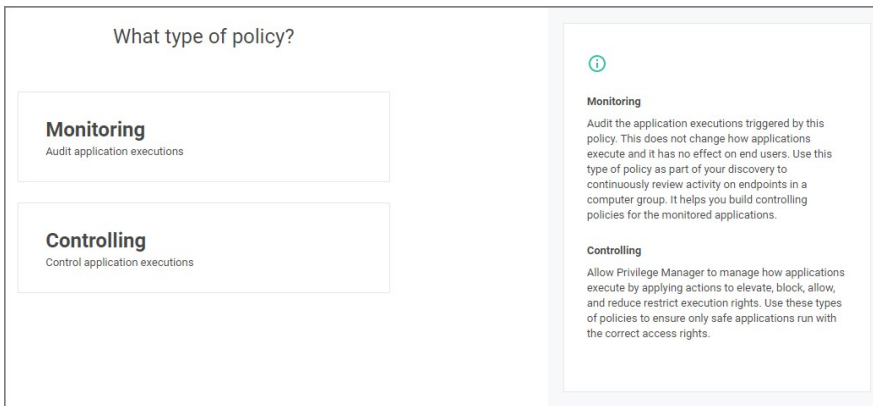
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Block Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

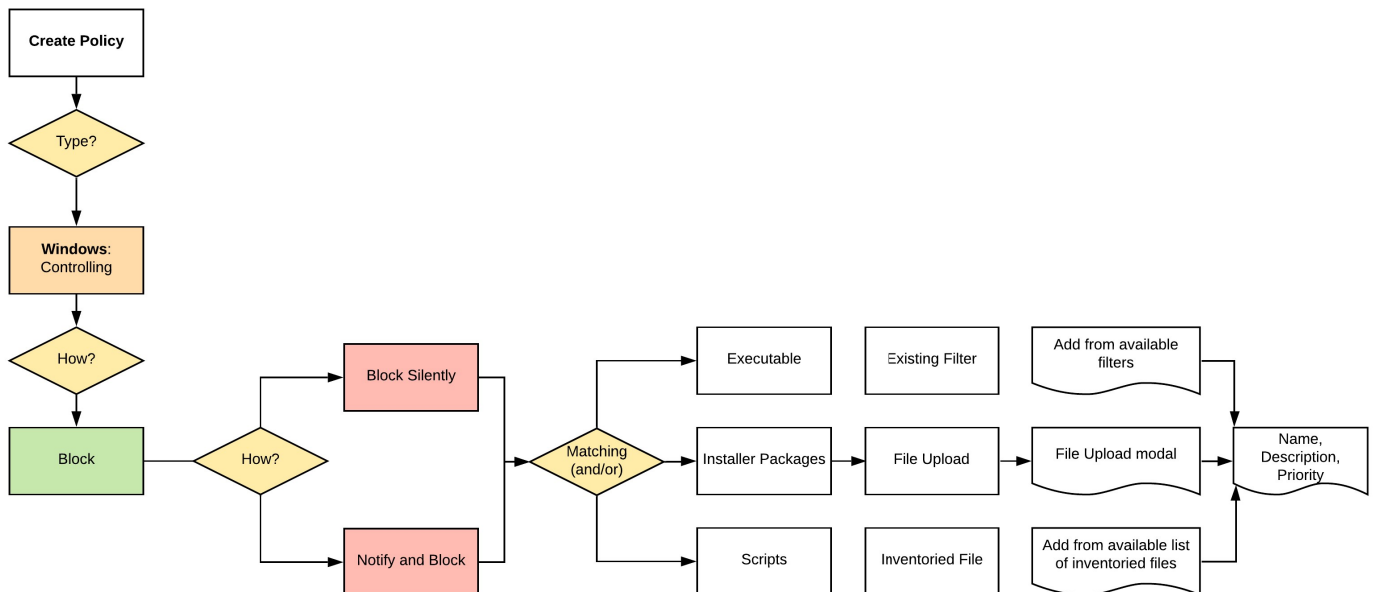


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



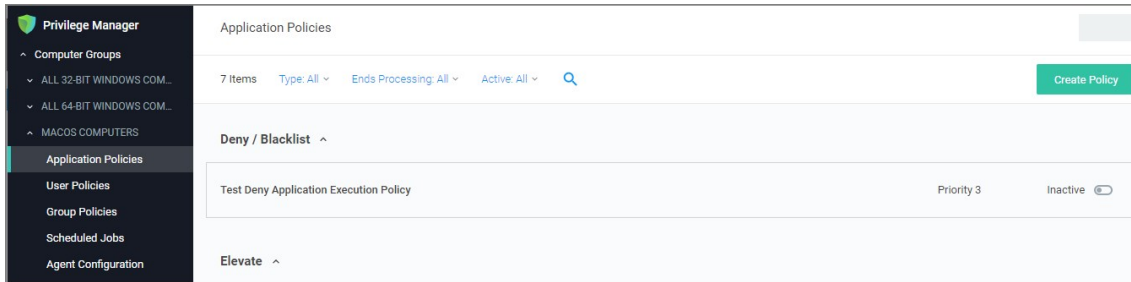
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

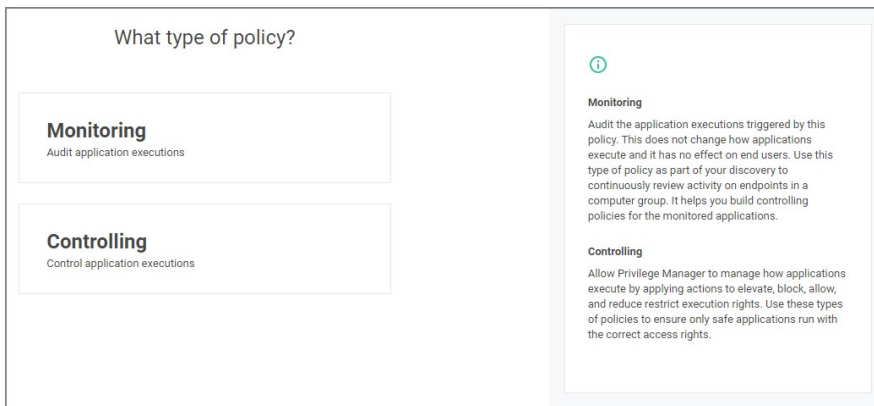
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Elevation Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

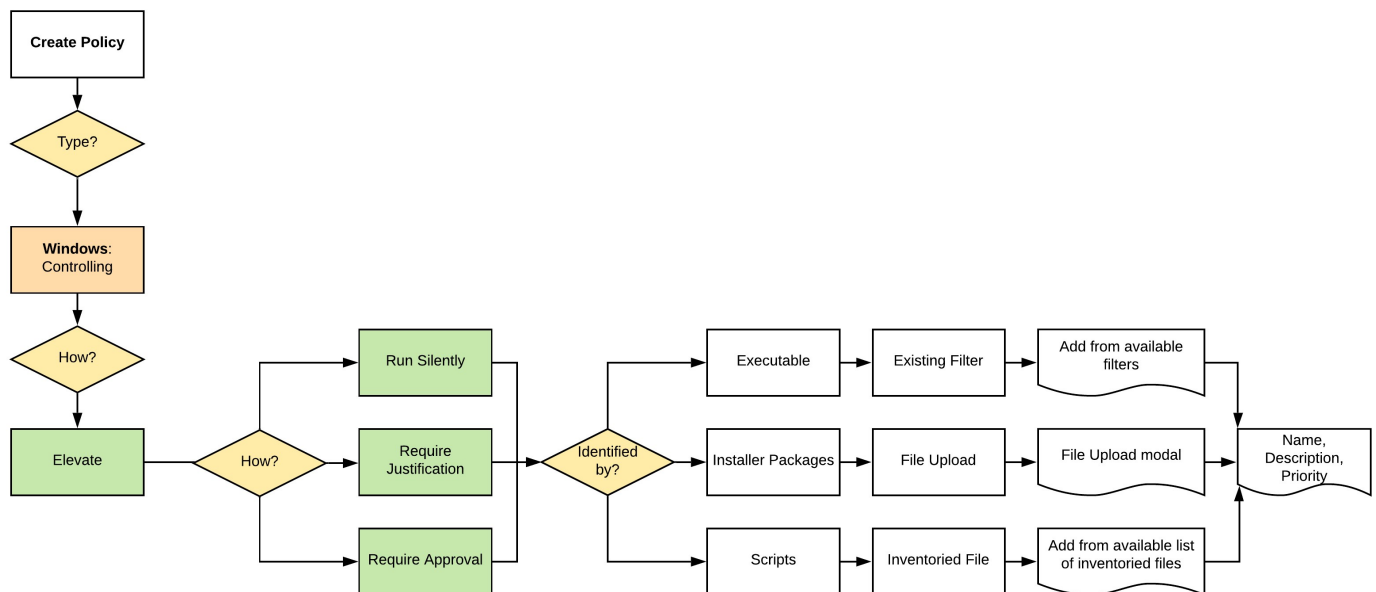


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



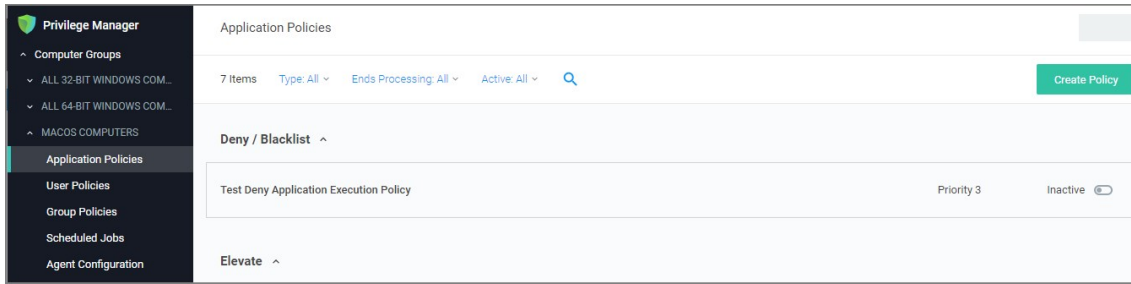
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

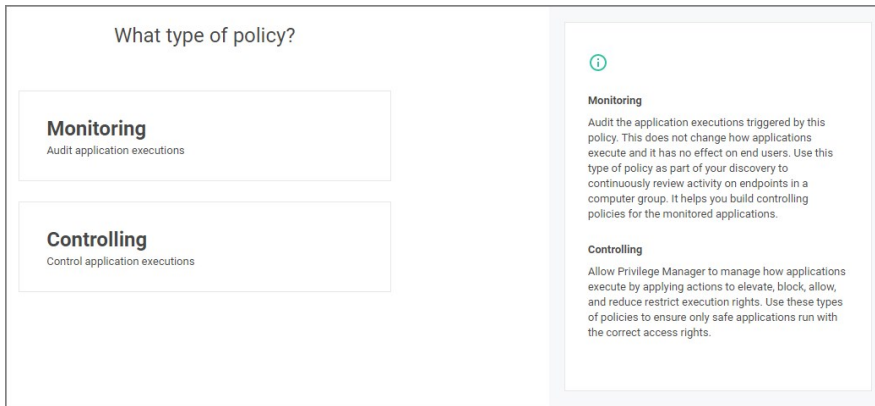
The wizard provides on page help explaining the different options available to the user.

Creating a Controlling Restrict Policy for Windows

1. For any of your Computer Groups navigate to **Application Policies**.

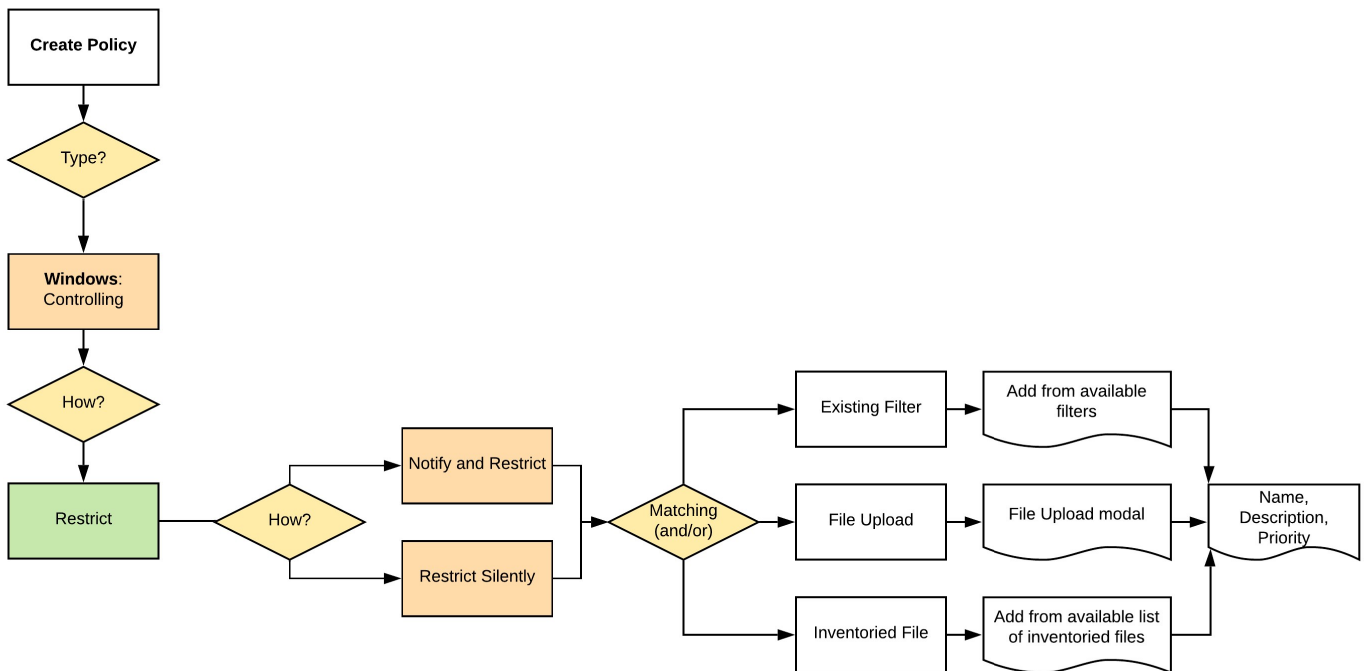


2. Click **Create Policy**.



Make your selection and click **Next** to get to the next wizard page.

For the steps through the wizard, follow these decision points:



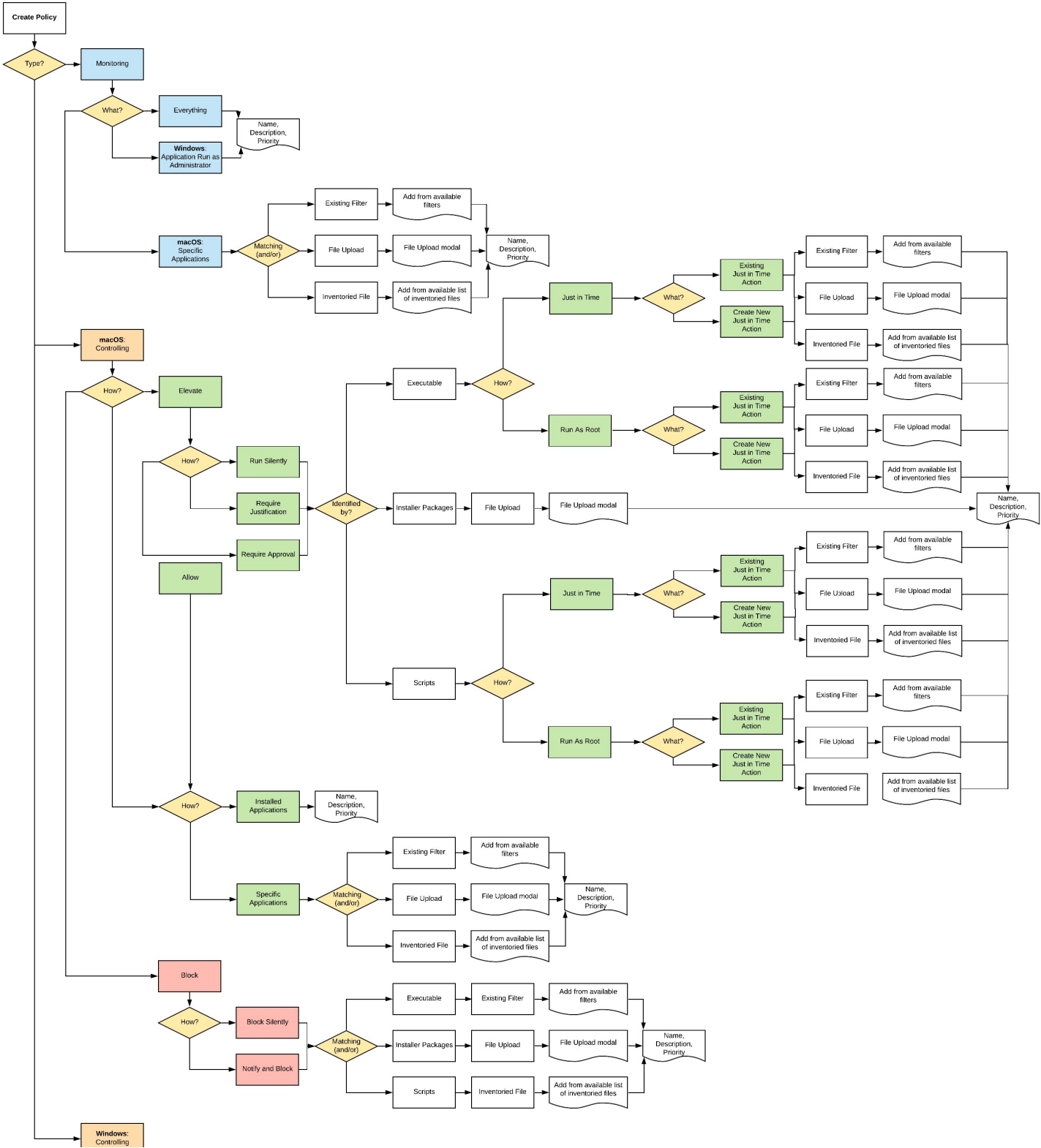
3. After assigning a name, description and verifying the priority number, click **Create Policy**.

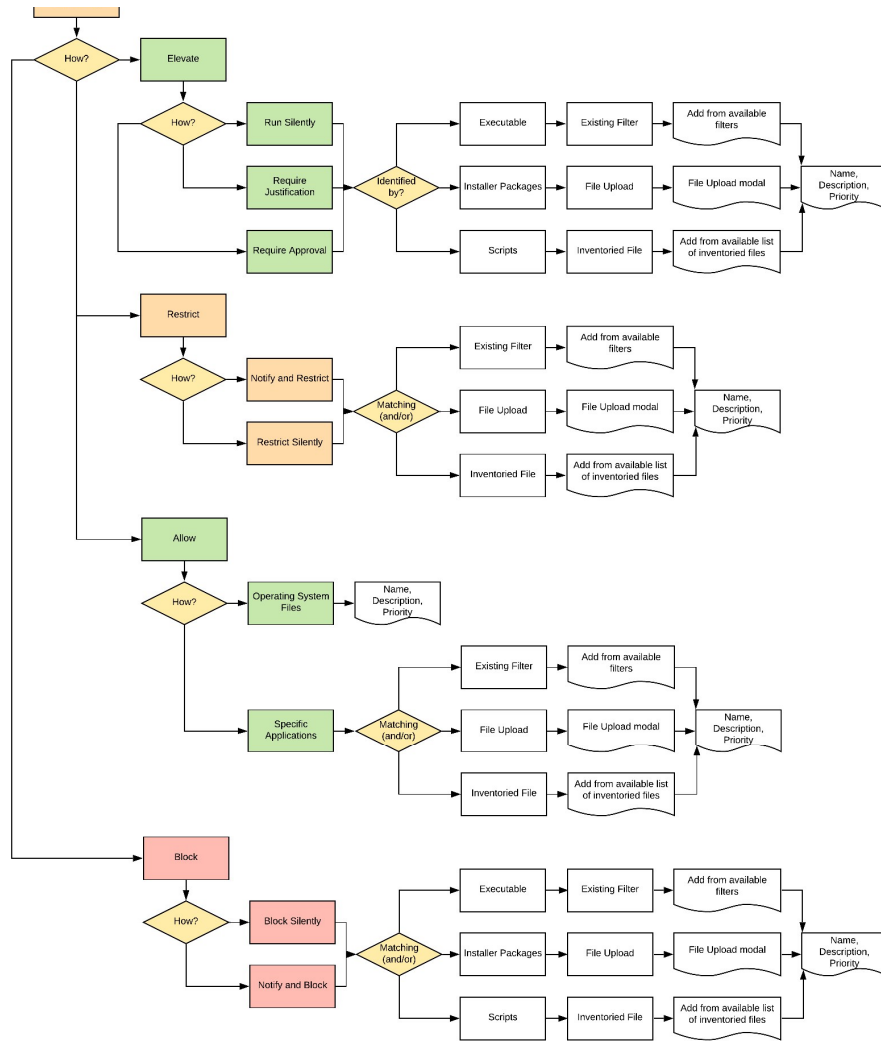
While in the wizard you can navigate back to previous pages via the **Previous Step** link to select another path. However, any **Previous Step** navigation clears selected options on accessed wizard pages.

The wizard provides on page help explaining the different options available to the user.

Full Policy Wizard Diagram

Note: The diagram shows macOS actions "Run as Root" and "Just in Time" which will only work with the system extension based agent introduced with Privilege Manager 10.8.2.





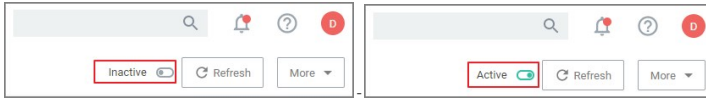
What's on the Policy Page

Once a policy is created, it can be customized. The following screen capture shows a policy example that denies the execution of a specific batch file.

□

Policy Activation

By default newly created policies are inactive and to activate them, the switch needs to be set to active.



Policy Details

The Policy Details section provided information about and customization options for:

- **Computer Groups Targeted** can be edited by either
 - deleting the current target by clicking the **x** next to the computer group name, or
 - adding another computer group by clicking **Add**
- **Deployment**, provides information about the deployment status at endpoints. Click the explanation point next to Deployment to run the **Resource and Collection Targeting Update Task**
- **Last Modified** provided a quick history on the last edit to the policy, time and by whom.
- **Priority**, modify the priority if needed, specific deny policies get lower priority values than monitor, allow, or elevate policies.

Conditions

Under Conditions edit the

- Applications Targeted,
- Inclusions, and
- Exclusions.

Actions

Under Actions edit which message action to use, if child actions are applicable, and if you wish to audit all activities this policy is detecting.

Show Advanced

Clicking **Show Advanced**, provides access to setting Policy Enforcement options, like:

- Continue Enforcing
- Applies to All Processes
- Enforce Child Processes
- Stage 2 Processing
- Skip Policy Analysis at Start-up.

Refer to [Policy Enforcement](#) for further details.

Priority

In Privilege Manager your Policies are evaluated in a certain order for each application that runs. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur.

The Policy Priority setting can be found on the Policies main screen in the left column. By default, policies are ordered according to their priority. You can edit this setting under the General tab after clicking into a policy.

Why Policy Priority Matters

To illustrate the way policies are applied in order, this use case will define two policies to

- block MMC.EXE, but
- allow a specific MMC Snap-in.

Deny MMC.EXE Policy setup

1. We will create a policy at with a default priority level of 10. This policy will block the execution of MMC.EXE.

Privilege Manager provides a filter to identify the executable mmc.exe. This can be used in this policy to block mmc.exe. Search for mmc.exe from the main screen search tool. Select the filter named Microsoft Management Console (mmc.exe). Review how the Filter is setup. Note that both File Name and File Path parameters are used.

2. Create the deny mmc.exe policy.

1. Under your **Computer Group** select **Application Policies**.
2. Click **Create Policy**.
3. Select **Controlling** and click **Next Step**.
4. Select **Block** and click **Next Step**.
5. Select **Block Silently** and click **Next Step**.
6. Select **Executables** and click **Next Step**.
7. Select **Existing Filter**.
8. Search for **mmc.exe**.
9. Next to **Microsoft Management Console (mmc.exe)** click Add.
10. Click **Update**.
11. Click **Next Step**.
12. Set the **Inactive** switch to **Active**.
13. Click **Add Exclusion** to set an exception filter to not have this policy apply to Administrators.
14. Search for the **Administrators (Include Disabled)** filter.
15. Click **Add**.
16. Click **Update**.
17. Click **Save Changes**.

The screenshot shows the configuration page for a policy named 'Deny mmc.exe'. The policy is currently 'Active'. The 'Policy Details' section includes:

- Computer Groups Targeted:** 1 (1 total endpoints) - Windows Computers
- Deployment:** 0% (1 endpoint, 0 with the latest version)
- Last Modified:** Jul 21, 2020, 3:49:44 PM by WIN-E6GKPM7J7TF\Administrator
- Priority:** 10
- Description:** This policy blocks the specified executables from running

The 'Conditions' section includes:

- Applications Targeted:** Microsoft Management Console (mmc.exe)
- Inclusions:** Add Inclusions
- Exclusions:** Administrators (Include Disabled)

The 'Actions' section includes:

- Actions:** Deny Execute, Deny Execute Message
- Child Actions:** Add Child Actions
- Audit Policy Events:** Record all activity detected by this policy in Policy Events

The policy will now be listed on the Application Policies page under the deny group. Once the policy is delivered to the endpoint agent, mmc.exe will be denied execution for all users without administrator credentials on all target computers. See details on how to deliver policies to the endpoint in the [Sending Policies to Endpoints](#) topic.

Once the policy is delivered to the endpoint, test running mmc.exe to see the results.

Allow specific MMC Snap-in

Next, we will create a policy that has a priority of less than 50 and it will allow specific MMC snap-ins. Having a priority less than 50 means this policy will be examined before the Deny MMC Console Application Control Policy.

1. As a short cut to this use case, start by duplicating the policy we just created, select **More | Duplicate**

- Name the new policy Allow Print Management Plug-in Application Control Policy.
- Click **Create**
- Set the **Policy Priority** value to 9. (This level is not required, only defined for this use case.) This means that this policy will be examined prior to the policy that blocks the mmc console. If the conditions are met, printmanagement.msc will run with elevation.
- Under **Conditions**, click **Add Inclusions** and search for the **printmanagement.msc Commandline Filter**.
- Click **Add**.
- Click **Update**. This filter will identify the mmc.exe file ONLY if the printmanagement.msc is run.
- Under **Actions**, click **Edit**
- Next to **Deny Execute** and **Deny Execute Message**, click **Remove**.
- Search for **Add Administrative Rights**, click **Add**.
- Click **Update**.
- Click **Save Changes**. You will now see your two policies in your Policies List. Once this policy is delivered to the endpoint agent, printmanagement.msc will be elevated with administrative rights.

The screenshot displays the configuration page for the policy 'Allow Print Management Plug-in Application Control Policy'. The policy is currently 'Inactive'. The configuration is divided into three main sections: Policy Details, Conditions, and Actions.

- Policy Details:**
 - Computer Groups Targeted:** 1 (1 total endpoints) Windows Computers x
 - Deployment:** Not deployed (Policy is inactive)
 - Last Modified:** Jul 21, 2020, 4:21:35 PM by WIN-E6GKPM7J7TF\Administrator
 - Priority *:** 10
 - Description:** This policy blocks the specified executables from running
- Conditions:**
 - Applications Targeted:** Microsoft Management Console (mmc.exe)
 - Inclusions:** printmanagement.msc Commandline Filter for MMC Snap-in
 - Exclusions:** Administrators (Include Disabled)
- Actions:**
 - Actions:** Add Administrative Rights
 - Child Actions:** Add Child Actions
 - Audit Policy Events:** Record all activity detected by this policy in Policy Events

Test this use case

- Run MMC.EXE from an endpoint where the user is NOT an administrator. This MMC.EXE execution will be denied execution.
- Run printmanagement.msc from an endpoint where the user is NOT an administrator. This MMC snap-in will run with elevation.
- Change the Policy Priority of your "Allow Print Management Plug-in Application Control Policy" to Priority 11 rather than priority 9. Repeat the second test. When you now run printmanagement.msc, the application will be blocked despite your elevation policy. This is why it is crucial to keep the priority levels that are set for your policies in mind and adjust them to meet your intended system requirements.

List of Default Policies

Here is the complete list of policies that come with Privilege Manager out-of-the-box, grouped by folder type. Once you create custom policies they are listed along the default policies under the tab respective to the template used, as the template associates the folder type.

Process Hardening

Remove Advanced Privileges for Interactive Users	Removes advanced privileges for users interacting with a system via Desktop	n/a	50	n
--	---	-----	----	---

System Options

Client Option - Elevate Adding Printers via Control Panel	Elevates privileges of users to allow printer drivers to be installed through the Control Panel	Elevate	60	n
Client Option - Elevate Adding Printers via PrintUI.exe	Elevates privileges of users to allow printer drivers to be installed by the PrintUI Utility	Elevate	60	n
Client Option - Elevate Changing Time and Date	Elevates privileges of users to allow them to change the system time and date	Elevate	60	n
Client Option - Elevate Device Pairing	Elevates privileges of users to allow new drivers to be installed during the device pairing wizard.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (Vista/7)	Elevates privileges of users to allow them to defragment their hard disks on Windows Vista and Windows 7.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (XP)	Elevates privileges of users to allow them to defragment their hard disks on Windows XP.	Elevate	60	n
Client Option - Elevate Installing Display Languages	Elevates privileges of users to allow display languages to be installed	Elevate	60	n
Client Option - Elevate Network Adapter Settings	Elevates privileges to allow user to change network adapter settings.	Elevate	60	n
Client Option - Elevate Resource and Performance Monitoring	Elevates privileges of users to allow them to run Windows Resource and Performance Monitor utilities	Elevate	60	n
Client Option - Elevate Windows Backup	Elevates privileges of users to allow them to run Windows Backup	Elevate	60	n

Privilege Management

Limit Internet Browser and Mail Clients Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for standard Internet browsers and mail clients. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Instant Messaging Application Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for instant messaging applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Media Player Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for media player applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Process Rights for Unclassified Applications Discovered in the Last Week	This policy implements the fundamental security principle of least privilege by restricting the process rights for an application. Unnecessarily running applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within an application. This policy affects applications that have been discovered locally in the last week.	Reduce	95	n
User Access Control (UAC) Override Policy	This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.	Elevate	15	n
User Requested Elevation Justification Policy	This policy allows users to request applications to run with Administrative Rights if they provide a justification.	Elevate	15	n

Application Analysis

Administrative Rights Required Detection Policy (Application Compatibility)	This policy detects applications that are deemed to require Administrative rights by Windows.	Elevate	45	n
Administrative Rights Required Detection Policy (Security Manifest)	This policy detects applications that contain a security manifest that specifies administrative rights are required.	Elevate	45	n
Event Discovery Audit Elevated Privileges Policy	This policy will detect all applications that are run with Administrator Rights on endpoints with the agent. This policy can be configured on the Event Discovery Configuration page.		45	n
Setup Detection Policy	This policy reports on applications that are detected as an installer.		45	n

Windows Policies

Event Discovery Testing Computers Audit Policy (Windows)	This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group.	97	n	
Elevate Privilege Manager Remove Programs Utility Policy	This policy needs to be enabled if users are supposed to be able to remove programs and apps via the Remove Programs Utility.	2	n	

macOS Policies

--	--	--	--	--

Event Discovery Testing Computers Audit Policy (MacOS) This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group. 97 n

Automatic Elevation via Windows Client System Settings

Common Windows client settings can be deployed to endpoint agents the same way as any policy. These settings target **All** Windows Computers with Application Control Agent Installed (Target)* as the default resource target. Once a setting is selected from the list, the resource target can be modified to include specific computer or other existing resource targets can be assigned on screen.

Add Devices	Allow users to add drivers, installing drivers as necessary.
Add Printers	Allow users to add printers, installing drivers as necessary.
Backup the System	Allow users to perform system backup operations.
Change the Date and Time	Allow users to change the date, time and timezone.
Change Network Adapter Settings	Allow users to change the network adapter settings.
Defragment the Disk	Allow users to perform disk defragmentation operations.
Install Language Packs	Allow users to install operating system display languages.
Monitor Performance	Allow users to run the Windows Performance Monitor utility.

ActiveX

ActiveX Setting define which sites can run ActiveX controls for standard users.

To create an ActiveX setting, a new policy must be created based on the ActiveX policy type template.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

Firewall

An Application Firewall Policy policy type allows for firewall rules to be applied as an Action in an Application Control Policy.

To create Firewall rules, a new policy must be created based on the Windows Application Policy type template.

When defining the Firewall Policy an Application Classification must be set. An Action of type Application Classification can then apply that classification to an Application Control Policy, which then enforces all of the defined Firewall Policies that are defined with that classification.

General

The policies available on the General tab are covering the basic Privilege Manager functionality and are enabled by default. Most of these policies are fulfilling utility functions otherwise also considered tasks.

Basic Inventory (Initial, Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (Initial, Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.
Basic Inventory (Windows)	Instructs computers to report changes to their Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server on a scheduled basis, like once a week for example.
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.
Cleanup sent Privilege Manager Events (Mac OS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Cleanup sent Privilege Manager Events (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Default File Inventory Policy (MacOS)	The purpose of this policy is to inventory software programs running on the managed computer.
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Local User Inventory Policy (MacOS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Perform Resource Discovery (Mac OS)	Schedule on which agents will check with server to determine if any local resources require discovery.
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.
Retry errored TMS Events (Mac OS)	Scan Agent queue for any events that require retransmission.
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.

Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.
Scheduled Registration (Mac OS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.
Scheduled Registration (Windows)	Initiate agent registration with server.
Update Agent Commands (Mac OS)	When this policy is triggered the Agent will update agent command items.
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.
Update Applicable Policies (Mac OS)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies (Windows)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes less frequently than internal clients.
Update Provisioned Resource Client Items (MacOS)	
Update Provisioned Resource Client Items (Windows)	
User Logon Inventory Policy	Updates user logon data on the given schedule.
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.

Not Enabled

COM Inventory Policy	The purpose of this policy is to inventory COM+ and DCOM packages installed on the client.
Disable Local Guest Accounts	Provisioning policy to disable local Guest accounts on Windows computers.
Randomize Administrator Password	
Shared Folder Inventory Policy	The purpose of this policy is to inventory shared folders on the client.

Example Policies

This section contains examples on how to configure and use policies in Privilege Manager.

The following topics are available:

- [Approval Policies](#)
 - [Offline Approvals](#)
 - [HelpDesk Approvals](#)
 - [Setup a Policy to use Google Authenticator](#)
- [Allow Policies](#)
 - [Google Application with File Upload](#)
 - [Microsoft Security Catalog](#)
- [Elevation Policies](#)
 - [UAC Override Policy](#)
 - [Elevating the Privilege Manager Remove Programs Utility Policy](#)
 - [Elevate Applications launched from Network Share Policy](#)
 - [Elevate msi launched from a Network Share](#)
 - [Elevate Applications whose Execution Requires Approval](#)
 - [Elevate Applications that Require User Justification](#)
 - MS Visual Studio Installations - Filters and policy now provided via Configuration Feeds. Refer to [Config Feeds](#) for download and installation information.
- [Greylisting Policies](#)
 - [Using a Catch All Policy](#)
 - [Reputation Checking Policies](#)
- [Blocking Policies](#)
 - [Blocking Specific Applications](#)
 - [iTunes with File Upload](#)
 - [Quarantine Specific Malware](#)
 - [Catch-all Blocking Policy](#)
- [macOS Specific Policies](#)
 - [Allow Copy/Install of Applications](#)
 - [Request Application Installation](#)
 - [Application Self-elevation](#)
 - [Use Discovery to Determine if an Application Requires Admin Privileges](#)
 - [Require Justification for Firefox](#)
 - [Deny Photos Application](#)
 - [Adding macOS Agents to a Computer Testing Group](#)
 - [Inventoring .pkg Files](#)

Approval Policies

Approval policies require an end-user justification and use an admin approval workflow.

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

The following examples are available:

- [Offline Approvals](#)
- [HelpDesk Approvals](#)
- [Google Authenticator approval](#)
- [macOS Approval Process](#)

Offline Approvals

Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. If an endpoint is offline, an end user needs a way to also request an approval for an application to continue to execute, for such a situation an Offline Approval process has been implemented.

During an offline approval process a prompt is triggered for a 6-digit numeric pin also called request code. The end user then calls the Help Desk and provides system information to the Help Desk representative. The Help Desk representative generates and provides a 12-character alphanumeric response code for the deployed policy residing on the offline endpoint. Once the end user enters the response code the application execution continues and other actions can be performed, for example adding administrative rights.

The message actions used in the Offline Approval policy are OS specific. Use the action:

Windows:

NAME	DESCRIPTION	TYPE	SUPPORTED
Approval Request (with Offline Fallback) Form Action	This action will display an approval request form for approval before...	Display Advanced (Xaml) Windows Message	
Approval Request (with ServiceNow Request Item Number) Form ...	This action will display an approval request form for approval before...	Display Advanced (Xaml) Windows Message	
Approval Request Form Action	This action will display an approval request form for approval before...	Display Advanced (Xaml) Windows Message	

macOS:

NAME	DESCRIPTION	TYPE	SUPPORTED
Application Approval Request (with Offline Fallback) Message Ac...	Application Approval Request Message Action for Mac OS	Display Advanced Message Action	
Application Approval Request (with ServiceNow Request Item Nu...	Application Approval Request Message Action for Mac OS	Display Advanced Message Action	
Application Approval Request Message Action	Application Approval Request Message Action for Mac OS	Display Advanced Message Action	

Notifications for approvals can also be issued to mobile devices. Refer to [Mobile App section - Configure the Notification Settings](#)

Creating an Offline Approval Policy

For offline approvals to work, a message action supporting offline fallback needs to be configured. This example uses the macOS based message action.

1. Create an Offline Approval Policy, by specifying the specific message action:
 1. Navigate to Actions and click **Edit**
 2. Search for and **Add** the action **Application Approval Request (with Offline Fallback) Message Action**.
 3. Click **Update**.
2. Click **Save Changes**.

Offline approval for Photos

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (0 total endpoints) MacOS Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jul 27, 2020, 3:49:56 PM by WIN-E6GKPM7J7TF\Administrator

Priority * 50

Description This policy elevates the rights for specified executables

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted Wizard Generated App Bundle Filter for Photos Edit

Inclusions Add Inclusions

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.

Audit policy events reports all application executions back

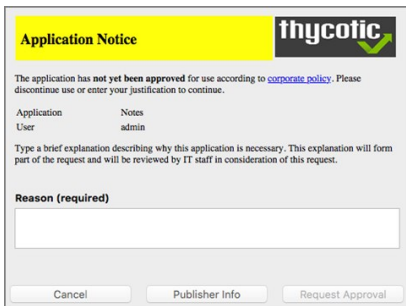
Actions Application Approval Request (with Offline Fallback) Message Action Run as Root Edit

Child Actions Add Child Actions

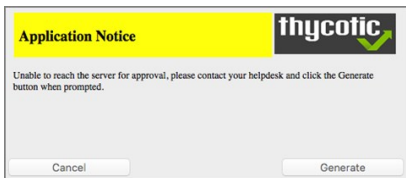
Endpoint Offline Approval

When the policy created above applies, the system first attempts an online approval request and if the server is unavailable it uses the request and response codes to verify authorization.

1. When trying to install an application that is not explicitly white-listed via policy while offline, the following Application Notice opens:

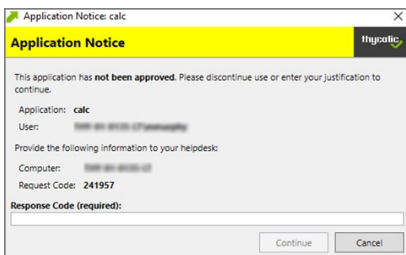


2. When the system is offline, the following notice opens:



3. Follow the instructions to contact your helpdesk and only click **Generate** when prompted.

4. You will then see:



Provide the information to the helpdesk, they will need the 6-digit code, in this example 191279, to create a response code.

5. Once your helpdesk contact verifies the authenticity of the request, you will be provided a 12-digit **Response Code** that needs to be entered in the text field.
6. Click **Continue** after entering the Response Code.

At this point the application installation should be able to continue.

Privilege Manager Offline Approval

The following procedures provides detailed steps about the offline approval process in the Privilege Manager UI.

1. Navigate to **Admin | Tools | Offline Approval**.

Offline Approvals

Search for the endpoint that is requesting a response code. After selecting the endpoint, enter the request code provided by the end user. Press 'Generate response code' to the end user to allow their desired application execution to continue.

Select Computer

Computer Name Select... ¹

Select Computer ²

Domain
[All] ▾

OS Name
[All] ▾

Computer Name

Max Rows *
10000

2. Click **Select...** and search to access the list of Computers with open offline approval requests.
3. Verify the customer's name is in the list.
4. Select the customer's computer from the list and click the **Select** button.

Offline Approvals

Search for the endpoint that is requesting a response code. After selecting the endpoint, enter the request code provided by the end user. Press "Generate response code" and provide this response code to the end user to allow their desired application execution to continue.

Select Computer

Computer Name

Create New Approval

Request Code

5. Enter the **Request Code** provided by the customer and click **Generate Response Code**.
6. Read the Response Code back to the customer to enter at the endpoint.

Help Desk Approvals

Privilege Manager enables end users to request elevation and then have their request approved or denied by the helpdesk. You can approve or deny requests via the Privilege Manager console, or forward requests to a third-party ticketing system such as ServiceNow.

Creating a Helpdesk Policy

1. Using the Policy Wizard, create a controlling policy that elevates requiring approval.
2. Select what file types you want targeted with the approval elevation.
3. Choose your targets. You can specify several different targets.
4. Name your policy and click **Create**.

HelpDesk Elevate Process Rights Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) Windows Computers x Add

Deployment Not deployed (Policy is inactive)

Last Modified Jul 28, 2020, 8:38:20 AM by WIN-E6GKPM7J7TF\Administrator

Priority * 50

Description This policy elevates the rights for specified executables

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. Filters

Applications Targeted Wizard Generated Win 32 Filter for 'explore.exe' Edit

Inclusions Add Inclusions

Exclusions Add Exclusions

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. Actions

Actions Add Administrative Rights Approval Request Form Action Restrict File Dialogs Edit

Child Actions Add Child Actions

Audit Policy Events Record all activity detected by this policy in Policy Events

The important wizard added actions on this policy are:

- o **Approval Request From Action**
- o **Restrict File Dialogs**
- o **Add Administrative Rights**

5. Set the **Inactive** switch to **Active**.

Once the agent receives the update, users receive a message action dialog to enter their written request in the Reason (required) field which then sends a request to either the Privilege Manager console or integrated Helpdesk.

Workflow

When end users try to open a restricted application, they must enter a reason for needing the application and send it for approval. While the request is being evaluated, whenever end users start the application a status pending message will appear. Once the request has been approved or denied, end users receive an approval or denial.

Approve requests

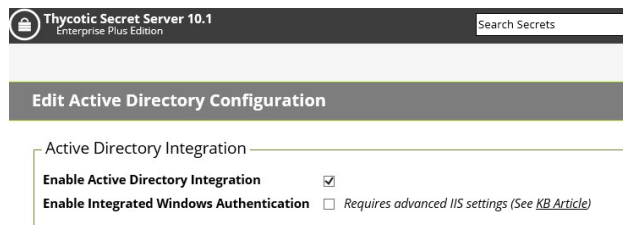
To approve or deny requests in the Privilege Manager Console, go to **Admin: Tools | Manage Approvals** to view all application requests.

Google Authenticator

This topic describes how to set up a Privilege Manager policy for enabling two-factor functionality with Google Authenticator.

Follow the steps described below to set up a policy for enabling two-factor functionality with Google Authenticator.

1. If you are using the Secret Server login for Privilege Manager, make sure you log in with an Active Directory credential. If you are currently using a Secret Server credential, you need to enable Active Directory Integration.



1. Once you log in with an Active Directory credential go to this URL:

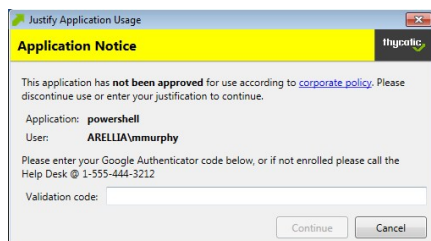
[https://\[ServerName\]/Tms/Account/Totp](https://[ServerName]/Tms/Account/Totp)

2. There you will see the QR Code or Secret to input into Google Authenticator in order for your user account to authenticate on the endpoint. Each user will need to go to this URL after logging in to Secret Server and add this QR Code to their authenticator app. Users can NOT re-use the same authenticator code that they are using for Secret Server.
3. After you have done that with one of your user accounts, you need to import an XML file as follows:
 1. Access the topic, [XML for Challenge Response Message Actions](#). It contains XML code, copy all that XML code.
 2. Go to [https://\[ServerName\]/Tms/PrivilegeManager/#/item/xml](https://[ServerName]/Tms/PrivilegeManager/#/item/xml)
 3. Paste the contents of the XML code (which you copied in a previous sub-step) into the text field and click the Import button.

4. You can then go to each policy for which you want to enable the two-factor prompt and add the "Challenge/Response Message Action" as an action.

Note: It is not recommended that you do this for ALL applications that are being run.

5. The end users will then see a prompt such as shown below, when they go to launch an application which triggers that action:



NOTE: Justification prompt messages are customizable.


```

</Style>
<!--
<Style x:Key="ImageHeadingBorderStyle" TargetType="Border">
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Padding" Value="8" />
<Setter Property="Background" Value="Black" />
</Style>

<Style x:Key="ImageHeadingStyle" TargetType="Image">
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Source" Value="Images/logo-white.png" />
<Setter Property="Height" Value="18" />
</Style>
-->
<!-- content area -->

<Style x:Key="ContentPanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="8" />
</Style>

<Style x:Key="InformationRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource BaseRichTextBoxStyle}">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Section x:Key="InformationTextSection" xml:space="preserve">
<Paragraph FontFamily="Segoe UI" FontSize="12"><Run>This application has </Run><Bold>not been approved</Bold><Run> for use according to </Run><Hyperlink Foreground="Blue" TextDecorations="Underline" TargetName=".blank"
NavigateUri="http://www.example.com/policy.html"><Run>corporate policy</Run></Hyperlink><Run>. Please discontinue use or enter your justification to continue.</Run></Paragraph>
</Section>

<Style x:Key="PropertiesPanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Style x:Key="ApplicationNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Text" Value="Application:" />
</Style>

<Style x:Key="ApplicationFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnlyFieldStyle}">
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Text" Value="{Binding ProcessName}" />
</Style>

<Style x:Key="UserNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Text" Value="User:" />
</Style>

<Style x:Key="UserNameFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnlyFieldStyle}">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Text" Value="{Binding UserName}" />
</Style>

<Style x:Key="InstructionRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource BaseRichTextBoxStyle}">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Section x:Key="InstructionTextSection" xml:space="preserve">
<Paragraph FontFamily="Segoe UI" FontSize="12"><Run>Please enter your Google Authenticator code below, or if not enrolled please call the Help Desk @ 1-555-444-3212</Run></Paragraph>
</Section>

<Style x:Key="ChallengeResponsePanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="0,8,0,5" />
</Style>

<Style x:Key="ChallengeLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Text" Value="Request code:" />
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="0" />
</Style>

<Style x:Key="ChallengeTextStyle" TargetType="TextBlock">
<Setter Property="Text" Value="{Binding ChallengeToken,Mode=OneWay}" />
<Setter Property="VerticalAlignment" Value="Center" />
<Setter Property="FontWeight" Value="Bold" />
<Setter Property="FontSize" Value="15" />
<Setter Property="Margin" Value="0,0,0,8" />
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="1" />
</Style>

<Style x:Key="ResponseLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Text" Value="Validation code:" />
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="0" />
</Style>

<Style x:Key="ResponseTextBoxStyle" TargetType="TextBox">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="MaxLength" Value="40" />
<Setter Property="Text" Value="{Binding ResponseToken,Mode=TwoWay,UpdateSourceTrigger=PropertyChanged}" />
</Style>

<Style x:Key="ButtonPanelStyle" TargetType="StackPanel">
<Setter Property="Orientation" Value="Horizontal" />
<Setter Property="HorizontalAlignment" Value="Right" />
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Style x:Key="ContinueButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}">
<Setter Property="Content" Value="Continue" />
<Setter Property="Command" Value="{Binding ContinueWithChallengeResponseCommand}" />
<Setter Property="CommandParameter" Value="{Binding ResponseToken}" />
</Style>

<Style x:Key="CloseButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}">
<Setter Property="Content" Value="Cancel" />
<Setter Property="Command" Value="{Binding CloseCommand}" />
</Style>

</Window.Resources>

<StackPanel Style="{StaticResource MainWindowPanelStyle}"
  adx:WindowHelper.Title="{Binding Result,Source={StaticResource WindowTitle}}">

<Border Style="{StaticResource HeadingBorderStyle}">
  <Grid>
    <Grid.ColumnDefinitions>
      <ColumnDefinition Width="*" />
      <ColumnDefinition Width="Auto" />
    </Grid.ColumnDefinitions>

    <Border Style="{StaticResource TitleHeadingBorderStyle}">
      <TextBlock Style="{StaticResource TitleHeadingStyle}" />
    </Border>
    <Border Style="{StaticResource ImageHeadingBorderStyle}">
      <Image Style="{StaticResource ImageHeadingStyle}"

```



```
        acs:ImageSourceHelper.EncodedImage="{StaticResource EncodedLogoImage}"
        adx:ImageSourceHelper.EncodedImage="{StaticResource EncodedLogoImage}" />
    </Border>
</Grid>
</Border>
<StackPanel Style="{StaticResource ContentPanelStyle}">
    <!-- Information of why this dialog needs attention -->
    <RichTextBox Style="{StaticResource InformationRichTextBoxStyle}"
        ac:RichTextBoxHelper.Section="{StaticResource InformationTextSection}"
        adx:RichTextBoxHelper.Section="{StaticResource InformationTextSection}" />
    <!-- Details about detected process -->
    <Grid Style="{StaticResource PropertiesPanelStyle}">
        <Grid.ColumnDefinitions>
            <ColumnDefinition Width="Auto" />
            <ColumnDefinition Width="*" />
        </Grid.ColumnDefinitions>
        <Grid.RowDefinitions>
            <RowDefinition />
            <RowDefinition />
        </Grid.RowDefinitions>
        <TextBlock Style="{StaticResource ApplicationNameLabelStyle}" />
        <TextBlock Style="{StaticResource ApplicationFieldStyle}" />
        <TextBlock Style="{StaticResource UserNameLabelStyle}" />
        <TextBlock Style="{StaticResource UserNameFieldStyle}" />
    </Grid>
    <!-- Instruction for Challenge/Response fields -->
    <RichTextBox Style="{StaticResource InstructionRichTextBoxStyle}"
        ac:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}"
        adx:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}" />
    <Grid Style="{StaticResource ChallengeResponsePanelStyle}">
        <Grid.ColumnDefinitions>
            <ColumnDefinition Width="Auto" />
            <ColumnDefinition Width="*" />
        </Grid.ColumnDefinitions>
        <Grid.RowDefinitions>
            <RowDefinition />
            <RowDefinition />
        </Grid.RowDefinitions>
        <!-- Challenge field -->
        <!-- <TextBlock Style="{StaticResource ChallengeLabelStyle}" />
        <TextBlock Style="{StaticResource ChallengeTextStyle}" />
        <!-- Response field -->
        <TextBlock Style="{StaticResource ResponseLabelStyle}" />
        <TextBox Style="{StaticResource ResponseTextBoxStyle}" />
    </Grid>
    <!-- Buttons at bottom -->
    <StackPanel Style="{StaticResource ButtonPanelStyle}">
        <Button Style="{StaticResource ContinueButtonStyle}"
            adx:ButtonHelper.IsDefault="true" />
        <Button Style="{StaticResource CloseButtonStyle}"
            adx:ButtonHelper.IsCancel="true" />
    </StackPanel>
</StackPanel>
</StackPanel>
</Window>
]]></Xaml>
</CustomXamlExecutionActionContract>
```

Allow Listing Policies

Allow listing is a type of policy that allows applications to run on your endpoints. You can think of allow listing as a neutral policy type because it does not alter an application's default permissions, it merely signifies that the application is "known/trusted" and allowed to run. Although simple allow listing follows normal, user-level credentials, allow listed applications are also often paired with Elevation Policies outlined [Elevation Policies](#).

