



# Delinea

Secret Server

Documentation © 10.8.0



# Table of Contents

Secret Server Documentation	34
Introduction	34
Documentation	34
Primary Documentation	34
Getting Started	34
Best Practices	34
Security Whitepapers	34
Help	35
Download Secret Server	35
Integration Guides	35
<i>Current</i>	35
<i>Legacy</i>	35
Release Notes	35
Secret Society (Forum)	35
Developer Resources	35
Video Tutorials	35
Getting Started Tutorial	36
Step 1: Trial Installation Prerequisites	37
<i>System Requirements</i>	37
<i>Hardware Requirements</i>	37
<i>Software Requirements</i>	37
Checklist	37
SQL Server	37
Application Server	37
<i>Application Configuration</i>	37
Service Account	37
Active Directory Group Sync	38
Discovery	38
Test Accounts	38
Email Notifications	38
SSL Certificate	38
Firewalls and Ports	38
Step 2: Installation	39
<i>Process</i>	39
<i>Licenses</i>	39
Step 3: Secret Server Dashboard	40

Step 4: Security Best Practices	41
<i>Local Admin Account Best Practices</i>	41
<i>SSL (HTTPS) Best Practice</i>	41
Step 5: Backups	42
Step 6: Active Directory Integration	43
<i>Setting up Active Directory</i>	43
<i>Enabling Active Directory Users</i>	43
<i>Managing Active Directory Users via a Distributed Engine</i>	43
Step 7: Secret Server Framework	44
Step 8: Discovery	45
Step 9: Remote Password Changing	46
<i>Enabling Remote Password Changing</i>	46
<i>Performing a Manual RPC</i>	46
<i>Common RPC Error Codes</i>	46
Step 10: Heartbeats	47
<i>Enabling Heartbeat</i>	47
<i>Running Heartbeat</i>	47
Step 11: Audits and Reports	48
Step 12: Secret Access and Workflow	49
Step 13: Secret Launchers	50
Step 14: Recording Sessions	51
Step 15: Secret Server APIs and CLI	52
Step 16: Additional Resources for Secret Server	54
Help	55
Document Conventions	56
<i>Capitalization</i>	56
<i>Code and Command Line Text</i>	56
<i>Keyboard Shortcuts</i>	56
<i>Notes</i>	56
<i>Other Special Text</i>	56
<i>Screen Components and Attentional Targets</i>	57
Secret Server Glossary	58
Self-Help Resources	62
<i>Forums</i>	62
<i>Thycotic Blog</i>	62
Technical Support	63
<i>Technical Support Coverage</i>	63
Accessing Upgrades	63
Requesting New Features	63
Access Requests	64

Approving a Request	65
Duo Push Notifications	66
<i>Prerequisites</i>	66
<i>Assigning the Duo Approval Permission</i>	66
Requesting Access After Approval Is Granted	67
Setting up Access Requests for Secrets	68
<b>Secret Server Administration</b>	69
Administration Auditing	70
<i>Audit Data Retention</i>	71
In This Section	71
Overview	71
Data Retention Policies	71
Permissions	71
Procedures	71
<i>Viewing the Status and History of Audit-Data Retention Policies</i>	71
<i>Editing Audit Data Policies</i>	73
<i>Running an Old Audit-Data Purge Right Now</i>	74
<i>Giving Application Pools Event Log Access</i>	76
Overview	76
Required Registry Permissions	76
Applying Windows Event Log Permissions	76
<i>Report Auditing</i>	78
<i>Secret Audit Log</i>	79
<i>Viewing a User Audit Report</i>	80
Administration Page	81
Administration Configuration Tabs	86
<i>Email Tab</i>	86
<i>Folders Tab</i>	86
<i>General Tab</i>	86
<i>HSM Tab</i>	88
<i>Local User Passwords Tab</i>	88
<i>Login Tab</i>	88
<i>Security Tab</i>	89
<i>SAML Tab</i>	89
<i>Session Recording Tab</i>	89
<i>Ticket System Tab</i>	90
Application Dashboard	91
<i>Dashboard Components</i>	92
Home Tab	92
<i>Dashboard Widgets</i>	92

<i>Widget Types</i>	92
<i>Managing Widgets</i>	93
Overview Tab	93
Customized Tabs	93
<i>Dashboard Tools and Help Menu</i>	94
Tool Section	94
Help Section	94
<i>Themes</i>	95
Overview	95
Choosing Themes	95
<i>Running Dashboard Bulk Operations</i>	96
Encryption and Security	97
<i>Advanced Encryption Standard</i>	98
<i>Restricting IP Addresses</i>	99
Creating IP Address Ranges	99
Editing and Deleting IP Address Ranges	100
Assigning an IP Address Range	101
<i>Security Compliance Standards</i>	103
FIPS Compliance	103
PCI Datacenter Compliance	103
<i>SSL Certificates</i>	104
Maintenance Mode FAQ	105
<i>What is Maintenance Mode?</i>	105
<i>Why do we need Maintenance Mode?</i>	105
<i>Can I still access my Secrets when Maintenance Mode is turned on?</i>	105
<i>How long does Maintenance Mode last?</i>	105
Secret Server Authentication, Encryption, and Security	106
Configuring SAML Single Sign-on	107
<i>SAML Overview</i>	107
<i>Prerequisites</i>	107
Licensing and Version	107
.NET Framework 4.6.2+	108
Administer Configuration SAML Role Permission	108
<i>Setting up Secret Server</i>	110
<i>Setting up IDPs</i>	112
<i>Lockout Workaround</i>	112
Enabling FIPS Compliance	114
<i>Overview</i>	114
<i>Procedure</i>	114
Task 1: Enable FIPS in Secret Server	114

Task 2: Enable FIPS in Windows	114
Task 3: Reset the IIS Server	114
<i>Related Information</i>	115
Installing a Self-Signed SSL Certificate	116
<i>Overview</i>	116
<i>Obtaining an SSL Certificate</i>	116
<i>Installing a Self-Signed Certificate</i>	116
Task One: Generate an IIS Self-Signed Certificate	116
Task Two: Bind the Self-Signed Certificate to the IIS Site	116
Task Three: Test the Self-Signed Certificate	117
Thycotic One and Secret Server	118
<i>Overview</i>	118
<i>Cloud versus On-Premise</i>	118
<i>Procedures</i>	118
Logging in with Thycotic One	118
Configuring Thycotic One	119
<i>Secret Server Cloud</i>	119
<i>Secret Server On-Premise</i>	120
Generating a Thycotic One Credential	121
X.509 Certificate Security Chain Options	124
<i>Setting the Certificate Verification Policy</i>	124
<i>Certificate Validation Options</i>	125
X509RevocationMode	125
X509RevocationFlag	126
X509VerificationFlags	126
<i>Troubleshooting</i>	127
Accessing MS SQL Server with IWA	128
<i>Introduction</i>	128
<i>Creating a Domain Service Account</i>	128
<i>Granting Access to SQL Server database</i>	128
<i>Assigning Account as Identity of Application Pool</i>	128
Configuring CredSSP for WinRM with PowerShell	129
<i>Introduction</i>	129
<i>Enabling CredSSP for WinRM in Secret Server</i>	129
<i>Configuring CredSSP for WinRM on the Secret Server Machine</i>	130
<i>Configuring CredSSP for WinRM on a Distributed Engine</i>	130
<i>Enabling CredSSP on Secret Server Agents for PowerShell Script Dependencies</i>	133
Integrated Windows Authentication	135
<i>Enabling Integrated Windows Authentication</i>	135
<i>Configuring IIS</i>	135

<i>Logging on As a Local Account</i>	135
<i>Configuring Integrated Windows Authentication</i>	136
Introduction	136
Setting Up Windows Authentication	136
Task 1: Configuring Secret Server	136
Task 2: Configuring IIS	139
Task 3: Configuring Secret Server Launchers	141
Task 5: Configuring Client Certificates	148
Troubleshooting	150
Error "403 Forbidden" Message Is Displayed When Logging in	150
AD User Prompted for Credentials Even Though IWA Is Active	150
Logging in as a Local Account Is Not Available	150
Installing Windows Authentication in Windows Server 2012 Manager	151
SAML	152
Secret-based Credentials for PowerShell Scripts	153
Overview	153
RunAs Secret Precedence	153
Remote Password Changing	153
Secret Dependencies	153
Checkout Hooks	153
Procedures	153
Setting the Default PowerShell Credential for a Site	153
Using the Site PowerShell Credentials for Discovery	154
Two-Factor Authentication	155
Duo Security Authentication	156
Task 1: Create a Duo Application Representing Your Secret Server (Admin)	156
Task 2: Configure Secret Server to Use Duo (Admin)	156
Task 3: Setting up Duo (User)	157
Email Two-Factor Authentication	158
FIDO2 (YubiKey) Two-Factor Authentication Configuration	159
FIDO2	159
YubiKey	159
Configuration	159
RADIUS User Authentication	160
Configuring RADIUS	160
Enabling RADIUS for a User	160
Enabling RADIUS Two-Factor Authentication	161
TOTP	162
Configuring TOTP for Users	163
Disabling TOTP for Users	164

Enabling TOTP for Secret Server Users	165
Enabling TOTP for Launchers	166
<i>Secret Template Setup</i>	166
<i>TOTP Secret Setup</i>	166
Resetting TOTP for Secret Server Users	169
Viewing a TOTP for a Web Secret	170
<b>Backup and Disaster Recovery</b>	172
Backing up Secret Server to a Network Share	173
Backup Folder Permissions	175
Backup Settings	176
<i>Overview</i>	176
<i>File Path Settings</i>	176
Common Backup Errors	177
File Attachment Backups	178
Manually Backing up Secret Server	179
RabbitMQ Durable Exchanges	180
<i>Overview</i>	180
<i>Manually Creating Durable RabbitMQ Exchanges</i>	181
<i>Creating Durable RabbitMQ Exchanges with a PowerShell Script</i>	181
Using the Script	181
Script	182
Restoring Secret Server from a Backup	191
<i>Restoring the Application</i>	191
<i>Restoring the SQL Server Database</i>	191
Scenario One: Database and Secret Server Are in the Same Location	191
Scenario Two: The Database and Secret Server Are in Different Locations	192
Scheduled Backups	194
Server Clustering	195
SQL Server Mirroring	196
<i>Introduction</i>	196
<i>Procedures</i>	196
Setting up Databases for Mirroring	196
SQL Server Configuration	196
Configuring Mirroring	196
Configuring Secret Server for Mirroring	197
Testing Mirroring	199
Database SSL Configuration	199
Unlimited Administration Mode	201
<b>Developer Resources</b>	202
Custom Reports	202

General Scripting	202
REST API	202
Scripting Dependencies	202
Scripting Tools and CLI	202
SOAP API	203
Directory Services	204
Active Directory	205
<i>Active Directory Rights for Synchronization Account</i>	206
Recommended Permissions	206
<i>Object Tab</i>	206
Minimum Required Permissions	206
<i>Object Tab</i>	206
<i>Properties Tab</i>	206
<i>Configuration Parameters</i>	207
<i>Configuring Active Directory</i>	208
Step 1: Enabling Active Directory Integration	208
Step 2: Adding a Domain	208
Step 3: Setting Up Synchronization Groups	208
Step 4: Adding Groups	208
Step 5: Enabling Active Directory Synchronization	208
Step 6: Choosing Synchronization Groups	209
Step 7: Running Active Directory Synchronization	211
<i>Converting Local Users to Domain Users</i>	212
<i>Creating Active Directory Users</i>	213
<i>Enabling and Disabling Active Directory Users</i>	214
<i>Syncing and Authenticating AD Users via a Distributed Engine</i>	215
Local Versus Distributed Engine Sites	215
<i>Understanding Active Directory Automatic User Management</i>	217
Overview	217
Examples	217
<i>Example One</i>	217
<i>Example Two</i>	217
<i>Example Three</i>	217
Lightweight Directory Access Protocol (LDAP)	218
Discovery	219
Overview	219
How Discovery Works	219
<i>Automated Discovery</i>	219
Automated Discovery Terms	219
<i>Discovery Source</i>	219

<i>Discovery Scanner</i>	219
<i>Discovery Input Template</i>	219
<i>Discovery Output Template</i>	219
Example Automated Discovery Process	220
<i>Manual Discovery</i>	220
Discovery and Sites—Where Does Secret Server Run Discovery Scans?	221
Discovery Performance	221
Extensible Discovery	221
Account Permissions for Discovery	222
<i>Unix</i>	222
<i>ESXi</i>	222
<i>Local Windows Accounts</i>	222
<i>Windows Services, Scheduled Tasks, App Pools, and COM+ Applications</i>	222
AWS Account Discovery	223
<i>Enabling AWS Discovery</i>	224
<i>Password Management in AWS</i>	225
Amazon IAM Keys	225
Amazon IAM Console Password	225
Permissions Required for Secret Key Changes	225
Permissions Required for Changing the Amazon IAM Console Password	225
Discovery Best Practices	227
<i>Overview</i>	227
<i>Global Settings</i>	227
Enabling Port Scanning	227
<i>Introduction</i>	227
<i>Accessing Port Scanning</i>	228
<i>Additional Reasons to Consider Discovery Port Scanning</i>	228
<i>Lowering the Discovery Scanner Timeout May Cause Issues</i>	228
<i>Secrets with Multiple Dependencies May Create Especially Long Timeouts</i>	228
When to Run Discovery	228
Discovery Settings	229
<i>Environment-Specific Considerations</i>	229
Discovery Scan Offset Hours	229
Advanced Settings	230
<i>Run Secret Computer Matcher Once per Discovery</i>	230
<i>Limit the Network Traffic Caused by Nested Organizational Units</i>	231
<i>Engines and Engine Workers</i>	232
Enabling Active Directory Domain Discovery	233
Enabling Secret Server Discovery	234
Enabling Specific OU Domain Discovery	235

Unix Account Discovery	236
VMware ESX/ESXi Account Discovery and RPC	237
<i>Overview</i>	237
<i>Details</i>	237
<i>Download Locations</i>	238
<i>Troubleshooting and Issues</i>	238
<i>ESXi Certificate Settings</i>	238
Distributed Engines	240
Overview	240
Architecture and Workflow	240
<i>Main Components</i>	240
<i>Ports</i>	241
<i>Security</i>	241
<i>Engine Workflow</i>	242
Configuring Distributed Engines	242
FAQ	242
Configuration and Sizing	244
<i>Requirements</i>	244
Windows Server 2012	244
Distributed Engine Offline and Online Events	245
Internal Site Connector	246
Security	247
Events and Alerts	248
Secure Syslog/CEF Logging	249
<i>Overview</i>	249
<i>Configuring a Secure TCP Syslog/CEF External Audit Server in Secret Server</i>	249
Compatible Audit Servers	249
Configuring an External Audit Server	249
<i>Caching Syslog Audits</i>	250
<i>Configure Auditing for TLS Connections</i>	250
<i>Adding Client Certificate Thumbprints</i>	251
<i>Determining the Status of a Remote Audit Server</i>	251
<i>Compatibility Notes for Client Certificates</i>	251
IIS Application Pool Certificate Permissions	251
AlienVault	252
Alert Notification Center (Inbox)	253
<i>Marking Alerts as Viewed</i>	253
Event Pipelines	255
<i>Overview</i>	255
<i>Definitions</i>	255

Event Pipelines	255
Event Pipeline Policies	255
Event Pipeline Filters	255
<i>Secret Policy Filters</i>	255
<i>User Policy Filters</i>	256
Event Pipeline Policy Targets	256
Event Pipeline Tasks	256
<i>Secret Tasks</i>	257
<i>User Tasks</i>	258
Event Users	259
Event Variables	259
<i>Secret Field Tokens</i>	259
<i>Event Setting Tokens</i>	259
<i>Secret Setting Tokens</i>	259
<i>Additional Tokens</i>	261
<i>Secret</i>	261
<i>Folder</i>	261
<i>Event User</i>	261
<i>Target User</i>	262
<i>Custom Task Variables</i>	262
<i>Global Variable</i>	262
<i>Item Variable</i>	262
Target User	262
Triggers	262
<i>Secret Triggers</i>	262
<i>User Triggers</i>	263
<i>Permissions</i>	264
<i>Procedures</i>	264
Event Pipelines	264
<i>Activating or Deactivating Event Pipelines</i>	264
<i>Creating New Event Pipelines</i>	264
<i>Step One: Create EP</i>	264
<i>Step Two: Add Triggers</i>	264
<i>Step Three: Add Filters</i>	265
<i>Step Four: Choose Tasks</i>	265
<i>Editing Existing Event Pipelines</i>	265
<i>Viewing Event Pipelines</i>	265
Event Pipeline Policies	265
<i>Activating or Deactivating Event Pipeline Policies</i>	266
<i>Adding an Existing Event Pipeline</i>	266

<i>Assigning Folders and Secret Policies to Event Policy Targets</i>	266
<i>Folders</i>	266
<i>Secret Policies</i>	266
<i>Creating, Importing, and Duplicating Event Pipeline Policies</i>	266
<i>Monitoring Event Pipeline Policies</i>	267
<i>Ordering Event Pipelines in Event Pipeline Policies</i>	267
<i>Removing Event Pipelines from Event Pipeline Policies</i>	267
<i>Infinite Loops</i>	267
<i>Configuring Advanced Settings</i>	268
Event Subscription Page	269
<i>Creating Event Subscriptions</i>	270
<i>Deleting a Subscription</i>	271
<i>Editing a Subscription</i>	272
<i>Event List</i>	273
System Log	277
Viewing Event Subscription Logs	278
Mobile Computing	279
Setting Maximum Time for Offline Caching	280
<i>Overview</i>	280
<i>Procedure</i>	280
<i>Example</i>	281
Secret Server Networking	282
Changing SQL Server Connection Parameters	283
RabbitMQ Naming Conventions for Queues	285
<i>Introduction</i>	285
<i>Secret Server Roles</i>	285
<i>Queue Names</i>	285
Section1	285
Section2	286
Section3	286
<i>Secret Server Roles and Queues</i>	286
Background Worker Role Queues	286
<i>Active Directory Synchronization</i>	287
<i>Bulk Operation</i>	287
<i>ConnectWise Integration</i>	287
<i>Discovery</i>	287
<i>Duo Integration</i>	287
<i>Email Processing</i>	287
<i>Event Pipelines</i>	288
<i>Heartbeat and Remote Password Change</i>	288

<i>Import</i>	289
<i>Management: Backup, and Cleanup</i>	289
<i>Distributed Engine Management</i>	289
<i>Password Generation</i>	289
<i>Reports</i>	290
<i>Run Now</i>	290
<i>Scheduled Tasks</i>	290
<i>Search</i>	291
<i>SSH Terminal</i>	291
<i>Thycotic Privilege Behavior Analytics Integration</i>	291
<i>Thycotic Privilege Manager Integration</i>	292
<i>Thycotic Telemetry</i>	292
<i>Thycotic One Identify Provider Integration</i>	292
Engine Role Queues	292
<i>Active Directory Synchronization</i>	292
<i>Discovery</i>	293
<i>Heartbeat, Remote Password Change, and Dependency</i>	293
<i>Management</i>	294
<i>Proxy</i>	294
<i>Scripting</i>	294
<i>Syslog Integration</i>	294
<i>Thycotic Privilege Behavior Analytics Integration</i>	294
<i>Ticketing System Integration</i>	295
Engine Worker Role Queues	295
<i>Active Directory Synchronization</i>	295
<i>Discovery</i>	295
<i>RDP Proxy, SSH Proxy, and SSH Terminal</i>	295
<i>Syslog Integration</i>	296
<i>Heartbeat, Remote Password Change, and Dependency</i>	296
<i>Thycotic Privilege Behavior Analytics Integration</i>	297
<i>Distributed Engine Management</i>	297
Session Recording Worker	297
<i>Post Recording</i>	297
<i>Video Conversion</i>	297
<i>Post Recording (Legacy)</i>	298
<i>Management</i>	298
RDP Proxy Configuration	299
<i>Overview</i>	299
<i>Recommended Method</i>	299
How It Works	299

Configuration	299
Configuration Settings	300
<i>Alternative Method</i>	300
How It Works	300
Configuration	301
<i>Known Issues</i>	301
"Could not load file or assembly..." Error	301
RDP Proxy Does Not Work with FIPS Validation	301
Secret Server Clustering	303
<i>Overview</i>	303
Clustering and Background Thread Changes in 10.7.	303
Clustering Overview	303
<i>Nodes</i>	303
<i>Backbone Bus</i>	303
<i>Engine Response Bus</i>	303
<i>Worker Roles</i>	303
<i>Component Communication</i>	303
<i>Server Node Configurations</i>	304
<i>Scheduled Background Operations</i>	305
<i>Procedures</i>	306
Markdig.Syntax.Inlines.EmphasisInline	306
Upgrading Secret Server in a Clustered Environment	307
<i>Overview</i>	307
<i>Procedure</i>	308
Upgrading Database Mirroring	308
Upgrading Disaster Recovery Installations	309
Load Balancing Secret Server Clusters	309
<i>Custom URL Configuration</i>	309
<i>SSL Recommendations</i>	309
<i>Configuring Client's IP Address (X-Forwarded-For)</i>	310
<i>Clustering Errors</i>	310
Secret Server Support for HTTP/2	311
SSH Proxy Configuration	312
<i>Enabling Proxy</i>	312
<i>Web Application Proxy Performance</i>	312
Minimum Hardware	312
Session Activity	312
<i>Proxy Connections</i>	312
<i>SSH Proxy with Multiple Nodes</i>	314
Ports Used by Secret Server	315

<i>Overview</i>	315
<i>Port Listing</i>	315
<i>Related Articles and Resources</i>	317
<b>Remote Password Changing</b>	318
Automatic Remote Password Changing	319
<i>Auto Change Schedule</i>	319
<i>Understanding Expiration, Auto Change and Auto Change Schedules</i>	321
Definition	321
Examples	321
<i>Scenario One: Expiration with Auto Change and No Auto Change Schedule</i>	321
<i>Scenario Two: Expiration with Weekly Auto Change</i>	321
<i>Scenario Three: Expiration with No Auto Change</i>	321
Important Considerations and Best Practices	321
<b>Configuring Secret Dependencies for RPC</b>	323
<i>Creating Custom Dependencies</i>	324
<i>Dependency Groups</i>	325
<i>Dependency Settings and Information</i>	326
<i>Manually Adding Dependencies</i>	328
<i>Using Regex with Dependencies</i>	329
Overview	329
UNC Names	329
Examples	330
<i>XML Configuration Files</i>	330
<i>Example One</i>	330
Source	330
Regex	330
<i>Example Two</i>	330
Source	330
Regex	330
<i>Windows Initialization (.ini) Files</i>	330
Source	330
Regex	330
<i>SQL Server Connection Strings</i>	330
Source	330
Regex	330
<i>Oracle Connection Strings</i>	331
<i>Example One</i>	331
Source	331
Regex	331
<i>Example Two</i>	331

Source	331
Regex	331
YAML	331
Source	331
Regex	331
Custom Password Changers	332
Changing Ports and Line Endings	333
Creating a Custom Password Changer	334
Deactivating Password Changers	335
Distributed Engines and RPC	336
Editing Custom Commands	337
RPC-Mapped Text-Entry Fields	337
Associated Reset Secrets	337
Check-Result Commands	338
Enabling RPC	339
Mapping Account Fields for RPC	340
Mapping an SSH Key or Private Key Passphrase for Authentication	341
Minimum Requirements for Windows Local Accounts	343
Modifying Password Changers	344
Password Changing Scripts	345
Creating Scripts	345
Testing Scripts	345
Using Scripts	345
Viewing Audits	345
Privileged Accounts and Reset Secrets	346
RPC Error Codes	347
RPC for Service Accounts and SSH Keys	348
Service Accounts	348
SSH Keys	348
RPC Logs	349
Running a Manual RPC	350
Treating Specific Heartbeat "Unknown Errors" as Connection Failures	351
Procedure	351
Triggering an RPC When Defined Errors Occur	354
Procedure	354
Password Changer List	358
Overview	358
List	358
PostgreSQL and ODBC Remote Password Changing	361
Overview	361

<i>Create an ODBC Password Changer</i>	361
<i>Example Reset Commands</i>	361
<i>Adding Connection Strings</i>	361
Adding Connection Strings to Password Changer Settings	361
Adding Connection Strings to Secrets	362
<i>Troubleshooting</i>	362
<i>PostgreSQL with Distributed Engines</i>	362
Remote Password Changing with PowerShell	363
<i>Overview</i>	363
<i>Procedure</i>	363
Task 1: Creating the Active Directory Verify Password Script	363
Task 2: Creating the Active Directory Change Script	363
Task 3: Testing the Scripts	363
Task 4: Configuring a Password Changer for Secret Server Version 10.0.000006 and Later	364
Task 5: Creating a Secret Template	365
Task 6a: Finishing the Secret Template Configuration for Secret Server 10.0.000006 and later	365
Task 6b: Finishing the Secret Template Configuration for Secret Server 8.8.000000 to 10.0.000000	365
Task 7: Creating Secrets Using PowerShell Remote Password Changing	366
<i>Errors</i>	367
Salesforce.com Password Changer	368
Reports	369
Built-in Reports	371
<i>Activity</i>	371
<i>Discovery Scan</i>	371
<i>Folders</i>	371
<i>Groups</i>	371
<i>Legacy Reports</i>	371
<i>Password Compliance</i>	372
<i>Report Schedules</i>	372
<i>Roles and Permissions</i>	372
<i>Secrets</i>	372
<i>Secret Policy</i>	372
<i>Users</i>	372
Creating and Editing Reports	374
<i>Creating a Custom Report</i>	374
<i>Editing Reports</i>	377
<i>Report SQL Scripts</i>	378
Overview	378
Dynamic Parameters	378
Viewing Secret Server SQL Database Information	378

<i>Database Paging</i>	378
Deleting or Undeleting Reports	379
Modifying Report Categories	380
Report Page	381
<i>Reports General Tab</i>	381
<i>Reports Security Hardening Tab</i>	381
Configuration Section	381
Database Section	382
Environment Section	382
SSL Section	382
<i>Reports User Audit Tab</i>	383
Reporting and Dual Controls	384
Saving Reports to File	385
Scheduled Reports	388
<i>Creating New Schedules for Reports</i>	388
<i>Viewing Existing Report Schedules</i>	388
<i>Editing Schedule Settings</i>	388
Using Dynamic Parameters in Reports	389
<i>Primary Parameters</i>	389
#STARTDATE	389
#ENDDATE	389
#USER	389
#ORGANIZATION	389
#GROUP	390
#FOLDERID	390
#FOLDERPATH	390
#CUSTOMTEXT	390
<i>Additional Parameters</i>	390
Parameters	390
Example	391
<i>Coloring Your Reports</i>	391
Viewing Auditing for a Report	392
Viewing Reports	393
<b>Roles</b>	394
Assigning Roles to a User	395
Creating Roles	396
Editing Role Permissions	397
Secret Server Role Permissions List	398
<i>Overview</i>	398
<i>Complete List</i>	398

<b>Secret Checkout</b>	408
Checking Out Secrets	409
Checkout Hooks	410
<i>Overview</i>	410
<i>Checkout User Variables for Scripts</i>	410
Configuring a Secret for Checkout	411
Configuring Password Changing on Check-in	412
Exclusive Access	413
<b>Secret DoubleLocks</b>	414
Assigning a DoubleLock to a Secret	415
Assigning a User a DoubleLock Password	417
Assigning Users to Existing DoubleLocks	419
Creating a DoubleLock and a DoubleLock Password	423
DoubleLock Objects and Relationships	428
Password Loss and Assignment	429
Resetting a DoubleLock Password	430
Using a DoubleLock	432
<b>Secret Folders</b>	433
Folder Permissions	434
<i>Personal Folders</i>	434
<i>Required Role Permissions for Managing Folders</i>	434
Folder Synchronization	435
<i>Synchronizing with the ConnectWise API</i>	435
<i>Synchronizing with a Database (Advanced)</i>	437
Managing Folders	438
<i>Adding and Moving Secrets Between Folders</i>	439
<i>Assigning Secret Policies to Folders</i>	441
<i>Creating Folders</i>	442
<i>Editing Folder Permissions</i>	443
<i>Enabling Personal Folders</i>	447
<i>Modifying Folders with Secret Policies</i>	449
<i>Moving Folders</i>	451
<b>Secret Heartbeats</b>	452
Alerts on Heartbeat Failure	453
Configuring Heartbeat	454
Enabling Heartbeat in RPC	455
Heartbeat Logs	456
Heartbeat Status Codes	457
Remote Accounts Supported	458
Running Heartbeat for a Secret	459

Secret Import and Export	460
Exporting Secrets	461
Import and Export File Format	462
Import and Export Secret Template Settings	463
Importing Secrets	464
<i>Configuring Data for Importation</i>	464
<i>Importing Secrets with the Secret-Server Migration Tool</i>	465
<i>Importing Secrets with Advanced XML Importation</i>	466
Importing Secrets with XML	467
<i>Notes</i>	467
<i>Sample XML</i>	467
Secret Launchers and Protocol Handlers	470
Built-In Launcher Types	471
Custom Launcher for SecureCRT (SSH)	472
<i>Step 1: Creating the Custom Launcher</i>	472
<i>Step 2: Creating a Custom Secret Template (optional)</i>	475
<i>Step 3: Associating the Launcher with a Secret Template</i>	475
Custom Launchers	477
<i>Creating Custom Launchers</i>	478
<i>Custom Launcher Errors</i>	482
<i>Custom Launcher Process Arguments</i>	483
Syntax	483
Examples	483
Enabling CAC/PIV Smart Cards for Secret Launchers	484
<i>Overview</i>	484
<i>Enabling Globally with User Settings</i>	484
<i>Enabling on a Specific Secret</i>	484
Enabling Launchers	485
<i>Introduction</i>	485
<i>MSI Installer</i>	485
<i>Installing by Group Policy</i>	486
Launcher Configuration and Support	487
<i>Adding a Program Folder to the Windows PATH</i>	488
<i>Common Launcher Errors</i>	489
<i>Configuring Launchers on the Secret</i>	490
<i>Configuring SSH Proxies for Launchers</i>	491
<i>Default Launcher Requirements</i>	495
<i>Managing Superuser Privilege</i>	496
<i>Session Recording and Launchers</i>	499
Launching Sessions	500

Limiting Launcher Domains	501
Remote Desktop Launchers	502
<i>Adding Remote Desktop Launchers</i>	503
<i>Browser Configuration</i>	504
<i>Editing RD Launchers</i>	505
<i>Setting Up Secret Templates for RD Launchers</i>	506
Web Launchers	507
<i>Configuring Web Launchers for Secrets</i>	508
<i>Creating a Configuration</i>	509
<i>Launching to a Website</i>	510
<b>Secret Management</b>	511
Procedures	512
<i>Creating Secrets</i>	513
<i>Customizing the All-Secrets Page</i>	516
Customizing Visible Columns	516
Filtering Search Results	516
Sizing Columns	516
<i>Deleting and Undeleting Secrets</i>	517
<i>Duplicating Secrets</i>	518
<i>Editing Secrets</i>	519
<i>Overriding the Secret Template's Password Requirements</i>	520
<i>Setting Up Password Masking</i>	521
<i>Sharing Secrets</i>	522
Permissions	522
Procedure	522
<i>Viewing Secrets</i>	524
Searching and Search Indexer	525
<i>Searching for Secrets</i>	525
<i>Search Indexer</i>	525
Secret Configuration Options	529
<i>Common Configuration Options</i>	529
<i>Advanced Configuration Options</i>	529
Secret Expiration	530
<i>Forcing Expirations</i>	531
<i>Resetting Expired Secrets</i>	532
<i>Setting up Secret Templates for Secret Expiration</i>	533
<i>Setting up Secrets</i>	534
Secret Tabs	535
<i>Secret Dependencies Tab</i>	536
<i>Secret Expiration Tab</i>	537

<i>Secret Launcher Tab</i>	538
<i>Secret Personalize Tab</i>	539
<i>Secret RPC Tab</i>	540
<i>Secret Security Tab</i>	541
<b>Secret Server Cloud</b>	542
Secret Server Cloud Architecture	543
<i>Diagram</i>	543
<i>Details</i>	543
1: Service Buses	544
2: Web Application Firewall (WAF)	544
3: Content Delivery Network (CDN)	544
4: RADIUS	544
5: Distributed Engine (DE)	544
6: Certificate CRLs	544
<b>Secret Server End User Guide</b>	546
What Is Secret Server?	546
What Is the Purpose of the End User Guide?	546
Getting Help	546
Logging on Secret Server	546
Secrets	548
Secret Folders	548
Using Secrets on Websites (Web Password Filler)	548
Checking out Secrets	549
Getting Notified of Secret Events	549
Learning More About Secret Server—the Getting Started Tutorial	549
<b>Secret Server Setup</b>	550
Licensing	551
<i>Understanding Licenses</i>	551
<i>Activating Licenses</i>	551
<i>Installing New Licenses</i>	551
<i>Converting from Trial Licenses</i>	552
<i>Licensing Limited Mode</i>	552
<i>License Activation FAQ</i>	553
Upgrading	555
Upgrading Secret Server with Web Clustering	556
<i>Introduction</i>	556
<i>Before Beginning</i>	556
<i>Upgrading a Clustered Environment</i>	556
<i>EFS and DPAPI Encryption</i>	556
<i>Upgrading Database Mirroring</i>	557

<i>Upgrading Remote DR Instances</i>	557
<i>Error Conditions</i>	557
Installation	558
<i>Enabling SQL Server Encryption</i>	559
<i>Manual IIS Installation</i>	561
Roles and Features	561
<i>Roles</i>	561
<i>Features</i>	562
Step One: Windows Server 2012–2019 IIS Installation	562
Step Two: Configure the IIS Website	563
Step Three: Ensure IIS Does Not Stop the Worker Process	564
Step Four: Ensure the User Profile Always Loads	565
<i>Running the IIS Application Pool As a Service Account</i>	566
Overview	566
Procedure	566
<i>Task 1: Creating a Domain Service Account</i>	566
<i>Task 2: Granting Access to the SQL Database</i>	566
<i>Task 3: Assigning the Identity of Application Pools</i>	567
<i>Task 4: Granting Folder Permissions</i>	567
<i>Task 5: Configuring User Rights</i>	568
<i>Option 1: Setting User Rights Assignment on the Domain</i>	568
<i>Option 2: Setting User Rights Assignment Locally</i>	568
<i>Advanced (Manual) Installation</i>	570
Procedure	570
<i>Step 1: Downloading the Secret Server Application Files</i>	570
<i>Step 2: Creating Folders and Extracting Contents</i>	570
<i>Step 3: Configuring IIS</i>	570
<i>Step 4a: Installing Secret Server as a Virtual Directory</i>	570
<i>Step 4b: Installing Secret Server as a Website</i>	571
<i>Step 5: Completing Secret Server Installation from the Website</i>	571
Troubleshooting Notes	571
<i>Basic (Automatic) Installation</i>	573
Introduction	573
<i>Secret Server Is an ASP.NET Website</i>	573
<i>SQL Server Is Usually Required</i>	573
<i>Administrative Access</i>	573
<i>Review the Prerequisites</i>	573
<i>System Requirements Overview</i>	573
<i>Additional Recommendations</i>	573
Procedure	573

<i>Step 1: Downloading the Latest Version of Secret Server</i>	573
<i>Step 2: Running the Installer</i>	574
<i>Welcome Page</i>	574
<i>Database Page</i>	574
<i>Pre-Requisites Page</i>	574
<i>Database Connection Page</i>	574
<i>Create User Page</i>	574
<i>Email Server Page</i>	574
<i>Review Page</i>	574
<i>Install Page</i>	574
<i>Step 3: Reviewing the Log Files (Optional)</i>	574
<i>Step 4: Opening Secret Server</i>	574
<i>Step 5: Learning Secret Server</i>	575
<b>Installing and Configuring SQL Server</b>	576
Creating a SQL Account	576
SQL Authentication	576
Windows Authentication	576
Configuring Database Access in Secret Server	576
SQL Location	576
SQL Authentication	576
<b>Installing RabbitMQ</b>	578
Overview	578
What is RabbitMQ?	578
Why do you need to install it?	578
RabbitMQ and Encryption	578
Prerequisites	578
General	578
SSL Certificate	578
Installation	578
Task 1: Secret Server	578
Task 2: RabbitMQ Host	580
Troubleshooting	581
<b>SQL Server 2014 Express Edition Installation</b>	582
Overview	582
Procedures	582
Downloading SQL Server Express with Tools	582
Installing SQL Server Express 2014	583
Creating the SQL Server Database	590
Adding a SQL Server User	590
<b>SQL Server 2016 Standard Edition Installation</b>	592

Overview	592
Procedures	592
<i>Installing SQL Server 2016</i>	592
<i>Installing SQL Server Management Studio</i>	597
<i>Creating the SQL Server Database</i>	599
<i>Adding a SQL Server User</i>	599
Prerequisites	601
<i>System Requirements</i>	601
<i>Hardware Requirements</i>	601
<i>Software Requirements</i>	601
Checklist	601
SQL Server	601
Application Server	601
System Requirements for Secret Server	602
<i>Minimum Requirements for Basic Deployments</i>	602
<i>Recommended Requirements for Basic Deployments</i>	602
<i>Minimum Requirements for Advanced Deployments</i>	602
<i>Recommended Requirements for Specific Features</i>	603
<i>Notes</i>	603
Upgrading Secret Server Without Outbound Access	605
<i>How Upgrades Work</i>	605
<i>Procedure</i>	605
Step 1: Open the Upgrade Secret Server Wizard	605
Step 2: Get and Upload the Latest .zip File	606
Step 3: Upgrade Secret Server	606
Secret Templates	607
Managing Secret Templates	608
<i>Activating and Deactivating Templates</i>	609
<i>Changing a Secret's Template</i>	610
<i>Configuring Secret Template Permissions</i>	611
<i>Creating or Editing Secret Templates</i>	614
Secret Template Settings	618
<i>Field Slug Names</i>	619
<i>Secret Template Field Types</i>	620
<i>Secret Template Text-Entry Field and Control Settings</i>	621
SSH Authentication Templates	622
Template Character Sets	623
Template Naming Patterns	624
Template Password Requirements	625
<i>Creating a Custom Password Requirement</i>	626

<i>Setting the Password Requirement for a Secret Template</i>	630
<b>Secret Workflow Templates</b>	632
Multi-Level Workflow	632
Multiple Approvers to Advance	632
Approval Process Workflow	632
Workflow Versus Basic Access Requests	633
Accessing the Workflow Designer	634
Assigning Workflows to Secret Policies	636
Creating New Workflow Templates	639
Deleting Workflow Templates	642
Duplicating Workflow Templates	644
Editing Workflow Templates	647
Understanding Workflow Template Design Best Practices	648
<b>Security and Hardening</b>	649
Secret Server Telemetry	650
<i>Overview</i>	650
<i>Checking for and Downloading Updates</i>	650
<i>License Activation</i>	650
<i>Reporting Anonymized Usage Metrics</i>	650
<i>Setting and Viewing Secret Server Telemetry</i>	651
Securing ASP Cookies	653
Security Hardening Guide	654
<i>Introduction</i>	654
<i>Overview</i>	654
<i>Best Practices</i>	654
General	654
Active Directory	654
Database	654
Application Server	655
Application Settings	655
<i>Security Hardening Report</i>	656
Configuration Section	656
<i>Allow Approval for Access from Email</i>	656
<i>Browser AutoComplete</i>	656
<i>File Attachment Restrictions</i>	656
<i>Frame Blocking</i>	657
<i>Force Password Masking</i>	657
<i>Login Password Requirements</i>	657
<i>Maximum Login Failures</i>	657
<i>Remember Me</i>	658

<i>Secure Session and Forms Auth Cookies</i>	658
<i>Markdig.Syntax.Inlines.EmphasisInline</i>	658
<i>Zero Information Disclosure Error Message</i>	658
Database Section	658
<i>SQL Account Using Least Permissions</i>	658
<i>SQL Server Authentication Password Strength and Username</i>	659
<i>Windows Authentication to Database</i>	659
Environment Section	659
<i>Application Pool Identity</i>	659
<i>DPAPI or HSM Encryption of Encryption Key</i>	659
SSL Section	660
<i>Require SMTP SSL</i>	660
<i>Require SSL</i>	660
<i>SSL/TLS Hash</i>	660
<i>SSL/TLS Key</i>	660
<i>SSL/TLS Protocols</i>	661
<i>Using HTTP Strict Transport Security</i>	661
Security Settings Not in the Hardening Report	661
Apply TLS Certificate Chain Policy and Error Auditing	661
Enable FIPS Compliance	661
Key Rotation	662
Two-Factor Authentication	662
SAML	662
Email	662
Soft Tokens	662
RADIUS	662
Duo Security	662
Enabling Two-Factor Authentication	662
<i>Enabling for Users</i>	662
<i>Enabling per Domain</i>	663
Roles	663
Controlling Access to Features Using Roles	663
<i>Limiting Role Access to the Export Permission</i>	663
<i>Unlimited Administration Mode</i>	663
<i>Limiting Role Access to Secret Templates</i>	663
<i>Monitoring Roles with Event Subscriptions</i>	663
Using Two Roles for Access to Unlimited Administration Mode	663
Encryption	664
DPAPI Encryption	664
Overview	664

<i>Enabling and Disabling DPAPI</i>	664
<i>Using Clustering with DPAPI</i>	665
Protecting Your Encryption Key Using EFS	665
SSL (TLS) and HSTS	666
SSH Key Validation	666
Mapping an SHA1 Digest to Secrets	666
Validating SHA1 Digests for Unix Account Discovery	666
<i>Disabling IIS HTTP Headers</i>	666
Introduction	666
Procedure	666
<i>Additional Resources</i>	667
Session Recording	668
Basic Session Recording	668
Advanced Session Recording	670
Session Recording Tab	671
Caveats and Recommendations	672
<i>General</i>	672
<i>Database</i>	672
<i>Network Bandwidth and Video</i>	672
<i>Session Recording</i>	673
<i>macOS Catalina Security</i>	673
Configuring Session Recording	675
<i>Overview</i>	675
<i>Configuration</i>	675
Using Legacy Video Codecs	675
Enabling Session Recording on Secrets	675
Extending Session Recording with Custom Launchers	676
<i>Record Multiple Windows Option</i>	676
<i>Record Additional Processes Option</i>	677
<i>Example</i>	677
Advanced Session Recording	677
<i>Metadata Recording</i>	677
<i>Record All Sessions</i>	677
Session Recording Settings	678
<i>Hide Recording Indicator</i>	678
<i>Enable On-Demand Video Processing</i>	678
<i>Enable Inactivity Timeout (Minutes)</i>	678
<i>Max Session Length (Hours)</i>	678
<i>Use Hardware Acceleration</i>	678
<i>Save Videos to</i>	678

<i>Archive Location Dependent on Site</i>	679
<i>Folder Path</i>	679
<i>Encrypt Archive on Disk</i>	679
<i>Enable Archiving to Disk</i>	679
<i>Enable Deleting</i>	679
<i>Setting Notes</i>	679
<i>Using Network Share Path</i>	679
Session Recording Requirements	681
<i>Advanced Session Recording</i>	682
<i>Basic Session Recording</i>	683
Stability and Compatibility with Older ASRAs	684
<i>Enabling Inactivity Timeout</i>	685
<i>Enabling On-Demand Video Processing</i>	686
<i>Record All Sessions</i>	687
<i>Recording Metadata</i>	688
System Capacity Specifications	689
Thycotic Support	690
Step One: Gather Information You May Need	690
Step Two: Get a Mandatory Support PIN	690
Step Three: Choose a Support Method	690
Step Four: Contact Support	690
<i>Phone Support</i>	690
<i>Email Support</i>	691
<i>Ticketing System Support</i>	691
Ticketing System Integration	692
BMC Remedy Integration	693
<i>Configurable Settings</i>	694
Validating Ticket Status	694
View Ticket URL Template	694
Ticket Number Format Pattern (Regex)	694
Ticket Number Validation Error Message	694
Service Endpoint URL	694
System Credentials	694
Authentication	694
Add Comments to Ticket	695
Comment Work Type	695
<i>Requirements</i>	696
<i>Testing Your Integration Setup</i>	697
PowerShell Ticketing Integration	698
<i>Configurable Settings</i>	698

View Ticket URL Template	698
Ticket Number Validation Pattern (Regex)	698
Ticket Number Validation Error Message	698
The PowerShell RunAs Credentials	698
System Credentials	698
<i>Validating Ticket Status</i>	698
Overview	698
Sample Script	698
<i>Adding Comments to Tickets</i>	699
<i>Adding Comments to a General Audit Log</i>	699
ServiceNow Integration	700
<i>Configurable Settings</i>	701
View Ticket URL Template	701
Ticket Number Format Pattern (Regex)	701
Ticket Number Validation Error Message	701
Instance Name	701
System Credentials	701
Add Comments to Ticket	701
<i>Requirements</i>	702
<i>Testing your Integration Setup</i>	703
Ticket Number Validation	704
Ticket System Tab	705
Troubleshooting and Notices	706
Changing IIS to Not Stop Worker Process in IIS 7.0 and Later	707
Overview	707
Procedure	707
HTTP 404.2 Error ISAPI/CGI Restrictions Stopping .NET Framework 4.5.1	708
Error	708
Resolution	708
HTTP Error 404.17 - Not Found After Upgrading .NET Framework Version	709
Error	709
Resolution	709
Windows Server 2012 or 2012 R2	709
Load User Profile Setting Must Be Enabled for Application Pool	710
Notice: jQuery CVE-2019-11358	711
Relevance	711
Technical Issue	711
Resolution	711
Related Articles and Resources	711
Notice: jQuery CVE-2020-11022	712

<i>Relevance</i>	712
<i>Technical Issue</i>	712
<i>Resolution</i>	712
<i>Related Articles and Resources</i>	712
Troubleshooting Invalid Domain Errors	713
<i>Troubleshooting Procedure</i>	713
<i>Configuring the DNS Record on Your Server</i>	714
<i>Resolving Other DNS Issues</i>	714
Windows Local-Account Access-Denied Error Workaround PowerShell Scripts	716
<i>Overview</i>	716
<i>Additional Requirements</i>	716
<i>Remediation Options</i>	716
<i>Option 3: Modifying the Default GPO</i>	716
PowerShell Script Description	716
Download	716
Script Argument Help	717
<i>Command Prompt Help</i>	717
<i>Parameters</i>	717
-ComputerNames (string)	717
-Username (string)	717
-GroupName (string)	717
-ForceGPUUpdate	717
<i>Examples</i>	717
Related Articles and Resources	718
<i>Option 4: Creating a Heartbeat GPO Workaround</i>	718
User Groups	721
Assigning Group Owners	722
Assigning Users to Groups	726
Creating User Groups	729
User Teams	730
What Are Secret Server Teams for?	730
Team-Related Permissions	730
Configuring Teams Management	731
Creating Teams	732
Deactivating Teams	738
Editing Teams	740
Troubleshooting Teams	745
Viewing a User's Teams	746
Users	749
Bulk Operations on Users	750

Configuring Users	751
Creating Users	752
Deleting Users	753
Password Settings	754
Removing Deactivated User PII	755
<i>Overview</i>	755
<i>Removing the PII</i>	755
<i>Active Directory Considerations</i>	755
Unlocking Local Accounts	756
User Login Settings	757
User Owners	758
User Preferences	759
<i>General Tab</i>	759
<i>Launcher Tab</i>	759
User Restriction Settings	760
User Settings	761
Webservices	762
Enabling Webservices	763
Integrated Windows Authentication Webservice	764
Using the Java Console API to Access Secret Values	765
Secret Server Release Notes	766
Current	766
Secret Server On-Premises Legacy	766
Secret Server Cloud Legacy	766
Documentation Releases	766

## Introduction

Thycotic Secret Server (SS) is an enterprise-grade, privileged access management solution that is quickly deployable and easily managed. With SS, you can automatically discover and manage your privileged accounts through an intuitive interface, protecting against malicious activity, enterprise-wide. This section of the Thycotic Document Portal (TDP) supports SS.

**Note:** Navigate using the dynamic table of contents on the left, the page contents on the right, or by entering a search term above. Many pages in this documentation have sub-pages. The container (parent) pages can have introductory text or simply a heading with no text. Please click the table of contents on the left to see any sub-pages it might have.

## Documentation

- [Thycotic Documentation Portal](#): You are at the home page of the current Thycotic Document Portal for Secret Server. It contains:
  - Converted knowledge base articles. These are marked as *deprecated* in the legacy knowledge base.
  - Links to legacy knowledge bases article that have yet to be converted or retired
  - Links to legacy PDF documentation
  - New material
- [Knowledge Base Articles](#): Use the Search text box at the top of the page. This is the legacy platform that we are replacing with the Thycotic Documentation Portal (where you are right now). This portal does not yet contain all SS documentation. For now, there are many locations here where this online documentation links to legacy documentation.

**Important:** The SS portion of the Thycotic Documentation Portal is in a transitional phase and does not yet contain all SS documentation. For now, there are many locations here where the SS TDP links to legacy documentation. In addition, there are still topics that are only on the [Knowledge Base Articles](#) (use the Search text box at the top of the page).

- [End User Guide](#) (for non-technical users)
- [Getting Started Tutorial](#) (for technical users)
- [Installation Guides](#)
- [System Requirements](#)
- [Best Practices](#)
- [Discovery Best Practices](#)
- [High Availability and Disaster Recovery](#)
- [Secret Server Government Edition—Common Criteria Hardening Guide](#)
- [Security Hardening Guide](#)
- [Distributed Engine Security](#)
- [Launcher Security](#)
- [Meltdown and Spectre Security Information](#)
- [\\*nix Management](#)
- [Security Model](#)

- [Web Services Security](#)

## Help

- [Document Conventions](#)
- [Secret Server Glossary](#)
- [Self-Help Resources](#)
- [Technical Support](#)

[Download Secret Server](#)

## Current

[Integration Guides](#)

## Legacy

- [ConnectWise](#)
- [Devolutions](#)
- [F5 BIG-IP](#)
- [HP ArcSight](#)
- [HSM](#)
- [IBM Verify](#)
- [OpenID Connect](#)
- [SCIM Connector](#)
- [SecureLink](#)
- [Syslog](#)

[Release Notes](#) (On-Premises and Cloud)

- [Forum](#) (legacy—replaced by Secret Society)
- [Thycotic Secret Society](#): An Educational Community, replacing the Forum.

[Developer Resources](#)

**Note:** Many of these tutorials feature legacy versions of SS.

[Video Tutorials](#)

## Getting Started Tutorial

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server (SS) is a powerful application with many facets. As such, approaching it for the first time can be daunting. To counter that, we created this section, which is an introductory guided tutorial, for new users. The tutorial suggest an order to learn topics and points to specific sections of documentation for details.

**Important:** This tutorial is oriented toward system administrators and other technical professionals. We recommend that non-technical users start with our [End User Guide](#).

Below are our suggested guidelines for preparing to run a trial or proof-of-concept (POC) of SS.

## System Requirements

Please review the detailed [System Requirements for Secret Server](#). The *Minimum Requirements* are for trial, sandbox, and POC environments. The *Recommended Requirements* are for production deployments.

## Hardware Requirements

SS can be installed on a physical server or virtual machine.

If you would like to set up front-end (application) clustering, you need to have two or more servers available.

For testing of high availability for the SQL Server, you can use either existing Microsoft AlwaysOn infrastructure or database mirroring. If you choose to test this, this is something your database team needs to prepare in advance.

## Software Requirements

### Checklist

- Windows Server 2012 or newer (recommended) (one server, minimum)
- SQL Server (one instance, minimum)
- Application server prerequisites
- SSL certificate

### SQL Server

You can create the SQL database in an existing SQL instance, or a new installation of SQL Server. For high availability, this needs to be a paid edition of SQL Server (not SQL Express). If you are using a new installation of SQL Server, please have this installed beforehand.

Detailed instructions for installation and configuration of SQL Server are included in one of the installation guides below (choose the guide matching the OS that SQL server will be installed on).

### Application Server

We recommend installing SS on Windows Server 2012 or greater. Include IIS, ASP.NET and .NET Framework. Refer to the System Requirements KB above to view prerequisite details.

## Application Configuration

### Service Account

Set up a service account:

1. Log on as a batch job (on the server that SS runs on)
2. Modify permissions to the SS application directory (typically C:\inetpub\wwwroot) and C:\Windows\temp.
3. Provide access to your SQL Server instance by adding the db\_owner permission to the SS database.

For detailed instructions on how to configure the permissions for the service account, see [Running Secret Server IIS Application Pool with a Service Account](#) (KB). The installation guides include instructions for assigning db\_owner permission to the service account in SQL Server.

If you would like to test features that rely on Active Directory, such as AD group sync or discovery, you should also have accounts available

with the appropriate permissions (described below). One option is to use the same account for both features.

## Active Directory Group Sync

Active Directory group synchronization means that SS can automatically add users and enable or disable them to log into SS based off of their Active Directory group membership. You can choose which groups to sync. When configuring AD group sync in SS, you are required to specify an account that can read the properties of users and groups. See [AD Synchronization Rights for Synchronization Account](#) for a detailed list of required permissions.

## Discovery

To test discovery, please have some machines available for SS to connect to for discovering accounts. An account is required to sync with AD and also scan the machines found for Windows local account and service account discovery. [Account Permissions for Discovery](#) (KB) describes the permissions required for an AD account to be used for discovery.

## Test Accounts

We recommend having a few test accounts available to represent the types of accounts you want to manage using SS. These could be local Windows accounts, service accounts running scheduled tasks or services, SQL server accounts, and others.

## Email Notifications

To test email notifications, which can be used for event subscription notifications or requests for approval to passwords, you need configuration information for the company SMTP server:

- Service account to run the application and connect to SQL
- Domain (test or production)
- Domain account to be used for AD sync and discovery
- Test machines (if testing discovery)
- Test accounts
- SMTP server settings

## SSL Certificate

We recommend setting up SSL (or https) for access to SS. To do so, you will need an SSL certificate. You may use an existing wildcard certificate, create your own domain certificate, or purchase a third-party SSL certificate for the SS.

## Firewalls and Ports

SS must connect directly to a target system to change its password. For devices that are firewalled off from SS, remote agent can provide connectivity to them, but they also require connectivity from them to the target systems for password changing.

Please see [Ports Used by Secret Server](#) (KB) for a list of ports needed by SS for password changing, discovery, and other features.

## Process

Run the Installer: SS comes with an installer that walks you through the entire process from start to finish. Once you have the prerequisites ready to go, download and run your installer, and the wizard will take you through the installation process. Please see our [installation articles](#).

## Licenses

See the [Licensing](#) section.

The SS Dashboard is the main page for searching and viewing secrets. Nearly everything you do in SS starts with the Dashboard. See [Secret Server Dashboard](#) for details.

As you start using SS, we strongly recommend configuring the following security settings. While these are optional, setting them is a best practice.

## Local Admin Account Best Practices

Even if you plan to [integrate with Active Directory](#) to log into Secret Server, chances are you will need to use this account again. This is the first account you created during the installation process. Keep this account secure and avoid being locked out of SS by following these suggestions:

- Store the credentials in a secure location that you can access if you lose all access to SS.
- Enable the **Allow Users to Reset Forgotten Passwords** setting to provide a way of resetting the password if account is locked out or if the password is forgotten:
  1. Select **Admin > Configuration**. The Configuration page appears.
  2. Click the **Local User Passwords** tab to locate the setting.
  3. Click the **Edit** button to edit the setting.
  4. Click the **Save** button when finished.

**Note:** This requires having an [SMTP server configured](#) (KB).

- Configure the other **Local User Passwords** settings to enforce your password requirements, expiration, password history, and other password policies.

## SSL (HTTPS) Best Practice

We recommend requiring SSL access to SS. This requires setting up an SSL certificate for the website, preferably with a domain certificate. However, if you don't have a certificate, see [Installing a Self-Signed Certificate](#) (KB). Once you have your certificate:

1. Configure the HTTPS binding for your SS website using the certificate you choose.
2. Ensure your certificate is trusted on the SS users' machines. See [Trusting an SSL Certificate on a Client Machine](#) (KB) for instructions.
3. Enable **Force HTTPS/SSL** on the **Security** tab of the Secret Server **Configuration** settings.

Configure backups to avoid losing your data. SS provides the option to automatically take a backup on the interval you specify, sending the backups to a local or network location. There are two components of an entire backup of Secret Server: the Web application files and the database. Find these settings by selecting **Backup** from the **Admin** menu. See [Backup and Disaster Recovery](#) for more information.

To configure the backup paths, see [Backup Configuration File Path Settings](#) (KB).

**Note** The file paths configured on this page by default need to be either changed or created on each server that the SS application and database reside on.

To allow users to log in with their Active Directory (AD) credentials, you can configure your AD domain settings in SS and then add users either individually or by group.

## **Setting up Active Directory**

See [Configuring Active Directory](#).

## **Enabling Active Directory Users**

See [Enabling and Disabling Active Directory Users](#).

## **Managing Active Directory Users via a Distributed Engine**

See [Syncing and Authenticating AD Users via a Distributed Engine](#).

To try out SS, you must have folders, roles, users, and secrets to operate on:

1. Setup some folders and roles: We encourage is for you to setup a folder structure and a few roles. The folder structure is how you will keep your secrets organized, and provide access to shared secrets. Additionally, roles ensure you are able to control access to different parts of SS and assign permissions to view certain folders and secrets. See [Secret Folders](#) and [Roles](#).
2. Add users if you have not already from AD. See [Creating Users](#) and [Creating User Groups](#).
3. Add an Active Directory or other secrets. If you plan on using discovery, the account will also need permissions to scan computers on the network for accounts. See [Managing Secrets](#).

SS has a discovery feature that can automatically find local Windows accounts, Active Directory service, Unix, VMware ESX/ESXi, and Active Directory domain accounts. Account and dependency types not supported out-of-the-box in SS can still be discovered by writing PowerShell scripts that can be run as custom scanners. This allows administrators to quickly import accounts found by SS on specified domains or IP addresses.

**Note:** Please see the [Discovery Guide](#) for a comprehensive guide to configuring and using discovery.

To run discovery on a domain, IP address range, or a custom source, you need to first enable the discovery feature for SS. Second, you must enable discovery for each discovery source you would like to be scanned.

See the followings to set up Active Directory discovery:

- [Enabling Discovery for Secret Server](#)
- [Enabling Discovery for an Active Directory Domain](#)
- [Enabling Discovery for Specific OUs of a Domain](#)

SS remote password changing (RPC) provides the ability to either start a password change manually or schedule automatic password changes to occur at a regular interval.

## **Enabling Remote Password Changing**

See [Enabling RPC](#).

## **Performing a Manual RPC**

See [Run a Manual RPC](#).

## **Common RPC Error Codes**

See [RPC Error Codes](#).

Heartbeat allows you to determine from SS whether the credentials in a secret authenticate successfully with their target system. By default, heartbeat is turned off in SS. See [Heartbeats: Automatically Testing Secret Credentials](#) for general information.

## **Enabling Heartbeat**

See [Enabling Heartbeat in RPC](#).

## **Running Heartbeat**

See [Running Heartbeat for a Secret](#).

Before running reports and audits, you must create something to report on—to that end:

- Import a few accounts or create secrets manually
- Rotate passwords a few times
- View a couple of your secrets

This generates enough audit logs to provide meaningful outputs in your reports:

- Security Hardening Report
- What secrets have been accessed
- What secrets failed heartbeat
- Failed login attempts
- Secret activity

See [List of Built-In Reports](#) for the most up-to-date list of reports included.

For details on using reports, see:

- [Creating and Editing Reports](#)
- [Viewing Reports](#)

Sometimes, depending on your scenario, you want to add extra protections to highly sensitive secrets. SS has a access request and workflow features:

- [Secret Check-Outs](#): Grant access to a single user
- [Basic Secret-Access Requests](#): Require approval prior to accessing a secret for a defined time period
- [Advanced Secret-Access Requests with Workflow Templates](#): Require multi-level and multi-user approval prior to accessing a secret for a defined time period
- [Secret DoubleLocks](#): Add another security layer by encrypting secret data with a supplemental custom encryption key that is only accessible with an additional password, regardless of regular permissions.

A secret *launcher* opens a connection to the remote computer or device or logs into a website using the secret's credentials directly from the Web page. While this provides a convenient method of opening RDP and PuTTY connections, it also circumvents users being required to know their passwords. A user can still gain access to a needed machine, but it is not required to view or copy the password out of SS. A Web launcher automatically logs into websites using the client's browser.

SS launchers, also called protocol handlers, come in three primary types:

- **Remote Desktop:** Launches a Windows Remote Desktop session and automatically authenticates the user to the machine.
- **PuTTY:** Opens a PuTTY session and authenticates the user to a Unix system.
- **Web Password Filler:** Uses a bookmarklet or a Chrome extension to automatically log the user into a website with secret credentials. See our separate documentation for Web Password Filler.
- **Web Launcher:** An alternative method to automatically log on websites. See [Web Launcher](#).

See [Secret Launchers](#) for more information.

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session recording works for any launcher, including PuTTY and SSH, Windows Remote Desktop, Microsoft SQL Management Studio, and custom executables. The resulting movie is viewable from the secret audit. There are two types of session recording:

- [Basic Session Recording](#)
- [Advanced Session Recording](#)

You can access SS without using the user interface for automation and integration purposes. Currently, there are two APIs:

- An asynchronous REST (representational state transfer) API for Web services, which is based on JSON (JavaScript Object Notation). This is the preferred method. It is faster and easier to read than the SOAP API and is still actively updated.
- A synchronous SOAP (Simple Object Access Protocol) for Web services, which is based on XML. This method is deprecated, but we still support it. It is based on an older technology, which has largely been replaced in recent years. There will be no enhancements to this API. There are, however, a few, rarely used capabilities that only our SOAP API has.

We offer a software development kit (SDK) that contains a .NET framework and a command line interface (CLI) for accessing the REST API with Windows applications or scripting languages.

Both APIs, the .NET framework, and the CLI support:

- GET Requests: Retrieve information from SS, including entire secrets, individual secret fields, and security tokens
- POST Requests: Create SS data
- PUT Requests: Update SS data
- DELETE Requests: Remove SS data
- Once-per-session permissions (tested once and then based on the IP address), administered with a SS rule

SDK Documentation:

- [Secret Server SDK Guide](#): Includes these topics:
  - SS configuration
  - Roles and permissions
  - SDK client installation
  - Connecting to SS
  - SDK client caching
  - Examples
- [Secret Server SDK Downloads](#): Includes these topics:
  - SDK downloads
  - Download
  - SDK release notes
  - NuGet packages
- [SDK Integration Document](#): Includes these topics:
  - Integrating using C#
  - Integrating using the web.config file
  - Methods of the SecretServerClient() class

REST API Documentation:

- [REST Web Services API - Secret Server](#): Links to online reference guides (by SS release)
- [REST API PowerShell Scripts - Getting Started](#)
- [REST API Perl Examples](#)
- [REST API Java Examples](#): Downloadable Zip file

SOAP API Documentation:

- [SOAP Web Services API - Secret Server](#): Reference guide in a downloadable PDF
- [Using Web Services with SOAP and JavaScript](#)

- [SOAP-based Web services API - Getting Started](#)

You have finished this "Getting Started" introduction to SS. There is much more to explore within SS, such as scripting, third-party Integrations (SIEM, CRM, HSM, and more), and connecting to Privilege Manager to monitor and protect endpoints. We look forward to working with you!

See [Additional Resources](#) to learn more about SS and other Thycotic products.

## Help

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Capitalization

Technical writing is typically so awash in capitalization that it often denotes nothing and harms legibility. To counter that, in general, this document follows the IBM Style Guide rule:

*"Do not capitalize the names of features and components unless they are sold separately or are trademarked."*

More specifically, the only things capitalized in this document are:

- Company, person, country, geographic place, or organization names
- Official or trademarked products or services, unless they officially have atypical capitalization, for instance *iPod*.
- Acronyms and initializations
- When referring to any UI labels that are capitalized
- When the word begins a sentence or phrase

## Code and Command Line Text

Variable text in literal typed-in text and command-line parameters follow these industry-wide standards:

- All code and command-line interface text appears in monospaced text.
- Required parameters appear in angle brackets: `ping <hostname>`
- Optional parameters appear in square brackets: `mkdir [-p] <dirname>`
- Repeated parameters are followed by ellipses: `cp <source1> [source2...] <dest>`
- Multiple choice items are separated by vertical bars and grouped by curly brackets: `netstat {-tl-u}`

## Keyboard Shortcuts

- Keyboard keys are bolded and surrounded with square brackets: **[Enter]**
- Concurrent key presses are denoted with plus signs: **[Ctrl]+[Alt]+[Del]**
- Sequential key presses are denoted by commas: **[Page Down], [Enter]**

## Notes

There are three types of notes: *regular*, *important* and *warning*.

**Note:** Regular notes have a title, either "Note" or something custom, which appears as a phrase followed by a colon at the beginning of the note. A note contains tangential (an aside) or supplemental information (a tip or clarification).

**Important:** Important notes contain substantive information that should be heeded, or negative consequences can occur, involving frustration, wasted time, or minor data loss.

**Warning:** Warning notes contain substantive information that should be heeded, or negative consequences can occur, involving injury, major data loss, or equipment damage.

## Other Special Text

- Email addresses and URLs are usually denoted by a colored underline: [support@thycotic.com](mailto:support@thycotic.com).
- When URLs are part of the instruction, as opposed to clickable link, they appear in monospaced text: Type `https://www.somewhere.com` Or click <https://www.somewhere.com>.
- Cross-references to headings are hyperlinks: See [\[Booting a Server\]](#)[].
- Document or article names (not sections) appear in italics: See the *Server Administration Guide*. They may or may not be hyperlinks.
- All file and folder paths appear in monospaced text: `app\bin\web_config.xml`

- File names by themselves do *not* appear in monospaced text: web\_config.xml. If the file name contains spaces, the name is surrounded by quotation marks: "web config.xml".

**Note:** Ending punctuation may be omitted for clarity when following typed-in text, including URLs.

## Screen Components and Attentional Targets

- Mouse-click, keyboard, and other attentional targets (anything a looks for) are denoted by bold type: **OK** button or **Login** link.
- Attentional Targets and screen component names in system *responses* are not bolded: "The OK button appears" verses "Click the **OK** button."
- Names of screen components, such as tabs, buttons, and text boxes, are corrected for spelling and capitalization. The component type appears in lowercase. Example: **SEARVER CONFIGURATION** window becomes **Server Configuration** window.

**Table:** Terms and Definitions

2FA	<i>Two-Factor Authentication</i>
AD	<i>Active Directory</i>
Administrator	<i>Administrator</i> is a default role that comes preconfigured with SS. Roles control access to features within SS. This role can be customized to have different permissions. In this guide, administrator (lowercase) is used when referring to users who manage the system and have control over global security and configuration settings. Note that administrators in SS do not automatically have access to all data stored in the system—access to data is still controlled by explicit permissions on that data.
AES	<i>Advanced Encryption Standard</i>
API	<i>Application Programming Interface</i>
ASCII	<i>American Standard Code for Information Interchange</i>
ASP	<i>Advanced Server Pages</i>
AWS	<i>Amazon Web Services</i>
CAC	<i>Common Access Card</i>
CEF	<i>Common Event Format</i>
CHG	<i>Change</i>
CIDR	<i>Classless Inter-Domain Routing</i>
CRM	<i>Customer Relationship Management</i>
CSV	<i>Comma-Separated Values</i>
DBA	<i>Database Administrator</i>
DE	Distributed Engine (Secret Server)
DES	<i>Data Encryption Standard</i>
DPAPI	<i>Data Protection Application Programming Interface</i>
DSS	<i>Data Security Standard</i>
EC2	<i>Elastic Compute Cloud</i>
ESX	<i>Elastic Sky X</i>

FIPS	<i>Federal Information Processing Standard</i>
FQDN	<i>Fully Qualified Domain Name</i>
GDPR	<i>General Data Protection Regulation</i>
HSM	<i>Hardware Security Module</i>
HSTS	<i>HTTP Strict Transport Security</i>
IAM	<i>Identity and Access Management</i>
IIS	<i>Internet Information Services</i>
IP	<i>Internet Protocol</i>
ITSM	<i>Information Technology Service Management</i>
KB	<i>Kilobyte or Knowledge Base</i>
KBA	<i>Knowledge Base Article</i>
LDAP	<i>Lightweight Directory Access Protocol</i>
NAT	<i>Network Address Translation</i>
NATO	<i>North Atlantic Treaty Organization</i>
NIST	<i>National Institute of Standards and Technology</i>
NSA	<i>National Security Agency</i>
NTLM	<i>NT LAN Manager</i>
OATH	<i>Open Authentication</i>
OS	<i>Operating System</i>
OTP	<i>One-Time Password</i>
OU	<i>Organizational Unit</i>
PCI	<i>Payment Card Industry</i>
PDF	<i>Portable Document Format</i>
PII	<i>Personally Identifiable Information</i>
PIV	<i>Personal Identity Verification</i>

PuTTY	<i>Popular SSH and Telnet Client</i>
QR	<i>Quick Response (code)</i>
RADIUS	<i>Remote Authentication Dial-In User Service</i>
RBAC	<i>Role-Based Access Control</i>
RBS	<i>Role-Based-Security</i>
RD	<i>Remote Desktop</i>
RDP	<i>Remote Desktop Protocol</i>
Remote Password Changing	SS can automatically change passwords on remote devices and various platforms, including the following: Windows accounts, database logins, Active Directory accounts, Unix and Unix-like accounts (including root passwords), network appliances or devices and more.
REST	<i>Representational State Transfer</i>
Role-based Security	SS uses role-based access control, which provides the ability to set strict, granular permissions for each user. All features in SS are available to users based on permissions, which collectively make up roles.
RPC	<i>See Remote Password Changing</i>
SAML	<i>Security Assertions Markup Language</i>
SEC	<i>Security and Exchange Commission</i>
Secret	A piece of information that is stored and managed within SS is referred to as a secret. Secrets are derived from secret templates. Typical secrets include, but are not limited to, privileged passwords on routers, servers, applications, and devices. Files can also be stored in secrets, allowing for storage of private key files, SSL certificates, license keys, network documentation, Microsoft Word or Excel documents and more.
Secret Template	Secret templates are used to create secrets and allow customization of the format and content of secrets to meet company needs and standards. Examples include: local administrator account, SQL Server account, Oracle account, credit card and Web password. Templates can contain passwords, usernames, notes, uploaded files, and drop-down list values. New secret templates can be created, and all existing templates can be modified.
SHA1	<i>Secure Hashing Algorithm 1</i>
SIEM	<i>Security Information Event Management</i>
SMS	<i>Short Message Service</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SOAP	<i>Simple Object Access Protocol</i>
SP	<i>Service Pack</i>

SQL	<i>Structured Query Language</i>
SS	<i>Secret Server</i>
SSH	<i>Secure SHell</i>
SSL	<i>Secure Socket Layer</i>
TCP	<i>Transmission Control Protocol</i>
TOTP	<i>Time-Based One-Time Password</i>
UDP	<i>User Datagram Protocol</i>
UI	<i>User Interface</i>
UNC	<i>Universal Naming Convention</i>
Unlimited Administration Mode	An emergency, break-the-glass mode that gives administrators access to all content within the system, regardless of explicit permissions. Access to unlimited administration mode is controlled using role permissions.
URL	<i>Uniform Resource Locator</i>
VM	<i>Virtual Machine</i>
VPN	<i>Virtual Private Network</i>
WS	<i>Web Services</i>
XML	<i>eXtensible Markup Language</i>

## Forums

[Forums](#). Forums are oriented toward admins and other technical users.