The following examples are available:

- [Allow MS Security Catalog](#)
- [Allow Google Application with File Upload](#)

Git App with File Upload

In evaluation and production installations, proactive introduction of executables into Privilege Manager can be accomplished with a feature called File Upload. File Upload allows you to quickly introduce a file, then create a Filter and/or a Policy to govern the application. As example, here's how to introduce the Git Installer into Privilege Manager and use the file information to allow list Git applications.

For this use-case you will need to have access to downloaded Git installer files.

1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select what process types you want the policy to allow, for this example it's **Specific Applications**.
3. Choose your target, for this example **File Upload**.
4. Click **Choose File** and select a file to upload.
5. Click **Upload File**.
6. On the **Manage Application** page select all the identifying factors you want the filter to target.

Manage Application

File Name

File Path

Internal Name

Original File Name

Product Name

Company Name

File Version

Product Version

Copyright

Signed By

7. Click **Create Filter**.

← Back to Application Policies

Policies

What do you want to target?

Existing Filter
Add existing filters to this new policy

File Upload
Upload a file to create a filter that targets it

Inventoried File
Create a new filter from a file that was discovered during File Inventory

Selected Filters

Existing Filter

File Upload
Wizard Generated Win 32 Filter for 'Git:2.23.0-... Remove

Inventoried File

8. Click **Next Step**.

9. Name your policy and add a description, click **Create Policy**.

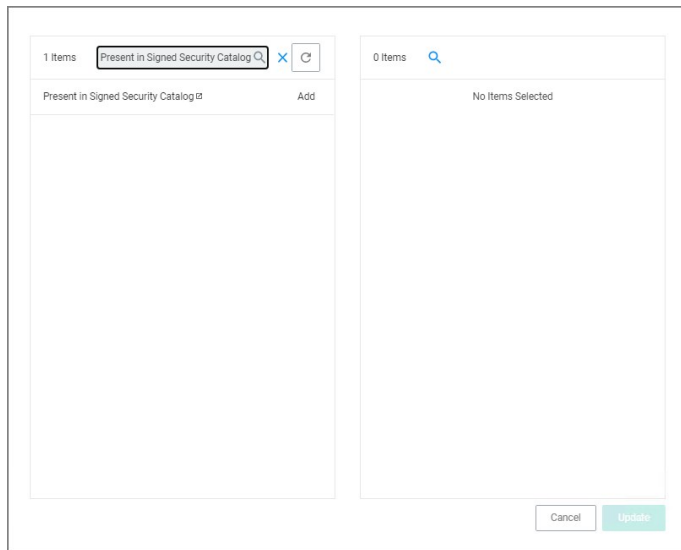
The screenshot displays the configuration page for an application policy in the Delinea Privilege Manager console. The page is titled 'Allow Git Application Policy' and includes a search bar, notification bell, help icon, and a red alert icon. Below the title, there are tabs for 'General', 'Policy Events', and 'Change History'. The 'General' tab is active, showing the policy's status as 'Inactive' with a toggle switch, and buttons for 'Refresh' and 'More'. The 'Policy Details' section includes a description: 'Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.' It lists 'Computer Groups Targeted' as '1 (1 total endpoints) Windows Computers' with an 'Add' button. The 'Deployment' status is 'Not deployed (Policy is inactive)'. The 'Last Modified' date is 'Jul 28, 2020, 10:43:33 AM by WIN-E6GKPM7J7TF\Administrator'. The 'Priority' is set to '85'. The 'Description' field contains the text: 'This policy allows the specified applications.' The 'Conditions' section includes a description: 'Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.' It lists 'Applications Targeted' as 'Wizard Generated Win 32 Filter for 'Git-2.23.0-64-bit.exe'' with an 'Edit' button. There are also links for 'Add Inclusions' and 'Add Exclusions'. The 'Actions' section includes a description: 'Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy.' It lists 'Actions' with an 'Add Actions' button, 'Child Actions' with an 'Add Child Actions' button, and 'Audit Policy Events' with a toggle switch and the text 'Record all activity detected by this policy in Policy Events'.

10. Set the **Inactive** switch to **Active**.

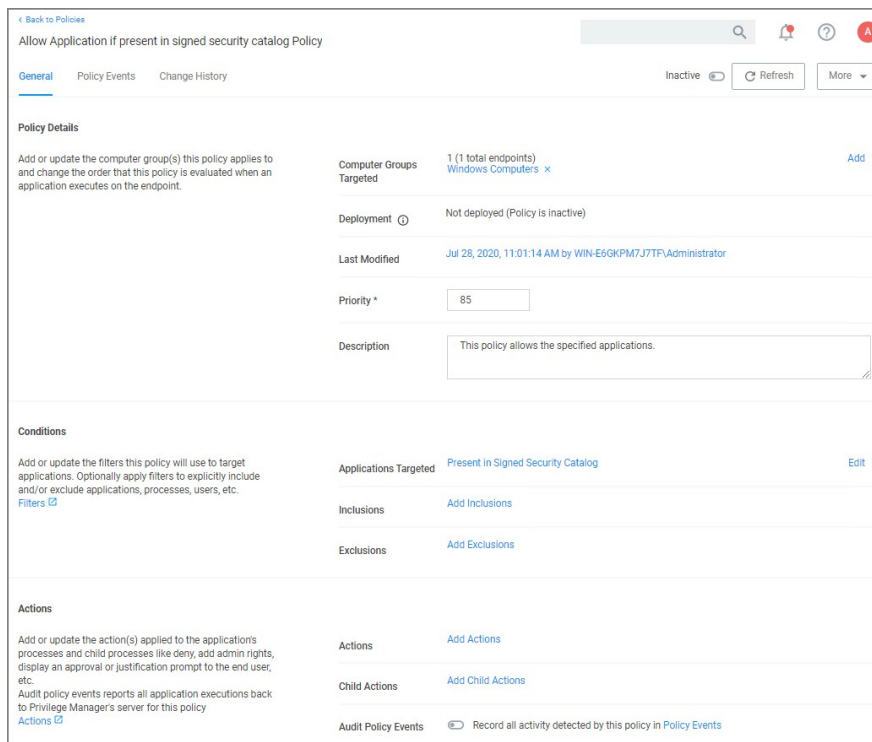
MS Security Catalog

This policy uses a built-in filter to allow list Microsoft's Signed Security Catalog. This filter is often used to dynamically allow to update items from Microsoft. Allow listing these executables clears them so they are not effected by any other policy, (i.e. they are allowed to run).

1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select what process types you want the policy to allow, for this example it's **Specific Applications**.
3. Choose your target, for this example **Existing Filter**.
4. Search for and **Add the Present in Signed Security Catalog** filter.



5. Click **Update**.
6. Click **Next Step**.
7. Name your policy and add a description, click **Create Policy**.



8. Set the **Inactive** switch to **Active**.

There is no need to add actions under the Actions tab, because these applications are allow listed, they are allowed to run with default permissions.

Elevation Policies

Distinct from allow policies where applications are simply allowed to run with default user level privileges, an Elevation Policy will apply Administrator credentials to specified applications. This type of policy is often paired with allowlisting to save IT Administrators time when many employees must perform trusted tasks that require Administrator credentials to complete, like installing a trusted application (Adobe) or device (printer).

In Privilege Manager 10.7 the [Restrict File Dialogs](#) action has been added to the product. Thycotic recommends using this action on elevation policies to prevent the misuse of file open and save dialogs for elevated applications.

Topics in this section:

- [Setting up ActiveX Policies](#)
- [UAC Override Policy](#)
- [Elevating the Privilege Manager Remove Programs Utility Policy](#)
- [Elevate Applications launched from Network Share Policy](#)
- [Elevate msi launched from a Network Share](#)
- [Elevate Applications whose Execution Requires Approval](#)
- [Elevate Applications that Require User Justification](#)
- MS Visual Studio Installations - Filters and policy now provided via Configuration Feeds. Refer to [Config Feeds](#) for download and installation information.

Application Execution Requires Approval

This policy type requires a user to provide a justification reason as to why they need to run a process (installer or executable). Then, the reason is submitted to specified managers via Privilege Manager **Admin: Tools | Manage Approvals** for approval. It also depends on whether or not the Manual Approval process is used. For instance, if you have configured Service Now as your approval process handler, these approval requests won't appear in the **Admin: Tools | Manage Approvals** area. There are several pieces to the Actions in this policy. Because Conditions and Actions are independent, these actions for approval can be applied to any condition. In this use case, we will apply this action to the LICEcap gif creator.

First create a filter that will identify the process/executable on which Privilege Manager will act.

1. Navigate to **Admin | Filters**.

2. Click **Create Filter**.

Note: In this use case, we will target the LICEcap application (LICEcap.exe).

3. From the **Platform** drop-down select **Windows**.

4. From the **Filter Type** drop-down select **Blank Win32 Executable Filter**.

5. Add a name and description, click **Create**.

6. Enter **LICEcap.exe** in the File Name field under File Specifications as well as in the Original filename field under File Details.

LICEcap filter

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Filter Details

Name: LICEcap filter

Description:

Platform: Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name: LICEcap.exe

File Path:

Include subdirectories

First Discovered: Anytime In the last 0 minute(s)

File Details

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character (*) is allowed only at the end. All values specified must match the file detail for the file to be included in the set.

Internal name:

Original filename: LICEcap.exe

File version:

7. Click **Save Changes**.

Create a Policy using this Filter

1. Using the Policy Wizard, create a controlling policy that elevates requiring approval.

2. Select what file types you want targeted with the approval elevation, for this example select **Executables**.

3. Choose your targets. You can specify several different targets, for this example select **Existing Filter**.

4. Search for and add the LICEcap filter created previously.

5. Click **Update**. You may also use **File Upload** to upload the LICEcap.exe file or **Inventoried File** if LICEcap.exe was inventoried for this computer group.

6. Click **Next Step**.

7. Name your policy and click **Create Policy**.

8. Set the **Inactive** switch to **Active**.

- Once the policy is delivered to the endpoint agent LICEcap.exe will require the user to enter a justification reason for running this application:
- Once the reason is entered by the user, the user clicks Continue to forward to the request to Privilege Manager for approval. On their desktop the Application Notice approval status is marked as Pending.
- Finally, a privilege manager user will approve this application request

To Approve Requests

1. Return to the Privilege Manager Dashboard and navigate to **Admin: Tools | Manage Approvals**.

2. Select the approval requested from the list and click on **Approve**.
3. Select **One Time or an allotted time frame for access** and **Manage Approve**.
4. You can now return to the desktop where the user initiated the executable, and you will see the request has been approved.
5. Click on **Continue** and the user is allowed to run that executable.

Note: To adjust this policy to apply to specific users or endpoints, use the option to add Inclusion/Exclusion filters and Computer Groups.

Elevate MSI Files on the Network Share

A wizard generated UNC or Network Share Path Elevation Policy elevates .exe files but not .msi files.

When launching an .msi file, the following command line is executed:

```
C:\Windows\System32\msiexec.exe /i "[path-to-network-share]\file]"
```

This means that the application is not elevated because the msiexec.exe file is not in the elevated Network Share directory.

This topic details two options for elevating .msi files from a network share.

Option 1

In order to enable elevation for .msi files on the network share, a command line filter can be created and added to the Elevation Policy.

1. In the Privilege Manager, navigate to **Admin | Filters**.
2. Click **Add Filters**.
3. From the **Platform** pull-down menu, select **Windows**.
4. From the **Filter Type** pull-down menu, select **Commandline Filter**.
5. Give this filter a custom name and description.
6. Click **Create**.
7. Under **Settings | Match Type**, select **Partial Match**.
8. In the Command line field, enter the network share path that needs to be elevated (such as \\share\folder_path).

9. Click **Save Changes**.
10. Navigate to your Elevation Policy. Under **Conditions** for **Application Targets** add the command line filter you just created.

Now MSI files in the network share will be elevated.

Option 2

An application control policy can be created that targets "msiexec.exe" and uses a secondary file filter as an include only filter.

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Elevate**, click **Next Step**.
6. In the policy wizard select **Run Silently**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **File Upload**.
 1. On the Upload a File modal, Click **Choose File**.
 2. Select the file(s) you wish to be targeted.
 3. Click **Upload File**.
 4. On the Manage Application dialog, check **File Name**.
 5. Click **Create Filter**.
 6. Click **Next Step**.
9. On the Finalize the Policy page, enter a name for your new policy. The policy will be created with a default priority of 50, since it is a silent elevation policy.
10. Click **Create Policy**.

- Click the **Packages for 'msi Elevate Process Rights Policy'** Filter and under **Settings** search for and add the **\share\to-path** filter previously created.

- Click **Save Changes**.
- Set the **Inactive** switch to **Active**.

MSI files in the network share will be elevated.

Adding the Secondary File Filter created to the Applications Targets under Conditions of the Policy will catch all instances where .msi files are run from %share%folder_path. Only msixec.exe will run .msi files, so the Secondary File Filter can be added to an Elevation Policy that has other Application Targets.

An Elevation Policy can be built with this Secondary File Filter as the Application Target and add the built-in Microsoft Installer File Filter as an Inclusion Filter to specifically target msixec.exe runs an .msi from %share%folder_path.

Network Share Applications

Many organizations put trusted installers on a network share that employees can use. Those installers can be elevated automatically from the shared network location by assigning an elevation policy to the network share location.

There are different options to elevate rights to launch applications from a network share location.

- One option is to create a file specification filter setting the path for the network share location. Then use that filter in a policy to apply administrative rights to all application launches from that path.
- The other option is to download the Application Control - UNC Elevation Policy Template via Config Feeds and customize the template.

Applying Administrator Rights to a Network Share

Creating the Filter

1. In the Privilege Manager Console navigate to **Admin | Filters**.
2. On the Filter page, click **Create Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the **Filter Type** drop-down select **File Specification Filter**. This also allows you to link in hashes or signatures.
5. Enter the name and a description for the filter, for example "network share" and "filter to elevate applications installed from network share".
6. Click **Create**.
7. Add the Path that points to your Fileshare folder, click **Save Changes**. Use the same UNC path format for both macOS and Windows endpoints.

Creating the New Policy

1. Navigate to **Computer Groups | Windows Computers**.
2. Select **Application Policies**.
3. Click **Create Policy**.
4. In the policy wizard select **Controlling**, click **Next Step**.
5. In the policy wizard select **Elevate**, click **Next Step**.
6. In the policy wizard select **Run Silently**, click **Next Step**.
7. In the policy wizard select **Installer Packages**, click **Next Step**.
8. In the policy wizard select **Existing Filter**.
9. Search and add the network share path filter previously created.
10. Click **Update**.
11. Click **Next Step**.
12. Name your policy and enter a description.
13. Click **Create**.
14. Set the **Inactive** switch to **Active**.

Using the UNC Elevation Policy Template

Use the UNC Elevation Policy Template to create a customized policy that lets you scan a network share and automatically elevates launches of MSI and EXE files from that share.

1. Navigate to **Admin Config Feeds**.
2. Find **Privilege Manager Product Configuration Feeds**, click **Select Items**.
3. Find **Application Control Solution**, click **Select Items**.
4. Find **Application Control - UNC Elevation Policy Template**, click **Download**. The template is being installed.
5. Navigate to **Admin | Folders**.
6. In the folder tree open **Privilege Manager Solutions | Application Control | Policies | macOS or Windows policies | Privilege Management**.
7. Click **Create**.
8. From the template drop-down select **UNC Share Elevation Policy**.
9. Enter a name and description.
10. Enter the UNC Path to the network share. Use the same UNC path format for both macOS and Windows endpoints.

New

Template

UNC Share Elevation Policy

Name *

Testing Group Network Share Elevation Policy

Description

UNC share elevation for testing group

UNC Path *

\\path-to\share\

Cancel Create

11. Click **Create**.
12. The Policy is created, but needs some attention. Confirm that this is an elevation policy and click **Set as Elevate**.

Testing Group Network Share Elevation Policy - EXE Files

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) All Windows Computers with Application Control Agent Installed (Target) x	Add
Deployment	Not deployed (Policy is inactive)	
Last Modified	Jul 31, 2020, 11:31:57 AM by Administrator	
Priority *	40	
Description	UNC share elevation for testing group	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted	c3f64399-45dc-4b82-ba68-7e0bd906ce2	Edit
Inclusions	Add Inclusions	
Exclusions	Add Exclusions	

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. [Actions](#)

Actions	Add Administrative Rights	Edit
Child Actions	Add Child Actions	
Audit Policy Events	<input type="checkbox"/> Record all activity detected by this policy in Policy Events	

13. Change the priority based on how this policy needs to interact with other policies for your organization, click **Save Changes**.

14. Set the **Inactive** switch to **Active**.

Setting up ActiveX Policies

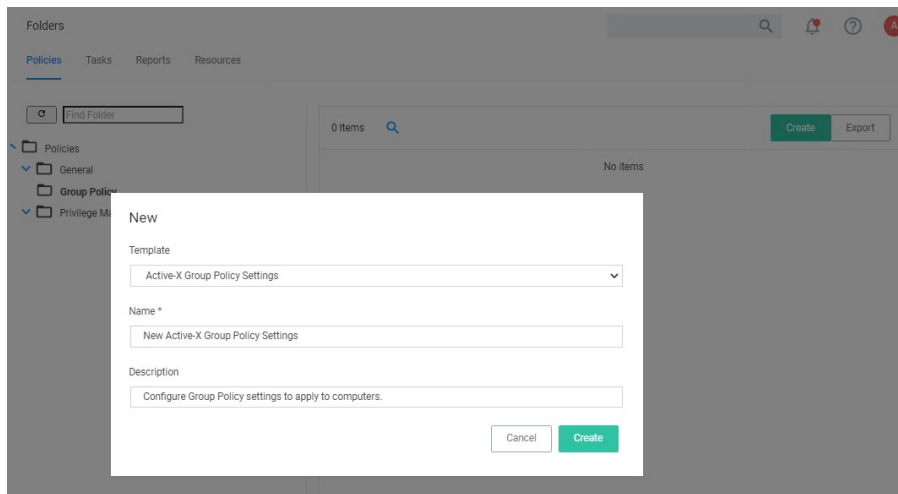
To allow add-ins to be installed via Internet Explorer, you need to create an allow policy for ActiveX.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

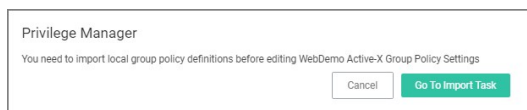
Refer to the Local Security topic, specifically [Manage Local Groups](#).

Creating the Policy

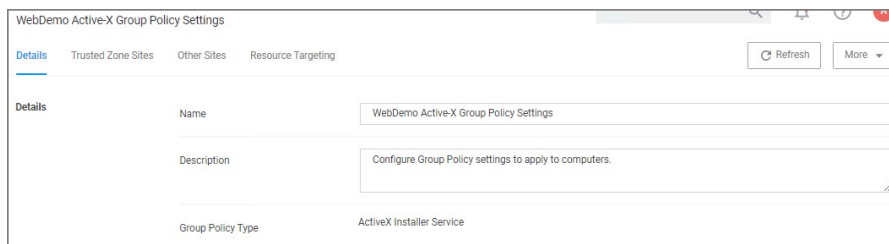
1. Navigate to **Admin | Folders**.
2. Select **Group Policies**.
3. Click **Create**.



4. From the **Template** drop-down, select **Active-X Group Policy Settings**.
5. Enter a name and description to identify the policy.
6. Click **Create**.
7. If you haven't already imported the Local Group Policy Definitions, Privilege Manager prompts you to import the definitions.



Click **Go to Import Task** and run the task. Return to the Active-X policy.



8. You can now add Trusted Zone sites and Other Sites and customize what actions to take when they are accessed.
 - Trusted Zone Sites tab:

Details **Trusted Zone Sites** Other Sites Resource Targeting Refresh More

ActiveX Control Installation Policy

This policy setting controls the installation of ActiveX controls for sites in Trusted zone. Enabled on computers with: No At least Windows Vista

If you enable this policy setting, ActiveX controls are installed according to the settings defined by this policy setting.

If you disable or do not configure this policy setting, ActiveX controls prompt the user before installation.

If the trusted site uses the HTTPS protocol, this policy setting can also control how ActiveX Installer Service responds to certificate errors. By default all HTTPS connections must supply a server certificate that passes all validation criteria. If you are aware that a trusted site has a certificate error but you want to trust it anyway you can select the certificate errors that you want to ignore.

Note: This policy setting applies to all sites in Trusted zones.

Other Sites tab:

Details Trusted Zone Sites **Other Sites** Resource Targeting Refresh More

This policy setting determines which ActiveX installation sites standard users in your organization can use to install ActiveX controls on their computers. When this setting is enabled, the administrator can create a list of approved ActiveX install sites specified by host URL. Enabled on computers with: No At least Windows Vista

If you enable this setting, the administrator can create a list of approved ActiveX install sites specified by host URL.

If you disable or do not configure this policy setting, ActiveX controls prompt the user for administrative credentials before installation.

Note: Wild card characters cannot be used when specifying the host URLs.

0 Items Add Site

- To customize, set the **Enabled on computers with: At least Windows Vista** to **Yes**.
- Click **Add Site**.

1 Items Add Site

HOST NAME	TRUSTED PUBLISHERS	SIGNED CONTROLS	UNSIGNED CONTROLS	CERTIFICATE VALIDATION	REMOVE
https://ActiveXWebDemoSiteC	Silently install	Silently install	Prompt the user	<input type="checkbox"/> Ignore unknown certification authority (CA) <input type="checkbox"/> Ignore invalid certificate name (CN) <input type="checkbox"/> Ignore invalid certificate date <input type="checkbox"/> Ignore wrong certificate usage	Remove

- Enter the Host Name (URL) for the site.
- Select from the Trusted Publishers and Signed Controls drop-down. The options are
 - Don't install
 - Prompt the user
 - Silently install
- Select from the Unsigned Controls drop-down. The options are
 - Don't install
 - Prompt the user
- Set any of the Certificate Validations switches to active specific ignore behavior, such as
 - Ignore unknown certification authority (CA)
 - Ignore invalid certificate name (CN)
 - Ignore invalid certificate date
 - Ignore wrong certificate usage
- Click **Save Changes**.
- On the **Resource Targeting** tab, Privilege Manager provides instructions for setting up how to deploy the Active-X policy to Resource Targets.
- In **Clone the following Policy**, click the **Policy** link to open the read-only client task.
- Duplicate the client task and give it a name identifying it as the task for your Active-X policy.

Active-X DemoSite task

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Scheduled Job Details

Name: Web Demo Active-X Task

Description: Task used in Active-X policy for scheduling

Computer Groups Targeted: 1 (1 total endpoints)
Windows Computers x Add

Deployment: Not deployed (Policy is inactive)

Job Settings

Command: Apply Group Policy Setting

Group Policy Setting *: WebDemo Active-X Group Policy Settings

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy will be run. Daily at 8:00:00 AM starting Mon Oct 01 2018 Add Trigger

Job Conditions

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions: Start the task only if the computer is idle

Power Conditions: Start the task only if the computer is on AC power
 Stop if the computer switches to battery power

1. From the **Job Settings | Command** drop-down, select **Apply Group Policy Settings**.
2. From the **Group Policy Setting** drop-down, select the Active-X policy created above.

Note: Apply Group Policy Settings when you have 2 or more ActiveX policies to add to the Parameters, otherwise use the Apply Group Policy Setting item.

13. Under Job Schedule modify the schedule and/or add triggers.

14. Set the **Inactive** switch to **Active**.

15. Click **Save Changes**.

On completing this configuration, Privilege Manager Triggers feature will then send the configured task to the targeted endpoint.

To view the Task, go to the **Task Scheduler**. You must have administrator access to view the task inside Thycotic folder.

UAC Override Policy

By creating a User Access Control (UAC) Override Policy you can override UAC prompts for end-users. You can create custom messages that require users to submit a reason for requesting administrator rights, which replace UAC prompts for credentials.

Using the Default Policy

- Under **Computer Groups** search for **User Access Control (UAC) Override Policy (Sample)**.

NAME	TYPE	MODIFIED	DESCRIPTION
Copy of Ensure UAC Override Setting (Windows)	Remote Scheduled Client Command	7/13/20, 3:26 PM	Ensures that the UAC Override Registry Key is set.
Copy of User Access Control (UAC) Override Policy	Application Control Policy	5/15/20, 2:38 PM	This policy allows standard users to provide a justification ...
Enable UAC Virtualization	GenericDetourAction	7/17/20, 11:15 AM	This action will turn on UAC virtualization for the target pro...
Ensure UAC Override Registry Key	Agent Executed Powershell Script	7/17/20, 11:15 AM	Script to ensure that UAC override is set in the registry
Ensure UAC Override Setting (Windows)	Remote Scheduled Client Command	7/17/20, 11:15 AM	Ensures that the UAC Override Registry Key is set.
Suppress User Account Control Consent Dialog	Set Environment Variable Action	7/17/20, 11:15 AM	This action will prevent the UAC consent dialog from being...
User Access Control (UAC) Override Policy (Sample)	Application Control Policy	7/17/20, 11:15 AM	This policy allows standard users to provide a justification ...
User Access Control Consent Dialog Detected	Environment Filter	7/17/20, 11:15 AM	This filter will match when an application that requires UAC...

The UAC Override Policy is a read-only item, that allows standard user to provide a justification for elevation instead of seeing the UAC prompt.

User Access Control (UAC) Override Policy (Sample)

This item is read-only.

General Policy Events Change History Inactive Duplicate More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers
Deployment	Not deployed (Policy is inactive)
Last Modified	Jul 17, 2020, 11:15:23 AM by Trusted Installer
Priority *	15
Description	This policy allows standard users to provide a justification for elevation instead of seeing the UAC pro...

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.
[Filters](#)

Applications Targeted	User Access Control Consent Dialog Detected
Inclusions	Interactive Users
Exclusions	Administrators (Include Disabled)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy
[Actions](#)

Actions	Add Administrative Rights Justify Application Elevation Action Restrict File Dialogs Suppress User Account Control Consent Dialog
Child Actions	No options selected
Audit Policy Events	<input type="checkbox"/> Record all activity detected by this policy in Policy Events

- To edit this policy, you need to make a copy and assign a different name, to do so click **Duplicate**.
- Under **Computer Groups Targeted** you may change the targeted endpoints.
- Under **Conditions** you edit the
 - Application Targets
 - Inclusion Filters
 - Exclusion Filters
- Under **Actions** you can edit
 - the actually actions for the policy like
 - the Justify Application Elevation Action
 - the Add Administrative Rights Action
 - the Suppress User Account Control Consent Dialog Action
 - if you want to Audit Policy Events (as a learning mode/monitoring feature)

- you can add Child Actions.

6. Click **Save Changes**, if you created a copy and made edits.

7. Set the **Inactive** switch to **Active**.


By default the UAC Override Policy has a priority setting of 15.


User Justification Required to Run


This policy type requires a user to provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition. In this use case, we will simply apply this action to a specific application.


1. Using the Policy Wizard, create a controlling policy that elevates application execution on endpoints.
2. Select **Require Justification**, and click **Next Step**.
3. Select what file type to target, for this example select **Executable**, and click **Next Step**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select a file to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.


Manage Application


File Name 
Git-2.23.0-64-bit.exe


File Path 
C:\Users\Administrator\Downloads\


Internal Name 


Original File Name 


Product Name 
Git

Company Name 
The Git Development Community

File Version 
2.23.0.1


Product Version 
2.23.0.23


Copyright 


Signed By 


8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.


Manage Application


File Name 
Git-2.23.0-64-bit.exe


File Path 
C:\Users\Administrator\Downloads\


Internal Name 


Original File Name 


Product Name 
Git

Company Name 
The Git Development Community

File Version 
2.23.0.1

Product Version 
2.23.0.23

Copyright 

Signed By 

11. Set the **Inactive** switch to **Active**.

The user will see a justification message as a result of the policy. When the user adds a reason, they will then click the **Continue** button and the application is allowed to execute.

Note: You can then view a user's provided reasons in Privilege Manager under **Reports | Application Justification Summary Details Report**.

Elevating the Privilege Manager Remove Programs Utility Policy

If standard users need to be able to use the Remove Program Utility the **Elevate Privilege Manager Remove Programs Utility Policy** needs to be elevated.

1. Search for **Elevate Privilege Manager Remove Programs Utility Policy**.

Search Results for Elevate Priv

elevate

NAME	TYPE	MODIFIED	DESCRIPTION
Elevate Privilege Manager Agent Preference Pane (Sample)	Application Control Policy	7/17/20, 11:15 AM	This policy is used to elevate the Privilege Manager Agent ...
Elevate Privilege Manager Remove Programs Utility Policy ...	Application Control Policy	7/17/20, 11:15 AM	This policy elevates the security rights for the Privilege Ma...

2. Click on the policy link **Elevate Privilege Manager Remove Programs Utility Policy**.

Elevate Privilege Manager Remove Programs Utility Policy (Sample)

This item is read-only.

General Policy Events Change History

Inactive Duplicate More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers
Deployment	Not deployed (Policy is inactive)
Last Modified	Jul 17, 2020, 11:15:23 AM by Trusted Installer
Priority *	2
Description	This policy elevates the security rights for the Privilege Manager Remove Programs Utility

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.

Applications Targeted	Privilege Manager Remove Programs Utility.exe File Specification Filter
Inclusions	No options selected
Exclusions	No options selected

Actions

Add or update the action(s) applied to the application's processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy.

Actions	Add Administrative Rights
Child Actions	No options selected
Audit Policy Events	<input type="checkbox"/> Record all activity detected by this policy in Policy Events

The default policy is read-only. If you need to customize any policy settings like the Conditions, Actions (like an approval action to run it), Policy Enforcement, or the Deployment, create a **Duplicate** to make edits.

3. Set the **Inactive** switch to **Active**.

Refer to [Using the Remove Programs Utility](#) for further details about the utility set-up and functionality.

Monitoring Policies

Monitoring Policies apply to any unknown applications that will attempt to run in your environment. It is important to discover unknown applications and determine whether to let them run or whether they are harmful. Monitoring provides a system for discovering the unknowns and adding an action that hinges on a reputation check.

The following examples are available:

- [Catch-All Policy](#)
- [Reputation Checking](#)

Catch-All Policy

A useful Learning Mode Policy to set up in Production environments is called a Catch-All Policy. This type of policy will gather information on any executables in your environment that are not satisfied by other Privilege Manager policies.

Note: These types of Catch-all monitor policies SHOULD NOT BE used for the Windows or Mac OS Computer Groups. Those groups apply to ALL computers in the environment and unless a monitor policy like this is setup to work with really good allow policies in front a lot of events will be sent.

1. Under Computer Group for which you want to monitor all activities select **Application Policies** and click **Create Policy**.
2. From the Policy Wizard select **Monitoring** and click **Next Step**.
3. Select **Everything** and click **Next Step**.
4. Enter a name, for example *Catch-all Monitor Policy*.
5. Click **Create Policy**.

Catch-all Monitor Policy

General Policy Events Change History

Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) testingLSS x	Add
Deployment	Not deployed (Policy is inactive)	
Last Modified	Jul 31, 2020, 7:41:46 AM by Administrator	
Priority *	200	
Description	This policy monitors the execution of all applications. Not recommend on more than a handful of machines.	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc.

Filters

Applications Targeted	Add Applications Targeted
Inclusions	Add Inclusions
Exclusions	Present in Signed Security Catalog Edit

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy.

Actions

Actions	Add Actions
Child Actions	Add Child Actions
Audit Policy Events	<input checked="" type="checkbox"/> Record all activity detected by this policy in Policy Events

6. Customize the policies Conditions, Actions, and Policy Enforcement, for example:
 - o Under Applications Targeted, click **Add Application Target** and search for and add **Interactive Users**.
 - o Under Exclusions, click **Edit** and add **LocalSystem and Service applications** to the exclusion list.

Catch-all Monitor Policy

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) testingLSS x	Add
Deployment	Not deployed (Policy is inactive)	
Last Modified	Jul 31, 2020, 7:41:46 AM by Administrator	
Priority *	<input type="text" value="200"/>	
Description	<input type="text" value="This policy monitors the execution of all applications. Not recommend on more than a handful of machines."/>	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted	Interactive Users	Edit
Inclusions	Add Inclusions	
Exclusions	LocalSystem and Service applications Present in Signed Security Catalog	Edit

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy [Actions](#)

Actions	Add Actions
Child Actions	Add Child Actions
Audit Policy Events	<input checked="" type="checkbox"/> Record all activity detected by this policy in Policy Events

- Under **Show Advanced | Policy Enforcement** set the switch for **Stage 2 Processing** to active and all others to inactive.

Policy Enforcement	
Continue Enforcing	<input type="checkbox"/> After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.
Applies To All Processes	<input type="checkbox"/> Policy will apply to system based processes. If setting is not enabled, policy will only apply to interactive users.
Enforce Child Processes	<input type="checkbox"/> Include child processes in the policy enforcement
Stage 2 Processing	<input checked="" type="checkbox"/> Only needed for catch-all deny policies to ensure that the policy only applies to applications NOT allowed directly or indirectly by a policy that applies to the parent process.
Skip Policy Analysis at Start-up	<input type="checkbox"/> Pauses policy analysis during boot-up (use only on filter heavy policies)

7. Click **Save Changes**

8. Set the **Inactive** switch to **Active**.

Reputation Checking

Privilege Manager analyzes applications in real-time. This unique feature allows for reputation analysis of any unknown applications that will mitigate endpoint attacks from Ransomware, Zero-day attacks, Drive-by Downloads, and other unknown malicious software.

The monitor approach used here is that all applications that meet a general condition (i.e. executed from a specific directory or directories) will be sent to VirusTotal for a reputation check. For this use case we will perform real-time reputation analysis of unknown applications using VirusTotal.

First, you will need to integrate Privilege Manager and VirusTotal by following the Integration steps listed in the [Setting Up VirusTotal for Reputation Checking](#) topic. That section will walk you how to do the following:

1. Configure VirusTotal Ratings Provider
2. Install VirusTotal in Privilege Manager
3. Create a Security Rating Filter for VirusTotal

For information and setup steps to configure reputation checking using Cylance, see the [Cylance Integration](#) topic.

Creating Security Rating Filter

Next you have to create a Security Rating Filter for VirusTotal. Follow these steps:

1. Navigate to **Admin | Filters**, then click **Create Filter**.
2. Select a platform, then **Security Rating Filter** as a Filter Type. Name the policy and add a description.
3. From the **Security Rating System** drop-down, select **Virus Total Rating System**.

Create Filter

Platform

Type

Name *

Description

Security rating system *

4. Click **Create**.
5. Under **Settings**, change the **Rating Level** drop-down to specify **Bad**.

New Security Rating Filter

Save changes? If you press cancel, all your changes will be lost.

Filter Details	Name	<input type="text" value="New Security Rating Filter"/>
	Description	<input type="text"/>
	Platform	Windows
Settings	Security Rating System	<input type="text" value="VirusTotal Rating System"/>
	Rating Level	<input type="text" value="Bad"/>
	Timeout	<input type="text" value="1"/> <input type="text" value="Second(s)"/>
Error Handling	On timeout, consider the result	<input type="text" value="Error Condition"/>
	On failure, consider the result	<input type="text" value="Error Condition"/>

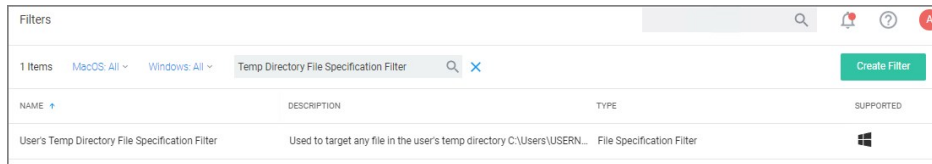
The rating level trigger is supposed to match what you want to accomplish with the policy that will be using this filter. A rating level of Bad should be used for Deny policies, and Clean for applications or files that are part of the safe list. A

rating level of Suspect can be used in justification and/or learning/discovery policies.

6. Click **Save Changes**.

Creating User's Downloads Location, Temp Dir, and Collection Filters

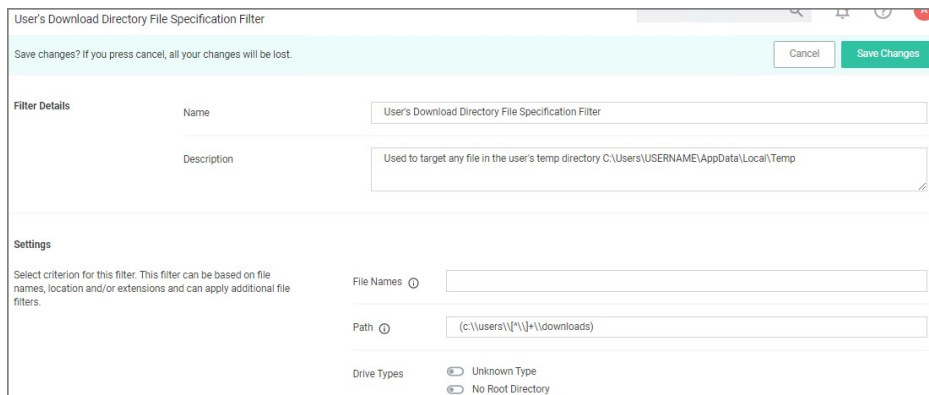
1. Navigate to **Admin | Filters** and search for **Temp Directory File Specification Filter**.



2. Select the filter **User's Temp Directory File Specifications Filter**, click **Duplicate**.

3. Name the new filter *User's Download Directory File Specification Filter*, provide a description and click **Create**.

4. Change the regular expression in the Path field to the following: `(c:\users\[^\]+)\downloads)`:



5. Click **Save Changes**.

6. Finally, combine the 2 filters into a single filter to target both directories:

1. Click **More | Duplicate**.
2. Enter the name for the new filter *User's Directory Collection File Specification Filter*, click **Create**.
3. Clear the data in the Path field.
4. Under Additional Filters, click **Add File filters**.
5. Search for **User's Download** and add the **User's Downloads Directory File Specification Filter**.
6. Search for **User's Temp Directory** and add **User's Temp Directory File Specification Filter** (this is a default filter).
7. Click **Update**.

User's Directory Collection File Specification Filter

Details Related Items Change History Refresh More

Filter Details

Name: User's Directory Collection File Specification Filter

Description: Used to target any file in the user's temp directory C:\Users\USERNAME\AppData\Local\Temp and C:\Users\USERNAME\Downloads

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names: []

Path: []

Drive Types:

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes:

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters: [User's Download Directory File Specification Filter | User's Temp Directory File Specification Filter] Edit

Include only filters: [Add Include only filters]

8. Click **Save Changes**.

Creating a Policy

Next you have to create a Policy and add the filters for VirusTotal:

1. Using the Policy Wizard, create a controlling policy that allows application execution on endpoints.
2. Select **Existing Filter**.
3. Search for and add the previously created **VirusTotal Security Rating Filter**.
4. Click **Update**
5. Name the policy **Allow Applications - VirusTotal Rating**, and add a description *Deny applications flagged by VirusTotal as bad*, click **Create Policy**.
6. Click **Add Inclusions**, search for and add the **User's Directory Collection File Specification Filter**.
7. Click **Update**

Allow Applications – VirusTotal Rating

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted: 1 (1 total endpoints) [Windows Computers](#) x [Add](#)

Deployment: Not deployed (Policy is inactive)

Last Modified: Jul 30, 2020, 6:32:28 PM by WIN-E6GKPM7J7TF\Administrator

Priority:

Description:

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted: [VirusTotal Security Rating Filter](#) [Edit](#)

Inclusions: [User's Directory Collection File Specification Filter](#) [Edit](#)

Exclusions: [Add Exclusions](#)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy. [Actions](#)

Actions: [Application Denied Message Action](#) [Edit](#)

Child Actions: [Add Child Actions](#)

Audit Policy Events: Record all activity detected by this policy in [Policy Events](#)

8. Click **Save Changes**.

9. Set the **Inactive** switch to **Active**.

Note: This policy will send any application run from the user's Downloads or Temp directory to VirusTotal for a reputation check in real-time. If the application is graded with Bad from VirusTotal, the application will be denied.

Viewing a File Security Ratings Report

To view a File Security Ratings report, search for **File Security Rating Details Report**. To see details of the applications in the report, click on the file name in the File column.

Blocking Policies

Blocking is a policy that denies applications from running on your endpoints based on application attributes, file hash, location, or certificates. This is a powerful type of policy and it may be used to block specific, known and unwanted applications from running. A block policy can target programs that prevent productivity for your end users or applications that are known malware. If malware, you can also add a quarantine action for your block policy as outlined in the second example below.

Thycotic Privilege Manager controls any application on a machine. When you configure Privilege Manager correctly, targeted applications can be elevated, allow listed, or blocked. But if you create new policies without careful consideration then you can potentially block core system processes.

Before you create new policies, keep in mind the following best practices:

- Do not enable policies until after you have configured them. As a safety precaution, all newly-created application control policies are turned off until you enable them.
- Important: New policies that you create will automatically target all applications until you add application filters that will narrow the scope.
- Additionally, Thycotic highly recommends testing all policies on a limited number of machines before they are deployed to the entire environment. See [Best practices for Application Control Solution policies](#) for more information.

The following examples are available:

- [Blocking Specific Applications](#)
- [iTunes with File Upload](#)
- [Quarantine Specific Malware](#)
- [Catch-all block Policy](#)

Catch-all Deny

A catch-all deny policy is the last policy executed following the execution of a group of allow list policies. This enables you to configure your allow list to allow approved applications, like the Windows directory or other installed applications, and then to deny everything else, like applications downloaded from the internet or a thumb drive.

To create a catch-all deny policy, follow these steps:

1. Under your Computer Group select Application Policies and click **Create Policy**.
2. Select **Skip the wizard, take me to a blank policy** to create a blank policy.
3. Enter a name and description, change the default priority value to a higher number, for example 99 and click **Create**.
4. Under **Conditions**, click **Add Exclusions**.
5. Search for and **Add** the **LocalSystem and Service applications** filter.
6. Click **Update**.
7. On the bottom of the policy page, click **Show Advanced**.
8. Under **Policy Enforcement**, ensure only **Stage 2 processing** is set to active.

Policy Enforcement	
Continue Enforcing Policies	<input type="checkbox"/> Once an application meets the criteria of this policy, subsequent policies will not be evaluated.
Continue Enforcing Policies for Child Processes	<input type="checkbox"/> Subsequent policies will not be evaluated for child processes.
Stage 2 Processing	<input checked="" type="checkbox"/> Policies that define behavior for child processes will be evaluated first.
Applies To All Processes	<input type="checkbox"/> Policy will only apply to interactive users.
Skip Policy Analysis at Start-up	<input type="checkbox"/> Pause policy analysis during boot-up (use only on filter heavy policies)

9. Click **Save Changes**.
10. Set the **Inactive** switch to **Active**.

If you are creating a new catch-all policy to be used in conjunction with allow list policies, please verify that the allow list is catching all system applications and that the new deny policy is the last policy executed. For additional safety you can define the exclude any parameter to exclude system and service applications.

iTunes with File Upload

As we've seen, there are multiple ways to introduce a new application into Privilege Manager before assigning a policy to it. For this example we will perform a File Upload for the iTunes installer to quickly deny list the iTunes program from running on target endpoints.

Note: When the iTunes default filter is used, verify the correct Company name is entered to match the application targeted by the policy.

1. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
2. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
3. Select what types you want the policy to block, for this example it's **Executables**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select the installer (iTunes.exe) to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.
8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.
11. Set the **Inactive** switch to **Active**.

Deny iTunes installation

General Policy Events Change History

Active Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) [Windows Computers](#) x [Add](#)

Deployment 100% (1 endpoints, 1 with the latest version)

Last Modified Jul 20, 2020, 9:16:07 PM by [Administrator](#)

Priority *

Description

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted [iTunes](#) [Edit](#)

Inclusions [Add Inclusions](#)

Exclusions [Present in Signed Security Catalog](#) [Edit](#)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. [Audit policy events reports all application executions back to Privilege Manager's server for this policy](#) [Actions](#)

Actions [Deny Execute](#) [Deny Execute Message](#) [Edit](#)

Child Actions [Add Child Actions](#)

Audit Policy Events Record all activity detected by this policy in [Policy Events](#)

Under the Actions tab, do not change the settings, but notice it is set to Deny Execute Message. This will produce a pop-up message to the user telling them this application execution is denied.

You can edit the policy further, if needed. Adjust the [Policy Priority](#) as needed.

Quarantine Specified Malware

For known cases of malware or ransomware, you can use Privilege Manager to prevent specified applications from running and place them in a quarantine. For this example we'll target the generic executable "malware.exe," but you can do this with any file name.

1. Navigate to **Admin | Filters** and click **Create Filter**.
2. From the platform drop-down select the OS to target, for this example **Windows**.
3. From the type drop-down select **File Specification Filter**.
4. Add a Name and Description, click **Create**.
5. On the filter page, under **Settings: File Names** type **malware.exe**.
6. Click **Save Changes**.
7. Under you Computer Group, select **Application Policies**.
8. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
9. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**, for this example we use **Block Silently**. Click **Next Step**.
10. Select what types you want the policy to block, for this example it's **Executables**.
11. Choose your target, for this example **Existing Filter**.
12. Search for and **Add** the **malware.exe** filter created in the above steps.
13. Click **Update**.
14. Click **Next Step**.
15. Name your policy and add a description, click **Create Policy**.
16. Under **Actions**, click **Edit**.
17. Search for **quarantine** and **Add** the **File Quarantine** and **Quarantine Message** actions.
18. **Remove** the **Deny Execute** and **Deny Execute Message** actions.

The screenshot displays two side-by-side search result panels. The left panel has a search bar containing 'quarantine' and shows two items: 'File Quarantine' and 'Quarantine Message', each with an 'Add' button. The right panel also has a search bar and shows two items: 'Deny Execute' and 'Deny Execute Message', each with a 'Remove' button. At the bottom of the interface are 'Cancel' and 'Update' buttons.

19. Click **Update**.

malware.exe Block Application Policy

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted	1 (1 total endpoints) Windows Computers x	Add
Deployment ⊙	Not deployed (Policy is inactive)	
Last Modified	Jul 28, 2020, 6:16:42 PM by WIN-E6GKPM7J7TF\Administrator	
Priority *	<input style="width: 80%;" type="text" value="10"/>	
Description	<input style="width: 95%; height: 20px;" type="text" value="This policy blocks the specified executables from running"/>	

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted	malware.exe File Specification Filter	Edit
Inclusions	Add Inclusions	
Exclusions	Add Exclusions	

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.
Audit policy events reports all application executions back to Privilege Manager's server for this policy [Actions](#)

Actions	File Quarantine Quarantine Message	Edit
Child Actions	Add Child Actions	
Audit Policy Events	<input checked="" type="checkbox"/> Record all activity detected by this policy in Policy Events	

20. Click **Save Changes**.

21. Set the **Inactive** switch to **Active**.

Once this policy has been applied to your endpoint/s, any executable called malware.exe will be automatically blocked and quarantined if prompted to run

Specific Applications

Using File Inventory

To create a new policy using file inventory data to block specific applications, follow these steps:

1. From the navigation menu select **File Inventory**.
2. From the table grid of inventoried files, select the application you want to block.

The screenshot shows the 'File Inventory' interface. On the left is a table with columns: FILE NAME, ORIGINAL FILE NAME, PRODUCT NAME, PRODUCT VERSION, and FIRST DISCOVERED. The row for 'tgittouch.exe' is highlighted with a red box. On the right is a detailed view for 'tgittouch.exe' with fields for Original File Name, Product Name, Product Version, Internal Name, Company Name, and Copyright. At the bottom right of the detailed view, there are two buttons: 'Create Filter' (with a red arrow pointing to it) and 'View File'.

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
New Loaded Resource	7/1/2020 3:21:56 PM			7/1/20, 3:21 PM
pingsender.exe	pingsender.exe	Firefox	77.0.1.7458	7/1/20, 3:21 PM
AccessibleMarshal.dll	AccessibleMarshal.dll	Firefox	77.0.1.7458	7/1/20, 3:21 PM
AccessibleHandler.dll	AccessibleHandler.dll	Firefox	77.0.1.7458	7/1/20, 3:21 PM
New Loaded Resource	7/1/2020 3:21:56 PM			7/1/20, 3:21 PM
helper.exe	helper.exe	Firefox	1.0.0.0	7/1/20, 3:21 PM
firefox.exe	firefox.exe	Firefox	77.0.1.0	7/1/20, 3:17 PM
opera_crashreporter.exe		Opera crash-reporter	68.0.3618.173	7/1/20, 3:17 PM
opera.exe		Opera Internet Browser	68.0.3618.173	7/1/20, 3:16 PM
tgittouch.exe	tgittouch.exe	tgittouch	2.8.0.8	6/30/20, 4:14 PM
TortoiseGitUDiff.exe	TortoiseGitUDiff.exe	TortoiseGitUDiff	2.8.0.8	6/30/20, 4:14 PM
TortoiseGitPlink.exe	TortoiseGitPlink.exe	TortoiseGit TortoiseGitPlink	0.70.0.70	6/30/20, 4:14 PM
TortoiseGitMerge.exe	TortoiseGitMerge.exe	TortoiseGitMerge	2.8.0.8	6/30/20, 4:14 PM
TortoiseGitDiff.exe	TortoiseGitDiff.exe	TortoiseGitDiff	2.8.0.8	6/30/20, 4:14 PM
TortoiseGitBlame.exe	TortoiseGitBlame.exe	TortoiseGitBlame	2.8.0.8	6/30/20, 4:14 PM
TGitCache.exe	TGitCache.exe	TortoiseGit	2.8.0.8	6/30/20, 4:14 PM
sendrpt.exe	sendrpt.exe	Doctor Dump	1.0.15.0	6/30/20, 4:14 PM
puttygen.exe	PuTTYgen	PuTTY suite	0.70.0.70	6/30/20, 4:14 PM

3. Click **Create Filter**.
4. On the **Manage Application** page select all the identifying factors you want the filter to target.
5. Click **Create Filter** or **Create and Add to Policy**. Use the **Create and Add to Policy** option if you already have a deny policy to target applications. Otherwise use **Create Filter** and then use the Policy Wizard or a blank policy to add that filter.

Using the Policy Wizard

To create a new policy using the policy wizard to block specific applications, follow these steps:

1. Using the Policy Wizard, create a controlling policy that blocks application execution on endpoints.
2. Select how you want the processes blocked, either **Block Silently** or **Notify and Block**. For this example we use **Block Silently**. Click **Next Step**.
3. Select what types you want the policy to block, for this example it's **Executables**.
4. Choose your target, for this example **File Upload**.
5. Click **Choose File** and select a file to upload.
6. Click **Upload File**.
7. On the **Manage Application** page select all the identifying factors you want the filter to target.
8. Click **Create Filter**.
9. Click **Next Step**.
10. Name your policy and add a description, click **Create Policy**.
11. Set the **Inactive** switch to **Active**.

Be sure to test the new policy on a few machines before you roll it out to the environment.

File Inventory

The file inventory page lists all files discovered based on the Basic Inventory policies.

The table grid contains the following columns:

- File Name
- Original File Name
- Product Name
- Product Version
- First Discovered

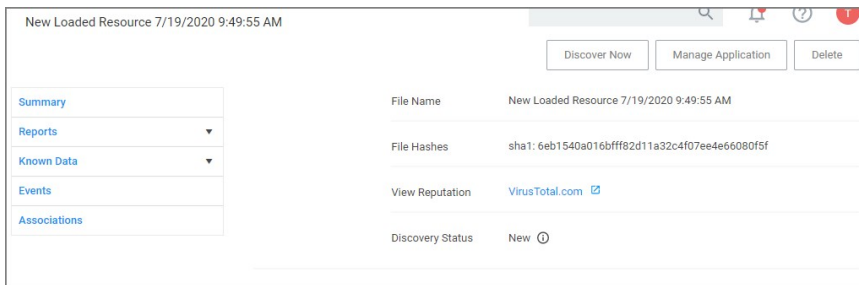
FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
devicecensus.exe	DeviceCensus.exe	Microsoft® Windows® Operating System	10.0.18362.1035	7/22/20, 7:05 AM
chrome.exe	chrome.exe	Google Chrome	84.0.4147.0	7/21/20, 9:27 AM
InstallAgent.exe	InstallAgent.exe	Microsoft® Windows® Operating System	10.0.14393.0	7/21/20, 9:25 AM
InstallAgentUserBroker.exe	InstallAgentUserBroker.exe	Microsoft® Windows® Operating System	10.0.14393.0	7/21/20, 9:25 AM
Explorer.EXE	EXPLORER.EXE	Microsoft® Windows® Operating System	10.0.14393.3808	7/21/20, 9:25 AM
shell32.dll	SHELL32.DLL	Microsoft® Windows® Operating System	10.0.14393.3808	7/21/20, 9:25 AM
New Loaded Resource 7/20/2020 8:38:21 PM				7/20/20, 8:38 PM
ActiveXControlSetUpInstructions.txt				7/15/20, 1:35 PM
ActiveXControlSetup.msi				7/15/20, 1:15 PM
New Loaded Resource 7/15/2020 1:15:39 PM				7/15/20, 1:15 PM
InetMgr.exe	InetMgr.exe	Internet Information Services	10.0.14393.0	7/15/20, 1:15 PM
New Loaded Resource 7/15/2020 10:25:38 AM				7/15/20, 10:25 AM
browser_assistant.exe		Opera Browser Assistant	69.0.3686.77	7/15/20, 10:23 AM
assistant_installer.exe		Opera Browser Assistant Installer	69.0.3686.77	7/15/20, 10:23 AM
ActiveXWebDemoSiteTwo.html				7/15/20, 9:50 AM
Royal RDP Connection Export defaults.csv				7/13/20, 7:25 AM

At the beginning of your policy creation process you will see many new events labeled as **New Loaded Resource**. This is because importing files in Privilege Manager is not the same thing as discovering information about the files. Discovery of file details is done [by scheduled tasks by default](#), but if you want to discover file details immediately, do the following:

1. Navigate to **File Inventory**.
2. Select **New Loaded Resource**.

FILE NAME	ORIGINAL FILE NAME	PRODUCT NAME	PRODUCT VERSION	FIRST DISCOVERED
Git-2.23.0-64-bit.tmp			0.0.0.0	7/1/20, 3:29 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
New Loaded Resource 7/1/2020 3:21:56 PM				7/1/20, 3:21 PM
firefox.exe	firefox.exe	Firefox	77.0.1.0	7/1/20, 3:17 PM
opera_crashreporter.exe		Opera crash-reporter	68.0.3618.0	7/1/20, 3:17 PM
opera.exe		Opera Internet Browser	68.0.3618.0	7/1/20, 3:16 PM

3. Click on a **New Loaded Resource** entry.



New Loaded Resource 7/19/2020 9:49:55 AM

Discover Now Manage Application Delete

Summary

Reports

Known Data

Events

Associations

File Name New Loaded Resource 7/19/2020 9:49:55 AM

File Hashes sha1: 6eb1540a016bffb82d11a32c4f07ee4e66080f5f

View Reputation [VirusTotal.com](#)

Discovery Status New

1. Check the Discover Status. The following states are available:

- **New**, the resource was just reported).
- **Pending Assignment**, the resource will soon be assigned to an agent for discovery).
- **Assigned to agent**, an agent was chosen to discover this resource.

Once an agent is assigned, you can click **Discover Now** to attempt to force the agent to immediately discover the resource. Many factors affect the agent's promptness in discovering the resource: agent up-time, current processing queue, etc. Please be patient.

4. Click **Discover Now**.

5. After the successful discovery, click **View File** or **Create Filter** as your next option to use the discovered or inventoried resource. You have the option to add it to a Policy.

Note: Files may not be discovered if they have already been deleted from your system.

Policy Events

Application control events or **Policy Events** are created if you choose to have one or more policies send feedback (from the endpoint to the server) each time the policy is triggered. Under **Policy Events** Privilege Manager provides access to all information collected and events discovered due to using monitoring policies with the **Audit Policy Events** switch set to active.

FILE NAME	# OF EVENTS	POLICY	LAST EVENT
Arellia Agent.InventoryHelper.exe	1271	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 12:15 PM
Arellia Agent.InventoryHelper.exe	1110	Everything Monitor Policy	7/21/20, 12:15 PM
Arellia Agent.InventoryHelper.exe	1110	Run with Administrator Rights Monitor Applications Policy	7/21/20, 12:15 PM
taskhostv.exe	343	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 12:15 PM
taskhostv.exe	306	Run with Administrator Rights Monitor Applications Policy	7/21/20, 12:15 PM
slui.exe	127	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 9:30 AM
slui.exe	107	Run with Administrator Rights Monitor Applications Policy	7/21/20, 9:30 AM
opera_autoupdate.exe	84	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 10:25 AM
chrome.exe	68	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 9:30 AM
InstallAgent.exe	67	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 11:35 AM
launcher.exe	63	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 10:25 AM
conhost.exe	62	New Monitor Applications Run with Administrator Rights Policy	7/21/20, 9:25 AM
opera_autoupdate.exe	58	Everything Monitor Policy	7/21/20, 10:25 AM
opera_autoupdate.exe	58	Run with Administrator Rights Monitor Applications Policy	7/21/20, 10:25 AM

The policy events are listed in a table grid and if you select an event, you can find discovered details on the right.

FILE NAME	# OF EVENTS	POLICY	LAST EVENT
launcher.exe	63	New Monitor Applications Run with Administrator ...	7/21/20, 10:25 AM
conhost.exe	62	New Monitor Applications Run with Administrator ...	7/21/20, 9:25 AM
opera_autoupdate.exe	58	Everything Monitor Policy	7/21/20, 10:25 AM
opera_autoupdate.exe	58	Run with Administrator Rights Monitor Application...	7/21/20, 10:25 AM
chrome.exe	53	Everything Monitor Policy	7/21/20, 9:30 AM
InstallAgent.exe	53	Run with Administrator Rights Monitor Application...	7/21/20, 11:35 AM
chrome.exe	52	Run with Administrator Rights Monitor Application...	7/21/20, 9:30 AM
launcher.exe	52	Everything Monitor Policy	7/21/20, 10:25 AM
launcher.exe	52	Run with Administrator Rights Monitor Application...	7/21/20, 10:25 AM
installer.exe	40	New Monitor Applications Run with Administrator ...	7/21/20, 10:25 AM
msfeedssync.exe	38	New Monitor Applications Run with Administrator ...	7/20/20, 7:38 PM
conhost.exe	37	Run with Administrator Rights Monitor Application...	7/21/20, 9:30 AM
installer.exe	31	Everything Monitor Policy	7/21/20, 10:25 AM
installer.exe	31	Run with Administrator Rights Monitor Application...	7/21/20, 10:25 AM
msfeedssync.exe	28	Run with Administrator Rights Monitor Application...	7/20/20, 7:38 PM

chrome.exe X

Policy
Everything Monitor Policy

Policy Description
This policy monitors the execution of all applications. Not recommend on more than a handful of machines.

Total Events
53

Create Filter

View File

The details provided are the application or process name that triggered the event and based on which policy the event was recorded, including a short policy description. You can also see how often this event has occurred.

Use the details view to either create a filter or view the file. If you choose to create a filter, you can also select to immediately add that filter to an existing policy.

Best Practices

In Privilege Manager the option to Send Policy Feedback is the main notification mechanism about application installation and execution on user endpoints. Using Send Policy Feedback is recommended while systems are in Event Discovery and Learning Mode. This helps administrators to gather data, analyze patterns, and then assign actions to application events retrospectively.

It is not recommended to use Event Discovery for all configurable options and all user endpoints all the time. Event Discovery in an established production environment should be targeted to not generate unnecessary and overwhelming amounts of data.

Privilege Manager isn't a SIEM tool, so it shouldn't be capturing events from every endpoint. On the Conditions tab of any policy, users can see what is being targeted. The Application Filters on the policies are typically built with the target file name (and with established naming conventions, the policies and filters are easier to filter and to determine what they are targeting). The Privilege Manager User role can be assigned to the employees who need to audit these policies. That role will give them the ability to read items in Privilege Manager but not make any changes. Those users, as needed, look at the policies to see what's being targeted and can then relay that information to administrators that need to know those details.

Privilege Manager should not be used to audit events on all endpoints, but small scope audit can be done. For those, an elevate policy can be copied and targeted to a specific user, machine, or very small group with send policy feedback. As long as it's a small sample, it shouldn't flood the database with events. This type of audit policy can be assigned to an AD group. Change what user or machine is in that group to change who/what is spot audited. It provides a small example of what is being elevated.

Privilege Manager includes policies to discover when an end user runs an application that requires administrative rights. Creating policies for any known applications and tasks should be first. Organizations are aware of applications that require elevated permissions to run or install. Collect any files that have already been identified and create policies targeting those applications.

Often different users have different rights on their endpoints, based by division, hierarchy, or other classifications. Privilege Manager can quickly inventory local groups and users. If current permissions are unknown, use Privilege Manager to discover which accounts have administrative permissions on each endpoint. Action can be taken to immediately remove suspicious or unwanted users and groups.

Understanding which users and groups have administrative rights, allows you to properly assess what permissions should exist on an endpoint.

Note: Do not elect to Send Policy Feedback for trusted applications for those specified groups that are cleared to use and install the applications.

Event Discovery

Event Discovery is Privilege Manager's process to determine which applications will require policies.

Based on your use cases, different Event Discovery policies should be enabled. Enable event discovery for the most common use cases like:

- applications that require elevated rights,
- installers, and
- processes that trigger a UAC prompt.

Privilege Manager admins will work through the results of Event Discovery and build policies targeting these applications. Admins will determine if a file should be added to an allow, deny, or elevation policy. If elevated, determine if the file will be silently elevated or if justification, approval, or another workflow will be required.

Add the applications that are discovered to policies with priorities to be triggered before Event Discovery. This will prevent those applications from continuing to be discovered by Event Discovery in the future.

Following this process will naturally clean up the results from Event Discovery.

Refer to [Discovery](#) in the Admin menu section.

Never Disable Event Discovery

Event Discovery is not a short process. It's an integral part of Privilege Manager. Once Event Discovery is enabled, it is never disabled.

Even after all policies have been built and all end user needs are met and the local admin groups are empty on all endpoints, you'll still want to know if there are new items that require elevated permissions. Or, after admin rights have been removed, you may want to setup Event Discovery to send feedback if someone runs an application in a context that is unexpected and highly suspicious.

What is discovered and who/which machines Event Discovery targets may change, but Event Discovery will always be used in some capacity.

Event Discovery will never be disabled – you will always want to discover new events that require elevated rights. Consider a maturity plan for Event Discovery.

- Begin by silently discovering applications and creating filters/policies.
- As policies are tightened, add a justification prompt for new items.
- When admin rights have been removed and policies are set, use an approval process or reputation check for newly discovered items.

Event Discovery cannot be sped up. Files will only be discovered when end users initiate a process. If a certain team has an application that is only used at the end of the quarter to finalize business, that application will only be discovered once it is run by the end user.

The scale can be adjusted to ensure the workload is manageable. Start small, understand the workload when the pipeline is slow, then scale to the workload that can be maintained.

Event notifications are helpful and important when administrators want to initially establish policies and to continually monitor the installation and execution of new/unknown applications.

For a production environment it is necessary to know when potentially dangerous applications are installed on a user endpoint. It is not important to be notified every time a white listed application is installed or run on a system.

Note: That means that silent elevation policies do not need an event notification and should not have Send Policy Feedback enabled. Information should only be given on application events that require a follow-up with actions.

Approval and justification policies always generate an event as required for an audit trail. These events cannot be subdued.

Self-elevation, deny list, and other events on an endpoint triggering UAC are part of the never-ending event discovery process in an organization.

Create policies that are used for a certain amount of time before they are revisited and potentially adjusted for current needs. Target specific systems or user groups with group specific policies. Once those requirements are set, define what events will need a follow-up action in your environment:

- What exceptions can be made if any
- When to use overrides
- What to block
- What to deny list.

For certain groups of users, it might also be an idea to target a specific machine routinely to use the data to fine-tune any policies that are enforced on the endpoint. Group policies based on existing groupings – AD OUs, AD user groups, SCCM groups, etc.

However, requirements and circumstances are not set in stone and revisiting existing and established policies is part of a best practice approach in PAM.

It is important for administrators to know when (and potentially why) deny listing policies are triggered. It indicates that employees are violating company policy. However, if this happens a lot, it might indicate that there is a business need for

this application and that the blocked software was not fully understood.

Send Policy Feedback

An UAC override policy allows a user to elevate a program not blocked by a deny listing or elevated by an allow list, by reentering their password to install/run, is a good candidate for sending policy feedback. It presents an exception to normal execution of programs as an unprivileged user. This type of event logging should be used to identify new programs to add to silent elevation policies if the frequency warrants, or to audit user usage to elevate items they shouldn't to mark them for blocking or follow up action.

Don't Send Policy Feedback

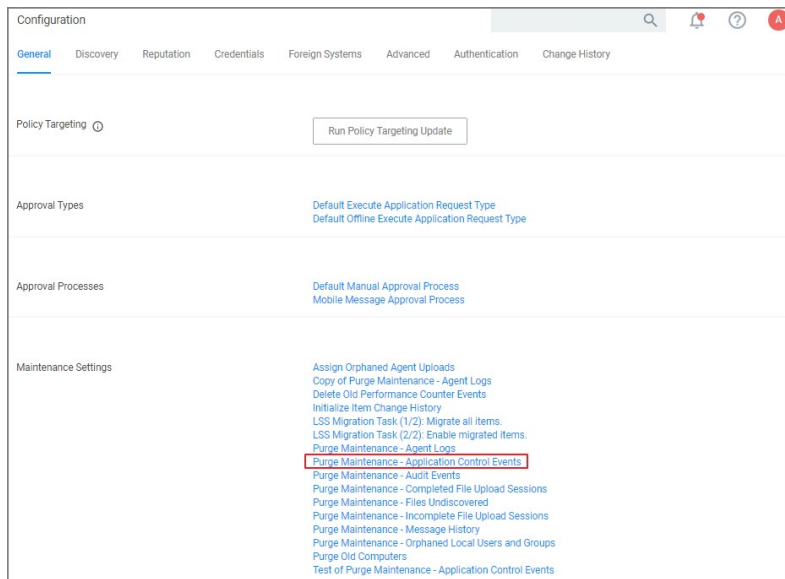
For most business organization it makes no sense to implement a policy that sends feedback when a MS Office product or the company wide instant messaging product is installed or run. For user groups like developers, programming tools are needed and running those should not trigger any notifications.

Events Maintenance

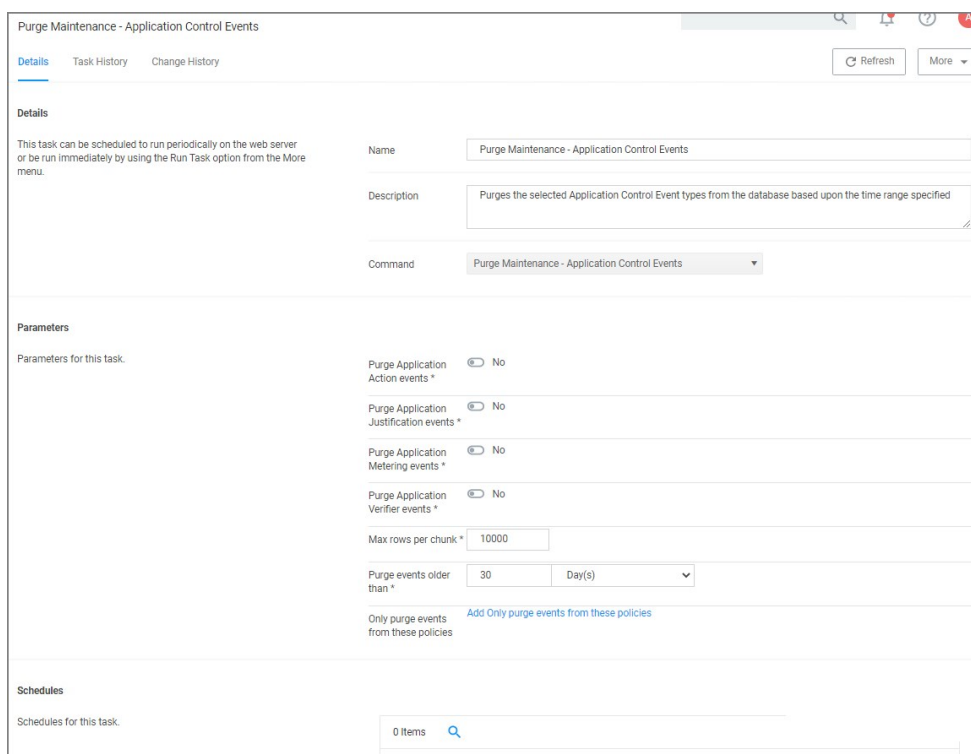
In Privilege Manager versions prior to 10.6, all events are stored unless **manually purged**. Event storage uses database space and can impact performance of dashboard queries so it is sometimes desirable to purge the stored events.

Privilege Manager version 10.6 and up, includes an option to specify the **maximum number of events** to be stored (rather than let the system continue to add events to be stored until manually purged).

1. Navigate to **Admin | Configuration** and select the **General** tab



2. In the **Maintenance Settings** section of this page, click on **Purge Maintenance - Application Control Events**.



The Description text explains what this feature does: "Purges the selected Application Control Event types from the database based upon the time range specified".

3. Under **Parameters**, set the switches and edit values based on how you want the maintenance to be performed for your instance.
4. Click **Save Changes**.

1. Navigate to **Admin I Configuration** and select the **Advanced** tab.

The screenshot shows the 'Configuration' page for 'Privilege Manager Server Monitor'. The 'Advanced' tab is selected. Under the 'General' section, the 'Maximum Application Event Count' is set to 1,000,000. This field is highlighted with a red box. Other settings include 'Save performance counters' (No), 'Load on Demand Flags' (31), 'Session Timeout' (720 minutes), 'Allow Agent Certificate Mismatch' (No), 'Prevent Legacy Agent Registration' (No), and 'Max time skew' (5 minutes).

The "Privilege Manager Server" section of the page shows the option "Maximum Application Event Count" and its default value, which is 1,000,000.

You can change the value, but storing a large number of events could cause database issues and slow down dashboard queries. Save your changes, if you edit the number.

Note: In the Cloud version of Privilege Manager, the Maximum Event Count cannot be changed by the user; it is fixed at its default value.

Maximum Event Count: Additional Information

The points below provide additional information about the Maximum Event Count:

- The count value is a total for all policies; it is not a per policy setting.
- The count is treated as a rolling window; if a new event would cause the count to exceed the maximum limit, the oldest event is removed.
- The manual purge, as described in a previous section, is still available.
- As mentioned in the previous section, the Maximum Event Count cannot be changed by the user in the Cloud version of Privilege Manager; there it is fixed at its default value.

Reports

Privilege Manager includes an array of reports. To access reports navigate to the top menu, click the Reports tab for a list of relevant out-of-the-box reports that span a spectrum of system activity and diagnostic information in Privilege Manager.

Click on the name of any of these reports to access details about your system.

Reports

Select Report Options

Actions

- Application Control Event Summary
- Application Justification Summary Details Report
- Summary of Application Actions by Mac Executable
- Summary of Application Actions by Product Name
- Summary of Application Actions by Win32 Executable
- Application Control Event Summary Acknowledgements
- Summary of Application Actions by Computer
- Summary of Application Actions by Operating System
- Summary of Application Actions by Product Version

Agent

- Agent Installation Summary
- Agent Summary by OS
- Managed Operating Systems
- Agent Installations
- Computers Without Agent Installations

Approvals

- Endpoint Group Member Authenticated Approvals
- Pending Execute Application Approvals
- Summary of Application Approval Requests by Computer
- Summary of Application Approvals and Denials
- Offline Approval Requests
- Summary of Application Approval Requests by Approver
- Summary of Application Approval Requests by User
- Summary of Application Approvals by Date

Detection

- All ActiveX Controls
- All Win32 Executables Report
- Discovered Files not Reported by File Inventory
- Files Pending Agent Discovery with no Discovery Agent
- All Mac OS Executables Report
- Application Verifier Logs
- File Security Rating Details Report

Diagnostic

- Agents missing a policy
- All policies not received by agents
- License Reservations
- Summary of Gauge States
- Agents missing current policy version
- Item Change History
- Product Licenses

Directory Services

- All Organizational Units Report
- Number of Computers in each Organizational Unit
- Directory Partners Report
- Users and Groups with Duplicate SIDs

Local Security

- All Computers with Managed Passwords
- Domain Groups as Local Administrators
- Password Disclosure History
- Summary of Users as Local Administrators
- Disclosure Summary (Local User)
- Local User/Group Summary
- Summary of Domain Users as Local Administrators

Security

- Application User Activity

The **Select Report Options** button lets users customize which of the default report options are shown on the Reports landing page.

Reports

Save Report Choices Cancel

Check the box next to the reports to have them appear on this page. Unselected reports will not appear.

Actions

- Application Control Event Summary
- Application Control Event Summary Acknowledgements
- Application Justification Summary Details Report
- Summary of Application Actions by Computer
- Summary of Application Actions by Mac Executable
- Summary of Application Actions by Operating System
- Summary of Application Actions by Product Name
- Summary of Application Actions by Product Version
- Summary of Application Actions by Win32 Executable

Agent

- Agent Installation Summary
- Agent Installations

By default all reports are listed on the Reports landing page. Use the switch to disable showing any given report.

Users can adjust the amount of data entries to display per page. When you adjust this number of rows on a page

Import Active Directory Data Agent Initialize

Command

10 items per page

Last updated: Jun 3, 2015 5:50:10 PM

The default number of data grid rows to display on pages across the Privilege Manager UI is set via [user preferences](#).

Privilege Manager reports can be exported via **CSV** and **PDF** export option buttons.

Filter Report
Refresh
CSV
PDF
Search

Once the **CSV** or **PDF** button is clicked, users can choose to

- export the current page or
- export all pages.

Configure Export Options

All Pages
 Current Page

Note: Selecting all pages might take some time to complete, depending on the overall size of the data records to export.

Reports and Queries

Each report in Privilege Manager runs a SQL query to return the results. The application does a great job opening the existing queries it uses and generating resolved queries to be used for testing.

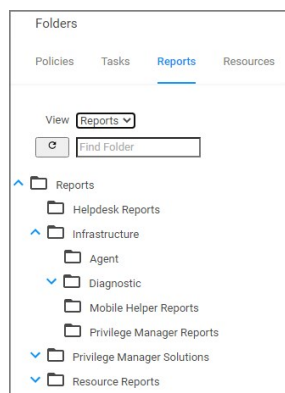
This makes it very easy to run Privilege Manager reports – including custom reports – outside of the application in SQL Server Reporting Services, SQL Server Management Services, or your favorite tool.

This topic gives an overview of finding and using the reports and SQL queries built-in to Privilege Manager.

Most users are probably familiar with the main Reports section of Privilege Manager, which is accessible from the menu at the top of any page. This page includes many common reports. There is a **Select Report Options** button on this page that allows a user to remove reports from this list.

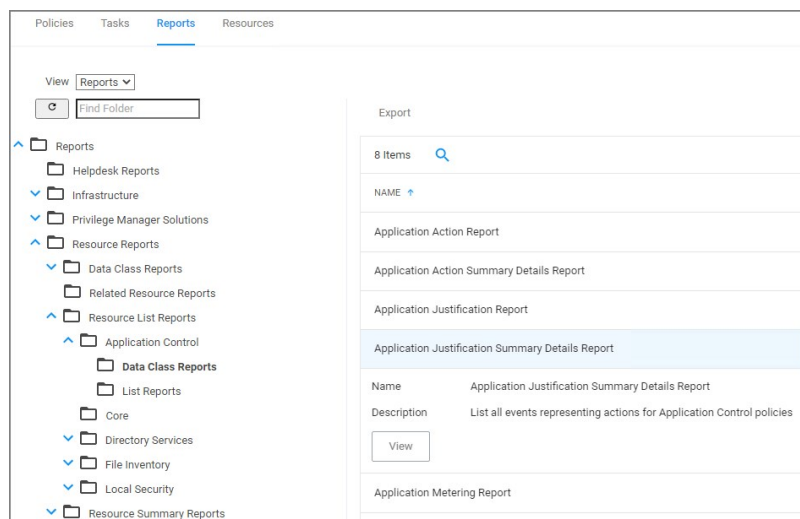
There are many more reports in the product.

To view all the reports in Privilege Manager, navigate to the **ADMIN | Folders | Reports** tab to see all the reports in a folder tree structure.



Expand the folder tree to explore the canned reports.

For example, to access the **Application Justification Summary Details Report**, navigate to **Reports | Resource Reports | Resource List Reports | Application Control | Data Class Reports** and select the **Application Justification Summary Details Report**.



Every report in Privilege Manager is a single XML object and references a separate XML object that contains the SQL query. By viewing the report object's XML, the SQL query object can be determined.

To view the report as an XML object, change the URL from:

[Your_TMS_URL]/PrivilegeManager/#!/item/_view_/9ba09fa5-ea7e-4352-8400-8eb58b8e4119

to:

[Your_TMS_URL]/PrivilegeManager/#!/item/_xml_/9ba09fa5-ea7e-4352-8400-8eb58b8e4119

st/TMS/PrivilegeManager/#/item/xml/9ba09fa5-ea7e-4352-8400-8eb58b8e41f9

[Back to Application Justification Summary Details Report](#)

Application Justification Summary Details Report

[Application Justification Summary Details Report](#)

```

1 <Report xmlns:adc="http://schemas.arelia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/
2 <adc:Description>List all events representing actions for Application Control policies</adc:Description>
3 <adc:FolderId>8f59f691-ec7-404c-8735-cb37a2423e69</adc:FolderId>
4 <adc:ItemId>9ba09fa5-ea7e-4352-8400-8eb58b8e41f9</adc:ItemId>
5 <adc:Name>Application Justification Summary Details Report</adc:Name>
6 <adc:ProductId>27bedb8a-d837-4d53-b748-bc6651461fe4</adc:ProductId>
7 <adc:State i:type="adc:ItemState">
8 <adc:CreatedById>2dee6e6e-5098-44ac-ad36-6a1ae8fefa7</adc:CreatedById>
9 <adc:CreateDate>
10 <dc:DateTime>2019-05-31T16:52:14.5247318Z</dc:DateTime>
11 <dc:OffsetInMinutes>-420</dc:OffsetInMinutes>
12 </adc:CreateDate>
13 <adc:EffectiveSecuredId>a063e1d4-1876-4b6a-938e-00c476942ade</adc:EffectiveSecuredId>
14 <adc:EffectiveSecuredInheritedId>95ba3b94-bce2-40e9-b390-c8172d58d7dd</adc:EffectiveSecuredInheritedId>
15 <adc:IsCreated>true</adc:IsCreated>
16 <adc:ModifiedById>c44ad59e-9b47-4869-a1f5-295bfbcf8f96</adc:ModifiedById>
17 <adc:ModifiedDate>
18 <dc:DateTime>2020-06-02T14:38:11.2085195Z</dc:DateTime>
19 <dc:OffsetInMinutes>-240</dc:OffsetInMinutes>
20 </adc:ModifiedDate>
21 <adc:VisualStateId>ff2353f8-5880-5824-97be-71c44f116156</adc:VisualStateId>
22 </adc:State>
23 <adc:Strings />
24 <adc:Tags />
25 <ChartViews />
26 <ChildAssociations>
27 <arr:anyType i:type="adc:ItemAssociations">
28 <adc:AssociationTypeId>d819ac6c-1a7a-54b9-bbc0-752162e298f4</adc:AssociationTypeId>
29 <adc:AssociatedItemIds />
30 </arr:anyType />
31 <arr:anyType i:type="adc:ItemAssociations">
32 <adc:AssociationTypeId>5b7800bc-7e4f-54ec-88b0-9797c09c5506</adc:AssociationTypeId>
33 <adc:AssociatedItemIds>
34 <arr:guid>9a3d82a3-c7be-47cc-aa1c-48acc7964620</arr:guid>
35 </adc:AssociatedItemIds>
36 </arr:anyType />
37 </ChildAssociations>
38 <DefaultDataPresentation>Table</DefaultDataPresentation>
39 <LastRunDateTime>0001-01-01T00:00:00</LastRunDateTime>

```

[Upload Items File](#)

Viewing an item as XML helps in determining what folder it is located in (which will be explained in more detail below). Viewing a report as XML also reveals the XML object for the SQL query.

Use your mouse to hover over the GUIDs in the XML to reveal the name of each GUID's object. Within the section for ChildAssociations, there will be an association for the Report's DataSource. Hovering over the GUID for the AssociatedItemid before the Report's DataSource will reveal the report's query.

In the screenshot below, hovering over the GUID is 9a3d82a3-c7be-47cc-aa1c-48acc7964620 identified that item as the **Application Justification Summary Details Report Query**.

```

26 <ChildAssociations>
27 <arr:anyType i:type="adc:ItemAssociations">
28 <adc:AssociationTypeId>d819ac6c-1a7a-54b9-bbc0-752162e298f4</adc:AssociationTypeId>
29 <adc:AssociatedItemIds />
30 </arr:anyType />
31 <arr:anyType i:type="adc:ItemAssociations">
32 <adc:AssociationTypeId>5b7800bc-7e4f-54ec-88b0-9797c09c5506</adc:AssociationTypeId>
33 <adc:AssociatedItemIds>
34 <arr:guid>9a3d82a3-c7be-47cc-aa1c-48acc7964620</arr:guid>
35 </adc:AssociatedItemIds>
36 </arr:anyType />
37 </ChildAssociations>
38 <DefaultDataPresentation>Table</DefaultDataPresentation>
39 <LastRunDateTime>0001-01-01T00:00:00</LastRunDateTime>

```

Application Justification Summary Details Report Query

Clicking on this GUID will open the XML for the query object in another tab on this same screen:

Application Justification Summary Details Report [Application Justification Summary Details Report Query x](#)

```

1 <DataSourceItemContract xmlns:adc="http://schemas.arelia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/
2 <adc:FolderId>b96eeb86-4846-45eb-9a36-504a3b70f774</adc:FolderId>
3 <adc:ItemId>9a3d82a3-c7be-47cc-aa1c-48acc7964620</adc:ItemId>
4 <adc:Name>Application Justification Summary Details Report Query</adc:Name>
5 <adc:ProductId>27bedb8a-d837-4d53-b748-bc6651461fe4</adc:ProductId>
6 <adc:State i:type="adc:ItemState">
7 <adc:CreatedById>2dee6e6e-5098-44ac-ad36-6a1ae8fefa7</adc:CreatedById>
8 <adc:CreateDate>
9 <dc:DateTime>2019-05-31T16:52:14.4153582Z</dc:DateTime>
10 <dc:OffsetInMinutes>-420</dc:OffsetInMinutes>
11 </adc:CreateDate>
12 <adc:EffectiveSecuredId>8449e8ae-908b-4205-802b-dcc09b57d756</adc:EffectiveSecuredId>
13 <adc:EffectiveSecuredInheritedId>17969920-3bc4-4a44-89c4-44b62aab01f8</adc:EffectiveSecuredInheritedId>
14 <adc:IsCreated>true</adc:IsCreated>
15 <adc:ModifiedById>c44ad59e-9b47-4869-a1f5-295bfbcf8f96</adc:ModifiedById>
16 <adc:ModifiedDate>
17 <dc:DateTime>2020-06-02T14:38:11.1205194Z</dc:DateTime>
18 <dc:OffsetInMinutes>-240</dc:OffsetInMinutes>
19 </adc:ModifiedDate>
20 <adc:VisualStateId>1199377a-1cbf-556d-a669-5effa21fa04c</adc:VisualStateId>
21 </adc:State>
22 <adc:Strings />
23 <adc:Tags />
24 <DataSource i:type="RawSqlDataSource">
25 <Name>Application Justification Summary Details Report Query</Name>
26 <Parameters>
27 <adc:Parameter>
28 <adc:DataType>System.String</adc:DataType>
29 <adc:DefaultValue mss:type="mss:string">EN</adc:DefaultValue>

```

[Upload Items File](#)

The XML object for the query includes the direct SQL query that the application runs. However, viewing the query in Privilege Manager will give better query results to work with.

The SQL queries can be viewed in Privilege Manager under **ADMIN | Folders**, but it will be helpful to know the folder in which a specific query is located. In the XML object for query, hover over and click on the GUID for the FolderId.

```

Application Justification Summary Details Report  Application Justification Summary Details Report Query x
1 <DataSourceItemContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arr="http://schemas.m
2 <adc:FolderId>b96eeb86-4846-45eb-9a36-604a3b70f774</adc:FolderId>
3 <adc:ItemId>9a3d82a3-c7be-47cc-aa1c-488c796444a4</adc:ItemId>
4 <adc:Name>Application Justification Summary Application Control Query</adc:Name>
5 <adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
6 <adc:State i:type="adc:ItemState">

```

This will open the XML for the folder in which the query is contained.

```

Application Justification Summary Details Report  Application Justification Summary Details Report Query x  Application Control x
1 <FolderContract xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsof
2 <Attributes>NoModify NoReplication NoDelete HiddenOnEmpty</Attributes>
3 <Description>Application Control Report Queries Folder</Description>
4 <FolderId>6fd3706a-d884-498d-a106-a318b9a61201</FolderId>
5 <ItemId>b96eeb86-4846-45eb-9a36-504a3b70f774</ItemId>
6 <Name>Application Control</Name>

```

Click on the FolderId to open the XML for its parent folder, and continue until reaching the root folder – which will not have a FolderId attribute. For the SQL queries, the root folder is Queries.

```

Application Justification Summary Details Report  Application Justification Summary Details Report Query x  Application Control x  Report Queries x  Queries x
1 <FolderContract xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsof
2 <Attributes>NoModify NoReplication NoDelete NoClone NoExport</Attributes>
3 <DefaultSecuredId>8449e8ae-908b-4205-802b-dcc05b57d756</DefaultSecuredId>
4 <ItemId>17969920-3bc4-4a44-89c4-44b62aab01f8</ItemId>
5 <Name>Queries</Name>
6 <ProductId>b409b2ea-d875-4888-9083-ef3c6a26ea52</ProductId>
7 <State i:type="ItemState">
8 <CreatedById>2dee66e6-5098-44ac-ad36-6a18e8fefe7</CreatedById>
9 <CreatedDate>
10 <dc:DateTime>2019-05-31T16:24:10.4879414Z</dc:DateTime>
11 <dc:OffsetMinutes>-420</dc:OffsetMinutes>
12 </CreatedDate>
13 <EffectiveSecuredId>8449e8ae-908b-4205-802b-dcc05b57d756</EffectiveSecuredId>
14 <EffectiveSecuredInheritedId>17969920-3bc4-4a44-89c4-44b62aab01f8</EffectiveSecuredInheritedId>
15 <IsCreated>true</IsCreated>
16 <ModifiedById>c44ad59e-9b47-4869-a1f5-295fbcf8f96</ModifiedById>
17 <ModifiedDate>
18 <dc:DateTime>2020-06-02T14:35:14.9025071Z</dc:DateTime>
19 <dc:OffsetMinutes>-240</dc:OffsetMinutes>
20 </ModifiedDate>
21 <VisualStateId>cdd5c56e-f271-5fb7-b3f4-f3ea92758f3e</VisualStateId>
22 </State>
23 <Strings />
24 <Tags />
25 <ChildAssociations>
26 <arr:anyType i:type="ItemAssociations">
27 <AssociationTypeId>8acc2635-d98e-575d-81e3-679e838ff98a</AssociationTypeId>
28 <AssociatedItemIds>
29 <arr:guid>69efc824-8c95-4717-925c-8c5f589bb4a</arr:guid>

```

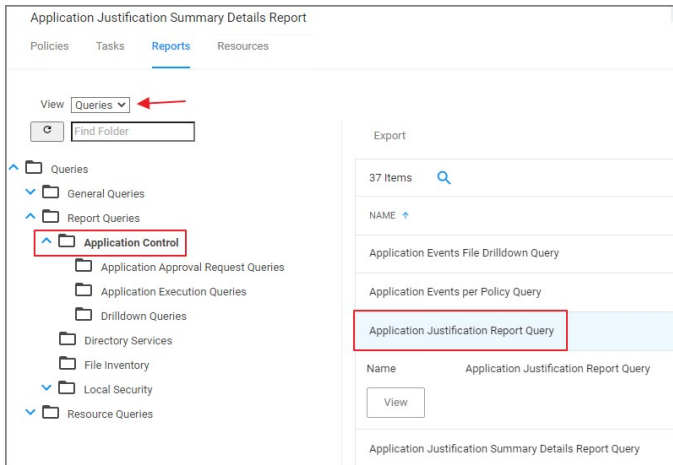
Edit

Upload Items File

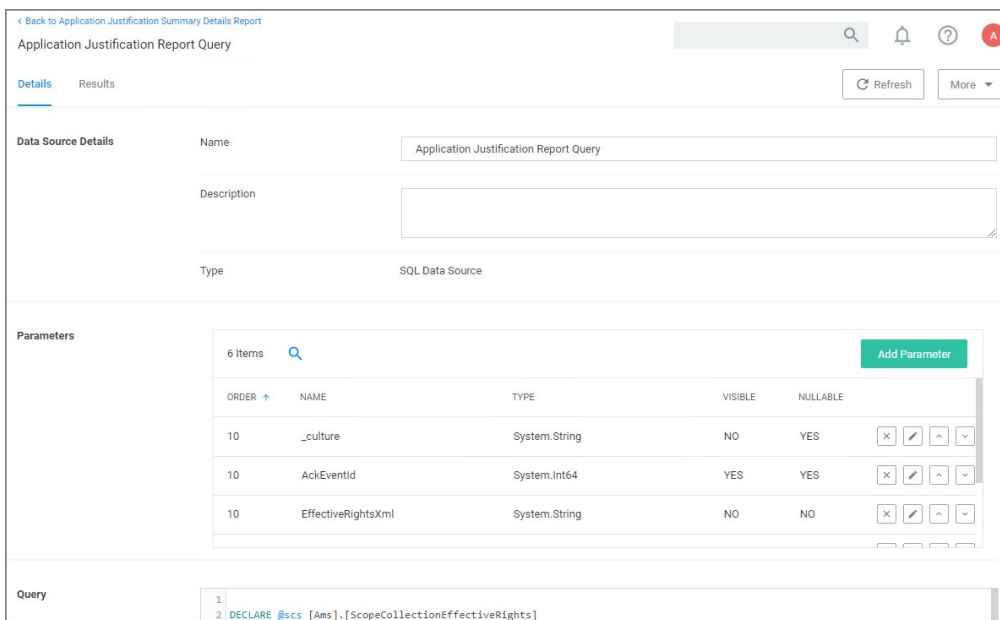
This XML view now shows the full folder location of this specific query: **Queries | Report Queries | Application Control**.

Access and Edit the Query from the Folder View

Navigate to **ADMIN | Folders** and select the Reports tab. From the View pull-down, select the Queries View. Then navigate the folder structure determined above: **Queries | Report Queries | Application Control**. Select the **Application Justification Report Query** from the center pane.



View this query object. The Query tab will show the SQL query that the application runs. This is the same query that appears in the XML of the object.



Scroll to the bottom section of the page to edit the query xml.

Resolved Query

The Resolved Query tab will give queries that can be used directly on the database to return the similar results that the application receives when it runs the query in the object. This makes it easy to run these queries – or customization of them – in SQL Server Reporting Services.

On the Resolved Query tab, checking the box to **Show Output as Executable Anonymous Block** will assign values to the Parameters the query uses. For the **Value Set** pull-down, select **Test** to assign the Parameters with appropriate values to run this query directly on your database.

Application Justification Report Query

Details **Resolved Query** Results Refresh More

Parameter Set:

Show as Anonymous Block: No

Copy To Clipboard

```

1
2 DECLARE @scs [Ams].[ScopeCollectionEffectiveRights]
3 insert into @scs select * from [Ams].[fnGetScopeCollectionEffectiveRights](@EffectiveRightsXml)
4
5 SELECT e._ItemId AS _ResourceId,
6        e.FileId AS _FileId,
7        e.UserId as _UserId,
8        fileItem.Name AS [File Name],
9        [Ams].fnGetLocalizedStringDefault('item.name', principal.ItemId, @_culture, principal.Name) [U
10       e.Executed,
11       e.Reason,
12       e.FilePath as [File Path],
13       _Date AS [Event Received]
14 FROM
15     [Ams.Event].Application_Justification e
16     LEFT OUTER JOIN [Ams].[Resource] R on R.[ResourceId] = e.[_ItemId]
17

```

Click **Copy To Clipboard** and then paste the resolved query in SSRS, SSMS, or your favorite tool.

Results

The Results tab provides options to change information of the query.

Application Justification Report Query

Details Resolved Query **Results** Refresh More

Parameters

Parameter Set:

AckEventId:

PolicyId *:

SummaryId *:

DataClassId *:

View Results

The parameters can be changed and specific item Ids can be entered.

Parameter Set:

- Default
- Default**
- Test
- Custom

AckEventId:

Change History Report

Administrators need to be able to look at changes done by other users in Privilege Manager. The need to be able to audit any issue causing changes to configuration settings, policies, filters, and actions. The new **Change History Report** allows Privilege Manager Administrators to track changes and their impact on endpoints.

As part of the audit the following information is recorded:

- User account initiating the change.
- Date/Time of the change.
- Description of the change made.

The following changes are reported:

- Configuration settings to Advanced, Discovery, and Reputation items (new tab on Configuration page)
- Changes to items, like
 - User and Group changes inside Roles
 - Credentials added or existing credentials updated
 - Foreign system added or existing updated
 - Any setting in the Advanced tab
- Changes to conditions of user editable resources.
- Policy, actions, filters, resource target changes, and additions (new tab on policy, actions, filters, resource target pages)
- Editing of task schedules (parameters and schedule of a task) - any change made to the schedule and parameters (New tab on task schedule page for each individual task)
- Imports and Saves of XML - differentiate between import and save

The reporting of any of these changes cannot be turned off and the results can be filtered by categories like Policy, Filter, Action, and Configuration.

Each save creates or adds to the revision history of items. The **Item Change History Report** cannot be used to revert to a previous state.

Item Change History					
Filter Report	Refresh	CSV	PDF	Search	
Drag column here for grouping					
Name	Operation	User	Date	Correlation ID	
New User Credential	CreateFromTemplate	Administrator	7/7/2020 9:10 AM	ed74b28d-999d-4a79-9141-3e691122b2a8	
Create inbound TCP firewall rule for Elevate Adding Inbound TCP Firewall Rule Privilege	CreateFromTemplate	Administrator	7/6/2020 11:00 PM	368940d4-94d9-4cee-8a8f-971f1808882c	
New Display Advanced User Message Action (MacOS)	Save	Administrator	7/6/2020 9:00 PM	3ca93080-bfa0-4e02-8cfa-277e2f05bab6	
New Display Advanced User Message Action (MacOS)	CreateFromTemplate	Administrator	7/6/2020 9:00 PM	6e1841e1-f2af-4c4d-af1f-6ee089e3088b	
Test of Application Denied Notification Action	Clone	Administrator	7/6/2020 8:24 PM	f96f463e-1c58-4058-b10f-2c81f3b24f09	
Copy of Deny Execute Message	Clone	Administrator	7/6/2020 8:07 PM	2b3ecc9f-5e52-4644-a488-854a07c1682b	
New Adjust Process Rights Action	Save	Administrator	7/6/2020 7:42 PM	c9675353-5e6e-4185-9e8f-18f9fa2956b	
New Adjust Process Rights Action	CreateFromTemplate	Administrator	7/6/2020 7:42 PM	c73da2d0-8fe5-4001-bae9-7ebe7c42b9a6	
New Set Process Security Descriptor	Save	Administrator	7/6/2020 7:24 PM	ec86ef31-4dfd-4692-b2dd-3aa633d69f84	
New Set Process Security Descriptor	CreateFromTemplate	Administrator	7/6/2020 7:24 PM	1b41a4cc-1651-4089-ab16-446c7b133ab4	

Domain Users in Administrator Group

You can get instant reports by clicking the Reports tab. To see which domain users are members of the administrators group, view the domain users as local administrators report.

Local Security All Computers with Managed Passwords Domain Groups as Local Administrators Password Disclosure History Summary of Users as Local Administrators	Disclosure Summary (Local User) Local User/Group Summary Summary of Domain Users as Local Administrators
---	--

Click the Summary of Domain Users as Local Administrators report to view details:

Reports > Summary of Domain Users as Local Administrators

Drag column here for grouping

Builtin	Account Type	Group Name	User Name	Computers
User Defined	Domain	administrators	anotheradmin	1
User Defined	Domain	domain admins	admin	1
User Defined	Domain	domain admins	admin@corp.it	1
User Defined	Domain	domain admins	anotheradmin	1
User Defined	Domain	domain admins	chuyngngasasnd	1
User Defined	Domain	domain admins	chuyngngasasnd	1
User Defined	Domain	domain admins	dev	1
User Defined	Domain	domain admins	dev	1
User Defined	Domain	domain admins	developer	1
User Defined	Domain	domain admins	jsquatch	1

Selecting any of the accounts listed, open the Drilldown report for that specific item:

Reports > Summary of Users as Local Administrators - Drilldown

Drag column here for grouping

Computer Domain	Computer	Builtin	Account Type	Domain	Group Name	User Name
name.yourdomain.com	GO-TEST-SYS	User Defined	Domain	TESTENV	domain admins	anotheradmin

Logon Session Summary Report

The Summary report for recent Logon Sessions.

1. Navigate to the Privilege Manager Dashboard.
2. In the Search field enter **Logon session**.

Search Results for Logon Session

10 Items Type: All

NAME	TYPE	MODIFIED	DESCRIPTION
Collect Windows Logon Events Client Task	Remote Client Task	6/2/20, 10:38 AM	Collects windows logon events for logon session logging
Logon Session - User Foreign Key	Data Class Association Type	6/2/20, 10:38 AM	
Logon Session Summary	Report	6/2/20, 10:38 AM	Summary report for recent Logon Sessions.
Logon Sessions	Folder	6/2/20, 10:38 AM	
Logon Sessions	Report	6/2/20, 10:38 AM	Basic report for recent Logon Sessions.
Logon Sessions Report Data Source	DataSource Item	6/2/20, 10:38 AM	
Logon Sessions Summary Report Data Source	DataSource Item	6/2/20, 10:38 AM	
Windows Logon Sessions	Data Class	6/2/20, 10:38 AM	Windows Logon Sessions
Windows Logon Sessions Data Class Provider	Report Provider	6/2/20, 10:38 AM	
Windows Logon Sessions Data Class Report	Report	6/2/20, 10:38 AM	

3. Click on **Logon Session Summary**.
4. The report contains the information for the Computer Name, User Name, total minutes and sessions.

Reports > Logon Session Summary

Filter Report Refresh CSV PDF Search

Drag column here for grouping

Computer Name	User Name	Total Minutes	Sessions
---------------	-----------	---------------	----------

Note: You can also run the **Collect Windows Logon Events Client Task** to get updated windows logon events for logon session logging.

1. Navigate to **Admin | Tasks | Client Tasks** and select **Local Security**.
2. Click the **Collect Windows Logon Events Client Task**.

Collect Windows Logon Events Client Task

Details Task History Change History Refresh More

Details

Remote tasks can be used to have a specific computer or group of computers do something immediately. In order to work, the server will need to be able to reach the endpoints to push the task, or endpoints will need a policy enabled to poll periodically for tasks.

Name: Collect Windows Logon Events Client Task

Description: Collects windows logon events for logon session logging

Command: Windows Logon Event Processor

Parameters

Parameters for this task. No parameters

Schedules

Schedules for this task.

0 Items

New Schedule

3. Run the task.

Performance Reporting

Performance Reporting is available for Privilege Manager 10.5 and up. Nightly tasks can collect performance information in the following reports:

- Item Processing Performance
- Processing Performance

1. Navigate to **Admin | Configuration**.
2. Select the **Advanced** tab.
3. Scroll to the **General** section, set the **Save performance counters** switch to yes.

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Privilege Manager Server

General

Save performance counters * Yes

Load on Demand Flags

4. Click **Save Changes**.
5. Once the **Save performance counters** box is checked, find the performance reports by searching for their names **Item Processing Performance** or **Processing Performance** in the search bar.

Search Results for Performance

22 Items Type: All

NAME	TYPE	MODIFIED
Delete Old Performance Counter Events	Powershell Script	6/2/20, 10:35 AM
Item Processing Performance	Report	6/2/20, 10:35 AM
Item Processing Performance Query	DataSource Item	6/2/20, 10:35 AM

6. Select the report you wish to view.

Item Processing Performance

Filter Report Refresh CSV PDF Search

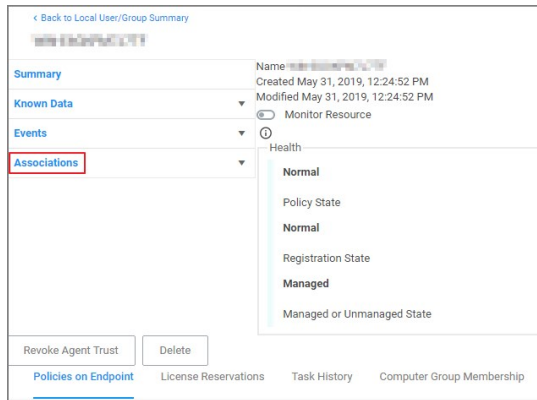
Drag column here for grouping

Name	Category	Total Time Ms	Count	First Event Start...	Last Event Com...	Average Ms	Events Per Seco...
fragment	bits	7	3	6/3/2020 3:18 PM	6/3/2020 3:20 PM	2	0
create-session	bits	5	3	6/3/2020 3:18 PM	6/3/2020 3:20 PM	1	0
close-session	bits	4	3	6/3/2020 3:18 PM	6/3/2020 3:20 PM	1	0
Configure Active Directory	gaugeupdate	85	3	6/3/2020 3:18 PM	6/3/2020 3:20 PM	28	0

Primary User

The primary user is calculated by the data reported from the Logon Session inventory policy. The primary user is considered to be the user with the most minutes on the machine.

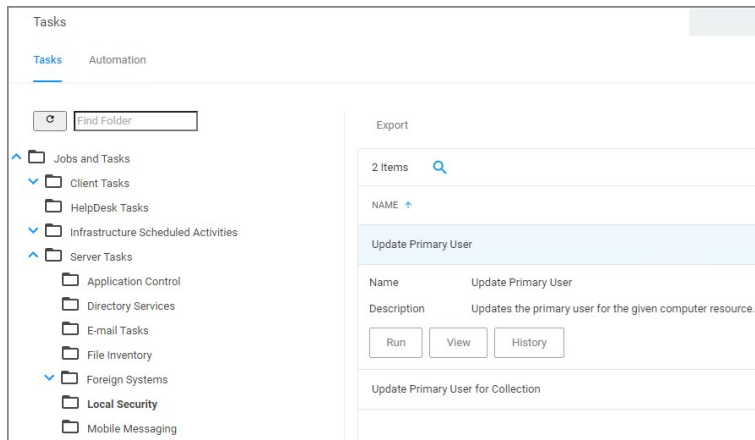
1. Navigate to your **Local User/Group Summary**.
2. Select the system for which you want to know the primary user.
3. Click on **Associations**.



4. This will display the **Computer Primary User**.

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **Admin | Tasks**.
2. Expand **Server Tasks**.
3. Click on **Local Security**.
4. From here you can run the **Update Primary User** or the **Update Primary User for Collection Task**.