## Thycotic Blog

[Thycotic Blog](#)

To have access to Thycotic Technical Support, you must have an equal number of unexpired user and support licenses. All support licenses expire 365 days after they are issued.

## Technical Support Coverage

Please see our [Technical Support](#) section.

**Note:** Please see our [Support Services Guide](#) for details about our support policy. The link above is a high-level summary of portions of that guide.

## Accessing Upgrades

Supported customers have access to all new releases (both minor and major). See [Secret Server Installation and Upgrade Guides](#).

## Requesting New Features

We encourage customers with active support licensing to participate on [feedback.thycotic.com](https://feedback.thycotic.com) where you can discuss and vote on new features.

## Access Requests

The access request feature allows a secret to require approval prior to accessing the secret. Note the following:

- Establishing a workflow model, the user must request access from the approval group or groups.
- An email is sent to everyone in the approval groups, notifying them of the request.
- The request can be approved or denied by any members of the approval groups.
- Access is granted for a set time period.
- If **Owners and Approvers also Require Approval** is enabled, then even owners or those in an approval group needs to request access.

Once a request for access to a secret has been made, approvers receive an email.

The email contains one link to the secret **Access Request Approval** page for that request in SS, and five additional links to approve or deny the request if the **Allow Approval for Access from Email** configuration setting is enabled.

The approver can either click one of the links contained in the email or navigate to the **Notification Center** in the user menu within SS.

Alert Notification Center



FILTER

Notification Type

☒ Event Subscription
 ☒ Secret Access Requests
 ☒ Application Access Requests
 ☒ System Alerts
 ☐ Include Archived

Priority

☒ Requires Interaction
 ☒ Critical
 ☒ Informational

PRIORITY	NAME	DESCRIPTION
	 Pending Engine	

If choosing the latter, in the displayed grid click the access request name. This takes you to the secret's Access Request Approval page.

From here, you can accept or deny the request as well as set an expiration date.

The requestor has access to the secret until the specified date.

Selecting the current date is the smallest window of time allowed and grants access to the end of the day.

With **Allow Approval for Access from Email** enabled, clicking one of the five additional links in the email allows access for 1, 2, 4, or 8 hours or deny the request, per the link description in the email.

**Note:** The expiration date referred to in approval requests is **not** the same as secret expiration.

Users can now approve secret access requests and workflows using Duo push notifications. The push notification includes information, displayed on the user's screen, that helps the approver make the access decision.

## Prerequisites

To use Duo push notifications:

- Duo must set up for SS. See [Duo Security Authentication](#).
- Duo user must be set up for Duo two-factor authentication. See [Setting up Duo \(User\)](#).
- The permission "Approve via DUO" must be granted to a role that is assigned to a group that includes all who will be approving requests via Duo. This allows enough flexibility so that those not wanting Duo push approvals can be configured to not receive them.

## Assigning the Duo Approval Permission

To associate the permission with users:

1. Go to **Admin > Roles**.
2. Click the **Create New** button to create a new role. Name it "Duo Push Approver" or another name of your choosing.
3. Assign the **Approve Via DUO Push** permission to the new role.
4. Click the **Save** button.
5. If you choose to create a separate group for approvers, do this by navigating to **Admin > Groups**.
6. Click the **Create New** button to create a new group.
7. Add the desired users (chosen approvers) to that group.

**Note:** You can also assign users to the group later. This method is a shortcut when creating a group.

8. Click the **Save** button.
9. Go to **Admin > Roles**.
10. Click the **Assign Roles** button. The View Role Assignment page appears.
11. Click the **Role** dropdown list to select the role you created. Note that there are no groups or users.
12. Click the **Edit** button. The Role Assignment page appears.
13. Assign the **Approve via DUO Push** role to the **Assigned** list box.
14. Click the **Save Changes** button. Setup is now complete.

**Note:** In addition to having the role you created, the user must be properly set up to receive Duo push notifications. See [Setting up Duo \(User\)](#).

**Note:** Any notifications will all be sent out at the same time, and the first response (approve or deny) will be the determinant response. A non-response will not result in either an approve or deny response.

To start the request process for access to a secret, the user must simply attempt to view the secret. The user is then sent to the Request page. In there, the user can explain the reason for the request and then click **Request Access** to submit the request.

If a member of the Approval Group either approves or denies the request (see below for details), the requestor is sent an email with the details. If approved, the requestor can access the secret via the link contained in the email.

To enable Access Request for a secret, navigate to the **Secret View** page for the secret:

1. Go into the **Security** tab and click the **Edit** button.
2. Check the **Enable Requires Approval for Access** checkbox to enable the setting.
3. Once enabled, select users or groups as approvers for the secret. Unless the **Owners and Approvers also Require Approval** option is turned on, owners or users that are members of the Approvers group do not need to request access to view the secret.

**Note:** Users need at least view access to the secret to be able to access the secret even with **Access Request** enabled. If the users do not have view permission they are unable to find the secret with search or browse.

**Note:** The email configuration settings need setting up, including valid email addresses, for the users in the approval group for emailing to work.

## Secret Server Administration

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS is highly customizable. Administrators can increase site security through various configuration settings such as force inactivity timeouts and specifying a SMTP server. This level of configuration allows SS to be altered to meet the needed requirements for the instance. The settings are explained in this section.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server stores information about what users did what activities within the application. This section discusses how to administer these audits.

## Audit Data Retention

### In This Section

- [Overview](#)
- [Data Retention Policies](#)
- [Permissions](#)
- [Procedures](#)
  - [Viewing the Status and History of Audit-Data Retention Policies](#)
  - [Editing Audit Data Policies](#)
  - [Running an Old Audit-Data Purge Right Now](#)

### Overview

Secret Server can automatically delete older audit and audit-like information (both are called "audit data" here). By default, SS does not delete any audit data.

**Important:** Do not configure automatic record deletion for compliance or other important data.

If enabled, old data deletion occurs automatically at 0200 EST every Sunday. Data deletion can be run immediately by clicking the "Run Now" button. The maximum record age for each audit-data retention policy is configurable to any value greater than or equal to 30 days.

### Data Retention Policies

The audit data retention offers two data retention policies:

- Personally Identifiable Information (PII): Tables containing identifiable user or organization data.
- Database Size Management: Tables that are prone to grow large, which may affect SS performance.

Each policy has a title and description, which are displayed to users, as well as a defined set of SS audit tables it manages. There is some overlap between the two policies' table sets as some tables fall under both PII and size management.

When an audit-data retention policy runs, all records in each table for that policy that are older than the set maximum record age in days are deleted from the database. This also includes all dependent records in other tables that would otherwise prevent deletion.

### Permissions

Access to the audit-data retention management pages in SS is limited to users with the roles "View Data Retention" and "Administer Data Retention." As the names imply, only the latter role can manage audit data retention, such as editing and running now.

**Note:** The "Unlimited Admin" role does not include audit data retention management at this time.

By default, these two audit-data retention roles are not assigned to users. An admin must first assign the roles to users requiring access.

### Procedures

#### Viewing the Status and History of Audit-Data Retention Policies

1. Go to **Admin > Data Retention Management:**

Admin > Data Retention Management

Data Retention
Audit

Configure automatic permanent deletion of older audit information. By default Secret Server does not delete any audit information. Do not configure deletion of records that you need for compliance or other purposes.

The deletion of old data occurs automatically at 2 AM EST every Sunday and can be run immediately by clicking Run Now below.

### Personally Identifiable Information (PII)

Personally identifiable information is information such as email addresses and names that can be used to identify an individual.

This list details which data is managed by this policy.

- Event Subscription Audit
- Dual Control Audit
- Group Audit
- Secret Audit
- Folder Audit
- Secret Policy Audit
- Workflow Template Audit
- Event Audit
- User Audit
- Admin Log

Enabled	Yes	Run Now	Edit
Max Record Age	365 Days	Edit	
Last Start Time			
Last Complete Time			

The Personally Identifiable Information (PII) policy is displayed on the Data Retention tab. If you scroll down, you will see the Database Size policy:

### Database Size Management

These tables may grow very large over time, which can impact performance.

This list details which data is managed by this policy.

- Group Audit
- SDK Client Audit
- Secret Audit
- Event Audit
- User Audit
- Secret Log
- Secret Item Transition History
- Secret History
- User Secret Event

Enabled	No	Edit
Max Record Age		
Last Start Time		
Last Complete Time		

2. Notice that each policy lists:

- The enabled status (editable)
- The maximum age audits are allowed to remain (editable)

- The last time the policy ran
- The last time the policy finished running
- All the audit data tables that the policy covers

3. To view a list of previous "runs," click the **Audit** tab. You can also hover the mouse pointer over individual records to view details:

Admin > Data Retention Management

+

JC

Data Retention
Audit

9 Audits

DATE RECORDED	NAME	USER	ACTION	NOTES
11/12/2019 3:29 pm	Personally Identifia...	ThycoticSystem	Truncate Records	Removed 65 total re...
11/12/2019 3:29 pm	Personally Identifia...	ThycoticSystem	Truncat	Removed 65 total records Removed 1 records from [Event Subscription Audit] Removed 0 records from [Dual Control Audit] Removed 0 records from [Group Audit] Removed 17 records from [Secret Audit] Removed 5 records from [Folder Audit] Removed 3 records from [Secret Policy Audit] Removed 0 records from [Workflow Template Audit] Removed 6 records from [Event Audit] Removed 8 records from [User Audit] Removed 13 records from [Admin Log] Removed 0 records from [Access Request] Removed 0 records from [Access Response] Removed 12 records from [Secret Access Request]
11/12/2019 3:29 pm	Personally Identifia...	Jonathan Cogley	Truncat	
11/12/2019 3:28 pm	Personally Identifia...	Jonathan Cogley	Edit	
11/12/2019 3:05 pm	Personally Identifia...	Jonathan Cogley	Edit	
11/12/2019 3:05 pm	Personally Identifia...	Jonathan Cogley	Edit	
11/2/2019 2:27 pm	Personally Identifia...	ThycoticSystem	Truncat	
11/2/2019 2:27 pm	Personally Identifia...	ThycoticSystem	Truncat	
11/2/2019 2:27 pm	Personally Identifia...	Jonathan Cogley	Truncate Records	Process Requested

## Editing Audit Data Policies

1. Go to **Admin > Data Retention Management**:

Admin > Data Retention Management

JC

Data Retention
Audit

Configure automatic permanent deletion of older audit information. By default Secret Server does not delete any audit information. Do not configure deletion of records that you need for compliance or other purposes.

The deletion of old data occurs automatically at 2 AM EST every Sunday and can be run immediately by clicking Run Now below.

### Personally Identifiable Information (PII)

Personally identifiable information is information such as email addresses and names that can be used to identify an individual.

This list details which data is managed by this policy.

- Event Subscription Audit
- Dual Control Audit
- Group Audit
- Secret Audit
- Folder Audit
- Secret Policy Audit
- Workflow Template Audit
- Event Audit
- User Audit
- Admin Log

Enabled	Yes	Run Now	Edit
Max Record Age	365 Days		Edit
Last Start Time			
Last Complete Time			

- Click the **Edit** link on the **Enabled** row on the policy that you wish to edit. A popup appears (not shown).
- Click to select the **Enabled** check box.
- Click the **Save** button. The policy becomes enabled.
- Click the **Edit** link on the **Max Record Age** row on the policy that you wish to edit. A popup appears (not shown).
- Type the number of days you want to retain the data (at least 30) in the **Max Record Age** text box.
- Click the **Save** button. The maximum record age changes.

## Running an Old Audit-Data Purge Right Now

- Go to **Admin > Data Retention Management**:

Admin > Data Retention Management

+

JC

Data Retention
Audit

Configure automatic permanent deletion of older audit information. By default Secret Server does not delete any audit information. Do not configure deletion of records that you need for compliance or other purposes.

The deletion of old data occurs automatically at 2 AM EST every Sunday and can be run immediately by clicking Run Now below.

### Personally Identifiable Information (PII)

Personally identifiable information is information such as email addresses and names that can be used to identify an individual.

This list details which data is managed by this policy.

- Event Subscription Audit
- Dual Control Audit
- Group Audit
- Secret Audit
- Folder Audit
- Secret Policy Audit
- Workflow Template Audit
- Event Audit
- User Audit
- Admin Log

Enabled	Yes	Run Now	Edit
Max Record Age	365 Days	Edit	
Last Start Time			
Last Complete Time			

- Click the **Run Now** link on the **Enabled** row on the policy that you wish to edit. A popup appears (not shown).
- Click the **Run Now** button. The popup disappears and the policy is run now.

**Note:** If a policy is currently running and you click the Run Now button. It will not work, and a popup will tell you so. There is a built-in five-minute wait after a policy finishes before you can run it again.

- The **Last Start Time** row changes to the current time, and a progress indicator appears.
- When the run is complete, the **Last Complete Time** row changes to the current time.

## Giving Application Pools Event Log Access

### Overview

When the database becomes inaccessible, Secret Server will try to log errors to the Windows event log. By default, network service and standard service accounts will not have permissions to the event log. Permissions must be added to specific event log registry keys.

### Required Registry Permissions

The follow permissions are required for the identity configured on the SS application pool in IIS:

#### HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > EventLog

Applies to key and subkeys

- Read permissions:
  - Query Value
  - Enumerate Subkeys
  - Notify
  - Read Control
- Set Value permission
- Create Subkey permission

#### HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > EventLog > Security

Applies to key and subkeys

Read permissions:

- Query Value
- Enumerate Subkeys
- Notify
- Read Control

### Applying Windows Event Log Permissions

1. Determine the account that is running SS:
  1. Log on SS.
  2. Go to **Admin > Diagnostics**.
  3. Look for any of the **Thread Identity** labels. These contain the identity of SS (often NT AUTHORITY\NETWORK SERVICE or IIS APPPOOL\SecretServer or the service account set up for IWA. See [Running the IIS Application Pool As a Service Account](#).

**Note:** You can also determine the identity by logging in and navigating to <http://yoursecretserverurl/Installer.aspx>. The first step of this page will tell you the application pool identity.

2. Open the Windows registry editor on the machine running SS (regedit at the command prompt or Window search text box).
3. On the left, navigate to **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > EventLog**.
4. Right click the **EventLog** folder in your registry editor and select **Permissions**. A permissions dialog box appears.

5. Click the **Advanced** button.
6. On the **Permissions** tab, Click the **Add** button. A Permission Entry dialog appears.
7. Click the **Select a principal** link. The Select User, Computer... dialog box appears.
8. Find the account running SS, such as Thycotic\_Service (svc\_thycotic@test.com).
9. Click the **OK** button. The dialog box closes.
10. In the **Basic Permissions** section of the **Permission Entry** dialog, click to select the **Read** check box.
11. Click the **Show advanced permissions** link. The pane switches.
12. Click to select the **Set Value** and **Create Subkey** check boxes in the **Advanced Permissions** section.
13. Click **OK** buttons on the remaining dialogs to apply the permissions. You are returned to the main registry editor window.
14. Navigate to **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > EventLog > Security**, right-click and select "**Permissions...**"
15. Right click **Security** folder and select **Permissions**. A permissions dialog box appears.
16. Click the **Add** button.
17. Find the account running SS.
18. Click the **OK** button.
19. Click to select the **Read** check box in the Allow column.
20. Click the **OK** button to apply the permission.

## Report Auditing

In addition to the user audit and individual secret audit, the reporting feature provides a series of activity, user, and secret reports. See [Built-in Reports](#) for the most up-to-date list of reports included.

**Note:** Users can also create their own, custom reports. See [Creating and Editing Reports](#).

## Secret Audit Log

The audit log for a secret can be accessed by clicking the **View Audit** button on the **Secret View** page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret.

**Note:** Audit logs are visible to anyone with the “list” permission. Thus, anybody with that permission can view permission changes, users whose permissions were changed, secret dependency information, and the machine.

Secret audits are taken for the following user actions:

- Adding, updating and removing secret dependencies
- Check out
- Editing permissions
- Forced expiration
- Hide launcher password changes
- Set for check-in
- Update
- View

For certain audit items, action notes are added providing additional details. For example, if permissions are edited, an audit record is generated detailing which users or groups gained or lost permissions. Detailed audit records add accountability to sensitive secrets where auditors or administrators need to know exactly what was modified.

Below the audit records is a **Display Password Change Log** check box. Clicking to select this check box displays logs for Heartbeat and Remote Password Changing amongst the audit items

## Viewing a User Audit Report

1. From the **Reports** page, click the **User Audit** tab.
2. From the dialog on the tab, select a user and a date range to view.
3. Click **Search History** to view the user's audit trail.

The audit search displays results for all the secrets the selected user has viewed or edited during the selected time period. The administrator has the option of expiring all the viewed secrets, to notify users to change sensitive information, or to force password changing (if the RPC is configured).

To get a full view of the actions taken on a secret, select that secret from the results list. The secret audit displays the specific user actions for a secret.

The Admin Page is a control panel for administering SS. You access it by clicking the Admin button on the dashboard menu and selecting See All from the list.

**Note:** The most commonly sought items appear in the same list, so you can go directly to them without having to go to the Admin page.

**Figure:** Admin Page (Simplified View)

What are you looking for?

Search for an admin option



[Simplified View](#) ▾



## Actions

Secret Server features that perform important jobs



## Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more



## Users, Roles, Access

These features help you organize users & permission settings within Secret Server



## Diagnostics, Logs, Security

Reference options for diagnostics, logs, and security features

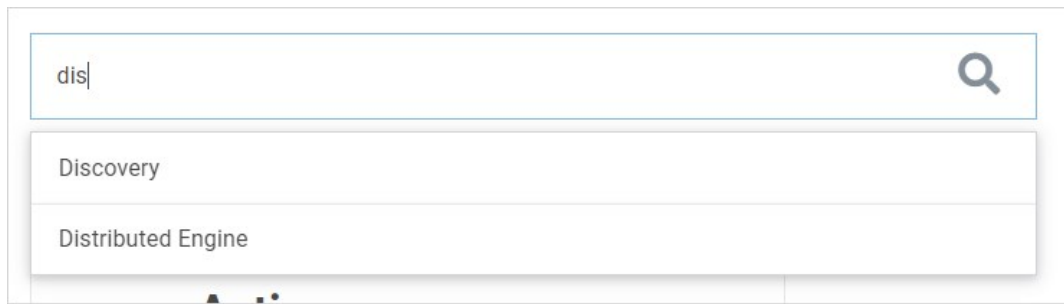


## Tools & Integrations

Find Secret Server tools and other product integrations here

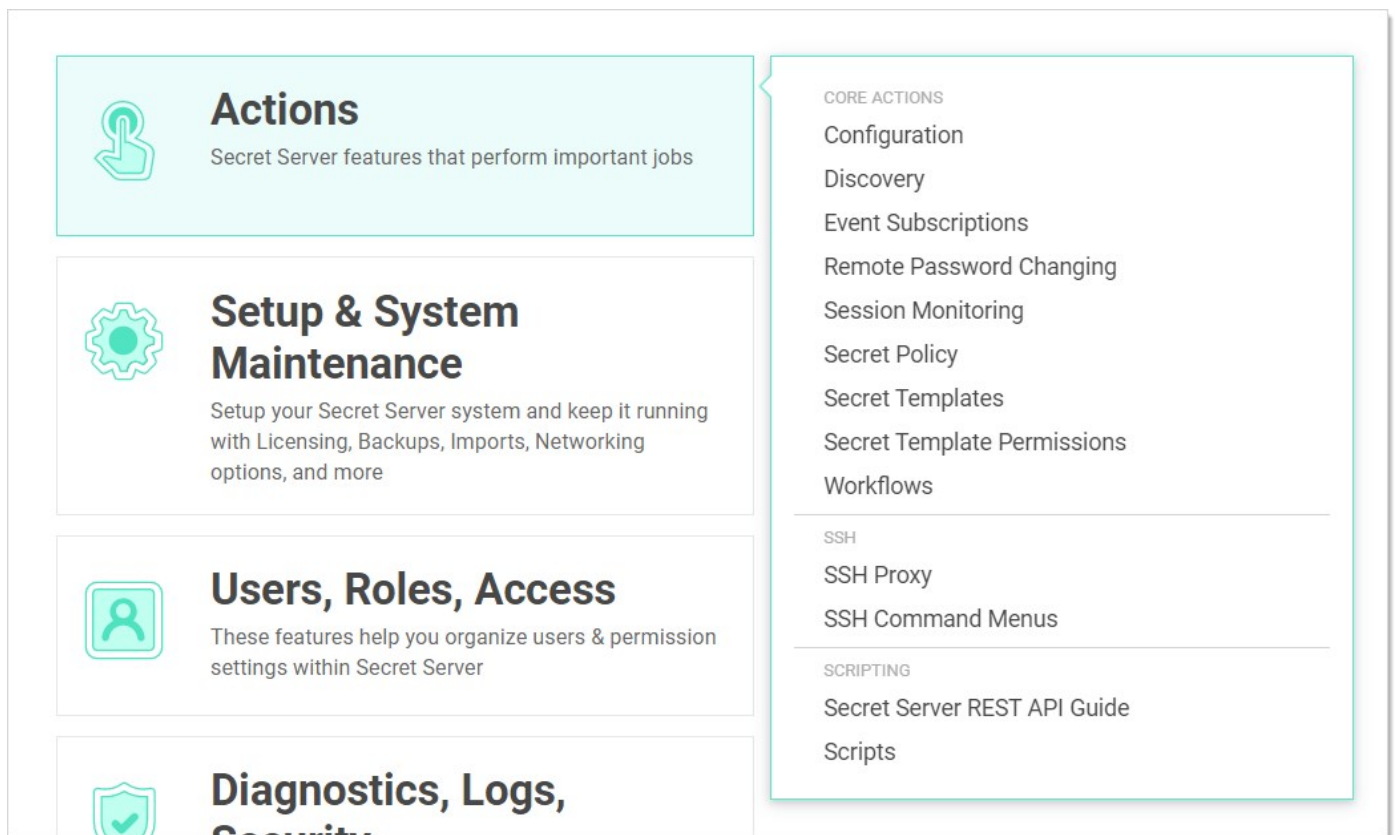
With it, you can quickly and easily find administration controls in several ways:

- **Text Search:** You can search for a concept, configuration, or component by typing a search term in the search text box. The text box automatically suggests items as you type:



Once you see the item you desire, you simply click and you are brought to that page.

- **Topic button:** You can click one of the large buttons to see a list of related items:



Once you see the item you desire, you simply click it, and you are brought to that page.

- **Views:** You have three views to choose from, which you set by clicking the view link. The link text states the current view. The views are:
  - Simplified View: The large, clickable buttons.
  - Alphabetized List: A text list of the available items:

## Admin

Active Directory	SDK Client Management
Backup	SSH Command Menus
Configuration	SSH Proxy
Connection Manager	Scripts
Database	Search Indexer
Dependency Templates	Secret Policy
Diagnostics	Secret Search Filters
Discovery	Secret Server REST API Guide
Distributed Engine	Secret Template Permissions
DoubleLock	Secret Templates
Dual Controls	Security Audit Log
Email	Security Hardening Report
Event Subscriptions	Server Nodes
Export	Session Monitoring
Folder Synchronization	System Log
Folders	Teams
Groups	Upgrade Secret Server
IP Addresses	Users
Import Secrets	Workflows
Internal Site Connector	
Launcher Tools	
Licenses	
Privilege Manager	
Privileged Behavior Analytics	
Remote Password Changing	
Roles	

- Category: A text list of the available items bunched by category:

CORE ACTIONS	SETUP & SYSTEM UPKEEP	USERS, ROLES, ACCESS MANAGEMENT
Configuration	Backup	Active Directory
Discovery	Database	Users
Dependency Templates	Email	Groups
Secret Search Filters	Licenses	Roles
Event Subscriptions	Search Indexer	Teams
Remote Password Changing	Upgrade Secret Server	IP Addresses
Session Monitoring		Folders
Secret Policy	IMPORT, EXPORT, SYNC	
Secret Templates	Import Secrets	
Secret Template Permissions	Export	
Workflows	Folder Synchronization	DIAGNOSTICS, LOGS, SECURITY
SSH	NETWORKING	Diagnostics
SSH Proxy	Distributed Engine	Security Hardening Report
SSH Command Menus	Server Nodes	System Log
	Internal Site Connector	Security Audit Log
SCRIPTING		DoubleLock
Secret Server REST API Guide		Dual Controls
Scripts	TOOLS & INTEGRATIONS	
	Launcher Tools	
	Connection Manager	
	SDK Client Management	
	Privilege Manager	
	Privileged Behavior Analytics	

**Note:** The [Security Hardening Guide](#) offers suggestion for many of the settings in this section.

## Email Tab

The Email tab contains the following configuration options:

- **Custom Port:** Optional custom port for the email server.
- **Domain:** The domain of the credentials to use (optional).
- **Email Server:** Specify the domain name or IP address of your SMTP server. For example: smtp.yourcompany.com.
- **From Email Address:** The return email address for SS emails.
- **Password:** Password for the email account
- **Use Credentials:** Whether to use credentials when sending emails. Requires username and password to be entered when enabled.
- **Use Custom Port:** Whether to use a custom port when sending emails. Requires a custom port to be specified when enabled.
- **Username:** Name for the email account.
- **Use Custom Port:** Whether or not to use a custom port on the email server.
- **Use SSL:** Whether to use SSL when sending emails.

## Folders Tab

The Folders tab contains the following configuration options:

- **Enable Personal Folders:** Each user has a personal folder created and assigned to them.
- **Personal Folder Name:** The name of the root personal folder. Each user's personal folder is named based on the user.
- **Require View Permission on Specific Folder for Visibility:** Users only see folders they have view permissions on.
- **Show user warning message:** Enable warning message for users when creating secrets.
- **Warning Message Text:** Warning message to display to the users, instructing them to store only work-related data in SS.

## General Tab

The following configuration settings are available in the General tab:

- **Allow Approval for Access from Email:** Adds links in request for approval emails allowing approvers to approve or deny access to a secret without logging into SS. See Requires Approval for Access for details.
- **Allow Automatic Checks for Software Updates:** Enable this option to be notified of a new SS release. If a new update is available, displayed at the top of each SS page is a link to the latest update. This feature is only available to those with support licenses.
- **Allow Duplicate Secret Names:** Allow users to create or rename secrets with the same name as existing secrets.
- **Allow Secret Server to Retrieve Website Content:** Enables the Web launcher to retrieve the Web site content in order to parse the form and find the login controls.
- **Allow Users to Select Classic Theme:** Enable access to the classic user interface.
- **Allow Users to Select Themes:** Allows users to customize the theme for SS. This selected theme would only apply to their login.
- **Allow View User To Retrieve Auto-Change Next Password:** Allow view-only users to get the next automatically changed password.
- **Allow Web Launcher Mappings to be Downloaded:** Enables a Web launcher configuration to download pre-approved website launcher settings from Thycotic.com.
- **Allow Web Launcher Mappings to be Uploaded Off-site:** Enables the user to upload successful Web launcher configurations to Thycotic.com where they are approved and shared with other customers.
- **Application Language:** The language that you want SS to default to.
- **Change Administration Mode:** Enables or disable a button that takes you to a page where you can enable or disable Unlimited

Administration mode.

- **Check in Secret on Launcher Close:** Enable if you want the related secret checked in when you close the launcher.
- **Click to Toggle Password Masking:** Enable or disable being able to remove password masking.
- **Close Launcher on Check in Secret:** Enable if you want the related launcher closed when you check in a secret.
- **Custom Logo (Collapsed):** Select an image to use as your collapsed logo.
- **Custom Logo (Full Size):** Select an image to use as your full-sized logo.
- **Default Date Format:** Default time format used for all users. This setting can be overridden by each user. See [User Preferences](#) for details.
- **Default New User Role:** Role to automatically apply to new users.
- **Default Theme:** Select the default SS theme users see.
- **Default Time Format:** Default date format used for all users. This setting can be overridden by each user. See [User Preferences](#) for details.
- **Default Secret Permissions:** Set to determine how permissions are propagated from folders to new secrets. See [Secret Folders](#) for more information.
- **Enable CredSSP Authentication for WinRM:** Allow credential delegation for PowerShell scripts that may need to access resources outside of the SS machine.
- **Enable Launcher:** Enables Remote Desktop Launcher capabilities for SS. See the Launcher section for details.
- **Enable New User Interface:** Enable access to the new SS user interface.
- **Enable New User Interface as Default for New Users:** Force new users to use the new, as opposed to the classic, user interface. Does not stop users from manually changing to the classic interface.
- **Enable Protocol Handler Auto-Update:** Enable if you want launchers to automatically update.
- **Enable Refresh Tokens for Webservices:** Whether or not to accept refresh tokens.
- **Enable Syslog/CEF Logging:** Allow SS to export logs to a SIEM tool server.
- **Enable Webservices:** Enable other applications to interact with SS (still requires them to login as a SS user).
- **Force Require Approval for Editors on Approval Secrets:** Do not let approvals to be disabled for editors for secrets requiring approvals.
- **Force Require Approval for Owners on Approval Secrets:** Do not let approvals to be disabled for owners for secrets requiring approvals.
- **Force Inactivity Timeout:** Time out a user's login after inactivity for the specified time interval. See [Configuring Users](#).
- **Force Password Masking:** For more information, see [Setting Up Password Masking](#).
- **Launcher Deployment Type:** Select either Protocol Handler (default) or ClickOnce.
- **Maximum Time for Offline Access on Mobile Devices:** Amount of time that a mobile device can be disconnected from the server before it removes cached SS data from the device.
- **Prevent Application from Sleeping When Idle:** Prevents the application pool that SS is running under from going to sleep.
- **Prevent Application from Sleeping When Idle:** Prevents the application pool that SS is running under from going to sleep.
- **Require Folder for Secrets:** Enable this setting to force users to select a folder to place a secret in when creating or moving a secret. See [Secret Folders](#) for more information.
- **Secret Password History:** Enforces whether a recent password can be set on a secret's password text-entry field based on the history. Defaults to 1, which means the same password cannot be immediately re-used on a secret.
- **Secret View Interval Minutes:** The number of minutes after which users must enter another comment when Require Comment is enabled.
- **Secret Server Custom URL:** A URL to use for SS, other than the default one.
- **Send Anonymized System Metrics to Thycotic:** Share anonymized data to help Thycotic improve SS.
- **Session Timeout for Webservices:** Set a session time limit on use of the Web services API. Once the Web services session token expires, the user must login again with their username and password.
- **Select Default Classic Theme:** Select the default color theme for the classic interface.
- **Time Zone:** Time zone that all dates are displayed in.
- **TMS Installation URL:** URL for the Thycotic Management Server. TMS is a term that refers to several products within the Privilege Manager toolkit.
- **UI Inactivity Timeout:** Time in minutes before SS times out from user inactivity.
- **WinRM Endpoint URL:** URL for WinRM, which is used for PowerShell hooks.

**Note:** No secret data is uploaded to Thycotic.com—only the website URL and control names are sent.

## HSM Tab

From the Hardware Security Module (HSM) tab, you can enable or disable HSM for encryption. For more details about HSM configuration, see our [HSM Integration Guide](#) (PDF).

## Local User Passwords Tab

This tab contains the following configuration options:

- **Allow Users to Reset Forgotten Passwords:** Allows users to reset their passwords in case they forget them.
- **Enable Local User Password Expiration:** Local user's passwords expire after a specified interval.
- **Enable Local User Password History:** Local users cannot change their password if it has been recently used.
- **Enable Minimum Local User Password Age:** Local users cannot change their passwords until the password meets a minimum age.
- **Local User Password is valid for:** Specifies the maximum time a local user can keep a password.
- **Lowercase Letters Required for Passwords:** Force all local users to include lowercase letters within their login passwords.
- **Minimum Password Length:** Require a minimum length on all local users' login passwords.
- **Numbers Required for Passwords:** Force all local users to include numbers within their login passwords.
- **Symbols Required for Passwords:** Force all local users to include special characters within their login passwords (%#@).
- **Uppercase Letters Required for Passwords:** Force all local users to include uppercase letters within their login passwords.
- **User Lockout Time:** Sets the time in minutes that users are locked out for too many failed log on attempts.

## Login Tab

The Login tab contains the following options:

- **Allow AutoComplete:** AutoComplete is a feature provided by most Web browsers to automatically remember and prefill forms for you. This can be a great security concern since they typically do not save the data in a secure manner. You can enable or disable Web browser prefill on the Login page by using this option.
- **Allow Remember Me:** This option enables the Remember Me checkbox on the login page. When a user chooses to use "remember me," an encrypted cookie is set in their browser. This enables users to revisit SS without the need to login. This cookie is no longer be valid when the "remember me" period has expired, and users have to log in again.
- **Allow Two-Factor Remember Me:** Allow users to elect to remember them on SS with two-factor authentication enabled. See "Allow Remember Me."
- **API Hostname:** Duo API host.
- **Attempt User Password:** SS normally passes the domain, username, and password to the RADIUS server. This setting ensures the user is asked for their password instead.
- **Cache AD Credentials for When Engines Are Offline:** Store Active Directory credentials in a local encrypted location.
- **Default Login Domain:** Allows for the selection of a default domain for user login.
- **Disable Radius NAS-IP-Address Attribute:** enabled, prevents NAS-Identifier from being sent with RADIUS requests.
- **Enable Domain Selector:** All users to select a domain at login.
- **Enable Duo Integration:** Enabling Duo integration allows users to use Duo two-factor authentication.
- **Enable Login Failure CAPTCHA:** Enforces a CAPTCHA image if the user fails one or more logins to prevent brute force attacks of user credentials or brute force lockouts.
- **Enable OpenID Connect Integration:** Enable OpenID Connect.
- **Enable RADIUS Integration:** Enabling RADIUS integration enables another form of two factor authentication for users.
- **Enable RADIUS NAS-Identifier:** When enabled, sends NAS-Identifier with RADIUS requests.
- **Enable SAML Integration:** Enabling SAML integration allows users to log-in to SS using your SAML identity provider.
- **Integration Key:** Duo integration key.
- **Maximum Concurrent Logins per User:** The number of times a user can be logged in at the same time.
- **Maximum Login Failures:** Set the number of login attempts allowed before a user is locked out of their account. Once locked out,

they need a SS administrator to reset their password and enable their account.

- **RADIUS Client Port Range:** Allowed computer ports for RADIUS.
- **RADIUS Login Explanation:** Text that appears, explaining the RADIUS login.
- **RADIUS Default Username:** The default username that appears at RADIUS login.
- **RADIUS Server Port:** The default RADIUS port.
- **Require Two Factor for these Login Types:** When enabled on a specific user logging into SS, you can choose from a list to enable it for website, Web service, or both.
- **Time Out (seconds):** RADIUS timeout in minutes.
- **Use RADIUS Username for Duo:** Pass the RADIUS username to Duo.
- **Visual Encrypted Keyboard Enabled:** Enables or disables the visual encrypted keyboard for logins.
- **Visual Encrypted Keyboard Required:** Require the visual keyboard for logins.

## Security Tab

The Security tab contains the following configuration options:

- **Additional Certificate Chain Policy Options:** Valid values for certificate chain policy options are any of the values in the Microsoft enumerations [listed here](#).
- **Allow HTTP Get:** Allows the HTTP Get verb for Web services. This allows REST-style calls to many Web service methods but reduces security.
- **Apply TLS Certificate Chain Policy and Error Auditing:** Add audits for TLS certificate validation. Auditing will apply to all Active Directory domains using LDAPS and Syslog using TLS. The default policy is very strict.
- **Enable Database Integrity Monitoring:** Database Integrity Monitoring is a SS tool for detecting changes made to primary database tables outside SS's user interface. It sends e-mails to configured addresses when it detects database changes made outside of SS.
- **Enable FIPS Compliance:** See [FIPS Compliance](#).
- **Enable File Restrictions:** Allow administrators to configure what kind of file attachments can be uploaded to secrets. This helps protect users from being tricked into downloading a malicious secret attachment. The file extension can be specified, such as: \*.7z, \*.bmp, \*.ca-bundle, \*.cer, \*.config, \*.crt, \*.csr, \*.csv, \*.dat, \*.doc, \*.docx, \*.gif, \*.gz, \*.id-rsa, \*.jpeg, \*.jpg, \*.json, \*.key, \*.lic, \*.p7b, \*.pcf, \*.pdf
- **Enable Frame Blocking:** Allow SS to be opened in an <iframe> HTML tag on another, potentially malicious, site.
- **Enable HSTS:** Enable HTTP Strict Transport Security. Not available if Force HTTPS/SSL is turned off.
- **Enable TLS Debugging and Connection Tracking:** When enabled, SS sends information logs to your audit server about when TLS connections are opened or closed.
- **Encrypt Key using DPAPI:** This encrypts the SS AES 256 key using the machine key. It provides protection from admins copying SS from the server to their own machine. Note that a backup of the encryption key should be made before using this option. Otherwise, disaster recovery is impossible if the server dies. After encrypting the key, an administrator of SS can decrypt it.
- **Force HTTPS/SSL:** Require HTTPS; users cannot access SS using HTTP.
- **Frame Blocking:** Prevents users from accessing the SS site if it is embedded in an iFrame.
- **Hide Secret Server Version Numbers:** Hide SS version numbers from users.
- **Ignore Certificate Revocation Failures:** Ignore certificate revocation failures for syslog using TLS.
- **Last Secret Key Rotation:** When the last rotation occurred.
- **Last Secret Key Rotation Status:** What was the result when the last rotation occurred.
- **Rotate Secret Keys (button):** Key rotation is the process by which the encryption key, used for securing Secret data, is changed and Secret data is re-encrypted.

## SAML Tab

See [SAML 2.0 Configuration Guide](#).

## Session Recording Tab

See [Session Recording](#).

## **Ticket System Tab**

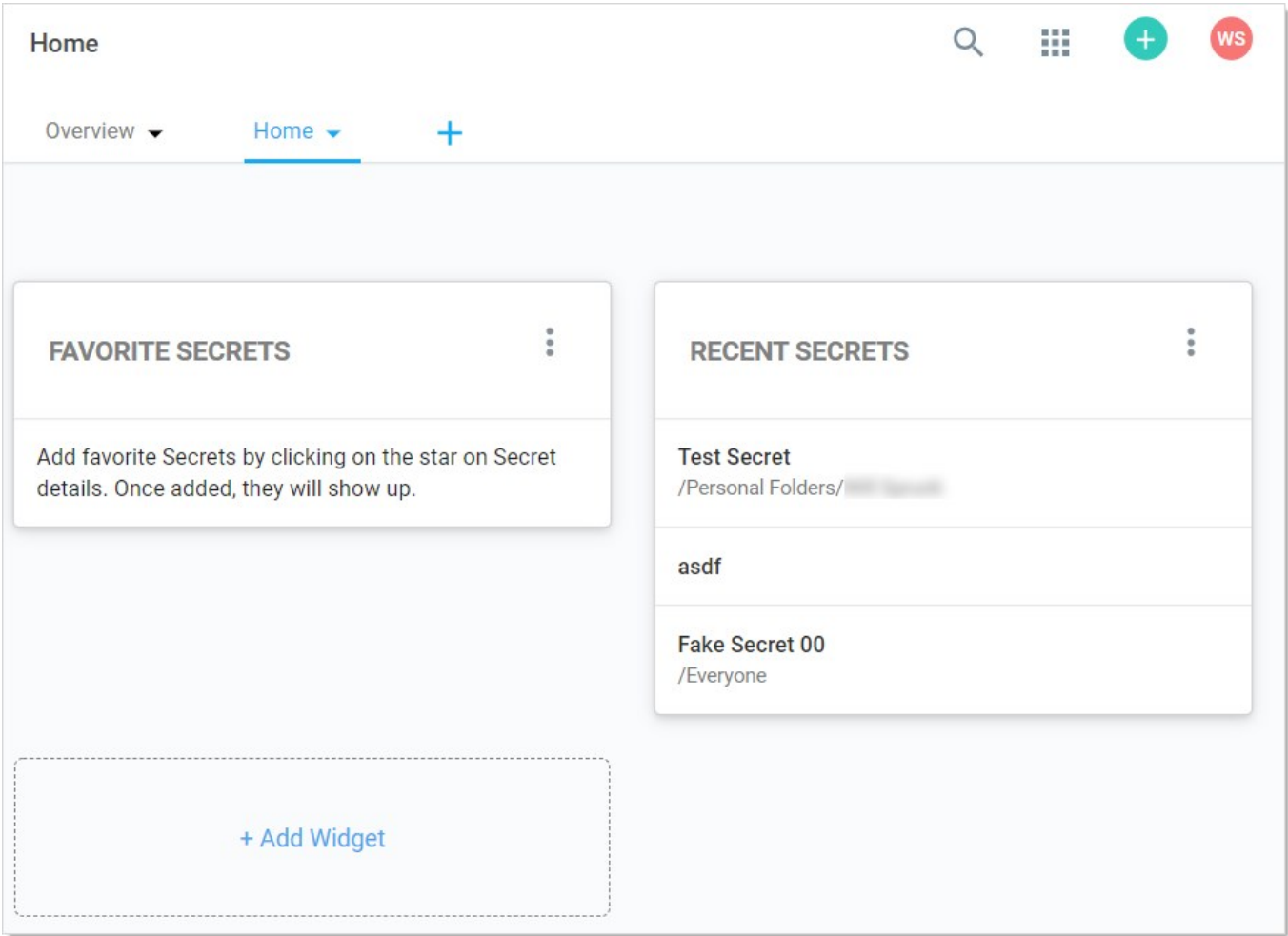
See [Ticketing System Integration](#).

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

The SS dashboard is the main page for searching and viewing secrets.

Dashboard Components

Home Tab



By default, it contains the Favorite Secrets, Recent Secrets, and + Add Widget widgets (function boxes) . You can add these widgets:

- Expired Secrets
- Out-of-Sync Secrets
- Reports
- Request Management

Dashboard Widgets

Widget Types

Table: Dashboard Widgets

Expired Secrets	Displays expired secrets.
-----------------	---------------------------

Favorite Secrets	Displays secrets marked as favorites.
Out-of-Sync Secrets	Displays secrets that are out-of-sync—the heartbeat or RPC have failed.
Recent Secrets	Displays the secrets viewed most recently.
Reports	Displays a report. Click the <b>Report Category</b> list to select a report from the drop-down menu. One report can be displayed per widget. Click the title of the report to navigate to the Report View page.
Request Management	Displays any requests pending for the logged in user.
+ Add Widget	When clicked, adds a widget that is not currently displayed to the Dashboard. This widget's function is duplicated automatically when you add a new Dashboard tab. You cannot remove this widget.

**Note:** The Search and Browse widgets cannot be rearranged. They always remain in the top left region of the tab.

## Managing Widgets

The following operations are available (by clicking the  icon) for managing widgets:

- **Delete:** Hide the widget.
- **Refresh:** Update the information in the widget. This is not available for all widgets.

## Overview Tab



The Overview tab provides several widgets for getting a quick understanding of your SS installation:

- **Active Monitoring Sessions:** Your current monitored sessions. See [Session Recording](#).
- **Approvals:** Your current in-process approvals. See [Secret Access Requests](#).
- **Heartbeat Status:** A graphic of the current status of your heartbeats: success, pending, or failed. When you click on one of the statuses, you are brought to a report page for that status. For example, **Reports > Secrets Failing Heartbeat**. When you click the **Current** link, you are brought to the **Reports > Heartbeat Status by Day** page. See [Secret Heartbeats](#).
- **Most Used Secrets:** A table of the most recently accessed secrets, listed by date and folder.
- **Password Rotation:** The state of your current password rotations. When you click the **Today** link you are brought to the **Reports > RPC by Day** report page. See [Remote Password Changing](#).

**Note:** To see an overview of incoming system and subscription alerts, see the [Alert Notification Center \(Inbox\)](#).

## Customized Tabs

The following operations are available for creating custom tabs:

- **Create:** Click the **+** to the right of the tabs to create a new empty tab.
- **Delete:** Click the  icon on a tab and select **Delete** to delete a tab. You can cancel changes by clicking the **Cancel** button. A confirmation pop up page appears.
- **Rename:** Click the  icon on a tab and select **Rename** to change the tab name. You can cancel changes by clicking the **Cancel** button.
- **Reorder:** Click and drag a tab to the left or right of an existing tab.

## Dashboard Tools and Help Menu

The Dashboard Tools Menu is available via the  button on the Dashboard. It includes links to:

### Tool Section

- Connection Manager
- Importing Secrets
- Exporting Secrets
- Manage Secret Access Request
- Launcher Tools
- Privilege Manager
- Privilege Behavior Analytics

### Help Section

- About
- Help
- Secret Server REST API Guide
- User Guide

## Themes

### Overview

By default, SS is set to a default theme unless specified within the Configuration settings. SS comes with three other bundled themes: Blue, Dark, and Green. The default theme can be set at **Administration > Configuration** on the general tab. Theming differences can be allowed by individual users with the **Allow User to Select Themes** permission.

### Choosing Themes

1. Click your user icon in the top right of the dashboard and select **Account Settings**.
2. Ensure the **General** tab is selected.
3. Click the **Edit** button.
4. Click the **My Theme** dropdown list to select the theme. Your choices are:
  - Secret Server Classic - Blue
  - Secret Server Classic - Dark
  - Secret Server Classic - Default
  - Secret Server Classic - Gray
  - Secret Server Classic - Green
  - Secret Server (New)
5. Click the **Color Mode** dropdown list to select the color mode (default, light, or dark) when **My Theme** is set to **Secret Server (New)**.

**Note:** The color mode only applies to Secret Server (New). If you change it while in one of the classic themes, nothing seems to happen; however, when you switch to Secret Server (New), the color mode you chose applies.

## Running Dashboard Bulk Operations

You can perform bulk operations from the Dashboard on multiple secrets:

1. Click to select the secrets you wish to include. To check them all, check the check box in the column header row.
2. Click to select the bulk operation from the dropdown list below the list of secrets. Available bulk operations include:
  - Add share
  - Assign secret policy
  - Assign to site
  - Change password remotely
  - Change to inherit permissions
  - Convert secret template
  - Delete
  - Disable autochange
  - Disable check out
  - Disable comment on view
  - Disable heartbeat
  - Edit share
  - Enable autochange
  - Enable check out
  - Enable comment on view
  - Enable heartbeat
  - Hide launcher password
  - Move to folder
  - Run heartbeat
  - Set privileged account
  - Undelete
  - Unhide launcher password

**Note:** Bulk operations differ by SS version.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This section discusses built-in security features of the SS application, including encryption and compliance standards.

## Advanced Encryption Standard

SS uses different types of encryption to ensure data security. Every text-entry field, except name, on a secret is encrypted at the database level with the Advanced Encryption Standard (AES) 256-bit algorithm. Database encryption prevents unauthorized access of sensitive data on the server.

The AES encryption algorithm provides a high security level for sensitive data. The National Institute of Standards and Technology (NIST) and National Security Agency (NSA) search for a replacement for the Data Encryption Standard (DES), which had numerous issues, namely small key size and efficiency, and finally settled on AES.

**Note:** Encryption algorithms use keys to obfuscate the data. While DES only had a key size of 56 bits, AES can have a key size of 128, 192 or 256 bits. Larger keys provide more security as their size makes brute force attacks infeasible.

**Note:** To address concerns from the cryptographic community, NIST embarked on a transparent selection process. During the selection process NIST solicited designs from the global cryptographic community and voted for a winner from within fifteen finalists. The eventual winner was a team of Belgian cryptographers with their submission of the Rijndael encryption method, which became AES. For more information about the technical specifications of AES, please see the official standard.

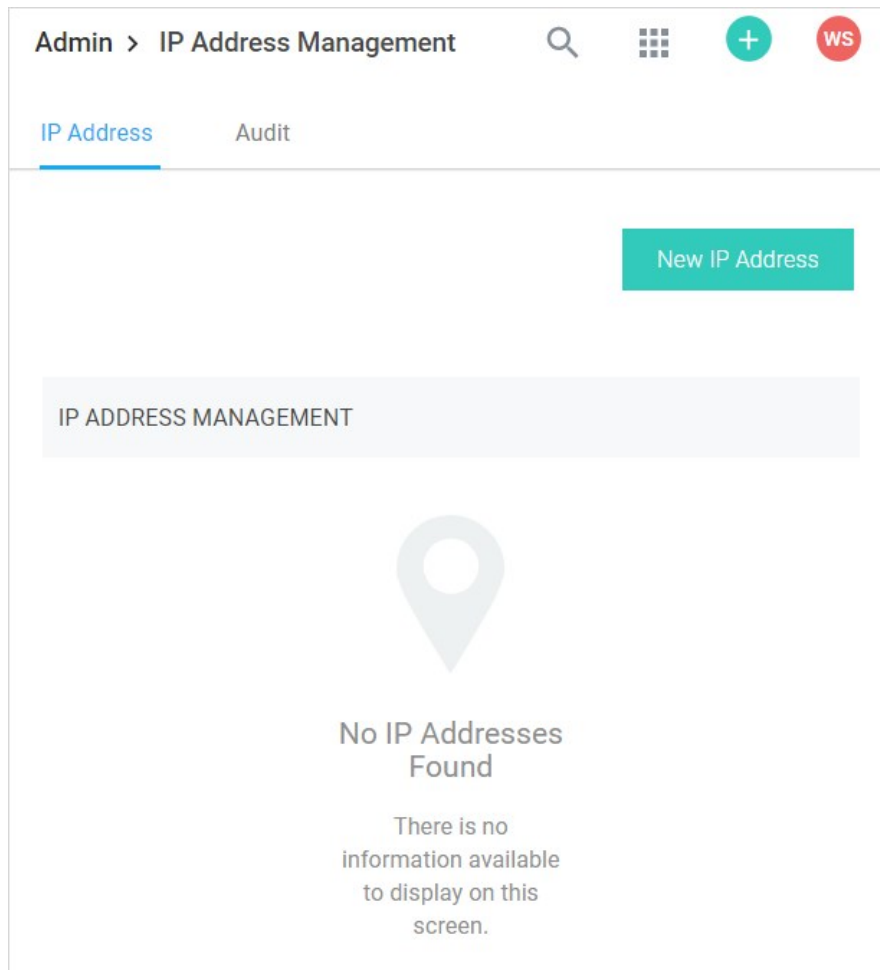
## Restricting IP Addresses

IP address restrictions allow you to control which IP address ranges users can use to log in to SS.

### Creating IP Address Ranges

To create an IP address range:

1. Go to **Admin > IP Addresses** under Administration. The IP Address Management page appears:



2. Click the **New IP Address** button. The Add New IP Address Range popup page appears:

### Add New IP Address Range

IP Address  
User/Network Name \*

IP Address Range \*

192.168.3.12  
192.168.42.147-192.168.42.194  
192.168.3.52/22

Cancel


Save

3. In the **IP Address User/Network Name** text box, type a descriptive name for your range.
4. In the **IP Address Range** text box, enter an IP Address or IP Address range. SS supports single IP Addresses (10.0.0.4), a range separated by a hyphen (10.0.0.1-10.0.0.255), and CIDR notation (10.0.0.0/24).
5. Click the **Save** button. The new address or range appears in the IP Address Management table:

New IP Address

IP ADDRESS MANAGEMENT

NAME	
IP ADDRESS RANGE	
Generic Internal	
192.168.1.1	<div>Edit Delete</div>

**Note:** You can show or hide columns in the table by clicking the  button.

## Editing and Deleting IP Address Ranges

To edit an IP address range, go to the **IP Address Management** page, click on a range, and click **Edit**. To delete a range, click on the range and click the **Delete** button.

## Assigning an IP Address Range

1. To assign a range to a user:
2. Go to **Admin > Users** page. The View User page appears:

### View User

User Name	wsprunk
Display Name	Will Sprunk
Email Address	
Domain	gamma.thycotic.com
Two Factor	< None >
Enabled	Yes
Locked Out	No
Application Account	No

#### IP Address Restrictions

None


#### Restricted By Team


No

1. Scroll to the bottom of the page and click the **Change IP Restrictions** button. The Edit IP Address Restrictions Page appears:

### Edit IP Address Restrictions

RESTRICTED	NAME	IP ADDRESS RANGE
<input type="checkbox"/>	Generic Internal	192.168.1.1

 Save

 Cancel

1. Click to select or deselect check boxes next to the ranges to choose which IP Addresses a user can use to access SS. If no boxes are checked, the user can access SS through any IP Address.
2. Click the **Save** button.

**Note:** Regardless of the restrictions, users can always log in when accessing SS on the server using a local IP address (127.0.0.1). This prevents total lockout from SS.

## Security Compliance Standards

### FIPS Compliance

The Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor (FIPS 140-2) are United States Government standards that provide a benchmark for implementing cryptographic software. SS has been tested within environments that are FIPS compliant. For instructions to enabling FIPS in SS, see the [Enabling FIPS Compliance in Secret Server](#) KB article.

### PCI Datacenter Compliance

SS can make it easier to comply with PCI-DSS requirements:

- **Requirement 8:** Assign a unique ID to each person with computer access: SS helps you comply with Requirement 8 by providing a secure repository for you to maintain an automated password changing schedule, forcing each user to have a unique, secured password. SS's Web-based access makes it easy to access these passwords.
- **Requirement 10:** Track and monitor all access to network resources and cardholder data: SS can monitor all access to network resources. By employing remote password changing to force password changes, administrators can monitor and update network resources on a customized scheduled. You can create a password changing schedule that best suits your environment.
- **Requirement 11:** Regularly test security systems and processes.
- **Requirement 12:** Maintain a policy that addresses information security: You can optimize SS's software's global configuration and template-driven data structure to fit the requirements of your current information security policy or assist in creating a policy based on SS. Configuration options include:
  - Applying two-factor authentication
  - Enabling launchers
  - Enabling Web services
  - Enforcing local-user password requirements
  - Forcing HTTPS/SSL
  - Requiring folders for secrets (for uniform permissions)

## SSL Certificates

SS can be configured to run using Secure Sockets Layer (SSL) certificates. We strongly recommend that SS installations run using SSL. Not using SSL significantly reduces the security of the contents of SS since browsers viewing the site are not using an encrypted connection.

## **What is Maintenance Mode?**

Maintenance mode prevents users from changing secrets or secret-related data such as dependencies, secret templates, and password requirements.

## **Why do we need Maintenance Mode?**

When secret key rotation takes place, or the HSM configuration is changed, SS needs to ensure that no data corruption occurs. To mitigate this, these operations turn on maintenance mode, which puts Secret Server into read-only mode. We also recommend manually enabling maintenance mode before performing upgrades.

## **Can I still access my Secrets when Maintenance Mode is turned on?**

Yes. Secrets will be read-only, but you can still view them, including secrets that are double-locked or protected by “require approval for access.” You are unable to change the checkout status of a secret during maintenance mode. This means if the secret is currently checked-in, you will be unable to check it out. If the secret is currently checked out, it cannot be checked in until the system leaves maintenance mode.

## **How long does Maintenance Mode last?**

Maintenance mode lasts until the operation triggering it is completed. The time required will vary based on the operation and the number of secrets in the system. Typically, maintenance mode lasts less than 30 minutes.

## Secret Server Authentication, Encryption, and Security

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server provides integration options for Windows authentication and SAML to automatically authenticate users to the application when they browse to SS on their workstations. SS also allows you encrypt data at various locations.

**Important:** This topic is for Secret Server v10.5 and later and assumes you have a running Identity Service Provider (IDP) with a signed certificate.

**Note:** Secret Server does not support using SAML when Integrated Windows Authentication (IWA) is enabled.

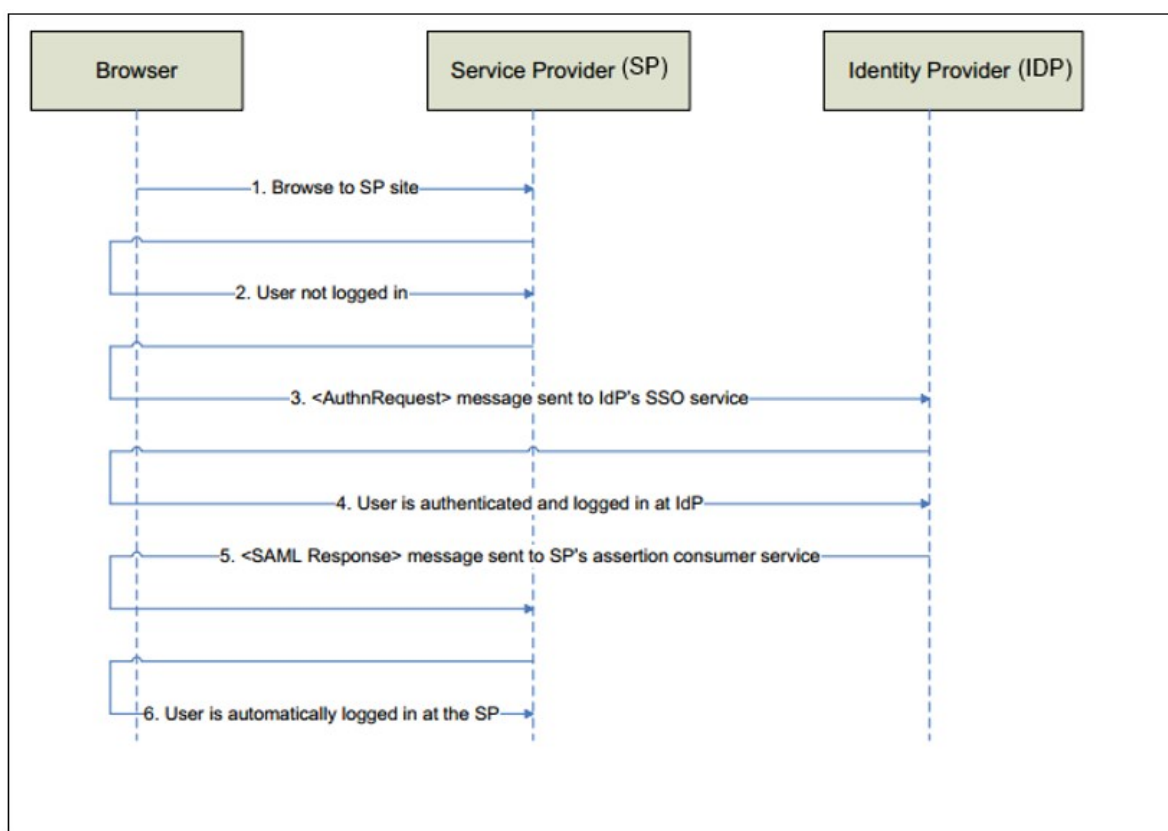
**Note:** This topic applies to Secret Server 10.5 and later. For earlier versions, please see [Configuring SAML in Secret Server](#) (KBA).

## SAML Overview

Secret Server allows the use of SAML Identity Provider (IDP) authentication instead of the normal authentication process for single sign-on (SSO). To do this, SS acts as a SAML Service Provider (SP) that can communicate with any configured SAML IDP.

In the diagram below, SS acts as the service provider. Any configured SAML IDP can be used for this process and there are several well tested providers, including OKTA, OneLogin, Azure ADFS, and Microsoft ADFS.

**Figure:** Secret Server as a SAML Identity Provider



## Prerequisites

### Licensing and Version

Secret Server Professional Edition or higher, upgraded to version 10.5 or later. To install a new SAML license, go to **Admin > Licenses > Install New License**.

## .NET Framework 4.6.2+

To use SAML 2.0, you must install .NET Framework 4.6.2 or higher on your Web server. This allows SS to use Microsoft's "next generation" CryptoNG API for signing SAML requests, instead of being limited to the much older CryptoAPI. This is often necessary to use modern SSL certificates and is strongly recommended as a security best practice.

To download and install the latest version of .NET Framework: See [Microsoft .NET Framework 4.8 offline Installer for Windows](#) for the latest version as of when this topic was written. If you have already installed SS on the same Web server, you have already done this.

### Administer Configuration SAML Role Permission

The "Administer Configuration SAML" role permission is required to use SAML to access SS. To grant a user this permission from an administrator account:

1. Go to **Admin > Roles**. The Roles page appears.
2. Click the **Create New** button. The Role Edit page appears:

**Role Edit**

Role Name \*

Enabled ☒

Created

**Permissions Assigned**

**Permissions Unassigned**

- Access Offline Secrets on Mobile
- Add Secret
- Add Secret Custom Audit
- Administer Active Directory
- Administer Backup
- Administer Configuration
- Administer Configuration Proxying
- Administer Configuration SAML
- Administer Configuration Security
- Administer Configuration Session Recording
- Administer Configuration Two Factor
- Administer Configuration Unlimited Admin
- Administer ConnectWise Integration
- Administer Create Application Accounts
- Administer Create Users

« « > » »

3. Type the name, such as SAML, in the **Role Name** text box.
4. Click to select the **Enabled** check box.
5. Click **Administer Configuration SAML** in the right side **Permissions Unassigned** list box.
6. Click the **<** button to move the permission to the other side.
7. Click the **Save** button. The Roles page returns.

8. Click the Assign Roles button.name link of the newly created role. The View Role Assignment page appears:

### View Role Assignment

[By Role](#)
[By User Or Group](#)

**Role**

Administrator

Save To File < 1 to 15 of 15 >

NAME	TYPE	CREATED
admin	User	5/15/2019
gamma.thycotic.com\	User	3/30/2020
gamma.thycotic.com\	User	3/26/2020
Developers	Group	8/9/2019
gamma.thycotic.com\	User	4/9/2020
gamma.thycotic.com\	User	8/9/2019
gamma.thycotic.com\	User	8/9/2019

9. Click the **Role** dropdown list to select the role you just created.

### View Role Assignment

[By Role](#)
[By User Or Group](#)

**Role**

SAML

There are no Groups or Users.

Back

Edit

10. Click the **Edit** button. The Role Assignment page appears:

### Role Assignment

Please note that changing role assignment could remove your access to Role Administration.

By Role

By User Or Group

Role

SAML

Assigned

Unassigned

<<

<

>

>>

admin

appaccount1

DevOps1

Duo Approvers

Everyone

gamma.thycotic.com\Access Control Assistance Operators

gamma.thycotic.com\Account Operators

gamma.thycotic.com\Administrators

gamma.thycotic.com\...

gamma.thycotic.com\...

gamma.thycotic.com\...

gamma.thycotic.com\... Password Replication Group

gamma.thycotic.com\...

gamma.thycotic.com\...ors

gamma.thycotic.com\...

Back


11. Move the desired users to the **Assigned** list using the same method as before.
12. Click the **Save Changes** button.

## Setting up Secret Server

1. Navigate to **Admin > Configuration**.
2. Click the **SAML** tab:


## SAML Configuration

[General](#)
[Login](#)
[SAML](#)
[Folders](#)
[Local User Passwords](#)
[Security](#)
[Ticket System](#)
[Email](#)
[Session Recording](#)
[HSM](#)


SAML instructs Secret Server to trust a separate server as its Identity Provider. When SAML is enabled, the Identity Provider is responsible for asking the user for their username or password, but Secret Server will still ask the user for any configured 2-factor.


### SAML GENERAL SETTINGS


SAML Enabled	No
Use Legacy SAML	No


Edit


### SAML SERVICE PROVIDER SETTINGS

**Name** SecretServerServiceProvider  
**Certificate**



Edit



Download Service Provider Metadata (XML)

### IDENTITY PROVIDERS

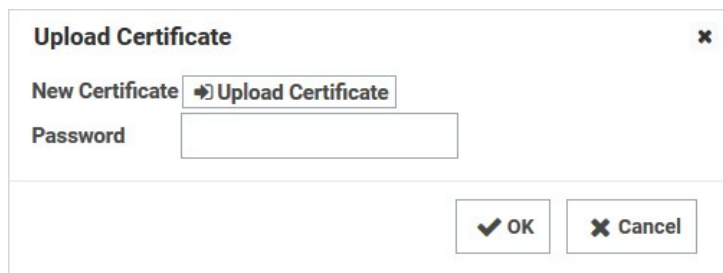

Create New Identity Provider

DISPLAY NAME	NAME	DESCRIPTION	CERTIFICATE THUMBPRINT	ACTIVE	ADVANCED
--------------	------	-------------	------------------------	--------	----------


View Log


View Audit

- Click the **Edit** button in the **SAML General Settings** section.
- Click to select the **SAML Enabled** check box.
- Click the **Save** button.
- Under General Settings, click **Edit**, then check the **SAML Enabled** checkbox. **Save** changes.
- Click the **Edit** button in the **SAML Service Providers** section.
- Type a name for your SS service provider, such as SecretServerServiceProvider, in the **Name** text box.
- Click the **Select Certificate** link. The Upload Certificate popup appears:



10. Click the **Upload Certificate** button to upload the certificate used for SS's HTTPS configuration.
11. Locate your certificate .pfx file and select it.
12. Click the **Open** button. The new certificate appears.
13. Type the access password for the private key of the certificate in the **Password** text box.
14. Click the **OK** button. The certificate is uploaded and tested, and the popup disappears. The certificate now appears in the SAML Service Provider Settings section.

**Note:** If you have an outdated version .NET Framework (earlier than 4.6.2), you may see an error recommending you upgrade to fix the error. Reload the certificate after you do so.

15. Click the **Save** button.
16. Click the Create New Identity Provider link. An Identity Provider popup appears.
17. Click the **Import IDP from XML Metadata** link.
18. Navigate to your SecretServerSAMLMetadata.xml file and select it. This is used for uploading into your IDP, which varies by provider. Follow instructions in the following section..
19. Click the Open button.

## Setting up IDPs

IDP setup varies by provider. Click one of the following links for instructions for your provider:

**Note:** You must be logged in to access these links.

- [How To Set Up Okta For SAML Integration](#) (KBA)
- [How To Set Up OneLogin For SAML Integration](#) (KBA)
- [How To Set Up Azure AD For SAML Integration](#) (KBA)
- [How To Set Up ADFS For SAML Integration](#) (KBA)

**Note:** The username returned from the IDP to SS within the SAML Response/Assertion's subject statement must match the desired format. The format of the username passed depends upon how the user was created within SS.

**Note:** If AD Sync was used to create SS users, the username returned from the IDP must match this format: SecretServerUsername@ADsyncDomain Or ADsyncDomain\SecretServerUsername. If using SLO, ensure that the NameID is set correctly in the IDP as an outgoing claim for the Secret Server Service Provider. If a user has different sAMAccountName and userPrincipalName in Active Directory, custom rules in the IDP can be created.

## Lockout Workaround

Locked Out? Here's how you get around SSO. If during the configuration process for SAML you lock yourself (as an administrator or a user) out of SS, you can log on SS without using the SSO workflow by using this URL string:

[YourSecretServerInstanceName]/login.aspx?preventautologin=true

The role permission needed for this is "Bypass SAML Login," which admins have by default.

## Overview

The Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor FIPS 140-2 are United States Government standards that provide a benchmark for implementing cryptographic software. Secret Server (SS) was tested and operates correctly in FIPS-compliant environments.

**Note:** The Microsoft .NET implementations of AES and SHA are not FIPS certified so Secret Server uses the Windows API versions for encryption functionality which *are* FIPS certified.

See [FIPS 140-2 Validation](#) for the FIPS certificate numbers for the Windows operating systems, including the algorithm implementations that we use. Supported operating systems include Windows Server 2008 R2 and above.

## Procedure

To enable FIPS compliance:

### Task 1: Enable FIPS in Secret Server

1. Ensure SS is already installed.

**Important:** Secret Server is unavailable and may give errors (such as "Parser Error Message: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms") until all the steps are completed.

**Important:** During SS installation, if FIPS compliance for Windows has already been enabled 'InvalidOperationException' error messages may result. To resolve the issue, please contact support for assistance.

**Important:** If FIPS is enabled as part of a domain group policy, it must be disabled before the option can be enabled in SS, otherwise an error may occur. It can be re-enabled using group policy once the feature has been enabled in the application.

2. In SS, go to **Admin > Configuration**.
3. Click the **Security** tab.
4. Click the **Edit** button at the bottom of the page.
5. Click to enable the **Enable FIPS Compliance** check box in the **FIPS Compliance** section.
6. Click the **Save** button.

### Task 2: Enable FIPS in Windows

1. At the Windows command prompt, run `secpol.msc`. The Local Security Policy application appears.
2. In the left pane, drill down to **Security Settings > Local Policies > Security Options**.
3. In the right pane double-click the **System Cryptography: Use FIPS Compliant algorithms for encryption, hashing, and signing** policy. Its properties appear.
4. Click to enable the **Enabled** selection button on the **Local Security Setting** tab.
5. Click the **OK** button.
6. Close the **Local Security Policy** application.

### Task 3: Reset the IIS Server

Run `iisreset` from the Windows command prompt. IIS resets.

**Note:** When using FIPS compliance mode in SS, we use the NIST-certified encryption algorithms within the Windows Operating System.

**Note:** There should be no need to enable FIPS on the database server operating system because the encryption applies between the application and the database, not between the operating systems. Data is encrypted before it reaches the database.

## Related Information

- [NIST Cryptographic Module Validation Program Information](#)
- [FIPS information for Windows](#)
- [IIS Reset](#) (KBA)

## Overview

An SSL (Secure Sockets Layer) certificate greatly enhances the security between the user's browser and the server your SS is installed on. It encrypts all data between the server and the client's browser so if an attacker were to look at the data being transmitted between the two, they would not be able to decipher it.

**Note:** SSL is required when using Integrated Windows Authentication.

## Obtaining an SSL Certificate

You can get a certificate from various companies such as [Thawte](#) or [VeriSign](#). If you already obtained a certificate from one of them, please follow their instructions for installing their certificates.

**Note:** Thycotic does **not** provide certificates.

## Installing a Self-Signed Certificate

You can create your own certificate for trial or sandbox environments:

**Note:** This requires IIS 7 or later.

### Task One: Generate an IIS Self-Signed Certificate

1. Open IIS manager (**inetmgr**) on your Web server.
2. Click on the server node (one of the root nodes) in the left panel.
3. Double-click the **Server certificates** icon.
4. Click the **Create Self-Signed Certificate** link in the **Actions** panel. The Specify Friendly Name dialog box appears.
5. Type any name you desire in the **Specify a Friendly name for the certificate** text box.
6. Click the **OK** button. You now have an IIS self-signed certificate that is valid for one year. It appears under the Server Certificates panel. The certificate common name (Issued To column) is the host name of the machine running the site.

### Task Two: Bind the Self-Signed Certificate to the IIS Site

1. In IIS Manager, click the server you want to bind to on the **Connections** panel tree.
2. Drill down to **Sites > Default Web Site**.
3. Click the **Bindings...** link in the **Actions** panel. The Site Bindings dialog box appears.
4. Click the **Add...** button. The Edit Site Binding dialog box appears.
5. Click the **Type** dropdown list and select **https**.
6. Click the **SSL certificate** dropdown list to select the certificate you just created.
7. Click the **OK** button. You return to the Site Bindings dialog box, where the HTTPS binding now appears.
8. Click the **Close** button. The dialog box closes.

## Task Three: Test the Self-Signed Certificate

1. In a browser, go to the Website using the certificate. You should see a warning that there is an issue with the site's security certificate—specifically, the security certificate was issued for a different website's address. This occurs because IIS uses the server's name as the common name when using a self-signed certificate, which usually does not match the hostname to access the site in your browser.
2. To access the website, click the "continue to the website" link or button. You will have to do this each time you access the site. Because this is a test environment, this should not be an issue.

**Note:** It is possible to remove the warning by adding the self-signed certificate to the trusted root certificate authorities, but that is beyond the scope of this instruction.

## Overview

Thycotic One is the single-sign-on provider for Thycotic applications. With Thycotic One, one user account can be granted access to multiple Thycotic products, such as Secret Server (SS), Privilege Manager, DevOps Secrets Vault, and Account Lifecycle Manager.

Thycotic One enables login integration using the OpenID Connect protocol, an industry standard single-sign-on method.

This article describes the Thycotic One configuration options available in SS.

## Cloud versus On-Premise

Thycotic One is the default identity provider in SS Cloud. When you set up the cloud instance, it will already be configured and ready to use Thycotic One. The initial admin user will log in with their Thycotic One account, and optionally, all newly created SS accounts can be synchronized with Thycotic One, so they can log in that way as well.

Thycotic One integration is off by default in the on-premise release of SS, but it is supported. You can turn on Thycotic One integration and configure it. For example you might want to share an identity provider between your on-premise instance, and one or more other cloud products.

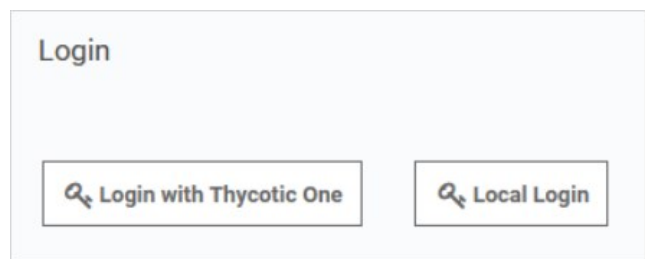
## Procedures

### Logging in with Thycotic One

When Thycotic One integration is turned on, all SS users can log in either with their local passwords or with Thycotic One. All SS permissions and configuration will apply to that user regardless of how they logged in.

However, the local username and password and the Thycotic One username and password are not necessarily the same thing. In Thycotic One, you'll log in with your email address rather than your username, and the password you use may very well be different from the SS password.

You'll see this on the login screen:



Clicking **Local Login** will bypass Thycotic One and allow the user to log in with their local SS password. Clicking **Login with Thycotic One** will redirect the user to Thycotic One to authenticate. Once that is successfully done, the user will be redirected back to SS.

After clicking **Login with Thycotic One**, users will type their email address and password:

Sign In

Email address

Enter Email Address

Next

[Create New Account](#)
[Reset My Password](#)

And then be redirected back to their dashboard in SS.

## Configuring Thycotic One

Thycotic One integration is configured on the **Admin > Configuration** page, under the **Login** tab. You can view the configuration there:

Enable Thycotic One Integration	Yes	<a href="#">Sync Now</a>
Thycotic One Server URL	https://login.thycotic.com/	
Add New Users to Thycotic One	Yes	
Use Thycotic One authentication as the default	Yes	

The **Sync Now** button provides a way for you to trigger a synchronization of your SS accounts with Thycotic One. In most cases, you will not need to use this, as synchronization will happen on a schedule or whenever a relevant event happens, such as enabling a user or performing an Active Directory synchronization. Only active user accounts with email addresses will be synchronized.

Click **Edit** at the bottom of the page to change the configuration. The available options are slightly different between the cloud and on-premise versions of SS.

## Secret Server Cloud

When editing the options in SS Cloud, you'll see something like this:

Enable Thycotic One Integration	<input checked="" type="checkbox"/>
Secret Server Redirect URI	https://yourcloudinstance.secretservercloud.com/signin-oidc
Thycotic One Server URL	https://login.thycotic.com/
Client Id	d9f43331-09d3-41b1-82ca-326c9c6dd419
Client Secret	< Saved >
Add New Users to Thycotic One	<input checked="" type="checkbox"/>
Use Thycotic One authentication as the default	<input checked="" type="checkbox"/>

Here are the available options:

- **Enable Thycotic One Integration:** Turn on to enable Thycotic One functionality. Turn off to completely disable Thycotic One logins and synchronization. Make sure you have an admin account with a working local password.
- **Secret Server Redirect URI:** For informational purposes, this shows the page address to which you are redirected after you have logged in with Thycotic One.
- **Thycotic One Server URL:** The Thycotic One server you have connected to. There is one separate Thycotic One instance in each SS Cloud region.
- **Client ID:** The client ID portion of the Thycotic One server credentials.
- **Client Secret:** Not shown, the client password portion of the credentials.
- **Add New Users to Thycotic One:** When checked, SS accounts will be synchronized with Thycotic One. Adding a user will send them a welcome email, where they can set up their Thycotic One account password and log into SS. When unchecked, users will not be synchronized and no email will be sent. New users will not be able to log in with Thycotic One, unless you click **Sync Now** on the **Admin > Configuration > Login** page, which will synchronize all active users.
- **Use Thycotic One authentication as the default:** When checked, Thycotic One authentication is used for the REST and SOAP APIs and mobile apps. Users who have logged in with Thycotic One use their Thycotic One account passwords for those activities, rather than their local SS account passwords. When unchecked, they will use their local SS account passwords for those activities.

In Cloud, the server URL, client ID, and client secret cannot be edited—they are set up for you when the instance is provisioned and cannot be changed.

## Secret Server On-Premise

When editing the options in SS on-premise, you'll see something like this:

Enable Thycotic One Integration	<input checked="" type="checkbox"/>
Secret Server Redirect URI	<a href="https://mysecretserverinstance.example.com/SecretServer/signin-oidc">https://mysecretserverinstance.example.com/SecretServer/signin-oidc</a>
Thycotic One Server URL	<input type="text"/>
Client Id	<input type="text"/>
Client Secret	<input type="text"/>
Add New Users to Thycotic One	<input type="checkbox"/>
Use Thycotic One authentication as the default	<input type="checkbox"/>

Unlike in Cloud, the server URL, client ID, and client secret can be edited in an on-premise instance. You can generate Thycotic One credentials using Thycotic's cloud management portal, Cloud Manager. Otherwise, the configuration options behave the same as in Cloud.

## Generating a Thycotic One Credential

To generate a credential for use in an on-premise SS instance, follow the steps below:

1. From Cloud Manager, choose a Thycotic One region under Other Login Options.
2. Log into Thycotic One as a user that will be managing your organization's credentials. Create an account if you have not yet done so.
3. Go to Cloud Manager at <https://portal.thycotic.com/>.
4. Click **Sign In**. You are redirected to our tech support portal login.
5. Click the button for the Thycotic One region you chose. Since you are already logged in to Thycotic One, this will redirect you back to Cloud Manager.
6. Next, choose a team: In the menu, go to **Manage > Teams**. You may already have one if you have an existing cloud product. If not, create one. Each team can handle multiple Thycotic One credentials.
7. Having selected your team, go to **Organizations**. Again, if you already have an organization, you can use it; if not, you can create one. An organization provides a way to manage the global login policies for all users.
8. Go to **Credentials**. Click **Add**. An Organization Credential dialog box appears:

Organization Credential

Name

My Secret Server Instance

Post-Login Redirect URIs

+

https://mysecretserverinstance.example.com/SecretServer/signin-oidc

Post-Logout Redirect URIs

+

Credentials

These credentials must be added to your application (for example, Secret Server) to connect to Thycotic One.

Endpoint

https://login.thycotic.com/

Client Id

c36b17ca-3e20-438c-bfa4-f0903ea54fcf

Client Secret

806f0ddc33d46994313b857468c97318d6e1fadf73efaa00b4dc05dec31c48cc

Make a note of this value, as it cannot be retrieved once it is saved.

Save

Cancel

9. The available fields are as follows:

- **Name:** A description of the application using this credential, for informational purposes.
- **Post-Login Redirect URIs:** A list of valid URIs that will be allowed to authenticate with this credential. The value of “Secret Server Redirect URI” from your on-premise instance should go here. If users access your instance with more than one URI, you may want to add all of them here by clicking the + button to create additional fields. Unless an application supplies a URI that is an exact match to one of these, Thycotic One will not complete the authentication.
- **Post-Logout Redirect URIs:** SS does not support this feature, so this may be left blank.
- **Credentials:** The fields in this area contain the values you need to put into the Thycotic One configuration in SS. Copy and paste them into the corresponding fields.

10. Once you capture all the values, click **Save**, and then save the configuration in SS as well. Your instance is now fully integrated with Thycotic One. If you selected the synchronization option, SS will immediately sync your active users with Thycotic One, and they'll

receive welcome emails describing how to continue the process.

Starting with version 10.4, Secret Server allows you to define a policy for validating X509 Certificates. This applies to all Active Directory domains using LDAPS. It also applies to any connections to syslog servers over TLS. Certificates that do not meet the policies specified in SS are rejected, denying connections to the server. All certificate validation failures are logged in the security audit log, which is available by going to **Admin > See All** and then **Security Audit Log**.

## Setting the Certificate Verification Policy

To set a verification policy:

1. Go to **Admin > Configuration**.
2. Click the **Security** tab.
3. Click the **Edit** button
4. Click to select the **Apply TLS Certificate Chain Policy and Error Auditing** check box. The TLS Auditing options appear:

TLS AUDITING

Apply TLS Certificate Chain Policy and Error Auditing
☒

Ignore Certificate Revocation Failures
☐

Additional Certificate Chain Policy Options
What are X509 Certificate Chain Policy Options?

X509RevocationMode.NoCheck

Enable TLS Debugging and Connection Tracking
☐

Advanced (not required)

*i*

Secret Server's IIS AppPool must be granted permission to use the Client Certificate, using the Windows HTTP Services Certificate Configuration Tool (WinHttpCertCfg.exe). Example usage:  
winhttpcertcfg.exe -g -c LOCAL\_MACHINE\MY -s "Certificate Subject" -a "HOSTNAME\IIS APPPOOL\SecretServer"  
Download WinHttpCertCfg - Official WinHttpCertCfg documentation

Client Certificate Thumbprint(s)

Enter Client Certificate Thumbprint Ids ...

- To change the policy, type a semi-colon delimited list of policy options in the **Additional Certificate Chain Policy Options** text box. To use a policy, enter the <full\_enumeration\_name>.<enumeration\_item>. For example, to validate the entire certificate chain, add X509RevocationFlag.EntireChain to the semi-colon delimited list of options. See [Certificate Validation Options](#) for details.
- If you wish to ignore certificate revocation warnings and allow revoked certificates, click to select the **Ignore Certificate Revocation Failures** check box.

## Certificate Validation Options

The following Microsoft enumerations are the available certificate chain policy options. For detailed descriptions of each option, see the linked documentation.

### X509RevocationMode

Specifies the mode used to check for X.509 certificate revocation.

NoCheck	0	No revocation check is performed on the certificate.
Offline	2	A revocation check is made using a cached certificate revocation list (CRL).
Online	1	A revocation check is made using an online certificate revocation list (CRL).

[Unexpected Link Text](#)

See [X509RevocationMode Enum](#) for details.

#### **X509RevocationFlag**

Specifies which X.509 certificates in the chain should be checked for revocation.

EndCertificateOnly	0	Only the end certificate is checked for revocation.
EntireChain	1	The entire chain of certificates is checked for revocation.
ExcludeRoot	2	The entire chain, except the root certificate, is checked for revocation.

[Unexpected Link Text](#)

See [X509RevocationFlag Enum](#) for details.

#### **X509VerificationFlags**

Specifies conditions under which verification of certificates in the X.509 chain should be conducted. These values can be bitwise combined to indicate multiple flags.

AllFlags	4095	All flags pertaining to verification are included.
AllowUnknownCertificateAuthority	16	Ignore that the chain cannot be verified due to an unknown certificate authority (CA).
IgnoreCertificateAuthorityRevocationUnknown	1024	Ignore that the certificate authority revocation is unknown when determining certificate verification.
IgnoreCtlNotTimeValid	2	Ignore that the certificate trust list (CTL) is not valid, for reasons such as the CTL has expired, when determining certificate verification.
IgnoreCtlSignerRevocationUnknown	512	Ignore that the certificate trust list (CTL) signer revocation is unknown when determining certificate verification.
IgnoreEndRevocationUnknown	256	Ignore that the end certificate (the user certificate) revocation is unknown when determining certificate verification.

IgnoreInvalidBasicConstraints	8	Ignore that the basic constraints are not valid when determining certificate verification.
IgnoreInvalidName	64	Ignore that the certificate has an invalid name when determining certificate verification.
IgnoreInvalidPolicy	128	Ignore that the certificate has invalid policy when determining certificate verification.
IgnoreNotTimeNested	4	Ignore that the CA (certificate authority) certificate and the issued certificate have validity periods that are not nested when verifying the certificate. For example, the CA cert can be valid from January 1 to December 1 and the issued certificate from January 2 to December 2, which would mean the validity periods are not nested.
IgnoreNotTimeValid	1	Ignore certificates in the chain that are not valid either because they have expired or they are not yet in effect when determining certificate validity.
IgnoreRootRevocationUnknown	2048	Ignore that the root revocation is unknown when determining certificate verification.
IgnoreWrongUsage	32	Ignore that the certificate was not issued for the current use when determining certificate verification.
NoFlag	0	No flags pertaining to verification are included.

[Unexpected Link Text](#)

See [X509VerificationFlags Enum](#) for details.

## Troubleshooting

If you enable certificate policy validation and logging, you may have server connections rejected due to certificates that violate the set policies. These errors are recorded in the security audit log. If the information logged there is not enough to determine why a certificate was rejected, you can get additional log details by enabling TLS Debugging. This adds detailed information to the logs about each certificate checked.

Due to the possibility of exposing sensitive information in the logs, TLS debugging requires two steps to enable:

1. Click to select the **Enable TLS Debugging and Connection Tracking** check box.
2. Change the global logging level to DEBUG. To do this, edit the `web-log4net.config` file in the root folder of your Web application. Follow the comments in the file to comment out the current log level line (the default is INFO), and uncomment the line that sets the value to DEBUG.

**Important:** Only enable TLS debugging when you are actively troubleshooting a certificate validation issue. Disable this option when you are not to prevent logging of certificate details.

**Note:** Please see the closely related article [Using a Service Account to Run the IIS App Pool & Access the Thycotic SQL Database – Best Practices \(Advanced\)](#) for additional information.

## Introduction

Integrated Windows Authentication (IWA) requires:

- Installing a SQL Server instance
- Creating a new domain service account
- Granting access to SQL Server database
- Registering a service account to run IIS and ASP.NET
- Assigning an account as an application pool identity

**Note:** For instructions on Creating the SQL account or Installing SQL Server see [Installing and Configuring SQL Server](#) (KBA).

## Creating a Domain Service Account

The account needs access to the application server and database server. Ensure password expiration is not enabled or the account could lock you out of Secret Server.

## Granting Access to SQL Server database

1. Connect to the Database instance using SQL Management Studio.
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) and select **New > Login**.
3. Enter the Login name as Domain\Username.
4. Ensure **Windows Authentication** radio button is selected.
5. If you have already created the database, then under **User Mappings** select the database and grant dbOwner permission. Otherwise, if you plan to have the Database created for you, under **Server Roles** select dbCreator.
6. Click the **Ok** button.

## Assigning Account as Identity of Application Pool

1. Open IIS (Run command inetmgr).
2. Click the Application Pool node.
3. Select Secret Server's Application Pool (default is SecretServerAppPool).
4. On the Right panel, Click .
5. Scroll down to the **Identity** row under **Process Model**.
6. In the popup, select **Custom Account > Set**.
7. Type the user as domain\username.
8. Type the password.
9. Click the **Ok** button.
10. Recycle the application pool by clicking the **Recycle..** button under the **Application Pool** tasks.

## Introduction

In some cases, a PowerShell script may need to access resources outside of a Secret Server (SS) machine. This requires that any credentials are delegated to the target machine. SS runs PowerShell scripts using Windows Remote Management (WinRM), which does not allow credential delegation by default. To allow credential delegation, the SS machine must have Credential Security Support Provider (CredSSP) enabled. CredSSP is a security support provider that allows a client to delegate credentials to a target server.

Some scenarios requiring CredSSP:

- The script needs to query or update a value in Active Directory.
- The script needs to query or update a value in a SQL Server instance.
- The script is used as part of extensible discovery for locating accounts or machines on a different domain or non-domain joined environment.

## Enabling CredSSP for WinRM in Secret Server

1. Go to **Administration > Configuration**. The General tab of the Configuration page appears:

APPLICATION SETTINGS	
Allow Automatic Checks for Software Updates	Yes
<a href="#">Anonymized System Metrics Information</a>	
Send Anonymized System Metrics to Thycotic	No <a href="#">View Metric Data</a>
<a href="#">View Webservices</a>	
Enable Webservices	Yes
Maximum Time for Offline Access on Mobile Devices	30 days
Session Timeout for Webservices	20 minutes
Enable Refresh Tokens for Web Services	No
Prevent Application from Sleeping When Idle	Yes
<a href="#">Syslog/CEF Logging Advanced Settings Information</a>	
Enable Syslog/CEF Logging	No
<a href="#">Test PowerShell with WinRM</a>	
WinRM Endpoint URL	http://localhost:5985/wsman
<a href="#">How do I configure CredSSP for WinRM?</a>	
Enable CredSSP Authentication for WinRM	Yes

2. Click **Edit** button at the bottom of the page.
3. Click to select the **Enable CredSSP Authentication for WinRM** checkbox.

4. Click the **Save** button.

**Note:** This is the global CredSSP settings and by default will configure CredSSP and connections to come *from* the Web server. This is used when **not using distributed engines**.

**Note:** If you are using distributed engines and you enable CredSSP at the site-specific level, these settings take precedence over this global CredSSP setting. Secrets will prioritize these site-specific settings. Therefore, if you plan on using CredSSP through a distributed engine, you should consider disabling the global setting seen below and only configure it at the site-specific level.

## Configuring CredSSP for WinRM on the Secret Server Machine

1. Log on to the machine running SS.
2. Run Windows PowerShell as an administrator.
3. Enable client-side CredSSP by running:

```
Enable-WSManCredSSP -Role Client -DelegateComputer <Secret Server fully qualified machine name>
```

For example:

```
Enable-WSManCredSSP -Role Client -DelegateComputer <localhost>
```

**Note:** localhost is the actual string that SS uses to generate the PowerShell run space. Sometimes customers need both localhost and FQDN entries. *In theory*, those entries should be the same, thus not needing a second one.

4. Enable server-side CredSSP by running:

```
Enable-WSManCredSSP -Role Server
```

5. The Web server always uses a specified account to run the PowerShell scripts. Considerations:
  - Ensure that account is added to the "Remote Management Users" local group on each Web server.
  - For RPCs with custom password changers, this would be "Change Password Using," and then select "Privileged Account."
  - For PowerShell password changers in the classic UI, this would be "Run PowerShell Using" and can alternatively be configured as the "Default Privileged Account" at the template level.
  - For custom dependencies using PowerShell scripts, this would be the "Run As" secret.
  - If you use any form of extensible discovery, this account needs to be the first secret that is linked to the scanner. Any additional secrets linked to the scanner are typically associated with authentication to the destination system.

## Configuring CredSSP for WinRM on a Distributed Engine

You can alternatively configure CredSSP and the credential delegation to occur from your distributed engines by changing this setting at the site level:

1. Go to **Admin > Distributed Engines**. The Distribute Engine Configuration page appears:

**Distributed Engine Configuration**

DISTRIBUTED ENGINE

[Distributed Engine Overview](#)

Enable Distributed Engine Yes

ENGINE CALLBACK SETTINGS

Protocol HTTPS  
 Url(s) https://qa-cust-01.gamma.thycotic.com/Playground  
 Default Callback Interval 300 seconds  
 Response Bus Site Connector: Default MemoryMq Service

ADVANCED ENGINE MESSAGE SETTINGS

Secret Heartbeat Message Time to Live 60 minutes  
 Secret Heartbeat Message Retry Time 90 minutes  
 Secret Password Change Message Time to Live 60 minutes  
 Secret Password Change Message Retry Time 90 minutes

[Back](#)
[Edit](#)
[Manage Sites](#)
[Manage Site Connectors](#)
[Download Engine Installer 64-bit](#)
[Download Engine Installer 32-bit](#)
[View Audit](#)

- Click the **Manage Sites** button. The Manage Sites page appears:

**Manage Sites**

< 1 to 3 of 3 >

SITE NAME	ACTIVE	ONLINE ENGINES	OFFLINE ENGINES	LAST ACTIVITY
Local	Yes	0	0	
Site1	Yes	1	0	3/10/2020 08:46 AM
Site2	Yes	0	1	5/22/2019 01:59 PM

☐ Show Inactive

[Back](#)
[Refresh](#)
[+ New Site](#)
[Manage New Engines](#)

- Click the **Site Name** link of the desired site. The Site View page for that site appears:

**Site View**

**i** You have reached the limit of engines per site allowed by your licensing.

Site Name	Site1
Status	Active
Site Connector	Site1 <a href="#">View Site Connector</a>
Engine Callback Interval	300
Secret Count	2
Processing	Heartbeats: 0. Password Changes: 0

[Test PowerShell with WinRM](#)

WinRM Endpoint URL http://localhost:5985/wsman

[How do I configure CredSSP for WinRM?](#)

Enable CredSSP Authentication for WinRM Yes

[Back](#)
[Edit](#)
[Reassign Secrets](#)
[Download Engine Installer 64-bit](#)
[Download Engine Installer 32-bit](#)
[View Audit](#)
[Validate Connectivity](#)

ENGINE NAME	CONNECTION STATUS
SRV-USP2-RMQ3C.thycotic.blue	Online

4. Click the **Edit** button. The Site Edit page appears:

**Site Edit**

Site Name	<input type="text" value="Site1"/>
Active	<input checked="" type="checkbox"/>
Site Connector	<input type="text" value="Site1"/>
Engine Callback Interval	<input type="text" value="30"/>
<a href="#">Windows Remote Management Explanation</a>	
WinRM Endpoint URL	<input type="text" value="http://localhost:5985/wsman"/>
<a href="#">How do I configure CredSSP for WinRM?</a>	
Enable CredSSP Authentication for WinRM	<input checked="" type="checkbox"/>

5. Click to select the **Enable CredSSP Authentication for WinRM** check box.

6. Click the **Save** button.

7. Log on to each of your distributed engines where CredSSP is enabled.

8. Run Windows PowerShell as an administrator.

9. Enable client-side CredSSP by running:

Enable-WSManCredSSP -Role Client -DelegateComputer <distributed engine fully qualified machine name>

Enable-WSManCredSSP -Role Client -DelegateComputer <localhost>

**Note:** localhost is the actual string that the Distributed Engine is using to generate the run space. Some customers need to have both the localhost and FQDN entry. *In theory*, both entries above should be the same, thus not needing a second entry.

## 10. Enable server-side CredSSP by running:

Enable-WSManCredSSP -Role Server

## 11. The distribute engine will always use a specified account to run the PowerShell scripts. Considerations:

- Ensure that account is added to the "Remote Management Users" local group on each engine where CredSSP is enabled.
- For RPCs with custom password changers, this would be "Change Password Using," and then select "Privileged Account".
- For PowerShell password changers in the classic UI, this would be "Run PowerShell Using" and can alternatively be configured as the "Default Privileged Account" at the template level.
- For custom dependencies using PowerShell scripts, this would be the "Run As" secret.
- If you use any form of extensible discovery, this account needs to be the first secret that is linked to the scanner. Any additional secrets linked to the scanner are typically associated with authentication to the destination system.

## 12. Ensure that the "Allow Delegating Fresh Credentials" group policy setting is enabled and is not disabled by a domain policy.

1. Open the gpedit.msc file on your SS machine or distributed engine, depending on where CredSSP is enabled
2. Navigate to **Computer Settings > Administrative Templates > System > Credentials Delegation**.
3. Edit the "Allow Delegating Fresh Credentials" setting.
4. Verify that it is Enabled.
5. Click "Show..."
6. Verify that the list contains an entry that begins with "wsman/" and ends with the fully qualified machine name of the SS machine or distributed engine.
7. If destination systems are non-domain joined or on another domain without a trust, it may be required for you to add in an entry for **each** destination system you wish to run the script or do discovery on (as examples). Consider collecting a list of all destination FQDNs for your specific use case and adding them all in one go.

## 13. Depending on where CredSSP is configured (Web server or distributed engine), run the following commands:

- View existing entries: Get-Item WSMan:\localhost\Client\TrustedHosts
- Adding computers if your TrustedHosts list is empty: Set-Item WSMan:\localhost\Client\TrustedHosts \*-Value\* <ComputerName>,[<ComputerName>]
- Adding computers to your existing TrustedHosts list: \$curList = (Get-Item WSMan:\localhost\Client\TrustedHosts).value Set-Item WSMan:\localhost\Client\TrustedHosts -Value "\$curList, Server01"

## 14. On the destination system, if it is on a separate domain without a trust or non-domain joined, add the reverse WSman entries so the destination system trusts either SS or your engines. Run one of the following commands:

Web server:

Set-Item WSMan:\localhost\Client\TrustedHosts \*-Value\* <Web Server 1 FQDN>,[<Web Server 2 FQDN>]

Engine:

Set-Item WSMan:\localhost\Client\TrustedHosts \*-Value\* <Distributed Engine 1 FQDN>,[<Distributed Engine 2 FQDN>]

## 15. Restart either SS or the engine you just trusted.

## Enabling CredSSP on Secret Server Agents for PowerShell Script Dependencies

**Note:** Remote agents were upgraded to distributed engines in SS version 8.9. This section only applies to SS versions 8.8.000020

and earlier.

**Note:** Remote Agents are only needed for networks that are not directly connected to the network that SS is installed on. If you are not using remote agents, disregard this section.

By default, SS agents inherit the "Enable CredSSP Authentication for WinRM" setting from SS; however, you can override this in the agent configuration file as follows:

1. On the machine running the agent, locate the the agent program files. By default, they are at C:\Program Files (x86)\Thycotic Software Ltd\Secret Server Agent.
2. Edit the SecretServerAgentService.exe.Config file in a text editor.
3. Locate the "UnencryptedSettings" section.
4. Add a new key to that section for EnableCredSSPForWinRM and set it to true. For example:  

```
<add key="EnableCredSSPForWinRM" value="true" />
```
5. Restart the "Secret Server Agent" service to apply the setting.

Windows integrated authentication allows Active Directory users that are synced with SS to log into workstations and be automatically authenticated to the application. A user's Active Directory credentials are automatically passed through to IIS, logging them into the site.

For further information, Microsoft has a [knowledge base article](#) troubleshooting some common client-side issues with integrated authentication.

## Enabling Integrated Windows Authentication

Active Directory integration and synchronization must be enabled before configuring integrated Windows authentication:

1. Navigate to **Administration > Active Directory**.
2. Click **Edit**.
3. Check the Enable Integrated Windows Authentication box.
4. Click **Save**.

## Configuring IIS

Open IIS and highlight your SS website or application. In the right pane, double-click **Authentication**. Enable Windows Authentication and disable **Anonymous Authentication**.

**Note:** For additional information on requirements and troubleshooting, see our [KB article on Integrated Windows Authentication](#).

## Logging on As a Local Account

After you have set up integrated Windows authentication, you may sometimes want to log in as a local admin account to configure SS, perform an upgrade, or if AD is down.

1. Log on your computer as an Active Directory account that has read access to the SS application directory but is not enabled in SS.
2. Browse to SS using Firefox or Chrome.
3. Go to your SS website. You may be prompted for your AD credentials. If you are, log on as a user with read access to the SS application directory that is not enabled in SS. You should then be redirected to the log on page of SS.
4. Select the "local" domain and enter your local account username and password.

## Configuring Integrated Windows Authentication

**Note:** This article applies to Secret Server 10.6 and later.

### Introduction

Integrated Windows Authentication (IWA) allows users to log into SS automatically if they are logged into a workstation with their Active Directory credentials.

**Note:** When using IWA, see [Using Mobile Devices with Windows Authentication Enabled](#) to connect mobile applications to SS.

**Note:** [Secure LDAP](#) only works with Integrated Windows Authentication in Server 2008 R2 and later.

**Important:** Customers using the IWA need to perform a workaround when upgrading to SS 10.6 with a distributed engine. Please see "[Task 4: Configuring Distributed Engines](#)."

### Setting Up Windows Authentication

#### Task 1: Configuring Secret Server

1. Log into SS as a user with Active Directory administration privileges.
2. Navigate to **Administration > Active Directory**:

Active Directory Configuration	
Active Directory Integration	
Enable Active Directory Integration	Yes
Enable Integrated Windows Authentication	No
Active Directory User Synchronization	
Enable Synchronization of Active Directory	Yes
Synchronization Interval for Active Directory	1 hour
User Account Options	User status mirrors Active Directory (Automatic)
<a href="#">Back</a> <a href="#">Edit</a> <a href="#">Edit Domains</a> <a href="#">Edit Synchronization</a> <a href="#">View Audit</a>	

3. Click the **Edit** button. The Edit Active Directory Configuration page appears:

**Edit Active Directory Configuration**

Active Directory Integration

Enable Active Directory Integration ☒

Enable Integrated Windows Authentication ☐ Requires advanced IIS settings (See [KB Article](#))

Active Directory User Synchronization

Enable Synchronization of Active Directory ☒ Enable to synchronize users by Active Directory Group

Synchronization Interval for Active Directory

Days: 0

Hours: 1

Minutes: 0

User Account Options: User status mirrors Active Directory (Automatic) v

Save Cancel

4. If necessary, click to select the following check boxes:
  - o Enable Active Directory Integration
  - o Enable Synchronization of Active Directory
  - o Enable Integrated Windows Authentication.
5. Select your desired option from the **User Account Options** dropdown list.
6. Type the in the **Days**, **Hours**, and **Minutes** text boxes to choose a synchronization interval, which is how often SS pulls in users from AD.
7. Click the **Save** button. The Active Directory Configuration page reappears:

**Active Directory Configuration**

Active Directory Integration

Enable Active Directory Integration Yes

Enable Integrated Windows Authentication Yes

Active Directory User Synchronization

Enable Synchronization of Active Directory Yes

Synchronization Interval for Active Directory 1 hour

User Account Options User status mirrors Active Directory (Automatic)

Back Edit Edit Domains Edit Synchronization View Audit

8. Click the **Edit Domains** button. The Active Directory Domains page appears:

**Active Directory Domains**

Save To File < 1 to 1 of 1 >

Domain	Friendly Name	Active	Login Enabled	Use LDAPS
testparent.thycotic.com	TestParent	Yes	Yes	No

[Back](#)
[+ Create New](#)

- Click the **Create New** button. The Active Directory Domain page appears:

**Active Directory Domain**

**Credentials**

Fully Qualified Domain Name \*

Friendly Name \*

Active ☒

Allow Logins From Domain ☒

Sync Secret No Selected Secret [Create New Secret](#)

Site Local

Enable Discovery Not Enabled Discovery is not enabled and will not be run. To enable it, go to the Discovery section under Administration.

[Advanced \(not required\)](#)

[Save And Validate](#)
[Cancel](#)

- Type the domain name for single-sign-on in the **Fully Qualified Domain Name** text box.
- Type the human-friendly name in the **Friendly Name** text box.
- Click the **Save and Validate** button. The Active Directory Configuration page reappears:

**Active Directory Configuration**

Active Directory Integration

Enable Active Directory Integration Yes

Enable Integrated Windows Authentication Yes

Active Directory User Synchronization

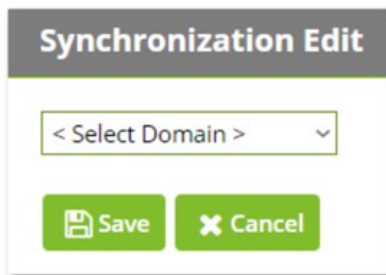
Enable Synchronization of Active Directory Yes

Synchronization Interval for Active Directory 1 hour

User Account Options User status mirrors Active Directory (Automatic)

[Back](#)
[Edit](#)
[Edit Domains](#)
[Edit Synchronization](#)
[View Audit](#)

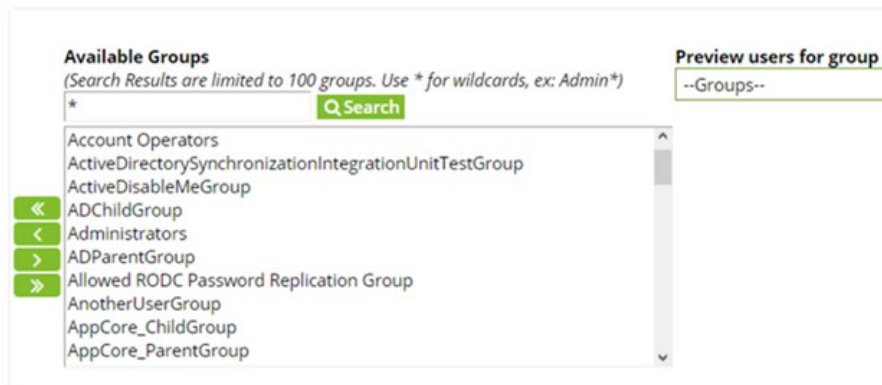
- Click the **Edit Synchronization** button. The Synchronization Edit page appears:



- Click the dropdown list to select the desired domain. The page changes to show the groups for that domain:



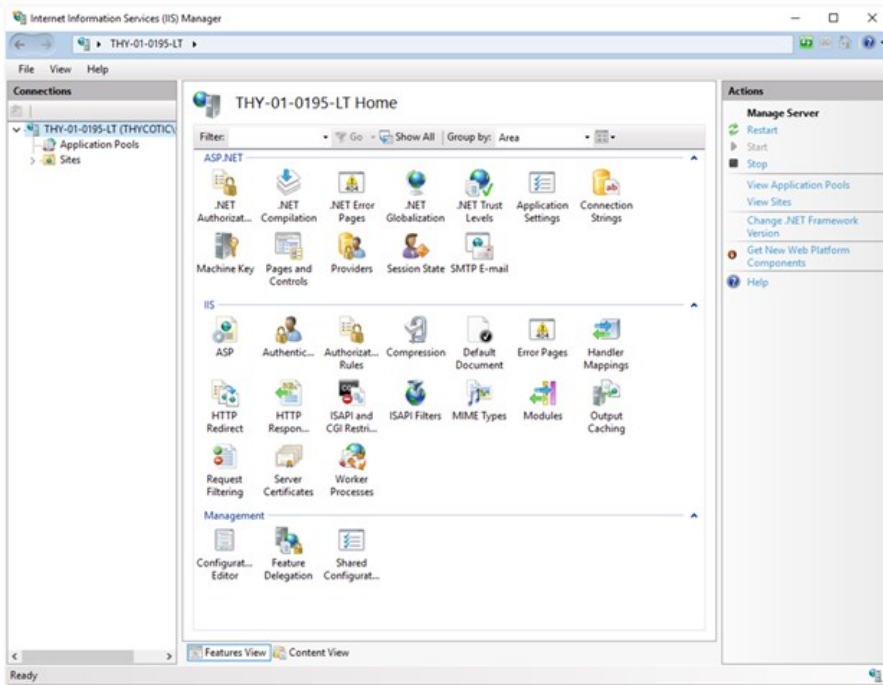
- Use the **Available Groups** text box and **Search** button to locate your desired groups. The matching groups appear in the list:



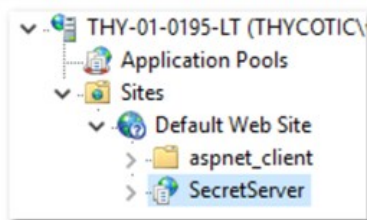
- Select the desired groups and click the < < button to move them into the **Synchronized Groups** list.
- Click the **Save** button. The Active Directory Configuration page reappears.
- Click the **Synchronize Now** button in the **Messages** section. This pulls all the users of the specified groups into SS.

## Task 2: Configuring IIS

- Start the Internet Information Services (IIS) Manager:



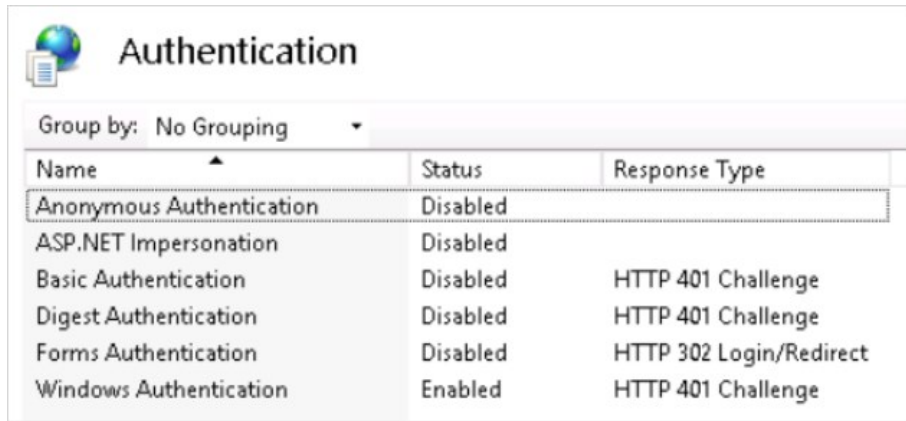
2. Navigate to and select your SS website in the **Connections** tree:



3. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.
4. Enable the **Windows Authentication** parameter by right-clicking it and selecting **Enable**. For now, ignore the alert if it appears in the Alert section.

**Note:** If Windows Authentication is not visible, ensure that the Windows Authentication Role service is enabled in Windows. This is different than earlier versions.

5. Disable the **Anonymous Authentication**.
6. Disable the **Forms Authentication**. The alert in the Alert section should disappear.
7. When finished, the Authentication settings should look like this:

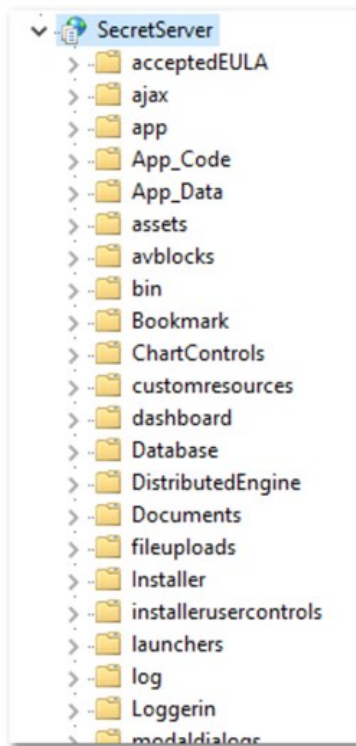


8. Restart your IIS server with an `iisreset` command.
9. On the SS folder, ensure users have read or higher permission, and ensure the security settings are set to be inherited by child objects. Because SS impersonates those users, they require access to SS files.
10. Log in to the SS site from an authenticated workstation.

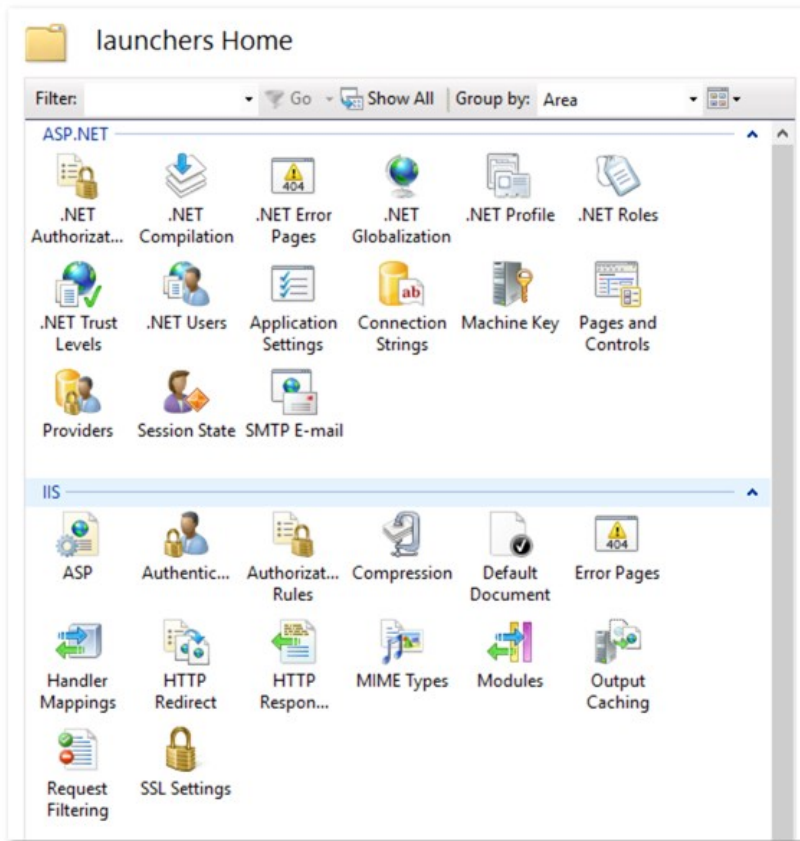
### Task 3: Configuring Secret Server Launchers

By default, a launcher will not work when using IWA, resulting in an HTTP 401: Unauthorized error. If this is an issue, ensure SS is on Windows Server 2008 or later and complete the following steps:

1. Open IIS and browse to your SS application.
2. Click the ► to see the application's folders:



3. Click to select the **launchers** folder. The launchers Home panel appears:

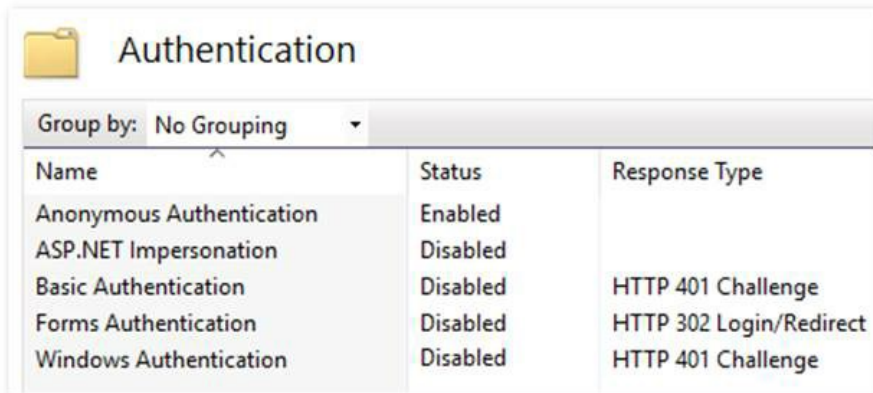


4. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.
5. Ensure the **Anonymous Authentication** is set to **Enabled**.
6. Ensure the **Windows Authentication** is set to **Disabled**.
7. Ensure all others are disabled. When you are finished, the settings should look like this:

Authentication		
Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

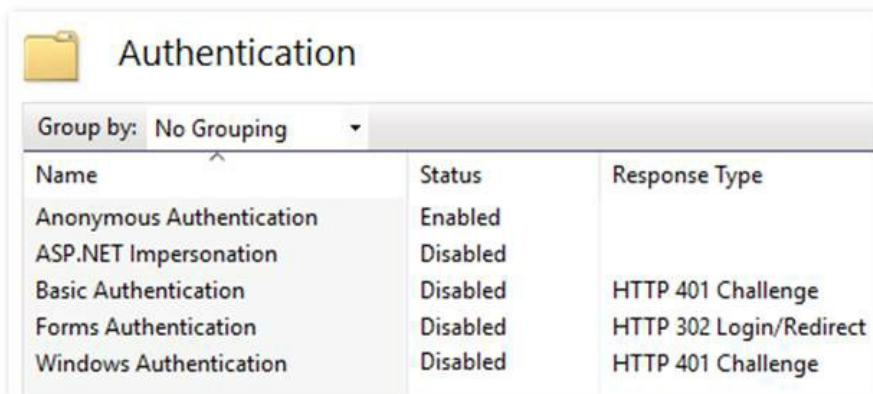
8. Click the **webservices** folder.
9. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.

10. Ensure the **Anonymous Authentication** is set to **Enabled**.
11. Ensure the **Windows Authentication** is set to **Disabled**.
12. Ensure all others are disabled. When you are finished, the settings should look like this:



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

13. Click the **rdp** folder.
14. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.
15. Ensure the **Anonymous Authentication** is set to **Enabled**.
16. Ensure the **Windows Authentication** is set to **Disabled**.
17. Ensure all others are disabled. When you are finished, the settings should look like this:

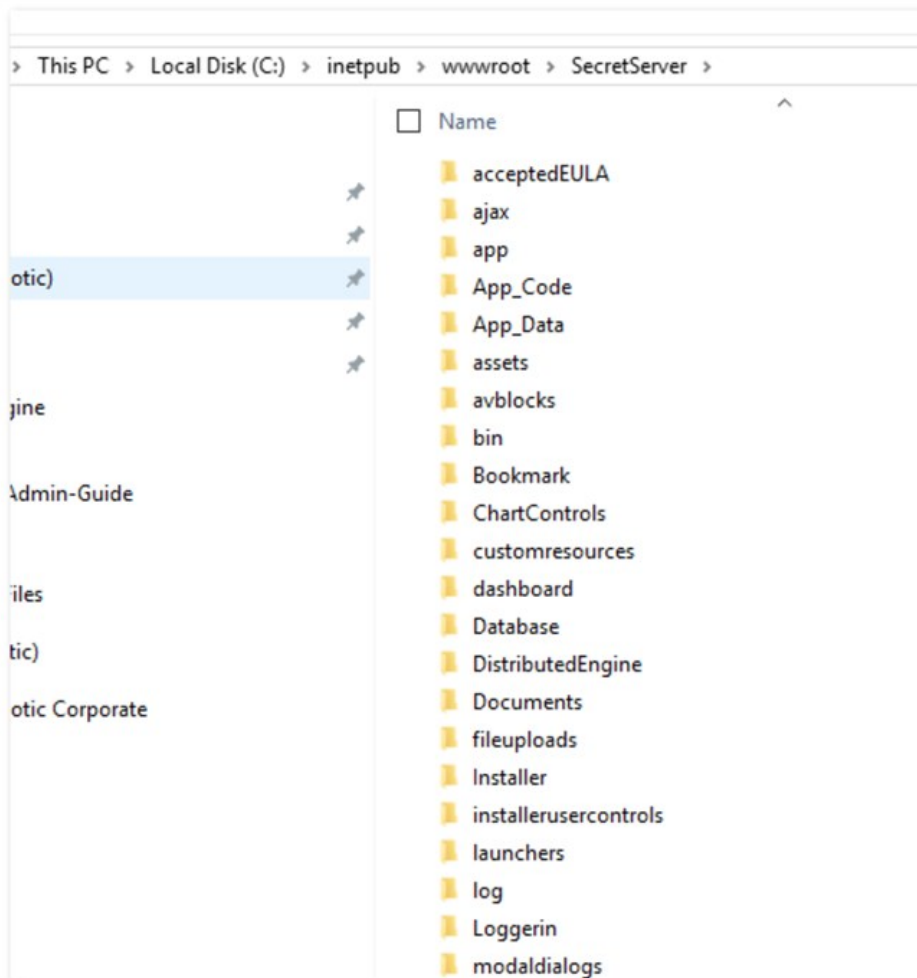


Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

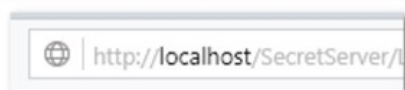
## Task 4: Configuring Distributed Engines

Similarly, SS with distributed engines will not work with IWA by default. If this is an issue, complete the following:

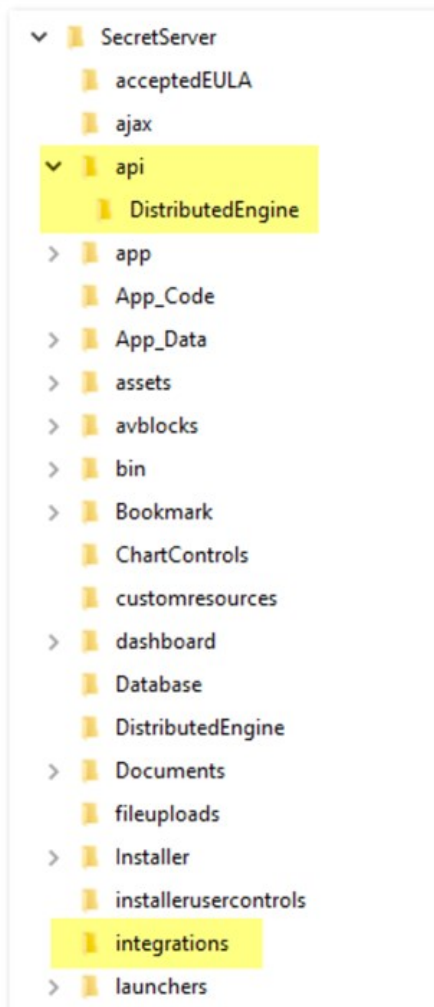
1. In Windows Explorer, navigate to the ...\\SecretServer\ folder:



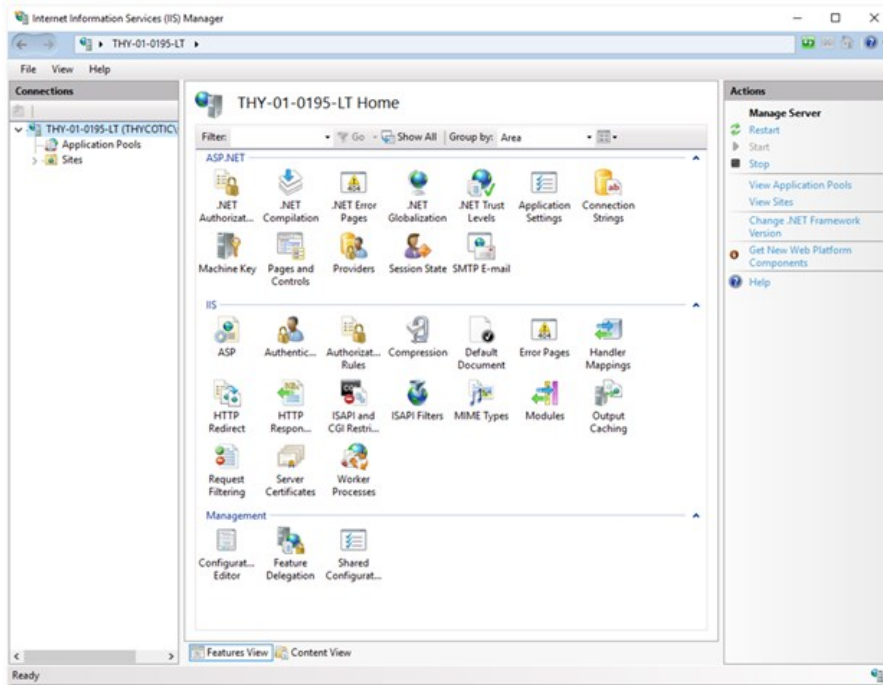
This folder is mapped to your SecretServer folder in your webserver:



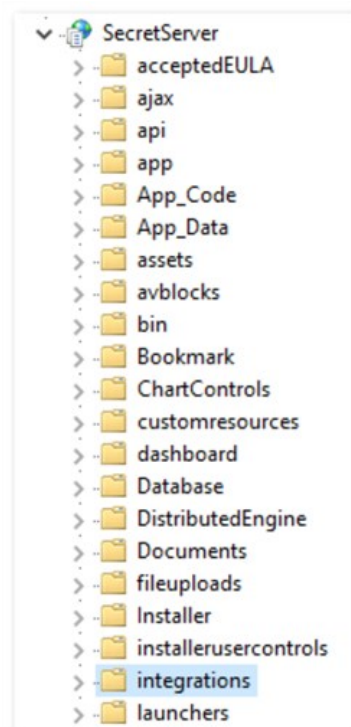
2. Create a subfolder named ...\\SecretServer\\integrations.
3. Create a subfolder called ...\\SecretServer\\api in the same location.
4. In your ...\\SecretServer\\api folder, create a subfolder named ...\\SecretServer\\api\\DistributedEngine.
5. When you are finished, the new folders appear as follows:



6. Start IIS Manager:



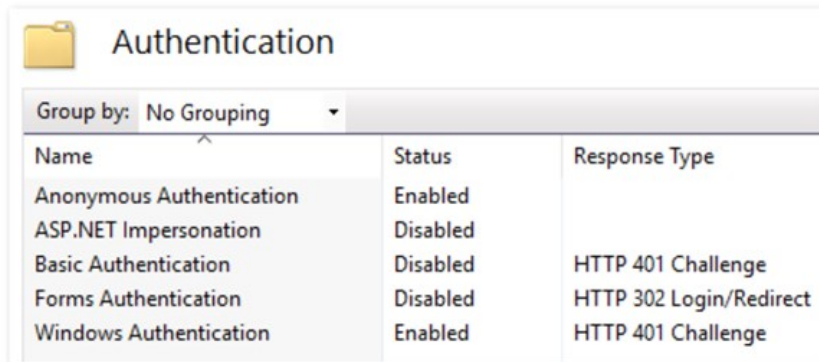
7. Navigate the **Connections** tree back to **integrations** folder in the **SecretServer** node:



8. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.

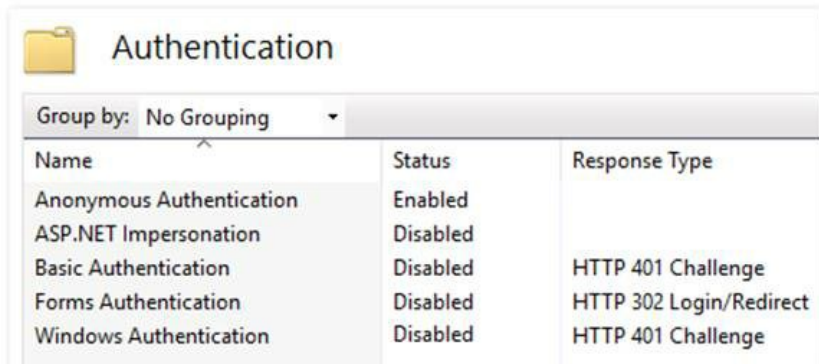
9. Ensure the **Anonymous Authentication** is set to **Enabled**.

10. Ensure the **Windows Authentication** is set to **Enabled**.
11. Ensure all others are disabled. When you are finished, the settings should look like this:



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

12. Navigate to the ...\\SecretServer\\api\\DistributedEngine folder.
13. Double-click the **Authentication** icon in the **IIS** section to open the **Authentication** pane.
14. Ensure the **Anonymous Authentication** is set to **Enabled**.
15. Ensure the **Windows Authentication** is set to **Disabled**.
16. Ensure all others are disabled. When you are finished, the settings should look like this:

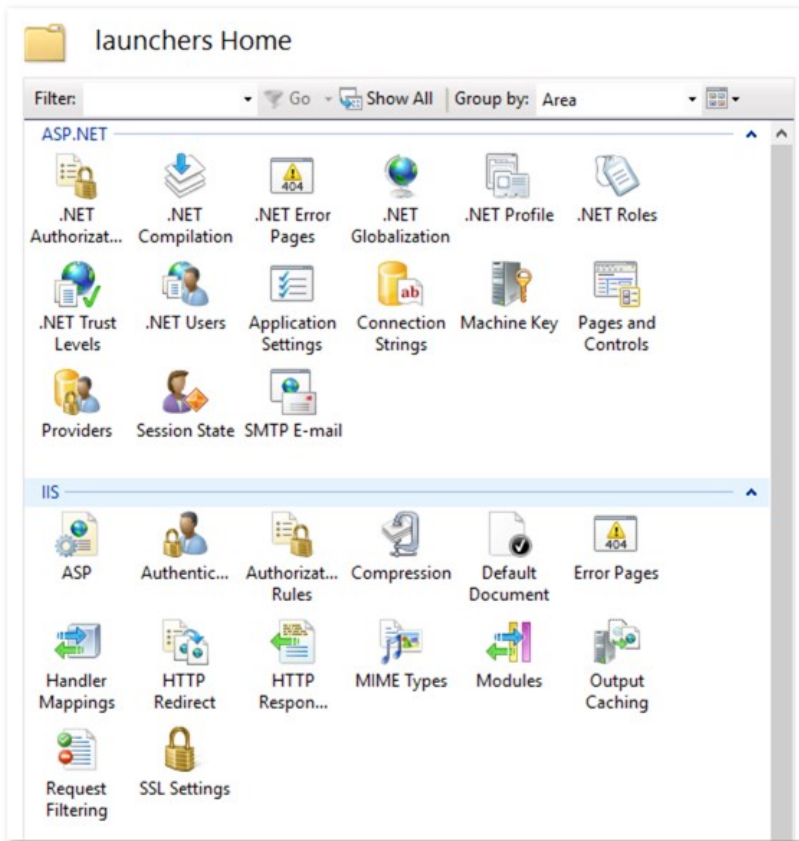


Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

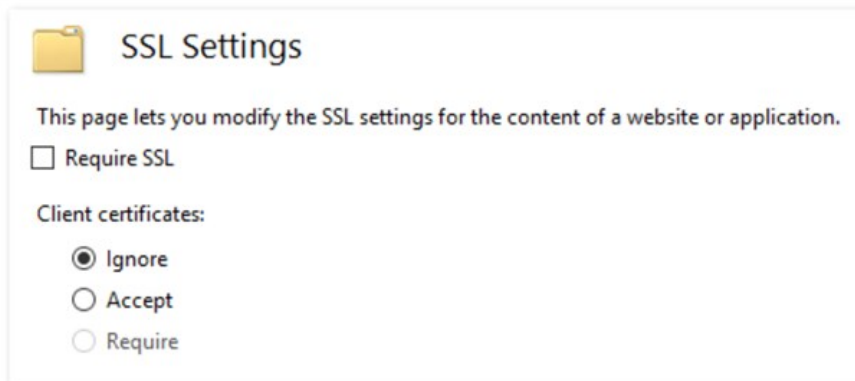
## Task 5: Configuring Client Certificates

If you are using client certificates, configure the following in IIS for launchers to work:

1. Click to select the **launchers** folder. The launchers Home panel appears:



2. Double-click the **SSL Settings** icon. The settings panel appears:



3. Click to set the **Client Certificates** selection button to **Accept**.
4. Click to select the **Webservices** folder.
5. Once again, double-click the **SSL Settings** icon.
6. This time, set the **Client Certificates** selection button to **Ignore**.

**Note:** If you are not automatically logged in to SS after setting up IWA, IIS may not be handling the credentials correctly. To fix this, recreate the web site in IIS.

**Note:** When testing IWA, keep in mind the requirements at [Internet Explorer May Prompt You for a Password](#).

**Note:** You may not be able to log in using IWA on the server running SS for Server 2008 or later because of security settings.

## Troubleshooting

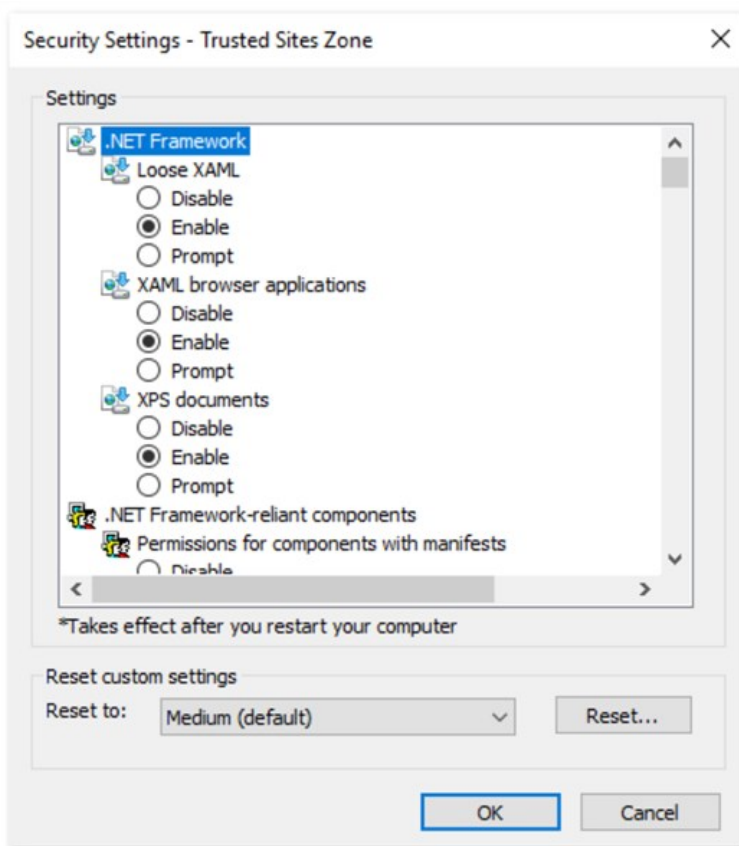
### Error "403 Forbidden" Message Is Displayed When Logging In

See the KB article [Integrated Windows Authentication Problem after Upgrading to Secret Server 10+](#).

### AD User Prompted for Credentials Even Though IWA Is Active

A user is logged onto their machine with the same Active Directory credentials they can log into SS with, but the browser still prompts them for their credentials to reach the site. Ensure your SS site is included in a security zone that allows for automatic logon:

1. In Internet Explorer, go to Internet **Options > Security**.
2. Click the **Trusted Sites** security zone.
3. Click the **Custom Level** button. The Security Settings – Trusted Sites Zone dialog box appears:



1. Scroll down to **User Authentication**.
2. Click to select the **Automatic logon with current user name and password** selection button.
3. Click the **OK** button.

### Logging in as a Local Account Is Not Available

In SS 10.0 and later, SS requires Integrated Mode in IIS. The Integrated Mode can only support either Window Authentication or Forms Authentication (used for local account authentication), not both. Because of this limitation, Forms Authentication must be disabled for the site when using Integrated Windows Authentication. Thus, logging in as SS local account is not available when IWA is enabled.

## Installing Windows Authentication in Windows Server 2012 Manager

1. In Server Manager, click the **Manage** menu and select **Add Roles and Features**. The Add Roles and Features wizard appears.
2. Click the **Next** button. The Select installation type window appears.
3. Select the installation type.
4. Click the **Next** button. The Server selection window appears.
5. Select the destination server.
6. Click the **Next** button. The Server roles window appears.
7. Click to expand **Web Server (IIS) > Web Server > Security**.
8. Click to select **Windows Authentication**.
9. Click the **Next** button. The Select features window appears.
10. Click the **Next** button. The Confirmation window appears.
11. Click the **Install** button. The Results window appears.
12. Click the **Close** button.

SS provides the option to integrate your SAML implementation to automatically authenticate users to the application:

- To configure SAML for versions 10.5+, see the [SAML 2.0 Configuration Guide](#).
- To configure SAML for versions 10.2-10.4, see the [SAML Configuration Guide for Secret Server 10.2-10.4](#).

## Overview

You can specify a secret to provide the default credentials for running all PowerShell scripts on a site. This allows sites in different data centers to have different default credentials. This applies to remote password changing, checkout hooks, and account discovery PowerShell scripts.

**Note:** If you want a specific secret checkout hook, secret password changer, or account discovery scanner to use different credentials you can still provide credentials in those areas, which will take precedence over the one set on the site.

## RunAs Secret Precedence

### Remote Password Changing

The precedence order for which RunAs secret to use for remote password changing is:

1. Privileged account on the secret RPC tab
2. Secret site's RunAs secret
3. Secret

### Secret Dependencies

The precedence order for which RunAs secret to use for PowerShell Secret dependencies is:

1. Privileged account on the dependency
2. Run As secret on the dependency group's site
3. Secret site's RunAs secret
4. Secret

### Checkout Hooks

The precedence order for which RunAs secret to use for checkout hooks is:

1. Privileged account on the hook
2. Secret site's RunAs secret
3. Secret

## Procedures

### Setting the Default PowerShell Credential for a Site

To set a default PowerShell credential for a site:

1. Go to **Admin > Distributed Engines > Manage Sites**.
2. Select the desired site.
3. Click **Edit**.

4. Click the secret picker link on the **Default PowerShell RunAs Secret** field.
5. Click **Save**.

## Using the Site PowerShell Credentials for Discovery

To use the site PowerShell credentials on a discovery scanner:

1. Add a PowerShell scanner to a discovery source or edit an existing scanner.
2. In the **Edit** dialog for the scanner, click to select the **Use Site RunAs Secret** checkbox.
3. Click **Save**.

**Note:** If no RunAs secret is set on the site, you will get an error message when you try to save.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server supports a second layer of authentication, called multi-factor authentication (MFA) or two-factor authentication (2FA), for added security. This section discusses several options.

## Duo Security Authentication

**Note:** Using this method of two-factor authentication requires that you have an active account for Duo Security.

**Note:** SS supports using Duo Security as a second factor of authentication. See below for setup instructions.

Note: For more information on Duo and Secret Server, see the [Thycotic Secret Server and Duo](#) page.

### Task 1: Create a Duo Application Representing Your Secret Server (Admin)

1. Sign up for a new Duo account, or log in to an existing one at [Duo Security](#).
2. Under **Applications**, create a new application of the **Thycotic Secret Server** type. Name the application as you wish.
3. Record the API hostname, integration key, and secret key from the new Duo application you just created.

### Task 2: Configure Secret Server to Use Duo (Admin)

**Note:** Because Duo is a service, the SS instance must have outbound access (TCP port 443) to reach the API host to work. If there is a firewall rule preventing access to Duo's servers, two factor authentication will not work.

1. Open SS.
2. From the **Admin** menu, select **Configuration**.
3. Click the **Login** tab, and then click **Edit**.
4. Select the **Enable Duo Integration** check box.
5. Enter the **API Hostname**, **Integration Key**, and **Secret Key** values.
6. Click the **Save** button.
7. Go to **Admin > Users** to create a test user. The Users page appears.
8. Click the **Create New** button. The **Edit User** page appears:

## Edit User

User Name

Display Name

Email Address

Domain

Local

▼

Password

Confirm

Two Factor

< None >

▼

Enabled

☒

Locked Out

☐

[Advanced](#)

Save

Cancel

9. Click the **Two Factor** dropdown list and select **Duo**.
10. Type or select the other parameters for the new user. See [Users](#).
11. Log on as the test user. If there are multiple two-factor devices available, you will be prompted to select one. If you are un-enrolled you will be given a link to perform self-enrollment. You are contacted via the Duo app, SMS, or a phone call for the second factor.
12. Add or configure actual users one at a time or by using bulk operations.

### Task 3: Setting up Duo (User)

1. Log on to SS.
2. After successful authentication, a new screen appears with the option to select a method to authenticate with.
3. Select one of the options (**Duo Push**, **Send SMS**, or **Phone**), depending on your setup with Duo) and complete the selected authentication process to log in.

## Email Two-Factor Authentication

SS requires that a connection to a SMTP server be properly configured to send out confirmation code emails. Enter the SMTP server information and an email address that is used to send notifications:

1. Click **Admin > Configuration**.
2. Click the **Email** tab.
3. Verify SMTP server availability with telnet using the command `telnet <your server name> 25`.

**Note:** If virus protection is running, you may need to add a firewall rule to allow aspnet\_wp.exe to send e-mails.

## FIDO2 (YubiKey) Two-Factor Authentication Configuration

### FIDO2

FIDO2 (Fast Identity Online, second edition) is an open authentication standard that uses physical devices for authentication. Thycotic uses it for two factor authentication (2FA) with FIDO2 providing the second authentication after a normal password entry—any FIDO2-enabled user attempting access to a SS account **must** have a FIDO2 device in hand. The device eliminates many password-related issues, such as phishing and man-in-the-middle attacks. It also speeds up the long on process over callback or texting 2FA.

### YubiKey

YubiKey is a FIDO2-compliant product series from Yubico, a commercial company. We recommend two of their devices--YubiKey 5 Series and Security Key by Yubico.

### Configuration

See [FIDO2 \(YubiKey\) Two-Factor Authentication Configuration](#) for details.

## RADIUS User Authentication

SS allows the use of *Remote Authentication Dial-In User Service* (RADIUS) two-factor authentication on top of the normal authentication process for additional security needs. SS acts as a RADIUS client that can communicate with any server implementing the RADIUS protocol.

### Configuring RADIUS

Set up RADIUS on the **Login** tab of the **Configuration** page. This requires enabling RADIUS Integration, specifying the server address, the ports, and the RADIUS shared secret. The shared secret is a specific term for RADIUS clients and is not a reference to secrets in SS.

You can customize the RADIUS "Login Explanation" to give users detailed instructions for entering their RADIUS information.

Once enabled, the **Test RADIUS Login** button appears on the **Login** tab for testing the communication with the RADIUS Server. If you have a failover RADIUS Server, you can specify it by clicking the **Enable RADIUS Failover** checkbox and entering the required information. If the primary RADIUS server cannot be accessed, the failover server is be used.

### Enabling RADIUS for a User

After enabling RADIUS on your SS, you must enable RADIUS two-factor authentication for each user on a per-user basis. On the **User Edit** page, type the **RADIUS User Name** for this user to match the RADIUS server. RADIUS can be enabled for new users by domain, see [Adding Domains](#).

## Enabling RADIUS Two-Factor Authentication

Secret Server allows the use of RADIUS two-factor authentication on top of the normal authentication process for additional security.

See the full [RADIUS Integration Guide](#) for additional information.