Note: The Update Primary User Task only updates the primary user for a given computer resource.

Application User Activity

Auditing for user activities like logins and logouts can be viewed via the Application User Activity report. The report is a chronological data collection of user login/logout events and relating data.

To access the report navigate to **Reports** and locate the **Security** reports, select **Application User Activity**.

Time	Operation	Sub Operation	User	Source IP	Authenticated User	Authentication Type
Mon Mar 16 2020 14:38:08 GMT-0400 (Eastern Daylight Time)	Login		SYS-TESTING1\Administrator	123:123:123		NTLM Authentication

User activity auditing is by default enabled. The following auditing data is stored and provided via report:

- User resource ID.
- Username associated with the resource ID.
- IP address from the system used to login.
- Date and time of the login/logout.
- Activity information, like successful login, unsuccessful login, logout, etc.

The report can be distributed via standard Email Report task.

How to...

This topic is a collection of articles covering "How to..." procedures for different tasks.

- Best Practices:
 - [Disaster Recovery](#)
 - [Using a Service Account to run the IIS App pool](#)
 - [Prevent Read and Write Access to File Types or Locations](#)
 - [Securing the IIS Server](#)
- Import, Export, and Migration:
 - [Export Items](#)
 - [Import Items](#)
 - [Migrate Local Security Policies](#)
- Azure:
 - [Add Thycotic One Users Manually](#)
- Infrastructure
 - [Azure Service Bus Configuration](#)
 - [Setup High Availability/Clustering](#)
 - [Setup Reverse Proxy](#)
 - [Moving MS SQL Server Database for Privilege Manager and Secret Server Combined Installation](#)
 - [VM Deployments](#)
- macOS:
 - [Preference Pane Targeting on macOS](#)
- Maintenance:
 - [Export Items](#)
 - [Import Items](#)
 - [How to Purge Computers](#)
 - [How to Purge the Action Items Table](#)
 - [Using the Remove Programs Utility](#)

The following topics are available:

- [Disaster Recovery](#)
- [Active Directory Import](#)
- [Using a Service Account to run the IIS App pool](#)
- [Prevent Read and Write Access to File Types or Locations](#)
- [Securing the IIS Server](#)

Active Directory Import - On-prem vs Cloud

On-premises

The support for on-prem AD import is better than the support for Azure AD. On-prem AD import has more usable data. For customers that want to target computers based on OU or Security Groups, this is the best option. Our customers can setup an AD foreign system with credentials and import directly using LDAP.

Cloud

In a cloud environment the Privilege Manager server(s) typically don't have direct access to Active Directory. Instead the customer can select a local machine on which to install the Directory Services Agent. The agent retrieves information, and sends data to the server on a schedule.

Full vs Differential Synchronization

Unless otherwise specified, both the server and agent imports attempt a differential synchronization of AD data. AD keeps an Update Sequence Number (USN) that goes up as changes are made and resources are added. The following 3 conditions must be met for a differential sync:

1. Privilege Manager has a record of a prior sync with a session ID and USN.
 - o On the server these are recorded in the database as data for the foreign system in the [Ams.Data].[DirectorySync] table.
 - o For the agent they're recorded in the registry under HKLM\Software\Arellia\Agent\DirectoryServices\Imports. Users can force a full sync by deleting this data.
2. The directory partner (Domain Controller Server) must be the same. Starting with Privilege Manager version 10.8 and later, a server will be automatically picked if none is specified. But on older versions of the product, no differential sync is available unless the server is specified.
3. The LDAP query must be the same query as the hash is stored.

Assuming the conditions are met, Privilege Manager takes the given LDAP query, and appends a condition that the USN is greater than the recorded last USN.

NOTE: In test environments it's common to have a sync "fail" because the agent has done a sync prior on a different PM server. For a new environment setup with a Directory Services Agent, remember to clear out the registry record of syncs.

Expected Performance

If connectivity is good (low latency is just as important as high throughput), the main bottleneck is writing item data to the Privilege Manager database. Small ADs with a few hundred resources complete in a couple minutes. Large ADs with hundreds of thousands may take 10 hours or more.

Status

For imports run via the Directory Services Agent, Privilege Manager contains a report to give basic status named **Agent-Based Directory Services Import Status**

Directory	Agent	Started	Minutes Run...	Progress	Completed	Pending Chu...	Last Error
ARELLIA		11/3/2020 12:51 PM	10096	1/unknown	11/10/2020 1:07 PM	0	System Timeou... The operation has timed out.
ARELLIA		11/3/2020 1:20 PM	10076	1/unknown		0	
ARELLIA		11/3/2020 1:20 PM	10076	1/unknown		0	
ARELLIA		11/3/2020 1:25 PM	0	1/1	11/3/2020 1:25 PM	0	

When Privilege Manager runs an LDAP query, the number of results returned or how long the process will take is an unknown. The agent reports the data as it gets it in chunks to the server. The Progress field shows the number of chunks the server has successfully processed vs the total number. Typically what happens is that the agent finishes importing from AD before the server imports all the chunks. This shows at a minimum that there is progress.

Azure AD Imports

The primary reason for imports from Azure AD is to configure authentication in Privilege Manager.

Users/Groups

Importing users and groups from Azure AD works well for authentication, and usually plays well with data from other sources.

Import Azure AD Resources

This is the primary task users should run to import from Azure AD.

< Back to Tasks

Import Azure AD Resources

This item is read-only.

Details Task History Change History

Details

Name	Import Azure AD Resources
Description	This task will import devices, users, and groups from Azure AD.

Parameters

Parameters for this task.

Directory *	<input type="radio"/> No option selected
Import devices *	<input type="checkbox"/> No
Import groups *	<input type="checkbox"/> No
Import users *	<input type="checkbox"/> No

Import Specific Azure AD Users and Groups

This task allows users to import selected users and groups, instead of importing all.

< Back to Tasks

Import Specific Azure AD Users and Groups

This item is read-only.

Details Task History Change History Duplicate More

Details

Name	Import Specific Azure AD Users and Groups
Description	This task will import the specified users, devices, groups, and optionally child groups, users, and devices from Azure AD.

Parameters

Parameters for this task.

Azure AD *	<input type="radio"/> No option selected
Group display names	<input type="radio"/>
User names	<input type="radio"/>

NOTE: For groups the search filter is by display name. For users either display name or UPN can be entered (or a partial with *). This is a common point of trouble - users often use account names or other names that don't match the Azure AD data. When in doubt, open the Azure AD portal and make sure the display names match.

Device Import

At this time, importing devices (computers) from Azure AD is discouraged. The usable data for Privilege Manager is very limited, and there is basically only one way to link an Azure AD device to an existing computer resource in Privilege Manager and that by Device ID. Refer to [Azure AD - Device ID](#) in the troubleshooting topic. Unless the agent is reporting this data, there are guaranteed to be duplicates and/or resources that will not work to assign policies.

On-Premises vs. Cloud

Since Azure AD is itself a cloud service, there's basically no difference between our support on-premises and in cloud.

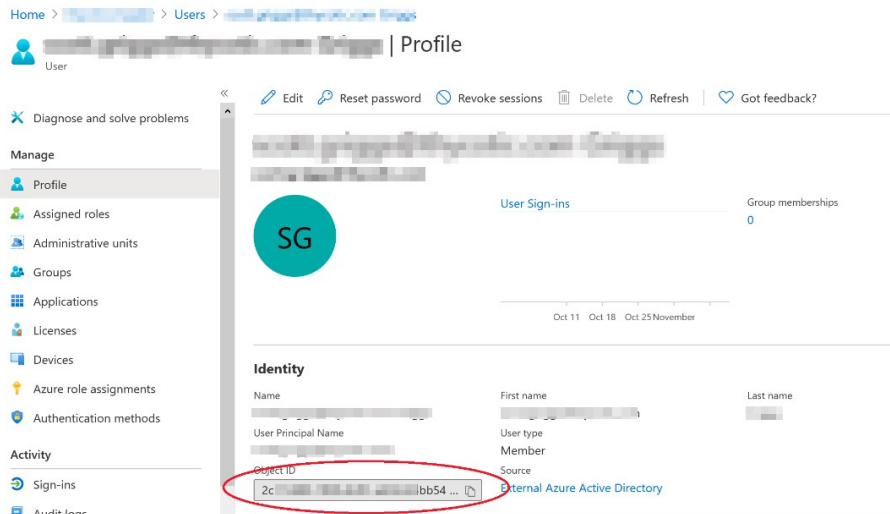
Troubleshooting AD Sync

Authentication

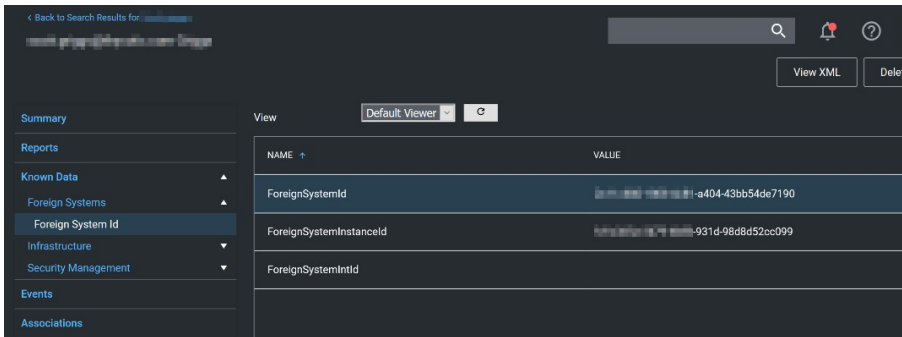
NOTE: Thycotic recommends that customers create a new user in Azure AD (one that is not sync-ed from AD) as a Privilege Manager *global administrator*. This user can be used as a backup access if other users fail to sync correctly.

When a user logs in to Privilege Manager with Azure AD, Privilege Manager gets back an object ID. A search of the database for that Object ID in Foreign System ID, provides what roles that user is a member of. The internal caching uses SID, so the user must also have a Global Account Details - SID. If there are any issues with the user authentication, it is recommended to check this data to make sure it exists, and make sure it matches the Azure portal data.

The object ID in the Azure portal:

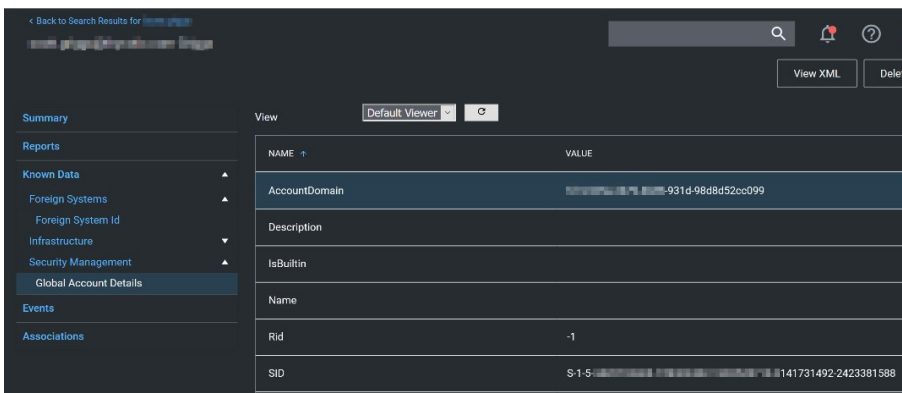


should match Foreign System ID in Privilege Manager:



NOTE: There may be multiple foreign systems entries here, when in doubt browse the Azure AD foreign system, not the GUID in the browser URL, and match that up in the list along with the object ID.

Users also need to have a Global Account Details - SID from the same Azure AD foreign system ID:



NOTE: There may be multiple entries here. If Privilege Manager doesn't have one where the AccountDomain matches the foreign system ID, that could potentially point to a problem.

Duplicates

The basic reason for duplicates is not having matching information when Privilege Manager imports resources, registers computers, or updates inventory.

Resource Type Keys

Privilege Manager identifies resources in several ways. The primary way is through "keys", which is basically just uniquely identifying data about a resource. Not all keys are available from all sources, so below each key is a table that lists availability.

Global Account Details - SID

This key is used to match computers, users, and groups based on the SID from their primary domain.

Availability

	Yes and No[^1]	Yes	Yes[^2]	N/A
Users	Yes and No[^1]	Yes	Yes[^2]	N/A
Groups	Yes and No[^1]	Yes	Yes[^3]	N/A
Computers	No	Yes	N/A	Yes[^4]

- [^1] Users and groups created natively in Azure AD will not have a SID.
- [^2] SID may not be available on all Azure AD systems. Users and Groups imported from AD will have a SID (by default, customers can change the settings in Azure AD Connect, so it's typical, but not a guarantee). Devices (computers) in Azure AD will typically not have this information.
- [^3] Starting with the 10.8 agent, when reporting AD domain users and groups that are members of a local group, the agent will include Global Account Details SID. But with older agents it's not reported, and this can be a likely source of duplicates.
- [^4] Starting with the 10.8 agent, when registering the agent will report its SID from the domain to which it's currently connected. Agents that are offline will cache this information for a period of time, but agents long disconnected from the domain will not be able to report this.

Global Windows Users - User Id & Domain Name

This is the key that has the longest history of use in Privilege Manager.

Availability

	No[^1]	Yes	Yes	N/A
Users	No[^1]	Yes	Yes	N/A
Groups	No[^1]	Yes	Yes	N/A

Computers	No	Yes	N/A	Yes
-----------	----	-----	-----	-----

[^1] Azure AD can be configured (Azure AD Connect) to report this information for users and groups, but we don't read it when importing. This is planned as a future product update.

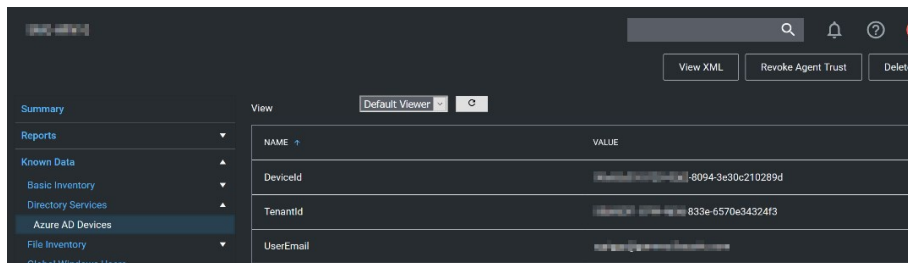
NOTE: Until recently, the agent didn't report SID for domain users and groups. So the agent would report users with name/domain, import from Azure AD would report SID, since there wasn't common data, this was a common source of duplication.

There are a couple of solutions to duplicates here:

1. Also run an import from AD (typically on-premises AD agent), and then run the task "Merge Duplicate Account SID Resources". Note that this will not work for computers - we can't get SID for computers from Azure AD.
2. Delete the duplicates. When you delete duplicates, delete the resource that is not an agent, and with the least information.

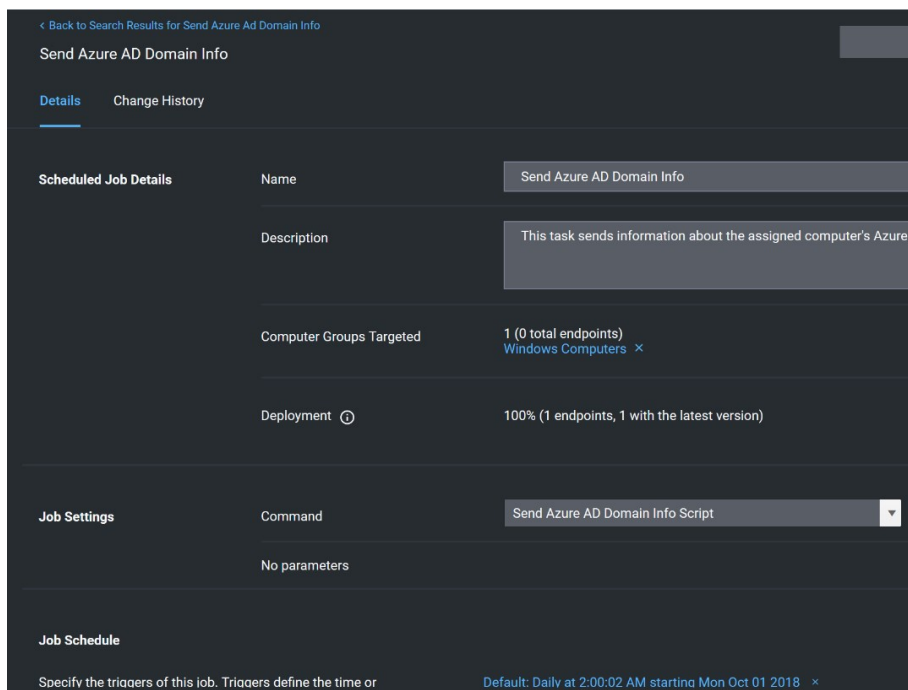
Azure AD - Device ID

This data was added in an attempt to support importing devices from Azure AD. The agent will report Azure AD domain join info which includes Device ID and Tenant ID, and when importing from Azure AD Privilege Manager will attempt to match existing computers before creating a new one.



Send Azure AD Domain Info

This is the agent-scheduled task that reports the Azure AD info, by default it runs at 2AM daily.

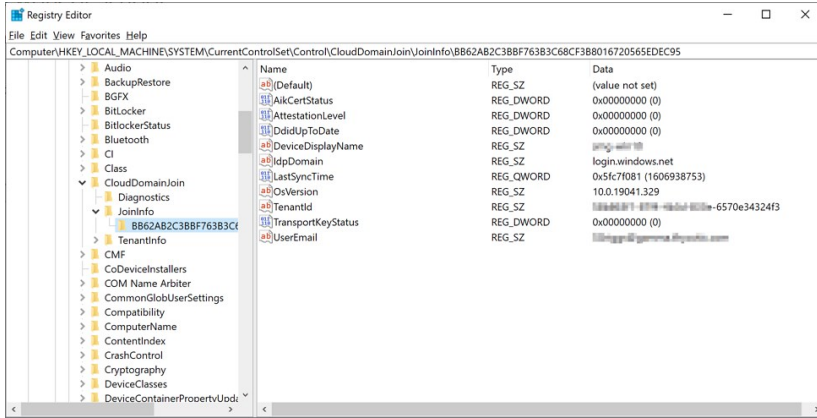


Limitations

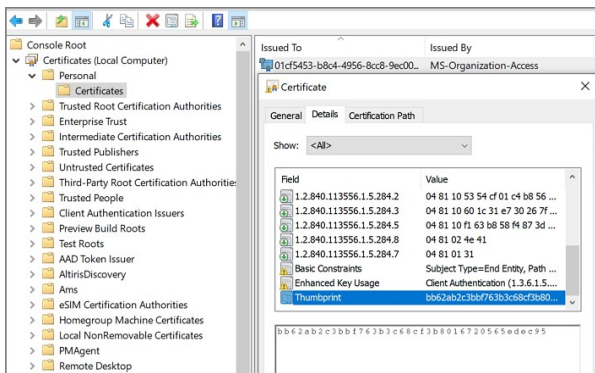
Unfortunately this data is limited to a very specific domain join. Hybrid domain joins (both AD and Azure AD) don't seem to support this. When using hybrid join, all the data seems to be per-user, and currently the agent task to report info only works if the data is global.

Registry/Certificates

If you want to troubleshoot why an agent isn't reporting this domain join info, you can follow in the registry to check the data for yourself. Go to HKLM\System\CurrentControlSet\Control\CloudDomainJoin\JoinInfo. The keys there are named by the hash of the relevant certificate (the image below is for a local user (the one that doesn't work), but the concept is the same):



In this case 6A901B... is referencing a certificate. The certificate will be in the local machine, personal store (again, the image below is actually for a user's cert, but the concept is the same):



So we find the certificate with thumbprint 6A901B... and its subject, in this case "58b863f1-87f4-4b3d-833e-6570e34324f3" is what will be reported, and what we can match up to the Device ID in Azure.

Privilege Manager Disaster Recovery

Any disaster recovery plan needs to include contingency plans for the event when a company's data center goes down, as such, it should always include storing backups of the latest web application and database offsite, potentially at multiple locations.

For Privilege Manager web application backups, Thycotic recommends creating a copy following any install/upgrade. For the database backups, SQL database backup recommendations should be followed.

Maintaining Privilege Manager in a Disaster

With Privilege Manager environments three types of Disaster recovery strategies can be implemented. The framework of a solid Privilege Manager Disaster Recovery Plan should follow these methods of maintaining operations:

- manual backups to restore (restoring/rebuilding from backup)
- passive failover (built and ready, but with a few manual switches)
- active fail-over via High Availability setup. Privilege Managers licensing allows for full clustering.

As a best practice for Privilege Manager databases, we recommend asynchronous replication. There are a lot of transactions - too many transactions for synchronous replication in most enterprise environments. Asynchronous replication works with a manual failover.

Simple Installation and Architecture

Privilege Manager operates on typical modern servers On-Premises, in the Cloud, and in virtual environments.

By design, Privilege Manager's installation is a quick and easy process. Keeping this process as quick and easy to install was a goal from the outset. This serves as a viable fallback option should redundancy plans fail. In a worst-case scenario where the host server fails, a cluster/mirror fails, and the other backup plans fail, Privilege Manager can be installed from scratch quickly and data imported from various methods.

Administrators familiar with Microsoft SQL and IIS can typically install Privilege Manager in about 30 minutes on a prepared server.

Refer to the following installation topics:

- [Privilege Manager Product Installation - Basic](#)
- [Privilege Manager Manual Installation](#)

Restoring from Backup

Thycotic recommends to make a back-up copy of your Privilege Manager web application folder after installation or following an upgrade. This back-up copy is used during disaster recover to restore the instance. Microsoft SQL database restores are simple as well, but require several steps, depending on the backup scenario. Refer to vendor details, such as [Back Up and Restore of SQL Server Databases](#).

Start by preparing servers for installation. When the servers are prepared, restore the Privilege Manager application on one and the database on the other. Some specific web configurations may be needed to match the previous IIS settings.

Restoring Privilege Manager from a Backup

When restoring from backup in the single-server configurations, be certain to make copies of the backup files on a different device or media.

Follow instructions as detailed under [Installing as a Virtual Directory](#).

High Availability

A Privilege Manager implementation based on a high availability setup plays well with any disaster recovery plan.

With HA clustering, there are more than one front-end web servers, and more than one active node. Allowing users to use Privilege Manager through more than one active node simultaneously requires enabling clustering within the application. Only one server handles background processes, meaning that one of the active nodes will be designated as the Primary Node at any given time (this can be changed manually, if necessary, in the application). In the event that the Primary Node becomes unavailable, the "Primary" status will be transferred to one of the other active nodes and users can continue using the application without interruption. There can be more than one active and passive server nodes (no limit), depending on the needs of the organization.

A Disaster Recovery Plan for High Availability consists of failover for Web Server or Microsoft SQL Server issues. If the failover members were to themselves fail, then Web Application Backups and Automated Application Database Backups can be used to restore functionality. If these Servers are virtualized, leveraging strategies such as making scheduled Snapshots or having a hot/cold Site may add additional layers of redundancy.

Refer to [Privilege Manager High Availability Setup](#).

Summary & Additional Support Resources

The integration of Privilege Manager into Business Continuity Planning should not present any unique challenges beyond normal server and database recovery. If your organization already has disaster recovery plans for servers and databases, Privilege Manager and its Microsoft SQL database should fit within your organization's current framework. Using server virtualization to assist with Business Continuity and Disaster Recovery in terms of snapshots, replication, and other 3rd party features are recommended where applicable.

Thycotic recommends setting up a domain service account that can both:

- access the Thycotic product's SQL database
- run the IIS Application Pool(s) dedicated to your Thycotic product

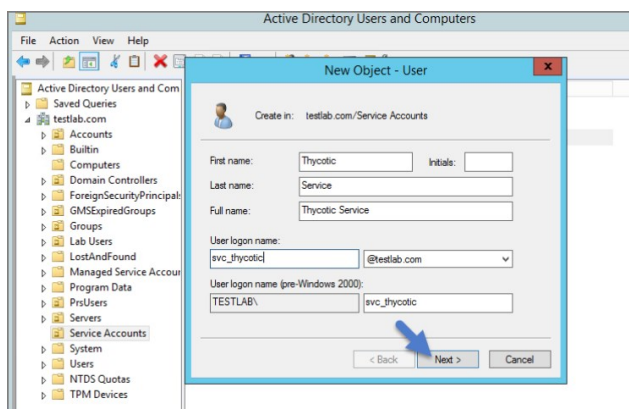
Note: The service account created in this KB should NOT be the same account that is created during the installation of SQL and used to manage SQL as a whole.

To set up this service account correctly you will need to:

1. Create a service account in Active Directory that will be dedicated to your Thycotic product (Domain).
2. Grant the service account access to the SQL Server database (Database).
3. Assign the service account as Identity of the Application Pool(s) in IIS (Web).
4. Grant folder permissions for the service account on two folders (Web).
5. Configure User Rights Assignment to the service account (Domain AND/OR Web).

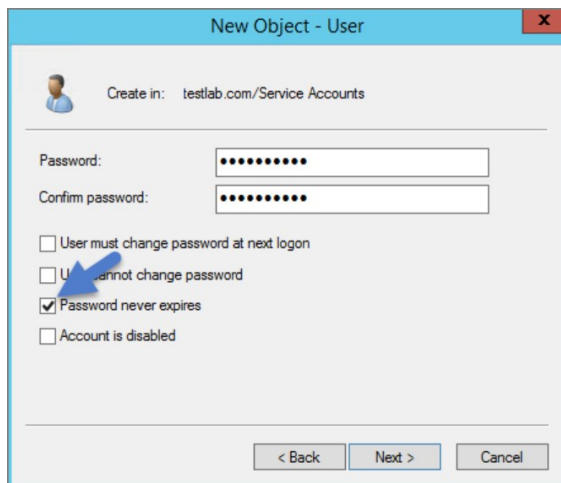
Creating a Domain Service Account

1. Open the **Active Directory Users and Computers** link from Administrative Tools.
2. Right-click the directory where you want to assign this account (i.e. testlab.com > Service Accounts).
3. Click **New and User**.
4. Add a name and logon name for the service account.
5. Click **Next**.



6. Enter a password.

Note: Uncheck "User must change password at next login if checked." Check Password never expires or the account could lock you out of Secret Server.



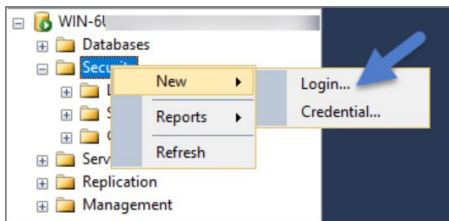
7. Click **Next**.
8. Click **Finish**. This account can now be given access to the database server and the application server.

Granting Access to SQL Database

You must have SQL installed on your database server before completing these steps:

1. Using SQL Management Studio (on your database server), connect to your Thycotic product's SQL Database using an Administrator account.
2. Right-click on the Security node (Ensure this is the top most Security node under the instance and not under the database name itself).

3. Click **New** and **Login**.

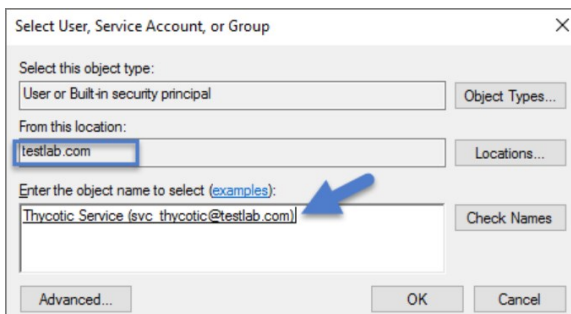


4. Ensure Windows Authentication radio button is selected.

5. On the New Login page click Search... Ensure that your domain/AD server is selected as the location.

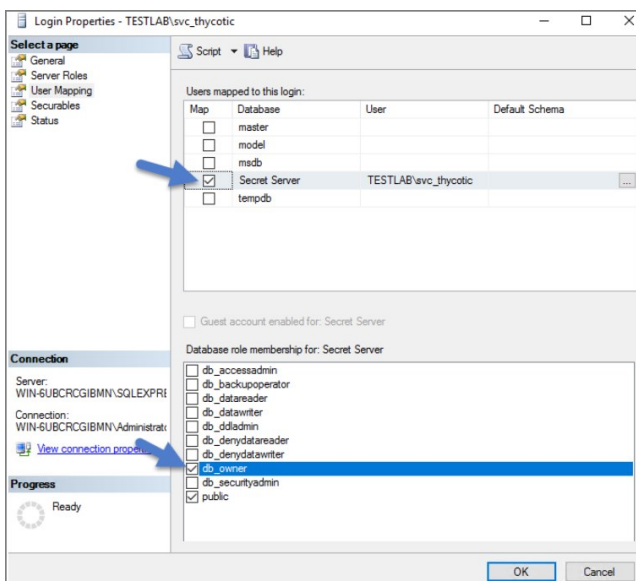
6. In the "Enter the object name to select" box enter the Login name created for your Thycotic service account (e.g., "svc_thycotic"). Click Check Names and select the correct account.

7. Click **OK**



8. If you have already created the database for your Thycotic product, under User Mappings select the database and check the box to grant the db_owner permission (example pictured below). OR - If you have not yet created the Database, Under Server Roles select db_creator

9. Click **OK**

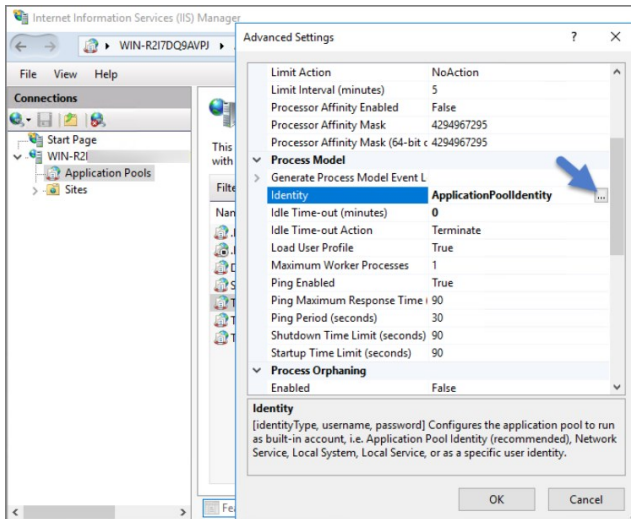


Assigning Identity of Application Pool(s) in IIS

1. Open IIS on your web server **Search I inetmgr**.

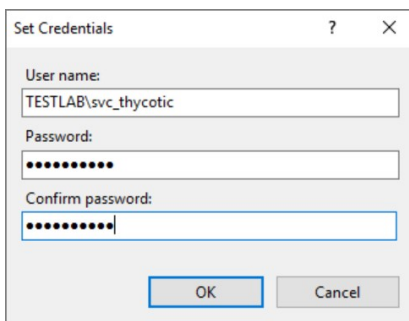
2. Locate the application pool(s) that your Thycotic product is using, right-click Advanced Settings.

3. The Identity box in the **Process Model** section, click the three dots on the right of the box.



4. Select the Custom Account radio button.
5. Click **Set** and enter your service account's name and password.
6. Click **OK**

Note: You will need to perform this step for multiple application pools for Privilege Manager.



Granting Folder Permissions

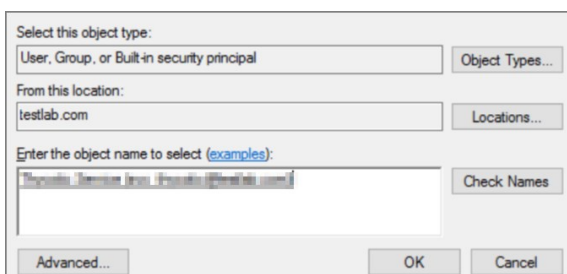
You must have the Thycotic product application files installed (on your web server) before completing this section.

Following the steps below you will need to give the service account **Modify** access to two folders:

- C:\Windows\TEMP
- The folder where your Thycotic product's application files are located (i.e.: C:\inetpub\wwwroot\SecretServer)

You must have the Thycotic Product Application Files installed on your web server before completing these steps.

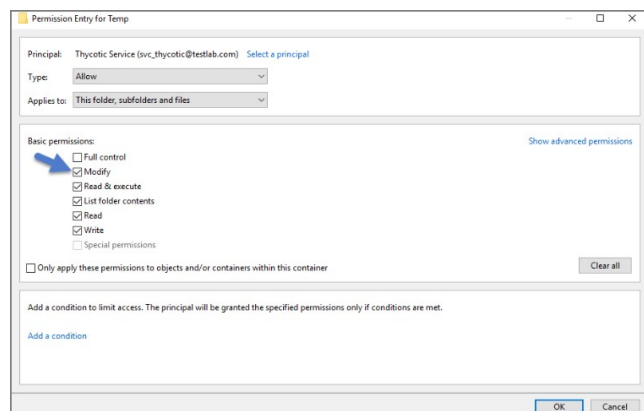
1. Open C:\inetpub\wwwroot\TMS and right-click the folder you are modifying.
2. Click **Properties** | **Security** | **Advanced**
3. Click **Add** and then select a principal.
4. Ensure the domain machine is listed as the Location and type the service account under the "Enter the object name to select" box, click Check Names and Enter network credentials for accessing your domain machine.
5. Click **OK**



6. Click the **Modify** checkbox.

Your service account should now have Modify, Read & execute, List folder contents, Read, and Write permissions for this folder.

7. Click **OK**, then **Apply**.



Note: If a Windows Security pop-up appears, click Yes. The service account will now be able to access this folder.

Note: The application folder only needs Write and Modify permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Configuring User Rights Assignment

The following settings are required for Thycotic Secret Server to function:

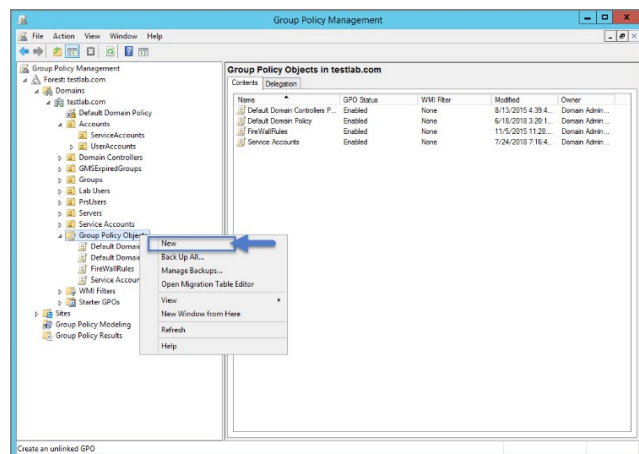
- Log on as a batch job
- Impersonate a client after authentication

You can adjust these settings either

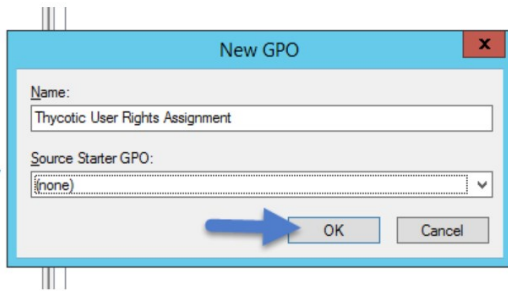
- At the Domain level using Group Policy
- Locally on your IIS Web Server using the Local Security Policy Console

Setting User Rights Assignment on the Domain

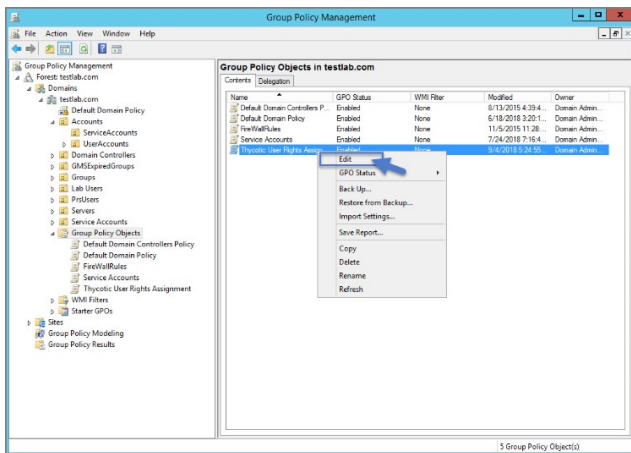
1. Open Group Policy Management Console and right-click your preferred GPO container (i.e. Group Policy Objects).
2. Click **New**.



3. Name the new GPO (i.e. Thycotic User Rights Assignment).
4. Click **OK**.
5. Right-click **new GPO**.
6. Click **Edit**.
7. Expand **Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies**.
8. Click **User Rights Assignment**.
9. Right-click **Log on as a batch job** and click **Properties**.



10. Ensure that the **Define these policy settings** box is checked
11. Click **Add User or Group**
12. Add your Thycotic Service Account.
13. Click **OK** then **Apply**.



14. Grant **Impersonate a client after authentication** permission to the service account under "User Rights Assignment" the same way "Log on as a batch job" was assigned above.
15. Link your new GPO to the OU where your Thycotic product machine accounts exist (web + database servers).

Note: This will overwrite any configuration in the local security policy. Utilizing the local security policy is a safer option if you are not sure about your usage across your domain.

Setting User Rights Assignment Locally

1. On the web server hosting IIS and your Thycotic Application files.
2. Open **Local Security Policy Console** (Run as administrator).
3. Expand **Local Policies | User Rights Assignment**
4. Right-click **Log on as a batch job | Properties | Add User or Group**.
5. Select your Thycotic Service Account and then click **OK**.
6. Do the same to set Impersonate a client after authentication.

Note: If you get a **Service Unavailable** after applying "Log on as a batch job" permissions, try updating your group policy settings:

1. Open the Command Console.
2. Type in **gpupdate /force**.
3. Restart the Windows Process Activation Service.

You can restrict access to specific file types or locations using Privilege Manager. To prevent read / write access to file types or locations, do the following steps:

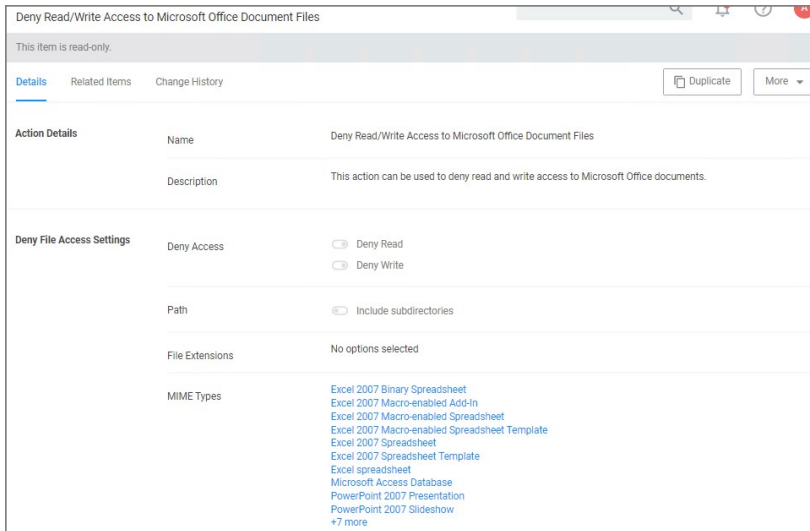
- Create a Deny File Access Action
- Create an Application Control Policy to which you will add the Deny File Access Action
- Test the privilege reduction you've just created

In the following scenario you will create a Microsoft Word document and save it on your machine to:

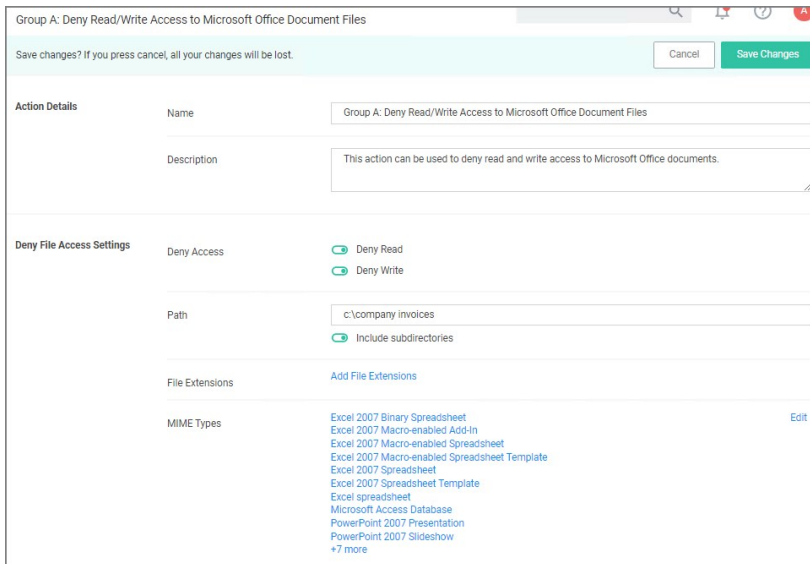
c:\company invoices\invoice 101.doc

Create a Deny File Access Action

1. Navigate to **Admin | Actions**.
2. Search for **Deny File Access Action**.
3. Click on **Deny Read/Write Access to Microsoft Office Document Files**.



4. Click on **Duplicate**.
5. Name the new copy of the action and click **Create**.
6. Enter the path of the file location (e.g., c:\company invoices), for our example we also set the switch to include subdirectories.



7. Click **Save Changes**.

Create an Application Control Policy

1. Under your Computer Group select **Application Policies**.

2. Click **Create Policy**.
3. Select **Skip the wizard, take me to a blank policy**.
4. Add Name and Description, click **Create Policy**.

Group A: Deny Read/Write Access to Microsoft Office Document Files Policy

General Policy Events Change History Inactive Refresh More ▾

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) [Add](#)
Windows Computers x

Deployment Not deployed (Policy is inactive)

Last Modified Jul 23, 2020, 6:58:59 PM by WIN-E6GKPM7J7TF\Administrator

Priority *

Description

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted [Add Applications Targeted](#)

Inclusions [Add Inclusions](#)

Exclusions [Add Exclusions](#)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc.

Audit policy events reports all application executions back to Privilege Manager's server for this policy [Actions](#)

Child Actions [Add Child Actions](#)

Audit Policy Events Record all activity detected by this policy in [Policy Events](#)

5. Under **Conditions | Applications Targeted**, click **Add Application Targeted**.
6. Search for **word** and add the **MS Word** filter.
7. Click **Update**.
8. Under **Actions**, click **Add Actions**.
9. Search for and add your **Deny Read/Write Access to Microsoft Office Document Files** Action.
10. Click **Update**.

Group A: Deny Read/Write Access to Microsoft Office Document Files Policy

General Policy Events Change History Inactive Refresh More

Policy Details

Add or update the computer group(s) this policy applies to and change the order that this policy is evaluated when an application executes on the endpoint.

Computer Groups Targeted 1 (1 total endpoints) [Windows Computers](#) x [Add](#)

Deployment Not deployed (Policy is inactive)

Last Modified Jul 23, 2020, 7:08:56 PM by WIN-E5GKPM7J7TF\Administrator

Priority * 65

Description Group A: .doc file deny

Conditions

Add or update the filters this policy will use to target applications. Optionally apply filters to explicitly include and/or exclude applications, processes, users, etc. [Filters](#)

Applications Targeted [MS Word](#) [Edit](#)

Inclusions [Add Inclusions](#)

Exclusions [Add Exclusions](#)

Actions

Add or update the action(s) applied to the applications processes and child processes like deny, add admin rights, display an approval or justification prompt to the end user, etc. Audit policy events reports all application executions back to Privilege Manager's server for this policy [Actions](#)

Actions [Group A: Deny Read/Write Access to Microsoft Office Document Files](#) [Edit](#)

Child Actions [Add Child Actions](#)

Audit Policy Events Record all activity detected by this policy in [Policy Events](#)

11. Click **Save Changes**.
12. Set the Inactive switch to **Active**.
13. Next to Deployment, click the **I** icon and run the **Resource and Collection Targeting Update**. After you run update, the appropriate endpoints will receive the new policy.

Test Access

Verify that the restricted access you set up was successful by applying the following tests:

- In Microsoft Word, open C:\company invoices\invoice 101.doc. The file is read only and can't be modified.
- Create a new document and attempt to save it to c:\company invoices\ . You will be unable to open it and will receive a File Permission error.
- Verify that you can create or modify a Word document in a different directory.
- In Microsoft Excel, save a spreadsheet to c:\company invoices\invoice 101.doc. The permissions are limited to Microsoft Word.

This is a list of items that IIS admin can implement to secure the IIS/Web server.

Patches and Updates

Run Microsoft Baseline Security Analyzer on a regular interval to check for latest operating system and components updates.

The latest updates and patches are applied for Windows, IIS server, and the .NET Framework. (These should be tested on development servers prior to deployment on the production servers.) Check the Microsoft Security Updates at <https://docs.microsoft.com/en-us/security-updates/> on a regular interval for up to date Microsoft technical security notifications.

Services

- Unnecessary Windows services are disabled.
- Services are running with least-privileged accounts.
- FTP, SMTP, and NNTP services are disabled if they are not required.
- Telnet service is disabled.
- ASP.NET state service is disabled and is not used by your applications.

Protocols

- WebDAV is disabled if not used by the application OR it is secured if it is required.
- TCP/IP stack is hardened.
- NetBIOS and SMB are disabled if not used (closes ports 137, 138, 139, and 445).

Accounts

- Unused accounts are removed from the server.
- Windows Guest account is disabled.
- Administrator account is renamed and has a strong password.
- IUSR_MACHINENAME account is disabled if it is not used by the application.
- If your applications require anonymous access, a custom least-privileged anonymous account is created.
 - The anonymous account does not have write access to Web content directories and cannot execute command-line tools.
- ASP.NET process account is configured for least privilege. (This only applies if you are not using the default ASPNET account, which is a least-privileged account.)
- Strong account and password policies are enforced for the server.
- Remote logons are restricted. (The "Access this computer from the network" user-right is removed from the Everyone group.)
- Null sessions (anonymous logons) are disabled.
- No more than two accounts exist in the Administrators group.

Files and Directories

- Files and directories are contained on NTFS volumes.
- Web site content is located on a non-system NTFS volume.
- Log files are located on a non-system NTFS volume and not on the same volume where the Web site content resides.
- The Everyone group is restricted (no access to Windows\system32 or Web directories).
- Web site root directory has deny write ACE for anonymous Internet accounts.
- Content directories have deny write ACE for anonymous Internet accounts.
- Remote IIS administration application is removed.
- Resource kit tools, utilities, and SDKs are removed.

Shares

- All unnecessary shares are removed (including default administration shares).
- Access to required shares is restricted (the Everyone group does not have access).
- Administrative shares (C\$ and Admin\$) are removed if they are not required.

Ports

- Internet-facing interfaces are restricted to port 80 (and 443 if SSL is used).
- Intranet traffic is encrypted (for example, with SSL) or restricted.

Registry

Remote registry access is restricted.

SAM is secured (HKLM\System\CurrentControlSet\Control\LSANoLMHash).

Auditing and Logging

- Failed logon attempts are audited.
- IIS log files are relocated and secured.
- Log files are configured with an appropriate size depending on the application security requirement.
- Log files are regularly archived and analyzed.
- Access to the Metabase.bin file is audited.
- IIS is configured for W3C Extended log file format auditing.

Sites and Virtual Directories

- Web sites are located on a non-system partition.
- "Parent paths" setting is disabled.
- Potentially dangerous virtual directories, including IISamples, IISAdmin, IISHelp, and Scripts virtual directories, are removed.
- MSADC virtual directory (RDS) is removed or secured.
- Include directories do not have Read Web permission.
- Virtual directories that allow anonymous access restrict Write and Execute Web permissions for the anonymous account.
- There is script source access only on folders that support content authoring.
- There is write access only on folders that support content authoring and these folder are configured for authentication (and SSL encryption, if required).
- FrontPage Server Extensions (FPSE) are removed if not used. If they are used, they are updated and access to FPSE is restricted.

Script Mappings

- Extensions not used by the application are mapped to 404.dll (.idq, .htw, .ida, .shtml, .shtm, .stm, .idc, .htr, .printer).

- Unnecessary ASP.NET file type extensions are mapped to "HttpForbiddenHandler" in Machine.config.

ISAPI Filters

Unnecessary or unused ISAPI filters are removed from the server.

IIS Metabase

- Access to the metabase is restricted by using NTFS permissions (%systemroot%\system32\inetrv\metabase.bin).
- IIS banner information is restricted (IP address in content location disabled).

Server Certificates

- Certificate date ranges are valid.
- Certificates are used for their intended purpose (for example, the server certificate is not used for e-mail).
- The certificate's public key is valid, all the way to a trusted root authority.
- The certificate is SHA 256 or better.

Machine.config

- Protected resources are mapped to HttpForbiddenHandler.
- Unused HttpModules are removed.
- Tracing is disabled <trace enable="false"/>
- Debug compiles are turned off. <compilation debug="false" explicit="true" defaultLanguage="vb">

Code Access Security

- Code access security is enabled on the server.
- All permissions have been removed from the local intranet zone.
- All permissions have been removed from the Internet zone.

Other Check Points

- HTTP requests are filtered.
- Remote administration of the server is secured and configured for encryption, low session time-outs, and account lockouts.

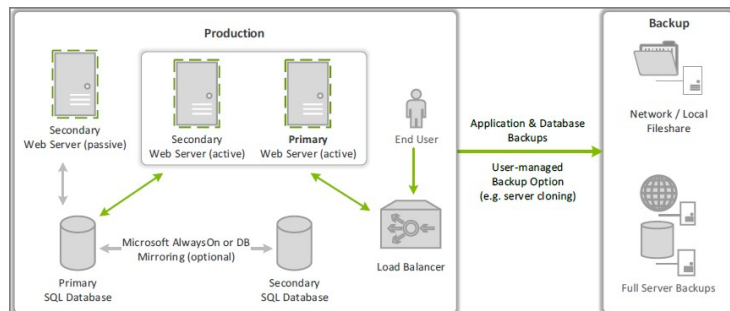
Other Considerations

- Do use a dedicated machine as a Web server.
- Do physically protect the Web server machine in a secure machine room.
- Do configure a separate anonymous user account for each application, if you host multiple Web applications.
- Do not install the IIS server on a domain controller.
- Do not connect an IIS Server to the Internet until it is fully hardened.
- Do not allow anyone to locally log on to the machine except for the administrator.

This sections contains topics around infrastructure set-up and/or changes:

- [Setting up Internet Connected Clients](#)
- [Setup High Availability/Clustering](#)
- [Setup Reverse Proxy](#)
- [VM Deployments](#)
- [Moving SQL DB](#)

This topic explains the steps involved to set up Thycotic Privilege Manager High Availability, also known as clustering.



Pre-Requisites

Make sure that Privilege Manager is installed and working on a primary node with an existing database.

To cluster Privilege Manager a secondary server must be prepared with the proper Privilege Manager pre-requisites. The pre-requisites check can be performed via standard Privilege Manager setup.exe. However, exit that automated installer once all pre-requisites clear.

Except for the Operating System, the following pre-requisites will be installed automatically by our installer. If you already have some of them installed or wish to install them yourself then the installer will skip over them.

System Requirements Overview

1. **Windows 2012 R2 or newer** operating system (2012 or newer is recommended)
2. Microsoft **SQL Server 2012 or newer** (Standard edition or higher is recommended)
3. Microsoft **Internet Information Services (IIS) 7 or newer**
4. Microsoft **.NET Framework 4.6.1 or newer**

Note: Windows Server 2016 comes with the .NET Framework already installed.

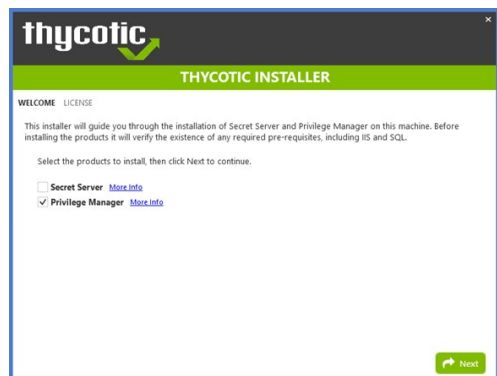
Using the Installer to Install/Confirm Pre-Requisites

The latest version of Privilege Manager is available for [download](#). By clicking the Installer (.exe) link, a setup.exe file will be downloaded to your machine. It is recommended to run the setup.exe file as an administrator.

Note: The setup executable will ONLY be used to install/confirm all pre-requisites are installed on the web server. After confirming the pre-requisites, the installer will be closed and a manual installer will be completed. The manual installation will allow for separate databases and custom file locations. Do NOT complete the installation with the setup executable.

Running the setup.exe will begin an installation wizard. This wizard will ONLY be used to install any remaining pre-requisites required on the web server. The wizard will walk through the initial installation steps, beginning with a Welcome page.

1. On the Welcome dialog, verify that Privilege Manager is selected and select the checkbox if not already checked.



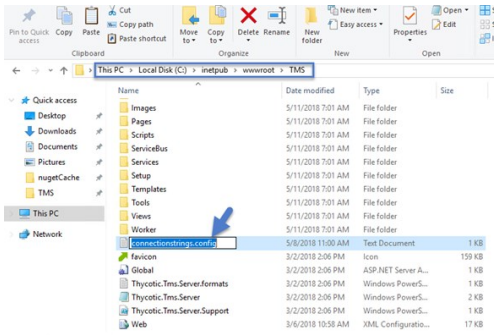
2. Click **Next**.
3. On the License dialog review the End User License Agreement (EULA) and click **Accept License**.
4. On the Database dialog select **Connect to an existing SQL Server**, click **Next**.
5. The Pre-Requisites dialog helps you to ensure everything that is required gets installed for Privilege Manager. Click **Fix Issues** to automatically install the necessary pre-requisites.
6. Close the installer once all pre-requisites are successfully installed.

Note: Do NOT continue installing the products with this installer.

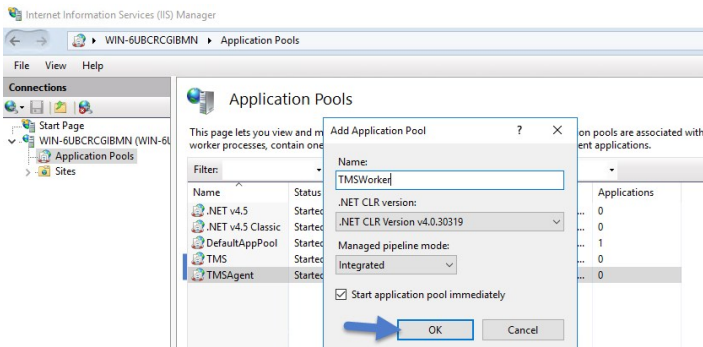
Manual Set-up of Secondary Node

In this procedure you will first copy the web application files from the primary server to the secondary server and then use those copied files to setup and configure the secondary Privilege Manager server.

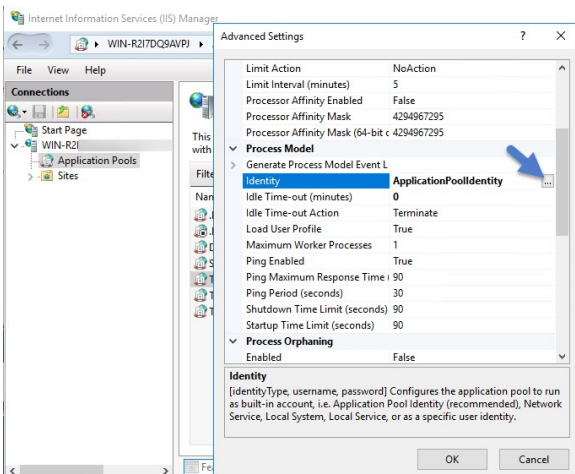
1. On the primary server, decrypt the **connectionStrings.config** by running the following command:
`C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "connectionStrings" -app "/Tms"`
2. Select and copy all contents of the Privilege Manager web application folder at
`C:\inetpub\wwwroot\TMS\`
 Including the unencrypted connectionStrings.config file.
3. On the secondary server, create the same folder path.
4. Paste the entire contents of the Privilege Manager web application folder from the primary web server to the similar location on the secondary web server.



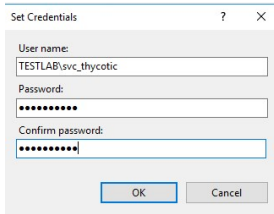
5. Open **Internet Information Services Manager** (inetmgr).
6. Under your local server, right-click **Application Pools** and select **Add Application Pool...**
7. **Add** three new application pools.
 1. **TMS**
 2. **TMSAgent**
 3. **TMSWorker**.



8. For each of the 3 app pools (TMS, TMSAgent, and TMSWorker),
 1. right-click on each app pool,
 2. select **Advanced Settings...**
 3. then the **Identity** box in the "Process Model" section,
 4. click the three dots on the right of the box.

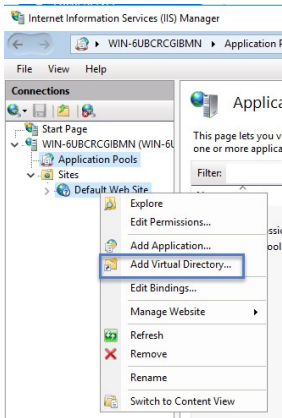


5. Select the **Custom Account** radio button.
6. Click **Set**, enter your service account's name and password.



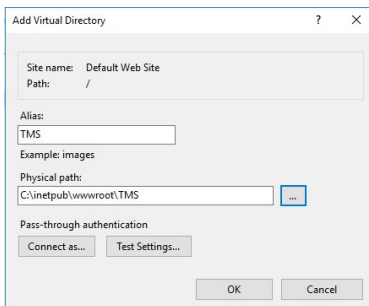
7. Click **OK**.

9. Right-click **Default Web Site** in IIS and select **Add Virtual Directory...**



10. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in <http://myserver/TMS>.

11. Next, enter the physical directory where you unzipped Privilege Manager (i.e., C:\inetpub\wwwroot\TMS).

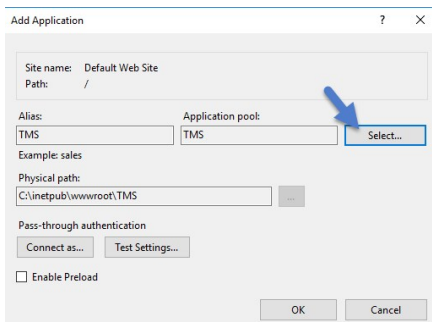


12. Click **OK**.

13. In the tree, right-click the new virtual directory and select **Convert to Application**.

1. Set the **Application Pool** to the one called **TMS**.

2. Click **OK**.



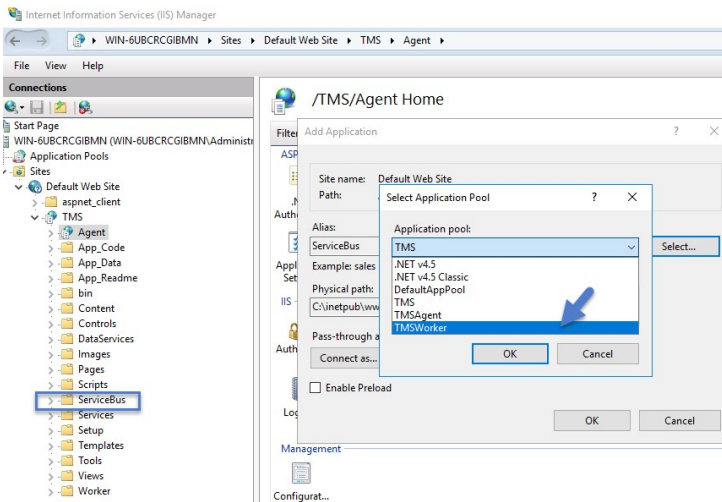
14. In the virtual directory expand the new **TMS** site,

1. right click the **Agent** Subfolder and select **Convert to Application**.

2. Set the **Application Pool** to the one called **TMSAgent**, click **OK**

15. In the virtual directory navigate to the **ServiceBus** Subfolder.

1. Right-click and select **Convert to Application**.
2. Set the **Application Pool** to the one called **TMSWorker** you created earlier, click **OK**



16. In the virtual directory select the **Services** Subfolder.

1. Right-click the new virtual directory and select **Convert to Application**
2. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**

17. In the virtual directory select the **Setup** Subfolder.

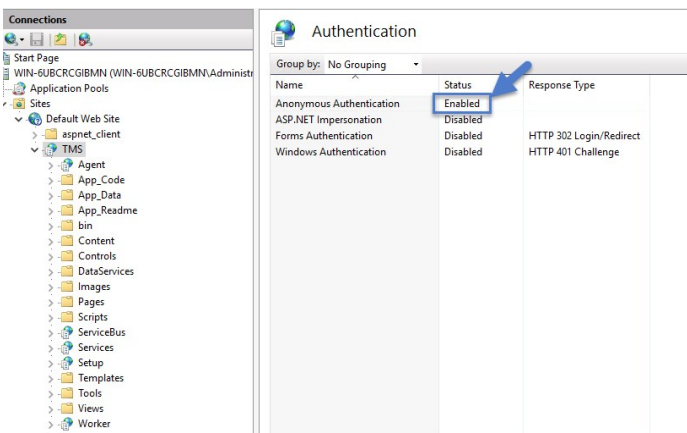
1. Right-click the new virtual directory and select **Convert to Application**.
2. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**

18. In the virtual directory select the **Worker** Subfolder.

1. Right-click the new virtual directory and select **Convert to Application**.
2. Set the **Application Pool** to the one called **TMSWorker**, click **OK**

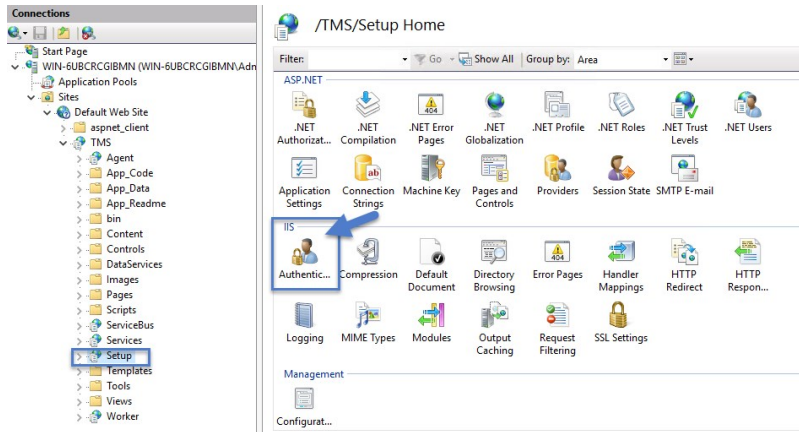
19. Select your **TMS** virtual directory.

1. Double-click **Authentication** in the features pane.
2. Make sure that only **Anonymous Authentication** is set to **Enabled**. Everything else should be set to disabled.



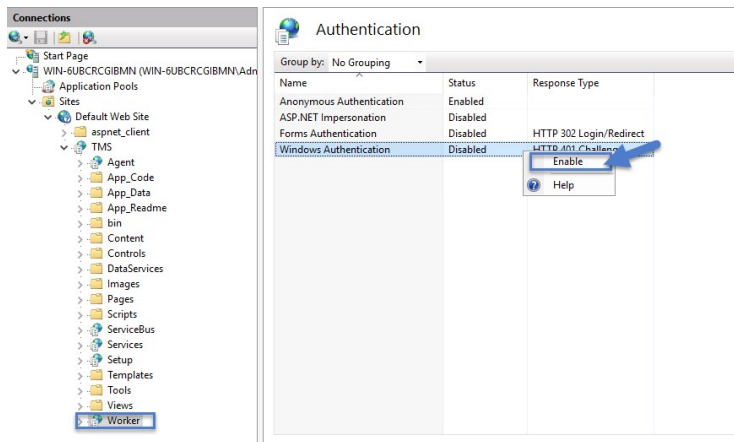
20. Select the **Setup** directory.

1. Double click **Authentication** in the features pane.
2. Make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.



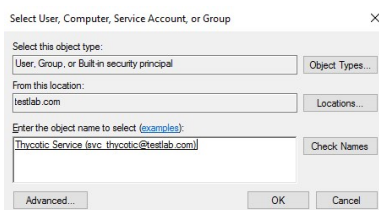
21. Select the **Worker**.

1. Double-click **Authentication** in the features pane and make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.

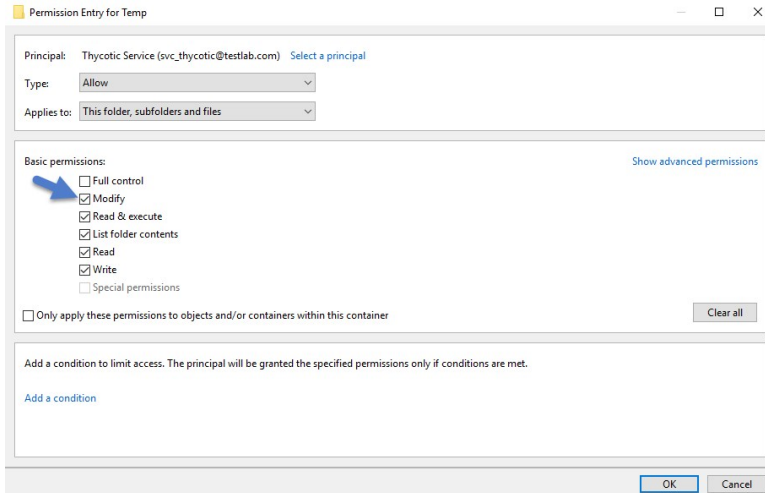


Folder Permissions to C:\Windows\Temp

1. Navigate to the **C:\Windows\TEMP** folder.
2. Right-click the folder and select Properties | Security | Advanced.
3. Click **Add** and **Select a principal**.
4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.
7. Under Basic permissions, select the **Modify** checkbox***

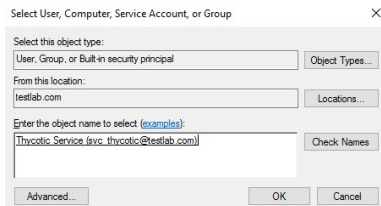


8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.

9. Click **OK** then **Apply**.

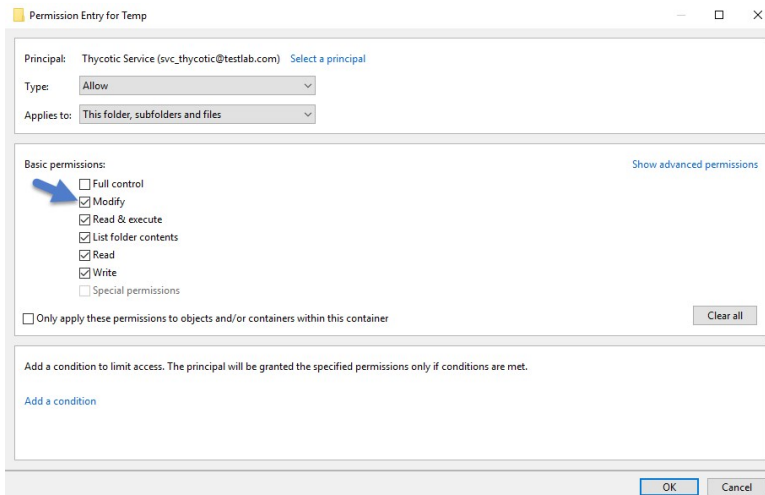
Folder Permissions to the Privilege Manager Application Folder

1. Navigate to the Privilege Manager application folder at **C:\inetpub\wwwroot\TMS**.
2. Right-click the folder and select Properties | Security | Advanced.
3. Select **principal**.
4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.

7. Under Basic permissions, select the **Modify** checkbox.



8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.

9. Click **OK** then **Apply**.

Note: The application folder only needs **Write** and **Modify** permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Permission to Certificate Private Key (prior to 10.6 only)

Note: This is only required for Privilege Manager prior to release 10.6.

TMS requires **Read** access to the private key of the certificate being used for the HTTPS binding. To set this:

1. Open **mmc.exe** as an administrator.
2. Add the certificate manager snap-in choosing to manage certificates for the computer account (**File | Add/Remove Snap-in...**)
3. Click **Certificates**.
4. then **Add | Computer account | Next | Local computer | Finish | OK**
5. Find the certificate that the HTTPS binding for your site is using.
6. Right-click on the certificate and select **All Tasks | Manage Private Keys**.
7. Grant **Read** access to the identity account for your application pools.

If the "Manage Private Keys" option is not available, you can set this permission in PowerShell.

Verify Login on Secondary Node

1. Navigate to Privilege Manager, ex: **http://localhost/TMS**. You should be able to authenticate to Privilege Manager.
2. After logging in, all policies and all data accessible on the primary node should be accessible on the secondary node.

Re-encrypt ConnectionStrings.config

1. On the **primary node**, run the following command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "connectionStrings" -app "/Tms"
```
2. On the **secondary node**, run the same command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pe "connectionStrings" -app "/Tms"
```

Privilege Manager has now successfully been clustered. A load balancer, GTM, VIP, etc. can be used to manage the traffic. The settings to configure this will be handled on the side of this infrastructure piece and is beyond the scope of this document. Contact Thycotic's Professional Services team if additional consultation is required.

Thycotic requires that **sticky sessions** are enabled on the load balancer to prevent a user from bouncing between servers on each request of a single session.

On-premises Privilege Manager instances need to use an Azure Service Bus for internet connected clients. The Azure Service Bus is a subscription service that external agents can connect to and use to communicate with an internal Privilege Manager Server (TMS) instance.

Note: Cloud customers don't need to use the Internet Connected Clients set-up, because their clients can already connect to the internet-based cloud instance.

With Privilege Manager 10.7 and up TLS 1.2 is supported.

This page is broken up into three sections:

- Azure Service Bus Queue Configuration
- Setting up the Service Bus as a Foreign System in Privilege Manager
- Configuring the Agents to use the Service Bus (if this is a new agent installation, the Agents can be pointed directly at the Service Bus namespace URL)

Azure Service Bus Queue Configuration

Thycotic requires a Service Bus relay for remote communication. For this a Service Bus Queue needs to be created, follow the procedure as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue](#).

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Do not check any of the options, using the defaults is fine. Take note of the queue name you gave it.

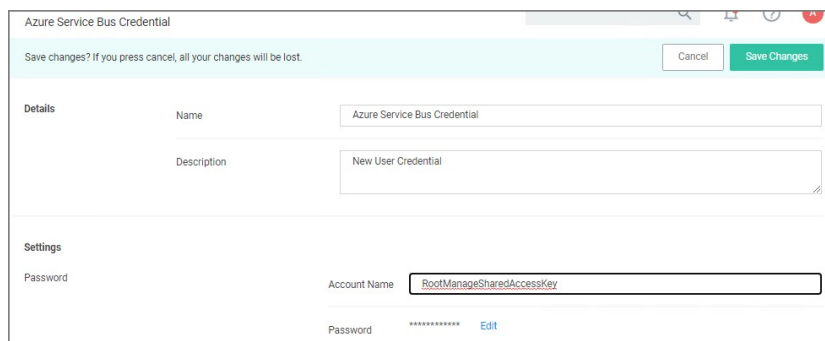
Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

Setting up the Service Bus Foreign System

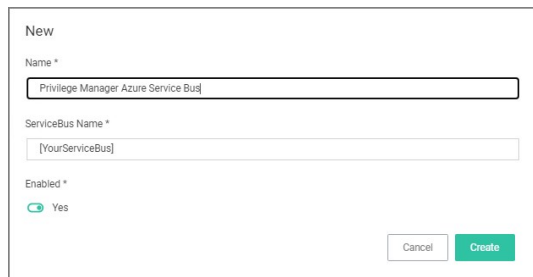
The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the Thycotic Privilege Manager Console, click **Admin | Configuration**.
2. Click the **User Credentials** tab.
3. Click **Create**.

1. Enter a **Name**, for example *Azure Service Bus Credential*.



2. Set the Account name to **RootManageSharedAccessKey**.
3. Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Azure Service Bus Queue Configuration" above.
4. Click **Save Changes**.
4. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
5. Click the **Azure Service Bus** option.
6. Click **Create**.



1. Enter a **Name**, for example *Privilege Manager Azure Service Bus*.
2. Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above). Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).
3. Set the **Enabled** switch to **No** for now.
4. Click **Create**.

The screenshot shows a configuration interface for a 'Foreign System'. The 'Foreign System Details' section includes a 'Name' field with the value 'Mobile App Azure Service Bus' and a 'Description' field with the text 'Provides internet client connectivity via the Azure Service Bus'. The 'Settings' section includes a 'Credential' dropdown menu, an 'Enabled' toggle switch currently set to 'No', and a 'URL' field containing '[YourServiceBus]'. Below these are five empty input fields for 'QueueName', 'QueuePolicyName', and 'QueuePolicySecret'.

5. Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).
 6. Leave the URL field as is (and ignore the fact that it's called URL – it's just the Service Bus name).
 7. Make sure the URI matches the first part of the namespace created in Azure.
 8. Set the QueueName to the same queue name created above in **step 4** under "Azure Service Bus Queue Configuration".
 9. Set the Queue Policy Name to **RootManageSharedAccessKey**.
 10. Set the Queue Policy Secret to the **Primary Key** as obtained in **step 3** under "Azure Service Bus Queue Configuration" above.
 11. Click **Save Changes**.
 12. Enable the Service Bus, set Enabled switch to **Yes**.
7. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:
- o **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>
- Wait for the page to respond.

Configuring Agents to Use the Service Bus

When setting the URL for Agent communication, Internet connected clients need to use the Service Bus URL created above.

Note: For new installations, the agents can be set up to communicate with the service bus during the initial installation process when the **TMSURL** and installation codes are provided, refer to [Bundled Install](#).

Using regedit

1. Open the Registry Editor (**regedit**).
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**.
3. Right click **BaseUrl** and select **Modify**.
4. In the **Edit String** dialog box, change the **BaseUrl** to your Privilege Manager (TMS) Address based on the **Azure Service Bus Queue** configuration, for example [https://\[your company\].servicebus.windows.net/](https://[your company].servicebus.windows.net/), which in our example is <https://testing.servicebus.windows.net/>
5. Close the Registry Editor.
6. Restart the Agent service.

Using PowerShell

To modify the TMS address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\PowerShell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server, enter the **Azure Service Bus Queue URL**, for example [https://\[your company\].servicebus.windows.net/](https://[your company].servicebus.windows.net/), which in our example is <https://testing.servicebus.windows.net/>.

If you have a combined installation of Privilege Manager and Secret Server and wish to move/migrate the MS SQL Server databases, follow the steps below for the case that applies to you:

- **Case I:** Keeping all data in the current database: Backup the existing databases and restore them to the new SQL Server using the instructions below:
 - For Privilege Manager: see Moving the Privilege Manager DB topic below.
 - For Secret Server: <https://thycotic.force.com/support/s/article/Moving-Microsoft-SQL-Server-Database-to-another-machine>

If you have successfully performed the backup and restore (per the applicable instructions above), your site will be connected to the new database.

- **Case II:** Abandoning all data and starting fresh:
 1. In Privilege Manager, go to [https:// <SERVERNAME>/Tms/Setup/Database/ConnectDatabase](https://<SERVERNAME>/Tms/Setup/Database/ConnectDatabase)
 2. Provide the new database connection and click **OK**
 3. Install desired Thycotic products like Privilege Manager and/or Secret Server.

Moving the Privilege Manager DB

Step 1: Backup and Restore the Database

1. Stop the TMS site (Ams site for Arellia) in Internet Information Server (IIS) to prevent any changes to the database
2. Stop the TMS, TMSAgent, and TMSWorker application pools (Ams and AmsWorker application pools for Arellia).
3. Back up the database by accessing SQL Management Studio and right-clicking on the database to select Tasks > Back Up.
4. Select a file location for the .bak file. Transfer this file to the new server.
5. On the new database server, through SQL Management Studio, restore the database backup (the .bak file).
6. Create and/or grant access to the account that will be accessing the database (see TMS Installation Guide for account creation instructions)

We recommend taking the old database offline.

Step 2: Connect to the new database (configure the database connection details)

1. Restart TMS website.
2. Check that the TMS, TMSAgent, and TMSWorker application pools are running.
3. Browse to your TMS URL database connection page e.g. [https:// <YOUR_URL_INSTANCE>/TMS/setup/database/connectdatabase](https://<YOUR_URL_INSTANCE>/TMS/setup/database/connectdatabase) (for Arellia this URL would be slightly different e.g. [https:// <YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase](https://<YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase)) and you will see a page to enter your new database connection details.
4. Enter your new SQL Server and the account information.
5. Click Next and the site will connect to the new database.

Your site is now pointing to the new database.

If also migrating to new web servers or doing a reinstallation, copy the tmsEncryption.config file(s) to the new web servers(s). The file is located on the web server at the root of the TMS web site and should be copied to the same place on the destination server(s): `inetpub\wwwroot\TMS` This file is only applicable if current servers are on version 10.5 or higher. (refer to [Item Encryption](#))

To roll back changes and restore the original database, simply start back at Step 1 and move the database back to the original database server.

Note: Thycotic Management Server, or "TMS", is an umbrella term for our base application layer that Privilege Manager runs on top of. For this guide you only need to recognize that "Tms" is programmed into your Privilege Manager URL string for configuration purposes.

Many organizations as a best practice restrict their privilege manager web server from inbound and outbound internet traffic. However this can cause a functional issue as agents not connected to the corporate network would not be able to reach the server to receive policy updates or submit event feedback.

To resolve this functional issue while maintaining security Thycotic supports agent connections through a Reverse Proxy which can live in the DMZ. The proxy will filter connection requests and only forward those from the agents allowing communication while significantly reducing the potential attack surface. Proxies can be configured using many different networking tools and in this document we will show how to do so with Windows Application Request Routing in IIS.

In this setup, only the endpoint agent needs to be accessible via HTTPS. It is important to note that the certificate being used for HTTPS communication should be the same certificate that is installed on your Privilege Manager web server.

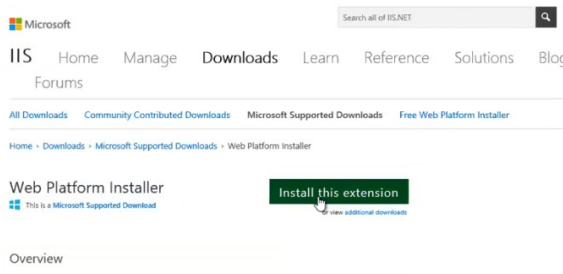
System Specifications

These are the minimum system specifications for a server that is used as a reverse proxy:

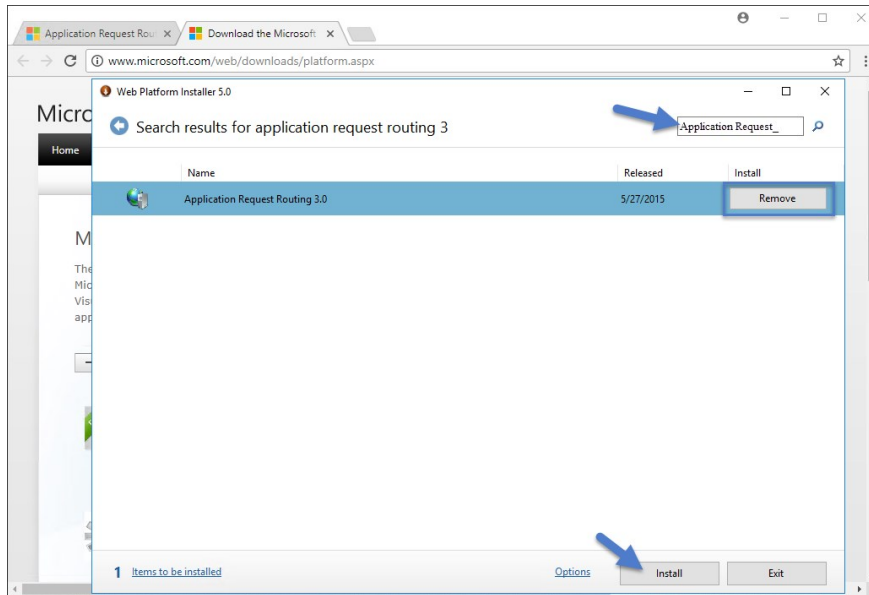
- 2 Cores
- 4 GB RAM
- 40 GB hard drive

Server Configuration

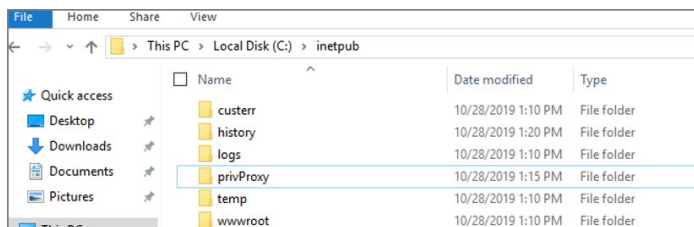
1. Setup a new server or modify an existing server to be in the DMZ.
2. Download [Web Platform Installer](#) on your new Reverse Proxy server. This allows you to add updated IIS extensions from Microsoft.



3. In the search bar of the Web Platform Installer, enter **Application Request Routing #3.0**. Click **Add** and then **Install**. You will need to accept the license terms.



4. Create an empty folder under C:\inetpub\ named **privProxy**.

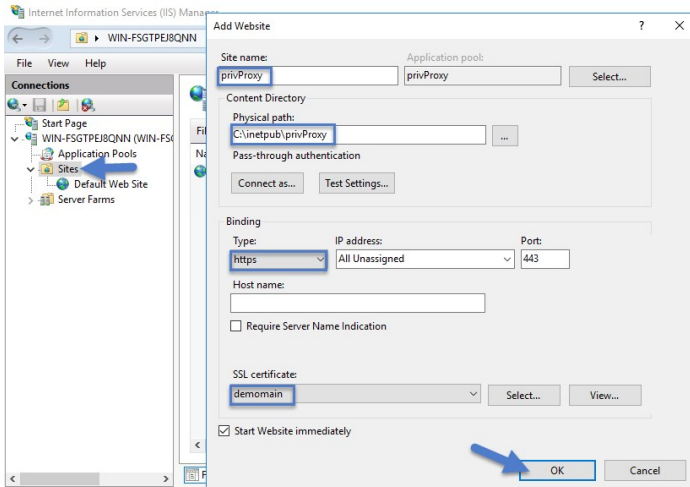


- Open IIS Manager and right-click **Sites** and select **Add Web Site**.
- Name the site **privProxy** and set the **Physical Path** to the folder under C:\inetpub named **privProxy**.
- Change the binding to **HTTPS**.
- Use the default port of 443.

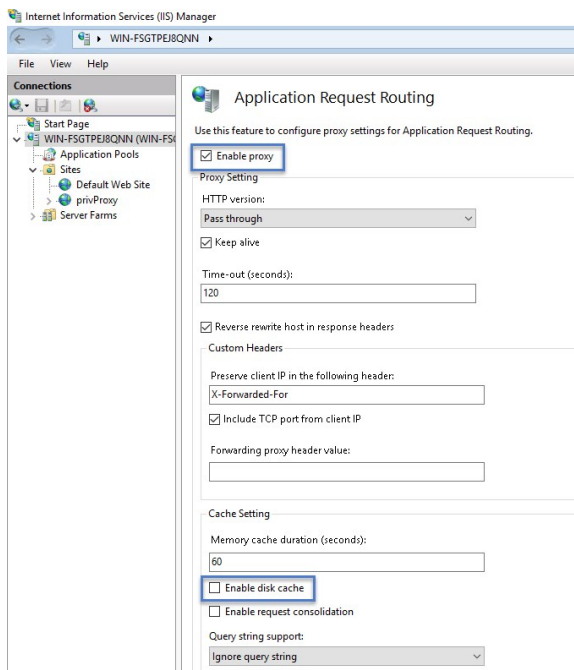
Note: If there are other applications using port 443 on this server, such as Symantec CEM, then set the privProxy to use a different port, such as **45593**. If you use a port other than 443, make sure to add the appropriate firewall rule.

- Select a certificate for the binding to use and Click **OK**. The certificate being used for HTTPS communication should be the same certificate that is installed on your Privilege Manager web server. Follow [these instructions](#) to install a certificate on your Reverse Proxy server.

Note: The certificate used for HTTPS binding on the Web App Server needs to be exported then imported into the Root and Intermediate certificate stores on the Proxy Server.



- In the IIS Manager's left hand navigation pane select the server node.
- Open **Application Request Routing** from the middle pane.
- Select **Server Proxy Settings** in the right hand actions pane
- In the **Application Request Routing** pane, select **Enable Proxy** and deselect **Enable disk cache**.

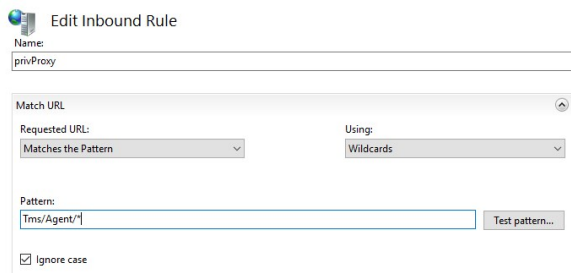


- Select **Apply** under the actions pane and then select **URL Rewrite**.
- Select **Add Rule(s)** on the actions pane and then under **Inbound rules** select **Blank rule**.

16. Name the rule **privProxy**.

17. In the Edit Inbound Rule window, do the following steps:

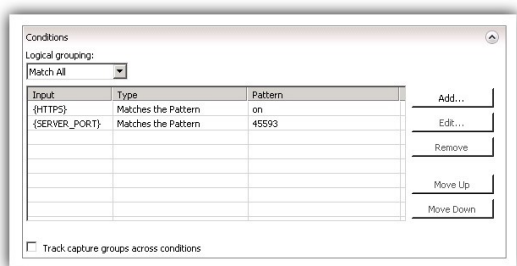
1. Under **Match URL** from the **Requested URL** menu, choose **Matches the Pattern**.
2. From the **Using** menu, choose **Wildcards**.
3. From the **Pattern** menu, choose **Tms/Agent/***.
4. Select **Ignore case**.



18. Under **Conditions**, from the **Logical Grouping** menu, choose **Match All**.

19. Add a condition for : **Matches the pattern: on**

20. (optional) You can also add a condition and set it to the port number configured above.



21. Under **Action**, from the **Action Type** menu, choose **Rewrite**.

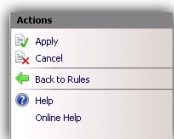
22. Under **Action Properties**, in the **Rewrite URL** field, type the URL `https://server.example.com/Tms/Agent/{R:1}`

23. Select **Append query string**

24. Select **Stop processing of subsequent rules**



25. In the **Actions** pane, click **Apply**.



Now your internet-connected agents will be able to communicate with the Privilege Manager server through <https://external-name.domain.com:45593/Tms/> or <https://external-name.server.com/Tms/>, depending on the port you chose.

Testing Agent URLs

To test registered agent URLs use the following, based on Privilege Manager version:

- /agent/agentregistration4.svc
- /agent/agentregistration3.svc
- /agent/agentregistration2.svc