To configure RADIUS for the SS instance:

1. Log on SS with an account with "Administer Configuration" and "Administer RADIUS" permissions.
2. Navigate to **Administration menu > Configuration > Login**.
3. Click the **Edit** button.
4. Type the following:

- **RADIUS Server IP** (IP address to your RADIUS Server)
- **RADIUS Client Port** (default 1812)

**Note:** If your RADIUS server runs on the same machine as SS, the client and server ports must be different.

- **RADIUS Server Port** (default 1812 for RSA and 1812 for AuthAnvil).
- **RADIUS Shared Secret**, which must match chosen RADIUS shared secret on your RADIUS Server. (Shared Secret is a RADIUS term and not related to any Secret Server secret.)
- **RADIUS Login Explanation** (custom message or instruction). Defaults to "Please enter your RADIUS passcode."

5. Click the **Save** button.

To test RADIUS settings:

1. Click the **Test RADIUS Login** button. A popup appears.
2. Type the RADIUS username and password.
3. Click the **OK** button.
4. After enabling RADIUS on SS, you must enable RADIUS two-factor authentication for each user:
  1. Sign into an account with "Administer Configuration" and "Administer RADIUS" permissions.
  2. Navigate to **Administration > Users**. The Users page appears.
  3. Select the desired user.
  4. Click the **Edit** button.
  5. Click to select the **RADIUS Two Factor Authentication** check box.
  6. Type the username in the **RADIUS Username** text box.

**NOTE:** Secret Server defaults this value to its username. If you wish to use this default name, it must match the username on the RADIUS server.

7. Review the settings and click **Save**.
8. Repeat these steps for each user that needs to use RADIUS.

## TOTP

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS supports using any type of soft token or mobile app authentication using the *Time-Based One-Time Password* (TOTP) RFC6238 algorithm. TOTP's are usually generated by a mobile app using an algorithm that incorporates the current time to ensure that each one-time password (OTP) is unique. This includes Google Authenticator and Microsoft Authenticator. In addition, SS can be an OTP generator, allowing for TOTP authentication for RPC and launchers.

## Configuring TOTP for Users

## Disabling TOTP for Users

To disable soft token two-factor authentication, follow almost the same process as enabling soft token two-factor authentication for a user, select **Disable TOTP Auth Two Factor** from the bulk operation drop-down menu instead of **Enable TOTP Auth Two Factor**.

## Enabling TOTP for Secret Server Users

1. From the **Admin** menu, select **Users**.
2. Select the check box beside each user to enable two-factor authentication for.
3. From the **< Select Bulk Operation >** drop-down menu, select **Enable TOTP Auth Two Factor**.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user(s) are now required to complete the soft token setup with a mobile device the next time they log into SS. See **User Setup of Soft Token Two-Factor Authentication** for details on the account and mobile app setup that follow.

## Enabling TOTP for Launchers

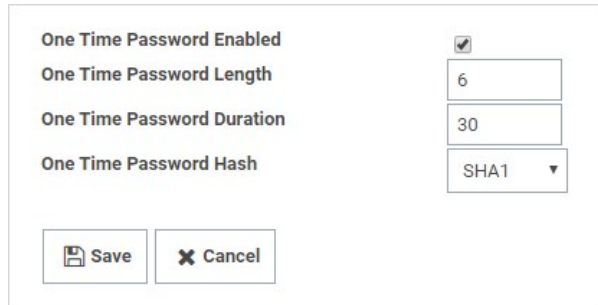
Most commonly, time-sensitive one-time passwords (TOTPs) are generated by a mobile application, such as Google Authenticator or Microsoft Authenticator. Additionally, SS can be used as the TOTP generator for RPC or launchers (for web password secrets only at this time). Both the secret and the secret template require configuration for this use.

### Secret Template Setup

To enable TOTP on a SS template:

1. Go to **Admin > Secret Template**.
2. Select the desired template, and click the **Edit** button. The Secret Template Designer appears.
3. Navigate to the **Settings** section of the page, and click **Edit**.
4. Click to select the **One Time Password Enabled** check box. This enables the option with default settings:

Length: 6 Duration: 30 Hash: SHA1



The screenshot shows a configuration window for a secret template. It contains four settings: 'One Time Password Enabled' with a checked checkbox, 'One Time Password Length' with a text input field containing '6', 'One Time Password Duration' with a text input field containing '30', and 'One Time Password Hash' with a dropdown menu showing 'SHA1'. At the bottom, there are two buttons: 'Save' and 'Cancel'.

One Time Password Enabled	<input checked="" type="checkbox"/>
One Time Password Length	6
One Time Password Duration	30
One Time Password Hash	SHA1 ▼

**Note:** These are the values that most one-time password instances, such as Google and Microsoft Authenticator, use today. If you use these settings with another OTP provider and are unable to successfully use generated codes to authenticate, please review their documentation and adjust these settings as required.

5. Save the secret template. Any web password secret based upon this template can now use TOTP.

### TOTP Secret Setup

Once a secret template is set up for TOTP, each secret based on that template also needs to be set up:

1. Click the **Secrets** menu item in the dashboard.
2. Open the desired secret.
3. Click the **Settings** tab:

Thycotic Web Password ☆

General
Security
Audit
RPC
Dependencies
Sharing
Settings

EMAIL NOTIFICATIONS - PERSONALIZED USER SETTINGS

Send Email When Viewed

No

Send Email When Changed

No

Send Email When Heartbeat Fails

No

TIME-BASED ONE-TIME PASSWORD (TOTP)

Generate One-Time Passwords

☐

Cancel
Save

- Click to select the **Generate One-Time Passwords** check box in the **TOTP** section. This exposes two text boxes:

Generate One-Time Passwords

☒

TOTP Key \*

.....

Show

TOTP Backup Codes

.....

Show

Cancel
Save

- Type the TOTP key in the **TOTP Key** text box. The TOTP Key is generated by the OTP-protected asset when you set up your account to use TOTP. Usually, you are prompted with a QR bar code that you can scan with a mobile device, or you can expose the key that the QR code represents. This text string is the value that is placed into the TOTP Key field.

**Important:** Treat the TOTP key and backup codes like you would any other password! If anyone obtains the key, it can be used to set up a valid TOTP generator for that account on any device, allowing that person to bypass the protection. Similarly, the backup codes allow users to temporarily bypass protection.

**Note:** If you have an account that has been TOTP protected and you did not save the TOTP key upon creation, you must

deactivate TOTP on that account and then reactivate it to retrieve the TOTP key to set up SS.

6. Type the TOTP backup codes in the **TOTP Backup Codes** text box. The TOTP Backup Codes are often presented to a user while initially setting up an account for TOTP. These backup codes are single-use codes for use if a TOTP generator is not available or working. Again, these codes will be valid and allow the holder to get past the two-factor authorization to access an account, so protect them as you would a password!

## Resetting TOTP for Secret Server Users

1. From the **Admin** menu, select **Users**.
2. Select the check box beside the user to reset two-factor authentication for.
3. Click select **Reset TOTP Auth Two Factor** on the **< Select Bulk Operation >** drop-down menu.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user is now required to complete the soft token setup with a mobile device the next time they log into SS. See **User Setup of Soft Token Two-Factor Authentication** for further details on the account and mobile app setup that follow.

## Viewing a TOTP for a Web Secret

To view or copy the TOTP generated for an account:

1. Navigate to and open the desired secret.
2. Click the **General** tab:

Thycotic Web Password ☆

General
Security
Audit
RPC
Dependencies
Sharing
Settings

Secret Name \*

Thycotic Web Password

Edit

Template

Web Password

Edit

URL \*

http://www.thycotic.com

Edit

UserName \*

myUserName


Edit

Password \*

\*\*\*\*\* Show

Edit


One Time Password


Generate One Time Password

Notes

Edit


Launchers


Web Password Filler

Show Advanced
Edit all fields

3. Click the **Generate One Time Password** link next to the **One Time Password** setting.
4. A dialog box appears with an OTP:

One Time Password for Thycotic Web Password

754 544


Click the One Time Password to copy to clipboard

Close

1. Click the OTP to copy it to the clipboard.
2. Click the **Close** button.

**Note:** The "Generate One Time Password" link also appears on the preview pane when you click a secret on the All Secrets page.

## Backup and Disaster Recovery

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS supports manual and scheduled database and IIS directory backups. The database access settings support SQL mirror and automatic failover. As an additional disaster recovery measure, administrators can export secrets to a CSV spreadsheet.

Secret Server can be configured to backup to a network share instead of a local folder on the server. For example, you may want to do this such as when the SS database (SQL) is located on a different server than the web application server (IIS).

To back up:

1. Ensure the SS IIS Application Pool is running as a service account if it is not already. See [Running the IIS Application Pool As a Service Account](#).
2. Grant access to the network share (using Windows ACLs) to the account running the SS IIS Application Pool (so that SS can backup the application folder and zip it to the network share).
3. Grant access to the network share (using Windows ACLs) to the account running Microsoft SQL Server service. (so that Microsoft SQL Server can backup the SS database to the network share). You can change the service account running Microsoft SQL Server by going to SQL Server Configuration Manager.
4. Go to **Admin > Backup**. This may require you to go to **Admin > All** and search for **Backup**.

### Backup Configuration

The AppPool running Secret Server must be configured to not shutdown. See the following KB Article.  
Secret Server is currently running as "GAMMA\ss\_iis\_svc", you will need to grant Full Control to the backup folder specified for this user.

To backup to a network share, see the following KB Article.

Enable Web Application Backup	Yes
Backup File Path	c:\backup
Enable Database Backup	Yes
Backup Database File Path	c:\backup
Database Backup SQL Timeout (Minutes)	30
Enable Copy-Only Database Backups	No
Keep Number of Backups	10
Notify Administrators on backup failure	No
Enable Scheduled Backup	Yes
Backup Start Time	5/15/2019 10:18 AM
Backup Every	1 days 0 hours 0 minutes
Next Scheduled Backup	5/28/2020 10:18 AM
Enable TMS Backup	No
TMS Installation Path	

← Back
 Edit
 View Audit
 Backup Now

5. Note that the two file paths are from two different perspectives—Backup File Path is from the ASP.NET application server and Backup Database Path is from the Microsoft SQL Server (these may be on the same box in your environment, or they might not be depending on how you have configured SS).
6. Click the **Edit** button.
7. Type the SS backup path, such as \\server01\backup\secretserver\, in the **Backup File Path** text box.
8. Type the database backup path in the **Backup Database Path** text box.
9. Click the **Save** button.

From the Backup Administration page, specify the correct directory paths for the IIS SS file directory and the database backups to be stored. The backup path must be local to the server where the SS database or file directory exists. The directories must also have the proper permissions to allow SS to automatically store backups at those locations. The account that requires permission is displayed as an alert on the Backup page.

## Overview

The following configuration options are available on the **Tools > Backup** page of SS:

- **Backup Database File Path:** This folder must be accessible by the SQL server and stores the database.bak file. See [File Path Settings](#).
- **Backup File Path:** This directory must exist on the Web server and stores the zip file of the application directory. See [File Path Settings](#).
- **Database Backup SQL Timeout (Minutes):** Number of minutes that SS waits for the database backup to complete successfully before timing out.
- **Enable Scheduled Backup:** Enables automatic backups on a set schedule.
- **Keep Number of Backups:** Number of previous backups to keep.
- **Notify Administrators on Backup Failure:** Users with the Administer Backup role permission are notified if the backup fails.
- **Days to Keep Operational Logs:** Sets the period to keep backup-related logs that might contain PII. SS automatically deletes logs older than that (in days).

## File Path Settings

There are two file path settings on the **Admin > Backup** page (ConfigurationBackup.aspx). The "Backup File Path" setting corresponds to the application backup. The "Backup Database Path" setting corresponds to the SQL server backup.

Generally, the "Backup File Path" setting can be set to a path local to the application server for backing up of application files. If SS is running under an account that does not have permission to write to a local path, then a network share can be used. If the SQL server is located on the same server as the Web application server, the "Backup Database File Path" setting can be set to a local path.

If the SQL server is not located on the same server as the Web application server then a network share should be used. The account under which SQL server service is running either must have modify rights to that path or must be a member of a group with modify rights to that path. You must use UNC (Universal Naming Convention) notation to write to a network path. For example: \\TESTVM0\\c\$\\backupDirectory.

If you get an error stating "Cannot open backup device... Operating system error 3," this is often due to an invalid path value.

**Note:** For SS to delete old database backups, the backup database path must also be accessible by the SS Application Pool account.

## **Cannot open backup device... Operating system error 3**

This is often due to an invalid path value for the "Backup Database File Path" setting. For more information on the proper values for this setting, see [File Path Settings](#).

## **Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.**

This is often due to an overly-large database. The SS database likely contains too many log entries. To clear these, within SS, select System Log from the Administration menu. Click the "Clear" button below the data grid that contains the log entries. If the timeout occurs with the clear as well, an upgrade to the latest version should resolve this. If the timeout issue persists with the backup, additional SQL database clean-up may be necessary. Contact [Thycotic Support](#) for instructions on shrinking the reserve database size.

## **The process cannot access the file... because it is being used by another process**

The cause of this message is typically multiple backup threads running simultaneously with all attempting to write to the same file. To fix this, open IIS Manager and ensure the "Maximum Worker Processes" setting for SS's application pool is set to 1. If it is not, set the value to 1 and then either recycle the application pool or perform an `iisreset`.

## **Unable to complete backup. The following exception occurred: System.Threading.ThreadAbortException: Thread was being aborted**

If this error message appears in combination with the application backup files not completed or the size of the file is unusually small, the backup process may have been interrupted by anti-virus software. Disabling scanning of the backup folder should resolve the issue.

Also see: [Backing up Secret Server to a network share](#) (KBA)

Files uploaded to secrets can be backed up using the standard SS backup function. Upon backup completion, they retain their encrypted status and are inside the application backup file (the .zip file).

To back up your SS installation:

**Note:** Your SS instance may be running during this procedure.

1. Navigate to the directory where SS is installed.
2. Copy the folder (holding the application) to your back up location.
3. Open your SQL Server Management Studio.
4. Right click the database your SS is running on, and select **Tasks > Backup**.
5. Click the **Add** button. You will be prompted to enter a file path.
6. Make sure SQL Server has permissions for this location.
7. Copy the resulting database backup file to your backup location.

**Note:** You can also automate steps 2-4 using the command: `osql -S myserver\SQLEXPRESS -E - Q "BACKUP DATABASE SECRETSERVER TO DISK = 'c:\backup\ss.bak' .`

## Overview

As of SS 10.7.59, the SS MessageQueue Client attempts to create RabbitMQ durable exchanges, logging the activity. A durable exchange is normally automatically re-created if RabbitMQ restarts for any reason. Any legacy non-durable exchanges disappear when RabbitMQ goes down and can only be manually recreated.

If the MessageQueue client detects that creating a durable exchange failed, it will log an error and attempt to create a non-durable one.

**Important:** Any existing non-durable exchanges, from previous versions of SS, will also cause durable exchange creation to fail.

See [Manually Creating Durable RabbitMQ Exchanges](#).

Non-durable RabbitMQ exchanges for SS would look similar to this, whether created by an earlier SS version or by a durable-version-creation failure:

Overview	Connections	Channels	Exchanges	Queues	Admin
<b>Exchanges</b>					
▼ All exchanges (10)					
Pagination					
Page 1 of 1 - Filter: <input type="text"/> <input type="checkbox"/> Regex ?					
Name	Type	Features	Message rate in	Message rate out	+/-
(AMQP default)	direct	D			
amq.direct	direct	D			
amq.fanout	fanout	D			
amq.headers	headers	D			
amq.match	headers	D			
amq.rabbitmq.trace	topic	D I			
amq.topic	topic	D			
thycotic-sr-agent-response	topic		0.00/s	0.00/s	
thycotic-ss	topic		0.00/s	0.00/s	
thycotic-ss-engine-response	topic				

Note the absence of a 'D' in the Features column, meaning that exchange is not durable. Durable exchanges, created by the current SS version (10.7.59+), look like this:

The screenshot shows the 'Exchanges' tab in the RabbitMQ management interface. It displays a table of 11 exchanges. The table has columns for Name, Type, Features, Message rate in, Message rate out, and a +/- toggle. The exchanges listed are: (AMQP default), amq.direct, amq.fanout, amq.headers, amq.match, amq.rabbitmq.trace, amq.topic, thycotic-sessionrec, thycotic-sr-agent-response, thycotic-ss, and thycotic-ss-engine-response. The 'thycotic-ss' exchange shows a message rate of 0.20/s in and out.

Name	Type	Features	Message rate in	Message rate out	+/-
(AMQP default)	direct	D			
amq.direct	direct	D			
amq.fanout	fanout	D			
amq.headers	headers	D			
amq.match	headers	D			
amq.rabbitmq.trace	topic	D I			
amq.topic	topic	D			
thycotic-sessionrec	topic	D	0.00/s	0.00/s	
thycotic-sr-agent-response	topic				
thycotic-ss	topic	D	0.20/s	0.20/s	
thycotic-ss-engine-response	topic	D			

Earlier versions of SS (before 10.7.59) created non-durable RabbitMQ exchanges during a SS server or IIS restart. If the environment is clustered, the same is true of every node in that cluster. The current durable exchanges persist during any IIS restart, eliminating the need to restart SS or recreate the exchanges.

However, any existing non-durable exchanges prevent the creation of the newer durable ones. To remedy that, you need to restart all of the RabbitMQ servers in the cluster at the same time or manually delete the non-durable exchanges.

## Manually Creating Durable RabbitMQ Exchanges

To enjoy the benefits of the durable exchanges, you must first eliminate any legacy non-durable exchanges from your RabbitMQ server or servers. There are two ways to do this:

- Restart the RabbitMQ server or all of the RabbitMQ servers in the cluster at the same time. You can also stop the RabbitMQ service in services.msc.

**Note:** Customers usually reset or turn off all servers via third party tools, but some prefer to shut off the service via services.msc because of their system configuration.

- Delete the exchanges manually:
  - Click to select each SS non-durable exchange, including distributed engine ones.
  - Scroll to the bottom of the window.
  - Click the **Delete** button.
  - Restart all of the SS instances and distributed engines to recreate the exchanges and connections.

## Creating Durable RabbitMQ Exchanges with a PowerShell Script

### Using the Script

```
powershell.exe -file exchangedurability.ps1 -username "guest" -password "guest" -computerName "localhost" -port "15672"
```

The user has access to the RabbitMQ admin interface. The computername and port is where the admin interface is located.

The script:

1. Removes all of the exchanges that are not durable and any that are not the `thycotic-sr` ones for legacy ASRAs.
2. Kills all of the connections. This forces the distributed engines and SS to reconnect to the durable exchanges.

## Script

```
param([string] $computerName = "",
      [string] $userName = "",
      [string] $password = "",
      [string] $port = ""
)

$defaultComputerName = if ($computerName -eq "") { "localhost" } else { $computerName }
$defaultVirtualHost = "/"
$defaultUserName = if ($userName -eq "") { "guest" } else { $userName }
$defaultPassword = if ($password -eq "") { "guest" } else { $password }
$defaultPort = if ($port -eq "") { "15672" } else { $port }
$defaultHttp = "http" #Use https if ssl

$defaultCredentials = New-Object System.Management.Automation.PSCredential ($defaultUserName, $(ConvertTo-SecureString $defaultPassword -AsPlainText -Force))

#LICENSE FOR LINKS - All the RabbitMQ PowerShell calls are based on this:
#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/LICENSE
#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/GetConnection.ps1

function Get-RabbitMQConnection
{
    [CmdletBinding(DefaultParameterSetName='defaultLogin', SupportsShouldProcess=$true, ConfirmImpact='None')]
    Param
    (
        # Name of RabbitMQ Connection.
        [parameter(ValueFromPipeline=$true, ValueFromPipelineByPropertyName=$true)]
        [Alias("Connection", "ConnectionName")]
        [string[]]$Name = "",

        # Name of the computer hosting RabbitMQ server. Default value is localhost.
        [parameter(ValueFromPipelineByPropertyName=$true)]
        [Alias("HostName", "hn", "cn")]
        [string]$ComputerName = $defaultComputerName,

        # Username to use when logging to RabbitMQ server.
        [Parameter(Mandatory=$true, ParameterSetName='login')]
        [string]$UserName,

        # Password to use when logging to RabbitMQ server.
        [Parameter(Mandatory=$true, ParameterSetName='login')]
        [string]$Password,

        # Credentials to use when logging to RabbitMQ server.
        [Parameter(Mandatory=$true, ParameterSetName='cred')]
        [PSCredential]$Credentials
    )

    Begin
    {
        $Credentials = NormaliseCredentials
    }
    Process
    {
        if ($pscmdlet.ShouldProcess("server $ComputerName", "Get connection(s): $(NamesToString $Name 'all)'))
        {
            $result = GetItemsFromRabbitMQApi -ComputerName $ComputerName $Credentials "connections"

            $result = ApplyFilter $result 'name' $Name

            $result | Add-Member -NotePropertyName "ComputerName" -NotePropertyValue $ComputerName

            SendItemsToOutput $result "RabbitMQ.Connection"
        }
    }
}
```

```

    }
    End
    {
    }
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/PreventUnEscapeDotsAndSlashesOnUri.ps1
if (-not $UnEscapeDotsAndSlashes) { Set-Variable -Scope Script -name UnEscapeDotsAndSlashes -value 0x2000000 }
function GetUriParserFlags {

    $getSyntax = [System.UriParser].GetMethod("GetSyntax", 40)
    $flags = [System.UriParser].GetField("m_Flags", 36)

    $parser = $getSyntax.Invoke($null, "http")
    return $flags.GetValue($parser)
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/PreventUnEscapeDotsAndSlashesOnUri.ps1
function SetUriParserFlags([int]$newValue) {
    $getSyntax = [System.UriParser].GetMethod("GetSyntax", 40)
    $flags = [System.UriParser].GetField("m_Flags", 36)

    $parser = $getSyntax.Invoke($null, "http")
    $flags.SetValue($parser, $newValue)
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/PreventUnEscapeDotsAndSlashesOnUri.ps1
function PreventUnEscapeDotsAndSlashesOnUri {
    if (-not $UriUnEscapesDotsAndSlashes) { return }

    Write-Verbose "Switching off UnEscapesDotsAndSlashes flag on UriParser."

    $newValue = $defaultUriParserFlagsValue -bxor $UnEscapeDotsAndSlashes

    SetUriParserFlags $newValue
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/PreventUnEscapeDotsAndSlashesOnUri.ps1
function RestoreUriParserFlags {
    if (-not $UriUnEscapesDotsAndSlashes) { return }

    Write-Verbose "Restoring UriParser flags - switching on UnEscapesDotsAndSlashes flag."

    try {
        SetUriParserFlags $defaultUriParserFlagsValue
    }
    catch [System.Exception] {
        Write-Error "Failed to restore UriParser flags. This may cause your scripts to behave unexpectedly. You can find more at get-help about_UnEscapingDotsAndSlashes."
        throw
    }
}

if (-not $defaultUriParserFlagsValue) { Set-Variable -Scope Script -name defaultUriParserFlagsValue -value (GetUriParserFlags) }
if (-not $UriUnEscapesDotsAndSlashes) { Set-Variable -Scope Script -name uriUnEscapesDotsAndSlashes -value (($defaultUriParserFlagsValue -band $UnEscapeDotsAndSlashes) -eq $UnEscapeDotsAndSlashes) }

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/Invoke_RestMethodProxy.ps1
function Invoke-RestMethod {
    [CmdletBinding(HelpUri = 'http://go.microsoft.com/fwlink/?LinkID=217034')]
    param(
        [Microsoft.PowerShell.Commands.WebRequestMethod]
        ${Method},

        [Parameter(Mandatory = $true, Position = 0)]
        [ValidateNotNullOrEmpty()]
        [uri]
        ${Uri},

        [Microsoft.PowerShell.Commands.WebRequestSession]
        ${WebSession},

        [Alias('SV')]
        [string]
        ${SessionVariable},

```

```

[pscredential]
${Credential},

[switch]
${UseDefaultCredentials},

[ValidateNotNullOrEmpty()]
[string]
${CertificateThumbprint},

[ValidateNotNull()]
[System.Security.Cryptography.X509Certificates.X509Certificate]
${Certificate},

[string]
${UserAgent},

[switch]
${DisableKeepAlive},

[int]
${TimeoutSec},

[System.Collections.IDictionary]
${Headers},

[ValidateRange(0, 2147483647)]
[int]
${MaximumRedirection},

[uri]
${Proxy},

[pscredential]
${ProxyCredential},

[switch]
${ProxyUseDefaultCredentials},

[Parameter(ValueFromPipeline = $true)]
[System.Object]
${Body},

[string]
${ContentType},

[ValidateSet('chunked', 'compress', 'deflate', 'gzip', 'identity')]
[string]
${TransferEncoding},

[string]
${InFile},

[string]
${OutFile},

[switch]
${PassThru},

[switch]
${AllowEscapedDotsAndSlashes})

begin {
    try {
        $outBuffer = $null
        if ($PSBoundParameters.TryGetValue('OutBuffer', [ref]$outBuffer)) {
            $PSBoundParameters['OutBuffer'] = 1
        }

        $wrappedCmd = $ExecutionContext.InvokeCommand.GetCommand('Microsoft.PowerShell.Utility\Invoke-RestMethod',
[System.Management.Automation.CommandTypes]::Cmdlet)

        # check whether need to disable UnEscapingDotsAndSlashes on UriParser
        $requiresDisableUnEscapingDotsAndSlashes = ($AllowEscapedDotsAndSlashes -and $Uri.OriginalString -match '%2f')

        # remove additional proxy parameter to prevent original function from failing
    }
}

```

```

        if ($PSBoundParameters['AllowEscapedDotsAndSlashes']) { $null = $PSBoundParameters.Remove('AllowEscapedDotsAndSlashes') }

        $scriptCmd = { & $wrappedCmd @PSBoundParameters }
        $steppablePipeline = $scriptCmd.GetSteppablePipeline($myInvocation.CommandOrigin)
        $steppablePipeline.Begin($PSCmdlet)
    }
    catch {
        throw
    }
}

process {
    try {
        # Disable UnEscapingDotsAndSlashes on UriParser when necessary
        if ($requiresDisableUnEscapingDotsAndSlashes) {
            PreventUnEscapeDotsAndSlashesOnUri
        }

        $steppablePipeline.Process($_)
    }
    finally {
        # Restore UnEscapingDotsAndSlashes on UriParser when necessary
        if ($requiresDisableUnEscapingDotsAndSlashes) {
            RestoreUriParserFlags
        }
    }
}

end {
    try {
        $steppablePipeline.End()
    }
    catch {
        throw
    }
}
}
<#
.FowardHelpTargetName Invoke-RestMethod
.FowardHelpCategory Cmdlet
#>

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/GetRabbitMQCredentials.ps1
function GetRabbitMQCredentials {
    Param
    (
        [parameter(Mandatory = $true)]
        [string]$userName,

        [parameter(Mandatory = $true)]
        [string]$password
    )

    $secpasswd = ConvertTo-SecureString $password -AsPlainText -Force
    return New-Object System.Management.Automation.PSCredential ($userName, $secpasswd)
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/NamesToString.ps1
function NamesToString {
    Param
    (
        [string[]]$name,
        [string]$saltText = ""
    )

    if (-not $name) { return $saltText }

    return $name -join ','
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/ApplyFilter.ps1
function ApplyFilter {
    Param (
        [parameter()]
        [PSObject[]]$items,

```

```
[parameter(Mandatory = $true)]
[string]$prop,

[string[]]$name
)

if (-not $name) { return $items }

# apply property filter
$filter = @()
foreach ($n in $name) { $filter += '$_' + $prop + '-like "' + $n + '"' }

$sb = [scriptblock]::create($filter -join ' -or ')
return $items | ? $sb
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/NormaliseCredentials.ps1
function NormaliseCredentials() {
    switch ($PsCmdlet.ParameterSetName) {
        "defaultLogin" { return GetRabbitMqCredentials $defaultUserName $defaultPassword }
        "login" { return GetRabbitMqCredentials $UserName $Password }
        "cred" { return $Credentials }
    }
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/SendItemsToOutput.ps1
function SendItemsToOutput {
    Param
    (
        [parameter()]
        [PSObject[]]$items,

        [parameter(Mandatory = $true)]
        [string[]]$typeName
    )

    foreach ($i in $items) {
        $i.PSObject.TypeNames.Insert(0, $typeName)
        Write-Output $i
    }
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/GetItemsFromRabbitMQApi.ps1
function GetItemsFromRabbitMQApi {
    [CmdletBinding(DefaultParameterSetName = 'login')]
    Param
    (
        [parameter(Mandatory = $true, ParameterSetName = 'login', Position = 0)]
        [string]$cn,

        [parameter(Mandatory = $true, ParameterSetName = 'login', Position = 1)]
        [string]$userName,

        [parameter(Mandatory = $true, ParameterSetName = 'login', Position = 2)]
        [string]$password,

        [parameter(Mandatory = $true, ParameterSetName = 'login', Position = 3)]
        [string]$fn,

        [parameter(Mandatory = $true, ParameterSetName = 'cred', Position = 0)]
        [string]$computerName,

        [parameter(Mandatory = $true, ParameterSetName = 'cred', Position = 1)]
        [PSCredential]$cred,

        [parameter(Mandatory = $true, ParameterSetName = 'cred', Position = 2)]
        [string]$function
    )

    Add-Type -AssemblyName System.Web
    #Add-Type -AssemblyName System.Net

    if ($PsCmdlet.ParameterSetName -eq "login") {
```

```

$computerName = $cn
$cred = GetRabbitMqCredentials $userName $password
$function = $fn
}
Write-Output $computerName
$url = $defaultHttp + "://" + ([System.Web.HttpUtility]::UrlEncode($computerName)):$defaultPort/api/$function
Write-Verbose "Invoking REST API: $url"

return Invoke-RestMethod $url -Credential $cred -DisableKeepAlive -AllowEscapedDotsAndSlashes
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/GetExchange.ps1
function Get-RabbitMQExchange {
    [CmdletBinding(DefaultParameterSetName = 'defaultLogin', SupportsShouldProcess = $true, ConfirmImpact = 'None')]
    Param
    (
        # Name of RabbitMQ Exchange.
        [parameter(ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true)]
        [Alias("ex", "Exchange", "ExchangeName")]
        [string[]]$Name = "",

        # Name of RabbitMQ Virtual Host.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [Alias("vh")]
        [string]$VirtualHost = "",

        # Name of the computer hosting RabbitMQ server. Default value is localhost.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [Alias("HostName", "hn", "cn")]
        [string]$ComputerName = $defaultComputerName,

        # Username to use when logging to RabbitMQ server.
        [Parameter(Mandatory = $true, ParameterSetName = 'login')]
        [string]$UserName,

        # Password to use when logging to RabbitMQ server.
        [Parameter(Mandatory = $true, ParameterSetName = 'login')]
        [string]$Password,

        # Credentials to use when logging to RabbitMQ server.
        [Parameter(Mandatory = $true, ParameterSetName = 'cred')]
        [PSCredential]$Credentials
    )

    Begin {
        $Credentials = NormaliseCredentials
    }
    Process {
        if ($?cmdlet.ShouldProcess("server $ComputerName", "Get exchange(s): $(NamesToString $Name '(all)')")) {
            $exchanges = GetItemsFromRabbitMQApi -ComputerName $ComputerName $Credentials "exchanges"

            $result = ApplyFilter $exchanges 'vhost' $VirtualHost
            $result = ApplyFilter $result 'name' $Name

            $result | Add-Member -NotePropertyName "ComputerName" -NotePropertyValue $ComputerName

            SendItemsToOutput $result "RabbitMQ.Exchange"
        }
    }
    End {
    }
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/RemoveExchange.ps1
function Remove-RabbitMQExchange {
    [CmdletBinding(DefaultParameterSetName = 'defaultLogin', SupportsShouldProcess = $true, ConfirmImpact = "High")]
    Param
    (
        # Name of RabbitMQ Exchange.
        [parameter(Mandatory = $true, ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true, Position = 0)]
        [Alias("Exchange", "ExchangeName")]
        [string[]]$Name,

        # Name of RabbitMQ Virtual Host.
        [parameter(ValueFromPipelineByPropertyName = $true)]

```

```
[Alias("vh", "vhost")]
[string]$VirtualHost = $defaultVirtualhost,

# Name of the computer hosting RabbitMQ server. Defalut value is localhost.
[parameter(ValueFromPipelineByPropertyName = $true)]
[Alias("HostName", "hn", "cn")]
[string]$ComputerName = $defaultComputerName,

# Username to use when logging to RabbitMq server.
[Parameter(Mandatory = $true, ParameterSetName = 'login')]
[string]$UserName,

# Password to use when logging to RabbitMq server.
[Parameter(Mandatory = $true, ParameterSetName = 'login')]
[string]$Password,

# Credentials to use when logging to RabbitMQ server.
[Parameter(Mandatory = $true, ParameterSetName = 'cred')]
[PSCredential]$Credentials
)

Begin {
    $Credentials = NormaliseCredentials
    $cnt = 0
}
Process {
    if ($pscmdlet.ShouldProcess("server: $ComputerName, vhost: $VirtualHost", "Remove exchange(s): $(NamesToString $Name '(all)')")) {
        foreach ($n in $Name) {
            $url = $defaultHttp +
                "://$([System.Web.HttpUtility]::UrlEncode($ComputerName)):$defaultPort/api/exchanges/$([System.Web.HttpUtility]::UrlEncode($VirtualHost))/$([System.Web.HttpUtility]::UrlEncode($n))"
            Write-Output $url
            $result = Invoke-RestMethod $url -Credential $Credentials -AllowEscapedDotsAndSlashes -DisableKeepAlive -ErrorAction Continue -Method Delete

            Write-Verbose "Deleted Exchange $n on server $ComputerName, Virtual Host $VirtualHost"
            $cnt++
        }
    }
}
End {
    if ($cnt -gt 1) { Write-Verbose "Deleted $cnt Exchange(s)." }
}

#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/AddExchange.ps1
function Add-RabbitMQExchange {
    [CmdletBinding(DefaultParameterSetName = 'defaultLogin', SupportsShouldProcess = $true, ConfirmImpact = "Medium")]
    Param
    (
        # Name of RabbitMQ Exchange.
        [parameter(Mandatory = $true, ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true, Position = 0)]
        [Alias("Exchange", "ExchangeName")]
        [string[]]$Name,

        # Type of the Exchange to create.
        [parameter(Mandatory = $true, ValueFromPipelineByPropertyName = $true)]
        [ValidateSet("topic", "fanout", "direct", "headers")]
        [string]$Type,

        # Determines whether the exchange should be Durable.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [switch]$Durable,

        # Determines whether the exchange will be deleted once all queues have finished using it.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [switch]$AutoDelete,

        # Determines whether the exchange should be Internal.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [switch]$Internal,

        # Allows to set alternate exchange to which all messages which cannot be routed will be send.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [Alias("alt")]
        [string]$AlternateExchange,
    )
}
```

```

# Name of RabbitMQ Virtual Host.
[parameter(ValueFromPipelineByPropertyName = $true)]
[Alias("vh", "vhost")]
[string]$VirtualHost = $defaultVirtualHost,

# Name of the computer hosting RabbitMQ server. Defalut value is localhost.
[parameter(ValueFromPipelineByPropertyName = $true)]
[Alias("HostName", "hn", "cn")]
[string]$ComputerName = $defaultComputerName,

# UserName to use when logging to RabbitMq server.
[Parameter(Mandatory = $true, ParameterSetName = 'login')]
[string]$UserName,

# Password to use when logging to RabbitMq server.
[Parameter(Mandatory = $true, ParameterSetName = 'login')]
[string]$Password,

# Credentials to use when logging to RabbitMQ server.
[Parameter(Mandatory = $true, ParameterSetName = 'cred')]
[PSCredential]$Credentials
)

Begin {
    $Credentials = NormaliseCredentials
}
Process {
    if ($pscmdlet.ShouldProcess("server: $ComputerName, vhost: $VirtualHost", "Add exchange(s): $(NamesToString $Name '(all)')")) {

        $body = @{}
        $body.type = "$Type"

        if ($Durable) { $body.Add("durable", $true) }
        if ($AutoDelete) { $body.Add("auto_delete", $true) }
        if ($Internal) { $body.Add("internal", $true) }
        if ($AlternateExchange) { $body.Add("arguments", @{ "alternate-exchange" = $AlternateExchange }) }

        $bodyJson = $body | ConvertTo-Json

        foreach ($n in $Name) {
            $url =
$defaultHttp+":"/{([System.Web.HttpUtility]::UrlEncode($ComputerName))}:$defaultPort/api/exchanges/{([System.Web.HttpUtility]::UrlEncode($VirtualHost))}/{([System.Web.H
ttpUtility]::UrlEncode($n))}"
            Write-Verbose "Invoking REST API: $url"

            $result = Invoke-RestMethod $url -Credential $Credentials -AllowEscapedDotsAndSlashes -DisableKeepAlive -ErrorAction Continue -Method Put -ContentType
"application/json" -Body $bodyJson

            Write-Verbose "Created Exchange $n on server $ComputerName, Virtual Host $VirtualHost"
            $cnt++
        }
    }
}
End {
    if ($cnt -gt 1) { Write-Verbose "Created $cnt Exchange(s)." }
}
}

#Modified to allow + in url.
#https://github.com/mariuszwojcik/RabbitMQTools/blob/master/RemoveQueue.ps1
function Remove-RabbitMQConnection {
    Param
    (
        # Name of RabbitMQ connection.
        [parameter(Mandatory = $true, ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true, Position = 0)]
        [Alias("ConnectionName")]
        [string] $Name = "",

        # Name of the computer hosting RabbitMQ server. Defalut value is localhost.
        [parameter(ValueFromPipelineByPropertyName = $true)]
        [Alias("HostName", "hn", "cn")]
        [string]$ComputerName = $defaultComputerName,

        # Credentials to use when logging to RabbitMQ server.

```

```

[Parameter(Mandatory = $false)]
[PSCredential]$Credentials = $defaultCredentials
)

$url = $defaultHttp + "://" + ([System.Web.HttpUtility]::UrlEncode($ComputerName)):$defaultPort/api/connections/([System.Web.HttpUtility]::UrlEncode($Name))"
$url = $url.Replace("+", "%20")
Write-Output $url
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("X-Reason", "Removing To Create Durable Exchanges")
$result = Invoke-RestMethod $url -Credential $Credentials -Headers $headers -DisableKeepAlive:$InvokeRestMethodKeepAlive -ErrorAction Continue -Method Delete
Write-Output "Url closed."

Write-Verbose "Closed connection $n to server $ComputerName"
}

function MakeExistingExchangesDurable() {
    Param(
        [string] $HostName = $defaultComputerName,
        [string] $UserName = $defaultUserName,
        [string] $Password = $defaultPassword,
        [string] $VirtualHost = "/",
        [bool] $IgnoreConfirms = $false
    )

    $exchanges = Get-RabbitMQExchange
    $nondurableExchanges = New-Object System.Collections.ArrayList
    Foreach ($exchange in $exchanges) {
        if ($exchange.name -and -not ($exchange.durable) -and -not $exchange.name.Contains("thycotic-sr")) {
            $nondurableExchanges.Add($exchange) > $null
        }
    }
    if ($nondurableExchanges.Count -eq 0) {
        Write-Output "All the exchanges are durable."
        return
    }

    Write-Output "r`nFound these exchanges as not durable:"
    Write-Output $nondurableExchanges | ForEach-Object { '{0}' -f $_.Name }

    $confirmation = "
    if ($IgnoreConfirms -eq $false) {
        $confirmation = Read-Host "Are you Sure You Want To Proceed [y/n]"
    }
    if ($confirmation -eq 'y' -or $IgnoreConfirms -eq $true) {
        try {
            Foreach ($nondurableExchange in $nondurableExchanges) {
                Remove-RabbitMQExchange -Name $nondurableExchange.Name -VirtualHost $nondurableExchange.vhost -Confirm:$(-not $IgnoreConfirms)
                Add-RabbitMQExchange -Name $nondurableExchange.Name -Durable:$true -Type $nondurableExchange.type -AutoDelete:$nondurableExchange.auto_delete -
                Internal:$nondurableExchange.Internal -VirtualHost $nondurableExchange.vhost -Confirm:$(-not $IgnoreConfirms)
            }
            $connections = Get-RabbitMQConnection
            Foreach ($connection in $connections) {
                if ($connection.Name)
                {
                    Remove-RabbitMQConnection $connection.Name
                }
            }
        }
        catch {
            throw $_
        }
        Write-Output "Exchanges are now durable."
    }
    else {
        Write-Output "Not going to make the exchanges durable."
    }
}

MakeExistingExchangesDurable -IgnoreConfirms $true

```

To restore your Secret Server from a backup:

## Restoring the Application

1. Extract your backup zip file of the SS application directory, or copy the files from your other backup location to the physical file path that your virtual directory is pointing to.
2. If you have configured encryption of your `encryption.config` using EFS or DPAPI, you will need to replace the file from the backup with the unencrypted one.
3. Check that FIPS mode is not enabled on the server to avoid an error during the process.

## Restoring the SQL Server Database

Choose one of the following scenarios:

### Scenario One: Database and Secret Server Are in the Same Location

1. Open SQL Server Management Studio and connect.
2. Right click **Databases** and click the **Restore Database** button.
3. In the **To database** text box, type the database name or select it from the drop down list.
4. Click to select the **Device** radio button.
5. Browse to your database backup file.
6. In the **Restore Database** window Options section, ensure the **Force Restore over Existing Database** check box is checked.
7. Click the **Ok** button.
8. If you get an error saying that Management Studio was unable to get exclusive access to the database:
  1. Right click on the SS database and go to **Properties**.
  2. At the very bottom, change the **Restrict Access** property to "SINGLE\_USER". This closes all other connections to the SS database.
  3. Re-attempt the restore.
9. Disable **Force SSL** if there is no certificate installed on the server you are restoring to.
10. In SQL Server Management Studio, expand the databases and select the database for SS.
11. Select **New Query** at on the menu bar to open a query pane.
12. Copy the following command: `UPDATE [dbo].[tbConfiguration] SET ForceHttps = 0` into the query pane
13. Click **Execute** on the menu bar.
14. After the query executes successfully, restart Internet Information Server (IIS) by running `iisreset` from the command line.

**Note:** If you are prompted for database credentials when accessing SS and are unable to re-connect, you may need to remap the user.
15. Expand the **Security > Users** folder under the SS database.
16. Remove the user that SS will use to access the database.

17. Expand the **Security > Logins** folder under the SQL Server root.
18. Right click on the log on corresponding to SS and select **User Mappings**.
19. Re-map the log on to the SS database.
20. If necessary, activate your licenses by going to the **Licenses** page.

## Scenario Two: The Database and Secret Server Are in Different Locations

1. Delete the `database.config` file from the SS folder.
2. Restart Internet Information Server (IIS) by running `iisreset` from the command line.
3. Use your Web browser to navigate to the new instance of SS. This redirects you to the Web installer because the `database.config` file is missing and it thinks you have not installed yet.
4. Open SQL Server Management Studio and connect.
5. Right click **Databases** and click the **Restore Database** button.
6. In the **To database** text box, type the database name.
7. Click to select the **Device** radio button.
8. Browse to your database backup file.
9. In the Restore Database window options make sure the Force Restore over Existing Database Check box is checked.
10. Click Ok.
11. If you get an error saying that Management Studio was unable to get exclusive access to the database:
  1. Right click on the SS database and go to **Properties**.
  2. At the very bottom, change the **Restrict Access** property to "SINGLE\_USER". This closes all other connections to the SS database.
  3. Re-attempt the restore.
12. Disable **Force SSL** if there is no certificate installed on the server you are restoring to.
13. Copy the following command: `UPDATE [dbo].[tbConfiguration] SET ForceHttps = 0` into the query pane
14. Click **Execute** on the menu bar.
15. Navigate through the Web installer to Step 3.
16. Type the new database credentials (new server location, username, and password).
17. If you are unable to re-connect you may need to remap the user.

**Note:** If you are prompted for database credentials when accessing SS and are unable to re-connect, you may need to remap the user.
18. Expand the **Security > Users** folder under the SS database.
19. Remove the user that SS will use to access the database.
20. Expand the **Security > Logins** folder under the SQL Server root.

21. Right click on the log on corresponding to SS and select **User Mappings**.
22. Re-map the log on to the SS database.
23. Once past Step 3, you are finished. Go to the home.aspx page (click the Secret Server logo). There is no need to go any further with the install because the database.config has been recreated with the new information.
24. If necessary, activate your licenses by going to the **Licenses** page.

There are numerous options to consider when backing up SS. Backups can be scheduled to run on a specific time interval. To prevent the directory from growing too large, the number of backups to keep can be defined as well. Depending on size constraints or preferences of the DBA, the database backup can either truncate the transaction log or keep it intact. The additional schedule settings are available when "Enable Schedule Backup" is enabled, and the view page indicates the time and date of the next scheduled backup.

SS can run with multiple front-end Web servers. For a critical instance, clustering offers a redundant system to limit potential down time from a single point of failure. Clustering also allows users to load balance for better performance. For instructions on enabling clustering in SS, see [Setting up Clustering](#).

This topic describes the process of configuring Secret Server (SS) and SQL Server for a high-availability environment using Mirroring. The contents of this paper include:

- Configuring SQL Server 2016 for database mirroring with a failover partner and a witness
- The encryption used between the primary database and the mirror database
- Configuring SS to use mirroring to achieve high availability

**Note:** This topic uses SQL Server 2016, but it is very similar to earlier versions.

## Introduction

Three different SQL Server instances are required to implement this scenario:

- **Primary database:** The main application database
- **Mirror database:** Replicates all of the data on the primary database in a transactional manner
- **Witness database:** Monitors the health of the primary and mirror databases and initiates failover if necessary

In the setup described here, mirroring operates in synchronous mode, which means that a transaction does not commit on the primary database until it has committed on the mirror.

**Note:** See [Prerequisites, Restrictions, and Recommendations for Database Mirroring](#) for more on synchronous mirroring:

## Procedures

### Setting up Databases for Mirroring

To initiate database mirroring, the databases on the primary and secondary machines must have the same name. We recommend doing this before installation. To initially set up mirroring, in Microsoft SQL Server Management Studio, take a full backup of the database on the primary and then restore it onto the database on the secondary. When restoring the database, the "RESTORE WITH NORECOVERY" option must be selected.

### SQL Server Configuration

The three SQL Server instances should all be running under the same domain account. It is possible to run under different accounts but the configuration is more complex and not supported by Thycotic technical support. Each SQL Server instance should be configured to listen on TCP.

### Configuring Mirroring

To configure mirroring:

1. In Microsoft SQL Server Management Studio, drill down to the primary database in the Object Explorer.
2. Right click the primary database and select **Properties**. The Database Properties window appears.
3. Select the **Mirror** page.
4. Click on the **Configure Security** button. The Configure Database Mirroring Security Wizard appears on the introduction page.
5. Click the **Next** button. The Include Witness Server page appears.
6. Click to select the **Yes** selection button.
7. Click the **Next** button. The Choose Server to Configure page appears.
8. Click to select all three interface check boxes (principal, mirror, and witness servers).
9. Click the **Next** button. The Principal Server Instance page appears.
10. Click the **Principal server instance** dropdown list to select the current (primary) server.

11. Type a port number for connecting to the other servers in the **Listener port** text box. The port must be open for TCP communication on the machine's firewall and on any network devices that restrict access to this machine.
12. Click to select the **Encrypt data sent through this endpoint** check box. This enables RC4 encryption on data sent through this endpoint.
13. Type `Mirroring` in the **Endpoint name** text box. The endpoint name is for referencing the endpoint later.
14. Click the **Next** button. The Mirror Server Instance page appears.
15. Repeat the exact same configuration you set for the primary server instance with only the server instance name different (choose the mirror instance).
16. Click the **Next** button. The Witness Server Instance page appears.
17. Repeat the exact same configuration you set for the primary server instance with only the server instance name different (choose the witness instance).
18. Click the **Next** button. The Service Accounts page appears.
19. Type the domain user that SQL Server runs under for each instance's Service Accounts text box. For example `mydomain\sql_svc`.
20. Click the **Finish >>** button. Logins are created for each account and are given CONNECT permission on each endpoint, if needed. The Complete the Wizard page appears.
21. Click the **Finish** button.

## Configuring Secret Server for Mirroring

**Note:** The credentials used to access the primary database must also be valid on the mirror database for failover to work.

1. Go to **Admin > See All**. The admin panel appears.
2. Type `Database` in the **Search** text box and select **Database**. The Database Configuration page appears:

## Help

Secret Server supports Microsoft SQL Server versions 2012, 2014, 2016, 2017, and Express.

View [Collation Requirements](#). Need help installing or configuring SQL Server? View [Installing and Configuring SQL KB Article](#).

### Database Configuration

#### SQL SERVER LOCATION

Server Name	QA-CUST-SQL-01
Database	SS_Playground

#### SQL AUTHENTICATION

- ☒ Windows Authentication using Application Identity (GAMMA\ss\_iis\_svc) - **Recommended**  
(Advanced Setting. Windows Authentication requires a Service Account and advanced IIS setup. Detailed in [Windows Authentication KB](#).)
- ☐ SQL Server Authentication (SQL Authentication requires Mixed Mode. See setup in [SQL Authentication KB](#).)

#### [+] ADVANCED (NOT REQUIRED)



Edit



View Audit

3. Click the **Edit** button.
4. Click the **Advanced (Not Required)** link. A new section appears:

[-] ADVANCED (NOT REQUIRED)

SSL Encryption ? ☐ Enable

Trust Server Certificate ☐ Enable

Failover Partner ?

(Requires SQL Server Configuration change)

Multi-Subnet Failover ☐ Enable

(Enabling Multi-Subnet Failover for AlwaysOn Availability Groups requires SQL Server 2012 and higher with AlwaysOn enabled)

Connection Timeout (in seconds)

Save Database Connection Settings

Cancel

- Click the select the **SSL Encryption** check box.
- Type the mirror server name in the **Failover Partner** text box.
- Click the **Save Database Connection Settings** button.

## Testing Mirroring

This procedure is necessary to verify that failover will function correctly in the event that the primary server is unavailable or inoperable:

- Open SQL Server Enterprise Manager.
- Right click the primary database and select **Properties**.
- Click the **Mirroring** tab.
- Click the **Failover Now** button. This causes the database on primary to switch roles and become the mirror database. The mirror database becomes the primary. Clients using the application should be able to continue as before.

**Note:** One request may fail before SS begins making requests to the new primary database.

## Database SSL Configuration

**Note:** See [Enable encrypted connections to the Database Engine](#) for instruction on configuring SSL for SQL Server.

The certificate authority used for the SSL certificates must be trusted on all of the machines that are a part of SS's installation. The SQL Server service account must be granted access to the certificate.

Procedure:

- Open Microsoft Management Console by running `mmc` on the Windows command prompt.
- Drill down to **Console Root > Certificates > Personal > Certificates** in the navigation tree.
- Right click the certificate and select **All Tasks > Manage Private Keys**.

4. Grant the user account that SQL Server uses read permission.
5. Ensure SSL is enabled for both the primary and mirror database server. See [Configuring Secret Server for Mirroring](#). It is not necessary to configure SSL on the witness server.

*Unlimited administration mode* is a feature designed to allow an administrator access to all secrets and folders in their SS instance without explicit permission. This can be used in the instance a company has an emergency where access to a secret is needed when no users who have permission are available. Alternately, it can be used when company policies require administrators to have access to all information in the system.

**Note:** An alert visible to all users displays at the top of the Secret View page when unlimited administration mode is enabled.

For a user to be an unlimited administrator they must be assigned a role with the Unlimited Administrator permission and Unlimited Administration Mode must be enabled in Configuration settings.

To navigate to the **Unlimited Administration** section, select **Configuration** from the **Administration** menu, and then click **Change Administration Mode**. We recommend administrators have specific permissions to folders and secrets and this mode is only used temporarily to assign the correct permissions.

**Note:** Changes to the administration mode are logged in an audit grid. The grid shows the user, time of the change, and any notes made by the user.

## Developer Resources

This topic is a one-stop resource for Secret Server developers. It points to TDP topics, as well as legacy knowledgebase articles. See the main TDP [API and Scripting](#) section too.

- [Custom Reports Gallery](#)
- [Creating Custom Reports](#)
- [Using Dynamic Parameters in Reports](#)
- [Accessing Secret Server—PowerShell](#) (KBA)
- [Configure CredSSP for use with PowerShell](#)
- [Creating and Using PowerShell Scripts](#)
- [Creating and Using SSH Scripts](#) (KBA)
- [Creating and Using SQL Scripts](#) (KBA)
- [Exporting Secrets - PowerShell Export Script](#) (KBA)
- [Password Changing Scripts](#)
- [Searching Secret Server - PowerShell](#) (KBA)
- [Using Secret Fields in Scripts](#)
- [Using Webservices with IWA via PowerShell](#)
- [REST API PowerShell Script Examples](#)
- [REST Web Services API Reference and Download](#)
- [Change SQL service account without restarting the SQL service](#) (KBA)
- [Dependency Token List](#)
- [Understanding Dependency Script Errors for SSH, Powershell and SQL](#) (KBA)
- [PowerShell Dependency to Update the Default Content Access Account for SharePoint](#) (KBA)
- [Downloads for Secret Server Software Development Kit for DevOps](#)
- [Secret Server Software Development Kit for DevOps](#)

- [Thycotic Community GitHub Repository](#)
- [SOAP Web Services API Guide](#) (PDF)
- [SOAP API PowerShell Script Examples](#)

## Directory Services

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Directory (name) services, components of network operating systems, map the names of network resources to their network addresses. Their shared information infrastructure locates, manages, and organizes network resources, which can include volumes, folders, files, users, groups, devices, and much more. Active Directory is Secret Server's native directory service.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server can integrate with Active Directory by allowing users to use their Active Directory credentials to log on Secret Server.

**Note:** Before synchronizing or creating users, you need to create a secret to be used as the "sync secret." This secret should contain Domain Admin credentials (or an account with appropriate permissions to search and view the attributes to all your organization's users and groups).

## Active Directory Rights for Synchronization Account

Below is a listing of the Active Directory permissions required by the account used for synchronization.

### Recommended Permissions

#### Object Tab

This object and all descendant objects:

- List contents
- Read all properties

### Minimum Required Permissions

**Note:** These all require ADSI Edit - Allow (Active Directory Service Interfaces Editor) permission.

#### Object Tab

This object and all descendant objects:

- List contents

#### Properties Tab

This object and all descendant objects:

- Read objectClass

Descendant User objects:

- Read Display Name
- Read Distinguished Name
- Read E-mail-Address
- Read objectGUID
- Read Logon Name
- Read Logon Name (pre-Windows 2000)

Descendant Group objects:

- Read displayName
- Read Distinguished Name
- Read Group name (pre-Windows 2000)
- Read groupAttributes
- Read memberOf
- Read Members
- Read objectGUID

## Configuration Parameters

Active Directory configuration can be enabled by a user with the Administer Active Directory role. To change these settings, select **Active Directory** from the **Administration** menu and then click **Edit**.

The configuration screen offers several options:

- **Enable Active Directory Integration:** Enable or disable the Active Directory Integration feature.
- **Enable Integrated Windows Authentication:** Enable or disable the Windows integrated authentication feature.
- **Enable Synchronization of Active Directory:** Enable or disable the automatic synchronization of the selected Synchronization Groups from Active Directory. If you have manually added users and will not use the Synchronization group, do not enable this setting or manual users can be locked out.
- **Synchronization Interval for Active Directory:** Set the interval that SS synchronizes its users and groups with the Active Directory.
- User Account Options:
- **Users are enabled by default (Manual):** SS users are automatically be enabled when they are synced as new users from Active Directory. If they were disabled explicitly in SS, they are not be automatically re-enabled. If creating a new user causes the user count to exceed your license limit, the user is created as disabled.
- **Users are disabled by default (Manual):** SS users are automatically disabled when they are pulled in as new users from Active Directory. If they were enabled explicitly in SS, they are not automatically re-disabled.
- **User status mirrors Active Directory (Automatic):** When a new user is pulled in from Active Directory, they are automatically enabled if active on the domain. The exception is when this causes you to exceed your license count. For existing users, they are automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They are automatically re-enabled when they are part of a synchronization group and are active in AD.

## Configuring Active Directory

To allow users to log in with their Active Directory (AD) credentials, you can configure your AD domain settings in SS and then add users either individually or by group.

### Step 1: Enabling Active Directory Integration

1. Select **Admin > Active Directory**. The Active Directory Integration page appears.
2. Click the **Edit** button. The Edit Active Directory Configuration page appears.
3. Click to select the **Enable Active Directory Integration** check box.
4. Click the **Save** button.

### Step 2: Adding a Domain

1. Select **Admin > Active Directory**. The Active Directory Integration page appears.
2. Click the **Edit Domains** button. The Active Directory Domains page appears.
3. Click the **Create New** button. The Credentials tab appears.
4. Fill in the domain information and the username and password that will be used for connecting to the domain and synchronizing users and groups.
5. If you wish to use Secure LDAP, enable the **Use LDAPS** checkbox under the **Advanced** section. For more information on Secure LDAP, please see the Using Secure LDAP KB Article.
6. It is possible to set **Automatically enable Two Factor Authentication** for users synchronized from this domain. This option is also available under the **Advanced** section.
7. Click the **Save and Validate** button.

Now you are ready to add individual users or groups of users for access to SS with AD credentials. See the relevant section below for instructions.

### Step 3: Setting Up Synchronization Groups

Once a domain has been added, the **Synchronization Groups** needs to be set by clicking the **Edit Synchronization** button on the **Active Directory Configuration** page. The Available groups represent all accessible groups on the specified Active Directory domain. The user membership can be previewed with the **Group Preview** control. Select the desired group from the available groups that contains the Active Directory accounts for users you would like to create in SS. If the specific group does not exist, one can be created by your Active Directory administrator. If you create domain users manually or converting local users to domain users, then see the corresponding sections below before setting the synchronization group.

1. Click the **Save** button.

### Step 4: Adding Groups

SS can sync with security groups from AD to automatically add, enable, and disable users. This can streamline the process of managing which users are enabled.

**Note:** Enabled users count towards your SS user licensing.

### Step 5: Enabling Active Directory Synchronization

1. From the **Active Directory** page, click the **Edit** button. The Edit Active Directory Configuration page appears.
2. Click to select the **Enable Synchronization of Active Directory** check box. Additional settings appear.
3. Choose how often you want Secret Server to sync with AD by configuring the **Synchronization Interval**. The default value is one day.
4. Click the **User Account Options** Dropdown list to select a default status for users. See below for a description of each option. We recommend selecting **Users are disabled by default (Manual)** for initial testing. The options are:
  - **Users are enabled by default (Manual)**: SS users are automatically enabled when they are synced as new users from AD. If they were disabled explicitly in SS, they are not automatically re-enabled. If creating a new user will cause the user count to exceed your license limit, the user created disabled.
  - **Users are disabled by default (Manual)**: SS users are automatically disabled when they are pulled in as new users from AD. If they were enabled explicitly in SS, they are not automatically re-disabled.
  - **User status mirrors Active Directory (Automatic)**: When new users are pulled in from AD, they are automatically enabled if active on the domain. The exception is when this will cause you to exceed your license count. For existing users, they are automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They are automatically re-enabled when they are part of a synchronization group and are active in AD. See [Understanding Active Directory Automatic User Management](#).
5. Change the **Days to Keep Operational Logs** text box to set the period to keep AD-related logs that might contain PII. SS automatically deletes logs older than that (in days).
6. Click the **Save** button.

## Step 6: Choosing Synchronization Groups

Choose the security groups from AD you want to sync with SS:

1. Go to **Admin > Active Directory**.

## Active Directory Configuration

### ACTIVE DIRECTORY INTEGRATION

Enable Active Directory Integration Yes

Enable Integrated Windows Authentication No

### ACTIVE DIRECTORY USER SYNCHRONIZATION

Enable Synchronization of Active Directory Yes

Synchronization Interval for Active Directory 1 hour

User Account Options Users are disabled by default (Manual)

Advanced (not required)

Automatic User Management No

Months to Wait Before Disabling Users

Days to Keep Operational Logs 30

 Back

 Edit

 Edit Domains

 Edit Synchronization

 View Audit

- Click the **Edit Synchronization** button. The Synchronization Edit page appears:

### Synchronization Edit

< Select Domain > ▾

 Save

 Cancel

- Click the Select Domain dropdown list to choose your domain. More options appear:

### Synchronization Edit

gamma.thycotic.com

#### Synchronized Groups

Developers  
DnsUpdateProxy  
Product Management  
Professional Services  
Protected Users

Save
Cancel

#### Available Groups

(Search Results are limited to 100 groups. Use \* for wildcards, ex: Admin\*)

To view groups, click Search
Search

<<
<
>
>>

4. Click the **Search** button.

### Synchronization Edit

gamma.thycotic.com

#### Synchronized Groups

Developers  
DnsUpdateProxy  
Product Management  
Professional Services  
Protected Users

Save
Cancel

#### Available Groups

(Search Results are limited to 100 groups. Use \* for wildcards, ex: Admin\*)

To view groups, click Search
Search

<<
<
>
>>

Access Control Assistance Operators  
Account Operators  
Administrators  
Allowed RODC Password Replication Group  
Backup Operators  
Cert Publishers  
Certificate Service DCOM Access  
Cloneable Domain Controllers  
Cluster Admins  
Cryptographic Operators

#### Preview users for group

--Groups--

5. Select the group(s) you would like to sync from the **Available Groups** list, then click the single left arrow **<** to add them to **Synchronized Groups**.

6. Click the **Save** button.

## Step 7: Running Active Directory Synchronization

From the **Active Directory** page, click the **Synchronize Now** button to run a sync. As the sync progresses, you can click the **Refresh** button to monitor the logs until you see the message **Completed Domain synchronization for all domains**.

## Converting Local Users to Domain Users

Local users can be converted to a domain user in a one-way irreversible process. This feature helps existing customers with extensive groups and permissions setup for a local user that they want to convert to an Active Directory user. The page can be accessed on the **Administration > Users** page by clicking the **Migrate to AD** button. For the conversion to work, the domain user must not exist within SS. The username is changed to match the domain user throughout the system.

## Creating Active Directory Users

Active Directory users can be created manually by a user that has the Administer Users role. You can do this by going to **Administration > Users**, then clicking the **Create New** button. See [Creating a User](#).

## Enabling and Disabling Active Directory Users

If you selected a manual setting for **User Account Options**, you can now enable or disable your AD users' access to SS:

1. Go to **Admin > Users**. The Users page appears.
2. To enable users:
  1. Click to select the **Show Inactive Users** check box.
  2. Click to select the check box next to the users to enable.
  3. Click The **Bulk Operation** dropdown list and select **Enable Users**.
3. To disable users, use the same process, selecting **Disable Users** from the **Bulk Operation** dropdown list.

## Syncing and Authenticating AD Users via a Distributed Engine

### Local Versus Distributed Engine Sites

SS connects to the domain: from the Web server *or* routed through a distributed engine. If your Web server can reach your domain without issue, then using the local site option is recommended. When a user authenticates or AD synchronization is run, the connection to the domain is from the Web server. If your Web server cannot connect to the target domain, if it is a VM in a cloud environment for example, you can setup an engine on-premises and assign it to the domain. When a user authenticates, SS routes the domain calls through the on-premises engine, eliminating the need for site to site connections or persistent VPNs. Review the Distributed Engine guide for steps on setting up sites and engines.

**Note:** The Active Directory secret is used to synchronize users and groups, it requires permission to search and view the attributes of the users and groups. If you plan on using discovery, the account also needs permissions to scan computers on the network for accounts.

To setup AD to sync from a DE:

1. Create a synced secret. Before synchronizing or creating users, create a secret for use as the sync secret. This secret should contain Domain Admin credentials (or an account with appropriate permissions for read access to all your organization's AD objects).
2. Specify the domain to authenticate against:
  1. Before synchronizing or creating users, you must first specify which domains SS can authenticate against. SS can synchronize with any number of domains.
  2. Go to **Admin > Active Directory**. The Active Directory Configuration page appears.
  3. Click the **Edit Domains** button.
  4. Click the **Create New** button. The Active Directory Domain page appears.
  5. Type the domain information that you want to authenticate to.
  6. Click the **Link a Secret** selection button.
  7. Click the **Sync Secret** list to select the AD secret you created earlier.

**Note:** If you do not have a secret setup yet, click the **Create New Secret** link to create your AD secret.

**Note:** The AD sync secret is used to synchronize users and groups. It requires permission to search and view the attributes of the users and groups. If you plan on using SS discovery, the account will also need permissions to scan computers on the network for accounts.

8. Click the **Save and Validate** button.
3. Set up the synchronization groups:
  1. Once the domain has been added, go to **Admin > Active Directory**. The Active Directory Configuration page appears.
  2. Click the **Edit Synchronization** button. The Synchronization Edit page appears. The Available Groups represent all accessible groups on the specified AD domain. You can preview the user membership with the Group Preview control.
4. Select the desired group from the Available Groups that contains the AD accounts for users you would like to create in SS.
5. Configure AD:

**Note:** See [Active Directory Configuration Parameters](#) for more information.

1. Go to **Admin > Active Directory**. The Active Directory Configuration page appears.
2. Click on the **Edit** button. The Edit Active Directory Configuration page appears.
3. Click to select the **Enable Active Directory Integration** check box.
4. Click to select the **Enable Synchronization of Active Directory** check box.
5. Click the **Save** button.
6. Turn on AD sync.

## Understanding Active Directory Automatic User Management

### Overview

When Active Directory (AD) Sync is run with the "User status mirrors Active Directory (Automatic)" option, it creates groups and users in SS to mirror the organization's configured AD groups and users. A Secret Server user is created or enabled for every enabled AD user in the selected groups.

Thus, every enabled AD user in every synched group consumes a SS license, whether or not they use Secret Server. As a result, an organization can end up paying for far more SS licenses than they need.

AD Automatic User Management addresses this issue by automatically disabling the accounts of users who have not logged in to SS in a specified number of months. This saves unnecessary licensing costs as inactive users do not count against the number of user licenses required by SS.

You can configure the setting on the Edit Active Directory Configuration page. See [Configuring Active Directory](#). There is a checkbox to enable or disable the feature and a textbox to set the number of months before a user is auto-disabled. The default is three, but you can set it from one to 12.

Newly-added users remain enabled until the first synchronization after the configured number of months have passed. When a user whose account has been disabled by this feature attempts to log in they automatically have their account enabled, provided there are licenses available.

### Examples

#### Example One

1. Maria joined the company today.
2. The next AD synchronization creates a SS account for Maria.
3. Maria never logs in to SS because she does not need it for her job.
4. Once the defined number of months have passed, the next AD synchronization disables Maria's SS account.
5. The SS license used by Maria's account becomes available for use.

#### Example Two

1. Joe gets added to SS but never logs in.
2. The defined number of months later, Automatic User Management disables his account, freeing his license.
3. Joe gets promoted to a job that requires SS.
4. Joe logs into SS.
5. His account is automatically re-enabled, and he now takes up a license.
6. Joe gets demoted to his old job, which does not require SS.
7. A defined number of months later, Automatic User Management disables his account, and the license is freed up once again.
8. Joe has no idea any of this has happened—the automated process is hidden from him.

#### Example Three

1. Rupert logs in to SS several times per month.
2. The defined number of months for Automatic User Management to disable his account is never reached.
3. Rupert's account stays current and his license remains his. The entire process is invisible to Rupert.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

LDAP is an open, industry-standard application protocol for accessing and maintaining distributed directory information services over IP networks.

## Discovery

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Discovery is the process where SS scans an environment to find accounts and associated resources called *dependencies*. Once accounts are found, they can be used to create new secrets in SS. Users with the “administer discovery” role permission can either manually import accounts or can create an automated process, called a *discovery rule*, to do so. Using discovery does not stop users from manually creating their own secrets.

Some typical accounts that discovery can find include Windows local admin, Windows domain, and Unix non-daemon. Some typical dependencies discovery can scan for include scheduled tasks running as a domain user, application pools running as a domain user, and services running as a domain user.

**Note:** Account and dependency types not supported out-of-the-box in SS can still be discovered by writing PowerShell scripts that can be run as custom scanners. See [Extensible Discovery](#).

### Automated Discovery

The following is a high-level overview of how the most common type of automated discovery works without customization. Discovery is organized into an ordered set of discovery scans that pass information based on input and output templates. This is all configured by default. You cannot alter the out-of-the-box discovery scanners, but you can copy them and then modify the copy.

#### Automated Discovery Terms

First, discovery has several terms that need defining:

##### Discovery Source

A named collective, ordered system that conducts discovery. There are four broad types: Active Directory, Amazon Web Services, Unix, and VMware ESX\ESXi.

Configuring discovery is defining the parameters of the discovery source, once the general type is chosen.

##### Discovery Scanner

A discovery component that collects information during a discovery. There are four general types, called *scan templates* (in their sequential running order): Find host ranges, Find machine, Find local accounts, and Find dependencies.

A discovery source consists of an ordered sequence of discovery scanners. Each scanner has a defined input and output. A discovery source can have more than one scanner of a given type.

##### Discovery Input Template

The defined input type for a discovery scanner. An instance of the template contains the data needed to conduct the scan. The input template is often, but not always, an output template of the preceding scanner in the sequence. Some examples include Active Directory Domain, AWS Discovery Source, Organizational Unit, and Windows Computer.

##### Discovery Output Template

The defined output type for a discovery scanner. An instance of the template contains the data produced by the scan. The output template is often, but not always, an input template of the next scanner in the chain. Other times, the output may be used by another non-adjacent scanner in the discovery source. Some examples include: Active Directory Account, AWS Access Key, ESXi Local Account, Host Range, Organizational Unit, and Windows Local Account.

## Example Automated Discovery Process

A typical automated discovery process for Active Directory domains, running on an interval, looks like this:

**Note:** The majority of current discovery processes are for AD discovery source type. The others types differ by input and output but follow a similar process.

**Note:** Even though automatic discoveries run on a set interval, you cannot schedule when those occur. The interval is from whenever the discovery last ran.

1. Discovery matching runs. The discovery matcher creates a link between existing active secrets and any existing secrets in SS based on their machine names, accounts and dependencies. The matcher is automatic. When matches are found, the corresponding existing discovery results appear as "managed" in the discovery network view with a link to the existing secret or dependency.
2. Discovery rules run and attempt to match any unmanaged discovery results to the rule's parameters. If a rule matches the results, discovery automatically imports the results using the settings in the discovery rule. Once finished, discovery begins:
3. The Find Host Ranges scanner (using the Windows Discovery base scanner) runs with an Active Directory Domain input template. The scanner determines which OUs are to be scanned and populates its Organizational Unit output template with a list of those OUs. The output template will be used by the following Find Machine scanner and also by the Find Local Accounts scanner, which does not require machine information.
4. The Find Machine scanner (using the Windows Discovery base scanner) examines OUs from its Organizational Unit input template via LDAP and creates a list of machines with which it populates its Windows Computer output template. This is the list of computers to run a dependency scan on. The Find Dependencies scanner uses this instance of the output template as its input template.
5. The Find Local Accounts scanner (using the File Load Discovery base scanner) examines OUs from its Organizational Unit input template via LDAP and creates a list of all AD admin accounts with which it populates its Active Directory Account output template. This is the list of discovered admin accounts.
6. The Find Dependencies scanner (using the Windows Discovery base scanner) examines a list of machines from its Windows Computer input template using various technologies. For example, applications pools use Microsoft Web Administration (WMA) or, failing that, Windows Management Instrumentation (WMI). Services use WMI, and scheduled tasks use Windows' task scheduler interfaces. The Find Dependencies scanner can return any number of output templates as desired. These include: Com+ Application, Computer Dependency (Basic), PS Dependency, Remote File, SQL Dependency (Basic), SSH Dependency (Basic), SSH Key Rotation Dependency, Windows Application Pool, Windows Scheduled Task, and Windows Service.

The discovered dependencies for local accounts are displayed at Admin > Discovery > Discovery Network View > Local Accounts Tab. Returned accounts for AD users are displayed at Admin > Discovery > Discovery Network View > Domain > Cloud Accounts.

**Note:** Any dependencies that were discovered in prior discovery runs that are no longer present are removed from the discovery results, and their secret dependencies are deactivated.

## Manual Discovery

You can also run discovery manually by going to Admin > Discovery and clicking "Run Now" button on the Discovery and Computer Scan tabs on that page. We recommend that you wait for any automatic discovery to idle before starting another discovery run. When you click the "Run Now" button on the Discovery tab, the first four of the automated steps above are run. When you click the "Run Now" button on the Scan Computers tab, the last two are run. These steps are the most time intensive steps because many machines may be scanned.

Like many operations in SS, you can configure discovery to run locally on IIS machines running SS using website processing or by running through a distributed engine. Distributed engines are agents that you can deploy to remotely process work. They are useful for scenarios where performance is an issue or the work must take place in a remote network where the ports required by discovery are not available. You can configure discovery to use a single site location per discovery source or on a per-OU basis for AD. For more information about distributed engines and other related SS architecture, please refer to the [Distributed Engine Guide](#).

Please see our [Discovery Best Practices Guide](#) to learn about optimizing discovery performance.

You can customize discovery by changing parts of it to use PowerShell. The information a discovery scanner outputs is defined by its scanner template. For standard templates, the input and output information types are fixed. Extensible discovery allows you to customize or replace the unmanaged account, IP address and OU, account, and dependency discovery steps above. Extensible discovery does still have limitations on what information is passed between discovery scanners. For more information, see the [Extensible Discovery Overview](#) (KBA).

## Unix

The scanning account needs to be able to connect over SSH and read the contents of `/etc/passwd`. This includes the minimum permissions for taking over accounts during import sudoer permissions then sudoer permissions on `/etc/passwd`

## ESXi

The scanning account needs "Shell Access" and the "Query VRM Policy" permission.

## Local Windows Accounts

The scanning account needs the "Access This Computer From the Network" permission. To find this permission:

1. Open the local group policy editor (`gpedit.msc`).
2. Go to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
3. For Windows 2016/Win10 endpoints, edit the security policy for "Network Access: Restrict Clients allowed to make remote calls to SAM," adding the account used for discovery and giving it "Allow" permissions.

**Note:** For more information refer to [Network access: Restrict clients allowed to make remote calls to SAM](#).

## Windows Services, Scheduled Tasks, App Pools, and COM+ Applications

**Note:** There are special considerations for discovering service accounts running COM+ Applications, please see the following for instructions: [COM+ Dependency Scanner](#) (KBA).

To scan for service accounts, the account entered must be a domain account that is in the Administrators group on the target machines. Follow the instructions below in either case to ensure your account has the appropriate privileges to run a successful scan:

1. Open the group policy editor for your domain policy.
2. Go to **Computer Configuration > Preferences > Control Panel Settings**.
3. Right-click **Local Users and groups** and select **New > Local Group**.
4. Leave the **Action** dropdown list set to **Update**.
5. Click to select **Administrators (Built-in)** in the **Group Members** dropdown list.
6. Click the **Add...** button.
7. Search for the account you will use for discovery scanning.
8. Click the **OK** button to save your changes. The next time the group policy updates across your environment, the discovery account will be part of the local administrators group.
9. For strong security, configure the group policy to limit the logon privileges of that account:
  1. Open the group policy editor
  2. For your domain policy, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
  3. Add your discovery account to the **Deny log on locally** policy.
  4. Add your discover account to the **Deny log on through Remote Desktop Services** policy.
  5. (Optional) Ensure the account is not part of the remote desktop users group.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

**Note:** Discovery must be enabled in SS to discover AWS accounts.

SS can scan Amazon Web Services (AWS) for accounts that can access the cloud resource. Two types of secrets can be discovered and managed through SS:

- AWS Access Key: Keys used for programmatic integration with AWS.
- AWS Console Account: User login accounts for AWS.

## Enabling AWS Discovery

1. For SS to communicate with AWS, users with sufficient privileges need to create an access key for their account in AWS Identity and Access Management (IAM). The account used to do this requires the following permissions to discover users and access keys:

- iam:ListUsers
- iam:GetLoginProfile
- iam:ListAccessKeys

**Note:** These permissions are limited to the resources the user is allowed to access.

2. Once this access key is created, use the access key and secret key to create a secret in SS using the Amazon IAM key template.
3. Create a new AWS discovery source and use the Amazon IAM key as the credentials secret for the discovery source.

**Note:** AWS only allows programmatic integration through access keys. This type of secret is required for discovery to work. Discovery must be enabled in SS for this feature to work.

## Password Management in AWS

SS can manage password and access keys for AWS IAM accounts.

### Amazon IAM Keys

Password changing, privileged password changing, and running heartbeats are available for Amazon IAM key secrets. When an Amazon IAM key has its password changed through SS, the new secret key is generated automatically and is not set by user input.

During password changing, you can disable or remove old keys through settings available in the advanced configuration:

- `<add key="ShouldDeletePreviousKey" value="true" />`
- `<add key="ShouldInactivatePreviousKey" value="true" />`

**Important:** Altering advanced settings can significantly impact the performance and behavior of SS, so there is no direct link anywhere in SS to the Advanced Settings page. If you need to change any advanced setting (as mentioned in this guide), please contact Thycotic Technical Support.

### Amazon IAM Console Password

Password changing, and privileged password changing are available for Amazon IAM console password secrets. Due to AWS IAM's restrictions on programmatic integration, this secret type cannot use SS heart beat.

In addition, an Amazon IAM key secret must be associated with an Amazon IAM console password secret for password changing to occur. To associate the two:

1. Create the Amazon IAM console password secret, and an Amazon IAM Key secret for an account that has the permissions to change the console user's password. This can be the console account's own access keys, if the user has permission.
2. Navigate to the RPC tab of the Amazon IAM Console Password.
3. Under **Change Password Using Privileged Account** select **Edit**, and choose the IAM key secret created in the previous step. RPC should now be possible on the console password secret.

### Permissions Required for Secret Key Changes

**Note:** These permissions are at the most granular level. You can implement broader methods through wildcard resource restrictions, permission policies, or groups.

Privileged Permissions: (those the AWS account needs to change another users' access keys):

- iam:DeleteAccessKey ON RESOURCE arn:aws:iam::<account>:user/<otherUserName>
- iam:UpdateAccessKey ON RESOURCE arn:aws:iam::<account>:user/<otherUserName>
- iam:CreateAccessKey ON RESOURCE arn:aws:iam::<account>:user/<otherUserName>
- iam:ListAccessKeys ON RESOURCE arn:aws:iam::<account>:user/<otherUserName>

Basic Permissions (those the AWS account needs to change its own access keys):

- iam:DeleteAccessKey ON RESOURCE arn:aws:iam::<account>:user/\${aws:username}
- iam:UpdateAccessKey ON RESOURCE arn:aws:iam::<account>:user/\${aws:username}
- iam:CreateAccessKey ON RESOURCE arn:aws:iam::<account>:user/\${aws:username}
- iam:ListAccessKeys ON RESOURCE arn:aws:iam::<account>:user/\${aws:username}

### Permissions Required for Changing the Amazon IAM Console Password

**Note:** These permissions are at the most granular level. You can implement broader methods through wildcard resource restrictions, permission policies, or groups.

The permissions are:

- Privileged Permission: iam:UpdateLoginProfile ON resouce arn:aws:iam::account>:user/<otherUserName>
- Basic Permission: iam:ChangePassword ON RESOURCE arn:aws:iam::<account>:user/\${aws:username}

## Overview

This document covers the most common settings to tune to make discovery more efficient. Environmental factors contribute to some these settings.

## Global Settings

The settings below might make discovery more efficient, regardless an organization's size.

### Enabling Port Scanning

#### Introduction

*Port scanning* is a scan that can be conducted before the regular discovery scan to potentially reduce discovery time—if specified ports are unavailable on a given machine, the standard discovery scan will eventually timeout (the default is five minutes). Port scanning eliminates that timing out process, which saves time.

**Figure:** Edit Discovery Scanner for Windows Local Accounts

Edit Discovery Scanner - Windows Local Accounts

ADVANCED SETTINGS

Get Additional Local Account Info
☐
?

Local Account Discovery Method
Remote Procedure Call (RPC)
?

Scanner Timeout (minutes)
5
?

Port Scan Enable
☐
?

Port Scan Timeout
30
?

Port Scan List
135,445
?

Exclude By Name List (semi-colon)
?

✓ OK

✗ Cancel

Port scanning for discovery has three configurations or controls:

- Port Scan Enable: Whether to port scan at all. Defaults to unchecked.
- Port Scan Timeout: How long (in seconds) the port scan will try before giving up. Defaults to 30.
- Port Scan List: A comma-delimited list of ports to scan. These depend on the configuration of the systems you will scan. Defaults to NetBIOS (135) and Active Directory services (445).

Examples of scanners that have a port-scanning timeout option for Active Directory include:

- Windows local accounts
- Active Directory user accounts
- All dependency scanners

## Accessing Port Scanning

Simply go to **Admin > Discovery Configuration > Edit Discovery Sources (button) > Configure Discovery Scanners (button) > Accounts (tab)**, and then click the pencil icon for the desired scanner. If the configurations are on that page, that scanner supports port scanning. See the previous figure.

## Additional Reasons to Consider Discovery Port Scanning

### Lowering the Discovery Scanner Timeout May Cause Issues

If you lower the regular discovery scanner timeout, without port scanning enabled, you may kill a running scan. In addition, non-Active-Directory discovery scanners, such as a custom PowerShell scanner, that are slow or prone to hanging may also be disrupted or even crash if the regular discovery scanner timeout is set too low. As a best practice, we recommend enabling port scanning and not lowering the regular scanner timeout, which defaults to five minutes, unless Thycotic Support asks you to. Do not lower the port scanning timeout below 15 seconds.

### Secrets with Multiple Dependencies May Create Especially Long Timeouts

Without discovery port scanning enabled, discovery scanners rely on the standard timeout, which defaults to five minutes. If a secret has multiple dependencies, the system may have a chain of discovery timeouts to process, one at a time. With the default five-minute timeout on all the systems, timing out can take a long time, especially if you have a lot of machines turned off or unavailable. Discovery port scanning greatly reduces that.

To calculate the maximum timeout for discovery use this formula (with all systems using the same timeout value and each secret having the same number of dependencies):

$$(\text{number of secrets}) \times (\text{number of dependencies}) \times (\text{timeout value}) = (\text{maximum minutes for discovery scans})$$

For example, using the default five-minute timeout value for 35 secrets, each with three dependencies:

$$35 \times 3 \times 5 = 525$$

Thus, 8.75 hours (525 ÷ 60) of timeout are possible and enabling discovery port scanning becomes a really good idea, especially if you have a lot of machines down at any given time.

**Note:** We can ignore clustered objects as part of a discovery scan, but we cannot ignore disabled computer objects, so SS tries to scan each object that exists within AD. If you have a centralized area for disabled computer objects, consider configuring discovery to be OU specific and excluding your disabled computers OU to make discovery more efficient.

## When to Run Discovery

Currently, you cannot set when discovery runs via a control or setting. You can, however, approximately set when it runs by disabling and enabling it at the desired time. It runs daily around the same time as when it was first enabled and then again according to whatever the [discovery scan offset hours](#) interval was set to. If you are running discovery once per day, we suggest:

- Choosing a start time outside your normal business hours, such as midnight.
- First running several ad-hoc discoveries when your network traffic normally drops at the end of the day. Record how long each discovery process takes. Remember, this can vary greatly if a lot of machines are down, which is why we suggest conducting more than one discovery.

**Note:** It might be fun to run one test with discovery port scanning disabled, just to see the difference.


- Using the average time the test runs took, calculate when to start discovery at a time when no anticipated portion of the discovery period is during your high-traffic times. We suggest having an end buffer as long as possible to account for variability, so if your average discovery time is fairly long, it might be best to start discovery soon after your network traffic drops off for the evening. This is especially true if your machine pool is growing.

For example, if your tested average discovery time was four hours and your network traffic is busy between 0600 and 1800, you should run discovery between 1800 and 0200, the closer to 1800 the better.

## Discovery Settings

**Figure:** Discovery Settings Page in Edit Mode

DISCOVERY SETTINGS



The AppPool running Secret Server must be configured to not shutdown. See the following KB Article. Secret Server is currently running as "PSLAB\svc-ss-iis".

Enable Discovery

☒

Synchronization Interval for Discovery


Days

1

Hours


0

Ignore Cluster Node Objects

☐



Engine AD Discovery Batch Size

1



Discovery Scan Offset Hours

0



The settings are:

- Synchronization Interval for Discovery: How often you want the regular discover scan to occur.
- Ignore Cluster Node Objects: A check box that tells SS to not run discovery on machines identified as "msclustervirtualserver." Do not change this setting.
- Engine AD Discovery Batch Size: A legacy setting that should always be set to 1.
- See [Discovery Scan Offset Hours](#) for a discussion of the last setting.

**Note:** There is another "Discovery Batch Size" setting on the Advance Settings page, which is usually only available to Thycotic Customer Support. This setting, too, is legacy, and should not be set.

## Environment-Specific Considerations

### Discovery Scan Offset Hours

This section discusses a setting that allows you to quickly discover changes without greatly increasing traffic.

**Figure:** Discovery Settings Page in View Mode

DISCOVERY SETTINGS	
Enable Discovery	Yes
Synchronization Interval for Discovery	1 day 0 hours
Ignore Cluster Node Objects	No
Engine AD Discovery Batch Size	1
Discovery Scan Offset Hours	0

The “discovery scan offset hours” (DSOH) setting is for customers that need to detect new (to the network) systems quickly without excessive network traffic during business hours. For example, you might need this feature if you have lots of server testing (systems are up and down) or laptops (systems are connected or not). The trick is doing this while minimizing the networking load.

We accomplish this with discovery scan offsets. With these, you have multiple synchronization scans per day, rather than just one, where SS attempts to scan each and every system, but first SS looks up each system to see if that system is flagged for scanning. The process goes like this:

1. Initially, SS scans each discovered system and resets its DSOH timer, which is set to the number of hours defined by the DSOH setting value. SS has a separate timer for each scanned system.
2. Once set, each timer starts counting down. Until that timer runs out, SS ignores the scanned system if it runs a discovery scan.
3. When the timer is finished, the system is again flagged for scanning.
4. The next time SS does a discovery scan, it sees the flag is present and scans the system.

The period the “scan me” flag is down (the period the timer is running) is defined by the DSOH setting. Thus, DSOH essentially tells SS how long before scanning that discovered system again.

For example, if you have a discovery scan offset of 12 hours and a discovery interval of four hours:

1. Start: The first time discovery runs, it scans every object because each one’s timer is zeroed out, which makes it flagged for scanning. After scanning, each object’s timer starts to count down, which makes it unflagged for scanning.
2. At four-hours: The next time discovery runs, it ignores the objects that were scanned the first time (because their timer was set to 12 hours), but it does process any newly discovered objects.
3. At eight-hours: In four more hours the same happens—only new objects are processed.
4. At 12 Hours: In four more hours, the scan runs again. This time, the 12-hour scan offset has expired, and all the timers of the original objects are zeroed out. The process begins anew—discovery scans every object because its timer is zeroed out, which makes it flagged for scanning. After scanning, each object’s timer starts to count down, which makes it unflagged for scanning.

## Advanced Settings

**Note:** These settings reside in the ConfigurationAdvanced.aspx file, which you should not edit unless Thycotic Support asks you to.

### Run Secret Computer Matcher Once per Discovery

**Figure:** Secret Computer Matcher Once per Day

Remote Password Changing Heartbeat Interval (Seconds)	< Not Set >
Remote Password Changing: Check for DNS Mismatch	< Not Set >
Secret Computer Matcher Dependency Password Type	< Not Set >
Secret Computer Matcher Once Per Discovery	< Not Set >
Session Callback Interval (Seconds)	< Not Set >
Should Save Files to Database	< Not Set >

During the discovery process, secrets are matched with their machine. For smaller customers, this likely has little performance impact. For very large customers, the performance impact is noteworthy. We recommend that large businesses enable this option to decrease matcher resource use.

By default, the secret computer matcher runs once every five hours (this is non-configurable). This means the matcher runs four times per day, and only one of those times could coincide with discovery running at four-hour intervals. The other three will not run in tandem with discovery and thus will increase network traffic. If you enable this setting, the matcher will instead run after each discovery completes. If discovery only runs once, the matcher only runs once too. This more efficient because discovery can take hours to run, and having the matcher run several times during that period wastes processing.

## Limit the Network Traffic Caused by Nested Organizational Units

**Figure:** Discovery: Bypass "Scan Specific OUs"

Dependency Discovery: Ignore Domain Being Scanned	< Not Set >
Disable RADIUS NAS IP Address Attribute	< Not Set >
Disable SysLog Connection Caching	< Not Set >
Discovery: Bypass "Scan Specific Ous"	< Not Set >
Discovery Batch Size	< Not Set >
ESXi: Enable TLS Debugging and Connection Tracking	< Not Set >
ESXi: Certificate chain policy options	< Not Set >

If you configure discovery for Active Directory to scan by separate OUs and not by the entire domain, nested OUs can overwhelm your message bus. This occurs because each OU generates its own message unless you enable this setting. So if your enterprise has a complex tree of nested OUs, as many large businesses do, you could experience this issue. Smaller enterprises with single or a small number of nested OUs can ignore it. If you change the configuration in the Advance Configuration page file, it will affect all discovery source settings (some scanners have a similar configuration that only affects them). Alternatively, for more flexibility, you can configure this individually at the scanner level by checking the Bypass Specific OU Scan check box on the Settings - Active Directory tab for the scanner:

**Figure:** Tuning Active Directory Settings

Settings - Active Directory Computers

SECRET CREDENTIALS

1. svc-pslab-discovery

Add Secret
Add Secret Search Filter
Create Secret Search Filter

ADVANCED SETTINGS

Engine Max Concurrent Discovery Threads

Bypass Specific OU Scans
☐

✓ OK

✗ Cancel

## Engines and Engine Workers



The number of distributed engines and engine workers within your environment can affect how fast discovery completes. Increasing CPU counts on your existing engines may help them to complete a diverse set of tasks more efficiently but might not have much effect on discovery processing time. If an engine is doing discovery, only a subset of consumers run and they will run into a prefetch count limit (30 messages per engine). Thus, increasing the number of engines and engine workers might decrease total discovery time by increasing that prefetch limit.

1. On the **Administration** menu click **Active Directory**, and then click **Edit** Domains.
2. Click the domain value for the domain you would like to configure..
3. From the **Enable Discovery** dropdown menu, select **Entire Domain**.
4. Click **Save and Validate**.

1. On the **Administration** menu click **Discovery**, and then click **Edit**.
2. Select the **Enable Discovery** check box.
3. Fill in the **Synchronization Interval for Discovery** text-entry fields for days, hours, or minutes. This determines how often Discovery runs.

**Note:** See the "Discovery Best Practices Guide" for details about the other controls.

4. Change the **Days to Keep Operational Logs** text box to set the period to keep discovery-related logs that might contain PII. SS automatically deletes logs older than that (in days).
5. Click **Save**.

1. On the **Administration** menu click **Discovery**, and then click **Edit Domains**.
2. Click the **Domain** you would like to configure.
3. From the **Enable Discovery** dropdown menu, select **Specific OUs**.
4. Click **Save and Validate**.
5. If you are not already redirected there, click the **Specific OUs** tab.
6. Type an OU name in the **Include** box to add an OU to the list. If the OU is found, it auto-populates below the box. Click the name to add it to the list. An included OU appears with an  icon.
7. Type an OU name in the **Exclude** box to exclude it from Discovery. An OU is only available for exclusion if it is contained within an OU that has already been included. An excluded OU appears with an  icon.
8. To remove an OU from the list, click the to the right of the OU.
9. To set a specific site or secret to scan the computers in that OU with use the icon to the right of the OU.
10. Click **Save**.

**Note:** The ports required for Discovery are documented in [Secret Server Ports](#) (KB).

Please see the [Discovery Guide](#) for a comprehensive guide to configuring and using discovery.

**Note:** Please see the [Discovery Topic](#) for a comprehensive guide to configuring and using discovery.

Note: This topic is for Secret Server 10.6 and later. For earlier versions, see [VMware ESX/ESXi Password Changing & Discovery 10.5 and prior](#) (KBA).

## Overview

The ESX/ESXi (API) password changer verifies (using heartbeat) and changes VMware ESX/ESXi passwords via the vSphere API. Password changing and discovery for Secret Server 10.6 and later requires PowerCLI 6.5.1 or higher.

Either must be installed on the servers running discovery—your local SS machine or machines running distributed engine. Earlier versions of the password changer are now deprecated.

**Important:** VMware PowerCLI 11.5 does not work due to VMware.Binding.WsTrust.dll file missing from the directory.

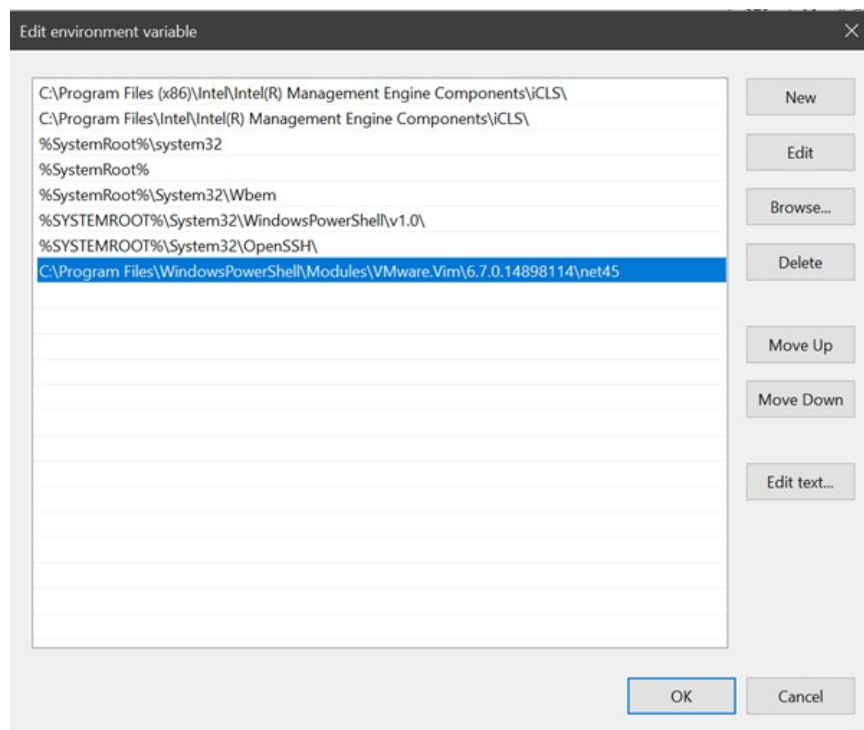
## Details

Secret Server searches the machine's Windows path PATH for the VMWare SDK, therefore installing the correct version of it is all that is needed. On the machine you install VMware PowerCLI, update the Windows "Path" environment variable to include the folder where the file VMware.Vim.dll is located.

**Note:** After installing the VMware PowerCLI, the default installation path is: C:\Program Files\WindowsPowerShell\Modules\VMware.Vim\[version]\net45. The PowerCLI installation path **must be** in the system PATH variable.

To edit your PATH:

1. Add C:\Program Files\WindowsPowerShell\Modules\VMware.Vim\[version]\net45 to the PATH using the system panel (sysdm.cpl).
2. From the **System Properties** dialog, select **Advanced** tab
3. Click **Environment Variables...**
4. Under the **System Variables** section, highlight **Path** then **Edit**. The Edit Environment Variable dialog box appears:



5. Click the **New** button
6. Type C:\Program Files\WindowsPowerShell\Modules\VMware.Vim\[version]\net45, similar to the example above:
7. Click the **OK** button when done.

## Download Locations

Download supported versions of PowerCLI from VMware:

[VMware PowerCLI 11.4.0](#)

## Troubleshooting and Issues

- The error "The VMware VIM API is not installed or is the wrong version" indicates that PowerCLI needs to be installed.
- We recommend not using an outdated SDK with an updated version of VMWare.
- Secret Server's VMWare password changer rejects self-signed SSL certificates. Make sure your VMWare servers have valid SSL certificates (see below for settings).
- The error "Exception: The remote certificate is invalid according to the validation procedure" indicates that vCenter server root certificates needs to be installed. More info [here](#).
- For SS installed editions, you may need to restart the SS website after installing PowerCLI. Do this by recycling the SS application pool or performing an IIS reset.
- For distributed engines, the distributed engine service may need to be restarted after PowerCLI is installed.

## ESXi Certificate Settings

**Note:** VMware recommends not including a CRL/CDP in certificate templates. To that end, we recommend adding the X509RevocationMode.NoCheck option to the ESXi.CertificateChainPolicyOptions Setting.

Thycotic added a configuration option for SS to allow ESXi TLS connections to ignore self-signed certificates, allow certificates from

specific issuers (even if issuer is not in trusted certificate lists), or completely skip certificate validation when using ESXi password changer, heartbeat, or discovery.

**Important:** For security reasons, we do **not** encourage customers to use self-signed certificates. Therefore, the new configuration settings listed below are not accessible through the UI. If you need to alter the default ESXi certificate validation settings, **submit a case through Thycotic's Support Portal** for assistance.

New advanced configuration settings include:

- **ESXi.IgnoreSelfSignedCerts:** If true, ignores any self-signed certs (subject = issuer) from ESXi hosts during heartbeat, RPC, and discovery.
- **ESXi.CertIssuersToIgnore:** Semi-colon delimited list of issuer names (in format shown on certificate---such as "O=Issuer Name"). Ignores partial chain errors due to certificate being issued by any issuer in this list when that issuer is not in the trusted root or intermediate CAs lists on the server.
- **ESXi.IgnoreAllCertErrors:** If true, certificate validation will not be performed. All certificate errors will be ignored.
- **ESXi.CertificateChainPolicyOptions:** Identical to TLS Audit option, but specifically for ESXi. Allows setting X509 options to be applied to certificate validation. This is a comma-delimited list of options. See TLS Auditing or the Details section for more information.
- **ESXi.ClientCertificateIds:** identical to TLS Audit option, but specifically for ESXi. If ESXi host requires the client to present a valid certificate, this is a semi-colon delimited list of client certificates on the server to try to present.
- **ESXi.AuditTlsErrorsDebug:** Identical to TLS Audit option, but specifically for ESXi. If set to true and SS (or DE) auditing is set to DEBUG, detailed debug messages about the certificate chain will be written to the log file.
- **ESXi.IgnoreDefaultHostCert:** Sets all the TLS configuration options necessary to not fail due to a default ESXi host certificate and its issuer not being in the trusted certificates lists. This is a combination of setting the issuer to ignore and not performing a revocation check. Setting this to true should be the first change to make when attempting to resolve heartbeat, RPC, or discovery issues to ESXi hosts when using PowerCLI versions later than 5.5.

**Note:** Issues with self-signed certificates previously implemented by customers were caused by a security update to the VMware vSphere PowerCLI in versions after 5.5 that no longer permits the use of self-signed certificates.

## Distributed Engines

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Out of the box, SS performs all functions from the Web server it is installed on; however, specific features can be routed through a distributed engine for enhanced performance. For example, synchronize and authenticate AD users can be done in SS via your local site or from a distributed engine (DE).

You can install a DE in a remote site and allow it to operate many functions. Communication with Secret Server Cloud also requires the distributed engine to be installed.

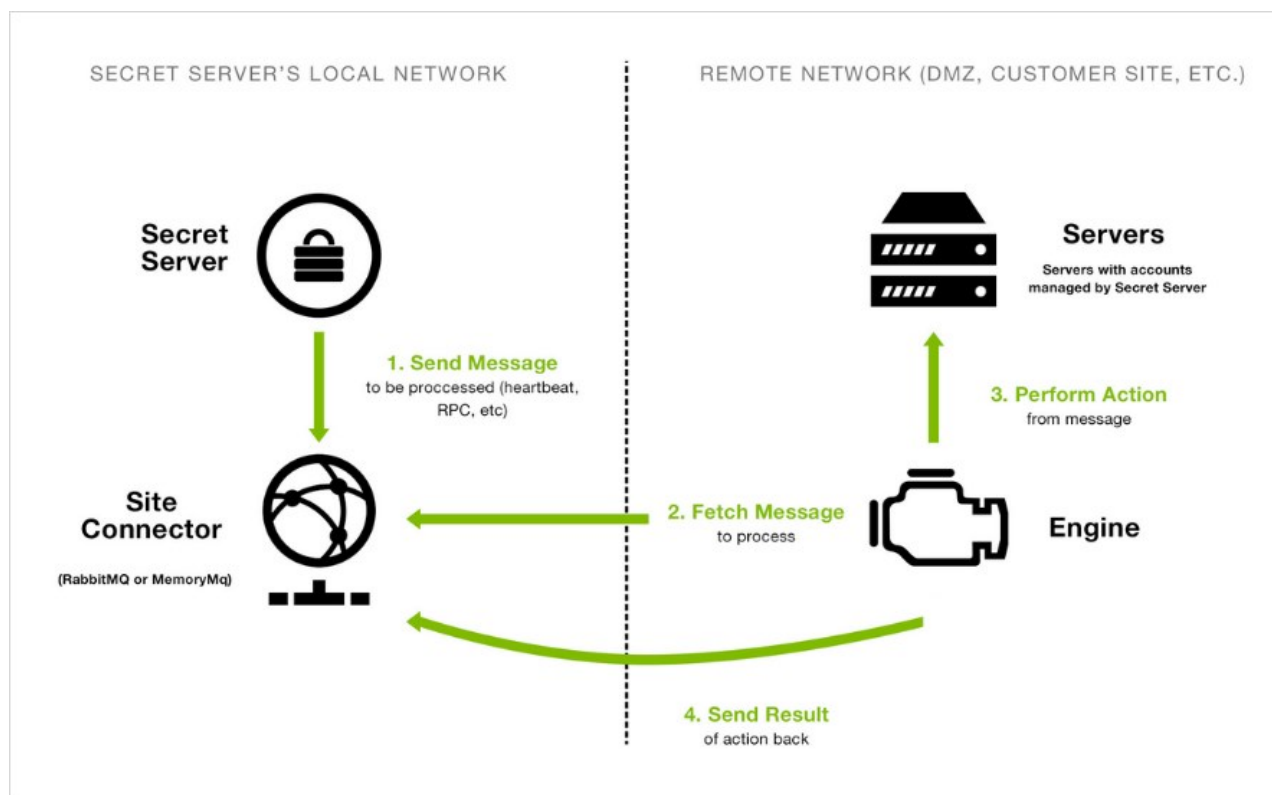
### Main Components

DEs support heartbeat, Remote Password Changing (RPC), and discovery. A DE is composed of site connectors, sites, and engines:

- An **engine** is a Windows service that does the actual work, such as password changing, heartbeat, Discovery, and more. Each engine belongs to a site.
- A **site** can be thought of as a bucket of work items for a particular network area. Each engine is assigned to a single site, but each site can include multiple engines, significantly increasing throughput.
- A **site connector** is a Windows service that holds the work items for a number of sites. The site connector can be either [RabbitMQ](#) or MemoryMQ (a built-in service developed by Thycotic). Each site can only be assigned to a single site connector, but you can have multiple site connectors running on separate machines, each storing work items for multiple sites. Those sites, in turn, distribute the work items among multiple engines. The ability to add new Site Connectors, Sites, and Engines as needed makes Distributed Engine a highly-scalable solution.

**Note:** For the highest scalability and reliability, Thycotic recommends using RabbitMQ. MemoryMQ is an easier but less capable alternative for customers who do not need many engines or sites.

**Figure:** Distributed Engine Components



**Note:** The above diagram is a simplified, conceptual one, not a network diagram. It does not show a callback port from the DE to SS. DEs require either an HTTPS or TCP port to communicate with SS for initial activation, updates, and continuous periodic check of site and site connector settings.

## Ports

DEs have two configurable ports: one for connecting to the site connector, and one for the engine to retrieve configuration information from SS at regular intervals. The callback port from an engine to SS can be configured to contact the website directly over HTTP, HTTPS, or TCP. HTTP and HTTPS connections use the existing IIS port bindings. All connections are outbound—no inbound connections are made from SS or the site connectors to the remote networks.

**Note:** If using Secret Server Cloud, port 9354 must also be opened for outbound messages.

Default ports:

- RabbitMQ: 5672 (non-SSL), 5671 (SSL)
- MemoryMQ: 8672 (non-SSL), 8671 (SSL)
- Secret Server: existing IP address bindings or custom port over TCP. We reserve one port for legacy upgrades, usually port 9999.
- Secret Server Cloud: 9354 (legacy port for NetMessaging in Azure Service Bus), used for outbound traffic for Engines to communicate with Secret Server Cloud instances

## Security

Distributed engines have multiple security layers:

- Engines must be approved within SS before they will be given access to a site.
- Work items are encrypted with a site-specific symmetric key prior to sending them to the site connector.
- Communication to the site connector supports SSL and TLS.
- Direct communication from engine to SS uses a public-private key exchange.
- The engine configuration file is DPAPI encrypted.

For more information about DE security, see the [Distributed Engine Security Guide](#).

## Engine Workflow

When an engine Windows service starts, the following steps occur:

1. The service contacts SS directly using the engine callback port.
2. The service receives configuration information for the site connector to connect to and what site to process work items for.
3. The service connects to the site connector and registers with the site for work item processing.
4. The service fetches a work item from the site.
5. The service processes the work item.
6. The service gives the site the result of the processing, such as heartbeat success or discovery results.
7. The service fetches another work item, and the process continues.

Below is a summary of the steps required to configure DEs:

1. Enable the DE and specify the engine callback settings.
2. Configure and Install the site connector.
  - If you plan to use RabbitMQ (recommended), follow the instructions [here](#). You can find general information on using RabbitMQ Helper to install RabbitMQ can be found in [Thycotic's GitHub Repository](#)
  - If you plan to use MemoryMQ, create the site connector record within SS then click the **Download Site Connector Installer** button to get the MSI. Run the MSI on the desired host.
3. Setup sites.
4. Install engines.
5. Assign secrets to sites. Secrets can be assigned to a site through their Remote Password Changing tab or via a bulk operation on the SS dashboard. Once assigned to a site, all heartbeat or password changing operations take place through that site.
6. Assign discovery sources to sites. To run discovery through a site, edit the discovery source and assign the site. Once assigned, all discovery operations for that discovery source take place through that site.

## What happens if SS sends work items to the site connector, but no engines are running to consume them?

Work items continue to build up in the site connector until a limit is reached. Heartbeat work items have a Time To Live (TTL) of 5 minutes,

Password Changing work items have a TTL of 20 minutes. Expired work items are thrown away and will not be processed. Once a heartbeat or password changing work item is sent to the site connector, SS will not send the same work item to the queue until 5 minutes after the TTL is up (10 and 25 minutes for heartbeat and password changing, respectively). This prevents multiple pending heartbeat or password changing work items for the same secret at the same time.

### **How many Sites can a Site Connector hold?**

MemoryMQ supports up to 100. RabbitMQ supports up to 200.

### **Can I cluster Site Connectors?**

RabbitMQ supports clustering, MemoryMQ does not.

### **Can I use both RabbitMQ and MemoryMQ?**

Yes. You can have as many site connectors, of either type, installed as needed. Note that while you can have both RabbitMQ and MemoryMQ installed on a single machine, you cannot have two RabbitMQ instances or two MemoryMQ instances on the same machine.

### **Can I convert a site connector from MemoryMQ to RabbitMQ or vice versa?**

Yes. You can install the new site connector, swap the sites over to the new service, and then decommission the old site connector.

## Requirements

### Windows Server 2012

Starting in Secret Server version 8.9.000000, DEs require that one of following two server features be installed when the SS website is running on a Windows Server 2012. This depends on which protocol is selected in the engine's callback settings. If HTTPS is selected, the HTTP activation is required. If TCP is selected, then TCP activation is required. This accomplished by going to one of the following in Windows Server 2012:

- **.NET Framework 4.5 Features > WCF Services > HTTP Activation**
- **.NET Framework 4.5 Features > WCF Services > TCP Activation**

If the feature is not installed, there will be an error message in the DE logs: (405) Method Not Allowed. ---> System.Net.WebException: The remote server returned an error: (405) Method Not Allowed.

As of version 10.7.000059, Thycotic updated the definition of distributed engines' offline status to be the configured heartbeat interval times three. For instance, if your heartbeat interval is configured at 5 minutes, the engine will report offline if SS and the engine do not successfully communicate within a 15-minute time period. Engine online and offline states were also added to subscription actions to allow notification to admins when engine states change.

Starting in Secret Server 10.2 it became possible to change how Secret Server processes messages by navigating to:

<Your Secret Server URL>/AdminBackboneBusConfigurationView.aspx

These messages are generated and placed on the internal site connector, or backbone bus, every time a background operation is triggered whether by a schedule or on-demand.

The internal site connector receives and processes messages as a result of numerous actions:

- Bulk Operations
- Generate Password
- Secret Import (CSV and XML)
- Run Heartbeat Now
- Run Heartbeat (Scheduled)
- Run Password Change Now
- Run Password Change (Scheduled)
- Run Discovery Now
- Run Discovery (Scheduled)
- Run AD Sync Now
- Run AD Sync (Scheduled)
- Elements of Session Recording

The internal site connector, using the internal hosted bus, is adequate for bulk operations, heartbeat, discovery, and the like, but some SS features, such as a clustered Web server node configuration or session recording, require a scalable messaging solution to boost processing performance. Our choice is [RabbitMQ](#), which is an intermediary messaging broker that can handle large-scale message processing.

The following is a typical internal hosted bus operation (for a bulk operation):

1. A SS user triggers the a bulk operation.
2. A message is formed and sent over a TCP connection to the internal hosted bus.
3. SS (on the same machine) receives the message.
4. SS (on the same machine) processes the message.

While the internal hosted bus is something we will constantly strive to improve, we recommend using RabbitMQ for a performance boost for those scalable operations. See [Installing RabbitMQ](#) for more information.

Please see [Thycotic Secret Server Distributed Engine Security](#).

## Events and Alerts

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret Server records specific events and optionally sends you alerts when they happen.

## Overview

Secret Server can send a copy of important log messages to an external syslog server for added security using the following protocols:

**Note:** Common Event Format (CEF) is an industry-standard format on top of syslog messages that ensures event interoperability between different platforms.

**Table:** Syslog Transportation Protocols

UDP	No	Least reliable. User Datagram Protocol (UDP) traffic is fire-and-forget with no assurance messages are delivered and no error checking.
TCP	No	More reliable. Transmission Control Protocol (TCP) ensures messages arrive in order, missing messages are resent, and has built in error checking.
Secure TCP	Yes	Establishes a secure connection — Transport Layer Security (TLS) 1.1 or 1.2 only. Syslog Server's certificate is validated by Windows to ensure it is trusted and not revoked. Can be used with or without client certificates (configured in <b>Configuration &gt; Security tab &gt; TLS Auditing &gt; Advanced</b> ).

Due to the sensitive nature of SS logs, we strongly recommend using Secure TCP.

## Configuring a Secure TCP Syslog/CEF External Audit Server in Secret Server

### Compatible Audit Servers

- syslog-ng
- Any Audit server that accepts TLS encrypted messages using the BSD syslog protocol

### Configuring an External Audit Server

1. Navigate to **Admin > Configuration**.
2. Click the **General** tab.
3. Click the **Edit** button at the bottom of the page.
4. Go to the **Application Settings** section.
5. Click to select the **Enable Syslog/CEF Logging** check box. A syslog/CEF section appears:

Syslog/CEF Logging Advanced Settings Information

Enable Syslog/CEF Logging	<input checked="" type="checkbox"/>
Syslog/CEF Server	splunk.qalab.thycotic.net
Syslog/CEF Port	6514
Syslog/CEF Protocol	SECURE TCP
Syslog/CEF Time Zone	UTC Time
Syslog/CEF Site	QASite
Write Syslogs As Windows Events	<input checked="" type="checkbox"/>

**Note:** syslog/CEF may require an additional license key. To install licenses, navigate to **Admin > Licenses > Install New License**. Once installed, the license requires activation. Contact your Thycotic Sales Representative with any questions.

- Type IP address or name for the IIS server hosting the syslog/CEF server in the **Syslog/CEF Server** text box.
- Type the port number where the logging information will be passed (6514 is the default port for secure TCP syslog) in the **Syslog/CEF Port** text box.

**Note:** SS requires outbound access to this server and port so communication can pass freely.

- Click the **Syslog/CEF Protocol** dropdown list and select **Secure TCP**. Secure TCP means either TLS v1.2 or v1.1 because other versions of SSL, such as SSL v3 and TLS v1.0, have known weaknesses.
- Click to select **Syslog/CEF Time Zone** list box to **UTC Time** or **Server Time**, depending on your preference.
- Click the **Save** button.

## Caching Syslog Audits

If the connection between the external syslog server and SS breaks once secure syslog logging is enabled in SS, syslog failure notification messages is cached in the SS database and re-sent at regular intervals until the connection between the syslog server and SS is reestablished.

## Configure Auditing for TLS Connections

To track problems with TLS connections (including whenever the connection fails), enable the TLS certificate chain policy and error auditing in S:

- Navigate to **Admin > Configuration**.
- Click the **Security** tab.
- Click the **Edit** button at the bottom of the page.
- Scroll to the **TLS Auditing** section.
- Ensure the **Apply TLS Certificate Chain Policy and Error Auditing** check box is enabled. If not, you cannot use client


certificates.

**Note:** If secure TCP is used for the syslog/CEF protocol and there are one or more client certificate thumbprints entered, SS checks the local computer's Web hosting and personal certificate store and uses the first one it finds.

## Adding Client Certificate Thumbprints

1. Navigate to **Admin > Configuration**.
2. Click the **Security** tab.
3. Click the **Edit** button at the bottom of the page.
4. Scroll to the **TLS Auditing** section.
5. Click the **Advances (not required)** link. A client certificate thumbprint section appears:

Advanced (not required)



Secret Server's IIS AppPool must be granted permission to use the Client Certificate, using the Windows HTTP Services Certificate Configuration Tool (WinHttpCertCfg.exe). Example usage:  
`winhttpcertcfg.exe -g -c LOCAL_MACHINE\MY -s "Certificate Subject" -a "HOSTNAME\IIS APPPOOL\SecretServer"`  
[Download WinHttpCertCfg - Official WinHttpCertCfg documentation](#)

Client Certificate Thumbprint(s) ?

Enter Client Certificate Thumbprint Ids...

6. Copy and paste a list of SHA1 SSL certificate thumbprints into the **Client Certificate Thumbprints(s)** text box. Separate each thumbprint (40 characters each) with a semicolon. Up to ten are allowed.

**Note:** SS's IIS application pool must be granted permission to use the client certificates, using the Windows HTTP Services Certificate Configuration Tool (WinHttpCertCfg.exe). See [Compatibility Notes for Client Certificates](#).

## Determining the Status of a Remote Audit Server

To view the logs for any TLS-Connection related errors, perform the following:

1. Open the **Microsoft SQL Server Management Studio**.
2. Navigate to your SecretServer database at **< DB Machine Name > > Databases > SecretServer**.
3. Set up a new query.
4. Type and enter `select from tbSecurityAuditLog` to view the events from the TLS audit.

**Note:** For more detailed troubleshooting reporting, reference the logs on the SS Web server at `C:\inetpub\wwwroot\SecretServer\log`. View the `SS.log`, `SS-BSSR.log` (background scheduler), and `SS-BSWR.log` (background worker) for any errors.

## Compatibility Notes for Client Certificates

### IIS Application Pool Certificate Permissions

SS's IIS application pool must be granted permission to use the client certificates, using the Windows HTTP Services Certificate Configuration Tool (WinHttpCertCfg.exe).

For example: `winhttpcertcfg.exe -g -c LOCAL_MACHINEMY -s "Certificate Subject" -a "HOSTNAME\IIS APPPOOL\SecretServer"`

You can download the tool at:

[Windows HTTP Services Certificate Configuration Tool \(WinHttpCertCfg.exe\)](#)

You can view the documentation at:

[WinHttpCertCfg.exe, a Certificate Configuration Tool](#)

Otherwise, if SS is configured to use a client certificate, and IIS does not have permission, errors like this may appear in the logs:

**TLS Error Detected (Authentication Error connecting to IP:PORT) - The credentials supplied to the package were not recognized.**

If you are using a client certificate, and a syslog-ng logging server, the following message may occasionally appear in the main syslog-NG log file:

**SSL error while reading stream; tls\_error='SSL routines:ssl\_get\_prev\_session:session id context uninitialized'**

On the SS side, this appears:

**TLS Error Detected (Authentication Error connecting to IP:PORT) - Authentication failed because the remote party has closed the transport stream.**

This is caused by Windows trying to cache secure connections when client certificates are used, but because syslog-ng has not configured the OpenSSL "session id context", OpenSSL displays this error when it tries to resume a previous session.

SS automatically reconnects and resends any missed messages, so the errors should not have an impact. However, you can disable Window's secure connection caching by adding the [ClientCacheTime](#) setting set to 0 in the Registry and then rebooting. This did not cause any significant performance impact in internal testing.

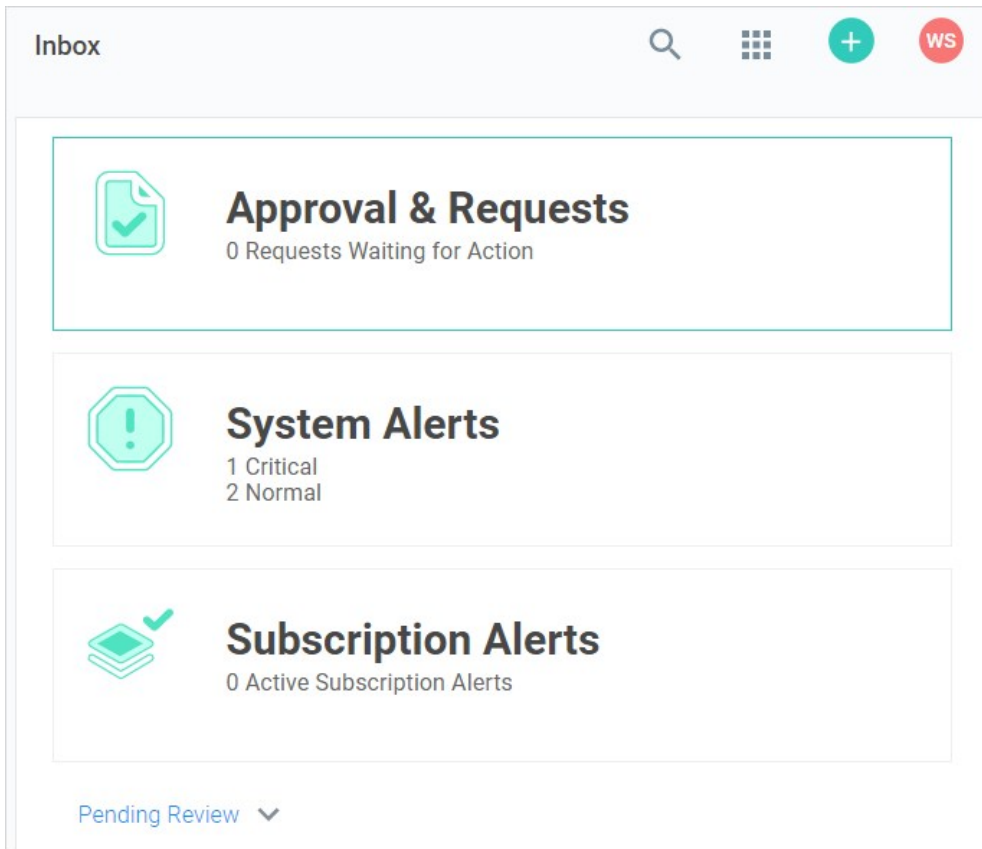
**Note:** If changing back to a previous syslog IP address and port, you will receive a closed connection TLS error on the first attempted syslog connection after making the change. A subsequent call will succeed as the first failure will clear the cached connection on Windows. This is due to the issue with syslog-ng.

**Note:** If syslog-ng configures their OpenSSL session id context, this error message correction is no longer needed.

## AlienVault

It is common for people to incorrectly use the client certificate thumbprints feature when setting up secure AlienVault for syslog. This can cause SS to try to connect to LDAPS with the AlienVault certificate, which can break LDAPS. Users should not use the SS client certificates thumbprint for specifying one certificate for syslog and another for LDAP. The certificate list is intended for each SS or DE to have its own, unique certificate.

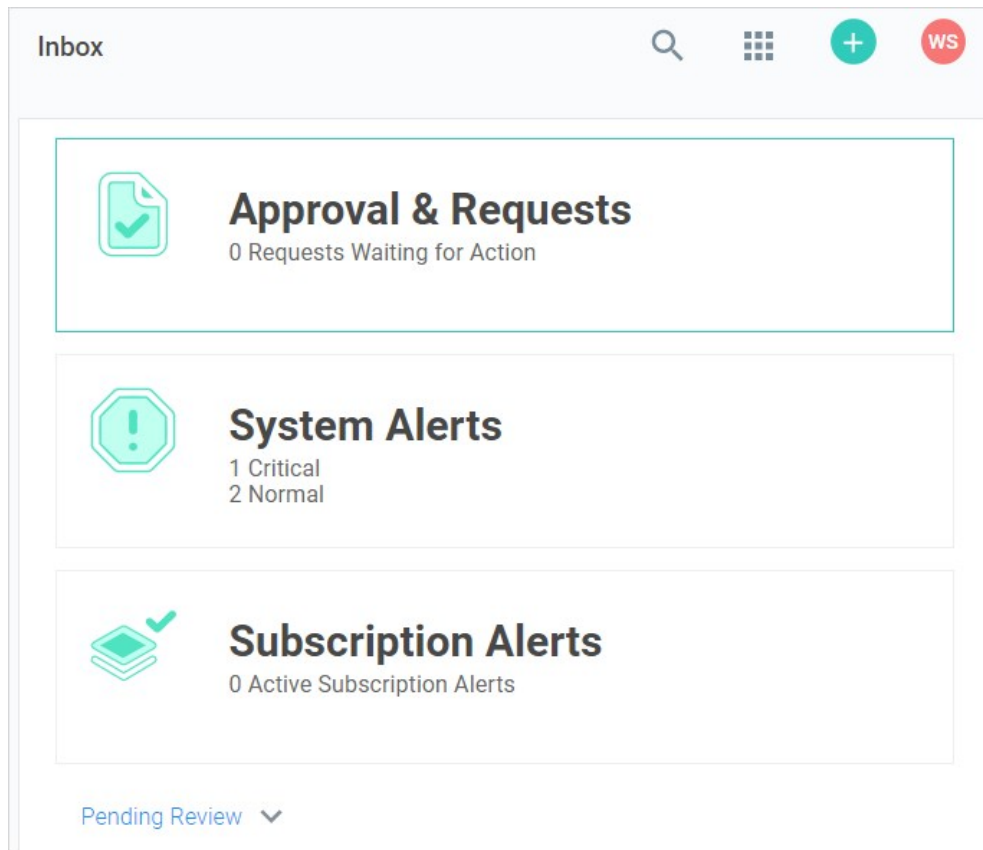
The *Alert Notification Center* page shows event subscriptions, access requests, and other configuration alerts in a single interface. You can access the alert notification center by clicking the **Inbox** button on the main menu.



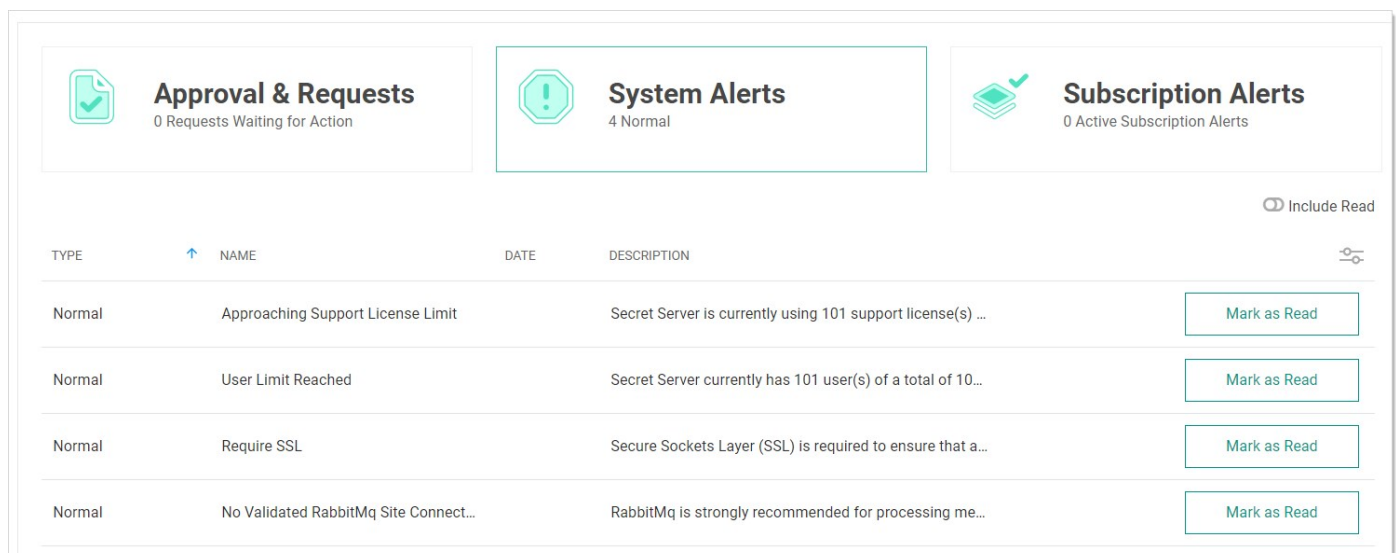
Event subscriptions disappear from the notification center after you view them. System alerts and access requests stay active until resolved.

## Marking Alerts as Viewed

1. Access the alert notification center by clicking the **Inbox** button on the main menu. The Inbox appears:



2. Click the **System Alerts** button. The System Alerts page appears:



3. Click the **Mark as Read** button for the each alert you no longer wish to view. The alert disappears, but you can still see it if you click the **Include Read** toggle button.

## Overview

*Event pipelines* (EPs) are a named group of triggers, filters, and tasks to manage events and responses to them. Event pipelines themselves can be grouped into EP policies. The SS EP system is essentially a flexible instruction set builder and manager for controlling events and responses.

## Definitions

Custom Task Variables

### Event Pipelines

An EP is a single named group of triggers, filters, and tasks. The same EP can be in multiple EP policies. Changing an EP affects all EP policies that EP is a part of. EPs do nothing if not assigned to an EP policy.

### Event Pipeline Policies

An EP *policy* is a named grouping of EPs. There are two types of policies: *secret* or *user*. Secret EP policies target secret policies or folders, and User EP policies target users in Groups. EP policies have no effect if the EP policy has no target. Similarly, an EP policy with no assigned EPs does nothing.

### Event Pipeline Filters

EP *Filters* are parameters that limit when an EP runs. All Filters have settings and can be added to an EP multiple times. The filters are:

#### Secret Policy Filters

The current secret policy filters:

- Custom Variable
- Day of Week
- Event Time
- Event User: Group
- Event User: Has Two Factor
- Event User: Role
- Event User: Role Permission
- Event User: Team
- Event User: User Domain
- Event User: User Last Login
- Event User: User Setting
- IP Address
- Group
- Policy on a Secret
- Role
- Role Permission
- Secret Access Role Permission
- Secret Field
- Secret has Field
- Secret has RPC enabled
- Secret Name
- Secret Setting

- Secret Template
- Site
- Target User: Two Factor Type
- Two Factor Type

## User Policy Filters

The current user policy filters:

- Custom Variable
- Day of Week
- Event Time
- Event User: Group
- Event User: Has Two Factor
- Event User: Role
- Event User: Role Permission
- Event User: Team
- Event User: User Domain
- Event User: User Last Login
- Event User: User Setting
- IP Address
- Multi-Group
- Target User: Group
- Target User: Has Two Factor
- Target User: Multi-Group
- Target User: Role
- Target User: Role Permission
- Target User: Team
- Target User: Two Factor Type
- Target User: User Domain
- Target User: User Setting
- Two Factor Type

Some filters prompt you for additional information when you select them.

## Event Pipeline Policy Targets

EP policy *targets* are SS folders, secret policies, or user groups that are the *subject* and EP policy is applied to. For secret EP types, the secrets inside the folders or secrets under the secret policies trigger the EPs in an EP policy. As targets, folders are not recursive—only the secrets directly in the folder can trigger an EP. For user EP types, only users in the selected groups can trigger an EP.

**Note:** EP targets are *not* the receivers of task action. Those receivers are usually components of SS. The term *target* is instead used for the *subject* of an EP policy—the policy targets the secret in the policy or folder to trigger the EPs to process.

**Note:** Event users are different than target users: The event user triggers the event. The target user is the recipient of the event.

## Event Pipeline Tasks

EP *tasks* are actions, which are triggered in an EP, assuming any filtering conditions are met.

**Note:** EP targets are *not* the receivers of task action. Those receivers are usually components of SS. The term *target* is instead used for the *subject* of an EP policy—the policy targets the secret in the policy or folder to trigger the EPs to process.

Note: To reference the additional secrets in the script's Args field for the update secret with a script task or run script, use \${ADD:1}

before the token. For example: `${ADD:1}$USERNAME` to reference additional secret one and `${ADD:2}$USERNAME` to reference additional secret two.)

## Secret Tasks

The secret tasks are:

- Add Custom Audit
- Add Share
- Assign Secret Policy
- Assigning Site to Secret
- Change Password Remotely
- Change Secrets to not require a comment when viewed
- Change Secrets to not require Check Out
- Change Secrets to require Check Out
- Change Secrets to require Comment on View
- Change to Inherit Permissions
- Delete
- Disable Auto Change
- Disable Heartbeat
- Edit Share
- Enable Heartbeat
- Expire Secrets
- Fail with a message
- Hide Launcher Password
- Move to Folder
- Post Slack Message (WebHook)
- Retry with new random password
- Run Heartbeat
- Run Script
- Schedule Pipeline
- Secret: Add Custom Audit
- Secret: Add Share
- Secret: Assign Secret Policy
- Secret: Assigning Site to Secret
- Secret: Change Password Remotely
- Secret: Change Secrets to not require a comment when viewed
- Secret: Change Secrets to not require Check Out
- Secret: Change Secrets to require Check Out
- Secret: Change Secrets to require Comment on View
- Secret: Change to Inherit Permissions
- Secret: Delete
- Secret: Disable Auto Change on Secret
- Secret: Disable Heartbeat
- Secret: Edit Share
- Secret: Enable Auto Change on Secret
- Secret: Enable Heartbeat
- Secret: Expire Secrets
- Secret: Fail with a message
- Secret: Move to Folder
- Secret: Retry with new random password
- Secret: Run Heartbeat

- Secret: Send Email to Owners
- Secret: Set Privileged Account
- Secret: Stop RPC
- Secret: Undelete
- Secret: Update Secret by field
- Secret: Update Secret Name
- Secret: Update Secret with a script
- Secret: Viewing Password Does Not Require Edit
- Secret: Viewing Password Requires Edit
- Send Email to Event User
- Send Email to Group
- Send Email to List
- Send Email to Owners
- Set Custom Variable
- Set Privileged Account
- Stop RPC
- Undelete
- Unhide Launcher Password
- Update Secret by field
- Update Secret Name
- Update Secret with a script
- Update Secrets to automatically change the password

## User Tasks

The user tasks are:

- Post Slack Message (WebHook)
- Run Script
- Schedule Pipeline
- Send Email to Event User
- Send Email to Group
- Send Email to List
- Set Custom Variable
- Target User: Add User to Group
- Target User: Add User to Team
- Target User: Disable Duo Two Factor
- Target User: Disable Email Two Factor
- Target User: Disable FIDO2 Two Factor
- Target User: Disable RADIUS Two Factor
- Target User: Disable TOTP Auth Two Factor
- Target User: Disable Users
- Target User: Enable Duo Two Factor
- Target User: Enable Email Two Factor
- Target User: Enable FIDO2 Two Factor
- Target User: Enable RADIUS Two Factor
- Target User: Enable TOTP Auth Two Factor
- Target User: Enable Users
- Target User: Force Logout
- Target User: Lock User
- Target User: Remove User from Group
- Target User: Remove User from Team

- Target User: Reset FIDO2 Two Factor
- Target User: Reset TOTP Auth Two Factor
- Target User: Send Email to Target User
- Target User: Unlock User

## Event Users

An event user is the user making the action. For example: Admin updated user Jane's email. Admin is the event user.

## Event Variables

Event variables are used in EP filters or tasks. They are:

### Secret Field Tokens

These can be any secret field name in the tbSecretField table that is not a Password (IsPassword=0) or File (IsFile=0) type. For example, for an Active Directory Account (SecretTypeID=6001), these tokens are available: \$Username, \$Domain, or \$Notes.

### Event Setting Tokens

**Table:** Event Setting Tokens with Filter Values

Token	Description	Type
\$ByUser	Username that initiated the event	Text
\$ByUserDisplayName	Display name of user that initiated event	Text
\$ContainerName	Folder name for the event	Text
\$EventAction	Action that occurred on the event entity type. See list of triggers.	Text
\$EventDetails	Event notes. For heartbeats and RPC, this contains the status and any error message.	Text
\$EventUserKnownAs	Username for user that caused the event. If a domain account exists, then this appears as domain\username.	Text
\$ItemId	Secret ID for the event	Text
\$ItemNameForDisplay	Event secret name	Text

### Secret Setting Tokens

**Table:** Secret Setting Tokens with Filter Values

Token	Description	Type
\$Secret.Active	Active	Boolean
\$Secret.AutoChangeOnExpiration	Auto change on expiration	Boolean

\$Secret.ChangePasswordNow	Change password now	Boolean
\$Secret.CheckOutChangePassword	Checkout change password	Boolean
\$Secret.CheckOutEnabled	Checkout enabled	Boolean
\$Secret.EnableInheritPermissions	Enable inherit permissions	Boolean
\$Secret.EnableInheritSecretPolicy	Enable inherit secret policy	Boolean
\$Secret.Expired	Expired	Boolean
\$Secret.HideLauncherPassword	Hide launcher password	Boolean
\$Secret.IsDoubleLock	Double lock	Boolean
\$Secret.IsSessionRecordingEnabled	Session recording enabled	Boolean
\$Secret.IsSSHProxyEnabled	SSH proxy enabled	Boolean
\$Secret.LastHeartBeatStatus	Status of last heartbeat	AccessDenied; AccountLockedOut; ArgumentError; Disabled; DnsMismatch; Failed; IncompatibleHost; Pending; Processing; Success; UnableToConnect; UnableToValidateServerPublicKey; UnknownError
\$Secret.PasswordChangeFailed	Password change failed	Boolean
\$Secret.PasswordChangeOutOfSync	Password change out of sync	Boolean
\$Secret.PasswordChangeStatus	Password change status	None; Pending; Processing
\$Secret.PasswordComplianceCode	Password compliance code	Pending; Pass; Fail
	Require	

\$Secret.RequireApprovalForAccess	approval for access	Boolean
\$Secret.RequireApprovalForAccessForEditors	Require approval for access for editors	Boolean
\$Secret.RequireApprovalForAccessForOwnersAndApprovers	Require approval for access for owners and approvers	Boolean
\$Secret.RequireViewComment	Require view comment	Boolean
\$Secret.RestrictSshCommands	Restrict SSH commands	Boolean
\$Secret.RPCAttemptCount	RPC attempt count	Boolean
\$Secret.SecretId	Secret ID	Text
\$Secret.SecretPolicyId	Secret policy ID	Text
\$Secret.SecretTemplateName	Secret template name	Text

## Additional Tokens

### Secret

- \$SecretName
- \$SecretId

### Folder

- \$FolderId
- \$FolderName
- \$FolderPath

### Event User

- \$EventUserDomain
- \$EventUserKnownAs
- \$EventUserName

- \$EventUserLastLogin
- \$EventUserId

#### Target User

- \$TargetUser.DisplayName
- \$TargetUser.IsApplicationAccount
- \$TargetUser.IsSystemUser
- \$TargetUser.UserEmail
- \$TargetUser.UserEnabled
- \$TargetUser.UserName
- \$TargetUser.Domain
- \$TargetUserId
- \$TargetUserKnownAs
- \$TargetUserLastLogin
- \$TargetUserName

#### Custom Task Variables

These are variables created with the EP task. There are two types, global and item, both of which are referenced in the same way.

**Note:** You must set a custom variable before using it. Thus, you cannot set a variable and use it in the same pipeline. The way around this is to create two pipelines in a policy—the first pipeline sets the variable and the second one uses it.

#### Global Variable

- \$GlobalVariable.CustomVariableName
- This custom task variable is global, so there should only be one per variable name.

#### Item Variable

- \$ItemVariable.CustomVariableName
- This variable is per SecretId (secret pipeline) or UserId (user pipeline).

Add note:

#### Target User

A target user is the affected user. Example: Admin updated user Jane's email. Jane is the target user.

#### Triggers

EP *triggers* are events in SS that cause the EP to begin processing. All triggers have no settings and can only be added to an EP once. The triggers are:

#### Secret Triggers

- Access Approved
- Access Denied
- Cache View
- Check In
- Check Out
- Copy

- Create
- Custom Audit
- Custom Password Requirement Added To Field
- Custom Password Requirement Removed From Field
- Delete
- Dependency Added
- Dependency Deleted
- Dependency Failure
- Edit
- Expired Today
- Expires in 1 Day
- Expires in 15 Days
- Expires in 3 Days
- Expires in 30 Days
- Expires in 45 Days
- Expires in 60 Days
- Expires in 7 Days
- Export
- File Save
- Heartbeat Failure
- Heartbeat Success
- Hook Create
- Hook Delete
- Hook Edit
- Hook Failure
- Hook Success
- Launch
- Password Change
- Password Change Failed
- Password Change Maximum Attempts Reached
- Password Displayed
- Pre-Check Out
- Secret Policy Change
- Session Recording View
- Undelete
- View
- Viewed Secret Edit
- Web Password Fill

## User Triggers

- Added to Group
- Challenge Applied
- Challenge Cleared
- Disable
- Enable
- Lockout
- Login
- Login Failure
- Logout
- Owners Modified
- Remove Personally Identifiable Information

- Removed From Group
- Two Factor Changed
- Two Factor Reset Failure
- Two Factor Reset Success
- User: Create
- User: Edit
- User: Password Change

## Permissions

There are three permissions:

- **Administer Pipelines:** Allows the user to create, edit, and remove EPs and EP policies.
- **Assign Pipelines:** Allows the user to assign an EP policy to secret policies, or folders.
- **View Pipelines:** Allows the user to view EP policies and policy activities.

## Procedures

### Event Pipelines

#### Activating or Deactivating Event Pipelines

To control if an EP is available to all EP policies, you can toggle the EP's active status:

1. Go to the **Event Pipelines** page.
2. Click the **Pipelines** tab.
3. Locate the card for the EP you want to activate or deactivate.
4. Click the **Active/Inactive** toggle button. A confirmation popup appears.
5. Click the **OK** button. The EP's status is changed for all EP policies it belongs to.

#### Creating New Event Pipelines

**Note:** You can create EPs from the Event Pipelines list (shown below) or an EP policy's details view. With the former method, you will have to add the EP to an EP policy separately. With the latter method, the EP is automatically added to the EP policy you are viewing. You can later manually add additional EPs to the policy as desired.

To create a new EP:

#### Step One: Create EP

1. Go to the **Event Pipeline** page.
2. If necessary, click the **Pipelines** tab. The Event Pipeline Pipelines page appears.
3. Click the **Add Pipeline** button. The New Pipeline popup page appears.
4. Click to select the EP type: **Secret** or **User**.
5. Click to select the **Create New Pipeline** selection button.
6. Click the **Create** button. The New Pipeline wizard appears on the Choose Triggers page.

#### Step Two: Add Triggers

1. In the **Add Triggers** section, click the **+** button next to the triggers you desire. You can also search for a trigger by typing in the search text box. The selected triggers appear in the Selected Triggers list. Consider the following when selecting triggers:
  - Currently triggers are centralized around events that are linked to a secret.
  - You can add multiple triggers.

- You can limit when the EP runs by adding filters.
- Multiple triggers are logically ORed (not XORed) together. Each trigger is considered individually, and only one needs to apply for the EP to run—if concurrent triggers do not apply, it does not matter. If multiple triggers do apply, the EP will only run once per EP policy.

2. Click the **Next** button. The Choose Filters page of the wizard appears.

### Step Three: Add Filters

1. Use the exact same method to add filters to the EP. All filters present a popup page for you to provide additional information when you click on them. Consider the following when selecting filters:
  - Whereas triggers focused on secrets, filters can access secret and user information.
  - Because the same filter can differ by its settings, you can add the same filter multiple times to an EP.
  - Filters are logically ANDed together—all filters apply at once and all matter.
2. Click the **Next** button. The Choose Tasks page of the wizard appears.

### Step Four: Choose Tasks

1. Use the exact same method to add tasks to the EP. Many tasks present a popup page for you to provide additional information when you click on them.
2. Set the task order. Tasks run in order of their appearance in the **Task** tab of the **Event Pipeline** page. To change the task running order, hover the mouse pointer over the one you want to move, and use the anchor on the left of its card to drag the task to the order you wish it to run. If a Task fails, then the following tasks will not run.

**Warning:** Tasks are very powerful and thus can be dangerous. You can alter SS in dramatic, sometimes irreversible ways. We strongly recommend testing EPs in a safe sandbox environment before applying them to production SS servers.