For example using `https://PrivilegeManagerAppServerName.DomainName/TMS/Agent/agentregistration4.svc` at the agent agent point, should successfully return XML like the following:


```

<?xml:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xs="http://schemas.xmlsoap.org/2004/09/mex" xmlns:i0="http://tempuri.org/"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/wss-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsa10="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wspap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:wsc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsm="http://www.w3.org/2007/05/addressing/metadata" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tms="http://arellia.com/services/Agent/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsm="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" name="Thycotic.Tms.Services.Agent.AgentRegistration4" targetNamespace="http://arellia.com/services/Agent/"
<wsdl:import namespace="http://tempuri.org/" location="https://localhost/TMS/Agent/AgentRegistration4.svc?wsdl-wsdl1"/>
<wsdl:types/>
<wsdl:service name="Thycotic.Tms.Services.Agent.AgentRegistration4">
  <wsdl:port name="CustomBinding_IAgentRegistration2" binding="i0:CustomBinding_IAgentRegistration2">
    <soap12:address location="https://localhost/TMS/Agent/AgentRegistration4.svc"/>
    <wsa10:EndpointReference>
      <wsa10:Address>https://localhost/TMS/Agent/AgentRegistration4.svc</wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
  <wsdl:port name="CustomBinding_IAgentRegistration21" binding="i0:CustomBinding_IAgentRegistration21">
    <soap12:address location="http://win-e6gkpm7j7tf/TMS/Agent/AgentRegistration4.svc"/>
    <wsa10:EndpointReference>
      <wsa10:Address>
        http://test-system/TMS/Agent/AgentRegistration4.svc
      </wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

Note: Make sure that the server acting as the reverse proxy trusts and matches the certificate that the Privilege Manager web server is using for its HTTPS binding. If the certificate is not trusted, the proxy will return a 500.21 Gateway error.

Agent Configuration

When you set up the Agent, make sure that the BaseURL has been set to the DMZ Server Address by following the steps in [Setting the Privilege Manager Server Address](#).

Important: The Privilege Manager server is **not** able to push tasks to agents when the agents are not connected to the same network. However, the internet connected clients will automatically pull tasks from the server on a scheduled interval.

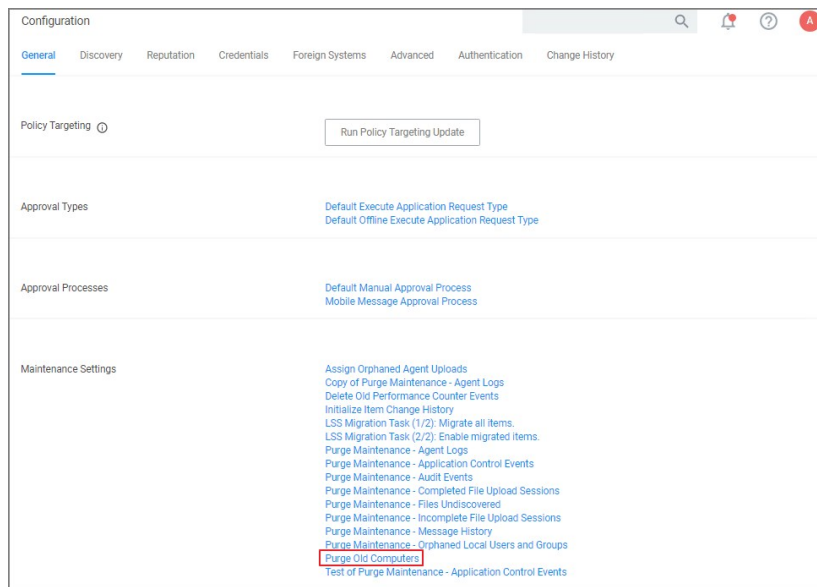
This topic is a collection of articles covering maintenance procedures for different areas of the Privilege Manager product.

The following topics are available:

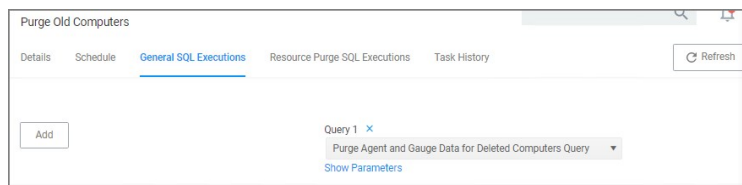
- [How to Purge Computers](#)
- [How to Purge the Action Items Table](#)
- [Using the Remove Programs Utility](#)
- [Export Items](#)
- [Import Items](#)
- [Migrate Local Security Policies](#)

After using Privilege Manager for a certain amount of time, you may have computers that haven't communicated with the Privilege Manager server for an extended period of time. This can be done via the Purge Computers task, which can be found under Configuration on the General tab.

1. Navigate to **Admin 1 Configuration** and select the **General** tab.
2. Under the Maintenance Settings section click **Purge Old Computers**.

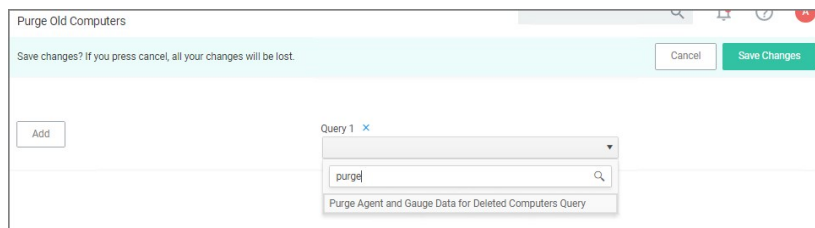


3. On the **Purge Old Computers** page select the **General SQL Executions** tab.
4. Verify that **Query 1** is set to **Purge Agent Gauge Data for Deleted Computers Query**.



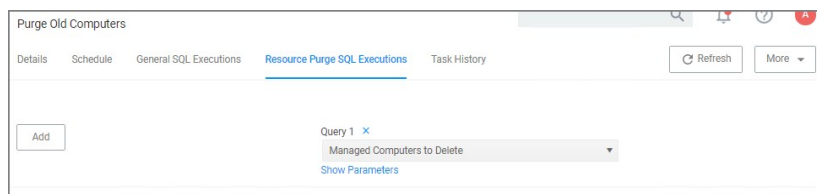
If for whatever reason that specific query is not listed or if you need to add other queries,

1. Click **Add** to either replace the query currently listed or add this query.
2. Start typing the query name *Purge Agent Gauge Data for Deleted Computers Query* and select the query from the results list.



3. Click **Save Changes**.

5. Select the **Resource Purge SQL Executions** tab.
6. Verify that **Query 1** is set to **Managed Computers to Delete**.



If that specific query is not listed,

1. Click **Add** to either replace the query currently listed or add this query.
 2. Start typing the query name *Managed Computers to Delete* and select the query from the results list.
 3. Click **Save Changes**
7. Click **Show Parameters**. The Days field indicates after how many days a system is considered to be an old computer and thus should be purged. The default value is 90 days. If you want a different value, enter a number to change the number of days.

Purge Old Computers

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Add

Query 1 ×
Managed Computers to Delete
[Hide Parameters](#)

Parameters

days *

1. Click **Save Changes**.
8. Click **More | Run Task**
9. On the **Task Name** modal, you may change the task name and click **Run Task**
10. On the **Task History** tab you can view the status of the running task by selecting the task from the table grid.

Purge Old Computers

Details Schedule General SQL Executions Resource Purge SQL Executions **Task History** Refresh More

View from 4/24/2020 to 7/24/2020 Refresh

NAME	STARTED	FINISHED	STATUS
Interactive run on Thu Jul 23 2020	7/23/20, 7:58 PM	7/23/20, 7:58 PM	Closed

If the application action table frequently grows too large, you can use the steps below to create a scheduled event to purge old application action events.

Creating a Scheduled Event for Purging

1. Launch **Privilege Manager**.
2. Click **Admin | Configuration**.

Configuration

General | Discovery | Reputation | Credentials | Foreign Systems | Advanced | Authentication | Change History

Policy Targeting ⊙ Run Policy Targeting Update

Approval Types Default Execute Application Request Type
Default Offline Execute Application Request Type

Approval Processes Default Manual Approval Process
Mobile Message Approval Process

Maintenance Settings Assign Orphaned Agent Uploads
Copy of Purge Maintenance - Agent Logs
Delete Old Performance Counter Events
Initialize Item Change History
LSS Migration Task (1/2): Migrate all items.
LSS Migration Task (2/2): Enable migrated items.
Purge Maintenance - Agent Logs
Purge Maintenance - Application Control Events
Purge Maintenance - Audit Events
Purge Maintenance - Completed File Upload Sessions

3. Click **Purge Maintenance – Application Control Events**

Purge Maintenance - Application Control Events

Details | Task History | Change History Refresh More

Details

This task can be scheduled to run periodically on the web server or be run immediately by using the Run Task option from the More menu.

Name

Description

Command

Parameters

Parameters for this task:

Purge Application No
Action events *

Purge Application No
Justification events *

Purge Application No
Metering events *

Purge Application No
Verifier events *

Max rows per chunk *

Purge events older than *

Only purge events from these policies [Add Only purge events from these policies](#)

Schedules

4. Under **Parameters**.
 1. Set the **Purge Application Action events** switch to **Yes**.
 2. Under **Purge events older than** you may change the default of 30 days to another value.

Note: You can also select the other events to purge as well.
5. Click **Save Changes**.
6. Under **Schedules** click **New Schedule**.

Tasks

Save changes? If you press cancel, all your changes will be lost. Cancel Save Changes

Schedule Details

Task to run [Purge Maintenance - Application Control Events](#)

Schedule Name

Schedule

Schedule Type

Once **Daily** Weekly Monthly

Starting

Recur every day(s)

[Show Advanced](#)

Parameters

Purge Application Action events * Yes

Purge Application Justification events * No

Purge Application Metering events * No

Purge Application Verifier events * No

Max rows per chunk *

Purge events older than * day(s)

Only purge events from these policies [Add Only purge events from these policies](#)

7. Enter in a **Schedule name** and the frequency you want the task to run. You can add other parameters here too. Parameters that were previously selected are locked at this point.

8. Click **Save Changes**.

The Remove Programs Utility provides a solution to the following problem that Windows standard users are not able to remove applications from the control panel because of Windows checking for admin rights. This utility is available for deployment via Privilege Manager.

Customers can use this utility in any of the following ways:

- Allow users to uninstall any and all applications by using the utility.
- Make the utility show an approval request for each uninstaller that is launched.
- Make the utility show an approval prompt when it launches.

The utility will list all the same applications as the Remove Programs in the Control Panel, but it can also hide software that end users should not be able to uninstall (such as the Thycotic agents).

With Privilege Manager version 10.7 Thycotic is introducing support for Windows 10 **Apps & Features** and the management of Windows Store apps via the **Remove Programs Helper**. Certain apps designed as a Windows 10 package are registered in **Apps & Features** but do not appear in the operating systems Add Remove Programs options. Privilege Manager locates those applications and provides management via the enhanced **Remove Programs Utility**.

Using the Configure Privilege Manager Remove Programs Policy

With the Privilege Manager 10.7 release the Remove Programs Utility has moved from being delivered via configuration feed to being fully integrated and delivered via the Server and Agent installation packages.

To allow standard users to use the utility refer to the [Elevating the Privilege Manager Remove Programs Utility Policy](#) set-up instructions.

Configuring the Remove Programs Utility

1. Under your **Computer Group** select **Scheduled Jobs**.
2. Search for **Configure Privilege Manager Remove Programs**.
3. Click on the policy link **Configure Privilege Manager Remove Programs**.

The screenshot displays the configuration interface for the 'Configure Privilege Manager Remove Programs' policy. At the top, there's a search bar and navigation icons. Below that, a message states 'This item is read-only.' The main content is divided into sections: 'Scheduled Job Details' and 'Job Settings'. The 'Scheduled Job Details' section includes fields for Name, Description, Computer Groups Targeted (showing 1 total endpoint: Windows Computers), and Deployment status (Not deployed). The 'Job Settings' section contains several checkboxes for customizing the utility's appearance and behavior, such as 'Create Start Menu Shortcut', 'Add to Control Panel', and 'Show Blocked Installers in List'. There is also a section for 'Products that can't be Uninstalled' with a dropdown menu currently showing 'Thycotic'.

If you need to customize the default policy, Thycotic recommends to create a copy.

4. Click **Duplicate** and name your policy.
5. Click **Create**.
6. Under **Job Settings**, customize the access and functions of the utility. For example:
 - o Choose whether a shortcut on the start menu or on the control panel should be created.
 - o List products that you want to prevent being uninstalled. There are two options for this:
 - If the "Show Blocked Installers in List" option is unchecked, the products will be hidden.
 - If the "Show Blocked Installers in List" option is checked, the products will just be disabled from being uninstalled.

If you selected "Create Start Menu Shortcut", the users will see Privilege Manager Remove Programs on the Start Menu. If you selected "Add to Control Panel", the users will see Privilege Manager Remove Programs in the Control Panel.

7. Under **Job Schedule**, customize the triggers, such as when to run the utility for inventory purposes. This determines how often you want the policy from the Task Scheduler on the endpoint to check to ensure the settings match.

Job Schedule

Specify the triggers of this job. Triggers define the time or events that will cause this policy to be run.

Daily at 10:00:00 PM starting Tue Jul 31 2018 (repeating every 2 hours for a duration of 24 hours)
 Upon task creation/modification
[Add Trigger](#)

Job Conditions

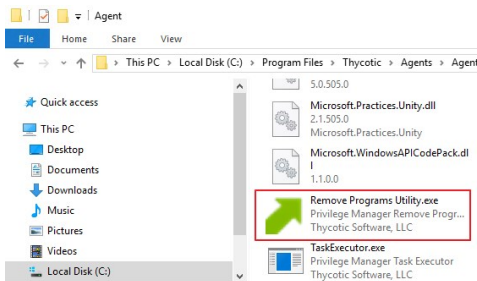
Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition here is not true.

Idle Conditions Start the task only if the computer is idle

Power Conditions Start the task only if the computer is on AC power
 Stop if the computer switches to battery power

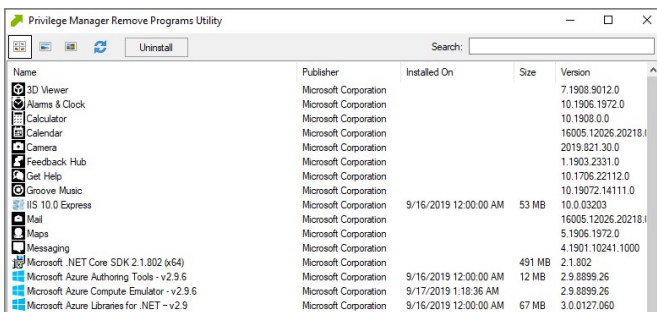
Advanced Conditions Allow task to be run on demand
 Run task as soon as possible after a scheduled start is missed
 If the task fails, attempt to restart
 Stop the task if it runs for longer than 3 day(s)
 If the task is already running, then the following rule applies: Default (Do not start a new instance)

8. Under **Job Conditions**, customize additional conditions that impact running the task, e.g. allowing the utility to be used on demand.
9. Set the **Inactive** switch to **Active**.
10. Click **Save Changes**.
11. Next to **Deployment**, click the **I** icon and select the **Resource and Collection Targeting Update** task.



Use the Utility

The utility is straightforward to use. It's installed on endpoints as part of the Agents installation. Users can select the row containing the program that they want to uninstall and then select the uninstall button.



Troubleshooting

This section contains a collection of troubleshooting articles to help with problems that might occur in your Privilege Manager integration/instance.

The following troubleshooting topics are available:

- [Troubleshooting Installation Issues](#)
- [10.5 Folder Permission for MachineKeys](#)
- [Retrieving the COM class factory error](#)

- [Agent Registration Error Following an OS Upgrade](#)
- [Running updateclientitems.ps1 on an Agent triggers an error](#)
- [Client Item List Downloads](#)
- [Advanced Messages not working for child processes of Microsoft Edge](#)

- [Endpoint Troubleshooting](#)
- [How to Recover an Unresponsive macOS Endpoint](#)
- [Catalina FileSystemWatcher Issue](#)

- [Where are My Server Logs?](#)
- [Where are My Agent Logs?](#)
- [SQL Server Transaction Log](#)
- [User Interface and Ports](#)

- [Improve Boot-up Performance](#)
- [Unable to access Privilege Manager](#)

- [Common Errors](#)
- [Error: Could not allocate space for object](#)
- [UI Storage Error Message](#)
- [Notify User Justification failed](#)
- [Invalid Product Identifier](#)
- [Installation Hangs with Error: Worker Role Monitor received exception during ping](#)

- [How to use the Thycotic Monitor for Troubleshooting](#)
- [Using Process Hacker for Troubleshooting](#)
- [Troubleshooting a Policy with Process Explorer](#)

The following topics about error messages in Privilege Manager are available:

- [Common Errors](#)
- [Error: Could not allocate space for object](#)
- [UI Storage Error Message](#)
- [Notify User Justification failed](#)
- [Invalid Product Identifier](#)
- [Installation Hangs with Error: Worker Role Monitor received exception during ping](#)

Access Denied

Error: "Access Denied. You do not have permission to view this directory or page using the credentials that you supplied."

To Resolve:

After logging in to Privilege Manager 10.3 with a user account that has Privilege Manager Administrator Role rights, if you experience this error, verify if SSL 3.0 and/or TLS 1.0 have been disabled. If those protocols have been disabled on the server, you'll need to replace C:\inetpub\wwwroot\Tms\bin\Thycotic.Owin.Security.dll With http://tmsnuget.thycotic.com/scripts/Thycotic.Owin.Security.dll

Recycle the TMS Application Pools in IIS and attempt to access Privilege Manager again.

Server Error In...

Error: "Server Error in '/' Application. Runtime Error"

Your Secret Server instance doesn't have the correct URL pointing at Privilege Manager.

To Resolve:

Go to your Secret Server instance (Tools | Secret Server). Then Admin | Configuration. Verify that your TMS Installation URL is set to ~/./TMS.

SSL Connectivity or Certificate Issues

Error: SSL Connectivity or Certificate Issues?

Trusting an SSL Certificate on a Client Machine (KB)

When a self-signed certificate is installed on a server for the Secret Server website, client computer browsers will generally give security warnings for that web site. This is because for public websites, only certificates issued by trusted authorities can be trusted as valid certificates. For certificates that will only be used within a company or domain, self-signed certificates the security warnings can generally be ignored.

However, the security warnings can also interfere with the use of the Secret Server Launcher and Web Password Filler. To resolve, the certificate can be installed on the client machine either through Internet Explorer or Certificates snap-in.

The following steps can be used to trust the certificate:

1. Make sure that the host to which the certificate is issued is the same as the host name for your Secret Server website.
 - o Open Internet Explorer and navigate to Secret Server
 - o Click Continue to this website if you are prompted
 - o Click the Certificate Error icon next to the navigation bar and then click View certificate. The value next to Issued to should match the host name for your website. For example, if your website is <https://www.mydomain.local/SecretServer>, it should say "Issued to: www.mydomain.local". If these fields do not match, the client will not be able to fully trust the certificate.
2. Obtain a copy of the certificate file and transfer it to the client computer.
 - o On the server that Secret Server is installed on, find Run from the start menu or screen and type in mmc, then hit Enter.
 - o From the File menu, select Add/Remove Snap-in.
 - o Select the Certificates snap-in, then click the right arrow button to add it.
 - o In the window that appears, select Computer Account, then Local Computer, and then click Finish.
 - o You should now see the Certificates (Local Computer) node. Expand the Personal folder and then the Certificates folder under it.
 - o Right-click the certificate that Secret Server uses, then click All tasks and select Export.
 - o Keep clicking Next to accept defaults in the wizard. Enter a filename, and then click Finish. The certificate has now been exported.
 - o Copy the certificate from your server and transfer it to your client computer. **Note:** If you have Firefox, the certificate can be saved to your client computer by viewing and exporting it after navigating to the website.
3. Install the certificate on the client computer.
 - o On the client computer, find Run from the start menu or screen and type in mmc, then hit Enter.
 - o From the File menu, select Add/Remove Snap-in.
 - o Select the Certificates snap-in, then click the right arrow button to add it.
 - o In the window that appears, select My user account, and then click Finish.
 - o Expand the Trusted Root Certification Authorities folder, then right-click the Certificates folder, and select All Tasks | Import.
 - o Click Next and Yes to accept default settings for all steps of the wizard.
 - o When prompted for the certificate file, select the file you saved in the previous step (2).

Note: You may need to reopen Internet Explorer and browse to Secret Server once more to see the change reflected on the client machine.

Granting Permissions on New SSL Certificate for Privilege Manager (KB)

If you change your certificate or if it is automatically renewed, you may need to grant permissions on your new SSL certificate to the service account that the TMS app pools run under. TMS accesses the SSL certificate to sign all of the policies that Privilege Manager sends out to agents, adding an extra security layer to your environment.

Messages you may see include:

- https: does not render
- Navigating to [https://\[ServerName\]/TMS/PrivilegeManager](https://[ServerName]/TMS/PrivilegeManager) loads a blank screen
- Agents stop receiving configuration information from the Privilege Manager Web Server.
- Http: TMS requires an https (SSL) / secure connection

For the fastest resolution to Permissions issues, you can run a Powershell script:

- Navigate to your TMS Website on your Privilege Manager web server (Usually located in c:\inetpub\wwwroot\), then navigate to Tms\App_Data\Tools\SSLHelper.ps1 on your Privilege Manager web server, right-click this and select Run with Powershell to execute.

To grant permissions manually, follow these steps

1. Using MMC on your Privilege Manager web server, open the certificates snap-in (File | Add/Remove Snap-in... | Certificates | click Add), then select Computer account to manage the local computer. Click Next, then Finish and OK.
2. Double click Certificates (Local Computer) and locate the certificate that your TMS site is using (it will most likely be under Personal\Certificates unless you specified a different location*)
3. Right click on the certificate and select All Tasks | Manage Private Keys

Grant Read Access to the account(s) that TMS is running under

If this is a user account then you may adjust permissions to the user account. To check, go to your app pool in IIS, right-click the IIS app pool | Advanced Settings... | "Identity" row: if your app pool "identity" is listed as something OTHER THAN "ApplicationPoolIdentity" in IIS, i.e. "THYCOTIC ISServiceAccount", then your app pool is using a user account.

If this IS the Application Pool Identity (i.e. not a user account) you will need to adjust permissions to three app pools: "IIS AppPool\TMS", "IIS AppPool\TMSWorker" and "IIS AppPool\TMSAgent." Note that names of app pools may vary depending

on your environment.

Recycle your TMS, TMSAgent, and TMSWorker app pools in IIS.

Note: If you are unsure which certificate matches the one you are using in IIS, follow these steps to ensure your certificate thumbprints match:

In IIS on your Privilege Manager web server, navigate to the site you are using to run Privilege Manager Right-click on this site, click Bindings. Choose the https port you need to update and select Edit. View the SSL Certificate this is attached to.

Next, choose the Details tab and scroll down to find the certificate's Thumbprint. copy the list of numbers and letters that make up your certificate's thumbprint (an sha1 hash)

Return to your certificates in MMC (step 2 above). Right-click Certificates (Local Computer) and select Find Certificates...

In the Contains box, paste your Thumbprint sha1 hash and select sha1 from the Look in Field drop down. Click Find Now. This will return the certificate name that your Privilege Manager Binding is currently linked to.

Tasks Stuck at Ready

Error: Are your tasks sitting at "Ready" for extended periods of time?

To Resolve:

1. Navigate to Admin | Configuration | Advanced and make sure the URL for the "Monitor Worker Role" are accurate for the bindings (Check the hostname in the Base local address and the Port).
2. Open IIS Manager, check to make sure the app pools have Read Access to the certificate that you've assigned to that binding via MMC Certificates plug-in. More instructions on how to do this in our Granting Permissions on New SSL Certificate for Privilege Manager KB, posted here.
3. Manually recycle the TMS and TMS Worker app pools.

CPU Issue

Error: CPU overworked in your Agent or 'Unexpected failure in ACS Agent background'

Your agent may be configured incorrectly.

To Resolve:

1. In Privilege Manager navigate to Admin | Agents.
2. Under the Windows tab, verify that your "Send Application events every" and "Refresh Client item cache every" settings are both set to 0.
3. Save changes, refresh your client item cache, enforce the update on your endpoint machine (Follow the update Powershell script instructions listed under "How do I Update Specific Agents Immediately?" above).

System Critical Error

Error: 'System Critical Error - execute/PolicyDetailComponent' in Firefox

To Resolve:

Open Privilege Manager in a different browser, such as Chrome or Internet Explorer 11. If you prefer Firefox as your web browser, download this zip file: <http://tmsnuget.thycotic.com/scripts/firefox.fix.zip> Unzip these files, then copy and paste into C:\inetpub\wwwroot\TmsSpa\PrivilegeManager\ on your Privilege Manager Server.

Refresh your Firefox browser.

This topic describes the following error while working with Privilege Manager:

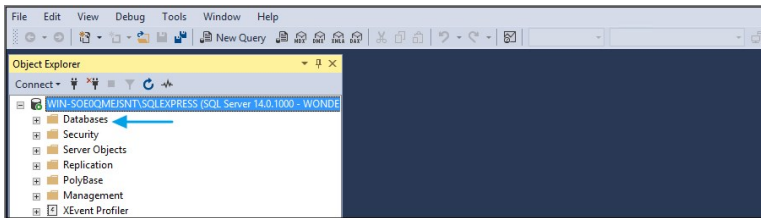
Could not allocate space for object 'Ams.ItemState'. 'UX_ItemState' in database 'ThycPrivMgr' because the 'PRIMARY' filegroup is full.



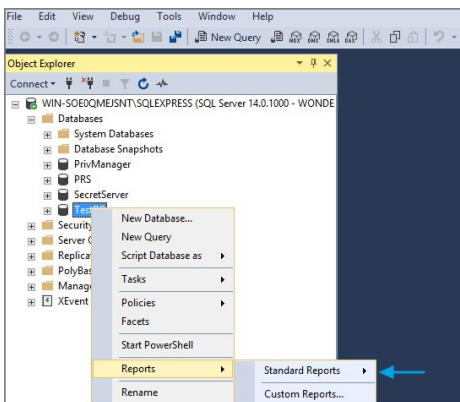
The error indicates that either the Privilege Manager database is full and out of space or the database server running is out of space.

Resolving the Error

1. Navigate to SQL Server Management Studio.
2. Click Connect.
3. Expand Databases.



4. Right-click on the Privilege Manager Database, select **Reports**.
5. Select **Standard Reports**.



6. Select Disk Usage by Top Tables report.

Table Name	# Records	Reserved (KB)	Data (KB)	Indexes (KB)	Unused (KB)
Ams Activities ActivityEvent	9,442	46,096	45,816	224	56
Ams ItemState	6,005	35,352	34,640	408	304
Ams ItemRole	39,435	8,728	2,280	6,376	72
Ams Activities TaskInstance	3,474	8,088	7,616	336	136

7. The report shows the top tables by data usage.
8. If the top table does contain a lot of data, locate the table which contains the highest number of files and open a support case. Provide the information collected with a screenshot of the report to determine the best way to reduce the size of the table.

If the top tables do not contain a lot of data, the issue could possibly be:

- o The database server is running out of disk space. You can check to see what drive the database is stored on to see how much space is left. This will be specific to your environment regarding disk space.
- o Check if there are other databases on the same server and investigate if a different database is taking up space.

During the installation of Privilege Manager the install hangs and is unable to proceed to the next step of the installation.

After checking the Thycotic Monitor, you see the below error in the log viewer:

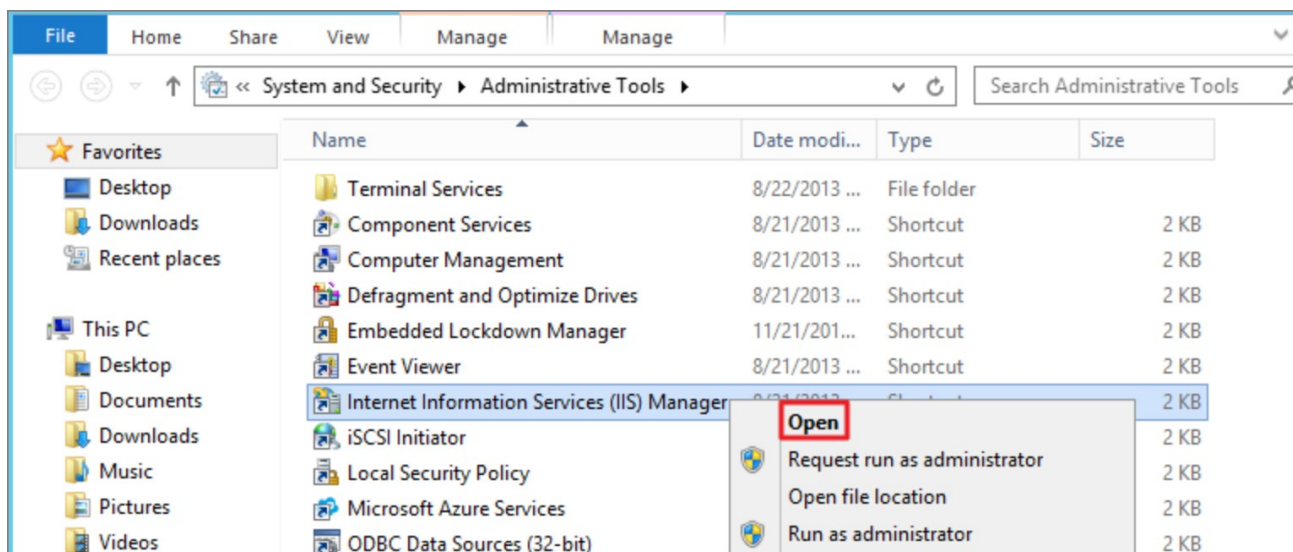
Worker Role Monitor received exception during ping: The HTTP request is unauthorized with client authentication scheme 'Negotiate'. The authentication header received from the server was 'Negotiate,NTLM'



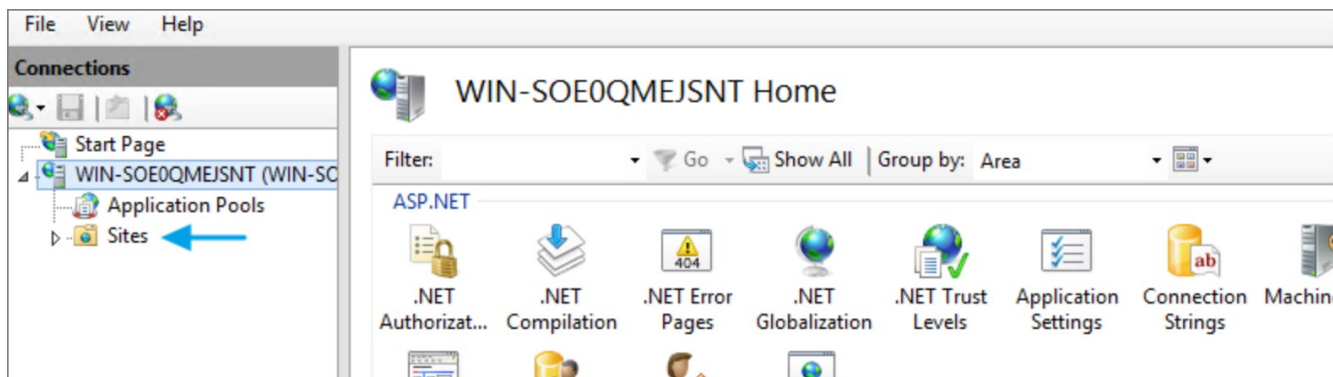
Note: This error is due to a host name in the binding within IIS.

Resolve

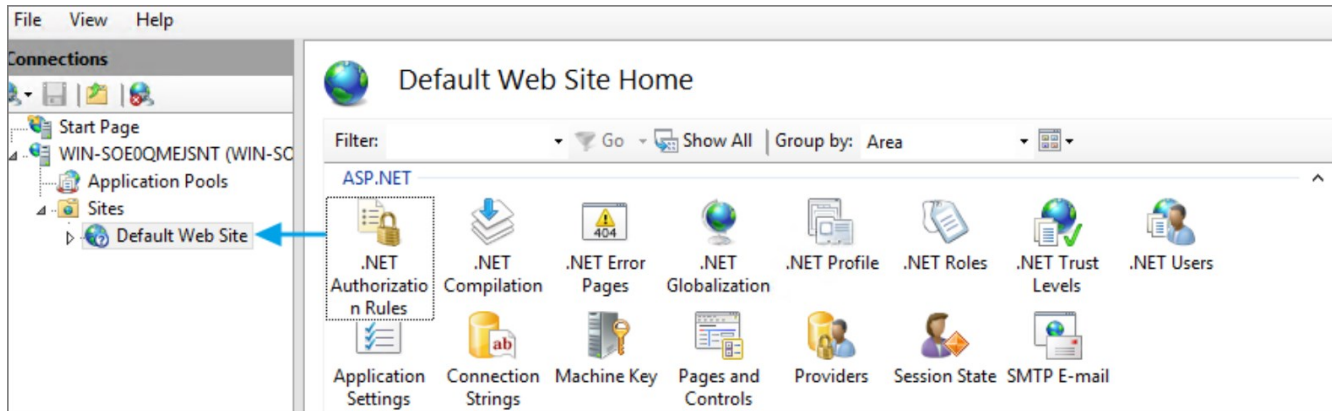
1. Open **Internet Information Services (IIS) Manager**.



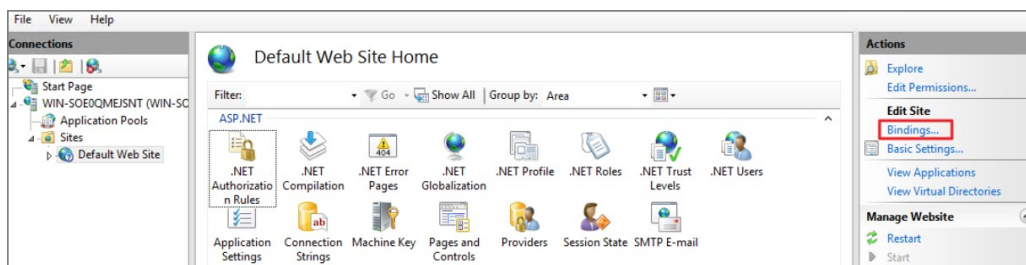
2. Expand down to **Sites**.



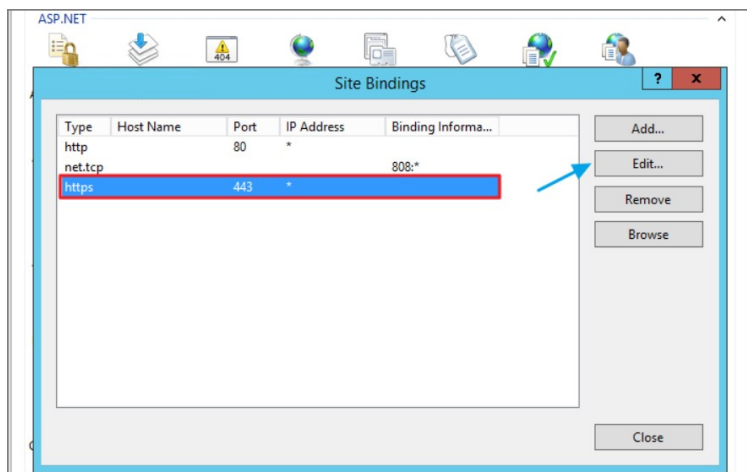
3. Click **Default Web Site** or the **top node site**.



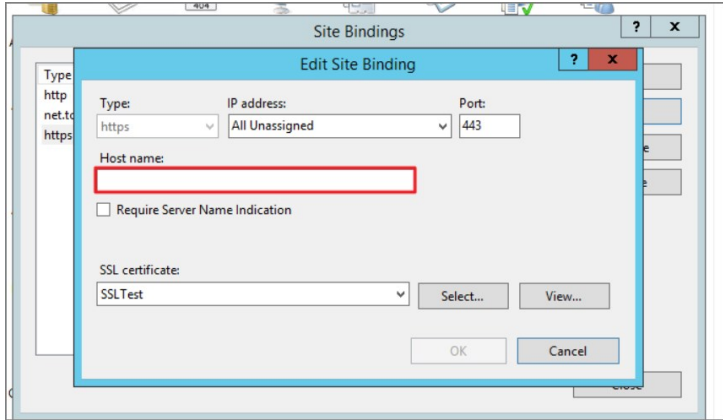
4. Click **Bindings**.



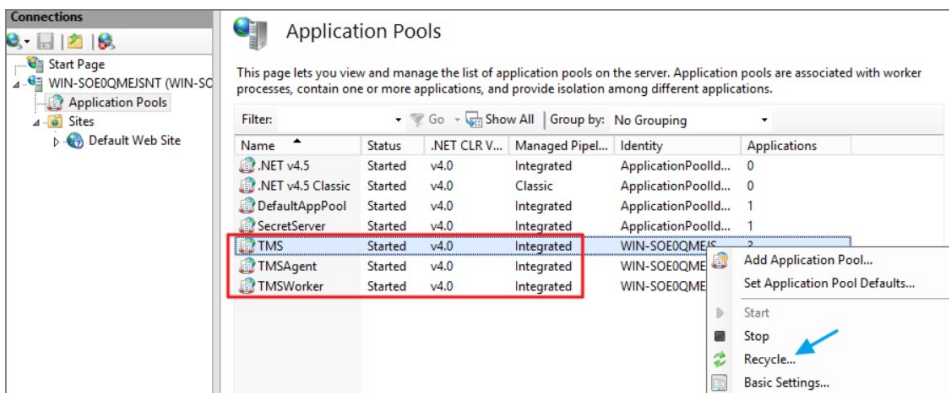
5. Select the **HTTPS binding** | click **Edit**.



6. Confirm that there is no Hostname included for the HTTPS binding for the TMS site. If so, please delete it.



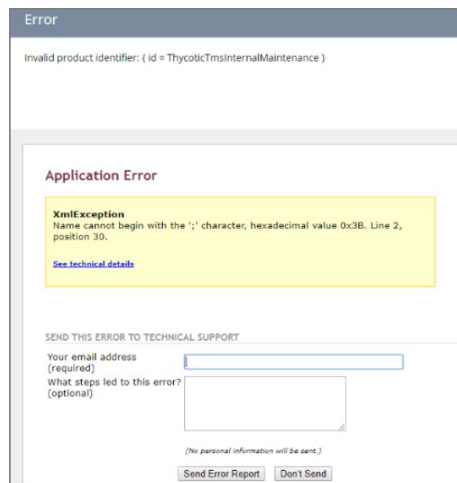
7. **Recycle** all the TMS application pools in IIS.



8. Try the install again by going to <https://localhost/TMS/Setup>

When attempting to upgrade Privilege Manager, you receive the following error:

Error: Invalid product identifier:

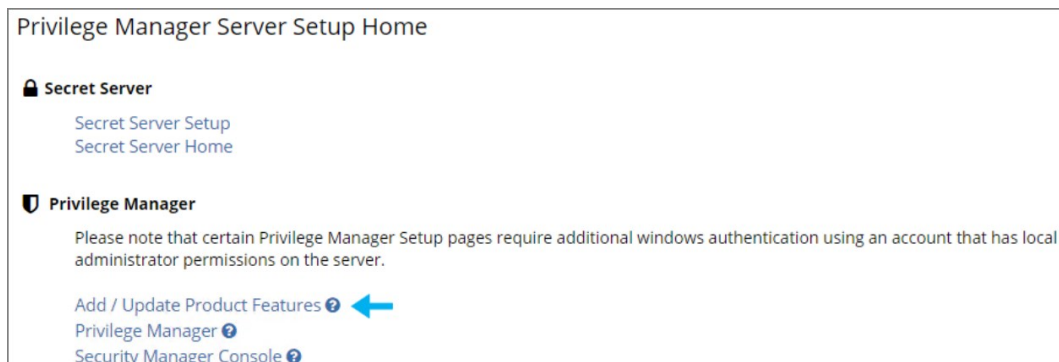


Resolve

1. Navigate to [https://\[YourInstanceName\]/TMS/Setup](https://[YourInstanceName]/TMS/Setup).
2. Click the **Upgrade Banner** at the top of the Privilege Manager home page.



3. Click **Add / Update Product Features**.



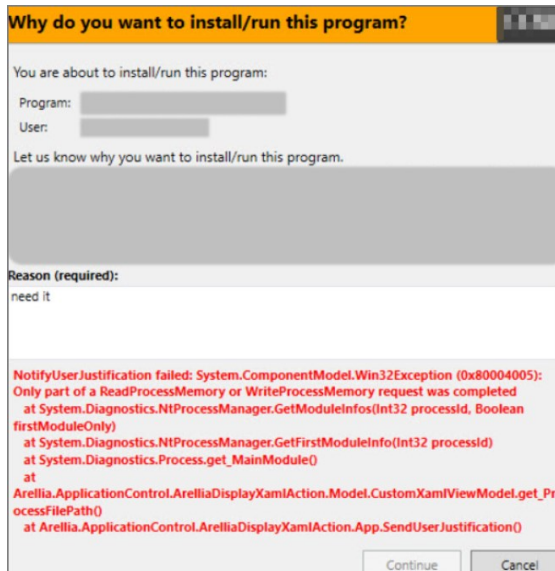
4. Click **Install/Upgrade Products**.

Product Name	Installed	Available	Published
Application Control Solution	18.5.1058	18.5.2007 Install	12/11/2018 7:05 AM
Directory Services Connector	18.5.1024	18.5.2004 Install	12/13/2018 9:50 AM
File Inventory Solution	18.5.1028	18.5.2004 Install	12/11/2018 7:05 AM
Local Security Solution	18.5.1014	18.5.2018 Install	12/11/2018 7:05 AM
Privilege Manager	18.5.1248	18.5.2002 Install	12/11/2018 7:05 AM
Privilege Manager Server Core Solution	18.5.1254	18.5.2008 Install	2/15/2019 12:40 PM
RDP Monitor Solution	18.5.1014	18.5.1014	8/15/2018 5:04 AM

[Install/Upgrade Products](#) [Refresh](#)

5. Select **ALL** of the required solutions.
6. Click **Install** and the upgrade process will begin.

You receive the following error when users attempt to run a program with a policy that uses the action for Notify User justification.

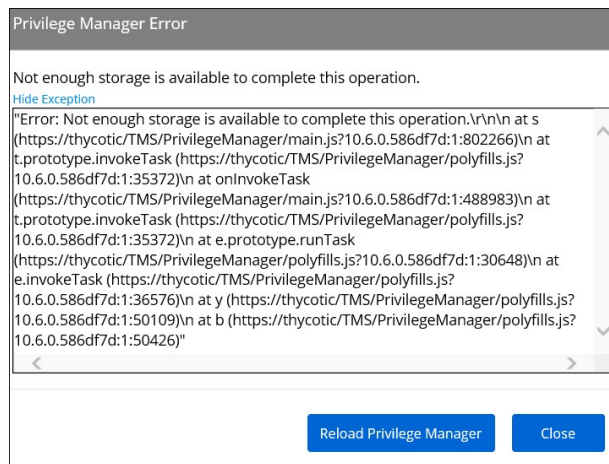


Resolve

1. Either disable the Anti-Virus Real time scan.
2. Or, set Anti-Virus Real-time scanning exclusions.

You might have to clear your browser cache if you get the following error in the Privilege Manager console:

Not Enough Storage is available to complete this operation



Resolution

1. Open your browser window and clear the cache.
2. Close and re-open the browser
3. Launch Privilege Manager and re-try the action.
Note: If the error continues, open a different browser and try to replicate the error. Save any screenshots and open a support case.
4. If this occurs while on the server, please ensure that there is enough disk space to complete the action.

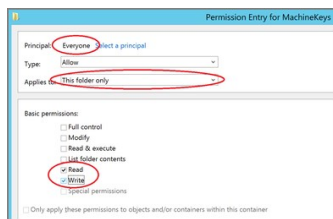
The following topics are available:

- [Troubleshooting Installation Issues](#)
- [10.5 Folder Permission for MachineKeys](#)
- [Retrieving the COM class factory error](#)

During installation of Privilege Manager 10.5 (or an upgrade from prior versions) Privilege Manager attempts to create a new self-signed certificate for internal use. If permissions on the folder %ProgramData%\Microsoft\Crypto\RSA\MachineKeys are incorrect, the install fails with a cryptographic exception and the text **Access Denied**.

Follow the steps below to add Everyone (Read, Write, This Folder Only) permissions to %ProgramData%\Microsoft\Crypto\RSA\MachineKeys.

1. Browse to %ProgramData%\Microsoft\Crypto\RSA\MachineKeys.
2. Right-click on the folder and select **Properties**.
3. Select the **Security** tab and click the **Advanced** button.
4. On the **Permissions** Tab, click the **Change permissions** button. (If you are already running as an administrator, you may not need this step.)
5. On the **Permissions** Tab, click **Add**.
6. On the next dialog, click the **Select a principal** link.
7. In the **Enter the object name to select** field, type **Everyone** and click **OK**.
8. You will see the dialog shown below, select **This folder only** and **Read and Write**.

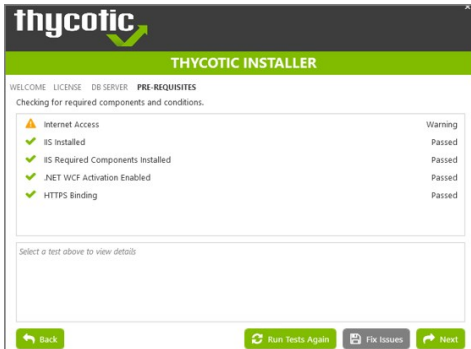


9. Click **OK** to add the entry.
10. Click **Apply** to apply the changes.
11. Navigate back to the Privilege Manager Setup page and select the repair option for the Privilege Manager Server Core Solution.

This article provided troubleshooting tips to help anyone who hits a snag during an install for Privilege Manager.

Internet Connection

If your server is not connected to the internet, you see the following:

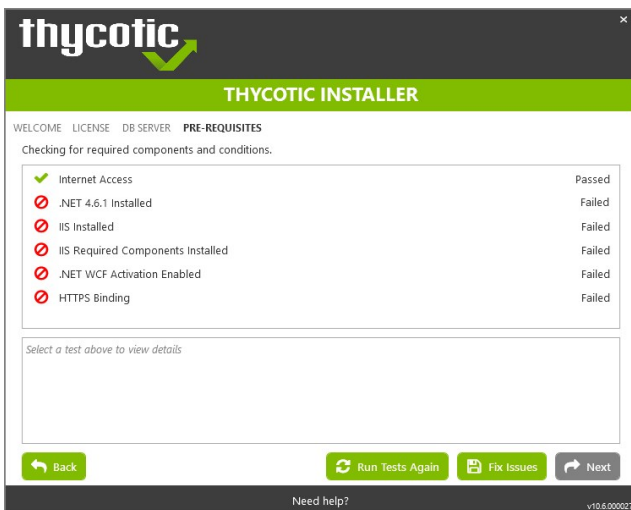


To Resolve:

Click **Next** to proceed through your installation offline.

.NET Dependency

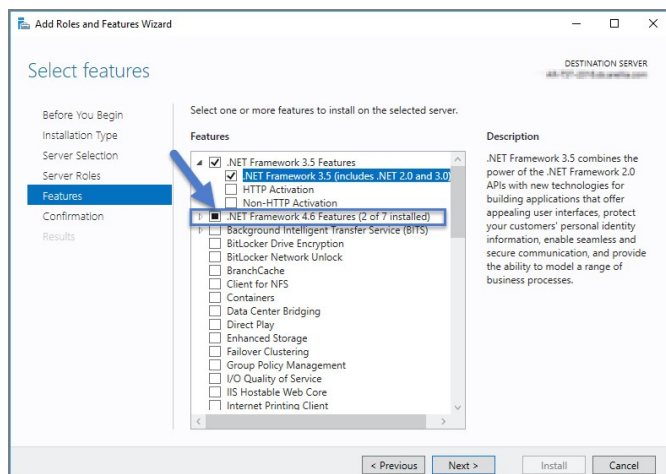
Don't have the required .NET version Dependency installed to accompany your SQL DB? This is what you will see:



To Resolve: Click the Fix Issues button on the Thycotic Installer, then run the pre-requisites check again.

If the error persists, manually install the recommended .NET version.

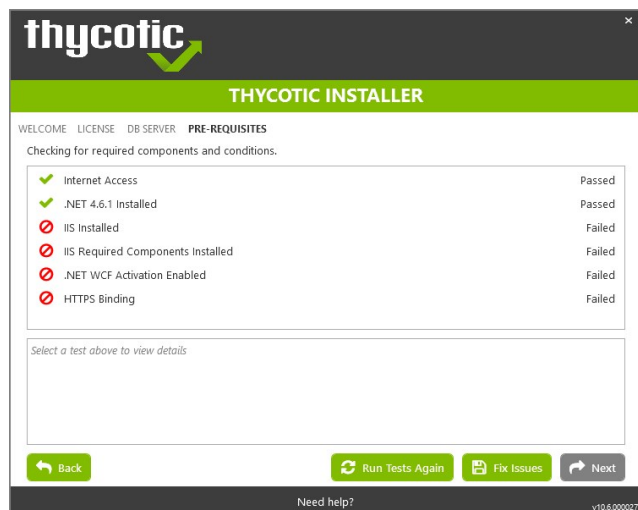
1. Open your Server Manager, in the upper right side of the screen, click Manage, then Add Roles and Features from the dropdown list. This will open your Add Roles and Features Wizard. Verify that the correct Destination Server is listed in the upper right-hand side of the screen.
2. Click Next through the Wizard steps until you arrive on the Features page.
3. Check the box next to the latest .NET Framework, here it is the .NET Framework 4.6 Features, click Next.



Follow the rest of the Wizard's steps until the install is completed. Once .NET 4.6 or greater framework is installed on your server, then run the pre-requisites check again.

IIS not installed

Don't have IIS installed yet? This is what you will see:



To Resolve:

Click the Fix Issues button on the Thycotic Installer. Then run the pre-requisites checks again.

HTTPS Binding Error

Did you encounter an HTTPS Binding Error? Does it not clear after using the Fix Issues button?

To Resolve:

Close and re-open the Thycotic Installer and run the pre-requisites checks again.

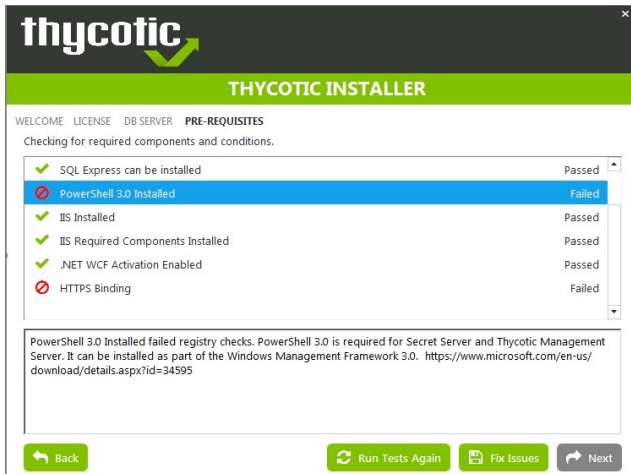
If the Binding Error persists, verify the following:

For combined Privilege Manager and Secret Server installations, did you previously move the Secret Server app pool in IIS to its own website, rather than allowing it to reside under the Default website? [see this KB for details.](#)

The installer checks the Default Web Site for an HTTPS binding, and whether there is a certificate assigned to it. This means that if you pre-created the Secret Server Web Application and assigned the HTTPS binding to that site, you may need to manually move your previously installed Secret Server IIS site to reside back under the Default Web Site in IIS when installing Privilege Manager.

PowerShell Error

Are you receiving a Powershell error? You may be trying to install Privilege Manager on an outdated server! Here's what you will see:



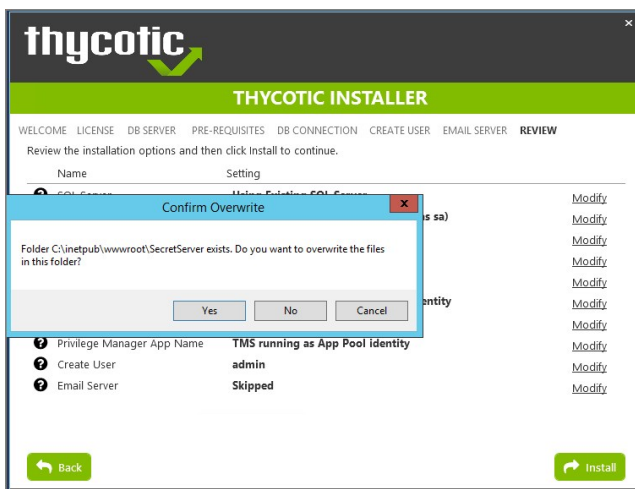
To Resolve:

You may need to update the server you are installing on. Please see our System Requirements Guide for supported servers. You can also manually download Powershell 3.0 and install it from Microsoft's website here.

Once Powershell is properly installed on your server run the pre-requisites checks again.

Secret Server and Privilege Manager Installed

Already have Secret Server installed on your server? Here is what you will see:



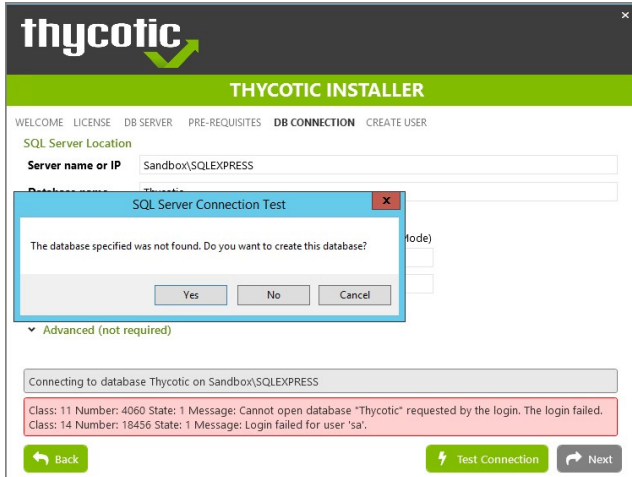
To Resolve:

We recommend installing new instances of Secret Server and Privilege Manager on a clean server.

If you do not already have an instance of Secret Server or Privilege Manager on this server to your knowledge, these files may exist due to an incomplete install. Check with anyone with access to this server who may have attempted this install previously. Only if you are confident that this is your first and only existing Secret Server or Privilege Manager instance click Yes to overwrite the existing files.

Error in DB File Path

Trying to test your connection to an existing SQL database? Here's what you will see:



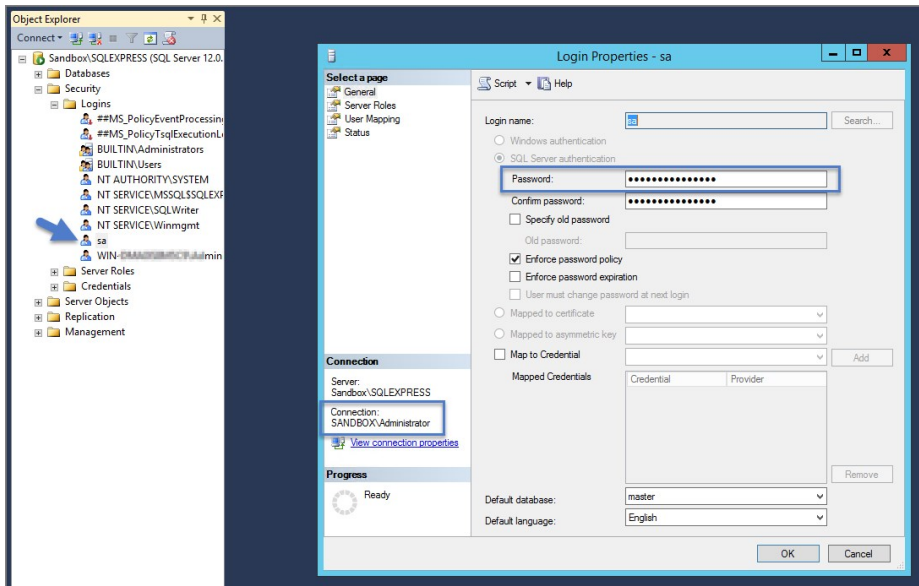
To Resolve:

This message means that your file path to your database is incorrect or your account does not have the correct permissions to access it.

If you have an existing database,

1. navigate to your SQL Server Management Studio and login.
2. Navigate to Security | Logins and right click on the account you are using for your Thycotic product, click Properties.

The information you need to enter in the Thycotic Installer for the connection path is listed in the bottom left corner under "Connection." You will also need to provide this account's password. Note that this account must have **db_creator** permissions.



Outdated Browser

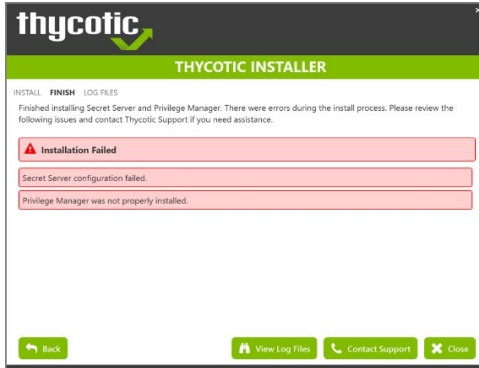
Are you trying to open your newly installed Privilege Manager in an outdated version of Internet Explorer? Here's what you will see:



To Resolve: Try opening Privilege Manager in a different browser, or update your Internet Explorer browser.

Integrated Authentication Error

Are you using Integrated Authentication and your installation failed? Here's what you will see:



To Resolve:

For clients using Windows Integrated Authentication, the Thycotic installer does not validate your database connection, so entering the wrong database server, database name, or if the user account provided does not have access to the database, your install will fail without warning you in advance. To resolve, please verify your database connection settings and enter them correctly under the **DB Connection** tab during the installation process.

While attempting to upgrade Privilege Manager, you receive an error message when accessing <https://YourInstanceName/TMS/Setup>.

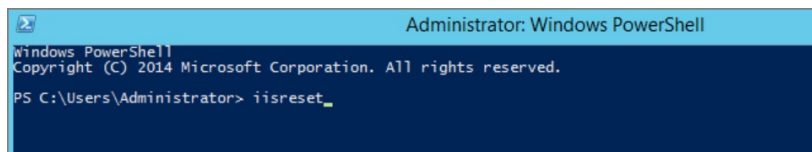
The window is unable to load with the following error message:

*Server Error in '/Tms/Setup/' Application.

Retrieving the COM class factory for component with CLSID (228FB8F7-FB53-4FD5-8C7B-FF59DE606C5B) failed due to the following error: 800703fa Illegal operation attempted on a registry key that has been marked for deletion. (Exception from HRESULT: 0x800703FA).*

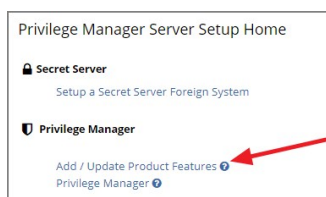
Resolve

1. Close the browser window.
2. Complete an IIS reset by searching for the Windows Powershell application.
3. Right-click and select Run as Administrator.
4. Enter in: **IISreset** | hit **Enter**.



5. Once the IIS reset has completed navigate back to <https://YourInstanceName/TMS/Setup>.

6. Click **Add / Update Product Features**.



7. Click **Install/Upgrade Products**.

Product Name	Installed	Available	Published	
Application Control Solution	10.8.1072	10.8.1072	7/15/2020 3:05 PM	Repair
Cylance Reputation Connector	10.8.1035	10.8.1072 New	7/15/2020 3:06 PM	Upgrade
Directory Services Connector	10.8.1121	10.8.1121	7/9/2020 5:53 PM	Repair
File Inventory Solution	10.8.1020	10.8.1020	7/6/2020 5:21 PM	Repair
Local Security Solution	10.8.1032	10.8.1032	7/9/2020 4:53 PM	Repair
Privilege Manager	10.8.1961	10.8.1961	7/16/2020 4:46 PM	Repair
Privilege Manager Application Programming Interface	10.8.1136	10.8.1136	7/1/2020 12:46 PM	Repair
Privilege Manager Mobile Console	10.8.1007	10.8.1007	5/1/2020 2:41 PM	Repair
Privilege Manager Server Core Maintenance	10.8.1396	10.8.1396	7/16/2020 4:18 PM	Repair
Privilege Manager Server Core Solution	10.8.1396	10.8.1396	7/16/2020 4:18 PM	Repair
Privilege Manager Silverlight Console	10.7.1447	10.7.1447	11/7/2019 2:30 AM	Repair
ServiceNow Connector	10.8.1006	10.8.1011 New	7/17/2020 5:48 PM	Upgrade
Symantec Management Platform Connector	10.7.1008	10.8.1002 New	7/1/2020 7:35 PM	Upgrade
SysLog Connector	10.8.1012	10.8.1012	5/25/2020 1:30 PM	Repair
System Center Configuration Manager Connector	10.8.1005	10.8.1011 New	7/1/2020 7:35 PM	Upgrade
VirusTotal Reputation Connector	10.8.1035	10.8.1072 New	7/15/2020 3:06 PM	Upgrade

Install/Upgrade Products Refresh

8. Select **ALL** required solutions.
9. Click **Install** and the upgrade process will begin.

This section provides a collection of possible performance issues and their remediation options.

The following topics are available:

- [Improve Boot-up Performance](#)
- [Unable to access Privilege Manager](#)

In environments with policies having many filters, starting policy analysis during boot-up can impact the overall boot performance.

If this is an issue in your environment you can pause the policy analysis during boot. Pause analysis during the boot-phase decreases CPU utilization and delays to the boot process.

The end of the boot-phase in which policy analysis is paused, is defined as the CPU utilization after start-up being below 25% for a minimum of 120 seconds. Once that benchmark is reached, policy analysis will start.

Warning: Using this feature opens your systems up to vulnerabilities during the boot-phase due to policies not being enforced for a certain amount of time, until the above mentioned condition is met.

Enable Pausing Policy Analysis during Boot-up

Each policy by default has a list of policy enforcement options under **Advanced | Policy Enforcement**.

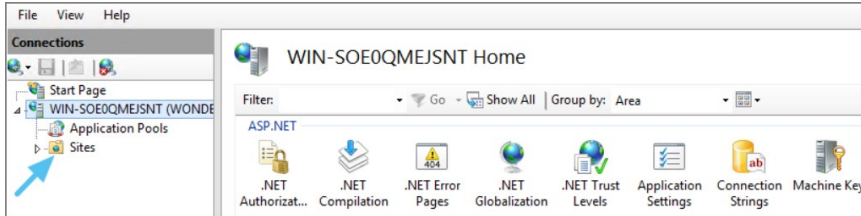
Policy Enforcement	
Continue Enforcing	<input type="checkbox"/> After an application meets the criteria of this policy, the agent will continue checking if it matches additional policies. If this setting is not enabled, subsequent policies will not be evaluated.
Applies To All Processes	<input type="checkbox"/> Policy will apply to system based processes. If setting is not enabled, policy will only apply to interactive users.
Enforce Child Processes	<input type="checkbox"/> Include child processes in the policy enforcement
Stage 2 Processing	<input type="checkbox"/> Only needed for catch-all deny policies to ensure that the policy only applies to applications NOT allowed directly or indirectly by a policy that applies to the parent process.
Skip Policy Analysis at Start-up	<input type="checkbox"/> Pauses policy analysis during boot-up (use only on filter heavy policies)

To enable pausing policy analysis during boot-up on filter-rich policies, set the **Pause Policy Analysis During Boot** switch to on and save the change.

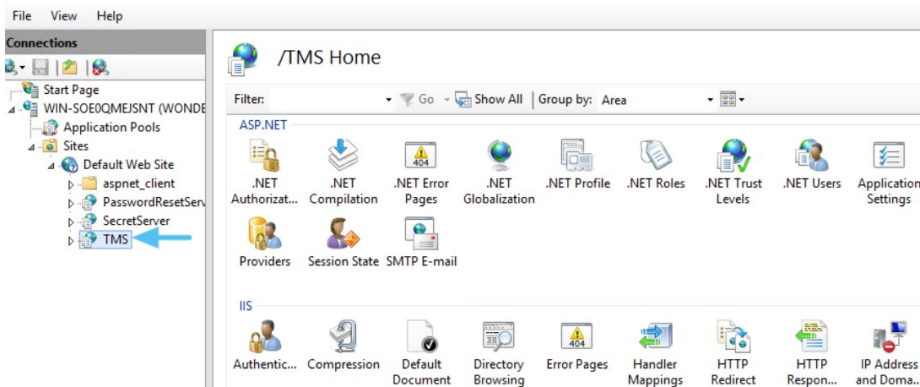
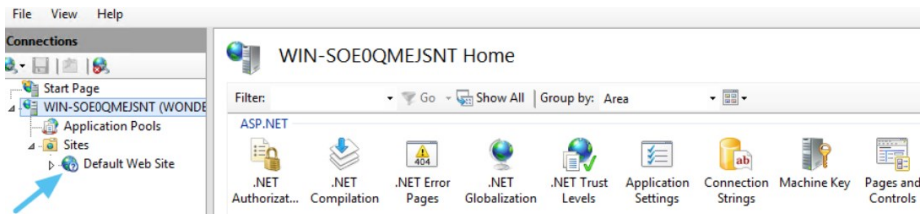
When attempting to login to Privilege Manager and you are unable to access the application window and you are continuously redirected to the login modal, verifying the IIS settings and resetting the app server might help.

Resolve

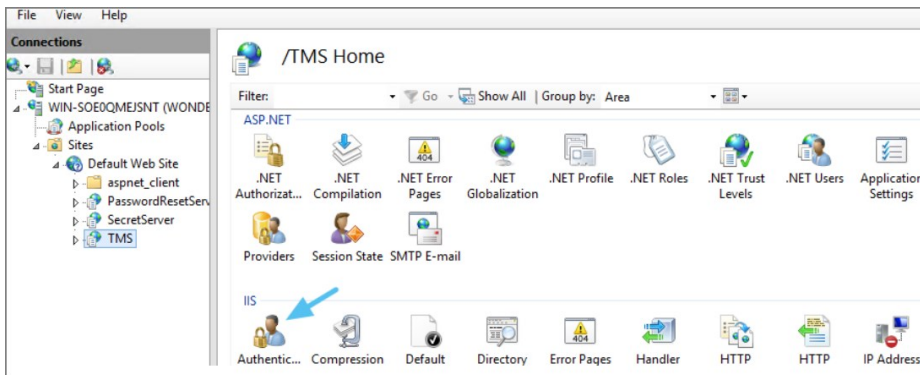
1. Open **Internet Information Services (IIS) Manager**.
2. Expand **Sites**.



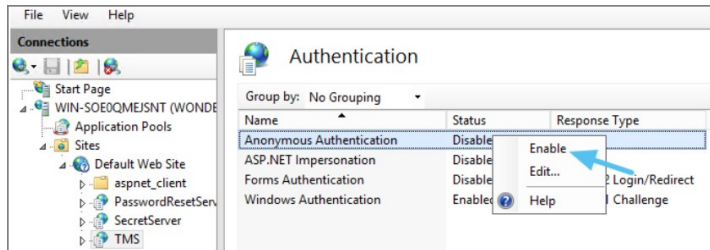
3. Click the **TMS** Site.



4. Click on **Authentication**.

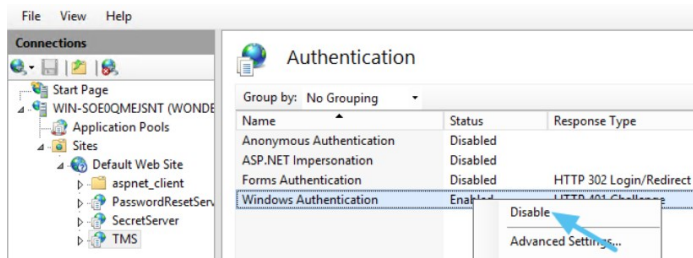


5. Right-click on **Anonymous Authentication**.
6. Click **Enable**.

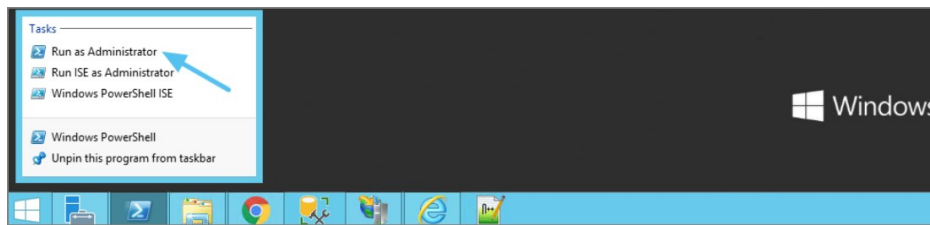


7. Right-click on **Windows Authentication**.

8. Click on **Disable**.



9. Open **Powershell**, type `isreset` and press **Enter**.



10. Launch **Privilege Manager**.

The following topics dealing with logs in Privilege Manager are available:

- [Where are My Server Logs?](#)
- [Where are My Agent Logs?](#)
- [SQL Server Transaction Logs](#)
- [User Interface and Ports](#)

When something goes wrong in any technological platform, the best clues about 'why' are usually buried in log files. In Privilege Manager, it depends on 'what' is happening to know where to look for clues first, but server log files are usually a good are to start.

All Server-Side Privilege Manager Logs are written to %PROGRAMDATA%\Thyctic\Logs. Usually that means the folder path on your server is C:\ProgramData\Thyctic\Logs.

Keep in mind that the shared folder ProgramData can be hidden. You can enter this path directly in your file explorer's navigation bar to find the logs.

Within the Logs folder, you will find one log file for each web app. (e.g. Tms.log, Tms-Setup.log, Tms-Worker.log, etc.). When submitting a case to Thyctic's Support team, it is always a good practice to send these log files.