3. Click the **Next** button. The Name Pipeline page of the wizard appears.
4. Type the EP's name in the **Pipeline** text box.
5. Type a description of the EP in the **Pipeline Description** text box.
6. Click the **Save** button.

### Editing Existing Event Pipelines

To create an EP:

1. Go to the **Event Pipeline** page.
2. If necessary, click the **Pipelines** tab. The Event Pipeline Pipelines page appears.
3. Click the title of the card representing the EP you want to edit. The EP wizard appears.
4. See [Creating New Event Pipelines](#) for instructions on using the wizard.

### Viewing Event Pipelines

Because EPs are not directly tied to a single EP policy, they can be viewed through an EP policy or directly from the EP list. The EP list is a tab on the main Event Pipeline Policy page directly after navigating from the Admin page. After selecting an EP policy, its associated EPs are displayed in cards.

### Event Pipeline Policies

## Activating or Deactivating Event Pipeline Policies

To control if an EP policies is available, you can toggle the EP policy's active status:

1. Go to the **Event Pipelines** page.
2. If necessary, click the **Policies** tab.
3. Locate the card for the EP policy you want to activate or deactivate.
4. Click the **Active/Inactive** toggle button. A confirmation popup appears.
5. Click the **OK** button. The EP policy's status is changed.

**Note:** The EPs belonging to the EP policy remain available to other EP policies.

## Adding an Existing Event Pipeline

**Note:** Adding Existing Pipeline enables the pipeline to be used in other policies. Only pipelines of the same type (Secret or User) can be added. Note: This does not create a copy of the existing pipeline, it creates a link. Thus, any changes to the pipeline will affect the other policies that use it.

1. Go to the **Event Pipelines** page.
2. If necessary, click the **Policies** tab.
3. Select the EP policy you want to add a pipeline to.
4. Click the **Add Pipeline** button.
5. Click the **Add Existing Pipeline** dropdown list and select the pipeline (only pipelines of the same type will show).
6. Click the **Create** button.

## Assigning Folders and Secret Policies to Event Policy Targets

### Folders

1. Go to the **Event Pipeline** page.
2. If necessary, click the **Policies** tab. The Event Pipeline Policies page appears.
3. Click the title of the EP policy on its card on the **Event Pipeline Policies** page. The page for that EP policy appears.
4. Click the **No Folder Selected** link in the **Targets** section. A destination page appears.
5. Click to select the check boxes for the desired target folders in the tree. Click the tiny arrow next to the check box to expand the tree. Remember, selecting a folder does *not* automatically select its subfolders.
6. Click the **Save** button.

### Secret Policies

1. Click **Admin > Secret Policies**. The Secret Policy page appears.
2. Click the desired secret policy's name in the list. The Secret Policy page for that policy appears.
3. Click the **Edit** button. The list becomes editable.
4. Click the **Event Pipeline Policy** dropdown list in the **Security Setting** section and select **Enforced**.
5. Click the **Save** button. All secrets under that secret policy are now affected by the EP policy.

## Creating, Importing, and Duplicating Event Pipeline Policies

**Note:** Newly added EP policies are deactivated by default.

1. Click **Admin > See All**.
2. Click the **Action** button and select **Event Pipeline Policy**.
3. If you plan to duplicate an existing EP policy, click the card for that policy in the **Event Pipeline Policies** list.

4. Click the **Add Policy** button, and you will be presented with the following options:

- **Create New Policy:** Click the selection button, and type a name in the **Policy Name** text box, and optionally type a description in the **Policy Description** text box.
- **Import Policy:** Import an exported EP policy in JSON format. This can be a policy exported from a separate SS instance. Click the selection button, and paste the JSON payload in the **Add Policy** text box, click the **Create** button.
- **Duplicate Selected Policy:** Copy an existing EP policy. Click the selection button, and then click the **Create** button.

The new EP appears in the Event Pipeline Policies list.

## Monitoring Event Pipeline Policies

There are two ways to monitor your EP policy:

- **Audit:** Shows changes to EP policies, targets, and EPs. Click the **Audits** tab on the **Event Pipeline Policies** page.
- **Activity:** Shows the actions each EP policy or single EP took each time it is triggered. This includes failures, skips, and successes. Click the card for the desired EP policy, and then click the **View Policy Activity** button on the right. Alternatively, you can click the title on the card. When the page for the EP policy appears, click the **Activity** tab.

## Ordering Event Pipelines in Event Pipeline Policies

Event Pipelines run in order they appear in the EP policy. Since EPs can be in multiple EP policies, the order is unique to each policy. To change the EP order in the EP policy:

1. Go to the **Event Pipeline Policies** page.
2. Click the name on the card for the EP policy you want to edit. The policy's page appears on the Details tab.
3. Hover the mouse pointer over the EP you want to reorder. An anchor appears on the left of the card.
4. Drag that anchor to the desired position.

**Note:** If an error occurs in a policy's EP, then the following EP still runs.

## Removing Event Pipelines from Event Pipeline Policies

To remove an EP from an EP:

1. Go to the **Event Pipeline Policies** page.
2. Click the name on the card for the EP policy you want to edit. The policy's page appears on the Details tab.
3. Click on an EP in the details of an EP policy. A panel appears on the right of the page.
4. Click the **Remove Pipeline** button.

**Note:** The button removes the EP from the EP policy, but it does not remove it from SS. Other EP policies using the EP still have access to it.

## Infinite Loops

It is possible for EPs to trigger each other over and over in an endless loop. For example:

1. Editing a secret triggers one EP to run a heartbeat on the secret.
2. The heartbeat triggers another EP to edit the secret.
3. Editing the secret triggers the original EP to run another heartbeat, restarting the cycle, creating an infinite feedback loop.

Fortunately, SS detects these loops and automatically deactivates the involved EPs. So, if you have EPs that seem to be deactivating themselves, look for circular logic paths involving the EPs.

**Note:** By default, pipelines are configured to consider any event that executes five tasks within five minutes from the same

trigger as an infinite loop. For example, "secret edit" is selected as a pipeline trigger, and "remote password change" is selected as the task. After the first edit is made on a secret, an RPC is triggered. Every time the RPC completes, a new edit is triggered, which, in turn, triggers another RPC. If this happens five times within five minutes, then an infinite loop is declared. If the RPC is slow, taking more than five minutes for five password changes to occur, then an infinite loop is **not** declared. In this case, use the "configuration advanced" page to change "event pipelines infinite loop time (minutes)" to a longer time.

## Configuring Advanced Settings

### Configuration Advanced Settings

There are a few new Advanced Setting that can be used with EP policies.

- **Event Pipeline Activity Log entries removed after (days):** The EP activity log entries stay in the log for this many days. Default value: 90.
- **Event Pipelines: Allow Confidential Secret Fields to be used in Scripts:** Allows confidential secret fields to be used in EP script, such as \$password. Default value: False.
- **Event Pipelines Infinite Loop Time (Minutes):** If an EP executes the number of times specified in the infinite loop threshold during the Infinite Loop Time period, it is marked as an infinite loop. Default Value: 5 (on premises), 20 (cloud).
- **Event Pipelines Infinite Loop Threshold:** Number of times that an EP can execute within the infinite loop time on an individual item before it is considered to be an infinite loop. Default Value: 5.
- **Event Pipelines Log Skipped Policies:** If true, the the pipeline activity log will log filtered policies runs. Default value: False.
- **Event Pipelines Maximum Script Run Time (Minutes):** Scripts ran by EP tasks are stopped after this many minutes. Default Value: 5 minutes.

**Note:** Please click the table of contents on the left to see the sub-pages to this one. Click the table of contents on the right to see headings on this page.

The Event Subscription Page includes:

- **Additional Email Recipients:** List of additional email addresses to send the email to.

**Note:** These entries are meant to be outside of the users' email addresses as known to SS. One of these might be, for example, the user's home email address.

- **Send Email Alerts:** Sends an email to both users and all the users contained in the groups for this subscription. It also sends an email to all email addresses in the Additional Email Recipients list (see below).
- **Send Email with High Priority:** Sends the email for this subscription with high priority set.
- **Subscribed Events:** List of the events that are contained in this subscription.
- **Subscribed Users:** List of the SS users and groups subscribed to this event.
- **Subscription Name:** Name for the subscription.

## Creating Event Subscriptions

To add an event subscription:

1. Navigate to **Administration > Event** Subscriptions.
2. Click **New**.
3. In the **Subscription Name** text box, enter a name for this new event subscription.
4. Add users and groups to this subscription by selecting them from the **Add New** list. They are added to the **Subscribed Users** list above the **Add New** list.
5. Add events to this subscription by adding rows to the **Subscribed Events** data grid. To do this, select an entity type from the list in the **Entity** column of the first row.
6. After an entity is chosen, you can now select an action, such as Create, Delete, or Edit Permissions.
7. After an action is selected, a condition may be available. Select the condition you wish to implement.
8. To add this event to the subscription, click the button. This must be done before the **Save** button at the bottom of the page is clicked in order to add this event to the subscription.
9. Click the **Save** button.

## Deleting a Subscription

To delete an event subscription:

1. Navigate to **Administration > Event Subscriptions**.
2. Click the subscription name.
3. Click **Delete** on the following page.

## Editing a Subscription

To edit an event subscription:

1. Navigate to **Administration > Event Subscriptions**, click the subscription name, and then **Edit**.
2. To remove a subscribed user, group, or event, click the button next to the entry in the appropriate list.
3. To add entries to either list, see [Creating Event Subscriptions](#).
4. Click **Save** to save all changes.

## Event List

The following events are available:

**Table:** Folder Events

Create	All, In this Folder
Delete	All, For this Folder, In this Folder
Edit Permissions	All, For this Folder, In this Folder
Secret Policy Change	All, For this Folder, In this Folder

**Table:** Secret Events

Access Approved	All, For this Secret, In this Folder
Access Denied	All, For this Secret, In this Folder
Cache View	All, For this Secret, In this Folder
Check In	All, For this Secret, In this Folder
Check Out	All, For this Secret, In this Folder
Copy	All, For this Secret, In this Folder
Create	All, In this Folder
Custom Audit	All, For this Secret, In this Folder
Custom Password Requirement Added to Field	All, For this Secret, In this Folder
Custom Password Requirement Removed from Field	All, For this Secret, In this Folder
Delete	All, For this Secret, In this Folder
Dependency Added	All, For this Secret, In this Folder
Dependency Deleted	All, For this Secret, In this Folder
Dependency Failure	All, For this Secret, In this Folder
Edit	All, For this Secret, In this Folder
Expired Today	All, For this Secret, In this Folder

Expires in 1 Day	All, For this Secret, In this Folder
Expires in 3 Days	All, For this Secret, In this Folder
Expires in 7 Days	All, For this Secret, In this Folder
Expires in 15 Days	All, For this Secret, In this Folder
Expires in 30 Days	All, For this Secret, In this Folder
Expires in 45 Days	All, For this Secret, In this Folder
Expires in 60 Days	All, For this Secret, In this Folder
Export	All, For this Secret, In this Folder
File Save	All, For this Secret, In this Folder
Heartbeat Failure	All, For this Secret, In this Folder
Heartbeat Success	All, For this Secret, In this Folder
Hook Create	All, For this Secret, In this Folder
Hook Delete	All, For this Secret, In this Folder
Hook Edit	All, For this Secret, In this Folder
Hook Failure	All, For this Secret, In this Folder
Hook Success	All, For this Secret, In this Folder
Launch	All, For this Secret, In this Folder
Password Change Maximum Attempts Reached	All, For this Secret, In this Folder
Password Copied to Clipboard	All, For this Secret, In this Folder
Password Displayed	All, For this Secret, In this Folder
Password Change	All, For this Secret, In this Folder
Secret Policy Change	All, For this Secret, In this Folder
Session Recording View	All, For this Secret, In this Folder
Undelete	All, For this Secret, In this Folder
View	All, For this Secret, In this Folder

View Secret Edit	All, For this Secret, In this Folder
Web Password Fill	All, For this Secret, In this Folder

**Table:** User Events

Added to Group	All, For this User, For this Group
Challenge Applied	All, For this User
Challenge Cleared	All, For this User
Create	-
Disabled	All, For this User
Edit	All, For this User
Enable	All, For this User
Lockout	All, For this User
Login	All, For this User
Login Failure	All, For this User
Logout	All, For this User
Owners Modified	All, For this User
Password Change	All, For this User
Removed From Group	All, For this User, For this Group
Two Factor Changed	All, For this User

**Table:** Other Events

Configuration	Edit
Dual Controls	Create, Delete, Edit
Encryption	HSM Disable, HSM Enable, Rotate Secret Keys, Rotate Secret Keys Cancel Requested, Rotate Secret Keys Failure, Rotate Secret Keys Success

Engine	Engine Activated, Create, Deactivate, Delete, Offline, Online
Export Secrets	Exported
Group	Owner Modified
Import Secrets	Imported
IP Address Range	Create, Delete, Group Assigned, Group Unassigned, Edit, User Assigned, User Unassigned
Licenses	Expires in 30 Days
Role	Assigned User or Group, Create, Edit, Role Disabled, Role Enabled, Unassigned User or Group
Role Permission	Added to Role, Removed From Role
Script - PowerShell	Create, Deactivate, Edit, Reactivate, View
Script - SQL	Create, Deactivate, Edit, Reactivate, View
Script - SSH	Create, Deactivate, Edit, Reactivate, View
Secret Policy	Create, Edit
Secret Template	Create, Create Secret Access Changed, Edit, Field Encrypted, Field Exposed, Owners Modified, Copy
Privileged Behavior Analytics Configuration	Edit
Site	Engine Added, Domain Assigned to Site, Create, Disable, Edit, Enable, Engine Downloaded, Engine Offline, Engine Online, Domain Removed from Site, Engine Removed
Site Connector	Create, Credential View, Disable, Edit, Enable
Unlimited Administrator	Disable, Enable
User Audit	Expire Now

The System Log is used to communicate the different events that are occurring while SS is executing. It can be helpful in troubleshooting unexpected behavior. The system log can be enabled by clicking **Edit** and checking the **Enable System Log** check box on the **Administration > System Log** page.

System log parameters include:

- **Maximum Log Length:** This is the maximum number of rows to keep in the system log table in the SQL database. When it reaches that amount, it is reduced by 25%.
- **Notify Administrators when System Log is Shrunk:** This setting is used to send an email to all system log administrators when the system log has been truncated. A system log administrator is any user in a role with the Administer System Log permission included.

To clear the system log of all its records, click **Clear**.

To view the events that have been triggered in a subscription, navigate to **Administration > Event Subscriptions** and click **View Audit**. In the Event Subscription Activity list, the most recent events to have been triggered are on top of the list. To select a specific time frame, click the ... buttons and select start and end dates at the top of the page. Click **Update Report** to return the corresponding log entries.

**Note:** It may take a few seconds for the events to make it into the log.

## Mobile Computing

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This section addresses issues related to Secret Server's interaction with mobile devices, such as smart phones.

## Overview

The **Maximum Time for Offline Access on Mobile Devices** setting in Secret Server determines how long to cache secret data on the mobile device. Once the device is not in contact with the server for longer than the specified amount of time, the device removes its cache of the stored secrets. The only way to view secrets on the device once the cache is cleared is to connect to SS again so that the secrets can be re-downloaded and cached.

## Procedure

To set the maximum time:

1. In Secret Server dashboard, click **Admin > Configuration**. The Edit Configuration page appears:

Configuration

[General](#)
[Login](#)
[SAML](#)
[Folders](#)
[Local User Passwords](#)
[Security](#)
[Ticket System](#)
[Email](#)
[Session Recording](#)
[HSM](#)

APPLICATION SETTINGS

Allow Automatic Checks for Software Updates	Yes
<a href="#">Anonymized System Metrics Information</a>	
Send Anonymized System Metrics to Thycotic	Yes <a href="#">View Metric Data</a>
<a href="#">View Webservices</a>	
Enable Webservices	Yes
Maximum Time for Offline Access on Mobile Devices	30 days
Session Timeout for Webservices	20 minutes
Enable Refresh Tokens for Web Services	No
Prevent Application from Sleeping When Idle	Yes

2. On the **General** tab, click the **Edit** button at the bottom of the page.
3. Click to select the **Enable Webservices** check box in the **Application Settings** section:

[View Webservices](#)

**Enable Webservices** ☒

[Maximum Time Offline Explanation](#)

**Maximum Time for Offline Access on Mobile Devices**

**Days**

**Hours**

**Session Timeout for Webservices**

☐ Unlimited

**Days**

**Hours**

**Minutes**

**Enable Refresh Tokens for Web Services** ☐

4. Type your preferred interval in the **Days** and **Hours** text boxes in the **Maximum Time for Offline Access on Mobile Devices** section.

**Note:** Setting the Maximum Time Offline to less than hour prevent the device from caching as the cache window is too small.

**Note:** Because caching all secrets creates an audit record in the database for each secret, we recommend not setting the window too short so that users constantly need to cache all secrets.

5. Click the **Save** button at the bottom of the page.

## Example

An example of a cache window:

If Maximum Offline Time is set to 7 days, a iPhone user can cache secrets. If the iPhone has connectivity every hour the iPhone is used, it will check in with the server. Each time the iPhone checks in the 7 days, the cache window is extended. Thus, if the user uses the app once every 7 days, the app cache will remain. If the user does not have connectivity (such as in Airplane Mode) or does not turn on the app for longer than 7 days, then the next time the app is used the cache will be cleared because the maximum allowed time offline has been surpassed.

## Secret Server Networking

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

**Note:** This is for Secret Server version 7.1 and later.

Once Secret Server is installed, it may be necessary to change the connection string that SS uses to connect to its database. You must be authenticated to access SS and have the Administer Configuration role permission.

1. Click **Admin > See All**.
2. Type **Database** in the search text box and select **Database** in the dropdown list. The Database Configuration page appears:

## Help

Secret Server supports Microsoft SQL Server versions 2012, 2014, 2016, 2017, and Express.

View [Collation Requirements](#). Need help installing or configuring SQL Server? View [Installing and Configuring SQL KB Article](#).

### Database Configuration

#### SQL SERVER LOCATION

Server Name	QA-CUST-SQL-01
Database	SS_Playground

#### SQL AUTHENTICATION

☒ Windows Authentication using Application Identity (GAMMA\ss\_iis\_svc) - **Recommended**  
*(Advanced Setting. Windows Authentication requires a Service Account and advanced IIS setup. Detailed in [Windows Authentication KB](#).)*

☐ SQL Server Authentication *(SQL Authentication requires Mixed Mode. See setup in [SQL Authentication KB](#).)*

#### [+] ADVANCED (NOT REQUIRED)

Edit

View Audit

3. Click the **Edit** button. The page enters edit mode:

## Help

Secret Server supports Microsoft SQL Server versions 2012, 2014, 2016, 2017, and Express.

View [Collation Requirements](#). Need help installing or configuring SQL Server? View [Installing and Configuring SQL KB Article](#).

### Database Configuration



This page modifies the Secret Server database connection settings, which are stored in C:\inetpub\wwwroot\Playground\database.config. This file can be backed up to revert or simply return to this page to reset the connection again. If you need to modify TMS database settings navigate to /setup/database/connectdatabase in the TMS web site.

#### SQL SERVER LOCATION

Server Name \* QA-CUST-SQL-01

*For example:*

*localhost*

*(local)*

*MYDBSERVER*

*localhost\SQLEXPRESS*

Database \* SS\_Playground

#### SQL AUTHENTICATION

☒ Windows Authentication using Application Identity (GAMMA\ss\_iis\_svc) - **Recommended**

*(Advanced Setting. Windows Authentication requires a Service Account and advanced IIS setup. Detailed in [Windows Authentication KB](#).)*

☐ SQL Server Authentication *(SQL Authentication requires Mixed Mode. See setup in [SQL Authentication KB](#).)*

#### [+] ADVANCED (NOT REQUIRED)



Save Database Connection Settings



Cancel

- Edit the parameters as desired.
- Click the **Save Database Connection Settings** button. A confirmation message appears. SS recycles its application pool (needed to clear the connection string cache), and then returns you to the SS dashboard.

## Introduction

This document addresses RabbitMQ naming conventions for its queues. These queues are useful for application troubleshooting and proactive application monitoring.

Secret Server is an asynchronous message-based system where operational instructions and data are passed back and forth between various components running in Web nodes or distributed Engines. A GUI interaction to perform an action, such as heartbeat, remote password change, or bulk operations publishes a message and then returns control back to the user. RabbitMQ is the message bus or broker that facilitates the message traffic.

**Note:** All SS messages are encrypted on the bus, so you cannot peek into the message contents during transit.

**Note:** Messages have a lifetime, and consumers discard expired messages. Therefore, any accumulation or backup of messages in any queue is abnormal and indicative of an application problem.

## Secret Server Roles

Secret Server divides its functionality by named and unnamed roles, and only named roles are configurable in a Web node via the GUI.

**Table:** Secret Server Roles Related to Message Queues

Background Worker	Named	Background work initiated by a task, schedule or UI interaction. Final action of the work might be done in the current Web node, another Web node or sent to a distributed Engine to complete.
Engine	Unnamed	Processes work related to but not limited to: Active Directory synchronization, discovery, heartbeat, and remote password change.
Engine Worker	Named	Processes the response sent back from an engine.
Session Recording Worker	Named	Background work dedicated to session recording processing.
UI	Unnamed	IIS/ASP.NET processing, inbound access controlled by a load balancer.
API	Unnamed	IIS/ASP.NET processing, inbound access controlled by a load balancer.

[Unexpected Link Text](#)

## Queue Names

A queue name is divided into three major sections with a colon (:) delimiter between each section:

Section1:Section2:Section3

### Section1

Section1 represents a RabbitMQ exchange name. There are three predetermined exchange names, two legacy predetermined exchange names, and then a variable number of exchanges determined by the number of SS sites.

**Table:** RabbitMQ Exchange Names

Background Worker	thycotic-ss	Predetermined	Web Node	
Engine	Site Name	Variable	Web Node or Distributed Engine	The out-of-the-box local site can be configured for either a Web node or a distributed engine. Any other site name is processed by a distributed engine.
Engine Worker	thycotic-ss-engine-response	Predetermined	Web Node	
Session Recording Worker	thycotic-sessionrec	Predetermined	Web Node	
Session Recording Worker	thycotic-sr	Predetermined-Legacy	Web Node	Legacy: background work dedicated to session recording processing.
Session Recording Worker	thycotic-sr-agent-response	Predetermined-Legacy	Web Node	Legacy: processes data sent by an advanced session recoding agent.

## [Unexpected Link Text](#)

Variable site exchanges: If the SS site is called local, then local: will also be the exchange name. If the Site is called Mars, then Mars: will be the exchange name.

## Section2

Section2 typically has a name which represents a functional area in SS code that is a consumer of the message.

## Section3

Section3 represents the message name.

## Secret Server Roles and Queues

This section of the message associates roles with queues and breaks the down by product functionality. Functionality can span multiple roles, for example, discovery is done by background worker, engine and engine worker roles while event pipelines is only done by a background worker role.

## Background Worker Role Queues

List of queues for background worker's functional areas:

## Active Directory Synchronization

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ActiveDirectorySynchronization.SynchronizationConsumer:Thycotic.ihawu.Business.Messages.Areas.ActiveDirectorySynchronization.Request.RunNowSynchronizationMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ActiveDirectorySynchronization.SynchronizationConsumer:Thycotic.ihawu.Business.Messages.Areas.ActiveDirectorySynchronization.Request.SynchronizationMessage

## Bulk Operation

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.BulkOperation.BulkOperationConsumer:Thycotic.ihawu.Business.Messages.Areas.BulkOperation.Request.BulkOperationMessage

## ConnectWise Integration

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ConnectWise.ConnectWiseConsumer:Thycotic.ihawu.Business.Messages.Areas.ConnectWise.Request.ConnectWiseMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ConnectWise.ConnectWiseConsumer:Thycotic.ihawu.Business.Messages.Areas.ConnectWise.Request.RunNowConnectWiseMessage

## Discovery

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.ComputerScanConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.ComputerScanMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.ComputerScanConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.RunNowComputerScanMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.DiscoveryConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.DiscoveryMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.DiscoveryConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.RunNowDiscoveryMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.DiscoveryRuleApplierConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.RunDiscoveryRuleApplierMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.SecretComputerMatcherConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.RunNowSecretComputerMatcherMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Discovery.SecretComputerMatcherConsumer:Thycotic.ihawu.Business.Messages.Areas.Discovery.Request.SecretComputerMatcherMessage

## Duo Integration

- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.Duo.DuoAuthConsumer:Thycotic.Messages.ihawu.Areas.Duo.DuoRequestMessage

## Email Processing

- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.Email.SendEmailConsumer:Thycotic.Messages.ihawu.Areas.Email.Request.SystemSendEmailMessage
- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.Email.VerifySendEmailConsumer:Thycotic.Messages.ihawu.Areas.Email.Request.VerifySendEmailRequest

## Event Pipelines

- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.EventPipelines.EventPipelineActivityConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.EventPipelineActivityEventMessage
- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.EventPipelines.PipelinePolicyProcessConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelinePoliciesProcessBlockingMessage
- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.EventPipelines.PipelinePolicyProcessConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelinePoliciesProcessMessage
- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.EventPipelines.PipelineProcessConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelineProcessBlockingMessageWithPolicies
- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.EventPipelines.PipelineProcessConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelineProcessMessageWithPolicies
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.EventPipelines.PipelinePolicyProcessEventConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelinePolicyProcessEventBlockingMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.EventPipelines.PipelinePolicyProcessEventConsumer:Thycotic.Messages.ihawu.Areas.EventPipelines.Request.PipelinePolicyProcessEventMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.EventPipelines.PipelineProcessScheduledEventConsumer:Thycotic.ihawu.Business.Messages.Areas.EventPipelines.ProcessPipelineScheduledEventMessage

## Heartbeat and Remote Password Change

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.CheckinExpiredCheckedoutSecretConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.CheckinExpiredCheckedoutSecretMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ExpiredSecretLocalPasswordChangeConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.ExpiredSecretLocalPasswordChangeMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ExpiredSecretLocalPasswordChangeConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.RunNowExpiredSecretLocalPasswordChangeMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ExpiredSecretPasswordChangeConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.ExpiredSecretPasswordChangeMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ExpiredSecretPasswordChangeConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.RunNowExpiredSecretPasswordChangeMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ProcessHeartbeatConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.ProcessHeartbeatMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ProcessHeartbeatConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.RunNowProcessHeartbeatMessage
- thycotic-

ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ProcessLocalHeartbeatConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.ProcessLocalHeartbeatMessage

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RemotePasswordChanging.ProcessLocalHeartbeatConsumer:Thycotic.ihawu.Business.Messages.Areas.RemotePasswordChanging.Request.RunNowProcessLocalHeartbeatMessage

## Import

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Import.SecretImportConsumer:Thycotic.ihawu.Business.Messages.Import.SecretImportBulkMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Import.SecretImportFileConsumer:Thycotic.ihawu.Business.Messages.Import.SecretImportFileMessage

## Management: Backup, and Cleanup

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.OnPremisesOnly.BackgroundWorkerTaskConsumer:Thycotic.ihawu.Business.Messages.Areas.OnPremisesOnly.BackgroundWorkerTaskMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.OnPremisesOnly.BackupConsumer:Thycotic.ihawu.Business.Messages.Areas.OnPremisesOnly.BackupMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.OnPremisesOnly.BackupConsumer:Thycotic.ihawu.Business.Messages.Areas.OnPremisesOnly.RunNowBackupMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.OnPremisesOnly.GenerateSLMConsumer:Thycotic.ihawu.Business.Logic.Areas.OnPremisesOnly.GenerateSLMMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.SessionArchiving.RecordedSessionsArchiveConsumer:Thycotic.ihawu.Business.Messages.Areas.SessionArchiving.Request.ArchiveRecordedSessionsMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.SessionArchiving.RecordedSessionsArchiveConsumer:Thycotic.ihawu.Business.Messages.Areas.SessionArchiving.Request.DeleteRecordedSessionsMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.SessionArchiving.RecordedSessionsArchiveConsumer:Thycotic.ihawu.Business.Messages.Areas.SessionArchiving.Request.RunNowDeleteRecordedSessionsMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.TruncateRecords.TruncateRecordsConsumer:Thycotic.ihawu.Business.Messages.Areas.TruncateRecords.TruncateRecordsForAllConfigurationsMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.TruncateRecords.TruncateRecordsConsumer:Thycotic.ihawu.Business.Messages.Areas.TruncateRecords.TruncateRecordsForConfigurationMessage
- thycotic-ss:Thycotic.MessageQueue.Common.Consumers.AutomaticSink.CreateAutomaticSinkConsumer:Thycotic.MessageQueue.Common.Messages.AutomaticSink.Request.CreateAutomaticSinkMessage

## Distributed Engine Management

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.DistributedEngine.EngineStatusUpdateConsumer:Thycotic.ihawu.Business.Messages.Areas.DistributedEngine.Request.EngineStatusUpdateMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.DistributedEngine.TruncateEngineLogConsumer:Thycotic.ihawu.Business.Messages.Areas.DistributedEngine.Request.TruncateEngineLogMessage

## Password Generation

- thycotic-

ss:Thycotic.ihawu.Business.Logic.Areas.PasswordGeneration.GeneratePasswordConsumer:Thycotic.ihawu.Business.Messages.Areas.PasswordGeneration.Request.GeneratePasswordMessage

## Reports

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Report.EmailReportConsumer:Thycotic.Messages.ihawu.Areas.Email.Request.EmailReportMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Report.ScheduledReportConsumer:Thycotic.ihawu.Business.Messages.Areas.Reports.Request.ProcessReportsMessage

## Run Now

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessDashboardJsonValidationConsumer:Thycotic.ihawu.Business.Messages.Areas.RunOnceTasks.RunNowProcessDashboardJsonValidationMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessFieldEncryptionChangesConsumer:Thycotic.ihawu.Business.Messages.Areas.RunOnceTasks.RunNowProcessFieldEncryptionChangesMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessFieldEncryptionChangesConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.ProcessFieldEncryptionChangesMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessSecretKeyRotationConsumer:Thycotic.ihawu.Business.Logic.Areas.SecretKeyRotation.Messages.RunNowProcessSecretKeyRotationMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessSecretPolicyChangesConsumer:Thycotic.ihawu.Business.Messages.Areas.RunOnceTasks.RunNowProcessSecretPolicyChangesMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowProcessSecretPolicyChangesConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.ProcessSecretPolicyChangesMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.RunOnceTasks.RunNowToggleHsmConsumer:Thycotic.ihawu.Business.Logic.Areas.SecretKeyRotation.Messages.RunNowToggleHsmMessage

## Scheduled Tasks

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.DatabaseCleanupConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.DatabaseCleanupMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.EventQueueMonitorConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.EventQueueMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.ExpiringLicenseTaskConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.ExpiringLicenseTaskMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.ExpiringSecretTaskConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.ExpiringSecretTaskMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.PasswordRequirementConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.PasswordRequirementMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.SqlReplicationConflictConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.SqlRepl

icationConflictMessage

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ScheduledTask.TruncateDatabaseCacheConsumer:Thycotic.ihawu.Business.Messages.Areas.ScheduledTask.Request.TruncateDatabaseCacheMessage

## Search

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.ProxySessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.ProxySessionDataHashIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.ProxySessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.ProxySessionDataHashReIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.ProxySessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RunNowProxySessionDataHashReIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.RdpSessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RdpSessionDataHashIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.RdpSessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RdpSessionDataHashReIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.RdpSessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RunNowRdpSessionDataHashReIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.SecretItemHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RunNowSecretItemHashIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.SecretItemHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.SecretItemHashIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.SessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.RunNowSessionDataHashReIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.SessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.SessionDataHashIndexRequest
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Search.SessionDataHashConsumer:Thycotic.ihawu.Business.Messages.Areas.Search.Request.SessionDataHashReIndexRequest

## SSH Terminal

- thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.SSHTerminal.TerminalCommandBackgroundConsumer:Thycotic.Messages.DE.Server.Areas.SSHTerminal.Request.TerminalCommandMessage

## Thycotic Privilege Behavior Analytics Integration

- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaAppendMetadataSinkConsumer:Thycotic.Messages.SA.Areas.Metadata.Request.SAAppendMetadataSinkMessage
- thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaCreateMetadataSinkConsumer:Thycotic.Messages.SA.Areas.Metadata.Request.SACreateMetadataSinkMessage

- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaDirectiveConsumer:Thycotic.ihawu.Business.Messages.Areas.PBA.Request.DirectiveProcessMessage`
- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaEventConsumer:Thycotic.Messages.SA.Areas.EventData.Request.SAEventMessage`
- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaEventUploadConsumer:Thycotic.Messages.SA.Areas.EventData.Request.SAEventUploadMessage`
- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.Pba.PbaMetadataUploadConsumer:Thycotic.Messages.SA.Areas.Metadata.Request.SAMetadataUploadMessage`
- `thycotic-ss:Thycotic.SecurityAnalytics.DataUploader.Consumers.DirectiveAddConsumer:Thycotic.Messages.SA.Areas.Directive.Request.SADirectiveSendMessage`
- `thycotic-ss:Thycotic.SecurityAnalytics.DataUploader.Consumers.DirectiveCheckConsumer:Thycotic.Messages.SA.Areas.Directive.Request.SADirectiveCheckMessage`
- `thycotic-ss:Thycotic.SecurityAnalytics.DataUploader.Consumers.HealthCheckConsumer:Thycotic.Messages.SA.Areas.Status.Request.SAHealthCheckMessage`
- `thycotic-ss:Thycotic.SecurityAnalytics.DataUploader.Consumers.HeartbeatConsumer:Thycotic.Messages.SA.Areas.Status.Request.SAHeartbeatMessage`

## Thycotic Privilege Manager Integration

- `thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.TmsNotifications.NotifyTmsDatabaseUpdatedConsumer:Thycotic.Messages.ihawu.Areas.TmsNotifications.Request.NotifyTmsDatabaseUpdatedMessage`
- `thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.TmsNotifications.NotifyTmsEmailSettingsUpdatedConsumer:Thycotic.Messages.ihawu.Areas.TmsNotifications.Request.NotifyTmsEmailSettingsUpdatedMessage`
- `thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.TmsNotifications.NotifyTmsLicenseUpdatedConsumer:Thycotic.Messages.ihawu.Areas.TmsNotifications.Request.NotifyTmsLicenseUpdatedMessage`

## Thycotic Telemetry

- `thycotic-ss:Thycotic.ihawu.BackgroundWorker.Logic.Areas.Telemetry.TelemetryConsumer:Thycotic.Messages.ihawu.Areas.Telemetry.Request.SendAnonymousTelemetryMessage`

## Thycotic One Identify Provider Integration

- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ThycoticOne.ThycoticOneSyncUserConsumer:Thycotic.ihawu.Business.Messages.Areas.ThycoticOne.Request.ThycoticOneScheduledSyncMessage`
- `thycotic-ss:Thycotic.ihawu.Business.Logic.Areas.ThycoticOne.ThycoticOneSyncUserConsumer:Thycotic.ihawu.Business.Messages.Areas.ThycoticOne.Request.ThycoticOneSyncUserMessage`

## Engine Role Queues

List of queues for engines' functional areas.

**Note:** In the example listed below, the SS site name is called "Gamma-Engines".

## Active Directory Synchronization

- `Gamma-Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.ADSyncRequestConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.ADSyncMessage`
- `Gamma-Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.AllUsersByDomainQueryConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.AllUsersByDomainQueryMessage`
- `Gamma-Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.GenericQueryConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.GroupsAndM`

embersQueryMessage

- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.GenericQueryConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.GroupsByDo  
mainQueryMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.GenericQueryConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.UsersByGrou  
psQueryMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.ResolveDomainNameConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.Resol  
veDomainDistinguishedNameMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.ActiveDirectory.ResolveDomainNameConsumer:Thycotic.Messages.DE.Engine.Areas.ActiveDirectory.Request.Resol  
veFullyQualifiedDomainNameMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.Authentication.AuthenticateByAdConsumer:Thycotic.Messages.DE.Engine.Areas.Authenticate.Request.Authenticate  
ByAdMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.AdSync.Areas.General.DomainCredentialTestConsumer:Thycotic.Messages.DE.Engine.Areas.General.Request.DomainCredentialTe  
stMessage

## Discovery

- Gamma-  
Engines:Thycotic.DE.Feature.SS.LocalAccountDiscovery.Areas.Discovery.HostRangeConsumer:Thycotic.Messages.DE.Engine.Areas.Discovery.Request.ScanHostR  
angeMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.LocalAccountDiscovery.Areas.Discovery.HostRangeConsumer:Thycotic.Messages.DE.Engine.Areas.Discovery.Request.SpecificOu  
ScanHostRangeMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.LocalAccountDiscovery.Areas.Discovery.LocalAccountConsumer:Thycotic.Messages.DE.Engine.Areas.Discovery.Request.ScanLoc  
alAccountMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.LocalAccountDiscovery.Areas.Discovery.MachineConsumer:Thycotic.Messages.DE.Engine.Areas.Discovery.Request.ScanMachine  
Message

## Heartbeat, Remote Password Change, and Dependency

- Gamma-  
Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.BlockingChangePasswordConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Request.Bl  
ockingPasswordChangeMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.BlockingPrivilegeChangePasswordConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Re  
quest.BlockingPrivilegedPasswordChangeMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.Heartbeat.SecretHeartbeatConsumer:Thycotic.Messages.DE.Engine.Areas.Heartbeat.Request.SecretHear  
tbeatMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.SecretBasicChangePasswordConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Reques  
t.SecretBasicPasswordChangeMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.SecretPrivilegeChangePasswordConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Req  
uest.SecretPrivilegedPasswordChangeMessage

- Gamma-Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.SecretRunDependenciesConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Request.SecretChangeDependencyMessage Gamma-Engines:Thycotic.DE.Feature.SS.PasswordChanging.Areas.Verification.VerifyPasswordConsumer:Thycotic.Messages.DE.Engine.Areas.Verify.Request.VerifyPasswordMessage
- Gamma-Engines:Thycotic.DE.Feature.SS.ServiceAccountManagement.Areas.Dependency.DependencyConsumer:Thycotic.Messages.DE.Engine.Areas.Discovery.Request.SecretDependencyMessage
- Gamma-Engines:Thycotic.DE.Feature.SS.ServiceAccountManagement.Areas.Dependency.SecretTestDependencyConsumer:Thycotic.Messages.DE.Engine.Areas.PasswordChanging.Request.SecretTestDependencyMessage

## Management

- Gamma-Engines:Thycotic.DistributedEngine.Logic.Areas.Connectivity.PingConsumer:Thycotic.Messages.DE.Engine.Areas.Connectivity.Request.PingMessage
- Gamma-Engines:Thycotic.MessageQueue.Common.ConsumersAutomaticSink.CreateAutomaticSinkConsumer:Thycotic.MessageQueue.Common.MessagesAutomaticSink.Request.CreateAutomaticSinkMessage

## Proxy

- Gamma-Engines:Thycotic.DE.Feature.SS.RdpProxy.AssignProxiedRdpSessionConsumer:Thycotic.Messages.DE.Engine.Areas.RDPProxy.Request.AssignProxiedRdpSessionMessage
- Gamma-Engines:Thycotic.DE.Feature.SS.SshProxy.Areas.Proxy.AssignProxiedSessionConsumer:Thycotic.Messages.DE.Engine.Areas.SSHProxy.Request.AssignProxiedSessionMessage

## Scripting

- Gamma-Engines:Thycotic.DistributedEngine.Logic.Areas.Script.ScriptConsumer:Thycotic.Messages.DE.Engine.Areas.Script.Request.PowerShellScriptMessage
- Gamma-Engines:Thycotic.DistributedEngine.Logic.Areas.Script.ScriptConsumer:Thycotic.Messages.DE.Engine.Areas.Script.Request.SqlScriptMessage
- Gamma-Engines:Thycotic.DistributedEngine.Logic.Areas.Script.ScriptConsumer:Thycotic.Messages.DE.Engine.Areas.Script.Request.SshScriptMessage

## Syslog Integration

- Gamma-Engines:Thycotic.DE.Feature.SS.AdvancedAuditing.Areas.SIEM.SysLogConsumer:Thycotic.Messages.DE.Engine.Areas.SIEM.Request.SysLogMessage

## Thycotic Privilege Behavior Analytics Integration

- Gamma-Engines:Thycotic.DE.Feature.SS.Pba.Areas.Event.PbaEventConsumer:Thycotic.Messages.SA.Areas.EventData.Request.SAEventMessage
- Gamma-Engines:Thycotic.DE.Feature.SS.Pba.Areas.Metadata.PbaAppendMetadataSinkConsumer:Thycotic.Messages.SA.Areas.Metadata.Request.SAAppendMetadataSinkMessage
- Gamma-Engines:Thycotic.DE.Feature.SS.Pba.Areas.Metadata.PbaCreateMetadataSinkConsumer:Thycotic.Messages.SA.Areas.Metadata.Request.SACreateMetadataSinkMessage
- Gamma-Engines:Thycotic.SecurityAnalytics.DataUploader.Consumers.DirectiveAddConsumer:Thycotic.Messages.SA.Areas.Directive.Request.SADirectiveSendMessage
- Gamma-Engines:Thycotic.SecurityAnalytics.DataUploader.Consumers.DirectiveCheckConsumer:Thycotic.Messages.SA.Areas.Directive.Request.SADirectiveCheckMessage
- Gamma-Engines:Thycotic.SecurityAnalytics.DataUploader.Consumers.HealthCheckConsumer:Thycotic.Messages.SA.Areas.Status.Request.SAHealthCheckMessage
- Gamma-Engines:Thycotic.SecurityAnalytics.DataUploader.Consumers.HeartbeatConsumer:Thycotic.Messages.SA.Areas.Status.Request.SAHeartbeatMessage

## Ticketing System Integration

- Gamma-  
Engines:Thycotic.DE.Feature.SS.SecretWorkflow.Areas.TicketingSystem.TicketingAddCommentConsumer:Thycotic.Messages.DE.Engine.Areas.TicketingSystem.Request.TicketingAddCommentBasicRequest
- Gamma-  
Engines:Thycotic.DE.Feature.SS.SecretWorkflow.Areas.TicketingSystem.TicketingAddCommentConsumer:Thycotic.Messages.DE.Engine.Areas.TicketingSystem.Request.TicketingAddCommentMessage
- Gamma-  
Engines:Thycotic.DE.Feature.SS.SecretWorkflow.Areas.TicketingSystem.TicketingGetStatusConsumer:Thycotic.Messages.DE.Engine.Areas.TicketingSystem.Request.TicketingGetStatusMessage

## Engine Worker Role Queues

List of queues for engine worker's functional areas:

### Active Directory Synchronization

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.ActiveDirectory.ActiveDirectorySynchronizationConsumer:Thycotic.Messages.DE.Server.Areas.ActiveDirectory.Request.ADSyncMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.ActiveDirectory.AllUsersByDomainQueryConsumer:Thycotic.Messages.DE.Server.Areas.ActiveDirectory.Request.AllUsersByDomainQueryMessage

### Discovery

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Discovery.ScanDependencyConsumer:Thycotic.Messages.DE.Server.Areas.Discovery.Request.ScanDependencyMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Discovery.ScanHostRangeResponseConsumer:Thycotic.Messages.DE.Server.Areas.Discovery.Request.ScanHostRangeMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Discovery.ScanLocalAccountConsumer:Thycotic.Messages.DE.Server.Areas.Discovery.Request.ScanLocalAccountMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Discovery.ScanMachineResponseConsumer:Thycotic.Messages.DE.Server.Areas.Discovery.Request.ScanMachineMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Discovery.SpecificOuScanHostRangeResponseConsumer:Thycotic.Messages.DE.Server.Areas.Discovery.Request.SpecificOuScanHostRangeMessage

### RDP Proxy, SSH Proxy, and SSH Terminal

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.RDPProxy.AppendKeystrokeDataConsumer:Thycotic.Messages.DE.Engine.Areas.RDPProxy.Request.AppendKeystrokeDataMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.AppendSessionDataConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.AppendSessionDataMessage

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.CloseSecretSessionConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.EndSessionDataMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.EndRdpProxySessionConsumer:Thycotic.Messages.DE.Engine.Areas.RDPProxy.Request.EndRdpProxySessionMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.GetStatusUpdatesRequestConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.GetStatusUpdatesMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.InitiateRDPProxiedSessionConsumer:Thycotic.Messages.DE.Engine.Areas.RDPProxy.Request.InitiateProxiedRdpSessionMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.InitiateSSHProxiedSessionConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.InitiateProxiedSessionMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.InitiateSshSessionDataCaptureSinkConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.InitiateProxiedSessionDataCaptureSinkMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.RdpProxySessionStatusesConsumer:Thycotic.Messages.DE.Engine.Areas.RDPProxy.Request.GetRdpProxySessionStatusesMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.UpdateSessionsRequestConsumer:Thycotic.Messages.DE.Server.Areas.SSHProxy.Request.UpdateSessionsMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHProxy.UpdateUserPasswordRequestConsumer:Thycotic.Messages.DE.Server.Areas.SSHTerminal.Request.UpdateUserPasswordMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SSHTerminal.TerminalCommandEngineConsumer:Thycotic.Messages.DE.Server.Areas.SSHTerminal.Request.TerminalCommandMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.UserSession.CloseUserSessionConsumer:Thycotic.Messages.DE.Server.Areas.UserSession.CloseUserSessionMessage

## Syslog Integration

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.SEIM.SysLogResultResponseConsumer:Thycotic.Messages.DE.Server.Areas.SEIM.Request.SysLogResultMessage

## Heartbeat, Remote Password Change, and Dependency

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Dependency.DependencyChangeConsumer:Thycotic.Messages.DE.Server.Areas.Dependency.Request.DependencyChangeMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Heartbeat.SecretHeartbeatConsumer:Thycotic.Messages.DE.Server.Areas.Heartbeat.Request.SecretHeartbeatMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.PasswordChanging.RemotePasswordChangeResponseStoreConsumer:Thycotic.Messages.DE.Server.Areas.PasswordChanging.Request.RemotePasswordChangeMessage

## Thycotic Privilege Behavior Analytics Integration

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.PasswordChanging.PbaDisableConsumer:Thycotic.Messages.DE.Server.Areas.PBA.PbaDisableMessage

## Distributed Engine Management

- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Connectivity.PingConsumer:Thycotic.Messages.DE.Server.Areas.Connectivity.Request.PingMessage
- thycotic-ss-engine-  
response:Thycotic.ihawu.EngineWorker.Logic.Areas.Maintenance.LogConsumer:Thycotic.Messages.DE.Server.Areas.Maintenance.Request.EngineLogMessage
- thycotic-ss-engine-  
response:Thycotic.MessageQueue.Common.Consumers.AutomaticSink.CreateAutomaticSinkConsumer:Thycotic.MessageQueue.Common.Messages.AutomaticSink.  
Request.CreateAutomaticSinkMessage

## Session Recording Worker

List of queues for session recording worker's functional areas:

### Post Recording

- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostMetadataConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.Requ  
est.ProcessUploadedMetadataMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostRecordedSessionConsumer:Thycotic.Messages.DE.Server.Areas.Advanced  
SessionRecording.Request.RecordedSessionChunkMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostRecordedSessionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecordi  
ng.Request.ProcessBusStreamedSessionMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostRecordedSessionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecordi  
ng.Request.ProcessUploadedSessionMessage

### Video Conversion

- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R  
equest.ConvertAllVideosMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R  
equest.ConvertVideoMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R  
equest.DeleteOldCompletedImagesMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R  
equest.RunNowConvertVideoMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R  
equest.RunNowSetStatusForTimedOutSessionsMessage
- thycotic-  
sessionrec:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.VideoConversionConsumer:Thycotic.Messages.ihawu.Areas.SessionRecording.R

equest.SetStatusForTimedOutSessionsMessage

## Post Recording (Legacy)

- thycotic-sr-agent-  
response:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostMetadataConsumer:Thycotic.Messages.DE.Server.Areas.AdvancedSessionRecording.Request.PostMetadataMessage
- thycotic-sr-agent-  
response:Thycotic.ihawu.SessionRecordingWorker.Logic.Areas.SessionRecording.PostRecordedSessionConsumer:Thycotic.Messages.DE.Server.Areas.AdvancedSessionRecording.Request.PostRecordedSessionMessage

## Management

- thycotic-sessionrec:Thycotic.MessageQueue.Common.ConsumersAutomaticSink.CreateAutomaticSinkConsumer:Thycotic.MessageQueue.Common.MessagesAutomaticSink.Request.CreateAutomaticSinkMessage

## Overview

The RDP Proxying feature allows RDP connections, established using a launcher, to be routed through SS. You can set it up one of two ways:

- Recommended method: The launcher connects to the newer RDP proxy with temporary credentials, and the RDP proxy connects to the remote server using the protected credentials from the secret. This method is preferred because it prevents the secret credentials from reaching the client machine. For this method, you simply configure the RDP proxy.
- Alternative method: The launcher uses an SSH proxy to tunnel a local RDP connection to a remote server. This method does not protect the credential from reaching the client machine. For this method you configure the SSH proxy and enable SSH tunneling.

**Note:** We provide the alternate method to support legacy installations and troubleshooting (it can potentially be more stable when the RDP proxy does not work).

These two approaches to RDP proxying are not compatible—you may use one or the other but not both. We performance tested both methods. Either can support 100 concurrent connections.

## Recommended Method

### How It Works

1. The user clicks the RDP launcher in SS.
2. The launcher executes on the client's machine.
3. The launcher establishes a connection to the RDP Proxy using credentials generated for the session. These credentials are short lived and can only be used once.
4. Once the launcher has successfully authenticated with the RDP proxy, the RDP proxy looks up the credentials and target hostname to connect to.

**Note:** The secret credentials *do not* get served to the client machine in this flow, which improves credential security.

5. The RDP proxy connects to the desired remote host with the secret credentials.
6. The RDP session is established.
7. RDP traffic is sent back and forth over the RDP proxy, session keystrokes are monitored if session recording is enabled.

## Configuration

1. Navigate to the **Admin > Proxying** page.
2. Click the **RDP Proxy** tab.

Admin > Proxying

SSH Proxy **RDP Proxy** Endpoints Proxy Audit

The RDP proxy is currently running on 0 site(s) and 0 engine(s). Please see the Endpoints tab for more details.

**RDP Proxy Settings**

- Secret Server can proxy Remote Desktop connections through a Distributed Engine to a Windows end point.
- You can configure your SSH server to only accept connections from the proxy, thus forcing all connections through Secret Server.
- With Session Recording enabled, you will be able to record keystrokes sent during RDP proxy sessions
- To enable RDP proxying, install at least one Distributed Engine and specify the Public Host and Bind IP address.
- Secrets with launchers which support proxying can have it enabled or disabled on an individual basis from their security tab. This setting can also be set via Secret Policy.

Enable RDP Proxy	Yes	<a href="#">Edit</a>
RDP Proxy Port	3390	<a href="#">Edit</a>
Validate Remote Certificates	Yes	<a href="#">Edit</a>
Allow AD Site Selection	Yes	<a href="#">Edit</a>
Proxy New Secrets By Default	Yes	<a href="#">Edit</a>
Days to Keep Operational Logs	30	<a href="#">Edit</a>
RDP Server Certificate	thyp2.pfx	<a href="#">Edit</a> <a href="#">Generate Self-Signed</a>

- If necessary, enable the RDP proxy.
- Click the **Endpoints** tab to ensure that your server nodes, sites, and engines are properly configured.
- Proxied RDP secrets now launch into the RDP proxy using short-lived credentials, protecting the secret credentials from the client machine.

## Configuration Settings

The RDP proxy configuration settings for the recommended method:

- Enable RDP Proxy:** This setting determines whether or not the RDP proxy is enabled
- RDP Proxy Port:** This setting is the port that the RDP proxy runs on (defaulting to 3390). You usually cannot set this to 3389 as that port is already occupied by default by the Windows operating system.
- Validate Remote Certificates:** Thycotic recommends that you operate in an environment where RDP server certificates are created by a controlled CA and are trusted by machines in the domain. If that is not possible, you can disable remote certificate validation to allow connection to machines that do not serve trusted certificates.
- Allow AD site selection:** This setting allows you to select any configured sites when using the RDP launcher on an Active Directory secret. This allows a secret credential to access machines that may exist in different network boundaries.
- Proxy New Secrets By Default:** This setting determines if SSH and RDP secrets are created with "Proxy Enabled" set by default. This setting is shared with the SSH proxy configuration.
- Days To Keep Operational Logs:** This setting determines how long, in days, the operational logs for the RDP proxy are kept.
- RDP Server Certificate:** This setting is the certificate that is served to the clients who connect to the RDP proxy. You can generate a certificate for a given DNS name, or you can upload your own.

## Alternative Method

**Note:** This approach is not recommended as it exposes the secret credentials to the client machine.

## How It Works

- The user clicks the RDP launcher in SS.

2. The launcher executes on the client's machine.
3. The launcher establishes a connection to the SSH proxy to begin port forwarding.
4. The launcher authenticates with the SSH Proxy.
5. The launcher opens a socket.
6. The launcher listens for a connection on an available ephemeral port (the forwarding port) on the client's machine.
7. RDP launches on the client machine using the secret credentials and connects locally to the forwarding port.
8. All RDP traffic for this session is routed through the SSH tunnel to SS, then forwarded to the target machine.
9. The RDP session is established.

## Configuration

1. Navigate to the **Admin > Proxying** page.

The screenshot shows the 'Admin > Proxying' page in the Delinea interface. At the top, there's a navigation bar with 'SSH Proxy', 'RDP Proxy', 'Endpoints', and 'Proxy Audit'. Below this, a status message states: 'The SSH proxy is currently running on 0 site(s) and 0 engine(s). Please see the Endpoints tab for more details.' The main section is titled 'SSH Proxy Settings' and contains a list of settings on the right and explanatory text on the left.

Setting	Value	Action
Enable SSH Proxy	Yes	<a href="#">Edit</a>
SSH Proxy Port	22	<a href="#">Edit</a>
Enable SSH Tunneling	No	<a href="#">Edit</a>
Proxy New Secrets By Default	Yes	<a href="#">Edit</a>
Enable SSH Proxy Inactivity Timeout	No	<a href="#">Edit</a>
SSH Proxy Banner	Welcome to the Secret Server SSH Proxy	<a href="#">Edit</a>
SSH Proxy Host Fingerprint	SHA1 - 8e:80:65:1f:d8:a7:84:c1:33:f2:80:7f:dc:84:48:d0:41:29:06:c7 MD5 - 99:0b:df:99:15:e4:a1:7f:7c:70:ec:12:87:16:8e:fb	<a href="#">Edit</a> <a href="#">Generate</a>
Days to Keep Operational Logs	50	<a href="#">Edit</a>

SSH Proxy Settings

- Secret Server can proxy connections through a Distributed Engine to an SSH server end point.
- Remote Desktop Sessions can also be proxied if enable SSH tunneling is set.
- You can configure your SSH server to only accept connections from the proxy, thus forcing all connections through Secret Server.
- All proxied traffic can be recorded for security and auditing purposes.
- To enable SSH proxying, install at least one Distributed Engine and specify the Public Host and Bind IP address.
- Secrets with launchers which support proxying can have it enabled or disabled on an individual basis from their security tab. This setting can also be set via Secret Policy.

2. Enable the **Enable SSH Tunneling** option.
3. Click the **Endpoints** tab to ensure that your server nodes, sites, and engines are properly configured.
4. Proxied RDP secrets now launch into the SSH proxy using local port forwarding.

## Known Issues

### "Could not load file or assembly..." Error

Error appears in SS.log or DE.log. Install the most recent version of the .NET Framework to correct it.

### RDP Proxy Does Not Work with FIPS Validation

RDP proxy does not work on machines the have the FIPS validation security policy active. No fix is currently available.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This document is a guide to Thycotic's Secret Server (SS) clusters for administrators and advanced users. SS can run with multiple front-end Web servers. For a critical instance, clustering offers a redundant system to limit potential down time from a single point of failure. Clustering also allows users to load balance for better performance.

## Overview

### Clustering and Background Thread Changes in 10.7.

There are two major architectural changes in SS 10.7:

**Note:** The first change is obvious in the SS user interface, and the second is hidden but very important to those supporting SS.

- **Primary Node:** We eliminated "primary nodes." Previously, some important background operations, such as password changing and heartbeat, would only run from the primary node. Now they run from all nodes. Given that, there is no longer a "Make Primary" button, and the ValidPrimaryNode setting no longer applies.
- **Background Operations:** There are no longer background threads for scheduled operations. Instead, operations are scheduled by Quartz.

## Clustering Overview

With SS clustering, you can easily scale SS for redundancy and performance. Basic SS clustering is simple—you install SS and then copy the installation to to another machine. SS clustering has four core concepts or components:

### Nodes

Each machine with SS installed on it, pointing to the same database, is a *node*. All nodes respond to Web requests and thus are Web servers.

### Backbone Bus

The backbone bus Internally handles all communication between the roles. In a clustered environment, the backbone bus should always be an installed RabbitMq messaging queue. This allows every node in the cluster to help with the workload. If the backbone bus is set to "internal," then each node is using its own internal backbone bus.

### Engine Response Bus

The engine response bus facilitates communication from SS to distributed engines and back.

### Worker Roles

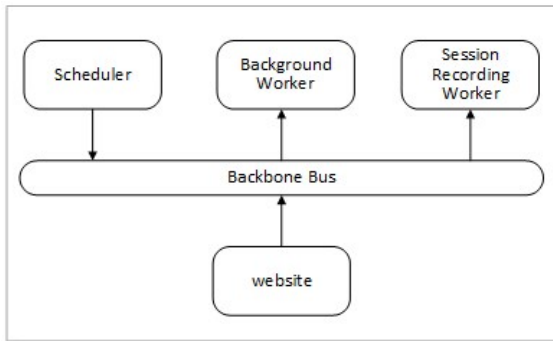
Each node can optionally run one or more worker roles: background Worker, engine worker, and session recording worker. Though they may run on the same machine, the roles do not directly communicate with each other.

Each node that is set to run the background worker role automatically runs the scheduler role as well. The scheduler role is responsible for running the vast majority of SS background operations. It uses Quartz to run "trigger jobs" that send a message on the backbone bus for each scheduled operation. One or more background worker roles then processes those messages.

**Note:** See the article [Troubleshooting Quartz Trigger Jobs](#) for more information about Quartz.

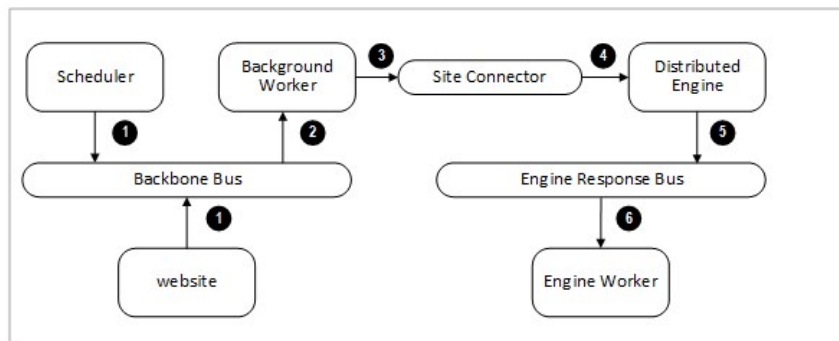
## Component Communication

**Figure:** Secret Server Internal Cluster-Component Communication



Messages are placed on the backbone bus by the Scheduler role and the website. Messages are retrieved from the backbone bus.

**Figure:** Secret Server Distributed Engine Communication



1. Manual or scheduled operation.
2. Background worker processes a message.
3. Outbound messages (password changes, heartbeats, and others) are placed on the site connector.
4. Distributed engine performs the operation.
5. Engine worker processes the response.

## Server Node Configurations

The work an individual node handles depends entirely on which boxes are checked on the Server Nodes page (in edit mode):

Server Nodes									
MACHINE NAME (ID)	BINARY VERSION	DATABASE	ERROR MESSAGE	LAST CONNECTED	IN CLUSTER	BACKGROUND WORKER	ENGINE WORKER	SESSION RECORDING WORKER	MAINTENANCE MODE
QA-CUST-01 (1) (Current Node)	10.7.000000	SS_Playground		8/13/2019 5:35:08 PM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Enable Clustering ☐ No

- **In Cluster** is a toggle that turns a server node on or off. If enabled this node can process Web requests, and (if configured) will run the background, engine, and session recording roles. If disabled, the node is just a backup—it cannot run any roles, and trying to access the website on the node will redirect to the server nodes page.
- **Background Worker** is a toggle for all background operations, such as password changing, heartbeat, and discovery. When it is set to false, only the bulk operations, password generation, email, and secret import operations run on the node. See the list of background operations below.
- The **Background Worker**, **Engine Worker**, and **Session Recording Worker** check boxes enable the corresponding roles for that node.
- **Engine Worker** enables or disables the engine worker role, which processes responses from distributed engines.
- **Session Recording Worker** enables or disables the session recording role, which encodes session videos.
- **Maintenance Mode** enables or disables a read-only mode where the node cannot change secrets or related data.

## Scheduled Background Operations

The current scheduled background operations in SS are:

- ActiveDirectorySynchronizationMonitor
- BackgroundWorkerTaskTriggerJob
- BackupMonitor
- Bulk Operations When triggered by user
- CheckOutMonitor
- ComputerScanMonitor
- ConnectWiseMonitor
- DatabaseCleanupTriggerJob
- DiscoveryMonitor
- EventQueueMonitor
- ExpiredSecretPasswordChangeTriggerJob
- ExpiringLicenseTaskTriggerJob
- ExpiringSecretTaskTriggerJob
- HeartbeatMonitor
- Local Heartbeat Trigger Job
- Local Password Change Trigger Job
- NodeClusteringMonitor
- NodeTaskTriggerJob
- PasswordRequirementTriggerJob
- PbaDirectiveTriggerJob
- PbaMetadataUploadTriggerJob
- PrimaryNodeTaskMonitor
- Process Field Encryption Changes Task
- ProcessDashboardJsonValidationTask
- ProcessSecretPolicyChangesMessage
- ScheduledReportMonitor
- SecretComputerMatcherMonitor
- SecretItemHashMonitor
- SqlReplicationConflictMonitor
- TelemetryTriggerJob
- ThycoticOneSyncUserTriggerJob
- TruncateDatabaseCacheTriggerJob
- TruncateEngineLogTriggerJob
- VideoConversionTriggerJob

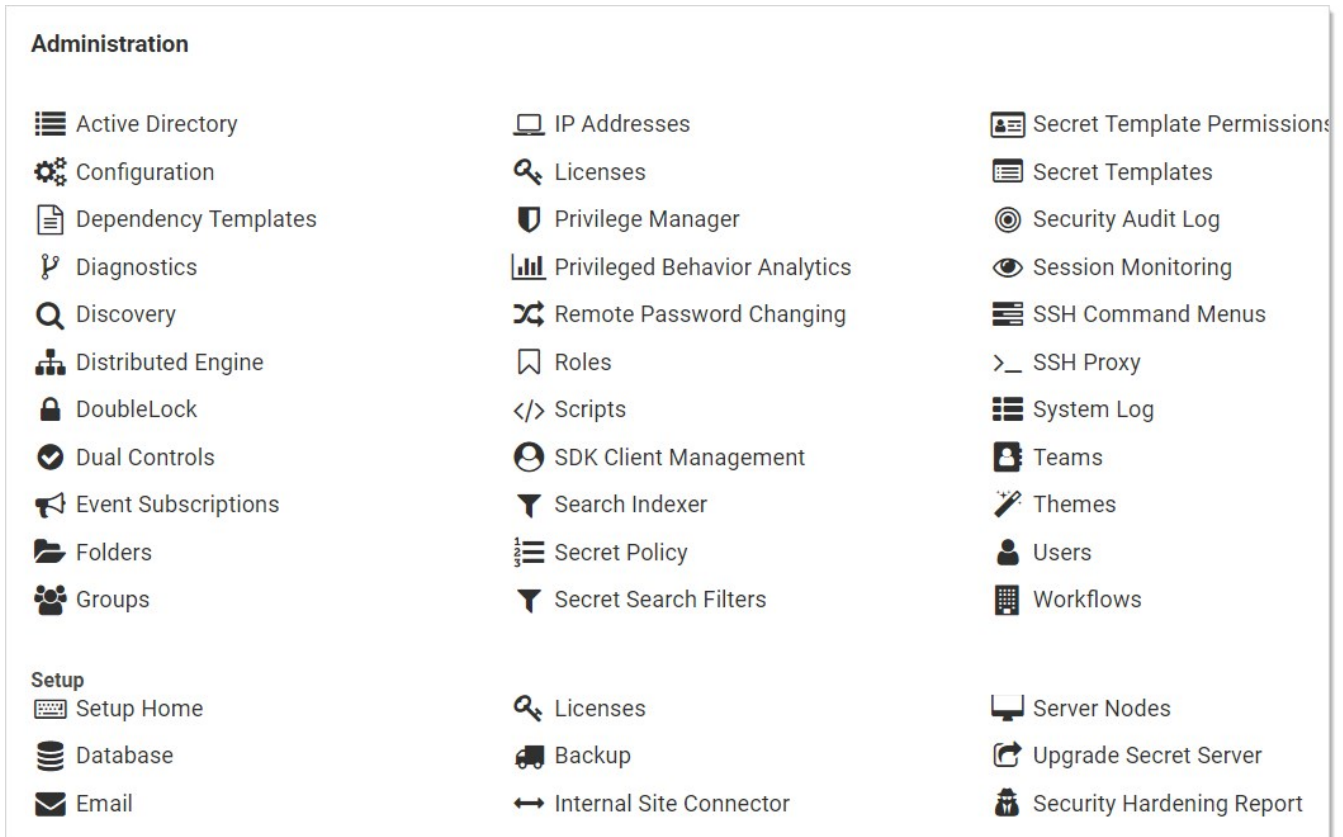
To see the current state of these jobs, such as the last time they ran and how long until they run again, go to **Admin > Diagnostics**.

## Procedures

### Markdig.Syntax.Inlines.EmphasisInline

**Note:** Clustering requires a Secret Server Premium add-on or Enterprise Plus edition license.

1. Have SS upgraded or installed and running on a server.
2. Enable clustering on the node:
  1. In SS, click **Admin** > **See All**. The Administration page appears:



2. Click the **Server Nodes** button in the **Setup** section. The Server Nodes page appears:

Server Nodes

MACHINE NAME (ID)	BINARY VERSION	DATABASE	ERROR MESSAGE	LAST CONNECTED	IN CLUSTER	BACKGROUND WORKER	ENGINE WORKER	SESSION RECORDING WORKER	MAINTENANCE MODE	
QA-CUST-01 (1) (Current Node)	10.7.000000	SS_Playground		8/13/2019 8:05:19 PM	Yes	Enabled	Enabled	Enabled	Disabled	

Enable Clustering

No

Back

Enable Clustering

SQL Server Replication

[KB Article: Server Nodes, Clustering and Worker Roles](#)

3. Click the **Enable Clustering** button.

3. Copy the entire SS application folder (typically c:\inetpub\wwwroot\SecretServer) from the existing node to the secondary node.

4. Follow the steps in the Installation Guide for setting up the application pool and virtual directory in IIS.

**Note:** If you use DPAPI encryption for your encryption.config file, you need to transfer the non-DPAPI-encrypted version of the file to the secondary node. You can turn on DPAPI encryption from that server node locally after SS is running. This setting can be found at **ADMIN > Configuration** on the **Security** tab.

5. If running SS 8.9.300000 or later, ensure that both servers are using the same date and time.

6. Once the secondary server is running, navigate to its SS using a Web browser.

7. Reset the database connection, following the instruction in [this KB article](#).

8. Activate licenses for the new node. You can do this on either server once the database connection is established on the secondary node.

9. Configure your load balancer for the two sites to have "sticky sessions" to prevent a user from bouncing between server on each request.

10. Configure the worker roles for the cluster:

- Each server node can optionally run the background worker, engine worker, and session recording worker roles.
- At least one instance of **each** type of those roles must be active in the cluster for the clustered SS application to function.
- You may run more than one instance of each role as desired to improve the performance of the clustered SS application.

**Note:** For more information on what the various roles do, please see the [Worker Roles](#) section.

## Upgrading Secret Server in a Clustered Environment

### Overview

SS has a built-in Web installer. That installer is a series of pages inside SS for downloading and updating SS. SS is accessible by users for most of the upgrade process. You can stop outside access to the site if you want to prevent users from making changes during the upgrade. Preventing user access will make restoring the database and site backups simpler if you decide to roll back the upgrade immediately afterward.

**Warning:** Before upgrading, **backup your SS folder and database**. See [Upgrading Secret Server - Single Instance and Web Clustering](#) for important steps for ensuring your data is backed up.

**Important:** Upgrading to SS version 8.9.000000+ requires Windows Server 2008 R2 or greater.

**Important:** If upgrading to SS version 8.5.000000+, there are changes in the required .NET Framework that may require additional steps in the upgrade process. For more information, see [Secret Server Moving to .NET Framework 4.5.1](#).

**Important:** Upgrading to SS 10.0.000000 and above requires configuring integrated pipeline mode on the SS application pool. Please see [Configuring IIS for Installing or Upgrading to Secret Server 10](#) for details.

**Important:** If using Integrated Windows authentication you will also need to update IIS authentication settings as detailed in [Setting Up Integrated Windows Authentication in Secret Server 10.0+](#). If you are at version 9.1.000000 and below, you will need to first upgrade to 9.1.000001 before you can upgrade to 10.0.000000+.

**Note:** You do **not** need to download the SS installer to perform an upgrade.

## Procedure

1. Before you start:
  - Ensure that you have account credentials information and access for the server hosting SS and the SQL Server instance hosting your SS database.
  - Have a recent backup of the application files and database available.
  - Stop the application pools on all of the servers except the one that you have chosen to upgrade.
2. Choose one SS server to upgrade
3. Perform a backup of that server.
4. Stop the Web servers of all other nodes.
5. Perform the upgrade using the same procedure as a single instance.

**Note:** If applicable, see [Upgrading Secret Server without Outbound Access](#).

6. Once SS is upgraded and working, copy the Web application folder (without the database.config or encryption.config files) to all other servers.

**Warning:** Never overwrite or delete the encryption.config file on a SS server.

**Note:** Both encryption.config and database.config are automatically propagated to the new servers from the original. If you need to copy those files because of database configuration changes and are using DPAPI, disable DPAPI encryption in SS by going to **Admin > Configuration** on the **Security tab**, and clicking **Decrypt Key to not use DPAPI** before copying those files to secondary servers.

**Note:** EFS encryption is tied to the user account running the SS application pool, so it is not machine-specific. Thus, it is not necessary to copy EFS encrypted files between SS instances, but it is allowed.

7. If Thycotic management server (TMS) is installed and clustered, copy the TMS directory to the secondary servers as well. The TMS directory is included by default for new installs of SS 10.2+. TMS is used by advanced session recording and Privilege Manager. If the TMS folder and site does not exist in IIS, then no additional actions are needed.
8. Start the secondary servers to confirm they still work.

## Upgrading Database Mirroring

1. If there is more than one Web server running SS, ensure all instances are pointing to their primary database.
2. Select one server to perform the upgrade on, stop all other web servers.
3. Perform the upgrade on the single instance.
4. Once upgraded and working, copy the Web application folder to all other Web servers.
5. Start all other Web servers and confirm they work
6. Ensure all instances are properly activated
7. Ensure that the primary database changes have been replicated to the mirror database.
8. If one of the servers was pointing originally to the secondary database, adjust it to point there again.

## Upgrading Disaster Recovery Installations

1. Perform the upgrade on the production instance.
2. Backup the production instance.
3. Copy the database backup to the remote DR instance and restore the database.
4. Once the database is upgraded and working, copy the web application folder (but not the database.config or encryption.config files) to the remote DR instance, overwriting the existing files.
5. Restart IIS or recycle the application pool running SS on the remote DR instance.
6. Confirm that the remote DR instance is working correctly.

## Load Balancing Secret Server Clusters

In a clustered Secret Server environment set up behind a load balancer, the accessible outside URL may be something other than the server name.

### Custom URL Configuration

In SS 8.5 and later, the Custom URL setting can be configured to ensure that links and resources are resolved correctly and are not based upon the server name:

1. Navigate to **Admin > Configuration**.
2. On the **General** tab, click the **Edit** button.
3. Go to the **Application Settings** section.
4. Click to select the **Custom URL** check box.
5. Type the desired URL in the **Secret Server Custom URL** text box.

### SSL Recommendations

For the best security, we recommend placing the SSL certificate on each of the Web servers. This ensures the traffic leaving the server is encrypted by SSL. Optionally, the load balancer would need the certificates as well for adding the client's IP address.

If the connection between the load balancer and the server is isolated in a security zone, you could leave HTTP between the load balancer

and the server and have the SSL on the load balancer.

## Configuring Client's IP Address (X-Forwarded-For)

Routing traffic through a load balancer will cause SS to audit the IP address of the load balancer instead of the end user. To avoid this:

First, configure the load balancer to pass along the client's IP address in the header.

Then add the appSettings key IpAddressHeader with the value of the name of the header field containing the client's IP address. This setting must be added to **all** SS Web servers. Depending on your SS version, do this in one of two ways:

For SS prior to 10.5.000000:

In the web-appSetting.config file in your SS directory, add the following key:

```
<?xml version="1.0" encoding="utf-8" ?>
<appSettings>
  <add key="IpAddressHeader" value="X-Forwarded-For" />
</appSettings>
```

For SS 10.5.000000 and later:

1. Go to <https://<SecretServerAddress>/ConfigurationAdvanced.aspx>.
2. Scroll to the bottom and click **Edit**.
3. Locate the **IP Address Header** text box, type X-Forwarded-For.
4. Click the **Save** button.

**Note:** The SSL certificate needs to exist on the load balancer and the Web server to ensure it has access to add the client IP address header.

## Clustering Errors

The following errors may arise when setting up or operating SS clustering:

- Encryption configurations do not match: See the [Encryption Key Does Not Match Error](#) knowledge base article.
- Server dates do not match: If the Web server dates do not match, the audit records could be bad. The fix is to set the servers to the same time.

**Note:** This only applies to SS before version 8.9.300000.

- SS version does not match: If some of the cluster nodes have been upgraded and others have not, their versions will conflict, producing this error. Nodes which have the wrong (older) version will not function correctly. To fix this issue, ensure that all the nodes in your cluster are upgraded. For nodes that are having this issue, you can copy the application folder (minus the database.config file) to replace the server files with the correct version.

HTTP/2 is supported in IIS 10. HTTP/2 is handled within IIS, so this is primarily a Microsoft question in regards to compatibility. Please see [HTTP/2 on IIS](#). At the end of this article, it clarifies when HTTP/2 is not supported

Secret Server does support Windows Integrated Authentication where a user's windows session is passed through for authentication to SS. That is, there is no log on page for SS. The majority of our customers are (and the default configuration for SS is) using forms-based authentication with a log on page. Only the latter is HTTP/2 compliant.

HTTP/2 is only compatible with HTTPS protocol. SS can also be configured to operate only on HTTPS (Admin > Configuration > Security > Force HTTPS/SSL), which we strongly recommend.

The Secret Server proxy routes SSH and RDP sessions and helps protect the endpoint credentials. There are two configuration options for proxying:

- Proxy through the SS Web application
- Proxy through a distributed engine

**Note:** To learn more about RDP Proxying, please see [RDP Proxy Configuration](#).

## Enabling Proxy

1. Go to **Admin > SSH Proxy**.
2. Enable **SSH Proxying**.
3. Generate a new key.
4. To enable proxying on Web nodes, edit the row in the **Endpoints** tab to set the **Public Host** and **Bind IP Address**. For a standard server, these can be the same, but if the public IP of the server is not set on the server (such as a load balancer or an EC2 instance with an elastic IP), they will be different.
5. To enable proxying for a specific site and all engines within that site, edit the row in the **Sites** section and enable proxying and set the **SSH Port**.
6. The engines for the sites are listed in the **Engines** section. The **Hostname/IP Address** is the public host or IP the launcher connects to and the **SSH Bind Address** is the IP on the server that the SSH proxy is listen on. Again, these will typically be the same, but may be different if the resolvable IP or host of the engine machine is different than the IP on the network adapter on the machine.
7. Enable proxying on a secret with a PuTTY launcher. The launcher now connects to the assigned site, which is set on the **General** tab. If the site has proxying enabled, it will go through the engines available in the site, otherwise it will use the SS Web application proxy.

## Web Application Proxy Performance

### Minimum Hardware

- Intel 3.7 GHz Quad Core
- 16 GB of RAM
- 100 MB/s plus network capability

### Session Activity

We tested sessions with standard usage, such as opening and modifying files and navigating the file system on Linux. On Windows, the activity was opening MMC snap-ins, editing files, and copying files through the RDP session. If you have constant large file transfers across multiple concurrent sessions or otherwise transferring large amounts of data (such as streaming a video through an RDP session), the maximum concurrent sessions will be significantly reduced.

**Table:** Concurrent Proxy Sessions

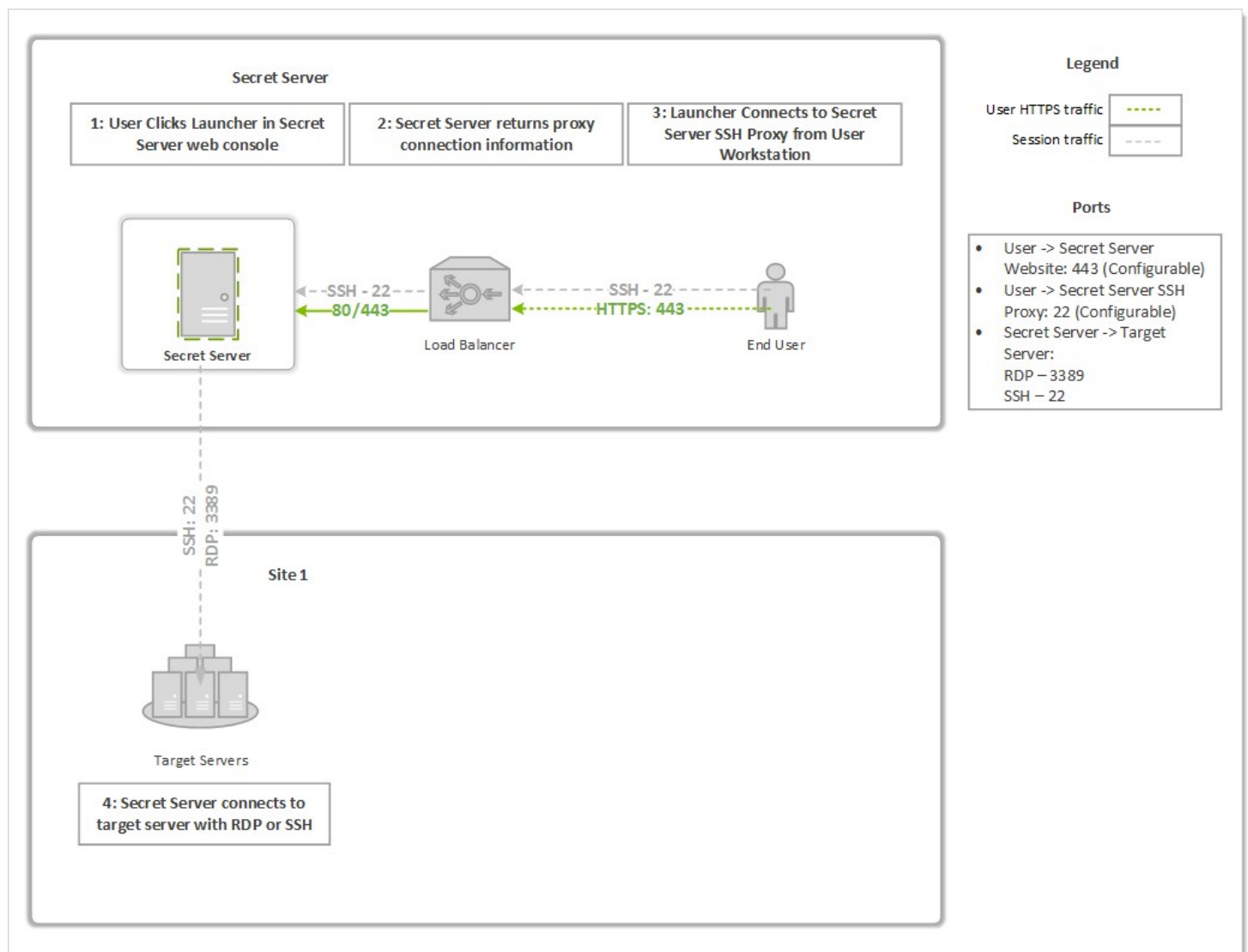
SSH	300
RDP	100

## Proxy Connections

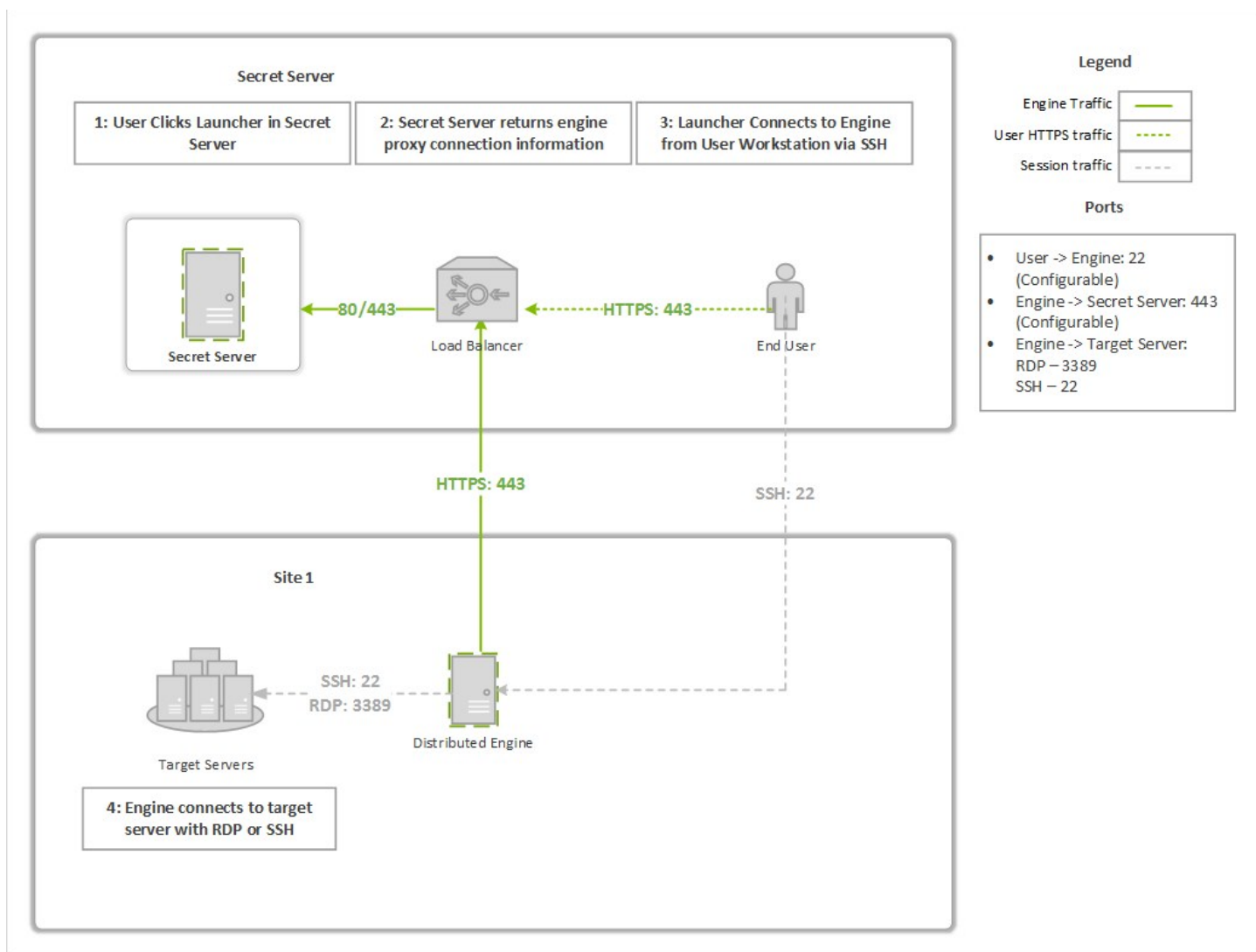
Connections from the user to the proxy are over SSH, and you can configure the port. The user's machine will connect to either an engine

SSH proxy or the SS Web application SSH proxy.

**Figure:** Default Secret Server Web Application Proxy (example)



**Figure:** Proxy through a Distributed Engine (example)



## SSH Proxy with Multiple Nodes

If you are using clustering with SS, you can pick exactly which of your nodes act as a SSH proxy by going to the **Admin > SSH Proxy** page and scrolling down to the **Nodes** section. For each node you wish to be a proxy, configure the **SSH Public Host** (must be an IP address, not a DNS name) and the **SSH Bind IP Address** (use 0.0.0.0 to easily bind to all IPv4 Ps on a server). There is no need to configure all nodes if you do not want them all to be proxies.

As soon as the IPs are saved for each node, the node should start listening on the SSH proxy port. You can verify that with netstat. If you do not see the node listening on your chosen port, perform an IIS reset and hit its SS website. It should be listening once SS starts up again. For example:

```
C:\Users\Administrator>netstat -ano | find ":22"
TCP 0.0.0.0:22 0.0.0.0:0 LISTENING 3600
```

Now, when a user connects to the SS Web page, if the node they are hitting is setup to be a SSH proxy, they will connect to that node's SSH public host IP. If the node they are connected to is not setup to be a SSH proxy, then users will round robin between the other nodes that are SSH proxies and connect to their SSH public host IP.

## Overview

This article lists ports typically used in Secret Server. Please note the following:

- The RPC Dynamic Port ranges are a range of ports utilized by Microsoft's Remote Procedure Call (RPC) functionality. This port range varies by operating system. For Windows Server 2008 or greater, this port range is 49152 to 65535 and this entire port range must be open for RPC technology to work. The RPC range is needed to perform Remote Password Changing since Secret Server will need to connect to the computer using DCOM protocol.
- The range can vary separately for Exchange servers. For more information about changing the RPC port range, see the related Microsoft's Knowledge Base article on how to configure RPC dynamic port allocation to work with firewalls.
- To see your ipv4 dynamic range on a given machine, type `netsh int ipv4 show dynamicport tcp` in the command line.
- To specify a specific port on your environment that Secret Server will communicate to, see the related article on enabling WMI ports on Windows client machines

## Port Listing

**Table:** Active Directory Sync Ports

LDAPS	TCP/636, UDP/636
LDAP	TCP/389, UDP/389
Kerberos	TCP/88, UDP/88
SMB/Microsoft-DS	TCP/445, UDP/445

**Table:** Discovery Ports

RPC Dynamic Port Range	TCP/49152-65535, UDP/49152-65535
SMB/Microsoft-DS	TCP/445, UDP/445
RPC Endpoint Mapper	TCP/135
SSH	TCP/22

**Table:** Remote Password Changing Ports

RPC Dynamic Port Range	TCP/49152-65535, UDP/49152-65535
SSH	TCP/22

Telnet	TCP/23
Microsoft SQL	TCP/1433, UDP/1434
SMB/Microsoft-DS	TCP/445, UDP/445
LDAP	TCP/389, UDP/389
LDAPS	TCP/636, UDP/636
Sybase	TCP/2638, TCP/5000
Oracle Listener	TCP/1521
Kerberos Password Change	TCP/464, UDP/464
Windows Privileged Account (WinNT ADSI Service Provider)	TCP/139

**Table:** Web Server Incoming Ports

HTTP	TCP/80
HTTPS	TCP/443

**Table:** Database Server Incoming Ports

SQL Connection	TCP/1433, UDP/1434

**Table:** Email Ports

SMTP	TCP/25

**Table:** RADIUS Server Ports

RADIUS Authentication	TCP/1812

**Table:** Syslog Ports

--	--

Syslog	TCP/514, UDP/514
--------	------------------

**Table:** Internal Site Connector Ports

RabbitMQ	TCP/5672 (non-SSL), TCP/5671 (SSL)
MemoryMQ	TCP/8672 (non-SSL), TCP/8671 (SSL)

**Table:** RabbitMQ Clustering Ports

EPMD	TCP/4369
Inter-node Communication	TCP/25672
Inter-node Communication	TCP/44002

## Related Articles and Resources

- [Enabling WMI port on Windows client machines](#) (KBA)
- [How to configure RPC dynamic port allocation to work with firewalls](#) (KBA)

## Remote Password Changing

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

*Remote Password Changing* (RPC) allows secrets to automatically update a corresponding remote account. Secrets can be set for automatic expiration, followed by automatic new password generation. SS automatically generates a new strong password and changes the remote password to keep all accounts synchronized with SS.

RPC allows SS to rotate passwords to meet domain password policy requirements. In most cases, RPC is configured with the secret "auto change" setting set to true. This causes the secret to rotate the password as soon as it expires. The "auto change schedule" setting changes the password on a set schedule, rather than when it expires. This provides the ability to change passwords when network activity is lower. You have a choice of changing the password as soon as the schedule interval arrives or only after the secret expires *and* the interval arrives. It is important to choose a large enough interval to complete all your password changes, otherwise any excess changes will have to wait for the next interval. Because the smallest interval is one day, this is only relevant if you have thousands of changes. If SS fails to change a remote password, an alert states there are secrets out of sync.

You can pair secrets with SS checkout, which is Thycotic's one-time password functionality (not the same as [TOTP](#)). This allows you to rotate the password on a particular expiration schedule and limit the password to a single user for a set time period, after which it is changed. This is for situations where you need the password to change after every use, such as vendors who need temporary access to a server or system. For additional security on sensitive systems, approval workflow or session recording can be paired with checkout to add layers of authentication to gain access to the secret and track how that secret is used.

Regardless of the timing of password change, you may want to rotate dependent resources (dependencies) right after you rotate the password on a secret. For example, a Windows domain account could be a service account that starts many windows services. In the event that you rotate that password, you would need to also rotate the password for this account on the services which start using that account. If you do not, starting those services will fail the next time they are restarted, which could cause other components to fail too. You can create dependencies on a secret for scheduled tasks, application pools, or services (with or without using PowerShell to undertake tasks at rotation time).

We have a large number of out-of-the-box RPC changers, which are expandable by writing your own SSH, SQL or PowerShell scripts to do RPC, which can get information from the secret. See [Configuring Secret Dependencies for RPC](#) and the [Password Changer List](#).

**Note:** You can configure [event pipelines](#) and [notifications](#) to track whether an RPC has failed. Heartbeats allow you to check whether a password is incorrect and the machine is online.

The Remote Password Changing tab contains the settings for configuring RPC on an individual secret. Enabling RPC *auto change* on a secret allows SS to remotely change the password when it expires. The user must have owner permission on the secret to enable auto change.

**Note:** If the password change fails, SS flags the secret as out of sync and continue to retry until it is successful. If the secret cannot be corrected or brought In sync, manually disabling auto change stops the secret from being retried.

## Auto Change Schedule

The Auto Change Schedule button is visible on the secret View RPC tab when RPC and autochange is enabled on a secret.

☒
**Auto Change**  
 Secret Server will automatically initiate a password change after a Secret expires or on a schedule.

**Next Password**

Randomly generated

**Auto Change Schedule**

When password expires (Expires every 30 day(s))

Cancel

Save

The Auto Change Schedule section, which appears when you set the Auto Change Schedule list box to other than “When password expires,” allows you to specify an interval (daily, weekly, or monthly), start date, start time, and time frame (interval count) for when the password can be changed:

☒
**Auto Change**  
 Secret Server will automatically initiate a password change after a Secret expires or on a schedule.

**Next Password**

Randomly generated

**Auto Change Schedule**

Daily

Change every
 
 days

Starting on \*

☐ Only change password if the Secret is expired

Cancel

Save

This setting is useful for having the RPC occur during off-hours in order to prevent disruptions. By default, this setting is “When password

expires," which allows the secret to be changed immediately upon expiration.

**Note:** There is a check box in the auto change schedule settings labeled "Only change password if the secret is expired." When it is enabled, auto change will not change the password until after the secret expires. The auto change occurs on the first scheduled time after the secret expires. If the box is unchecked, auto change occurs on the defined schedule, whether or not the secret has expired.

**Note:** While the password change is waiting for this next scheduled time, the RPC Log (visible by navigating to **Configuration > Remote Password Changing**) reports the secret could not be changed because of a time schedule. The secret also remains expired until this auto change schedule is reached, even if the secret was forced to expire.

## Understanding Expiration, Auto Change and Auto Change Schedules

### Definition

What is the difference between expiration, auto change and auto change schedules?

- **Expiration:** sets whether or not a secret in SS is marked as expired and the period SS counts down before marking the secret as expired.
- **Auto Change:** sets SS to automatically initiate a password change after a secret expires.
- **Auto Change Schedule:** sets the day and time to initiate the password change after the secret has expired. This cannot be configured without also enabling Auto Change.

### Examples

Some examples to illustrate this:

#### Scenario One: Expiration with Auto Change and No Auto Change Schedule

- A Secret has an expiration period of 30 days, and auto change is enabled. No auto change Schedule has been set.
- At the end of the 30-day expiration period, the secret will expire.
- Immediately after the secret expires, it will be queued for a password change.
- Once the password has been changed, the secret is no longer marked as expired and expiration is reset to count down again from 30 days.

#### Scenario Two: Expiration with Weekly Auto Change

- A secret has an expiration period of 30 days, auto change is enabled, and an auto change schedule is configured for Weekly, recurring once a week on Tuesday, changing at 0300.
- At the end of the 30-day expiration period, the secret will expire.
- Immediately after the secret expires, SS will comply with the auto change schedule to determine when a password change occurs.
- The secret is queued for a password change as soon as it becomes 0300 on a Tuesday.
- Once the password is changed, the secret is no longer marked as expired. Expiration is reset to count down again from 30 days.

#### Scenario Three: Expiration with No Auto Change

- A Secret has an expiration period of 30 days, and auto change is not enabled.
- At the end of the 30-day expiration period, the secret expires.
- The secret remains expired until the field it applies to (usually the password field) is updated on the secret. This happens by manually updating the field or by using the "Change Password Remotely" button on the Remote Password Changing tab of the secret.
- Once the password is changed, the secret is no longer be marked expired, and expiration is reset to count down again from 30 days.

### Important Considerations and Best Practices

- If you want to rely strictly on expiration for password changing, enable auto change but set the schedule to none. Leave "Only change password when Secret is expired" checked.
- If you want to set an auto change schedule to run daily at a specific time, the change will only happen at maximum once per day at that given time. If a change happens already within that same day for the same secret, you cannot adjust the auto change schedule to run later within the same day and then have a password change occur again within that same 24-hour period. For example, if the password

was already changed earlier in the day. The schedule is then adjusted to run a few minutes later within the same day. In that case, another password change will not occur until 24 hours has passed since the last change.

- If you set the auto-change schedule to run once per week, for example, on a Thursday, and “Only change password when secret is expired” is checked. Even if the secret expires on a Monday, a password change would not occur until the secret has expired and the scheduled time on Thursday has passed.
- If you set the auto change schedule to run once per week on a Thursday and “only change password when Secret is expired” is not checked, the password would be changed every Thursday, regardless of the secret’s expiration status.
- If a secret has an expiration period but auto change is not enabled, no password change occurs automatically. The expiration would only update when the password is manually updated or a remote password change is manually triggered through SS.
- If you want to change a password more frequently than once per day, we recommend using some of the advanced security features at the secret level or controlling the change through a secret policy. Use the check out feature combined with “Change Password on Check In” on the Security tab of a Secret. You can specify a custom interval to check out the secret. After the password check out interval expires or a user manually checks in the secret, the password is automatically changed.

**Important:** For the configuration above, ensure that these accounts have a password-related group policy in Active Directory that specifies that the “Minimum Password Age” is set to 0. We recommend creating fine-grained password policies to achieve this. Add all the accounts that need rotation more frequently than once per day to an AD security group assigned to the fine-grained password policy. See [Step-by-Step: Enabling and Using Fine-Grained Password Policies in AD](#) for more information.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.












*Secret dependencies* are items that rely on the username, password, or SSH private key stored in the secret. By adding them to the Dependencies tab, they are automatically updated when the secret's password is changed, ensuring they are up to date with the account on which they depend.

## Secret Dependency Templates Designer

[Explain](#)


+ Create New Dependency Template

Filter by Dependency Type All

Dependency Template Name	Dependency Type	Active	Options
Application Pool	 Application Pool	Yes	
Application Pool Recycle	 Application Pool Recycle	Yes	
COM+ Application	 COM+ Application	Yes	
Remote File	 Remote File (Regex Replace)	Yes	
Scheduled Task	 Scheduled Task	Yes	
Windows Service	 Windows Service	Yes	
SSH Key Rotation	 SSH Script	Yes	
SSH Key Rotation Privileged	 SSH Script	Yes	
ind	 PowerShell Script	Yes	 

☐ Show Inactive

← Back

 Configure Dependency Changers

Adding a custom dependency template may require additional settings (these settings are described in the following section):

## Creating Custom Dependencies

If there are different dependency types that you want to manage that are not supported out of the box, new ones can be created based on a script. A custom dependency consists of two components:

- **Dependency Template:** The dependency template defines how a dependency is matched to discovered accounts and how it updates the target after a password change occurs on the account. to create a new dependency template, go to **Admin > Secret Templates** and click the **Dependency Templates** button.
- **Dependency Changer:** A dependency changer is a script and the associated parameters to be passed into the script. Dependency changers can be created and modified by going to **Admin > Remote Password Changing > Configure Dependency Changers**.

**Note:** Please see the [Secret Server Discovery Guide](#) for a comprehensive guide to configuring and using dependency changers and dependency templates.

## Dependency Groups

By default, all dependencies are updated in the order listed. There are cases where you may want to split out different sets of dependencies into separate groups. Typically, this is because a single service account may run services across different segregated networks that can communicate with the domain but not each other and have different distributed engine sites assigned. In this case you can create two dependency groups and assign them to different distributed engine sites to solve connectivity issues.

## Dependency Settings and Information

Dependencies have the following settings:

**Note:** Not all dependency types have all these settings.




- **Change Fail Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that determines if SS was unable to update the public key on the dependency.
- **Change Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that updates the public key on the dependency.
- **Change Success Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that determines if SS was able to update the public key on the dependency.
- **Database:** For SQL script dependency types, the database name for the script.
- **Dependency Group:** Name of the group to run the dependency update in.
- **Description:** Description of the dependency for documentation purposes.
- **Enabled:** Whether SS attempts to update the dependency. A disabled dependency is ignored by SS.
- **File Path:** For Remote File Dependency types, this is the UNC file path on the remote server where the embedded password exists.
- **Machine Name:** Computer name or IP address on which the dependency is located.
- **Name:** Name of the dependency on the remote machine.
- **Port:** For SQL and SSH script dependency types, the port name for the script.
- **Privileged Account:** The account SS authenticates as when changing the dependency's credentials, so it must have privileges on the remote machine to edit the dependency.
- **Public Key:** For SSH key rotation and SSH key rotation privileged dependency types, this text-entry field holds the value of the public key stored on the dependency.
- **Regex:** For Remote File Dependency types, the regular expression used to locate the password embedded in the configuration file.
- **Restart:** Determines if the dependency is restarted once the account has been updated.
- **Run Condition:** Allows the dependency to run conditionally depending on the outcome of the dependencies above it.
- **Script:** Name of the PowerShell script, SSH script, or SQL script in the scripts repository configured on the Dependency Template. The actual script selected can be previewed by clicking the eye icon.
- **Server Key Digest:** For SSH key rotation and SSH key rotation privileged dependency types, a text-entry field that serves as a security control for specifying the SHA1 hash of the SSH host key on the remote server.
- **Server Name:** For SQL script dependency types, the server name for the script.
- **SSH Key Secret:** An account with SSH Key that SS uses to authenticate when executing the SSH Script or SSH Key rotation dependency types.
- **Template:** Whether the dependency is an IIS application pool, Scheduled Task, windows service, remote file, COM+ application. Custom dependencies can also be created using a SQL, SSH, or PowerShell script.
- **Verification Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that verifies

that the new public key on the dependency matches the private key on the secret.

- **Wait(s):** Time in seconds that SS pauses before changing the dependency.

Example values for a Windows service dependency on a remote computer might be: 192.11.158.99, Windows Service, aspnet\_state, OR DOMAIN\admin.

The following operations can be performed in the Dependency grid:

- **Delete:** Click the  icon to delete the dependency.
- **Edit:** Click the  icon to edit dependency text boxes. Cancel changes by pressing the Cancel button.
- **Run Dependency:** Click the second arrow icon to run the script on the selected dependency and set the password on the selected dependency to the current password for the secret
- **Test Connection:** Click the return arrow icon to test the dependency connection, the tests results are displayed afterward.
- **View Dependency History:** Click the  icon to view the activity logs for the dependency.

**Note:** Due to security constraints, scheduled tasks require an Active Directory domain user as the privileged account.

## Manually Adding Dependencies

To manually add a dependency:

1. Click on the plus icon next to **Create New Dependency** on the **Dependencies** tab.
2. Choose your dependency type from the **Template** list.
3. Fill in the dependency name, machine name, and other information depending on the dependency type.
4. To choose the account used to change the dependency password, click on the link next to the **Privileged Account** label. If the privileged account is blank, the current secret's credentials are used.
5. Click the **OK** button to finish adding the dependency.

## Using Regex with Dependencies

### Overview

In release version 7.8.00010 and later, SS allows a secret to have file dependencies. File dependencies allow text files with embedded credentials to be changed via Regex.

A Regular Expression (Regex) is a phrase in a language for matching text. For details on the .NET Regex language, see [.NET Framework Regular Expressions](#).

Secret Server replaces the contents of the first group (within parentheses) within the Regex.

Setting up a remote file dependency, requires:

- **File Path:** This is the file path on the remote server where the remote password exists. UNC paths do not work here. See [UNC Names](#).
- **Regex:** This regular expression to be used to locate the password embedded in the configuration file.
- **Machine Name:** Computer name or IP address where the dependency is located.
- **Privileged Account:** The account SS will authenticate as when changing the dependency. It must have privileges on the remote machine.

A typical filled in New Dependency page looks something like this:

Dependency Type	Remote File
Dependency Group	Default
File Path	C:\testFolder\testfile.config
Regex	Password=([^\;]+)
Machine Name	Hostname01.testdomain.local
Description	
Wait (s)	0
Enabled	<input checked="" type="checkbox"/>
Privileged Account	testdomain\myadaccount <a href="#">clear</a>

### UNC Names

UNC names, such as:

\\BARAKA\SHARE\test.txt Or

\\192.168.1.154\SHARE\test.txt

do **not** work in the file path. You can, however, put the machine name or IP address in the Machine Name text box, and put the rest of the path in the file path. For example:

In the **File Path** text box:

\SHARE\test.txt Or

SHARE\test.txt

In the **Machine Name** text box:

192.168.1.154 Or

BARAKA

## Examples

The following are some examples of using Regex within file dependencies:

### XML Configuration Files

#### Example One

##### Source

```
<Configuration>
  <User>
    <UserName>Bob</UserName>
    <Password>Password1</Password>
  </User>
  <User>
    <UserName>Sam</UserName>
    <Password>DontChangeThisOne</Password>
  </User>
</Configuration>
```

##### Regex

```
<UserName>Bob</UserName>\s*<Password>([^\<]+)</Password>
```

#### Example Two

##### Source

```
<Configuration>
  <User name="Bob" password="Password1" />
  <User name="John" password="Password1" />
</Configuration>
```

##### Regex

```
<User name="Bob" password="([^\"]+)" />
```

### Windows Initialization (.ini) Files

##### Source

```
[owner]
name=John Doe
password=Password1
organization=Acme Widgets Inc.
```

##### Regex

```
name=John\sDoe\s*password=([^\r\n]+)
```

### SQL Server Connection Strings

##### Source

```
Data Source=myServerAddress;Initial
Catalog=myDataBase;UserId=myUsername;Password=myPassword;Server=myServerAddress;Database=myDataBase;Trusted_Connection=False;
```

##### Regex

Password=([^\;]+)

## Oracle Connection Strings

### Example One

#### Source

```
Data Source=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=MyHost)(PORT=MyPort)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=MyOracleSID)));
```

```
User Id=myUsername;Password=myPassword;
```

#### Regex

Password=([^\;]+)

### Example Two

#### Source

```
Data Source=username/password@//myserver:1521/[my.service.com](http://my.service.com);
```

#### Regex

username/([^\@/]+)

## YAML

#### Source

```
receipt: Oz-Ware Purchase Invoice
```

```
date: 2007-08-06
```

```
user:
```

```
name: Dorothy
```

```
password: Password1
```

#### Regex

```
name:\s*Dorothy\s*password:\s*([^\v\n]+)
```

The Password Changers Configuration page can be accessed by navigating to **Admin > Remote Password Changing > Configure Password Changers**.

There are a few password changing types that allow the user to enter in specific commands that are sent to the computer where the password is changing. This enables the system to accommodate for differences in the standard password change procedure. For example: The Unix system that is being changed prompts for the current password twice instead of only once before asking for the new password.

## Changing Ports and Line Endings

To change the port or line ending used on a password changer, click the password changer on the **Configure Password Changers** page and then click **Edit**. There, you can choose the line ending and port used by the device. By default, line endings are set to New Line (\n), however some devices and applications (such as HP iLO) use a different line ending system. The port defaults to 22 for SSH connections and 23 for Telnet connections.

For the built in Windows password changer there is a ports text-entry field available that can be filled in to help ensure a computer is listening. This can be used if DNS returns multiple IP addresses for a single box and only one is valid. For example, a laptop might get two IP addresses for an Ethernet and wireless connection, but if it is unplugged the Ethernet IP is invalid. In this case, SS can do a reverse lookup and test each IP until it is able to connect on one of the specified ports. When it gets a response, it uses that IP for the password change.

## Creating a Custom Password Changer

1. From the **Password Changers Configuration** page, click **New**.
2. Select a base password changer. We recommend you select the option that most closely matches the type of password changer you are creating, as this determines which customizable parameters and test actions are available to you.
3. On the next page, make any customizations you would like. To save a new command, click the **+** icon at the end of the row. The command can be edited once more by clicking the edit button, which is labeled with a small pencil icon at the end of the row.
4. To access the test actions for your new password changer, click **Back** to return to the overview screen.
5. To edit additional parameters (if applicable), click **Edit** from the password changer overview to change settings such as the name, line ending, and custom port.

**Note:** For more information about creating a custom PowerShell password changer, see [PowerShell Remote Password Changing \(KB\)](#).

## Deactivating Password Changers

To make a password changer unavailable for use and to hide it from view in your list of password changers, you must mark it inactive:

1. From the **Password Changers Configuration** page, click the password type name of the password changer you would like to make inactive.
2. Click **Edit**.
3. Uncheck the **Active** box.
4. Click **Save**.

To view inactive password changers, check the **Show Inactive** box at the bottom of the list of password changers. The Active column in the table indicates the status of the password changer.

## Distributed Engines and RPC

Distributed Engines allow RPC, heartbeat and discovery to occur on networks that are not directly connected to the network that SS is installed on. See the linked KB and its associated white paper for details on configuration and functionality.

**Note:** Distributed Engines were released in version 8.9.000000 and replaced remote agents.

## Editing Custom Commands

The SSH type changers use the SSH protocol to access the machine. This type contains custom commands for password reset and can contain commands for the verify password functionality but most SSH type changers simply verify that a connection can be established with the username and password. The Telnet type changers use the Telnet protocol in order to access the machine and contain custom commands for both the password reset and the verify password functionality. The verify functionality is used in the heartbeat, as well as verifying that the password was changed successfully.

SSH key rotation type changers also include post-reset success and failure custom commands. These extra command sets are run after both the reset and verify functions are run and are used to either finalize the key rotation and password change (success) or clean up after a failure. If both the reset and verify functions are successful, the post-reset success command set is run. If either the reset or the verify fail, the post-reset failure command set is run.

To edit the custom commands, click on the **Edit** Commands button. This sets the command grids into Edit mode where you can add, update, or delete the commands in order to suit their purpose.

Any secret text-entry field value can be substituted by prefacing the text-entry field name with a \$. For example, to echo the notes value for a secret, the user would enter: `echo $Notes` as a command. Along with these secret field values, the following variables are available in custom commands:

### RPC-Mapped Text-Entry Fields

- `$USERNAME` The username text-entry field mapped in RPC on the secret template.
- `$CURRENTPASSWORD` The password text-entry field mapped in RPC on the secret template.
- `$NEWPASSWORD` The next password (filled in Next Password textbox or auto-generated).
- `PRIVATEKEY` The private key text-entry field mapped in RPC on the secret template.
- `$NEWPRIVATEKEY` The next private key (filled in Next Private Key text box or auto-generated).
- `$CURRENTPUBLICKEY` The public key text-entry field mapped in RPC on the secret template.
- `$NEWPUBLICKEY` The next public key (generated from the next private key).
- `$PASSPHRASE` The passphrase text-entry field mapped in RPC on the secret template.
- `$NEWPASSPHRASE` The next passphrase (filled in Next Private Key Passphrase text box or auto-generated).

### Associated Reset Secrets

- `[$1]` Adding this prefix to any text-entry field targets the associated reset secret with order 1.
- `[$1]$USERNAME` The mapped username of the associated secret, identified by order. Can also reference any other property on the associated secret. Common examples include:
  - `[$1]$PASSWORD`
  - `[$1]$CURRENTPASSWORD`
  - `[$1]$PRIVATE KEY`
  - `[$1]$PRIVATE KEY PASSPHRASE`
- `[$SID:105]` Adding this prefix to any text-entry field targets the associated reset secret with a secret Id of 105.

- `$$[SID:105]$USERNAME` The mapped username of the associated secret, identified by secret id. Like referencing an associated secret by order, referencing by secret id can also access any text-entry field on the secret by name.

**Note:** Both the mapped text-entry fields and secret text-entry field names can be used.

## Check-Result Commands

- `$$CHECKCONTAINS <text>` Checks that the response from last command contains <text>.
- `$$CHECKFOR <text>` Checks that the response from the last command equals <text>.
- `$$CHECKNOTCONTAINS <text>` Checks that the response from last command does not contain <text>.

**Note:** If these conditions are not met the process fails and immediately returns a result.

If you want to exit out of the command set early without triggering a failure, echo an "OK" on the line immediately preceding the `exit 0`; statement. "OK" must be the only text in the response from the server for this to work.

You can test out your password reset and verify password command sets by clicking on the **Test Action** buttons next to the relevant sections. All communication between SS and the target machine is displayed when using these test buttons.

## Enabling RPC

RPC is enabled under the Administration, Remote Password Changing page. Click **Edit** to enable RPC, secret heartbeat, and secret checkout. Once enabled, all secret templates with RPC configured are available to use with RPC.

## Mapping Account Fields for RPC

All the secret templates with the prefix RPC have RPC configured by default. For creating a custom template that uses RPC it can be configured from the Secret Template Designer. **Enable Remote Password Changing** must be turned on for secrets created from the template to make use of this feature. Select the password type for the account and map the text-entry fields to be used for authenticating to the remote server. The secret fields must be mapped to the corresponding required text-entry fields based on the password change type. Do that in the **Secret Template Edit Password Changing** page for the secret template:

**Secret Template Edit Password Changing**

Enable Remote Password Changing

Yes

Retry Interval

1 hour

Maximum Attempts

10000

Enable Heartbeat

Yes

Heartbeat Check Interval

8 hours

**Password Type to use** Active Directory Account

PASSWORD TYPE	SECRET FIELD	SCRIPT VARIABLE
Domain	Domain	\$domain
Password	Password	\$password
User Name	Username	\$username
Domain Controller (DC)		\$domaincontroller
<b>Default Privileged Account</b>		< None >

Back

Edit

The **Retry Interval** text box is the amount of time that a secret waits before once again attempting to change a password after a password change is unable to succeed.

The **Default Privileged Account** text box is the secret that is set as the privileged account for all new secrets that are created with this secret template. Changing this does not affect any existing secrets.

## Mapping an SSH Key or Private Key Passphrase for Authentication

Some password changers may be customized to use SSH key authentication. SS needs to know which text-entry fields contain the key and the passphrase. These text-entry fields can be specified after clicking **Edit** from the password changer page.

### Unix Account Custom (SSH)

Verify Password Changed Commands

Test Action

AUTHENTICATE AS

Username

SUSERNAME

Password

\$CURRENTPASSWORD

Key

< None >

Passphrase

< None >

ORDER	COMMAND	COMMENT	PAUSE(MS)
Password Change Commands			
Test Action			
AUTHENTICATE AS			
<div>Username</div> <div>SUSERNAME</div>			
<div>Password</div> <div>\$CURRENTPASSWORD</div>			
<div>Key</div> <div>&lt; None &gt;</div>			
<div>Passphrase</div> <div>&lt; None &gt;</div>			
ORDER	COMMAND	COMMENT	PAUSE(MS)
1	passwd	Password Command	2000
2	\$CURRENTPASSWORD	Current Password	2000
3	\$NEWPASSWORD	New Password	2000
4	\$NEWPASSWORD	Confirmed Password	2000

[Advanced Post Change Commands](#)
[Advanced Settings](#)

Back

Edit

Edit Commands

Configure Scan Template

View Audit

The key and passphrase must be identified by a \$ sign and the secret text-entry field name, which can be obtained from the secret template.

To set which text-entry fields are your key and passphrase, go to the extended mappings for a secret template by clicking **Extended Mappings** from the **Secret Template Edit** page. Select the text-entry fields that correspond to the SSH private key and passphrase if applicable. No matter what you name your key text-entry field, SS knows what it is. This is set up by default, so you should not need to do this unless you've created custom Unix templates you want to use keys with.

Once SS knows which text-entry fields contain the private key and private key passphrases, it can automatically use them as a part of launchers.

## Minimum Requirements for Windows Local Accounts

Due to a security issue ([MS KB3178465](#)), we do not allow Windows local accounts to change their own passwords. Instead, we recommend using the discovery privileged account to change them. Each privileged account should meet the following requirements:

- Must be a domain user
- Must be a member of the local administrator group on all target end points

**Note:** The discovery account for SS can also be used for RPC.

## Modifying Password Changers

To modify a password changer, click the password changer name under **Admin > Remote Password Changing > Configure Password Changers** and then use the **Edit** or **Edit Commands** buttons to make changes. For more information about editing the custom PowerShell password changer, see [PowerShell Remote Password Changing](#) (KB).

**Note:** You can find the full, up-to-date list of password changers included with SS by default in [List of Built-In Password Changers](#) (KB).

## Password Changing Scripts

PowerShell scripts, SSH scripts, and SQL scripts for password changing, dependencies, and discovery custom actions can be created by administrators with the role permission called Administer Scripts. The scripts can be accessed by going to **Administration > Remote Password Changing > Scripts**.

**Note:** SS requires that WinRM is configured on the Web server. For instructions please see [Configuring WinRM for PowerShell](#).

### Creating Scripts

On the **Scripts** screen, select desired script tab and click **Create New** to enter the name of the script, a description, and the commands to run, then click **OK**. The script now shows up in the grid. Scripts can be deactivated and reactivated from the grid.

### Testing Scripts

All scripts run from the machine that SS is installed on, or the site assigned to the secret. To test a script, click the **Test** button on the grid next to the corresponding script.

PowerShell scripts run as the identity of the secret, so enter in an Active Directory credential to run the script as or select a secret to pre-fill the run-as credentials. Then enter in any command line arguments that the script requires. The output of the script is displayed above the grid for debugging purposes. To test the script over an engine, select a site from the **Site** list. This helps in diagnosing server specific issues where engines are installed.

### Using Scripts

To use a script as a password changer or Dependency, it must be wired up to the appropriate action under **Admin > Remote Password Changing** on the password changer or dependency changer.

Discovery scripting is done under **Admin > Discovery > Extensible Discovery**. For more information on configuring extensible discovery see the [Extensible Discovery Overview](#).

### Viewing Audits

A full history of each PowerShell script is kept and can be downloaded from the audit trail. Click **View Audit** to view the audit trail for PowerShell. Each time a script is updated, the previous one can be downloaded from the corresponding audit record.

**Note:** For additional information on setting up PowerShell scripts, please read the following KB article: [Creating and Using PowerShell Scripts](#).

## Privileged Accounts and Reset Secrets

By default, RPC uses the credentials on secret option, using the credentials stored in the secret to invoke a password change. For Windows and Active Directory accounts, a privileged account can be used instead by selecting the Privileged Account Credentials option and selecting an Active Directory secret with permission to change the account's password.

For secret templates with a custom commands password type, any number of associated reset secrets can assign for use in the custom commands. See [Custom Command Sets](#) (Professional or Premium Edition) for details on resetting secrets in custom commands.

When a secret is wired up with a privileged account or reset secrets, the ability to edit the username, host, domain, or machine is restricted if the user does not have access to those associated secrets. On the RPC tab, the user sees "You do not have access to View this secret" for the secret name and on the Edit page all text-entry fields mapped for RPC except the password is disabled. This added security prevents the user from changing the username and resetting another account's password.

**Note:** If the user does not have access to the privileged account or reset secrets, the ability to edit all secret text-entry fields mapped for RPC except the password text-entry field is restricted to prevent changing the password on another account.

## RPC Error Codes

The most common RPC errors are:

- **NERR\_PasswordPolicySettings:** The password SS attempted to set is a repeating password or one that does not meet domain password policy standards. A common reason is minimum password age, which is often defaulted to 24 hours.
- **ERROR\_ACCESS\_DENIED:** The user account's "Not Able to Change Password" setting could not be set or logon was denied.
- **ERROR\_INVALID\_PASSWORD:** Either the user does not exist (ensure the usernames match) or the password is not correct.

For more information about common error messages for Remote Password Changing, see [Remote Password Changing Errors](#) (KB).

## **RPC for Service Accounts and SSH Keys**

### **Service Accounts**

RPC can be performed on service accounts where the dependent services is automatically updated and restarted as the service account password is changed. Administrators are notified if a dependency fails to restart. The supported dependency types are IIS application pools, IIS application pool recycle, scheduled tasks, windows services, passwords embedded in .ini, .config, and other text files. Custom dependencies can be created using SSH, PowerShell, or SQL scripts. The application pool recycle only recycles the specified application pool, it does not update the password of the service account running the application pool. SS attempts to unlock the service account should the account become locked during the dependency password change if there is a privileged account assigned to the secret.

### **SSH Keys**

RPC can be performed on multiple public keys referencing the same private key in SS. The dependency types for this situation are SSH key rotation and SSH key rotation privileged.

## RPC Logs

The RPC logs for a specific secret can be accessed by clicking the **View Audit** button on Secret View page and ticking the check box at the bottom of the page for display password changing Log. The RPC logs for all secrets can be accessed by navigating to **Admin > Remote Password Changing**.

You can change the **Days to Keep Operational Logs** text box to set the period to keep RPC-related logs that might contain PII. SS automatically deletes logs older than that (in days).


## Running a Manual RPC

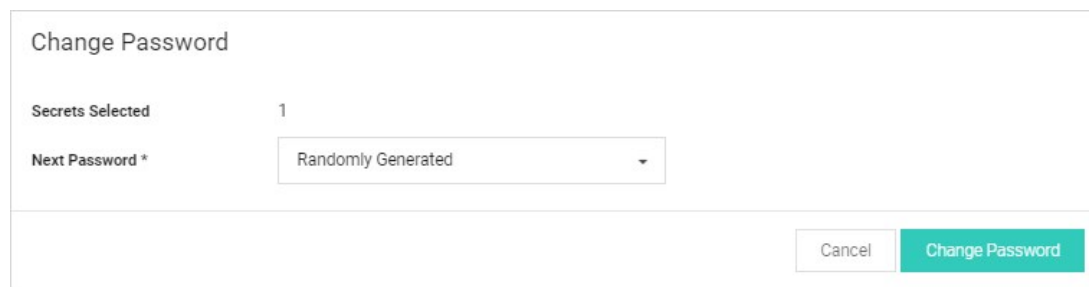
On the RPC tab there is a button called Change Password Remotely button that allows the use to change the password immediately instead of waiting for it to expire. When this button is clicked the user is taken to the Change Password Remotely page where they can enter in or generate the new password for the account. When the user clicks the Change button the secret enters the queue for having its password changed. The RPC Log found on the Remote Password Changing page details the results of the password change attempts and can be used for debugging.

If the secret is a Unix or Linux account and uses a password changer that supports SSH key rotation, the user can change the account's password, public and private keypair, and the private key passphrase. The user can enter or generate any of these items.

**Note:** If the password change fails, SS continues to retry until it is successful, or the change is canceled by the user. To manually cancel the change, click Cancel Password Change on the RPC tab.

To run a manual RPC:

1. From **Dashboard**, click its check box to select secret you want to test.
2. Click the  Change Password Remotely button. The Change Password popup page appears:



The image shows a 'Change Password' popup form. At the top, it says 'Change Password'. Below that, there is a label 'Secrets Selected' followed by the number '1'. Underneath, there is a label 'Next Password \*' followed by a dropdown menu currently showing 'Randomly Generated'. At the bottom right of the form, there are two buttons: 'Cancel' and 'Change Password'.

3. Click to select the **Next Password** dropdown list and select **Manual** or **Randomly Generated**. If you chose manual:
  1. The Password text box appears.
  2. Type the new password in the **Password** text box.
  3. Click the **Change Password** button.

Otherwise, click the **Change Password** button. The password change is now queued.

4. You can verify that the password change completed either by unmasking the password on this screen (click the lock icon beside the password field) or by looking at the **Remote Password Changing** log. You can find the Remote Password Changing log by going to **Admin > Remote Password Changing**.

## Treating Specific Heartbeat “Unknown Errors” as Connection Failures

**Note:** This setting was previously called “Password Change Error Code Translation (regex).”

The SS “Heartbeat Unknown Error to Unable to Connect Translation (regex)” setting can translate UnknownError heartbeat errors into connection errors based on text, such as the error code, in the error message. Using a regular expression, which you define, SS scans heartbeat UnknownError messages for specific text strings. When there is a match, SS changes the UnknownError to an “Unable to Connect” heartbeat error. This setting is useful if a custom command error is interpreted as UnknownError but the message indicates it actually was unable to connect. The translated connection error will cause SS to attempt another heartbeat.

**Figure:** Heartbeat Unknown Error to Unable to Connect Translation (regex) Setting

The screenshot shows the 'Active Directory Account' configuration page. It includes sections for 'Verify Password Changed Commands', 'Password Change Commands', and 'Password Change By Admin Credentials Commands', each with a 'Test Action' button and an informational message: 'This process is done through internal commands. The commands cannot be edited.' Below these is a 'Hide Advanced Settings' link. A table lists settings with their values and edit icons. The 'Heartbeat Unknown Error to Unable to Connect Translation (regex)' setting is highlighted in yellow. At the bottom are 'Back', 'Configure Scan Template', and 'View Audit' buttons.

SETTING	VALUE
Heartbeat Unknown Error to Unable to Connect Translation (regex)	
Attempt Password Change with new password when error contains (regex)	

**Note:** The UnknownError error is very common when running scripts and commands, making the regex discrimination desirable.

Logic:

(RPC UnknownError) AND (Regex match in error message) => RPC status changed to “Unable to Connect”

Example:

. \*error code is 10060.\* (any error with the code 10060 changes the RPC status to “Unable to Connect”)

### Procedure

To configure the unknown errors to trigger connection failures:

1. Go to **Admin > Remote Password Changing**. The Remote Password Changing Configuration page appears:

## Remote Password Changing Configuration

Enable Remote Password Changing	Yes
Enable Password Changing on Check In	No
Enable Heartbeat	Yes

Advanced (not required)

Days to Keep Operational Logs	30
-------------------------------	----

Back

Edit

Configure Password Changers

Configure Dependency Changers

Distributed Engine Configuration

View Audit

### Logs

Password Changing

Heartbeat

Run Now

Search...

50

90 minutes

Record Count 0

Page 1 / 1

« Prev

Next »

No results matching the current filter.

- Click the **Configure Password Changers** button. The Password Changers Configuration page appears:

## Password Changers Configuration

PASSWORD TYPE NAME	SCAN TEMPLATE	ACTIVE
Active Directory Account	Active Directory Account	Yes
Amazon IAM Console Password Privileged Account	AWS User Account	Yes
Amazon IAM Key	AWS Access Key	Yes
Blue Coat Account Custom (SSH)	SSH Local Account	Yes
Blue Coat Enable Password Custom (SSH)	SSH Local Account	Yes

3. Click the link for the desired password type. Its Account page appears:

Active Directory Account

Verify Password Changed Commands
Test Action

Password Change Commands
Test Action

This process is done through internal commands. The commands cannot be edited.

This process is done through internal commands. The commands cannot be edited.

Password Change By Admin Credentials Commands
Test Action

This process is done through internal commands. The commands cannot be edited.

Hide Advanced Settings

SETTING	VALUE
Heartbeat Unknown Error to Unable to Connect Translation (regex)	
Attempt Password Change with new password when error contains (regex)	

Back
Configure Scan Template
View Audit

4. If necessary, click the **Advanced Settings** link.

5. Click the pencil icon next to **Heartbeat Unknown Error to Unable to Connect Translation (regex)**. The Value text box appears.

6. Determine the desired text string to search for.

7. Type the desired regex in the **Value** text box.

8. Click the **Save** icon next to the text box

## Triggering an RPC When Defined Errors Occur

When the “Attempt Password Change with new password when error contains (regex)” setting is enabled, SS generates a new password to use during the next RPC attempt when the defined error is returned. Using a regular expression, which you define, SS scans the error message for specific text strings. When there is a match, SS generates and sets a new next password for the secret that will be used in the next RPC attempt, which will occur based on the templates RPC interval. To keep this process from generating too many next passwords, it is restricted to five attempts while failing RPC.

**Note:** Only the password field is updated. Passcodes and SSH keys are left alone.

**Figure:** Attempt Password Change with new password when error contains (regex) setting

The screenshot shows the 'Active Directory Account' configuration page. It has sections for 'Verify Password Changed Commands', 'Password Change Commands', and 'Password Change By Admin Credentials Commands'. Each section has a 'Test Action' button and a message: 'This process is done through internal commands. The commands cannot be edited.' Below these is a 'Hide Advanced Settings' link and a table of settings. The table has two columns: 'SETTING' and 'VALUE'. The setting 'Attempt Password Change with new password when error contains (regex)' is highlighted in yellow. At the bottom are buttons for 'Back', 'Configure Scan Template', and 'View Audit'.

SETTING	VALUE
Heartbeat Unknown Error to Unable to Connect Translation (regex)	
Attempt Password Change with new password when error contains (regex)	

Logic:

(RPC Error) AND (one or more regex matches) AND (five or fewer attempts) = > New password generated

Examples:

. \*UnknownError.\* (any unknown error)

. \* (any error)

. \*minimum.\* (minimum password length requirement error)

. \*0x80072035.\* (server rejects password error)

. \*0x80072035.\*!.\*minimum.\* (server rejects password or password length error)

## Procedure

To configure RPC in response to specific unknown errors:

1. Go to **Admin > Remote Password Changing**. The Remote Password Changing Configuration page appears:

## Remote Password Changing Configuration

Enable Remote Password Changing	Yes
Enable Password Changing on Check In	No
Enable Heartbeat	Yes

[Advanced \(not required\)](#)

Days to Keep Operational Logs	30
-------------------------------	----

[Back](#)
[Edit](#)
[Configure Password Changers](#)
[Configure Dependency Changers](#)

[Distributed Engine Configuration](#)
[View Audit](#)

### Logs

[Password Changing](#)
[Heartbeat](#)

[Run Now](#)

Record Count 0 Page 1 / 1 « Prev Next »

No results matching the current filter.

1. Click the **Configure Password Changers** button. The Password Changers Configuration page appears:

## Password Changers Configuration

PASSWORD TYPE NAME	SCAN TEMPLATE	ACTIVE
Active Directory Account	Active Directory Account	Yes
Amazon IAM Console Password Privileged Account	AWS User Account	Yes
Amazon IAM Key	AWS Access Key	Yes
Blue Coat Account Custom (SSH)	SSH Local Account	Yes
Blue Coat Enable Password Custom (SSH)	SSH Local Account	Yes

1. Click the link for the desired password type. Its Account page appears:

### Active Directory Account

#### Verify Password Changed Commands

[Test Action](#)

#### Password Change Commands

[Test Action](#)

**i** This process is done through internal commands. The commands cannot be edited.

**i** This process is done through internal commands. The commands cannot be edited.

#### Password Change By Admin Credentials Commands

[Test Action](#)

**i** This process is done through internal commands. The commands cannot be edited.

#### Hide Advanced Settings

SETTING	VALUE
Heartbeat Unknown Error to Unable to Connect Translation (regex)	<a href="#">✎</a>
Attempt Password Change with new password when error contains (regex)	<a href="#">✎</a>

[Back](#)
[Configure Scan Template](#)
[View Audit](#)

1. If necessary, click the **Advanced Settings** link.
2. Click the pencil icon next to **Attempt Password Change with new password when error contains (regex)**. The Value text box appears.
3. Determine the desired text string to search for.
4. Type the desired regex in the **Value** text box.
5. Click the **Save** icon next to the text box.



## Overview

Secret Server includes many pre-configured password changers that are used by Remote Password Changing (RPC). The following are commonly used password changers, and the list is always growing.

**Note:** To see the latest list, go to Admin > RPC > Configure RPC.

**Note:** Secret Server can use scripted password changers for devices that support SSH or Telnet (this allows for flexibility in changing passwords on less common devices). You can also run custom RPC PowerShell scripts to conduct password changes to other platforms.

## List

The followings are the current built-in password changers:

- Active Directory Account
- Amazon IAM Console Password Privileged Account
- Amazon IAM Key
- Blue Coat Account Custom (SSH)
- Blue Coat Enable Password Custom (SSH)
- Cisco Account Custom (SSH)
- Cisco Account Custom (Telnet)
- Cisco Enable Secret Custom (SSH)
- Cisco Enable Secret Custom (Telnet)
- ESX/ESXi (API)
- F5 BIG-IP Root Account (SSH)
- Generic Discovery-Only Credentials
- Generic ODBC (DataSource)
- HP iLO Account Custom (SSH)
- IBM iSeries Mainframe
- Juniper Account Custom (SSH)
- LDAP (Active Directory)
- LDAP (DSEE)
- LDAP (OpendLDAP)
- MySQL Account
- Office365 \*

- Oracle Account
- Oracle Account (AS SYS)
- Oracle Account (DataSource)
- PostgreSQL Account (x64)
- PowerShell Script \*\*
- SAP Account \*\*
- SonicWall NSA Web Admin Account
- SonicWall NSA Web Local User Account
- SQL Server Account
- SSH Key Rotation \*\*
- SSH Key Rotation (No Password) \*\*
- SSH Key Rotation Privileged Account \*\*
- SSH Key Rotation Privileged Account (No Password) \*\*
- Sybase Account
- Unix Account (SSH)
- Unix Account (Telnet)
- Unix Account Custom (SSH)
- Unix Account Custom (Telnet)
- Unix Account SU Takeover (SSH)
- Unix Account SUDO Takeover (SSH)
- Unix Root Account Custom (SSH)
- WatchGuard Custom (SSH)
- Web User Account (built-in support for AWS, Google, Salesforce)
- Windows Account
- z/OS Mainframe

\* Does not require an Advanced Scripting Add-On License. Will require PowerShell installation. \*\* Professional Edition add-on/Platinum Edition only

Other platforms that SS can change passwords on include:

- AS/400
- Linux / Mac
- Check Point

- Enterasys
- Dell DRAC

## Overview

You can create custom SQL password changers based on an ODBC driver. The Secret Server machine must have the corresponding ODBC driver installed. These can be downloaded from the corresponding database vendor sites.

ODBC connection strings vary depending on product. See [Example Connection Strings](#) below for sample ODBC connection strings for Microsoft SQL server and PostgreSQL.

## Create an ODBC Password Changer

1. In Secret Server, go to **Admin > Remote Password Changing**.
2. Click **Configure Password Changers**, and then scroll to the bottom of the page.
3. Click the **New** button.
4. Select **Generic ODBC (DataSource)** in the **Base Password Changer** dropdown list.
5. Type a name for your new custom password changer.
6. Under **Password Reset Commands**, type a command to reset a password (see below).

**Note:** Secret field variables can be used in a way similar to how they are used in a Linux or UNIX password changer, with the exception that they can be specified as ODBC parameters, assuming the command allows it. To parameterize a secret field variable, prefix it with the @ symbol instead of a \$.

## Example Reset Commands

Parameterized SQL server command:

```
EXEC sp_password @CURRENTPASSWORD, @NEWPASSWORD
```

**Note:** If the command does not support using parameters, the secret field values can be substituted into the command.

Substitution PostgreSQL command:

```
ALTER ROLE "USERNAME" WITH ENCRYPTED PASSWORD '$NEWPASSWORD'
```

Substitution MySQL command:

```
ALTER USER 'USERNAME' IDENTIFIED BY '$NEWPASSWORD';
```

## Adding Connection Strings

Each ODBC password changer requires a connection string. This can be specified within the password changer settings or in the secret itself.

### Adding Connection Strings to Password Changer Settings

Add a connection string to password changer settings:

1. In Secret Server, go to **Admin > Remote Password Changing**.
2. Click **Configure Password Changers**.

3. Click the name of your password changer.
4. Click the **Edit** button.
5. Type your database ODBC connection string in the **Connection String** text box.
6. Click the **Save** button.

## Adding Connection Strings to Secrets

The Connection String can also be specified on the secret by adding a new field to the template and mapping it to the **Data Source** property on the template's **Remote Password Changing** configuration. Otherwise, that mapping field can be left blank.

**Note:** See [Creating or Editing Secret Templates](#) for more information about adding fields to secret templates.

Example connection strings:

SQL 2012:

```
Driver={SQL Server Native Client 11.0};Server=$SERVER;Database=master;Uid=$USERNAME;Pwd=$PASSWORD;
```

PostgreSQL (x64):

```
Driver={PostgreSQL ANSI(x64)};Server=$SERVER;Port=$PORT;Database=$DATABASE;Uid=$USERNAME;Pwd=$PASSWORD;
```

## Troubleshooting

A common problem experienced with ODBC drivers is they require the IIS application pool to be set to either 32-bit or 64-bit mode to match the specified ODBC driver. When not set correctly, you will see an error in the system log when running heartbeat for a secret using that password changer.

PostgreSQL with 64-bit drivers will throw the following error if the IIS application pool is in 32-bit mode:

```
ExpiredSecretMonitor - System.Data.Odbc.OdbcException (0x80131937): ERROR [IM002] [Microsoft][ODBC Driver Manager] Data source name not found and no default driver specified
```

## PostgreSQL with Distributed Engines

A machine with a distributed engine installed requires the corresponding ODBC driver. In some cases, additional configuration may be necessary. For example, PostgreSQL requires adding an additional host entry:

1. Install the latest PostgreSQL ODBC drivers on the agent computer.
2. Modify the `pg_hba.conf` (for example: `/PostreSql/9.3/pg_hba.conf`) file to have a host entry for the agent computer IP address. For example, where 192.168.60.147 is the IP address of the distributed engine:

```
host all all 192.168.60.147/32 md5
```

## Overview

As of version 8.8, Secret Server supports running PowerShell scripts for Remote Password Changing (RPC) and heartbeat. Below are the steps for creating an Active Directory (AD) password changer that uses PowerShell scripts. The example is meant as a simple guide for how to wire-up the template to scripts as a proof of concept. Your actual PowerShell password changer scripts may be more complex depending on your environment and needs.

**Important:** Before you begin, please ensure password changing and heartbeat are enabled in **Admin > Remote Password Changing** and review the information on [Configuring CredSSP for use with WinRM/PowerShell](#), which will be necessary for most PowerShell password changing tasks.

## Procedure

The PowerShell scripts are created and accessed through the **Admin > Scripts** page. To create a PowerShell password changer, you need to create two scripts. The first script verifies the account's current password. The second script changes the account's password. These two scripts are linked to a new secret template.

### Task 1: Creating the Active Directory Verify Password Script

1. Navigate to **Admin > Scripts**.
2. Click the **+ Create New** button on the **PowerShell** tab.
3. Type the following information in the dialog:
  - **Name:** Active Directory Verify
  - **Description:** Script used to verify an Active Directory account
  - **Category:** Heartbeat
  - **Script:**

```
$domain = "LDAP://"+$Args[0];
$dn = New-Object System.DirectoryServices.DirectoryEntry($domain, $Args[1], $Args[2]);
if ($dn.name -eq $null){ throw "Authentication failed - please verify your username and password." };
```

4. Click the **OK** button to save the script.

### Task 2: Creating the Active Directory Change Script

1. On the **PowerShell** tab, click the **+ Create New** button.
2. Type the following information in the dialog:
  - **Name:** Active Directory Change
  - **Description:** Script used to change the password of an Active Directory account
  - **Category:** Password Changing
  - **Script:**

```
$Domain = $args[0]
$UserToChange = $args[1]
$NewPassword = $args[2]
$P_User = $args[0] + "\" + $args[3]
$P_PWord = ConvertTo-SecureString -String $args[4] -AsPlainText -Force
$Creds = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $P_User, $P_PWord
$pwd = ConvertTo-SecureString $NewPassword -AsPlainText -Force;
Set-ADAccountPassword -Server $Domain -Identity $UserToChange -NewPassword $pwd -Reset -Credential $Creds
```

3. Click the **OK** button to save the script.

### Task 3: Testing the Scripts

For the AD verification script:

1. Go to **Scripts > PowerShell tab**.
2. Click the Run Script arrow icon on the AD verify script. The Test Script popup appears.
3. Type the arguments (separated by spaces) in the **Arguments** text box: domain name (for you), username (yours), password (yours).  
For example: my.company.com ssadmin FD#@789Uik4\$
4. Type your domain name for the script-running account in the **Domain** text box.
5. Type the username in the **Username** text box for account that can run PowerShell scripts on the domain.
6. Type that user's password in the **Password** text box.
7. Click the **OK** button to test your script the with provided parameters.

For the Active Directory change script:

1. Go to **Scripts > PowerShell tab**.
2. Click the Run Script arrow icon on the AD change script. The Test Script popup appears.
3. Type the arguments (separated by spaces) in the **Arguments** text box: domain name (for you), username (yours), new password (yours), domain admin username, domain admin password. For example: my.company.com ssuser 08sSKthsoidPW ssadmin FD#@789Uik4\$
4. Type your domain name for the script-running account in the **Domain** text box.
5. Type the username in the **Username** text box for account that can run PowerShell scripts on the domain.
6. Type that user's password in the **Password** text box.
7. Click the **OK** button to test your script the with provided parameters.

**Note:** If successful, this will change the password on the account that is used for testing.

The remaining steps depend on the version of SS you are using. In Secret Server 10.0.000006 we introduced the ability to create multiple PowerShell password changers, each with their own set of password change and verify scripts. These password changers can be assigned to different scan templates to automatically assign different PowerShell password changer scripts to different types of local accounts when creating local account import rules in discovery. For more information about how scan templates and password changers are used in discovery and local account import rules, see our [Discovery Guide](#). Prior to 10.0.000006, there was only one PowerShell password changer and the scripts were assigned on the secret template.

#### Task 4: Configuring a Password Changer for Secret Server Version 10.0.000006 and Later

In Secret Server versions 10.0.000006 and later, after the scripts are tested and working correctly, the next step is to create a PowerShell password changer.

1. Go to **Admin > Remote Password Changing**.
2. Click the **Configure Password Changers** button.
3. Click the **New** button.
4. In the **Base Password Changer** dropdown list, select **PowerShell Script**.
5. Type the name of the new password changer.
6. Click the **Save** button. On the next page you will select the scripts to use for password changing and verification (heartbeat).
7. Under **Password Change Commands**:
  1. Select the script that you created to do password changes.

2. Type the following in the **Script Args** text box: \$DOMAIN \$USERNAME \$NEWPASSWORD \${1}\$USERNAME \${1}\$PASSWORD.
3. Click the **Save** button next to the **Script Args** text box.

8. Under **Verify Password Changed Commands**:

1. Select the script that you created to do heartbeats and verification.
2. Type the following in the **Script Args** field: \$DOMAIN \$USERNAME \$PASSWORD.
3. Click the **Save** button next to the **Script Args** text box.

**Note:** When SS runs the script, it replaces the fields with the matching secret field values. \$NEWPASSWORD is a special case for the new password that is generated by SS or specified by the user when performing a password change. For more information see [Using Secret Fields in Scripts](#).

**Important:** You must specify scripts for both sections and you must click the Save button next to each one for both to save.

## Task 5: Creating a Secret Template

The next step is to create the secret template:

1. Go to **Admin > Secret Templates**.
2. Click the **Create New** button.
3. Name the template PowerShell Active Directory.
4. Create the following new fields:
  - Domain Field Type: Text
  - Username Field Type: Text
  - Password Field Type: Password
  - Notes Field Type: Notes
5. Click the **Configure Password Changing** button.
6. Click the **Edit** button.
7. Click to select the **Enable Remote Password Changing** and **Enable Heartbeat** checkboxes.