```

TMS - Notepad
File Edit Format View Help
INFO - 2017-08-16T14:46:58 Searching for server cert in bindings for site "Default Web Site"
INFO - 2017-08-16T14:46:58 Using server certificate thumbprint "A6528C9D0866F8485D451F876E124C9F91DE3DC3" - demonmain.
INFO - 2017-08-16T14:46:58 Registering Service Locators
INFO - 2017-08-16T14:46:58 Database is configured
WARN - 2017-08-16T14:47:02 No proxy server is specified
INFO - 2017-08-16T14:47:02 Have 6 Console items
INFO - 2017-08-16T14:47:02 Mapping console 62a7e338-e2cd-47ac-bde8-45b5edebed174 route "HelpDesk" from url "HelpDesk/{*queryv:
INFO - 2017-08-16T14:47:02 Mapping console f2e19194-9b58-40b9-b508-b9d9bdc461d4 static route "PrivilegeManager" from url "Pri
INFO - 2017-08-16T14:47:02 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorer" from url "ResourcE
INFO - 2017-08-16T14:47:02 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorerAspx" from url "Resou
INFO - 2017-08-16T14:47:02 Mapping console 352214ad-df09-4842-aa6e-bc47451b6c59 route "SecurityManager" from url "SecurityMar
INFO - 2017-08-16T14:47:13 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:47:14 Platform Environment for Virtual App Default Web Site - /TMS (/TMS) Closing. Shutdown Reason Host:
INFO - 2017-08-16T14:47:14 SqlMessageBus got !immediate stop message, closing down SignalR processing.
INFO - 2017-08-16T14:47:14 SignalR: SQL message bus disposing, disposing streams
WARN - 2017-08-16T14:47:44 SqlMessageBus got immediate stop message.
INFO - 2017-08-16T14:47:44 SignalR Stream 0 : SqlReceiver disposed
INFO - 2017-08-16T14:53:18 Searching for server cert in bindings for site "Default Web Site"
INFO - 2017-08-16T14:53:18 Using server certificate thumbprint "A6528C9D0866F8485D451F876E124C9F91DE3DC3" - demonmain.
INFO - 2017-08-16T14:53:18 Registering Service Locators
INFO - 2017-08-16T14:53:18 Database is configured
INFO - 2017-08-16T14:53:19 Have 6 Console items
INFO - 2017-08-16T14:53:19 Mapping console 62a7e338-e2cd-47ac-bde8-45b5edebed174 route "HelpDesk" from url "HelpDesk/{*queryv:
INFO - 2017-08-16T14:53:19 Mapping console f2e19194-9b58-40b9-b508-b9d9bdc461d4 static route "PrivilegeManager" from url "Pri
INFO - 2017-08-16T14:53:19 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorer" from url "ResourcE
INFO - 2017-08-16T14:53:19 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorerAspx" from url "Resou
INFO - 2017-08-16T14:53:19 Mapping console 352214ad-df09-4842-aa6e-bc47451b6c59 route "SecurityManager" from url "SecurityMar
WARN - 2017-08-16T14:53:20 No proxy server is specified
INFO - 2017-08-16T14:54:29 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:55:40 AuditManager worker starting.
INFO - 2017-08-16T14:55:44 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:56:55 SignalR:Stream 0 : SQL notification change fired
    
```

By default, these log files will contain informational events, warnings, and errors.

Not included in your default logs are verbose/trace/debug errors, but this is configurable via the web-logging.config file in each web app directory discussed below. If interested in changing your log settings, you can find more information about the Log4Net Core "Level Value" options here: <https://logging.apache.org/log4net/log4net-1.2.11/release/sdk/log4net.Core.Level.html>

To edit log settings (i.e. Log trimming by size, type of recorded Log4Net Events) you can edit the code in your web-logging file, usually located in C:\inetpub\wwwroot\TMSweb-logging. By default, this file looks like this:

```

<?xml version="1.0" encoding="utf-8" ?>
<log4net>
<root>
<level value="INFO" />
<appender-ref ref="Thyctic.LogFileAppender" />
</root>
<logger name="Thyctic">
<level value="INFO" />
</logger>
<appender name="Thyctic.LogFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="$([ProgramData])\Thyctic\Logs\TMS.log" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="34" />
<maximumFileSize value="1 MB" />
<lockingModel type="log4net.Appender.FileAppender+MinimalLock" />
<layout type="Thyctic.Platform.Logging.Log4NetSimpleLayout,Thyctic.Platform"></layout>
</appender>
</log4net>
    
```

If something is going wrong on specific endpoints, another place to look for answers is in your Agent's Event Log Viewer.

In your endpoint machine, navigate to your Thycotic Agent files. This is usually located in C:\Program Files\Thycotic\Powershell\Arellia.Agent. Right-click on AgentLogViewer and select Run with Powershell. This will open your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server.

For remote access, Agent logs are also viewable through the Windows Event Viewer.

Scroll all the way to the top of the page to see the most recent activity from your Thycotic Agent. Uncheck the Information box on the upper righthand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.

TimeGenerated	Message	Source	Module
10/08/2017 14:15:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:16:51 PM	Arellia Agent	Arellia Agent Service
10/08/2017 14:15:51	Performing ACS ProcessEvents	Arellia Agent	Arellia Agent Service
10/08/2017 14:14:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:15:51 PM	Arellia Agent	Arellia Agent Service
10/08/2017 14:14:51	Performing ACS ProcessEvents	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:56	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:56	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:52	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:52	Completed TaskInstance f19311c0-00af-4401-804e-f3c21c91db7e - Client Command 'Resource Discovery Command'...	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:52	Resource discoverer 0120439e-267b-422a-bbd8f3e659534785 did not return any discovery/xml	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:52	Unable to locate a file with hash f1a1zTr2LNVB0gk3cGv8WmJAQb4+ for Resource (7f58334e-7d8b-5620-9EEA-99...	CFieResourceDisc...	ArelliaFileInvtAgent.dl...
10/08/2017 14:13:52	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:14:51 PM	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:51	Performing ACS ProcessEvents	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:51	Initiating taskinstance f19311c0-00af-4401-804e-f3c21c91db7e with clientCommandId 'Resource Discovery Command'...	Arellia Agent	Arellia Agent Service
10/08/2017 14:13:47	Queued Task f19311c0-00af-4401-804e-f3c21c91db7e - Command 'Resource Discovery Command' (77582ef2bd52...	Arellia Agent	Arellia Agent Service
10/08/2017 14:12:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:13:51 PM	Arellia Agent	Arellia Agent Service
10/08/2017 14:12:51	Performing ACS ProcessEvents	Arellia Agent	Arellia Agent Service
10/08/2017 14:11:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:12:51 PM	Arellia Agent	Arellia Agent Service
10/08/2017 14:11:51	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia Agent Service
10/08/2017 14:11:51	Performing ACS ProcessEvents	Arellia Agent	Arellia Agent Service
10/08/2017 14:11:47	Policy 'Event Discovery Testing Computers Audit Policy (Windows)' (398d5118-13ad-4425-9877b513bc4903db) priorit...	CASMonitor	ArelliaACSvc.exe

SQL Server maintains a history of all operations using a Transaction Log. If this transaction log becomes full, you may receive one or more of the following errors:

- System.ArgumentException: Cannot add two background tasks with the same name.
- Thycotic.Data.DataAccessorException: The transaction log for database " " is full. To find out why space in the log cannot be reused, see the log_reuse_wait_desc column in sys.databases

By default, a transaction log can grow to an unrestricted size. A transaction log may become full under the following circumstances:

- The drive where the transaction log file is kept is out of disk space.
- The transaction log file hits its growth limit.

Possible solutions include:

- Backing up the log.
- Freeing disk space so that the log can automatically grow.
- Moving the log file to a disk drive with sufficient space.
- Increasing the size of a log file.
- Adding a log file on a different disk.
- Completing or killing a long-running transaction.
- Switching to simple recovery mode and truncating the log.

For more detailed information on transaction logs in SQL, see <http://technet.microsoft.com/en-us/library/ms345583%28v=sql.90%29.aspx>

When something goes wrong in Privilege Manager, the UI has a few places worth checking:

- **Admin | Diagnostics** - this will give you information on Agents and Operating Systems, click **Console Logs** for more details.
- **Reports | Diagnostics** - A great place to look for some useful programmed reports on Agents, Remote Tasks, Policies Not Received by Agents, Summary of Gauge States, and Licensing.

Connectivity

Are you having Connectivity issues? A few things to keep in mind:

- Outbound access from the agent to the server is done by default over port 443 (the standard port for HTTPS communication), but you may specify a different port if desired.
- The only port that the agent listens on is port 5593. This is not required. For example, you can block this port and agents will pull from the server on a set schedule.

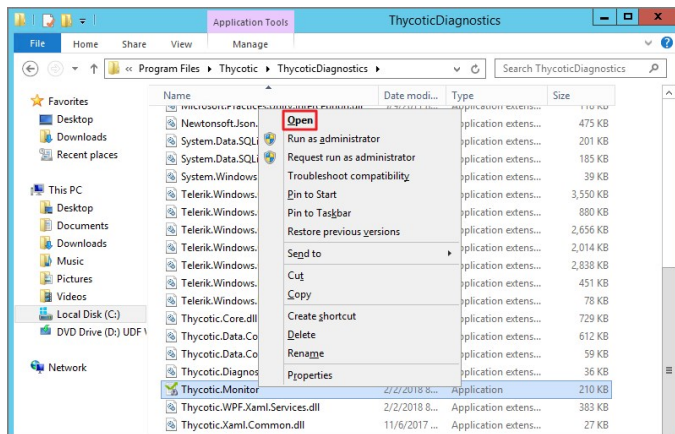
Using certain tools for troubleshooting purposes can help locating issues and finding a solution to a problem.

The following troubleshooting tools topics are available in this section:

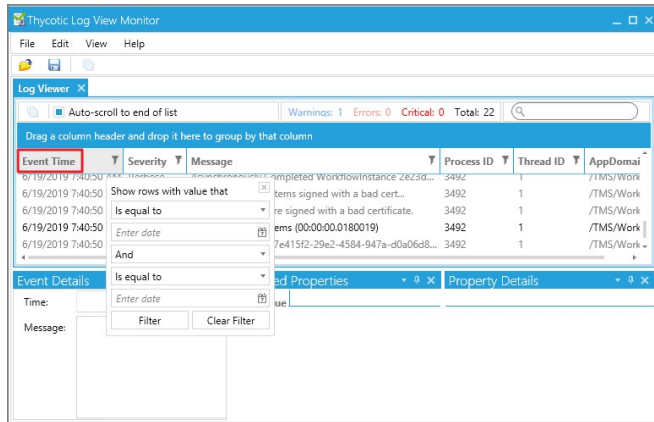
- [How to use the Thycotic Monitor for Troubleshooting](#)
- [Using Process Hacker for Troubleshooting](#)
- [Troubleshooting a Policy with Process Explorer](#)

While using Privilege Manager, you can utilize the Thycotic Monitor to help troubleshoot issues that occur on the web console.

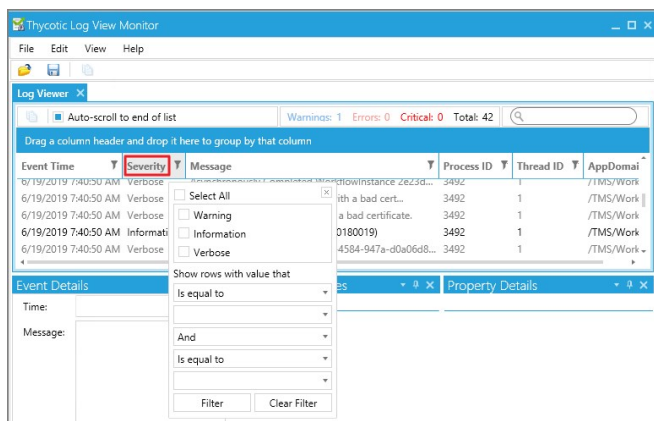
1. On the server with the Privilege Manager installation navigate to C:\ProgramFiles\Thycotic\ThycoticDiagnostics and open the Thycotic Monitor.
2. Right-click on Thycotic Monitor and select Open.



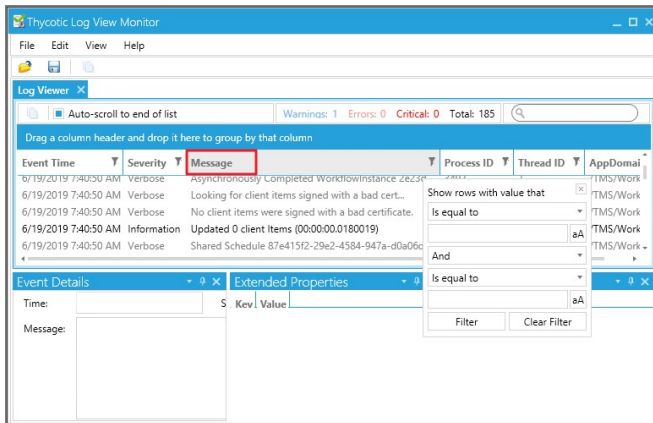
3. Left-click on the filter icon for Event Time to filter for specific times in order to better help find a specific event.



4. Left-click on the filter icon for Severity to filter for specific severity levels.



5. Left-click on the filter icon for Message to narrow down specific messages and GUID's to help find errors.



Note: If you're attempting to troubleshoot an issue open the Thycotic Monitor and replicate the issue on the server that Privilege Manager is installed on. It may also be helpful to grab a screenshot including a time-stamp from when you replicate the error in order to better help with troubleshooting.

1. Open the Thycotic Monitor.
2. Replicate the issue server-side.
3. Select **File**.
4. Select **Save**.

The file saves as a .tracelog file type. You can upload the tracelog to your support case or review the event details for further information.

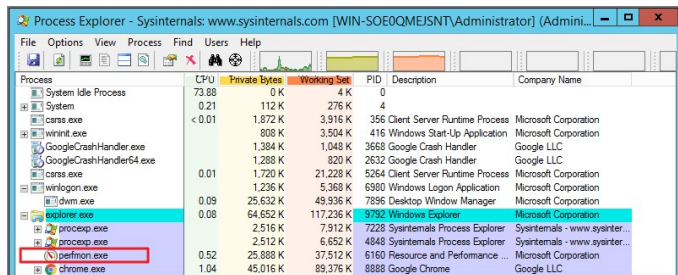
This topic describes how to troubleshoot a policy with Process Explorer. Process Explorer is used to look at policies that grant administrative privileges, but don't seem to work when

- an application is accessed, or
- actions are supposed to run.

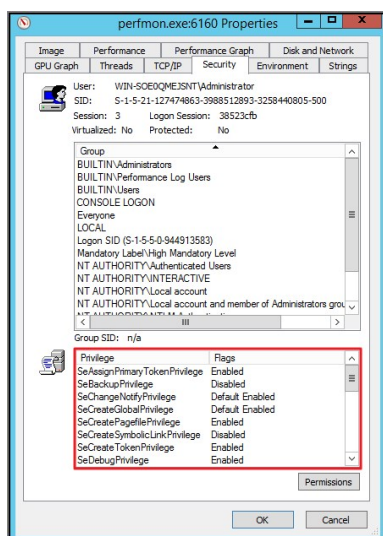
In the example below the policy allows resource monitor to run but the application is blank due to not having sufficient Windows Privileges. You can use Process Explorer to determine the correct Windows Privileges to add to the policy in order to use the resource monitor application.

Detailed Troubleshooting Steps

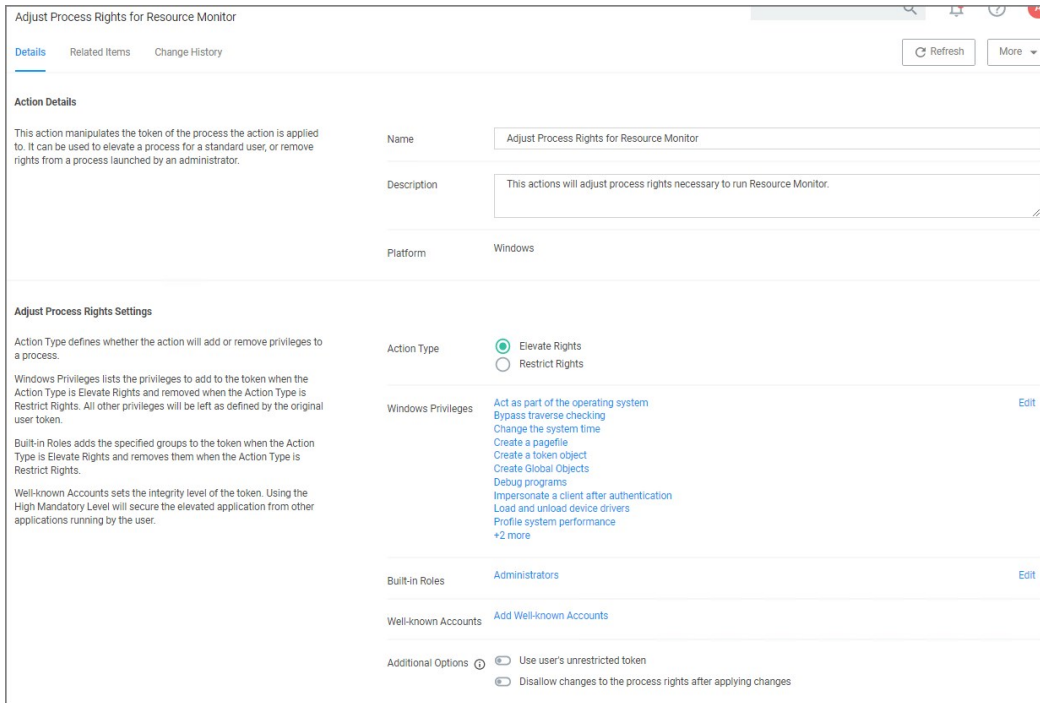
1. Download [Process Explorer from the Microsoft website](#) and extract the downloaded ProcessExplorer.zip file locally on your system.
2. Open **Process Explorer**.
3. Next open **Resource Monitor** as the Administrator.
4. Navigate back to the Process Explorer Window and find the Resource Monitor application (perfmom.exe).



5. Right-click and select **Properties**.
6. Select the **Security** tab.
7. Under the Privilege section, you can see all the flags that are enabled in order to use the application.



8. Launch Privilege Manager and navigate to **Admin | Application Policies**.
9. Select the policy that elevates privileges to run **Resource Monitor**.
10. Under **Adjust Process Rights**, modify settings.



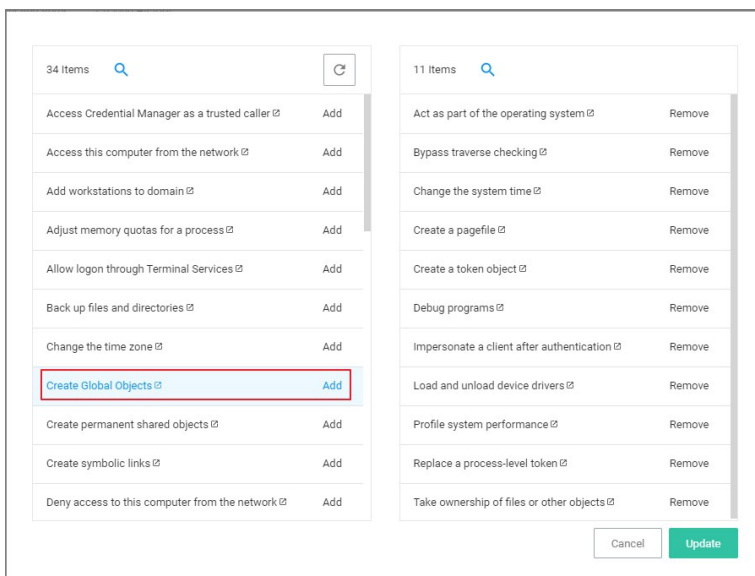
1. Select Add Administrative Rights or the elevation action you are using.

11. Under **Windows Privileges**, click **Edit**. (For this step you will have to determine which flags are enabled in Process Explorer in order to add the additional Windows Privileges to the action.)

12. In another window navigate to the following Microsoft web site @ <https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants>. The site will show the name of the Windows Privileges, along with the user right information that needs to be added to the action in Privilege Manager.

For Example: The privileges listed under the properties security tab show **SeCreateGlobalPrivilege** as enabled. On the Microsoft website for Privilege Constants @ <https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants> the user right for SeCreateGlobalPrivilege privilege is: **Create global Objects**.

13. Enter the User right into the search box and then select the user right from the returned list. In this example enter in Create global objects.



14. Click **Add**.

15. Remove any actions you don't need.

16. Click **Update**.

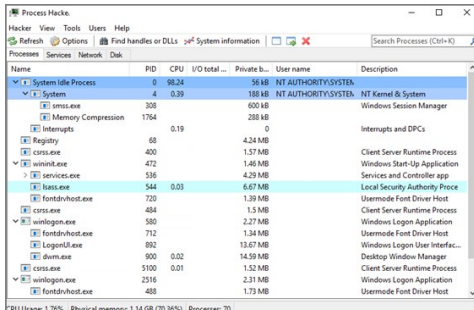
17. Click **Save Changes**.

Once the agent has received the updated policy, the additional Windows Privileges will be applied to the application next time it is launched.

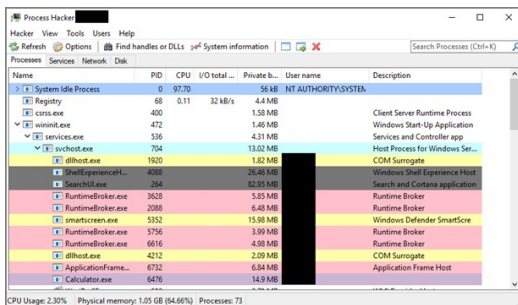
Process Hacker is a third-party tool that can be useful for troubleshooting as well. Please note that since this is a third-party tool, Thycotic is not responsible for any part of the application and has no control over it.

It can be used to determine whether a process you are trying to apply an action to is a parent process or a child process of another application. If you do not want to install Process Hacker on the endpoint you are troubleshooting from, there is a portable version available as well that does not require it to be installed on the machine.

When you open Process Hacker, you will notice a screen like the one below that shows the running processes on the machine.

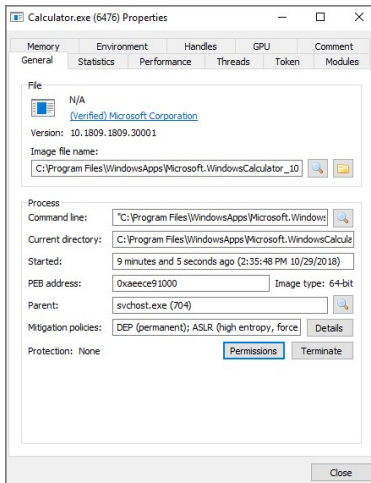


You will notice that some processes are listed underneath other processes. The processes listed under other processes are child processes of the top parent one. For example, after opening up the Calculator app on a test machine, the Process Hacker window looked like the screenshot below.



You can see at the bottom of the screenshot above that the Calculator.exe process is actually a child process of the svchost.exe process, which itself is a child process of the services.exe process, which is a child process of the wininit.exe process. Not all processes will be nested underneath as many parent processes as in this example.

You can also double-click on the process to open a window with more information about the process. You can find the parent process that way as well on the General tab of that window. The screenshot below is what the General tab shows for the Calculator.exe process.



You can see the Parent field, which shows you that the svchost.exe process is the parent of the Calculator.exe process. If you are viewing the parent process, then in the Parent field you will see "Non-existent process" instead of seeing a parent process listed.

You will also notice a Token tab in the screenshot above. That tab is useful in showing you whether the process is running elevated; it shows an "Elevated" field, with values Yes or No. It will also show you the process security tokens that the application needs to run. You normally do not need that information, but it is good to know where to find it, just in case.

As you can see from the information above, Process Hacker is a third-party tool that can be useful when troubleshooting why a policy is not applying like you think it should. For example, if you are trying to elevate a specific application or process, it might not be working correctly if that process is actually a child process. In that case, you can configure the policy to target the parent process and apply that same action to the child processes. You might not need to target the parent process in all situations, but sometimes it will be necessary.

Privilege Manager Mobile Application

The Privilege Manager Mobile console allows you to process approval requests, disclose passwords, and see alerts via the Privilege Manager Mobile Application on iOS and Android smartphones.

For the mobile app to work you must install the Privilege Manager Mobile Console, have Azure Active Directory setup to add an application registration, configure the Microsoft Azure Service Bus, and then install the Privilege Manager Mobile App.

The instructions are provided based on the assumptions, that

1. our customer is using Azure AD and has already configured the [Azure Active Directory App Registration](#) according to the docs to allow them to authenticate as an Azure AD user. The mobile application registration must be added to that **same domain**.
2. our customer has the ability to create an Azure Service Bus service.

To get started with the setup of the Privilege Manager Mobile Console, review and follow the instructions under the following topics in the order provided:

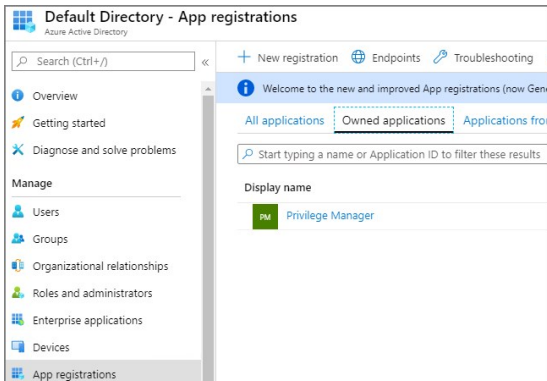
1. [Add the mobile application registration to your Azure Active Directory integration with Privilege Manager](#)
2. [Configure the Service Bus for Mobile](#)
3. [Install and Configure the Privilege Manager Mobile Console Solution on the Privilege Manager Server](#)
4. [Install the Privilege Manager Mobile App on a Mobile Device](#)
5. [Use the Mobile Application](#)

Configure Azure Active Directory

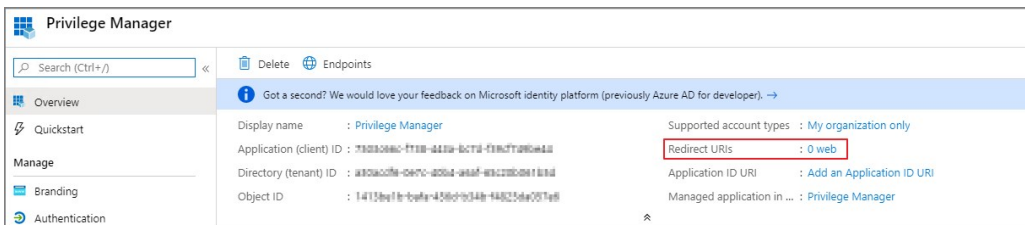
As a prerequisite for running the Privilege Manager Mobile Console, you must configure Azure Active Directory integration with Privilege Manager. Refer to [Setting Up Azure Active Directory Integration in Privilege Manager](#).

Once Azure AD integration for your Privilege Manager instance is configured, follow these steps to add an additional Redirect URI for the mobile application to the Azure AD application registration:

1. Open the **Azure Management Console**.
2. Navigate to your **Active Directory** instance.
3. Select **App registrations** from the menu.
4. Click the **Owned applications** tab.
5. From the list under Display name select your Privilege Manager registration.



6. Either select the **Redirect URI** links or the **Authentication** menu.



7. Select **Add a platform**.
8. Select **Mobile and desktop applications**.
9. Set the Redirect URI to exactly `http://ArelliaMobileClient`. There are two access points to do this either via:
 - o Redirect URI or
 - o Authentication menu.

The following table shows the steps you will see for each option:

<ol style="list-style-type: none"> 1. Click Add URI. 2. Enter <code>http://ArelliaMobileClient</code>. 	<ol style="list-style-type: none"> 1. Enter <code>http://ArelliaMobileClient</code>. 2. Click Configure.

Important: The URI value needs to exactly match `http://ArelliaMobileClient`.

10. Click **Save**.

On the **App registrations** page under **Owned applications**, take note of the **Application (client) ID**. You will need to use the client ID when you [Configure the Mobile Console in Privilege Manager](#).

The screenshot shows the 'Privilege Manager' application registration page. On the left is a navigation menu with 'Overview', 'Quickstart', and 'Manage' (containing 'Branding' and 'Authentication'). The main area shows the application details for 'Privilege Manager'. A red box highlights the 'Application (client) ID' value: 7803098c-f118-441a-bc7d-f19c7195e41d. Other visible values include 'Directory (tenant) ID' and 'Object ID'. A search bar and 'Delete'/'Endpoints' buttons are at the top.

Display name	: Privilege Manager
Application (client) ID	: 7803098c-f118-441a-bc7d-f19c7195e41d
Directory (tenant) ID	: a80a0c0e-047c-4004-a6a7-8a3278e0e18d
Object ID	: 1413be18-7c9e-458c-b348-f4625da907e9

Configure the Service Bus for Mobile

For this a Service Bus Queue needs to be created, always refer to the latest instructions as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue](#).

For this a Service Bus Queue needs to be created, refer to the latest instructions as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue](#).

If you already have an existing Service Bus in Azure, you are welcome to use the existing setup. You just need to create a new queue within your existing Service Bus to be used by the Mobile App.

The following steps explain what is required for the Mobile App integration:

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have to use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Do not check any of the options, using the defaults is fine. Take note of the queue name you gave it.

Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the Thycotic Privilege Manager Console, click **Admin | Configuration**.
2. Click the **User Credentials** tab.
3. Click **Create**.

1. Enter a **Name**, for example *Azure Service Bus Credential*.
 2. Set the Account name to **RootManageSharedAccessKey**.
 3. Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Creating a Service Bus and Queue in the Azure Portal" above.
 4. Click **Save Changes**.
4. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
 5. Click the **Azure Service Bus** option.
 6. Click **Create**.

1. Enter a **Name**, for example *Mobile App Azure Service Bus...*
2. Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above). Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).
3. Set the **Enabled** switch to **No** for now.
4. Click **Create**.

Configuration Change History Refresh More

Foreign System Details

Name Mobile App Azure Service Bus

Description Provides internet client connectivity via the Azure Service Bus

Settings

Credential

Enabled No

URL [YourServiceBus]

QueueName

QueuePolicyName

QueuePolicySecret

5. Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).
 6. Leave the URL field as is (and ignore the fact that it's called URL – it's just the Service Bus name).
 7. Make sure the URI matches the first part of the namespace created in Azure.
 8. Set the QueueName to the same queue name created above in **step 4** under "Creating a Service Bus and Queue in the Azure Portal".
 9. Set the Queue Policy Name to **RootManageSharedAccessKey**.
 10. Set the Queue Policy Secret to the **Primary Key** as obtained in **step 3** under "Creating a Service Bus and Queue in the Azure Portal" above.
 11. Click **Save Changes**.
 12. Enable the Service Bus, set Enabled switch to **Yes**.
7. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:
- o **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>
 - o **Cloud:** <https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc>

Wait for the page to respond.

You are now ready to install the Thycotic ACS application on your mobile devices.

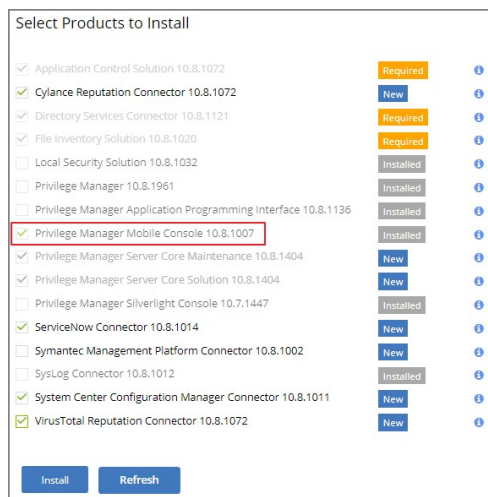
Install and Configure the Mobile Console in Privilege Manager

To configure the Mobile Console in Privilege Manager, you must:

1. Install the Privilege Manager Mobile Console.
2. Set the Client ID and Tenant ID.
3. Configure the notification settings.

The Privilege Manager Mobile Console needs to be installed on the same server that is running the Privilege Manager instance.

1. Navigate to your Privilege Manager setup page or select **ADMIN | More...** and select the **Add / Update Program Features**.
2. Click **Select Products to Install**.

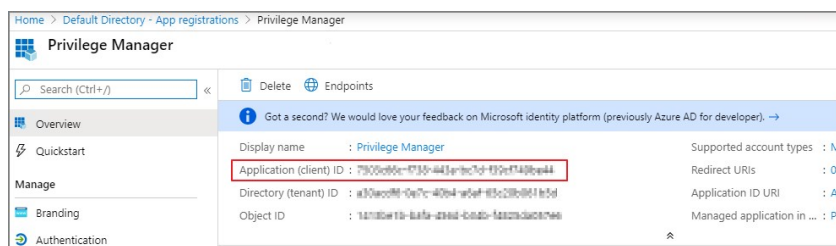


3. Select **Privilege Manager Mobile Console** and click **Install**.

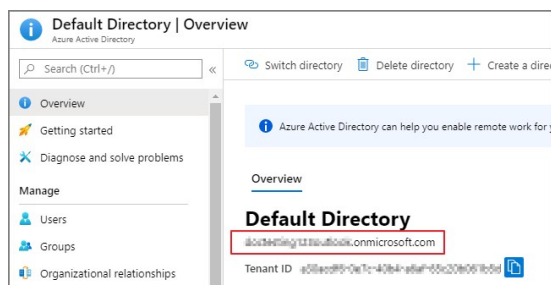
Once the installation completes click **Home** to navigate back.

After you have installed the Privilege Manager Mobile Console, set the Client ID and Tenant ID.

1. Navigate to **Admin | Configuration**.
2. Select the **Advanced** tab.
3. Scroll down and under **Thycotic Mobile Console Solution** under General enter values for:
 1. **Your client id**: In the **Your client id** field, enter the Client Id that you generated when you configured the Microsoft Azure Active Directory. In the Azure AD portal, you find this under App Registration. Look for the **Application (client) ID** value.



2. **Your tenant id** is the DNS name of the Azure Active Directory instance. You find it on the Azure AD Home page, between the friendly name and the Azure Tenant ID, for example **name.myinstance.com** or **MyCompanyName.onmicrosoft.com**.



Enter that DNS in the **Your tenant id** field.

Configuration

General Discovery Reputation Credentials Foreign Systems **Advanced** Authentication Change History

Privilege Manager Solution

Thycotic Mobile Console Solution

General

Your client id * ⓘ

Your tenant id * ⓘ

4. Click **Save Changes**.

The notification settings for the mobile app are available via general configuration and task automation.

1. Navigate to **Admin I Configuration**.
2. Select the **General** tab.

Configuration

General Discovery Reputation Credentials Foreign Systems Advanced Authentication Change History

Policy Targeting ⓘ

Approval Types

Default Execute Application Request Type
Default Offline Execute Application Request Type

Approval Processes

Default Manual Approval Process
Mobile Message Approval Process

3. Under Approval Processes click **Mobile Message Approval Process**

Mobile Message Approval Process

Secret Server and Thycotic One authentication aren't compatible with mobile.

Details Change History

Approval Process Details

Name

Description

Settings

Approval role allowed ⓘ

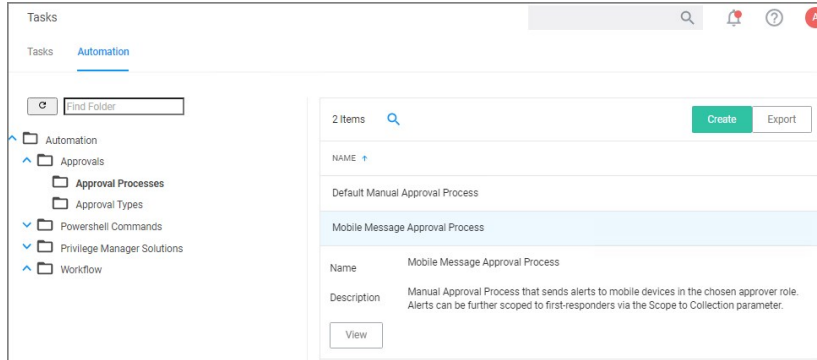
Scope to collection (optional) ⓘ

Message

Start activity ⓘ

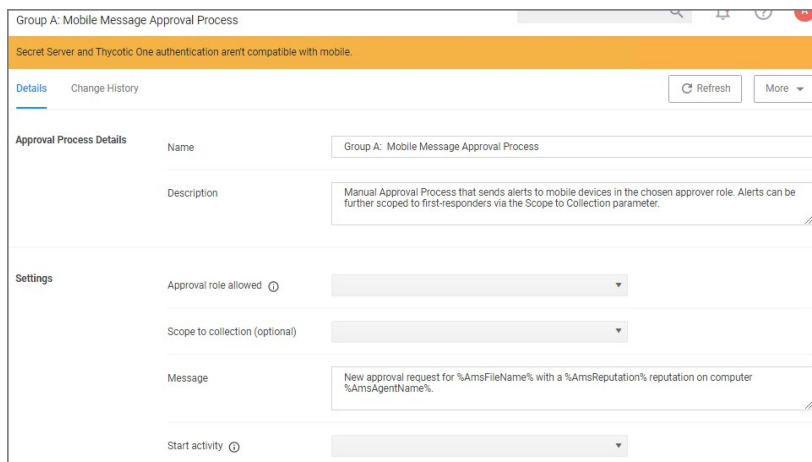
This task can also be accessed via **Admin I Tasks**, selecting the **Automation** tab and the in the

folder tree **Automation | Approvals | Approval Processes | Mobile Message Approval Process**.



4. For customization, duplicate the default task. Give it a meaningful name for your environment.

5. Click **Create**.



6. Under **Settings**, you specify

- o **Approval role allowed**, which roles have approval permissions. By default the alerts for new approval requests will only be sent to mobile users in the Administrators role. You can change this setting by adding the approver role to a different role.
- o **Scope to collection (optional)**, which is an optional setting, to scope these messages to a subset of users in that role.
- o **Message**, what message will be displayed to the approver when a approval request was triggered.
- o **Start activity**, which is an optional setting, any activity you wish to start as part of the approval.

7. Click **Save Changes**.

To start sending notifications to phones, select the **Default Execute Application Request Type** and change the **Approval Process** from the **Default Manual Approval Process** to the **Mobile Message Approval Process** and save the changes.

Note: The approval process change to Mobile Message Approval Process is only for the notification message that an approval was requested. The actual approval has to be followed through via HelpDesk interface. Currently approval requests cannot be approved via the Mobile app.

You can also send notifications based upon report data. These can be used to send alerts for suspicious activity, etc. An example of this can be found under **Tasks | Server Tasks | Mobile Messaging | Mobile Message Alert for Password Disclosures on VIP Systems**.

Mobile Message Alert for Password Disclosures on VIP Systems

This item is read-only.

Details Task History Change History Duplicate More

Details

Name	Mobile Message Alert for Password Disclosures on VIP Systems
Description	This task will send a mobile message alert when a password on a VIP System has been disclosed

Parameters

Parameters for this task.

Data source *	Password Disclosures on Monitored Computers Query
Target mobile devices *	

Schedules

Schedules for this task.

0 Items

New Schedule

This message can be executed on a schedule to send alerts for any password disclosures on VIP

Systems. VIP Systems are configured via the Monitored Computers parameter that allows you to choose a Collection of computers.

The Privilege Manager Mobile Console does currently not work with Secret Server or ThycoticOne as the authentication provider. If Secret Server is configured as the authentication provider in Privilege Manager, a warning message is shown on the Mobile Message Approval Process configuration page.

Mobile Message Approval Process

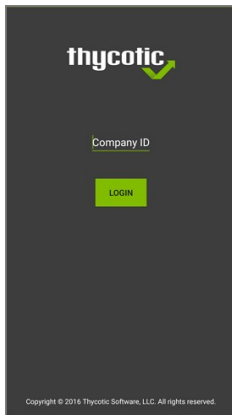
Secret Server and Thycotic One authentication aren't compatible with mobile.

Details Change History

Mobile App Install and Sign In

After installing and configuring the server components, help desk users can download the Mobile app for their smartphone via the appropriate app store by searching for **Thycotic ACS**. After you install the app, do the following:

1. Open the application on the mobile device.



2. When prompted for the **Company ID**, enter the name of your **Service Bus**. To find the name, open the Azure Portal, locate the Service Bus that is being used for this integration. Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance in the list of Service Bus instances).
3. Next enter the Azure Active Directory user credentials.
4. Create a pin to secure the Mobile app.

If you experience any issues completing those steps, try the following to solve the problem:

1. Verify that you can reach the Service Bus worker service by pointing your browser at the ServiceBus worker service. Enter the URL into your browser navigation bar:
 - o **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>
 - o **Cloud:** <https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc>

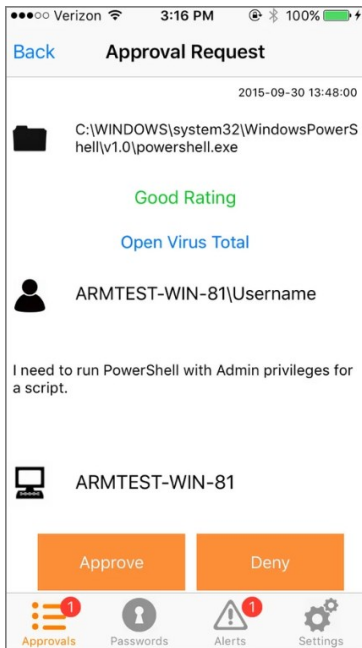
Wait for the page to respond.

2. Verify the Redirect URI setting in your Azure AD application registration matches the configuration values in Privilege Manager.
3. **Recycle the App Pools on the Privilege Manager Instance** following any changes for this integration. Without the recycle, the new settings won't be applied.

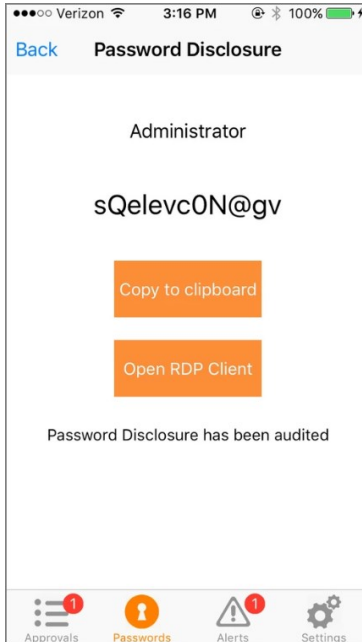
Cloud customers, please contact support for assistance to get these recycled. Unfortunately, this is a "must-contact" situation.

Use the Mobile Application

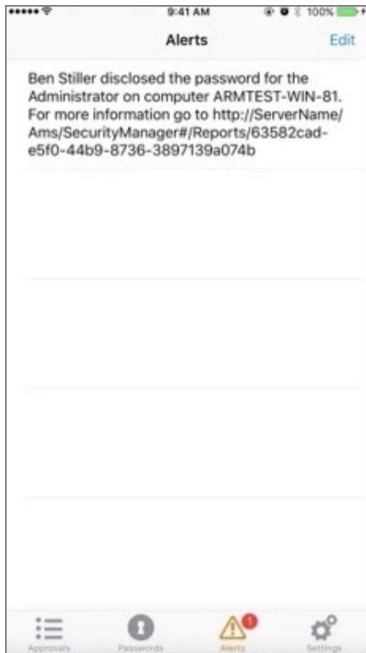
Approval Requests area provides the ability to approve/deny pending approval requests and the ability to view recently approved requests.



Password Disclosure area provides the ability to disclose managed user passwords that the mobile user has access to.



The Alerts area provides the ability to view non-approval request alerts, such as the Password Disclosures on VIP Systems. These alerts can be forwarded via e-mail or removed.



Release Notes

This section includes the most recent Privilege Manager Release Notes.

- [10.8.2 Release Notes - On-prem/Cloud](#)
- [10.8.1 Release Notes - On-prem/Cloud](#)
- [10.8.0 Release Notes - On-prem/Cloud](#)
- [10.7.1 Release Notes - On-prem/Cloud](#)
- [10.7.0 Release Notes - On-prem](#)
- [10.6 Release Notes - On-prem](#)
- [10.6 Release Notes - Cloud](#)
- [10.5 and previous releases Release Notes](#)

10.8.2 Release Notes

December 2nd, 2020:

Enhancements available with the 10.8.2 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Added [CorrelationID support to Server Logs](#).
- Added [Complex Password Policy enforcement for Privilege Manager users](#).
- Added API Client User logout option via delete method on [API Authentication](#) endpoint.
- Added [Visual Studio Installer Elevation](#) example policy and filters to configuration feeds.

Security

- Added Process Hollowing prevention for elevated applications. The 10.8.2 Privilege Manager agent adds memory checks for all processes that are elevated via Privilege Manager.
- Return of generic "Invalid username or password" messages.
- Unknown code fallback to generic error message, such as "unable to login".
- Generic HTTP response messages.
- Removed ASP.Net MVC Default HTTP Headers information.
- Updated jQuery to latest version.
- Updated Handlebars to latest version.
- Privilege Manager Cloud server side enforcement of TLS 1.2. On-premises instances can be configured to enforce TLS 1.2 at the OS level.

macOS

- In support of Apple's Catalina and Big Sur macOS System Extension based security enhancements, a [Privilege Manager agent for SYSEX based endpoints](#) is made available.
- New [Just-in-Time \(JIT\) Group Membership action](#) for elevation/approval policies.
- Added [elevation support for move to trash bin](#) when standard user is deleting from /Applications directory.
- Modified [policy with Allow Package Installation action workflow](#) behavior for .pkg installs on macOS endpoints.
- The [AdjustEffectiveProcessRightsContract](#) action has been deprecated for endpoints running macOS Big Sur. The [Run as Root](#) action has to be used in policies instead.
- Added SUDO Plugin for elevating from command line. Refer to [Sudo Plugin](#). Policies that previously just elevated a process no longer work and the elevation has to be run via sudo instead.
- Added [All macOS Big Sur Computers](#) Filter, with membership defined as any macOS Big Sur endpoint having an agent installed and registered.
- The default policy [Retry errored TMS Events - Catalina \(macOS\)](#) has been renamed to [Retry errored TMS Events - Catalina and later \(macOS\)](#).
- The default policy [Retry errored TMS Events - Catalina and later \(macOS\)](#) Computer Groups Targeted property has been changed to [All macOS Catalina and Later Computers with Application Control Agent Installed \(Target\)](#).

Agent Pertaining to Big Sur and Catalina

There are several features available with the KEXT version of the agent which are deprecated in the SYSEX version. There are others that are supported, but may require a change to policy configuration and/or user workflows.

Deprecated

- Allow Self-Elevate via Finder Extension – This feature provided the limited ability to right-click an application and have it run elevated. Depending on the application and how it was implemented, this may have had limited success for end-users.
- Run as Root applied to application bundles – This feature provided the limited ability to have an application bundle run elevated when it was launched via Finder. Depending on the application and how it was implemented, this may have had limited success for end-users.
- Run as Custom User, Run as Print Admin User – These Adjust Effective Process Rights actions are deprecated.

Supported, but may require workflow changes

- Run as Root applied to command-line binaries – If you have policies that elevate specific command-line binaries (e.g. systemsetup), you will need to inform your end-users that they should now precede these commands with sudo. This takes advantage of the new sudo plugin feature for elevating command-line binaries.* Endpoint Security system extension (SYSEX) replacing most functionality previously provided by the Kernel Extension (KEXT).

- The KEXT flavor of the macOS agent can experience high memory utilization during File Inventory.
- The 10.8.1 based Policy Events page does not always load correctly.
- Users removed from a Security Group in AD still show as members of the AD group inside Privilege Manager.
- Logging out does not invalidate the session/cookies that may have been previously stored/cached during a valid logon session.
- Changing the API Client User secret after token issuance, does not force an authorization error and logout.
- Approval reports don't provide drill-down details when accessed.
- X-Powered-By information returned in 301 and 400 http responses.
- Provide detailed DB error messages in log file only.
- Provide detailed error message via log file only.
- The Administrators group is showing up twice when viewing the Group Policies section.
- License counts are not correctly reflected per OS.
- Intermittent failure on approval requests.
- Saving Excel and Word files on SharePoint, MS Query, and Excel print issues due to Application Control Service.

- The combined installer released with Secret Server 10.9.000005/32 does not contain a NuGet folder as provided with previous combined installers. Customers can use the upgrade.zip provided via the [Software Downloads](#) topic for use with their manual and/or offline installs/upgrades. Refer to [Offline Upgrades](#) for details.
- User and group inventory may not reflect proper group membership the first time it runs on the endpoints. Subsequent runs will finish processing that information and will be accurate.
- With the Safari Browser, the behavior for default selection on drop-down menus might vary from other browsers.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the [Finder Extension](#) functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.
- If you have a policy allowing management of the /Applications folder via the Copy Install Application filter, deleting multiple applications from the /Applications folder will result in a dialog prompting for administrator credentials. The workaround is to have your end-users delete applications one at a time.
- If you have enabled the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to duplicate it and change the File Names to:


```
legacyLoader;legacyLoader-x86_64
```
- If you have already duplicated the Elevate Privilege Manager Agent Preference Pane (Sample) policy to elevate the Agent preference pane and you wish to target Big Sur, you will need to change the File Names to:


```
legacyLoader;legacyLoader-x86_64
```

10.8.1 Release Notes

October 8th, 2020:

Enhancements available with the 10.8.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Improved the way we treat cookies as they pertain to IIS header limits (see <https://docs.microsoft.com/en-us/troubleshoot/iis/http-bad-request-response-kerberos>) in user group memberships to avoid potential error conditions.
- Group Member Based Approvals for offline support via [Endpoint Group Member Approval Action](#).
 - Updates to the [ServiceNow Integration Setup](#) for supervisor roles based on group membership for ServiceNow integrations.
- Mobile and manual approvals now appear in the approval list in the Privilege Manager Console under **Tools | Manage Approvals**.
- Improved agent based Directory Services import for added computers.
- Improved applicable Application Control Configuration policy calculation to honor priority settings.

Cloud

- Privilege Manager now inventories domain users (full username, i.e. domain\username with SID) and groups in the Local Security Group Policy. Resource resolvers can use either to resolve to the unique resource for:
 - User Context Filter fields
 - GMA Action fields
 - Approval metadata reported during approval requests.
- The macOS agent can experience high memory utilization during File Inventory.
- 10.8.0 agent causes high CPU utilization.
- Unnecessary Change History records in DB that cause performance issues.
- Merge duplicate SID resources fails after on-prem AD sync.
- Changes to Syslog tasks can't be saved.
- XML entities in requests to ServiceNow would cause the request to fail.
- Database string reconfiguration does not work for integrated authentication.
- Promoting Windows domains to AD domains fails if the AD domain isn't available.
- The Application Justification Report by default shows all justification events for all computers instead of just events for the selected computer.
- Agent versions 10.4 and 10.5 cause error condition "Failed to resolve user SID" during approval workflow.
- RegEx syntax rules are broken when targeting secondary file filter information.
- When upgrading from 10.5 (and potentially other prior Privilege Manager versions), you may encounter an Item Not Found exception when first navigating to the console.
- Endpoints on Virtual Machines do not show local users associated with resources.
- In IE11 the dates in the agent log calendar view are rendered in the same color as the background and only readable when selected.
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.
- Custom Range in Console Log Viewer Only Displays Last Hour of Logs.
- The File Scan Results File Filter (Policy) shows the wrong description and references computers instead of a specific policy.
- Issue with using various VirusTotal and Cylance filters in different policies.
- In the Resource viewer the justification activity shows all justification events in the default "Application Justification Report".
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.
- Missing policy reports not working for all agents.
- After Upgrading to 10.8.0 AD Sync fails to run with "TypeError: Cannot read property 'Trigger' of null\n\n at active_directory".

Cloud

- Windows domain not promoted to AD domain after on-premises agent import.
- Sign out now working correctly.

macOS

- Scheduled commands are run later than their scheduled time due to the last run time timezone offset.
- Drag-n-drop app bundle from non-DMG can result in dialog asking for credentials.
- macOS Agent SecurityRatingFilterContract logic is inverted for the Failure and Timeout result.
- Predefined five XML entities in a policy name causes an exception when creating a ServiceNow approval request.
- Upgrading to Privilege Manager 10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **MacOS Computers**.

If you want to prevent this automatic merge, modify the XML of this item:

```
PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822
```

Add on line 2 <adc:Attributes>NoModify</adc:Attributes>.

- Offline upgrades on **multiple** servers will need to be done manually.
- With an approval policy targeting a PowerShell script (.ps1 file) via secondary file filter, the Approval Notice pop-up causes a critical error alert when accessing the .ps1 file via right-click Edit menu option.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the [Finder Extension](#) functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.

10.8.0 Release Notes

Enhancements available with the 10.8 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- New User Interface and User Experience. Refer to [Privilege Manager 10.8 User Interface](#).
 - New [Policy Wizard](#) driven Application Policy creation.
 - Resource Targets are now organized via [Computer Groups](#).
 - Activation of Policies and Policy Priority changes available from the [Application Policies](#) overview page.
 - [Dark theme](#) support.
 - Refer to the [Changelog](#) for details about restructured documentation topics in alignment with the new UI.
- Enhanced upgrade process for on-premises instances. Privilege Manager now checks if updates are available and downloads details prior to proceeding. Refer to [Updating Privilege Manager - Primary Node](#).
- The Application User Activity report provides audit details for user activities like logins and logouts. Refer to [Application User Activity](#).
- The **Specific Installer Detection Filter** and **Generic Installer Detection Filter** are now labeled as legacy filters. These filters are only to be used to detect legacy installers that require the Windows Application Compatibility flag to be set.
- Support for [multiple authentication providers](#), including multiple Active Directory domains, multiple Azure Active Directory domains, NTLM (on-premise), Secret Server, and Thycotic One authentication providers.
- [Standard Privilege Manager](#) users can be created to log into Privilege Manager in case a connected authentication provider is unavailable
- Additional metadata is included in Privilege Manager's approval workflow: SHA1 hash and commandline arguments
- Additional metadata is sent to ServiceNow for approval workflows: SHA1 hash, commandline arguments, company name, version
- User context filter supports local user and local group names match by text

macOS Specific Features

- Added macOS Agent Utility preference pane accessible via system preferences. Refer to [MacOS Agent Utility Preference Pane](#).
- Extended the **Agent Summary by OS** report to also contain macOS system serial number information.

Public API

Thycotic introduces [Privilege Manager's public API](#).

Cloud Specific Features

- Support import of On-Prem Active Directory Users and Groups into Privilege Manager Cloud instances via [Directory Services Agent \(AD\)](#). Also refer to [Bundled Install](#) and [Agent System Requirements](#).
- Integration with Thycotic's SaaS based behavior analysis product, [Privilege Behavior Analytics \(PBA\)](#), provides visibility into all processes interactively executed by end users.

- Users in nested groups are not shown as child items when importing specific Azure AD users and groups.
- Adding a New AD Domain Uses the Wrong User Object (Not the One Selected).
- Hyperlink from approval email notification redirected URL from browser is not working in cloud environment.
- The task Import Specific Azure AD Users and Groups creates errors.
- Parent and child actions are processing messages wrong.
- SQL Lite Agent Errors with, 'Database is locked' on client item update.
- When the Dacpac triggers a change in the schema of the itemstate table, locking errors can occur.
- Resource Data Class Data will not be imported, if Data Class was just added during install.
- AD Domain Controller Resource synchronization issues.
- Missing Trigger after importing a Remote Scheduled Client Command.
- Cloning an Active Directory Foreign system configuration and creating a new AD does not remove previous settings (SID, DC, etc).
- Executable not being caught when using just the file hash for the filter.
- Agent registration fails due to foreign key constraint error pointing to missing target.
- The Resource Explorer does not honor an OU name update for Active Directory Foreign Systems.
- An URL specified with "http" only does not apply strict transport security for communication.
- Users in Privilege Manager Cloud are unable to configure tasks to send email reports.
- Domain user groups cannot be added to the User Context Filter.
- Secondary file filter pre-filtering performance is lacking.
- Errors when clicking on bar graphs for Local Security statistics about Users.
- Customer accounts with an ampersand (&) in the company name or license cannot activate their license.
- An error is thrown when attempting to add a managed user to a resource target.
- The Report Summary of Application Action report only contains the first 3 to 5 records when exported to CSV.
- When exporting a report with many records, the **Select All** option for CSV exports does not export all records.
- Upgrade banners are not displayed for the latest version.
- When creating or cloning an action, the user is unable to reference built-in or well-known local groups.
- CSV Report export adds apostrophe before - and + symbols
- When an endpoint is using Azure Service Bus to communicate with a Privilege Manager On-Prem instance, policies with a message, approval, or justification action do not appear and the application does not launch.
- An exception is thrown when attempting to sync after creating an SCCM connection.
- The subject line certificate filter does not match the certificate on file.
- No details available for the Codesign Entitled Elevated Application Filter.
- Issue using Multiple Security Groups in Computer Group not reflecting the correct number of computers.
- Active Directory Computer merge is not working correctly.
- Squishrunner.exe not working correctly with Thycotic Application Control Agent installed.

macOS Specific

- System calculated due time for scheduled task as negative, causing an exception.
- macOS agents with a comma or equal sign in their name are not successfully registering.
- The approval/justification prompt appears twice for a policy elevating sudo commands.
- Slack's DMG application bundle is not correctly recognized as a finder copy candidate.

Agent Updates

- The agent is sending SHA1 and not SHA256 for Cylance integration.

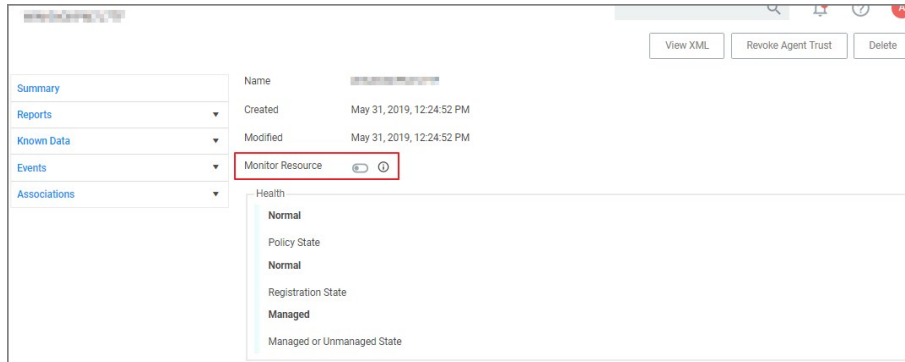
- Upgrading to Privilege Manager 10.8 causes a task to run to merge computer groups and remove unused system computer groups. This primarily affects the Application Control policies that are using resource targets/computer groups named **All Windows Computers with Application Control Agent Installed**. With 10.8, those policies will use the **Windows Computers** computer group and macOS will use **MacOS Computers**.

If you want to prevent this automatic merge, modify the XML of this item:

PrivilegeManager/#/item/xml/b2e02684-d154-48ca-9987-12b1759df822

Add on line 2 <adc:Attributes>NoModify</adc:Attributes>.

- When upgrading from 10.5 (and potentially other prior Privilege Manager versions), you may encounter an Item Not Found exception when first navigating to the console. The workaround for this is to recycle your app pools and then reload the console in your browser.
- When upgrading from 10.4 to the latest Privilege Manager version, the Admin menu might not load. The workaround for this is to recycle your app pools and then reload the console in your browser.
- When setting the **Monitor Resource** switch to active on a computer resource, an error is thrown.



- Offline upgrades on **multiple** servers will need to be done manually.
- The Directory Services Agent produced error messages about failed application control policy processing in the agent log.
- In IE11 the dates in the agent log calendar view are rendered in the same color as the background and only readable when selected.
- With an approval policy targeting a PowerShell script (.ps1 file) via secondary file filter, the Approval Notice pop-up causes a critical error alert when accessing the .ps1 file via right-click Edit menu option.

macOS Specific

- On endpoints using OneDrive, GoogleDrive, DropBox, or similar extensions, the endpoint will take about 2 min to correctly initialize the [Finder Extension](#) functionality after enabling the extension or after the upgrade to 10.8 with an enabled extension.

10.7.1 Release Notes

Release Date: Cloud 2020-03-05, On-premises 2020-03-12

Enhancements available with the 10.7.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- The Secret Server Vault integration does not require Secret Server to be set up as the authentication provider. Any supported authentication provider can be used, independent from using Secret Server as a Password Vault. Refer to [Setting up Integration between Privilege Manager and Secret Server](#).
- Computers in Domain Groups can be leveraged as resource targets to be used in policies. Computer groups can be set up to utilize Active Directory security groups and organizational units (OUs). These so called domain security groups and OUs can be imported via Active Directory or Azure AD. However, OUs do not exist in Azure AD. Refer to [Create New Computer Group](#).
- General in product user guidance improvement for Mobile Application configuration. Refer to [Privilege Manager Mobile Application](#).
- The policy **Agent Service Start / Stop Control (Windows)** is now obsolete. Users should disable that policy and/or delete it. We have added a new policy named **Restrict Account Permissions on Agent Services (Windows)**. Users should clone that policy, to edit and assign to the desired targets, and enable. Refer to [Agent Hardening](#)
- Improved verbose logging during token validation logic.
- Report export options allow to select all data sets vs. data sets currently displayed on the page. Refer to [Reports](#).
- On-premises only support for deployments with Amazon RDS database systems.

macOS Specific Features

- New Configuration Feed to ignore macOS Catalina Software Updates. For details refer to [Ignoring macOS Updates](#).
- Best Practices for macOS system preference panes have been added, refer to [Best Practices System Preferences](#).
- Improved and new macOS event discovery filters, refer to [List of Default Filters for Event Discovery](#). Beginning with macOS Catalina, Apple changed the location of the application bundles that ship with the operating system. Traditionally, these applications were located in /Applications. Now they are located in /System/Applications. That location however is masked by Finder. The new and improved filters work with both locations.
- It is no longer necessary to include the **.app** extension for the Bundle Name property of an App Bundle Filter (e.g. Console.app). The agent will account for its presence while performing policy evaluation and properly match the filter if it is applicable. Refer to [App Bundle Filter](#)

Cloud Specific Features

- Data centers in Canada and Singapore have been added.
- Secret Server can be used as a password vault independent from the authentication provider.
- ServiceNow connector is automatically installed for all new cloud instances.
- The integrated SMTP server is automatically configured for all customers during the cloud instance setup, alleviating the need for customers to connect their own SMTP server.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix. Bug Fixes are addressed for both versions On-premises and Cloud unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Long lists of resource items are not scrollable when trying to view or select items. For example when adding a user to Local Security Groups or when looking at the password history of a user, the form cannot scroll down the entire list of users.
- The 10.7 agent fails and prevents execution on certain Java based applications.
- Reports exported to CSV only include information of the data currently displayed in the UI and not all data records from that report.
- Grids in reports are not properly sorting date column data.
- The offline approval picker is not displaying parameters and computer list does not fit into page.
- When editing an Import Directory or Import Directory Computers task, the Directory ID and the Query parameters cannot be saved.
- Secondary file filters are ignoring items with spaces in their name and not triggering appropriate policy actions.
- Exporting a FileParameterCollectionFilterContract does not export the underlying file resources.
- When creating Filters for Windows systems and the user has the Privilege Manager macOS Administrators role, an exception is shown.
- Misleading counts when built-in local Admin users are backed-up by provisioned user.
- When creating a copy of an **Approval Request (with ServiceNow Request Item Number) Form** action, the contents cannot be edited.
- Security ratings reports pagination is not working correctly.
- macOS latency in updating a VNODE structure on disk is resulting in application execution being denied.
- Cannot add new policies with application targets and enable.
- Selected credentials on AD foreign system cannot be edited.
- Changing authentication providers throws an exception.
- A Privilege Manager client license count is exceeded message is displayed when it exceeds the 90% threshold and valid licenses are still available.
- Any domain groups added as a local administrator in the LSS Computer Groups disappear after being added.
- Creating a user context filter with a properly formatted SID that does not exist fails. A malformed SID results in an unfriendly error message.
- Users cannot add new machines to a managed computer group.
- For policies using a Group Member Authenticated Message Action, members in nested groups are not validated during the authentication process.
- Users in nested groups don't get the proper application role.
- Cross site anti-forgery token validation was using an email as a match, but the value was configured as a name.
- The Resource Target Computer List removes previously selected items when attempting to add additional computers.
- Privilege Manager installs prior to 10.5 cannot be upgraded to 10.7.0.
- Preferences cannot be fetched or saved by non-administrative users.
- Agent hardening removes permissions to modify/delete Agent Services.
- ServiceNow connector fails when upgrading Privilege Manager from 10.4 to 10.7.0.
- The **Domain Users as Local Administrators** and **Summary of Domain Users as Local Administrators** reports are timing out when run in large environments.
- Changes to the default file inventory from the Event Discovery page are not saved.
- UNC share policies imported from Config Feeds are not displayed under policies.
- Application control agents installed on Windows 10 machines are not reported on the **Application Control Agent Summary** report.

Agent Updates

Refer to [Software Downloads](#) for the latest available agent software downloads.

Core Thycotic Agent	10.7.2266	Rebuild with bundle to include Application Control Agent updates.
Application Control Agent	10.7.2257	Secondary file filter pre-filtering performance is causing slowness when there are large numbers of child processes launched (such as git.exe for each file).
	10.7.2256	System experiencing poor performance for the Group Member Authenticated Message Action.
	10.7.2239	Send SysLog ... template based tasks to send logs to server fails.
	10.7.2219	Initial 10.7.1 release version.

Privilege Manager macOS Agent	10.7.30	Users are locked out of their macOS device user account and unable to log in again, if the option to reopen the application on next login is enabled.
	10.7.27	The download filter policy is not triggering due to invalid URL partial match logic.
		Local groups on macOS without a SID prevents local user inventory from completing.
		MacOS agent experiences database contention when Office for Mac is installed or updated.
	10.7.21	Initial 10.7.1 release version.

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 and newer macOS endpoint agent.
- When installing Privilege Manager on a Windows Server 2012 pointed to a DB that is running on SQL Server 2017 or above, SSDT binaries will need to be leveraged, which are only available in .NET 4.6 or above. If your Server 2012 has .NET 4.5.1, make sure to update it to the recommended .NET 4.6.1 version.

10.7 On-prem Release Notes

Release Date: 2019-12-09

Enhancements available with the 10.7 On-premises release of Privilege Manager:

- [Security Manager migration support](#) has been added. The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.
- [Change History auditing](#) is available for resource items providing information on who initiated the change, at what date and time, and what type of change was made.
- The [Remove Programs Utility](#) in previous versions available via Configuration Feeds has been fully integrated with Privilege Manager Server and the Agents installation packages. The functionality has been expanded to also include Windows 10 App Store applications.
- [Export and import of policies](#) - including all dependent filter, action, and user context type items.
- A new [Reset Licensing task](#) was added.
- Support filtering on the subject name of a signed digital certificate allowing for much more generic certificate management.
- Dependency checks have been added to Privilege Manager for:
 - [Deleting Items](#)
 - [Task Parameter and Schedule Parameters](#)
- Agents Enhancements:
 - [Agent Hardening](#)
 - Agent will only receive new and updated policies that are relevant to that endpoint.
 - Enhance [Client Item Cache Log View](#) in Agent Utility.
- Support for [configurable session and inactivity timeouts](#) was added to the product.
- Allow right-click as a Thycotic Admin for .msu and .msc files.
- ServiceNow ticket request numbers are displayed within Privilege Manager's prompts.
- Restrict access rights of File-Open dialogs that are launched from elevated processes.
- Domain User support in User Context Filters.
- When choosing a resource target, if an OU (Organizational Unit) is synced, the UI will display the computer and site names in their proper hierarchical structure
- When choosing a domain user for a Role, the picker now shows the domain and group membership of that user.
- Ability to [bypass policy inspection during endpoint boot-up time](#) in order to not affect boot-up time.
- Performance improvements during agent registration.
- Admin controlled list of extensions that are excluded from agent hashing.
- Application's friendly name displayed in approval workflow prompts.
- The default log size can be set using configuration settings in the administrative policies tab.
- The default permissions on the Application Control Agent Configuration Policies have been updated as follows:
 - TMS Admins and Windows Admins have read/write to the Application Control Agent Configuration Policy (Windows)
 - TMS Admins and Mac Admins have read/write to the Application Control Agent Configuration Policy (MacOS)
 - TMS Admins, Windows Admins, and Mac Admins have Read/Create/Revoke access to Install codes
- MacOS specific features:
 - Target specific commands on macOS using wildcards (starts with, ends with, contains) and regular expressions.
 - [Secure Token](#) support.
 - MacOS discovery settings are more readily accessible on the discovery configuration page.
 - [PKG files can now directly be uploaded](#) within the Privilege Manager UI, alleviating the need to first perform file inventory of those applications on the endpoints. The application policy manager has added ability to inventory a PKG file to allow building of policies prior to the discovery of the package.
 - MacOS Catalina support.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- Changing the selected collection for an SCCM collection does not correctly update membership.
- Page goes blank when navigating to Admin I Configuration and "Enable Automatic Refresh of Privilege Manager Alerts in Browser" is disabled.
- Clear remote scheduled policy parameters when the command is changed.
- Message Action text editor in UI should support formatting included in XML.
- Double-clicking on column width adjustment in the Agent Log Viewer gives an Unhandled Exception.
- The Advanced Display Message Action is running in the background.
- New schedule updates do not display clearly in the schedule.
- The Application Justification Report returns no results.
- The Resource Monitor doesn't show counters after elevation.
- The COM Objects Elevation showing Windows UAC after canceling Thycotic prompt.
- The "folder" view in the item selector does not work.
- The Event Counts on the Privilege Manager home are incorrect.
- Events are duplicated in the Event Discovery view.
- Win32Exe filter correctly handles files that have the internal attributes stripped.
- Remote/cloud connected clients that pull tasks are broken with service hardening tasks.
- The Password Age chart is broken and does not return any results.
- The Agent falls back to using legacy services and no longer retries to connect to current services.
- Offline Approval access is not available for the Privilege Manager HelpDesk User role.
- MacOS Resource Targets are not updating when trying to add to a policy.
- On mouse-over the Statistics | Changes Period to Past Month report throws an exception.
- Changing an Azure User's Role membership in Azure is not reflected in Privilege Manager.
- An exception is thrown when navigating back to the Privilege Manager home after a session timeout.
- System does not handle logins to a machine without standard SIDs.
- The horizontal scrollbar is showing in the table for Windows Privilege Personas.
- The Policies table is congested when opened in smaller resolution.
- Reports displayed from the homepage may scroll pass the pagination controls.
- The Top Applications widget on the homepage throws an exception
- Several reports on the home page are not loading properly in Firefox.
- Updates to an exclusion filter name are not displayed after editing.
- The no licenses installed banner is missing.
- Redundant warnings appear about the anti-virus exclusion settings.
- An exception is thrown when navigating to the Foreign Systems tab on the Configuration page.
- AD synchronization does not work correctly for users with distinguished names in excess of 256 characters.
- The report generated from Purge Maintenance - Files Undiscovered has duplicate messages.
- The Agent configuration form does not show previous values when a user clicks cancel.
- Privilege Manager instances with Secret Server integration:
 - Secrets deleted from Secret Server create duplicate user credentials.
 - The expiration of a Secret Server session does not prevent access to Privilege Manager.

- Changing Secret Server Role Permissions for Privilege Manager requires recycling TMS application pool.

- If you are upgrading from an older Privilege Manager version (pre 10.5) contact Thycotic Support for assistance.
- Agent Hardening does not allow for an automated rollback. The workaround is to manually [Restore Default Agent Permissions](#).
- If an issue is encountered with local UI preferences, Thycotic recommends clearing the local storage cache to remove old preference values. This can be done by going to **Admin | Diagnostics** and clicking the **Clear Local Storage Cache** button.
- Creating copies of a Persona or currently selected task schedule does not work.
- The File Specification Filter definition does not work on macOS 10.15 (Catalina) when the File Names field starts with **com.apple.preference** and/or Path field starts with **/System/Library/PreferencePanes/**. Any Policies leveraging these filter definitions is also impacted.
- In Safari and Edge browsers column filtering for the Agent Policy State and Agent Policy State - Drilldown reports does not work.
- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 macOS endpoint agent.
- Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
 - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.
 - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 On-prem Release Notes

Release Date: 07/11/2019

Enhancements available with the 10.6 On-premises release of Privilege Manager include:

- The **Syslog Integration** options have been improved and support for HTTP/HTTPS was added. The HTTPS option specifically supports integrations with DEVO. (Also available in Cloud release.)
- A **Getting Started dialog** provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup.
- An **Offline Approval Process** has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- **Filters/Actions** have been added in support of various new Privilege Manager functionality:
 - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
 - Copy Install Application (macOS)
 - User Requested Run As Administrator Filter (macOS)
 - Executable Declared as Privileged Filter (macOS)
 - Codesign Elevated Application Filter (macOS)
- **Direct approval process selection for ServiceNow** is now available in the Privilege Manager UI, and no longer requires SilverLight.
- The Windows agent supports the **display of the ServiceNow approval request ID** after the approval has been submitted.
- **Integration to use Azure AD as an authentication provider has been improved.** It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. <https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server> Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. <https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync>
- **New macOS features** refer to the [Mac User Guide](#) for detailed information.
 - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
 - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A setting was put in place to **cap the maximum number of events** that can be sent back to the server at 1 Million events. Once that threshold is reached, the oldest event is purged from the list. This setting can be adjusted in the Advanced section of the Configuration page.
- A **browser-based server Log Viewer** is now available from the Admin menu.
- **Error notification and performance in high latency environments** have been greatly improved in this release.
- **Bulk delete actions** have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to "when ANY match" for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
 - When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
 - The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
 - Unable to edit configuration of "All Other Users and Groups" for groups in local security from "Ignore if found" to "Remove if found". When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the "RemoteScheduledClientCommandContract" for the group that is having the issue, removing the input parameters for the provisioned group, and then retrying the change.
 - Error upgrading to 10.5 U3 Directory Services for some specific conditions.
 - LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
 - The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
 - The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
 - The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
 - After reboot, the endpoint agent creates a certificate based on the UuidCache information causing an invalid agentID error.
 - A macOS account with a computed RelativeID (RID) that is null results in an exception that causes Local User Inventory to fail.
 - macOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
 - After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
 - During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
 - Built-in Privilege Manager User does not have read access to policies.
 - Privilege Manager relies on the Require Folders for Secrets Secret Server setting during integration set-up.
 - Login button is displayed after authentication with Secret Server.
 - Customer upgrading from version 8.x have issues deleting or saving items with GUID 71f3e19c-625c-4696-80e6-c9616554cb3c.
 - UAC Override policy does not go into effect until UAC Override scheduled task is run.
 - Event discovery resources stuck in Pending Assignment status.
 - On macOS endpoints with agent version 10.6.19 installed, depending on the user interaction with the approval dialog, it is possible that after clicking Continue or Cancel the dialog is redisplayed and cannot be dismissed.
-
- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.
 - If a customer implementation uses the Microsoft Azure Service Bus for their Internet connected clients, the clients will **NOT** be able to communicate with the Privilege Manager server after an upgrade to 10.6. Contact Thycotic Support if you are using Microsoft Azure Service Bus and are planning to upgrade. This does not impact implementations using a Reverse Proxy.
 - Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
 - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.
 - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 Cloud Release Notes

Release Date: 05/30/2019

In this new release, Thycotic expands its Enterprise-Grade Privileged Access Management (PAM) as a Service, offering Privilege Manager in the cloud and building upon its industry-leading cloud-ready solutions.

Enhancements available with the 10.6 Cloud release of Privilege Manager include:

- A Getting Started dialog provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup steps.
- An Offline Approval Process has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- Clear communication for regularly scheduled or emergency maintenance tasks:
 - In Privilege Manager Cloud environments regularly scheduled maintenance tasks will be announced via a maintenance banner at least 14 days prior to the maintenance window being in effect.
 - Thycotic will announce any regularly scheduled and emergency maintenance to inform customers when maintenance is performed on the cloud instance.
- Filters/Actions have been added in support of various new Privilege Manager functionality:
 - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
 - Copy Install Application (macOS)
 - User Requested Run As Administrator Filter (macOS)
 - Executable Declared as Privileged Filter (macOS)
 - Codesign Elevated Application Filter (macOS)
- Direct approval process selection for ServiceNow is now available in the Privilege Manager UI, and no longer requires Silverlight.
- The Windows agent supports the display of the ServiceNow approval request ID after the approval has been submitted.
- Thycotic One is the access portal to Privilege Manager Cloud and provides data center access/support via Thycotic One US East, EU, and Australia Azure geo locations.
- Integration to use Azure AD as an authentication provider has been improved. It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. <https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server>
Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. <https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync>
- macOS, refer to the Mac User Guide for detailed information on the new macOS features.
 - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
 - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A policy was put in place to cap the maximum number of events that can be sent back to the server at 25000 events. Once the 25000 event comes in, the oldest event is purged from the list. For troubleshooting purposes this can be temporarily adjusted by Thycotic support.
- A browser-based server Log Viewer is now available from the Admin menu.
- Error notification and performance in high latency environments have been greatly improved in this release.
- Bulk delete actions have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to "when ANY match" for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
 - When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
 - The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
 - Unable to edit configuration of "All Other Users and Groups" for groups in local security from "Ignore if found" to "Remove if found". When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the "RemoteScheduledClientCommandContract" for the group that is having the issue and removing the input parameters for the provisioned group and then retry the change.
 - Error upgrading to 10.5 US Directory Services for some specific conditions.
 - LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
 - The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
 - The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
 - The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
 - After reboot, the endpoint agent creates a certificate based on the UuidCache information causing an invalid agentID error.
 - A macOS account with a computed RelativeID (RID) that is null results in an exception that causes Local User Inventory to fail.
 - MacOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
 - After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
 - During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
 - Built-in Privilege Manager User does not have read access to policies.
-
- The Local Active Directory features exists, but requires a direct connection to the domain controller, which is often not permissible due to firewall configurations.
 - Secret Server integration for authentication and vaulting of local account credentials is not presently available.
 - All license key management is done via Thycotic and license keys are not visible on the licensing page. There are not presently options for customers to add additional licenses directly.
 - Access to the Security Manager console (Silverlight version) is not available.
 - Personas are not available.
 - Server-side Powershell scripts not signed by Thycotic are not allowed. Custom server-side work can be done via Professional Services engagements.
 - The setup is managed by Thycotic and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection option to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Thycotic during maintenance periods.

All other features and functionality of Privilege Manager On-premises and Cloud are the same.

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.

10.5 and Previous Releases

Release Date: 12/11/2018

Enhancements

Listed below are the enhancements being provided in this release:

- When creating a resource target for a policy, the "Groups" option is available to allow targeting of organization units (OUs). See article: <https://thycotic.force.com/support/s/article/User-Defined-Resource-Targets-and-Collections>
- A new report called "Server Node Status" will show the version installed on each server node in high availability environment. This report will inform customers of the installed version of Privilege Manager across multiple instances for high availability.

Bug Fixes

Listed below are the bugs that have been * Fixed in this release. (The product behavior is described as it was prior to the * Fix. In a few of the items below, the specific * Fix is also described.)

- Users with the Privilege Manager Helpdesk Users role are unable to approve items; get an error message.
- Authenticated XAML message does not work if agent cannot connect to domain. * Fix: When validating credentials, if the domain is not available Privilege Manager will now authenticate against the operating systems so that (if the domain isn't available) the agent will use the local database SAM cache.
- Purge Maintenance task times out on extremely large tables when performing a deletion of millions of records.
- Exporting the Application Summary Report to CSV fails.
- During upgrade, some servers don't have proper permissions to allow writing new certificates to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys. * Fix: A new error message was added for Privilege Manager servers that do not have proper permissions during the upgrade to write new certificates to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- After successfully adding the first license, message saying "No records to display" is still displayed.
- Licensing page does not display an error if importing an invalid or duplicate license.
- On some reports, some valid filterable values are not being displayed as a selectable option after selecting the "Filter Report" button.
- Labels and information displayed when viewing a task does not properly align when the screen size is small.
- Option to "Backup the System" under "Client System Settings" policies does not elevate without selecting to apply to child processing. * Fix: Elevation will now occur automatically without having to change the child processing setting.
- Some Role membership group names are in all lowercase, not Pascal case.
- On the Help page, the link for the user guide is pointing to the Preferences page instead of the actual user guide.
- User is unable to press the "Cancel" button on the Preferences page.
- When the browser is made smaller, the page to create scheduled tasks has overlapping text.
- When editing a copy of the "Approval Request Form Action", the selected value in the "Approval type" disappears when switching from view mode to edit mode.
- Changing the "Minimum Security Level" field in the console log settings is not limiting the records displayed in the logs.
- "Base URL" field for Privilege Manager server under Foreign systems reads as "Base URI". * Fix: Text of the "Base URI" label in a Foreign System has been changed to "Base URL".
- Selecting options besides the "Upper Case" option when configuring a user's password results in "Undefined" being displayed as a selected option.
- Incorrect error messages are displayed if a new User credential is saved without or with an incorrect password.
- After clicking "Import" on the Import Items page, the import button does not grey out to display feedback that the import is processing.
- Exception is thrown on "Client System Settings" page when the Assign Filter field is left blank.
- Assigning filters to any of the items in "Client System Settings" can cause the page to become unresponsive.
- On the Time of Day filter, changing the time under "Different Periods on Different Days" also incorrectly changes the times under "Same Period Every Day".
- Clicking the Sort column of an empty report causes page to error.
- When deleting a filter or an action that is used in a policy, Privilege Manager correctly prevents the deletion but displays an incorrect error message.
- When building resource target queries, starting with "All Computers" causes poor performance. * Fix: This been removed from the default way resource target queries are built.
- "OU Directory Scope Collection Update" task fails if Collection.LastUpdated is null.
- Applications hang if a new certificate is created and the agent requests new client items before it updates applicable policies or registers with the server.
- Installing a new agent on a Mac endpoint results in a corrupted schedules.plist file.
- Azure AD tokens are expiring within minutes. * Fix: Azure AD will now last as long as normally issued tokens.
- If the "UNC Elevation Policy Template" Config Feed is imported, the "UNC Content Query" is erroring.
- When Secret Server and Privilege Manager are installed together using the combined installer, and a separate domain account without write permissions is used, subsequent upgrades fail if the domain account running the application pool does not have Write permissions on the TMS web folder.
- "Advanced Deny Notification Actions" are not included in dashboard counts and the list of denied files.

Release Date: 9/25/2018

Bug Fixes

- Fixed issue where the Mac agent configuration did not have a default task check in interval saved.
- Fixed issue where queries for reports that are scoped to display only certain resources will fail if the Default Security Descriptor ID is null or empty.
- Fixed issue where large Active Directories caused the Collection and Resource Targeting Update task to run for too long.
- Fixed issue where Privilege Manager's authentication provider screen would crash if incorrectly configured. When Privilege Manager cannot reach an Active Directory domain, a useful error message is now displayed.
- Fixed issue where Privilege Manager task schedules are not properly saved and displayed.
- Fixed issue where the dashboard would display an unexpected error in a modal popup the state of a gauge undefined.
- Fixed issue where the sign-in page URL query string could be used to redirect a user to another URL by only allowing relative URLs.
- Fixed issue where Telerik grids were not able to be resized when zoomed in or out in Chrome, Firefox, and Edge.
- Fixed issue where the GetToken API returned an invalid token for unauthorized requests instead of a 401 response code.
- Fixed issue that allowed Privilege Manager to be embedded inside of an iframe.
- Fixed issue where a New Loaded Resource file is not assigned to an endpoint's agent after the Resource Discovery task is executed once.
- Fixed issue where the Resource Discovery task does not finish and will continue to display a spinner when discovering a New Loaded Resource file that is not assigned to an endpoint's agent.
- Fixed issue where a New Loaded Resource was not discoverable if the location has been discovered but the file has been removed from the endpoint.
- Fixed issue that displayed the HTTP status code instead of the actual server error when bad XML was imported to Privilege Manager.
- Fixed issue where the data grid within a policy that displays all the filters loads slowly.

Mac Agent Updates (version 10.5.12)

- Fixes issue where the Mac agent was not properly logging failed agent registration attempts when an invalid install code was used.
- Fixed issue where Mac agent was writing exceptions to the logs if v4 agent registration fails when connecting to a Privilege Manager version prior to 10.5.
- Fixed issues where initial basic inventory was not being removed after first running.

Release Date: 9/04/2018

Bug Fixes

- Fixed issue where Privilege Manager, when configured with Secret Server for authentication, did not properly fall back to NTLM authentication if Secret Server was not properly configured.
- Fixed issue where Privilege Manager upgrade failed if duplicate IDs existed in [Ams].FileUploads or [Ams.Data].Win32_OperatingSystem tables.
- Fixed issue where Privilege Manager did not prevent deletion of an item referenced by another object. For example, it did not block a filter from being deleted if that filter was also being used by an active policy.
- Fixed an issue where the delete operation of computers did not properly display completion for long-running deletes.

Release Date: 8/15/2018

Overview

Notable enhancements to 10.5 include a new dashboard as the home page, integration with Cylance reputation analysis, support for Azure Active Directory, performance enhancements, and improved agent security.

Important for Secret Server Combined Upgrades

If Secret Server is installed in conjunction with Privilege Manager, Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.

10.5 Agent Upgrades

Unless the "Prevent Legacy Agent Registration (10.4 and older)" option is checked (Admin > Configuration > Advanced), older agent versions will still function in Privilege Manager 10.5.000000, but Thycotic recommends that you do upgrade Privilege Manager agents to the 10.5 version due to security enhancements.

Note: That when installing new 10.5.000000 agents you will be prompted to install with a valid Install Code.

Enhancements

- New dashboard for deep reporting and visibility into the state of Privilege Manager.
- Integration with Cylance for real-time threat intelligence policy checks.
- Support for Azure Active Directory for authentication, resource targeting, and user context filters.
- Excel reports that are exported are sanitized to prevent macro injection attacks against end-users who open the Excel files.
- Cross site request forgery prevention implemented.
- Sensitive data encrypted on endpoint with machine, non-global key.
- Agent installation requires agent install code as a parameter or as a field entered when using the bundled installer for additional security.
- Redesign of agent/server trust requiring shared secret before agent can register with server and receive policies.
- Redesign of client item encryption to improve security.
- "Add new filter" and "Add to policy" buttons are on resource page for MSIs and scripts.
- Support for inventory filters added as secondary file filters to allow targeting of MSIs and scripts by hash.
- Support wildcards in fields of the Win32 executable filter. See inline help for details.
- Added SQL indexes for improved performance.
- Collection update and resource targeting update tasks are combined into task called "Run Policy Targeting Update."
- Allow unattended uninstall of Mac agent by adding command-line option to suppress the user confirmation prompt.
- Reduced the time it takes a newly installed agent to download policies.
- Advanced message options for justification window supports end user authentication.
- Default to validating client item signatures on Windows agents.
- Support and maintenance license are viewable on the licenses page.
- Option to "Apply action to child processes" is unchecked by default.
- Deployment tab of a policy will display a button to update the collection of resource targets on demand.
- EULA not shown upon product upgrade.

Bug Fixes

- Fixed issue where Administrator group incorrectly displayed SYSTEM account as a member.
- Fixed issue where Server URL on agent was not updated if server was changed.
- Fixed issue where setting password rotation for a one-time update failed to rotate the password.
- Resolved error when custom approval process was initiated.
- Processed events are purged up from the [AMS.DATA].FileUploads, [AMS.DATA].FileUploadChunks, and [AMS.DATA].FileUploadSessions tables.
- Fixed issue where changed numeric values on the Advanced tab of the configuration page were not saved.
- Resolved schedule creation error in certain time zones.
- Resolved an issue where provisioning a local user would enable a disabled account and/or disable an enabled account.
- All internal links to support documentation now utilize https.

Known Issues

- If Secret Server is installed in conjunction with Privilege Manager, Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.
- Agent trust is broken if VM UUID changes. Agent must be reinstalled to resolve.
- On the user screen in local security, the text "undefined" will appear if any option for password "Characters" is selected except 'Upper Case.'

Release Date: 3/28/2018

Bug Fixes

- Resolved issue to ensure the trimming of the table storing data from uploaded files

Release Date: 3/6/2018

Enhancements

- Support for SQL 2017
- Support for agent communication on Windows 7 systems with TLS 1.1 and SSL 3.0 disable
- Checks for a valid maintenance license to allow product upgrades
- Client item cache is cleared automatically
- Clicking the "Run" button for tasks indicates successful execution and prevents kicking off of multiple tasks
- Built-in administrator is prevented from being removed from group and the associated operation will display "Required Account"
- Support "log4net log (.log)" format in the Thycotic Monitor

Bug Fixes

- Reports on "Managed Local Users" and "Managed Local Group" will now allow users to select the account name as a drill through to a report on the computers the account exists on
- Breadcrumbs will display the correct name after renaming a computer group
- Upgrades will retain security ratings setting for VirusTotal
- Custom time of day filter correctly saves
- Simple policy view allows for new filter to be saved inline
- The popup allowing users to add a new account to a group allows sorting
- License correctly determines client and server types during basic inventory
- Ability to clone credentials has been removed when Privilege Manager stored credentials in Secret Server
- Resolved searching for filters from within the secondary file filter
- Upon saving group membership, the operation column correctly displays the action that will be taken on the associated account
- Resolved validation of password field for a managed user when using Edge browser
- Charts on the statistics page scale correctly for both small and large number of endpoints
- Resolved issue that prevented enabling of firewall policy
- Password scheduler saved when UTC is selected
- Allow domain groups to be members of roles
- Resolved issue preventing application inventory on network shares
- Prevent non administrative access to the Thycotic folder on local drive

Release Date: 1/17/2018

Enhancements

- Least Privilege Enforcement for Local Users and Groups
- Provision local users and groups across all endpoints
- Permanently remove accounts from privileged local groups
- Prevent group membership from being changed directly on the endpoint, even by an administrator
- Local Account and Credential Management
- Uniformly apply user properties to local accounts
- Set secure and unique passwords for local accounts by defining character requirements and password length
- Rotate local account passwords automatically on a scheduled basis
- New and Enhanced User Interface
- Least Privilege features are built on top of a new easy to use and manage interface within the Local Security section of the application.
- Policies are easily deployed to groups of users or endpoints, making it easy to deploy least privilege in a phased approach
- Dashboard, reporting, and statistics are built into the interface to understand the current state of local users and groups on the endpoint and any changes. Easily spot vulnerabilities and trends.
- Actionable tips will appear inline when the environment is not following best practices
- Usability enhancements to application control functionality
- All grids have filtering options to narrow down large datasets
- Integration with Secret Server
- When using both Privilege Manager and Secret Server, passwords can be stored in Secret Server's vault
- Intended for use on endpoint workstations where remote management of local or non-domain accounts is not possible
- Secret Server enterprise PAM features can be used upon secrets that are managed by Privileged Manager
- Role Based Access
- Define users of the Privilege Manager application: set administrators, read only users, Mac OS users, Windows OS users, and helpdesk users
- Security trimmed access specifically designed for help desk users, who's responsibility it is to disclose passwords and approve/deny applications
- Reporting and Dashboards
- New reports provide visibility into local user and group membership, an audit of passwords that have been disclosed, a summary of local administrators, and all computers with passwords being managed by Privileged Manager
- Contextual reporting for each group of users and computers where least privilege policies are being applied to understand the affect of policies on users
- Simple charts provide an understanding of all endpoints with each individual user or group
- Dashboard will display trends of user's group membership changes, users being added and removed from groups, and passwords being disclosed. Trends provide insight into understanding outliers and potential rogue activity.
- Endpoint Visibility Utility
- Simple console deployed directly on the endpoint to check the communication status, register with the server, get the latest policies, view and export the logs.
- Ideal for enhanced visibility and understanding, especially when working directly with internal Thycotic support or professional services.

Bug Fixes

- Language and text * Fixes on installer screens for non-English systems
- Issue where Privilege Manager's MacOS copy helper would perform the copy without waiting the approval to complete. After * Fixing, we can now target .pkg files with policies.
- Secondary file filter will detect scripts being executed on Windows 10, after changes were made on how PowerShell scripts are launched on the OS
- Allow install (and pre-req install) to succeed if PowerShell Execution Policy is set to RemoteSigned in Group Policy
- Editing the Application Control Configuration policy will not set some values as blank
- Allow for configuration of "days" parameter for Purge Old Computers Task
- On MacOS, track which certificate Privilege Manager received the most recent time it was registered.
- Ability to assign ServiceNow Process in Execute App Type through Privilege Manager UI

Known Issues

- On Windows 10 Enterprise edition with patch version 1709 (released October 26, 2017), UAC is not suppressed, and thus end users are prompted to enter admin credentials
- Unable to Clone Credential when Secret Server is used as vault
- Agent is not communicating to server on Windows 7 over TLS 1.1
- Creating a File Hash specific filter fails if there are spaces at the end of the hash

Release Date: 8/29/2017

Enhancements

- Implemented automatic and continuous server-side logging
- Incorporated sandbox actions, allowing policies to limit the environments in which applications can execute
- On demand retrieval of a newly discovered file after event discovery. When "New Loaded Resource" is displayed, the user can click a new button called "Discover Now" to retrieve resources data.
- New check box added to the Event Discovery configuration to find all applications that require administrator rights to run ServiceNow configuration improvements
- Option to run the installation just for Secret Server, without installing Privilege Manager
- Upgrade of Privilege Manager will not require local admin rights when installed in conjunction with Secret Server
- Display warning if policy does not target any application
- Policy creation screen will remember simple or advanced view preference
- Paginate Resources list view
- Improved error handling on installation and the addition of an error icon indicating an issue

- Fixed issues in the VirusTotal reputation calculation and service call handling
- Upgrading a product within the setup app will also update dependent products
- Log files are now being stored to disk
- Installation Summary report now includes the last time agents registered
- Enhancements within installer for web applications to run as a user account
- Enhancements to better show report rows and chart sections that can be clicked into for drill-down into another report

Bug Fixes

- HTTP binding is not required on Privilege Manager website
- VirusTotal configuration is retained after upgrade or repair
- Issue installing the file inventory with machines using non-US date/time
- Trailing slash () will not affect the path field in Win32 and File Specification filters
- Future changes to agent configuration policies will be preserved and not overwritten
- All system policies are prevented from being edited so the user can create a copy

Release Date: 7/12/2017

Enhancements

- Added an agent to allow deny and allow lists, approvals, and elevation on Macs.
- Added "easy Policies" to allow for simple ways of creating allow and deny lists.
- The dashboard is now a series of tiles designed to give a simpler experience.

Release Date: 4/12/2017

Enhancements

- Updated Installer
- New installer to handle more prerequisites for HTTPS Bindings, WCF, and SQL
- Updated setup home for managing product upgrades going forward
- Session Monitoring Agents
- A new agent and policy is available to record RDP and console sessions. Note that this requires a Secret Server installation and licenses.
- For more information on RDP monitoring policies see this KB article

Release Date: 1/18/2017

Enhancements

- Added page specific help into Privilege Manager console
- Added options in the Discovery for kicking off inventory tasks to expedite policy testing
- Brought EMET policy options into the Privilege Manager console
- Brought the Application Firewall policy options into the Privilege Manager console
- Added configuration feeds for uploading policies and other items from support.

Bug Fixes

- Fixed issue where adding a new Persona and going back to the persona home required a browser refresh to see the new Persona
- Fixed issues in IE where the Report title text on the report home was not a link.
- Fixed issues with configuring Active Directory domains.

Documentation Changelog

This topic provides a chronological list of documentation changes. Minor content alterations are not tracked.

- New 10.8.2 KEXT flavored macOS Agent download to address high memory utilization during File Inventory.
- Hotfix release notes entry related to Directory Services.
- Several documentation improvements addressing broken cross-references.
- Added [10.8.2 Release Notes](#).
- NuGet source zip for manual installs/upgrades provided via [Software Downloads](#) topic.
- Added [Platforms](#) section.
 - Moved [macOS Secure Token](#) to the [Platforms](#) section.
 - Moved [Best Practices](#) to the [Platforms](#) section.
 - Moved and edited [macOS Legacy Extensions](#) to reflect behavior and best practices for kernel and system extensions on Catalina and Big Sur.
 - Moved [File/Folder Access](#) to [Platforms](#) section.
 - Added topic on [Sudo Plugin](#).
- Added [Just-in-Time Group Membership Action](#) topic.
- Edits to [Server Logs](#) topic.
- Edits to [CorrelationID support to Server Logs](#).
- New subtopic [Complex Password Policy enforcement for Privilege Manager users](#).
- Added [MDM Profiles for macOS Agents](#) topic.
- Added [Visual Studio Installer Elevation](#) example policy and filters to configuration feeds.
- Removed topic [MS Visual Studio Installations](#).
- New topic [Active Directory Import - On-prem vs Cloud](#)
- New topic [Securing the IIS Server](#)
- Moved [VM Deployments](#) to the Agents/All Agents section.

Added [10.8.1 Release Notes](#).

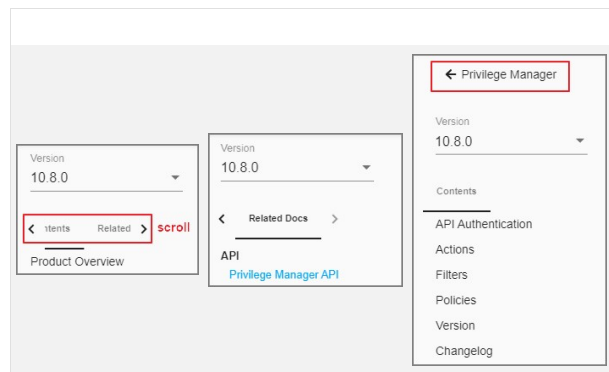
Group Member Based Approvals

- Added [Group Member Approval Action](#) topic.
- Added [Endpoint Group Member Approval Action](#) topic.
- Updates to the [ServiceNow Integration Setup](#) topic to include *over-the-shoulder* approvals at the endpoint.

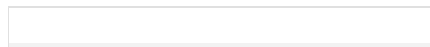
- New 10.8 UI introduction with changed user workflow and major documentation reorganization to accommodate the new UI layout.

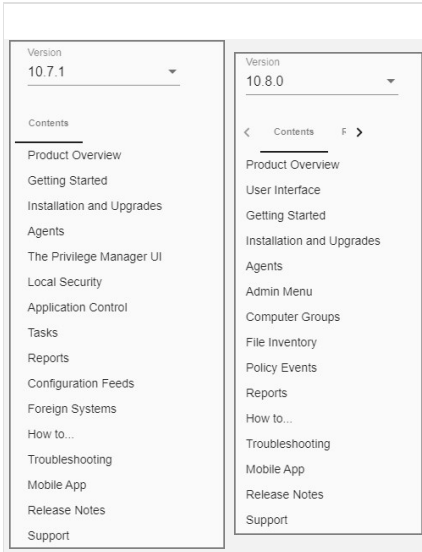
New Related Docs

The Privilege Manager Public API documentation can be accessed via Related Docs.



Restructure of Contents





The contents is aligned with the new Privilege Manager navigation flow for users. The following references where the contents moved to for all major topics.

Application Control	Now under Computer Groups
Application Control > Policies	Now under Computer Groups
Application Control > Filters	Now under Admin Menu
Application Control > Actions	Now under Admin Menu
Local Security	Now under Computer Groups
The Privilege Manager UI	Now under User Interface and only pertains to navigation and controls of the new UI.
The Privilege Manager UI > Configuration	Now under Admin Menu
The Privilege Manager UI > Diagnostics	Now under Admin Menu
The Privilege Manager UI > MacOS Specifics	Now under Computer Groups
The Privilege Manager UI > Resource Explorer	Now under Admin Menu
The Privilege Manager UI > Configuration	Now under Admin Menu
Tasks	Now under Admin Menu
Configuration Feeds	Now under Admin Menu
Foreign Systems	Now under Admin Menu

Refer to the [Admin Menu](#) topic for everything that was accessed via **ADMIN | More...** in the old UI.

Information about installing and upgrading Agents is available under [Installation and Upgrades > Agents](#). Information pertaining to the use, features, configuration, and troubleshooting of Agents is available under [Privilege Manager Agents](#). Agent topics are for the most part OS specific, with the exception of information under [Pertaining to All Agents](#).

If you have trouble finding a topic that you frequently consult, use the documentation platform's search option to find and bookmark accordingly. For example:

Thycotic Documentation / Privilege Manager

Version: 10.8.0

doc changes Print Article

Last Update: 7/16/20

Release Notes / Changelog

Documentation Changelog

This topic provides a chronological list of documentation changes. Minor content alterations are not tracked.

August 2020

- New 10.8 UI introduction with changed workflow and documentation reorganization to accommodate the new UI layout.

July 2020

- Added mid_server role to [ServiceNow integration](#) topic.

June 2020

IN THIS ARTICLE

- Documentation Changelog
- August 2020
- July 2020
- June 2020

Product Overview
User Interface
Getting Started
Installation and Upgrades
Agents
Admin Menu
Computer Groups
File Inventory
Policy Events
Reports

Thycotic Documentation

SEARCH

secure token

Items per page: 10 1 - 10 of 106

macOS Secure Token main page topic

Product: privman Version: 10.8.0 Score: 1.5441854 Last Update: 8/13/20

macOS **Secure Token** **Secure Token** is a macOS High Sierra or later account attribute, that is required to be added to a user account before that account can be enabled for FileVault encrypted Apple File System (APFS) volume. Once an account has a **Secure Token** associated with it, it can create other accounts which will in turn automatically be granted their **Secure Token**. In order for Privilege Manager to support **Secure Token** during account creation and for password management, a local account with **Secure Token** enabled must create [computer-groups/macOS/secure-token.md](#) relative URL in relation to version

Adjust Process Rights

Product: privman Version: 10.8.0 Score: 0.84816253 Last Update: 8/3/20

Microsoft with the release of Windows Vista introduced changes to **security** which included creating two **tokens** for users when they log in. But if necessary, the higher-privilege **token** be used by ACS when manipulating the process's **security** configuration. Adjust Process Rights Action Settings Explained The application action elevates or restricts the permissions at privileges held by a process **security token**. By default, each process inherits the user's **security token**. A restricted ID is an access **token** that modifies a user's access to **secureable** of [admin/actions/unrestricted-token.md](#)

System Settings

Product: privman Version: 10.8.0 Score: 0.05989004 Last Update: 8/13/20

Load On Demand Flags The value is a flag set specifying what item values are allowed to be on-demand loaded. 0 none, 1 strings, 2 tags, 4 **security**, 8 associations, 16 data class state all. Session Timeout This setting specifies the maximum time in minutes for a login session to be active without having to negotiate another **token**. The session **token** remains active does not need to be renegotiated when the inactivity timeout happens within the specified session timeout window. [admin/config/advanced/adv-pm-general.md](#)

Product: All
Access Controller
Account Lifecycle Manager
Bulletins
Connection Manager
DevOps Secrets Vault
Identity Bridge
Privileged Behavior Analytics search base
Privilege Manager
RabbitMq Helper
SCIM Connector
Secret Server

- Added mid_server role to [ServiceNow integration](#) topic.

- Added [Legacy System Extensions](#) topic.
- Updated [10.7.1 Release Notes](#) to reflect Agent software version updates and associated bug fixes.