## Task 6a: Finishing the Secret Template Configuration for Secret Server 10.0.000006 and later

**Note:** Complete either 6a or 6b, not both.

1. Select the password changer created in the previous section from the **Password Type to use** dropdown list.
2. Click to select **Domain** next to the **Domain** field.
3. Click to select **Username** next to the **User Name** field.
4. Click to select **Password** next to the **Password** field.
5. Click the **Save** button to save the mapping.

## Task 6b: Finishing the Secret Template Configuration for Secret Server 8.8.000000 to 10.0.000000

**Note:** Complete either 6a or 6b, not both.

1. Select **PowerShell Script** from the **Password Type to use** dropdown.

2. Click to select **Domain** next to the Domain field.
3. Click to select **Username** next to the User Name field.
4. Click to select **Password** next to the Password field.
5. Click to select **Active Directory Change** next to the **Remote Password Change Script** field.
6. Enter the following to the **Remote Password Change Args** field: `$DOMAIN $USERNAME $NEWPASSWORD ${1}$USERNAME ${1}$PASSWORD`.
7. Click to select **Active Directory Verify** next to the **Heartbeat Script** field.
8. Type the following next to the **Heartbeat Args** field: `$DOMAIN $USERNAME $PASSWORD`.

**Note:** When SS runs the script, it replaces the fields with the matching secret field values. `$NEWPASSWORD` is a special case for the new password that is generated by SS or specified by the user when performing a password change.

9. Click the **Save** button to save the mapping.

## Task 7: Creating Secrets Using PowerShell Remote Password Changing

Create the AD account secret PowerShell account:

1. Create three secrets (The first two **must** be different secrets):
  - One that is an Active Directory Account that has the necessary rights to run PowerShell on your domain
  - One that is an Active Directory Account that has the necessary rights to run a password change on your domain
  - One that is based on the new PowerShell Active Directory Template.
2. Create the Active Directory account secret PowerShell account.
3. On the dashboard, use the dropdown on the **Create Secret** widget and select **Active Directory Account**. Use the following parameters:
  - **Secret Name:** PowerShell Admin
  - **Domain:** Domain that the account exists on
  - **Username:** Account name that can run PowerShell scripts in the domain
  - **Password:** Password for the account
4. Click the **Save** button to save your secret and verify that it passes heartbeat.
5. Click the **Home** button to return to the dashboard.

Create the AD account secret for password changing:

1. On the dashboard, use the dropdown on the **Create Secret** widget and select **Active Directory Account**. Use the following parameters:
  - **Secret Name:** Password changing Admin
  - **Domain:** Domain that the account exists on
  - **Username:** Account name that can change passwords in the domain
  - **Password:** Password for the account
2. Click the **Save** button to save your secret and verify that it passes heartbeat.
3. Click the **Home** button to return to the dashboard.

Create the PowerShell Active Directory secret:

1. On the dashboard, use the dropdown on the **Create Secret** widget and select **PowerShell Active Directory Account**. Use the following parameters:
  - **Secret Name:** PowerShell AD user
  - **Domain:** Domain that the account exists on
  - **Username:** samAccountName of the account to be managed
  - **Password:** Password for the account
2. Click the **Save** button to save your secret and verify that it passes heartbeat.
3. Click the **Remote Password Changing** tab for the secret.
4. Click the Edit button.
5. Click to select **Privileged Account Credentials** in **Execute PowerShell**. The Privileged Account selector appears.
6. Click the **No Selected** Secret link.
7. Locate click on the **PowerShell Admin** secret.
8. Click the **Home** button to return to the dashboard.
9. In the **The following Secrets are available to be used in Custom Password Changing Commands and Scripts** section:
  1. Click the **No Selected Secret** link.
  2. Select your AD account secret for password changing.
  3. Click on the **Save** button.

Everything should now be configured for heartbeat and RPC on the Secret. Run **Heartbeat** (from the **General** tab in the Secret) to confirm that it works and run an RPC \*\* (from the **Remote Password Changing** tab of the secret) to confirm that it also works.

## Errors

If you receive the "The term 'Set-ADAccountPassword' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again." error, install the AD-Domain-Services in Powershell. To do this start PowerShell as an administrator then run the following command:

```
Install-windowsfeature -name AD-Domain-Services -IncludeManagementTools
```

Additionally you may need to install the Remote Server Administration Tools for your version of Windows and then in PowerShell run:

```
Import-Module Servermanager
```

As of version 8.6, Secret Server (SS) supports password changing for Salesforce.com accounts.

The password changer can be enabled on secrets that were created using the default Web Password Secret template or any custom template that is configured to use the Web User Account Password type.

The SS Web server's outbound IP Address must be added to the IP Address white list for your Salesforce.com organization. Please refer to the Salesforce.com documentation for instructions on how to set this up. See [Restricting Login IP Ranges for Your Organization](#).

In cases where this is not set up correctly, you may see the follow error in the Remote Password Changing logs:

Login failed: LOGIN\_MUST\_USE\_SECURITY\_TOKEN: Invalid username, password, security token; or user locked out.

Please note:

- Secret Server can only communicate to the following Salesforce default Login URLs: <https://test.salesforce.com> and <https://login.salesforce.com>.
- Having the domain URL in the secret will not work and will throw this exception: Login failed: INVALID\_LOGIN: Invalid username, password, security token; or user locked out. Only those two URLs work.
- There are three required Salesforce configurations:
  - Go to **Setup > Administration > Users > Profile**. Choose the user profile. Make sure that **Enabled API** is checked. This option is not available in all versions of Salesforce. Other versions will not have this enabled by default. Please see this ["Enable API" not available](#) article. If this setting is not enabled in salesforce you will get one of these errors: ERROR: Secret 'Salesforce Test' (Id = 1063) on Site 'EARTH' returned (LoginFailed). Exception: Login failed: API\_DISABLED\_FOR\_ORG: API is not enabled for this Organization OR Partner, System.Web.Services.Protocols.SoapException: API\_DISABLED\_FOR\_ORG: API is not enabled for this Organization or Partner.
- Configure network access and whitelist the distribute engine or SS IP address. If this is internal, use the public IP address.
  - Go to **Setup > Company Settings > My Domain**. Edit my domain settings and make sure that **Prevent login from** <https://login.salesforce.com> is unchecked.

## Reports

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

The reporting interface comes with a set of standard reports. These reports include a variety of 2D and 3D charting and graphing components and a full grid of data. Some of the reports are purely data detailed and have no charts. You can also create your own reports based on any SS data, such as user, audit, permissions, and folders. You can create report categories to aid in the organization of your reports. Reports can be arranged to provide access to auditors and meet compliance requirements. These reports can be accessed in the **General** tab on the **Reports** page.

**Figure:** Reports Page

Reports

General

Security Hardening

User Audit

Activity

Active Secret Sessions  
Active Secret Sessions Count  
Custom Report Activity  
Database Configuration Audit  
Distributed Engine Activity  
Dual Control Audit  
Engine Status  
Event Subscription Activity  
Folder Activity  
Heartbeat Status  
Heartbeat Status by Day  
Internal Communication Changes  
IP Address Range Audit  
License Audit  
RPC by Day  
Secret Activity  
Secret Activity Today  
Secret Activity Yesterday  
Secret Template Activity  
Session Recording Errors  
Unlimited Administrator behavior  
Users Activity

Discovery Scan

What Secrets failed to import by Discovery?  
What Secrets are pending import by Discovery?  
Discovery Scan Status  
What computers in Active Directory no longer exist?  
What computers have been successfully scanned?  
What computers that exist have not been successfully scanned?

Folders

What folder permissions exist?  
What folder permissions exist for groups?  
What folders can all users see?  
What folders can a user see?

Groups

Group Membership  
Group Membership By Group

Legacy Reports

Secret Expiration Health  
Secret Server Usage  
Secret Template Distribution  
Top Ten Viewers

Password Compliance

Secret Password Compliance Statuses  
What Secrets Do Not Meet Password Requirements?

Report Schedules

Report Schedules

Roles and Permissions

What role assignments exist?  
What role permission assignments exist?  
What role permissions does a user have?

Secret Policy

What Folders have Policies assigned?  
What Secrets have different Policies than their folders?  
What Secrets have policies assigned?

Secrets

What Secrets changed passwords in the last 90 days?  
What file types have been uploaded to Secrets?  
What file types have been uploaded to Secrets? (Pie Chart)  
What Secrets have not changed passwords for over 90 days?  
What Secrets have failed Heartbeat?  
Secret Permissions Mismatch.  
What Secret permissions exist for a group?  
What Secret permissions exist for a user?  
What Secret permissions exist?  
What Secrets have been accessed by an impersonated user?  
What Secrets have been accessed by a user?  
What Secrets have been accessed?  
What Secrets are expiring this week?  
Secrets with Failed Password Change  
Secrets Failing Heartbeat  
Secrets Pending Heartbeat  
What Secrets require approval?  
What Secrets don't require approval?  
Secret Count per Site  
What Secrets can all users see?  
What Secrets Do Not Have Distributed Engines?  
What Secrets Have Distributed Engines?  
What Secrets have Expiration?  
What Secrets require Comments?  
What Secrets can a user see?

System Reports

FolderPermissionsReportName  
FolderSecretsReportName  
GroupLookupReportName  
Privileged Behavior Analytics Configuration Activity  
PermissionLookupReportName  
RolePermissionsReportName  
UserAccessReportName

User

Failed login attempts  
Secret Template Permissions by User  
What users have had an admin reset their password?  
Who hasn't logged in within the last 90 days?

The *Security Hardening Report* checks aspects of SS to ensure security best practices are being implemented. While SS runs with all the items failing, administrators should be aware of possible security issues within an installation. For details on this, see [Reports Security Hardening Tab](#).

The User Audit Report shows all secrets accessed by a user during a specified period.

Secret Server includes many pre-configured reports that you can run or use as templates for creating custom reports. Below are the reports shipped with current release of SS:

**Note:** Unless otherwise designated, reports listed are available in all editions. However, older releases may not include all reports listed here.

## Activity

- Custom Report Activity
- Database Configuration Audit
- Distributed Engine Activity (**Professional**)
- Dual Control Audit
- Event Subscription Activity (**Professional**)
- Folder Activity
- Internal Communication Changes
- IP Address Range Audit
- License Audit
- Secret Activity
- Secret Activity Today
- Secret Activity Yesterday
- Secret Template Activity (**Professional**)
- Session Recording Errors
- Unlimited Administrator Behavior
- Users Activity

## Discovery Scan

**Note:** These are available in Professional edition. In prior versions they are available only in Enterprise Plus.

- Discovery Scan Status
- What computers in Active Directory no longer exist?
- What computers have been successfully scanned?
- What computers that exist have not been successfully scanned?
- What Secrets failed to import by Discovery?
- What Secrets are pending import by Discovery?

## Folders

- What folders can a user see?
- What folders can all users see?
- What folder permissions exist?
- What folder permissions exist for groups?

## Groups

- Group Membership
- Group Membership By Group

## Legacy Reports

- Secret Server Usage

- Secret Expiration Health
- Secret Template Distribution
- Top Ten Viewers **(Professional)**

## Password Compliance

- What Secrets Do Not Meet Password Requirements?
- Secret Password Compliance Statuses

## Report Schedules

Report Schedules **(Professional)**

## Roles and Permissions

- What role permissions does a user have?
- What role assignments exist?
- What role permission assignments exist?

## Secrets

- Secret Count per Site
- Secret Permissions Mismatch
- What file types have been uploaded to Secrets?
- What file types have been uploaded to Secrets? (Pie Chart)
- What Hooks and Dependencies use a script? **(Enterprise Plus/Premium add-on)**
- What Secret permissions exist for a group?
- What Secret permissions exist for a user?
- What Secret permissions exist?
- What Secrets are expiring this week?
- What Secrets can a user see?
- What Secrets can all users see?
- What Secrets changed passwords in the last 90 days?
- What Secrets Do Not Have Distributed Engines? **(Professional)**
- What Secrets don't require approval? **(Enterprise/Premium)**
- What Secrets have been accessed by a user?
- What Secrets have been accessed by an impersonated user?
- What Secrets have been accessed?
- What Secrets have Distributed Engines?
- What Secrets have Expiration?
- What Secrets have failed Heartbeat? **(Professional)**
- What Secrets have not changed passwords for over 90 days?
- What Secrets require approval? **(Enterprise/Premium)**
- What Secrets require Comments?

## Secret Policy

- What Folders have Policies Assigned?
- What Secrets have different Policies than their folders?
- What Secrets have policies assigned?

## Users

- Failed login attempts
- Who hasn't logged in within the last 90 days?
- What users have had an admin reset their password?
- Secret Template Permission by User

**Note:** You can find additional reports in the [Custom Report Gallery](#).

There are two ways to create a Report. From the Reports Edit page, click the **Add New** link at the bottom of a Report Category. Or alternatively, from the Reports View page, click the **Create it** link at the bottom of that page.

## Creating a Custom Report

1. Click the **+** icon on the right side of the **Reports** menu item. The Report Edit page appears:

**Report Edit**

[Report Definition](#)

**Report Name**

**Report Description**

**Report Category**

– Select Report Category ▾

**Chart Type**

None ▾

**Page Size**

15 ▾

**Use Database Paging**


☒


**Report SQL**


1

[Dynamic SQL Parameter KB Article](#)

[Show Secret Server SQL database information](#)

 Save

 Preview

 Cancel

2. Type the report name in the **Report Name** text box. This is the name that is displayed on the Reports page as a link underneath its containing category.
3. Type a description in the **Report Description** text box. This is displayed in the Report View page. It is also used as the Tooltip for the Report name on the Reports page.

4. Click the **Report Category** dropdown list to select the category the report will appear in on the Reports page.
5. Click the **Chart Type** dropdown list to select the type of chart to use for displaying the results. If set to None, a grid displays.
6. Click the **Page Size** dropdown list to select the page size limit for the data displayed in the grid.
7. Click to select the **Use Database Paging** check box if desired. See [Database Paging](#).
8. Paste your script in the Report SQL text box. See [Report SQL Scripts](#). Our completed report looks like this:

## Report Edit

[Report Definition](#)
[Report Preview](#)

Report Name

Active Users Custom Report

Report Description

This displays a user list with all active user activity on view and returns an user id. This defaults to the current logged in user.

Report Category

User

Chart Type

None

Page Size

15

Use Database Paging

☐

Report SQL

```

1 SELECT
2   tau.UserIdAffected,
3   tau.[Action],
4   tau.Notes,
5   tau.DateRecorded,
6   tau.IpAddress,
7   tau.MachineName,
8   tau.DatabaseName,
9   tu.UserId,
10  tu.UserName
11 FROM tbAuditUser tau INNER JOIN tbUser tu ON tau.UserId=tu.UserId WHERE tu.UserId=#USER

```

[Dynamic SQL Parameter KB Article](#)  
[Show Secret Server SQL database information](#)

Save

Preview

Cancel

9. (optional) Click the **Preview** button to see your report before creating it. Our preview looks like this:

## Report Edit

Report Definition [Report Preview](#)

### Active Users Custom Report

This displays a user list with all active user activity on view and returns an user id. This defaults to the current logged in user.

User

☐ Show Inactive Users

[▶ Update Report](#)

Save To File | Show All < 1 to 15 of 194 >

USERIDAFFECTED	ACTION	NOTES	DATERECORDED	IPADDRESS	MACHINENAME	DATABASENAME	USERID	USERNAME
6	LOGIN SUCCESS		6/25/2019 02:33 PM	192.168.113.18	QA-CUST- SQL-01	SS_Playground	6	
6	LOGIN FAILED	Attempted to use session key from a different IP address. Expected: 192.168.113.18	7/16/2019 03:36 PM	192.168.113.8	QA-CUST- SQL-01	SS_Playground	6	
6	LOGIN SUCCESS		7/16/2019 03:37 PM	192.168.113.8	QA-CUST- SQL-01	SS_Playground	6	

10. Click the **Report Definition** tab to return to your editing.

11. Click the **Save** button. The new report's page appears:

Reports > Active Users Custom Report

Filter Schedule Edit Delete View Audit Email Report

194 Items

USERIDAFF...	ACTION	NOTES	DATERECOR...	IPADDRESS	MACHINEN...	DATABASEN...	USERID	USERNAME	
6	LOGIN SUC...		6/25/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Attempted t...	7/16/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN SUC...		7/16/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Attempted t...	7/30/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN SUC...		7/30/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Attempted t...	8/7/2019 0...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN SUC...		8/7/2019 0...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Attempted t...	8/13/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGOUT		8/13/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Authenticati...	8/13/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN SUC...		8/13/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGIN FAIL...	Attempted t...	8/26/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGOUT		8/26/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGOUT		8/26/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		
6	LOGOUT		8/26/2019 ...	192.168.11...	QA-CUST-S...	SS_Playgrou...	6		

[Load More](#)

12. The new report now appears on the Reports page:

<b>User</b>
<a href="#">Active Users Custom Report</a>
<a href="#">Failed login attempts</a>
<a href="#">Secret Template Permissions by User</a>
<a href="#">What users have had an admin reset their password?</a>
<a href="#">Who hasn't logged in within the last 90 days?</a>

## Editing Reports

To edit a report:

1. Click the **Reports** menu item. The Reports page appears, listing all the reports.
2. Click the name of the report, which is a link. That report's page appears.
3. Click the **Edit** button. The Report Edit page appears. See [Creating a Custom Report](#) for details about the parameters.

**Note:** The SQL script text cannot be edited for non-custom (built-in) reports.

## Report SQL Scripts

### Overview

The best way to create SQL scripts is to view existing ones and the SS database structure. Click any existing report's link to arrive at its page. Then click the **Edit** button. The SQL appears in the Report SQL text box.

**Note:** Even though you are pressing the Edit button, you cannot edit non-custom reports. You can view their parameters, including their SQL script.

### Dynamic Parameters

Reports support the embedding of certain parameters into the SQL so you can dynamically change the resulting data set. Another option available for custom reports is to apply a different color to returned rows dependent on certain conditions. For more information as well as examples, see the [Using Dynamic Parameters in Reports](#) topic.

### Viewing Secret Server SQL Database Information

You can show SS's SQL database information to assist with creating custom reports. By selecting the SQL Table from the list, the details of the table's columns display in a grid. Click the **Show SS SQL database information** link to see the SQL Table list and SQL Table Columns grid. The link is also available on the Report Edit page.

You can click **Preview** button at the bottom of the page to see a preview of the chart. The resulting chart displays in the Report Preview section at the bottom of the page.

## Database Paging

Database paging allows the database to load large reports more quickly. We recommend database paging if the query is expected to pull large amounts of data for the report. Implementing database paging may not work if the SQL query uses some keywords, including TOP, OPTION, INSERT, UNION, WITH, or aliases containing the word FROM.

Example queries:

- Works using database paging: `SELECT * FROM tbSecret WHERE NAME LIKE 'Test%'`
- Does not work using database paging: `SELECT TOP 10 * FROM tbSecret WHERE SecretName LIKE 'Test%'`

To delete or undelete a report.

- **Delete:** To delete a report, click the **Delete** button.
- **Undelete:** To undelete a report, you must navigate to the Reports Edit page as deleted reports are not visible on the Reports View page. On the Reports Edit page, click the **Show Deleted** button. This displays a Deleted Report category, which contains all the deleted reports. Either drag the report to a report category that is not deleted or click the report name to go into its Report View page. In there, click the **Undelete** button.

For details on the Show Deleted button, see [Deleting and Undeleting Reports](#).

- **Rearrange:** Any item with the icon can be dragged and dropped to a new location. Report categories can be moved anywhere within the page. Reports can be moved from one report category to another.
- **Create New:** Click **Create Report Category** and specify a category name and description on the following page. Note that the Report Category Description is used as the tooltip for the report category on the Reports View page.
- **Delete:** Click the icon next to the report category name. This deletes all the reports in the category. To undelete the reports, see [Deleting and Undeleting Reports](#).
- **Edit:** Click the icon next to the report category name to change the name or description of the category.

## Reports General Tab

See [Built-In Reports](#) for the most up-to-date list of reports included.

The reports are listed under the report categories. To view a report, click on its name. This takes you to the **Report View** page.

You can view a record of all the actions performed on reports by clicking on the **View Audit** button. For more information on this, see [Administration Auditing](#).

For details on the **Edit** button, see [Creating and Editing Reports](#).

The **Create it** link is a shortcut for creating a new report.

You can adjust the look of the Reports View page. The report categories as well as the reports can be rearranged on the page. To do this, click **Edit** on the Reports page.

## Reports Security Hardening Tab

The Security Hardening Tab configures aspects of SS to ensure security best practices are being implemented. While SS runs with all the items failing, administrators should be aware of possible security issues within an installation. Below is an explanation of the different features:

### Configuration Section

- **Allow Approval for Access from Email:** This is a convenience option that allows users to approve or deny a secret access request by clicking a link in the request email sent by SS. Allow Approval From Email does not require a user to authenticate with SS when approving access to a secret. This can be a security concern if the approver's email account becomes compromised. Turn Allow Approval From Email off to get a pass result.
- **Browser AutoComplete:** Browser AutoComplete allows Web browsers to save the login credentials for the SS login screen. These credentials are often kept by the Web browser in an insecure manner on the user's workstation. Allowing AutoComplete also interferes with the security policy of your SS by not requiring the user to re-enter their login credentials on your desired schedule. To prevent the AutoComplete feature, disable the Allow AutoComplete option on the Configuration page.
- **File Attachment Restrictions:** File attachment restrictions allows administrators to configure what kind of file attachments can be uploaded to secrets. This helps protect users from being tricked into downloading a malicious secret attachment. The file extension and maximum file size can be specified, such as:

\*.7z, \*.bmp, \*.ca-bundle, \*.cer, \*.config, \*.crt, \*.csr, \*.csv, \*.dat, \*.doc, \*.docx, \*.gif, \*.gz, \*.id-rsa, \*.jpeg, \*.jpg, \*.json, \*.key, \*.lic, \*.p7b, \*.pcf, \*.pdf, \*.pem, \*.pfx, \*.pkey, \*.png, \*.ppk, \*.pub, \*.tar, \*.tif, \*.tiff, \*.tpm, \*.txt, \*.vdx, \*.vsd, \*.vsdx, \*.xls, \*.xlsx, \*.xml, \*.zip

This security check will fail if the file attachment restrictions is not enabled. This check will return warnings if a potentially dangerous file extension is allowed, maximum file size is not specified, or maximum file size is greater than 30 MB.

- **Force Password Masking:** Password masking prevents over-the-shoulder viewing of your passwords by a casual observer (when masked, passwords show as \*). To activate this option, click to select the **Force Password Masking** option on the **Configuration** page.
- **Frame Blocking:** Frame blocking prevents the SS site from being placed in an iFrame. This is to prevent clickjacking attacks. There may be legitimate reasons for placing SS in a frame, such as embedding the UI in another site. To turn frame blocking on, enable the setting under the Security tab in Configuration.
- **Login Password Requirements:** Login passwords can be strengthened by requiring a minimum length and the use of various character sets. A minimum password length of 8 characters or longer is recommended. In addition, all character sets (lowercase,

uppercase, numbers and symbols) are required to get a pass result. Turn on these login password settings on the Configuration page.

- **Maximum Login Failures:** The maximum number of login failures is the number of attempts that can be made to login to SS as a user before that user's account is locked. A user with user administration permissions is then required to unlock the user's account. The maximum failures allowed should be set to 5 or less to get a pass result. Change the "Maximum Login Failures" settings on the Configuration page.
- **Remember Me:** Remember Me is a convenience option that allows users to remain logged in for up to a specific period. This setting can be a security concern as it does not require re-entry of credentials to gain access to SS. Turn Remember Me off on the Configuration page to get a pass result. It must be set to be valid for 1 day or less to not get a fail result.
- **Secure Session and Forms Auth Cookies:** Cookies contain potentially sensitive information that can allow users to log onto application. By default, cookies are not marked with the secure attribute. That is, **they are transmitted unencrypted when a user accesses SS through HTTP instead of HTTPS.**

For more information about how to secure your cookies, see [Secure ASP Session and Forms Authentication Cookies](#) (KB).

- **Web Service HTTP Gets Allowed:** Web service HTTP get requests are allowed. Allowing HTTP GET requests allows REST-style calls to many SS Web service methods. This can be a security concern because simply clicking a link to the Web service, created by a malicious user, would cause it to be executed.
- **Zero Information Disclosure Error Message:** Replace all error messages with a custom "contact your admin" message. Error messages can be very helpful when diagnosing installation and configuration issues. However, having errors displayed to a potential attacker can provide him or her with the critical information they need to perform a successful attack.

## Database Section

- **SQL Account Using Least Permissions:** Use the fewest SS permissions as possible in the SQL Account used to access the database. We recommend using a least permission approach where the account only has dbOwner. See [Installing and Configuring SQL Server](#).
- **SQL Server Authentication Password Strength:** SQL Server authentication requires a username and password. The password must be a strong password to get a pass result. Strong passwords are 8 characters or longer and contain lowercase and uppercase letters, numbers and symbols. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.
- **SQL Server Authentication Username:** The SQL Server authentication username should not be obvious. The use of "sa", "ss" or "secretserver" triggers a fail result. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.
- **Windows Authentication to Database:** Windows authentication takes advantage of Windows security to provide secure authentication to SQL Server. The SQL Server authentication options can be changed by going to the installer (installer.aspx) and changing them on Step 3. Please see the [Installation Guide](#) for instructions on configuring Windows authentication to SQL Server.

## Environment Section

- **Application Pool Identity:** The Application Pool identity GAMMA\ss\_iis\_svc appears to be a member of the administrators group on the system. This puts the system at risk by giving more access than necessary.
- **DPAPI or HSM Encryption of Encryption Key:** Encrypt your SS encryption key, and limit decryption to that same server. Data Protection API (DPAPI) is an encryption library that is built into Windows operating systems. It allows encryption of data and configuration files based on the machine key. Enabling DPAPI Encryption in SS protects the SS encryption key by using DPAPI, so even getting access to the SS encryption key is not enough to be useful—the machine key is required. If you enable this option, back up your encryption key first, as a DPAPI encrypted file can only be used by the machine it was encrypted on.

## SSL Section

**Note:** SSL needs to be running with at least a 128-bit key size to get a pass result. A warning result indicates your key size is less than 128 bits. A fail result indicates you are not using SSL.

- **Require SMTP SSL:** SMTP SSL is required to ensure that all communication between SS and the email server is encrypted. Enable the "Use SSL" option in Secret Server to get a pass result.
- **Require SSL:** Secure Sockets Layer (SSL) is required to ensure that all communication between the Web browser and SS is encrypted and secure. Once the SSL certificate is installed, Force HTTPS/SSL in Configuration to get a pass result. Please see the [Installing a Self-Signed SSL/HTTPS Certificate](#) Knowledge Base article for instructions.
- **SSL/TLS Hash:** Check the digest algorithm of the certificate. If the algorithm is SHA1, this check returns a warning because SHA1 is being phased out. If the digest algorithm is MD2, MD4, or MD5, the check will fail because they are not secure. SHA256, SHA384, and SHA512 will pass. This check fails if SS cannot be loaded over HTTPS.
- **SSL/TLS Key:** Check the key size of the HTTPS certificate used. If it is RSA or DSA, the key must be at least 2048-bit to pass. If the signature algorithm of the certificate is ECDSA, the key size must be at least 256-bit to pass. If the algorithm of the certificate is unknown, the result shows "unknown". This check fails if SS cannot be loaded over HTTPS.
- **SSL/TLS Protocols:** Check for legacy SSL or TLS protocols, which should not be used in a secure environment. If the server accepts SSLv2 or SSLv3 connections, this check will fail. SSLv2 is not considered secure for data transport, and SSLv3 is vulnerable to the POODLE attack. If this server does not support TLSv1.1 or TLSv1.2, this check will give a warning because they are recommended. The SSL certificate used may affect what protocols can be used, even if they are enabled. This check will fail if SS cannot be loaded over HTTPS.
- **Using HTTP Strict Transport Security:** HTTP Strict Transport Security (HSTS) is an additional security layer for SSL. HSTS allows SS, Password Reset Server, or Group Management Server to inform browsers that it should only be accessible over HTTPS. With this setting enabled, visitors are automatically redirected by their browser to the HTTPS-enabled site.

## Reports User Audit Tab

User Audit Reports show all secrets accessed by a user during a specified period. For a more detailed explanation, see [User Audit Report](#).

If there are requirements around protecting potentially personally identifying information when running reports or viewing recorded sessions, you can enforce that another user has authorized you by enabling dual control for a secret or Report. You can configure Dual Controls by clicking **Admin** and then **Dual Controls**.

**Note:** Dual Controls is not in the **Admin** dropdown and must be accessed from the full administration menu.

When enabled a user in the approver group must enter in their credentials before a report or session can be viewed:

Once the approver has entered their credentials, the resource can be accessed. The following resources can have dual control applied.

- **Access Report:** Protects any report from the General tab of the Reports view.
- **Access User Audit Report:** Protects the user audit report for any user.
- **Create Report:** Requires dual control for anytime a user creates a custom report.
- **Secret Session Access:** Requires dual control for any recorded or live sessions for a secret

1. Click the **Reports** menu item. The Reports page appears:

Reports

+

WS

General

Security Hardening

User Audit

Activity

[Active Secret Sessions](#)
[Active Secret Sessions Count](#)
[Custom Report Activity](#)
[Database Configuration Audit](#)
[Distributed Engine Activity](#)
[Dual Control Audit](#)
[Engine Status](#)
[Event Subscription Activity](#)
[Folder Activity](#)
[Heartbeat Status](#)
[Heartbeat Status by Day](#)
[Internal Communication Changes](#)
[IP Address Range Audit](#)
[License Audit](#)
[RPC by Day](#)
[Secret Activity](#)
[Secret Activity Today](#)
[Secret Activity Yesterday](#)
[Secret Template Activity](#)
[Session Recording Errors](#)
[Unlimited Administrator behavior](#)
[Users Activity](#)

Discovery Scan

[What Secrets failed to import by Discovery?](#)
[What Secrets are pending import by Discovery?](#)
[Discovery Scan Status](#)
[What computers in Active Directory no longer exist?](#)
[What computers have been successfully scanned?](#)
[What computers that exist have not been successfully scanned?](#)

Folders

[What folder permissions exist?](#)
[What folder permissions exist for groups?](#)
[What folders can all users see?](#)
[What folders can a user see?](#)

Groups

[Group Membership](#)
[Group Membership By Group](#)

Legacy Reports

[Secret Expiration Health](#)
[Secret Server Usage](#)
[Secret Template Distribution](#)
[Top Ten Viewers](#)

Password Compliance

[Secret Password Compliance Statuses](#)
[What Secrets Do Not Meet Password Requirements?](#)

Report Schedules

[Report Schedules](#)

Roles and Permissions

[What role assignments exist?](#)
[What role permission assignments exist?](#)
[What role permissions does a user have?](#)

Secret Policy

[What Folders have Policies assigned?](#)
[What Secrets have different Policies than their folders?](#)
[What Secrets have policies assigned?](#)

Secrets

[What Secrets changed passwords in the last 90 days?](#)
[What file types have been uploaded to Secrets?](#)
[What file types have been uploaded to Secrets? \(Pie Chart\)](#)
[What Secrets have not changed passwords for over 90 days?](#)
[What Secrets have failed Heartbeat?](#)
[Secret Permissions Mismatch.](#)
[What Secret permissions exist for a group?](#)
[What Secret permissions exist for a user?](#)
[What Secret permissions exist?](#)
[What Secrets have been accessed by an impersonated user?](#)
[What Secrets have been accessed by a user?](#)
[What Secrets have been accessed?](#)
[What Secrets are expiring this week?](#)
[Secrets with Failed Password Change](#)
[Secrets Failing Heartbeat](#)
[Secrets Pending Heartbeat](#)
[What Secrets require approval?](#)
[What Secrets don't require approval?](#)
[Secret Count per Site](#)
[What Secrets can all users see?](#)
[What Secrets Do Not Have Distributed Engines?](#)
[What Secrets Have Distributed Engines?](#)
[What Secrets have Expiration?](#)
[What Secrets require Comments?](#)
[What Secrets can a user see?](#)

System Reports

[FolderPermissionsReportName](#)
[FolderSecretsReportName](#)
[GroupLookupReportName](#)
[Privileged Behavior Analytics Configuration Activity](#)
[PermissionLookupReportName](#)
[RolePermissionsReportName](#)
[UserAccessReportName](#)

User

[Failed login attempts](#)
[Secret Template Permissions by User](#)
[What users have had an admin reset their password?](#)
[Who hasn't logged in within the last 90 days?](#)

2. Click the link for the desired report. Its page appears:

Reports > What Secrets changed passwords in the last 90 days?



Schedule

Edit

Delete

View Audit

Email Report

SECRET NAME

LAST PASSWORD CHANGE



mpearson-gamma-admin

6/21/2019 08:37 am

Fake Secret 00

8/14/2019 12:29 pm

Fake Secret 01

8/14/2019 12:29 pm

Fake Secret 02

8/14/2019 12:29 pm

Fake Secret 03


8/14/2019 12:29 pm

- Click the  button in the top right of the page and select Export. The Export page appears:

## Export

Please enter your password for security purposes.

Folder

 [No Selected Folder](#)

Password

\*

Export with Folder Path

☒


Export Child Folders

☒

Export Format

☒ CSV ☐ XML

Enter any additional notes or explanations for the export.

 Export

- Click the **No Selected Folder** link to choose a folder.
- Type your SS password to ensure "you" are you.
- Click the **Export with Folder Path** check box to recreate the secret folder hierarchy in the OS folder.
- Similarly, click the **Export Child Folders** check box to include any child folders.
- Click the **Export Format** option button to select an output folder type.
- Type any notes in the unlabeled note text box.
- Click the **Export** button.

## Creating New Schedules for Reports

1. To create a schedule for a report, click **Schedule** on the **Report View** page. The Custom Report Schedules page appears.
2. Click the **Create New** button.

## Viewing Existing Report Schedules

1. To view existing schedules for a report, click **Schedule** on the Report View screen. A list of existing schedules for the report appear in the grid.
2. To view the details of a schedule, click the schedule name in the grid.
3. (Optional) Deleted schedules can be made visible by checking the **Show Deleted** box at the bottom of the grid.
4. Click the **View** link in the History column of the grid to view the history of all generated reports for that schedule.

## Editing Schedule Settings

When viewing a report, click Schedule and then the name of the report schedule to modify it. The following configuration options are available:

- **Schedule Name:** This is the name of the schedule for the report. This name must be unique to the SS installation.
- **Health Check:** This sends an email notification only when the report contains data.
- **Recurrence Schedule:** This specifies the schedule runs every X number of days, weeks, or months, with the option to specify days of the week or month as well. The date and time that the report schedule is effective can be specified in this section as well.
- **Save Generated Reports:** This saves the history of generated reports in the database for later viewing. Enabling this setting also allows you to specify the number of generated reports to save.
- **Send Email:** SS sends an email containing the generated report every time the schedule runs. Enabling this setting also allows you to specify whether the email is sent with the high priority flag and a list of SS users or groups that receive the generated report email. Add additional email recipients in the text box below the subscribers, separating recipients with a semi-colon.

The following configuration options appear if the report being scheduled contains at least one dynamic parameter in the SQL of the report:

- **User Parameter Value:** Value of the #USER parameter to set in the report when it is generated.
- **Group Parameter Value:** Value of the #GROUP parameter to set in the report when it is generated.
- **Start Date Parameter Value:** Value of the #STARTDATE parameter to set in the report when it is generated.
- **End Date Parameter Value:** Value of the #ENDDATE parameter to set in the report when it is generated.

**Note:** As version 7.0, Secret Server allows creation of Reports using custom SQL.

Reporting supports embedding certain parameters into the SQL to give the viewer controls to dynamically change the report. The supported parameters are:

## Primary Parameters

### #STARTDATE

This displays a calendar picker on view and returns a date. This defaults to beginning of the year and truncates the hours and minutes to 12:00 AM.

Example: display all users who have logged in after a certain date:

```
SELECT
    Domain,
    Username,
    LastLogin
FROM tbUser
    LEFT JOIN tbDomain ON tbUser.DomainId = tbDomain.DomainId
WHERE
    LastLogin > #STARTDATE
```

### #ENDDATE

This displays a calendar picker on view and returns a date. This defaults the current day and truncates the hours and minutes to 11:59 PM.

Example: display all users who have logged on a certain date:

```
SELECT
    Domain,
    Username,
    LastLogin
FROM tbUser
    LEFT JOIN tbDomain ON tbUser.DomainId = tbDomain.DomainId
WHERE
    LastLogin > #STARTDATE
AND
    LastLogin < #ENDDATE
```

### #USER

This displays a user dropdown list with all active users on view and returns an user id. This defaults to the current logged in user.

Example: display all audit entries for a certain user:

```
SELECT
    tau.UserIdAffected,
    tau.[Action],
    tau.Notes,
    tau.DateRecorded,
    tau.IpAddress,
    tau.MachineName,
    tau.DatabaseName,
    tu.UserId,
    tu.UserName
FROM tbAuditUser tau INNER JOIN tbUser tu ON tau.UserId=tu.UserId WHERE tu.UserId=#USER
```

### #ORGANIZATION

This is an internal parameter used for determining the current instance's organization code. This is only useful for Secret Server Cloud. There is no need to use this parameter in your reports for on-premises edition.

**Note:** As of Secret Server 7.8.000048 the #GROUP parameter is also available.

**#GROUP**

Displays a group dropdown list with all active groups on view and returns a group id. This defaults to the Everyone group.

Example: display the group details of the selected group:

```
SELECT
  GroupID,
  GroupName,
  Active
FROM tbGroup
WHERE GroupID = #GROUP
```

**#FOLDERID**

Displays a folder picker that shows all Folders and returns a folder id.

Example: Display secret names in a selected folder:

```
SELECT
  s.SecretName
FROM tbSecret s
WHERE s.Folderid = #FOLDERID
```

**#FOLDERPATH**

Displays a folder picker that shows all folders and returns the path of the folder.

Example: display folders that are child folders of the selected path:

```
SELECT *
FROM tbFolder f
WHERE FolderPath LIKE '% ' + #FOLDERPATH + '%'
```

**#CUSTOMTEXT**

Displays a text input where a user can put in arbitrary free text for searching.

Example: display secrets that have names that contain the text input:

```
SELECT *
FROM tbFolder f
WHERE FolderPath LIKE '% ' + #CUSTOMTEXT + '%'
```

**Additional Parameters**

The following additional parameters can be used to make your report more dynamic:

**Parameters**

**Table:** Additional Parameters

#ENDCURRENTMONTH	The last day of current month
#ENDCURRENTYEAR	December 31st of the current year

#ENDPREVIOUSMONTH	The last day of the previous month at 11:59:59 PM
#ENDPREVIOUSYEAR	December 31st of the previous year
#ENDTODAY	End of today at 11:59:59 PM
#ENDWEEK	End of the current week (Sunday) at 11:59:59 PM
#ENDYESTERDAY	End of Yesterday at 11:59:59 PM
#STARTCURRENTMONTH	The first day of current month
#STARTCURRENTYEAR	January 1st of the current year
#STARTPREVIOUSMONTH	The first day of the previous month at 12:00 AM
#STARTPREVIOUSYEAR	January 1st of the previous year
#STARTTODAY	Beginning of today at 12:00 AM
#STARTWEEK	Beginning of the current week (Monday) at 12:00 AM
#STARTYESTERDAY	Beginning of yesterday at 12:00 AM

## Example

For example, the following script would give you a list of all users who have logged on during the last calendar month:

```
SELECT
    Domain,
    Username,
    LastLogin
FROM tbUser
LEFT JOIN tbDomain ON tbUser.DomainId = tbDomain.DomainId
WHERE
    LastLogin BETWEEN #STARTPREVIOUSMONTH AND #ENDPREVIOUSMONTH
```

**Note:** As of Secret Server 7.8.000048, the #STARTWEEK and #ENDWEEK parameters are available.

## Coloring Your Reports

Another option when creating reports is to include a Column in your SQL query called "Color" this will give the row that particular color. See [HTML Color Names](#).

For example, to show users who haven't logged in within 90 days in Red:

```
SELECT DisplayName
CASE
    WHEN LastLogin < GetDate() - 90 THEN 'Red'
    ELSE 'White'
END AS Color
FROM tbUser
```

You can view a record of all the actions performed on a report by clicking on the View Audit button. For more information, see [Administration Auditing](#).

On this page you see the graph, chart, grid, etc. for the report. To see a grid representation of the report, click the **Show Data** link to expand that area. If there is no data, then no graph is visible and the text "There are no items" displays in the Show Data section.

Some reports use dynamic values like user, start date, and end date. Adjust these values to generate the report you need. Click the **Update Report** button to generate the new report.

The **Edit** button allows you to alter the report to fit your requirements. See the Creating and Editing a Report section below for details.

## Roles

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Modeled after the role-based access control (RBAC) mechanism, role-based security (RBS) is SS's method of regulating permission to system access. Each user and group must be assigned to a role. SS ships with three roles: Administrator, User, and Read-Only User. Each role contains various permissions to match the job function of the user. With RBS, strict granular access to SS is ensured. A list of role permissions and their descriptions can be found in the [Secret Server Role Permissions List](#).

You can assign multiple permissions to a role. For example, you could assign Administer Users, Edit Secret, Own Secret, and View Active Directory permissions to a role. That role can then be assigned to a user or group.

**Note:** The Unlimited Administrator permission allows the user to have unlimited administrator rights when Unlimited Administrator is enabled in the configuration. By default, it is disabled.

**Note:** to see the built-in roles and what permissions they possess, click the desired role link on the Admin > Roles page.

To assign roles to a user, click the **Assign Roles** button on the main **Roles** page. Depending on which tab is selected, this page allows you either view the roles that are assigned to users or view the users that are assigned to roles. To change these settings, click the **Edit** button. Now select a role from the list and assign or unassign users to the role. In the **By User or Group** tab, you can select a user or group from the list and assign or unassign roles to them in the selectable list boxes.

You can create roles from the Roles page. To get to the Roles page, navigate to **Administration > Roles**. Click the **Create New** button to add the role.

To add or remove permissions to an existing role, click the role name of the role you wish to edit.

On this Role View page, permissions can be added and removed from the role by clicking the **Edit** button. Use the arrow buttons to move permissions into and out of the current role. If needed, a role can also be enabled or disabled from this page. If you have finished with your changes, you must click the **Save** button to have the changes take effect.

## Overview

Secret Server uses role-based access control (RBAC) to regulate permissions. The roles are assigned to users or groups. A complete list of the permissions available to roles appears below:

**Note:** to see the built-in roles and what permissions they possess, click the desired role link on the Admin > Roles page.

## Complete List

### Access Offline Secrets on Mobile

Allows a user to cache their Secrets in the Secret Server mobile application for offline use. This permission does not automatically come with the Administrator role.

### Add Secret

Allows a user to create new Secrets. The Add permission no longer include the role permission View Secret.

### Add Secret Custom Audit

Allows a user to make a custom audit entry when accessing a Secret using the web services API.

### Administer Active Directory

Allows a user to view domains, edit existing domains, delete domains, and add new domains. Also allows a user to force synchronization or set the synchronization interval.

### Administer Backup

Allows a user to view and configure automated backups for Secret Server. Users with this role permission can change the backup path, disable backups, and set the backup schedule.

### Administer Configuration

Allows a user to view and edit general configuration options. For example, a user with this role permission can turn on "Force HTTPS/SSL" and disable "Allow Remember Me".

### Administer Configuration Proxying

Allows a user to view and edit SSH Proxy settings.

### Administer Configuration SAML

Allows a user to view and edit SAML integration settings on the Login tab of Configuration settings.

### Administer Configuration Security

Formerly "Administer Security Configuration," allows a user to view and edit security configuration options in Secret Server. Currently, these include enabling FIPS compliance mode and protecting the encryption key.

### Administer Configuration Session Recording

Allows a user to view and edit session recording settings on the Session Recording tab of Configuration settings.

### Administer Configuration Two Factor

Allows a user to change the configuration settings of the two factor authentication that are available for users logging into Secret Server.

## **Administer Configuration Unlimited Admin**

Formerly "Administer Unlimited Admin Configuration," allows a user to turn on Unlimited Admin Mode. When this mode is enabled, users with the "Unlimited Administrator" role permission can view and edit all Secrets in the system, regardless of permissions. Note that you can assign "Administer Unlimited Admin Configuration" to one user and "Unlimited Administrator" to another user. This would require one user to turn on the mode and another user to view and edit secrets.

## **Administer ConnectWise Integration**

Allows a user to view and edit configuration options for synchronizing with ConnectWise. This can be accessed through the "Folder Synchronization" link on the Administration page. Note that you need at least view access on the sync folder in order to set up or edit the ConnectWise integration.

## **Administer Create Application Accounts**

Formerly "Create Application Account", allows a user to create application user accounts to be used exclusively for accessing Secret Server via the API.

## **Administer Create Users**

Allows a user to create new local users in Secret Server, but not edit them once created.

## **Administer Custom Password Requirements**

Allows a user to view and edit custom password requirements that can be configured under the Security tab for individual Secrets.

**Administer Data Retention** Can manage audit data retention, such as editing and running now. This permission does not automatically come with the Administrator role.

## **Administer Discovery**

Allows a user to view and import computers and accounts that are found by Discovery.

## **Administer Distributed Engine Configuration**

Allows a user to update the Distributed Engine configuration.

## **Administer DoubleLock Keys**

Allows a user to view, edit, create, and disable DoubleLock keys. A DoubleLock key acts as a separate encryption key to protect your most sensitive secrets. This option allows users to access and use the "DoubleLocks" link on the Administration page.

## **Administer Dual Control**

Allows a user to view, edit, create, and disable Dual Control settings for reports and recorded sessions.

## **Administer Event Subscriptions**

Allows a user to view, edit and create event subscriptions.

## **Administer Export**

Allows a user to view the export log. Also allows users to export Secrets to which they have access to a clear text, CSV file.

## **Administer Folders**

Allows a user to view, edit, create, move, and delete folders. Users still need the relevant view, edit, and owner permissions on the folders to

perform these tasks.

## **Administer Groups**

Allows a user to view, edit, create, and disable groups. Also allows users to assign users to groups and remove users from groups.

## **Administer HSM**

Allows a user to change configuration or disable the use of a Hardware Security Module (HSM).

## **Administer IP Addresses**

Allows a user to create, edit, and delete IP Address Ranges. These ranges are used to restrict certain users to specific IP Addresses.

## **Administer Key Management**

Allows a user to enable, change, or disable the Key Management (Secret Server Cloud only).

## **Administer Languages**

Allows a user to change the default language of Secret Server.

## **Administer Licenses**

Allows a user to view, edit, install, and delete licenses.

## **Administer Nodes**

Allows a user to view and edit server nodes and clustering settings.

## **Administer OpenID Connect**

Allows a user to manage OpenID connections.

## **Administer Password Requirements**

Allows a user to view and edit character sets and password requirements.

## **Administer Pipelines**

Allows a user to create, edit, and remove event pipelines and event pipeline policies.

## **Administer Remote Password Changing**

Allows a user to turn Heartbeat and Remote Password Changing on and off globally. Also allows users to create new password changers and install password changing agents on remote machines.

## **Administer Reports**

Allows a user to view, edit, delete, and create reports. Also allows users to customize report categories.

## **Administer Role Assignment**

Allows a user to view which users and groups are assigned to which roles. Also allows users to assign users and groups to different roles.

## **Administer Role Permissions**

Allows a user to view, edit, create and delete roles. Also allows users to assign different permissions to each role.

## **Administer Scripts**

Allows a user to view, edit, and add PowerShell, SQL, and SSH scripts on the Scripts Administration page.

## **Administer Search Indexer**

Allows a user to view and edit search indexer options. These options control how searching in Secret Server works. For example, a user with this role permission could enable search indexing, which allows users to search on fields within a secret.

## **Administer Secret Policy**

Allows a user to create and edit Secret Policies."

## **Administer Secret Templates**

Allows a user to view, edit, disable, and create Secret Templates.

## **Administer Security Analytics**

Allows a user to view and edit the settings for Privilege Behavior Analytics.

## **Administer Session Monitoring**

Allows a user to view and terminate active launcher sessions.

## **Administer SSH Menus**

Allows a user to edit and create SSH Menus, used in whitelisting commands that can be used on a SSH session.

## **Administer System Log**

Allows users to view and clear the System Log, which shows general diagnostics information for Secret Server.

## **Administer Teams**

Users can create, delete, and view all teams.

## **Administer Template Custom Columns**

Allows a user to enable the "Expose for Display" setting of a Secret template field to make it available for use in Dashboard custom columns.

## **Administer Users**

Allows a user to create, disable, and edit users in the system.

## **Administer Workflows**

Allows users to manage workflows (advanced access management).

## **Advanced Import**

Allows a user to import Secrets from an XML file. Users with the this permission can import groups, folders, site connectors, sites, and secret templates, without having to create a secret. Users must have the Secret Server permissions needed for the objects listed in the XML.

## **Allow Access Challenge**

Allows a user be challenged by Privileged Behavior Analytics if their behavior deviates from their normal behavior and meets certain requirements set by Privileged Behavior Analytics. Administrators do not have this permission by default.

## **Approve Via Duo Push**

Allow a user to approve access requests via Duo push notifications. Administrators do not have this permission by default.

## **Assign Pipelines**

Allows the user to assign an event pipeline policy to secret policies, or folders.

## **Assign Secret Policy**

Allows a user to assign Secret Policies to folders and Secrets.

## **Bypass SAML Login**

Allows a user to login with local account without using SAML.

## **Copy Secret**

Allows a user to copy secrets when that user also has Own Secret role permission.

## **Create Root Folders**

Allows a user to create new folders at the root level of the folder structure.

## **Delete Secret**

Allows a user to mark secrets as deleted.

## **Delete Secrets from Reports**

Allows a user to run the delete Secrets action from a report.

## **Edit Secret**

Allows a user to edit secrets. Note that they still require the "Edit" or "Owner" permissions on the individual secrets they are editing.

## **Expire Secrets from Reports**

Allows a user to expire Secrets listed in a report."

## **Force Check In**

Allows a user to force a Secret that is checked out by another user to be checked in.

## **Own Group**

Allows a user to be an owner of a group. This permission is in the default Group Owner role, which is automatically assigned when that user is set as owner of a group.

## **Own Secret**

Formerly "Share Secret", allows a user to share secrets with other users. Also allows users to perform more advanced tasks on secrets of which they are "Owners", such as configuring expiration schedules, configuring the web launcher, converting secret template, and copying secrets (when a user also have the Copy Secret role permission.)

## **Own User**

Allows the user to become a user owner, used to configure specific users without the Administer Users permission.

## **Personal Folders**

Allows a user to have personal folder when the global personal folders configuration options is enabled.

## **Privilege Manager Administrator**

Allows the user to have the "Administrator" role for Privilege Manager, giving full access to the system.

## **Privilege Manager Helpdesk User**

Allows the user to have the "Help Desk" role for Privilege Manager, giving full access to approve or deny escalation requests.

## **Privilege Manager MacOS Admin**

Allows the user to have the MacOS "Administrator" role for Privilege Manager, giving full access to the system.

## **Privilege Manager Windows Administrator**

Allows the user to have the Windows "Administrator" role for Privilege Manager, giving full access to the system.

## **Privilege Manager User**

Allows the user to have the "User" role for Privilege Manager, giving read and write permissions to most items, but not rights to modify security permissions. Administrators do not have this permission by default.

## **Rotate Encryption Keys**

Allows a user to start a process that rotates the Secret encryption keys.

## **Session Recording Auditor**

Grants access to the session recording of a secret to a user with at least "List Access" permission on the secret. Administrators do not have this permission by default.

## **Unlimited Administrator**

Allows a user to view and edit all secrets in the system, regardless of permissions, when Unlimited Admin Mode is on. Note that another user with the "Administer Unlimited Admin Configuration" role permission would still need to turn this mode on.

## **Unrestricted by Teams**

Users can view all users, groups, and sites, regardless of team affiliation. Essentially, teams do not exist for the users with this permission, and the Teams page is not available to them. The default user role has this permission.

## **User Audit Expire Secrets**

Allows a user to view the "User Audit" report, which shows all secrets that have been accessed by a particular user in a specified date range. Also allows the user to force expiration on all these secrets, which would make Secret Server automatically change the password.

## **View About**

Allows a user to view the "About" page from the Help menu, which links to external resources such as Technical Support and the Thycotic blog.

## **View Active Directory**

Allows a user to view, but not edit, the Active Directory settings in the system.

## **View Advanced Dashboard**

Allows a user to view advanced dashboard. Without this permission, users will only be able to view basic dashboard.

## **View Advanced Secret Options**

Allows a user to view the Remote Password Changing, Security, and Dependency tabs on a Secret they have access to.

## **View Backup**

Allows a user to view, but not edit, the automated backup settings.

## **View Configuration**

Allows a user to view, but not edit, general configuration settings.

## **View Configuration Proxying**

Allows a user to view, but not edit, SSH Proxy settings.

## **View Configuration SAML**

Allows a user to view SAML integration settings on the Login tab of Configuration settings.

## **View Configuration Security**

Formerly "View Security Configuration," allows a user to view the security configuration of Secret Server.

## **View Configuration Session Recording**

Allows a user to view session recording settings on the Session Recording tab of Configuration settings.

## **View Configuration Two Factor**

Allows a user to view the configuration settings of the two factor authentication that are available for users logging into Secret Server.

## **View Configuration Unlimited Admin**

Formerly "View Unlimited Admin Configuration," allows a user to view the Unlimited Admin Mode configuration. Also allows a user to view the Unlimited Admin Mode audit log.

## **View ConnectWise Integration**

Allows a user to view, but not edit, the ConnectWise integration settings.

## **View Data Retention**

Can view retained audit data. This permission does not automatically come with the Administrator role.

## **View Deleted Secrets**

Allows a user to view Secrets that have been deleted in the system.

## **View Discovery**

Allows a user to view, but not edit, computers and accounts that are found by Discovery.

## **View Distributed Engine Configuration**

Allows a user to view the Distributed Engine configuration.

## **View DoubleLock Keys**

Allows a user to view which DoubleLock keys exist in the system.

## **View Dual Control**

Allows a user to view configured Dual Control settings for reports and Secret sessions.

## **View Event Subscriptions**

Allows a user to view event subscriptions.

## **View Export**

Allows a user to view the export log of the system to see when users exported secrets. Does not allow a user to export.

## **View Folders**

Allows a user to view, but not edit, folders in the system.

## **View Group Roles**

Allows a user to see which groups and users are assigned to which roles. Does not allow a user to change these assignments.

## **View Groups**

Allows a user to see which groups exist in the system. Also allows a user to see which users belong to each group.

## **View HSM**

Allows a user to view the Hardware Security Module (HSM) configuration settings.

## **View IP Addresses**

Allows a user to view IP Address Ranges that have been created to restrict access. Does not allow a user to edit these ranges.

## **View Key Management**

Allows a user to view the Key Management settings (Secret Server Cloud only).

## **View Launcher Password**

Allows a user to unmask the password on the view screen of secrets with a launcher. Typically, this includes Web Passwords, Active Directory accounts, Local Windows accounts, and Linux accounts.

## **View Licenses**

Allows a user to view, but not edit, the licenses in the system.

## **View Nodes**

Allows a user to view, but not edit, the Secret Server web server nodes.

## **View Password Requirements**

Allows a user to view character sets and password requirements.

## **View Pipelines**

Allows a user to view event pipeline policies and policy activities.

## **View Remote Password Changing**

Allows a user to view, but not edit, Heartbeat and Remote Password Changing settings.

## **View Reports**

Allows a user to view, but not edit, reports.

## **View Roles**

Allows a user to view roles in the system. Also allows a user to see which groups are assigned to which roles.

## **View Scripts**

Allows a user to view PowerShell, SQL, and SSH scripts on the Scripts Administration page.

## **View Search Indexer**

Allows a user to view, but not edit, search indexer settings.

## **View Secret**

Allows a user to only view which Secrets exist in the system.

## **View Secret Audit**

Allows a user to view Secret Audit.

## **View Secret Password History**

Allows a user to view previous passwords for a secret.

## **View Secret Policy**

Allows a user to view, but not edit, Secret Policies.

## **View Secret Templates**

Allows a user to view, but not edit, Secret Templates.

## **View Security Analytics**

Allows a user to view, but not edit, settings for Privilege Behavior Analytics.

## **View Security Hardening Report**

Allows a user to view the Security Hardening Report.

## **View Session Monitoring**

Allows a user to view active launcher sessions.

## **View Session Recording**

Allows a user to view recorded sessions within Secret Server.

## **View SSH Menus**

Allows a user to view existing SSH Menus, used in whitelisting commands that can be used on a SSH session.

## **View System Log**

Allows a user to only view the System Log, which shows general diagnostics information for Secret Server.

## **View Teams**

Users can view all teams. This is essentially a read-only Administer Teams.

## **View User Audit Report**

Allows a user to view, but not edit, the User Audit Report.

## **View Users**

Allows a user to view which users exist in the system.

## **Web Services Impersonate**

Allows a user to send an approval request to act as another user within their organization when accessing Secret Server programmatically. Administrators do not have this permission by default.

## Secret Checkout

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

The SS *checkout* feature forces accountability on secrets by granting exclusive access to a single user. If a secret is configured for check out, a user can then access it. If **Change Password on Check In** is turned on, after check in, SS automatically forces a password change on the remote machine. No other user can access a secret while it is checked out, except unlimited administrators. This guarantees that if the remote machine is accessed using the secret, the user who had it checked out was the only one with proper credentials at that time.

**Note:** The exception to the exclusive access rule is unlimited administrators. If Unlimited Administration is enabled, users with Unlimited Administrator role permission can access checked out secrets.

**Note:** Secrets with a doublelock cannot be configured for check out.

Each secret must be individually set to require check out:

1. From the **Secret View** page, open the **Security** tab to modify a secret's **Check Out** setting.
2. You must configure RPC before **Change Password on Check in** can be set.
3. Enable **Require Check Out** to force users to check out the secret before gaining access.
4. Enable **Change Password on Check In** to have the password change after the secret is checked in.

## Overview

In addition to changing the password on check in, secret owners can also specify administrator-created PowerShell scripts, called *hooks*, to run before or after checkout and check in. These are accessed from the **Hooks** tab of the secret, which only shows if checkout is enabled and PowerShell scripts have been created by an admin.

To specify a before- or after-checkout hook, click **Create New Hook** and specify the following settings:

- **Before/After:** Whether the PowerShell script should run before or after the event action.
- **Event Action:** The hook runs at either check in or checkout.
- **Name:** A descriptive name for the hook.
- **Description:** An extended description for the purpose of the hook.
- **PowerShell Script:** Administrator-created PowerShell script to run.
- **Arguments:** Any command line arguments to pass to the PowerShell script.
- **Stop on Failure:** If enabled, SS prevents the event action if the script returns an error. For example, if "Stop on Failure" is selected for a checkout action, then SS prevents the user from checking out the secret if the script fails.
- **Privileged Account:** If needed, the script can run as another secret's identity.

## Checkout User Variables for Scripts

Checkout user variables for scripts are special code variables that return information about the user or automated task making the checkout request, rather than system or secret information. For example, the \$USERNAME variable returns one or more user IDs related to a specific secret, whereas the \$SECRETSERVERUSERID checkout user variable returns the user ID of the logged-on user or automated task.

**Note:** These variables may also be useful for Active-Directory-related scripts.

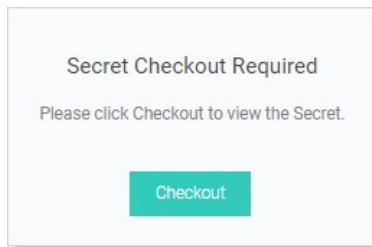
The variables are:

**Table:** Checkout User Variables for Scripts:

\$SECRETSERVERUSERID	Logged-on user's ID	-1
\$SECRETSERVERUSERNAME	Logged-on user's name	"System"
\$SECRETSERVERDISPLAYNAME	Logged-on user's display name	"System"
\$SECRETSERVEREMAILADDRESS	Logged-on user's email address	Empty string

**Note:** You can find the regular "system" variables in the [Editing Custom Commands](#) subsection of the Custom Password Changers section.


Enable “Require Check Out” for the secret—users are then prompted for check out when attempting to view that secret.





To configure password checking on check in, navigate to the **Remote Password Changing Administration** page and set **Enable Password Changing on Check In**. If RPC is turned off, enable it before configuring checkout. Once RPC and checkout are enabled, secrets can be configured for interval that specifies how long a user has exclusive secret access.


**Remote Password Changing Configuration**


Enable Remote Password Changing	Yes
Enable Password Changing on Check In	Yes
Check Out Interval	30 minutes
Enable Heartbeat	Yes


 Back

 Edit

 Configure Password Changers

 Configure Dependency Changers

 Distributed Engine Configuration

 View Audit

Any user attempting to view a checked-out secret is directed to a notification dialog informing them when the secret is available. SS automatically checks in secrets after either 30 minutes or the interval specified on the secret. Users can check in the secret earlier from the secret's page.

## Secret DoubleLocks

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.


SS's *doublelock* is a feature that provides an additional security layer by encrypting secret data with a supplemental custom encryption key that is only accessible with an additional password, regardless of regular permissions, SS login access, or physical access to the machine running SS. Doublelock uses private and public key encryption technology to securely share access to doublelock.

A shortcut way of thinking about doublelocks is as a special extra password for secrets that is held by a set group of users. In addition, both the password and the group of users are reusable for other secrets.

1. Navigate to the secret you wish to doublelock by clicking **Secrets** on the main menu.
2. Either drill down to the desired secret in the folders on the main menu, or click the secret in the **All Secrets** table to arrive at the secret's page:

Personal Folders > Will > Mudfin Gmail ☆

General
Security
Audit
RPC
Dependencies
Sharing
Settings

Secret Name *	Mudfin Gmail	Edit
Template	Web Password	Edit
URL *	https://mail.google.com	Edit
UserName *	smedlymufin	Edit
Password *	***** Show	Edit
Notes		Edit
Launchers	 Web Password Filler	

Show Advanced
Edit all fields

3. Click the **Security** tab.

Personal Folders > Will > Mudfin Gmail ☆

General Security Audit RPC Dependencies Sharing Settings

CHECK OUT Edit

Require Check Out No

APPROVAL Edit

Require Approval No

OTHER SECURITY Edit

Require Comment  
Users will be prompted for comment and ticket number when accessing a Secret. No

Enable DoubleLock No

Hide Launcher Password No

- Click the **Edit** link for the **Other Security** section. The section becomes editable:

OTHER SECURITY

Require Comment  
Users will be prompted for comment and ticket number when accessing a Secret. ☐

Enable DoubleLock ☐


Hide Launcher Password ☐

Cancel Save

- Click to select the **Enable DoubleLock** check box. The DoubleLock dropdown list appears.
- Click to select the doublelock you created earlier.


**Important:** Enabling doublelock on this secret only grants users access if they have access to to the doublelock and enter their doublelock password. Enabling doublelock disables the RPC features for the secret.


- Click the **Save** button. The doublelock is now enforced for the secret.


1. Click the  icon at the top right of SS. Your My Profile page appears:


## My Profile


GENERAL


Display Name	Will
User Name	Will
Email	
Domain	Local
Last Login	Mon, 13 May 2019 15:26:42 GMT


 Account Settings  
*Notifications, theming, password masking, and language settings.*


 Change Password  
*Change local Secret Server user password.*


 Change DoubleLock Password  
*Change the doublelock password associated to this user account*


 Reset DoubleLock Password  
*Reset the doublelock password associated to this user account*


 Manage Secret Access Requests  
*Approve or deny Secret access requests.*

 Application Access Requests  
*Manage applications requesting access to Secret Server on your behalf.*

 Sessions  
*View all active sessions for the current user.*


 Notifications  
*View all alert notifications for the current user.*

 View in Classic UI  
*Switch to use a classic Secret Server theme.*

 Logout  
*Log the current user out of Secret Server*

2. Click the **Change DoubleLock Password** button. The Change DoubleLock Password page appears:

### Change DoubleLock Password



Please enter a new DoubleLock password and press the Change Password button. This will allow you to access Secrets with DoubleLock.

Current Password \*

New Password \*

Confirm Password \*

✓ Change Password

✕ Cancel

3. Type your current doublelock password in the **Current Password** text box.

**Note:** You cannot create a doublelock password until you are associated with a doublelock. When you access your first doublelock, you are prompted to create a password.

4. Type your desired doublelock password in the **Password** and **Confirm Password** text boxes.

**Important:** It is critical that you remember or securely store this password. It cannot be recovered.

5. Click the **Change Password** button. The password is created.

1. Navigate to **Admin** > **See All**. The Administration page appears:

What are you looking for?

Search for an admin option



[Simplified View](#) ▾



## Actions

Secret Server features that perform important jobs



## Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more



## Users, Roles, Access

These features help you organize users & permission settings within Secret Server



## Diagnostics, Logs, Security

Reference options for diagnostics, logs, and security features



## Tools & Integrations

Find Secret Server tools and other product integrations here

2. Type and then click **DoubleLock** in the search text box. The DoubleLock Management page appears:

Admin > DoubleLock Management

DoubleLocks
Audit

Manage DoubleLock Password
Create New DoubleLock

DOUBLELOCK GROUP MANAGEMENT
Show Inactive

DOUBLELOCK GROUP NAME	NUMBER OF SECRETS	NUMBER OF USERS	CREATED	ACTIVE
Main DoubleLock	1 Secrets	1 Users	11/11/2019	✓
System Admin DoubleLock	1 Secrets	1 Users	1/31/2001	✓
Test DoubleLock	3 Secrets	1 Users	11/11/2019	✓

3. Click the desired doublelock. Its page appears:

Admin > DoubleLock Management > My DoubleLock

Doublelock Information

Summary information for this DoubleLock including when it was created and whether or not it is active / enabled. Once a DoubleLock is disabled any associated Secrets will be unable to be accessed.

DoubleLock Name My DoubleLock Edit

Date Created 11/14/2019

Enabled Yes Edit

Associated Secrets 0

Assign Users Add or Remove

Defines the users that are able to access Secrets using this DoubleLock or assign this DoubleLock to other Secrets. Note that only users who have already created a DoubleLock password can be added to a DoubleLock. Users must be part of a DoubleLock group to edit the users in the group. A user can not remove themselves from the DoubleLock

Users Assigned to DoubleLock

Accessible Secrets Associated with DoubleLock

Secrets that can only be accessed by using this DoubleLock. Note: Only Secrets to which you have access will show in this list.

No Secrets are currently using this DoubleLock.

- Click the **Add or Remove** link in the **Assign Users** section. An Add Users to DoubleLock section appears:

### Add Users to DoubleLock

All

Search

No users / groups match the search criteria that have created DoubleLock passwords. If a user is expected, ensure that they have created a DoubleLock password.


Cancel

Save

- (Optional) Click the dropdown list to limit the user search to a specific domain.
- Type the user's name in the search text box. The matching users appear below the search text box:

### Add Users to DoubleLock

john

☐  John Smith

Cancel

Save

- Click to select the check box next to the desired user. The users that appear do not already have a doublelock assigned to them.
- Repeat the process for other users.
- Click the **Save** button.

1. Navigate to **Admin** > **See All**. The Administration page appears:

What are you looking for?

Search for an admin option



[Simplified View](#) ▾



## Actions

Secret Server features that perform important jobs



## Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more



## Users, Roles, Access

These features help you organize users & permission settings within Secret Server



## Diagnostics, Logs, Security

Reference options for diagnostics, logs, and security features



## Tools & Integrations

Find Secret Server tools and other product integrations here

2. Type and then click **DoubleLock** in the search text box. The DoubleLock Management page appears:

Admin > DoubleLock Management

+

JC

DoubleLocks
Audit

Manage DoubleLock Password

Create New DoubleLock

DOUBLELOCK GROUP MANAGEMENT

Show Inactive

DOUBLELOCK GROUP NAME	NUMBER OF SECRETS	NUMBER OF USERS	CREATED	ACTIVE
Main DoubleLock	1 Secrets	1 Users	11/11/2019	✓
System Admin DoubleLock	1 Secrets	1 Users	1/31/2001	✓
Test DoubleLock	3 Secrets	1 Users	11/11/2019	✓

- Click the **Create New DoubleLock** button. If you have never created a doublelock before, you will have to create a doublelock password first:

Enter DoubleLock Password

Password \*

Enter Doublelock Password

Confirm \*

Confirm Doublelock Password

Forgot DoubleLock Password?

Cancel

Verify Password

**Important:** It is critical that you remember or securely store this password. It cannot be recovered.

Type the doublelock password in the **Password** and **Confirm** text boxes, and then click the **Verify Password** button.

Otherwise, you go directly to the Create New DoubleLock popup page because you already have a doublelock password in the system:

### Create New DoubleLock

**Name**

CancelOK

**Note:** Because it is a secondary password, your doublelock password does not have to (but can) meet the same strong requirements as regular SS passwords (as defined by your admin). Think of it as more of a PIN than a password.

**Note:** A new doublelock and doublelock password are created together. In fact, it is impossible to create a doublelock password without immediately assigning it to a doublelock. For an existing doublelock, you are assigned access to it by its creator. Upon first accessing it, you must create *your* doublelock password for it. At least one other user will already have created their password for the same doublelock—the creator plus anybody else they granted access to.

4. Type the new doublelock's name in the **Name** text box.
5. Click the **OK** button. The new doublelock's page appears:

Admin > DoubleLock Management > My DoubleLock

WS

### Doublelock Information

Summary information for this DoubleLock including when it was created and whether or not it is active / enabled. Once a DoubleLock is disabled any associated Secrets will be unable to be accessed.

DoubleLock Name

My DoubleLock

Edit

Date Created

11/14/2019

Enabled

Yes

Edit

Associated Secrets

0

### Assign Users [Add or Remove](#)

Defines the users that are able to access Secrets using this DoubleLock or assign this DoubleLock to other Secrets. Note that only users who have already created a DoubleLock password can be added to a DoubleLock. Users must be part of a DoubleLock group to edit the users in the group. A user can not remove themselves from the DoubleLock

Users Assigned to DoubleLock

### Secrets Associated with DoubleLock

Secrets that can only be accessed by using this DoubleLock. Note: Only Secrets to which you have access will show in this list.

No Secrets are currently using this DoubleLock.

**Important:** It is critical that you remember or securely store this password. It cannot be recovered.

6. Click the **Create Password** button. The password is created, and the DoubleLocks page reappears.

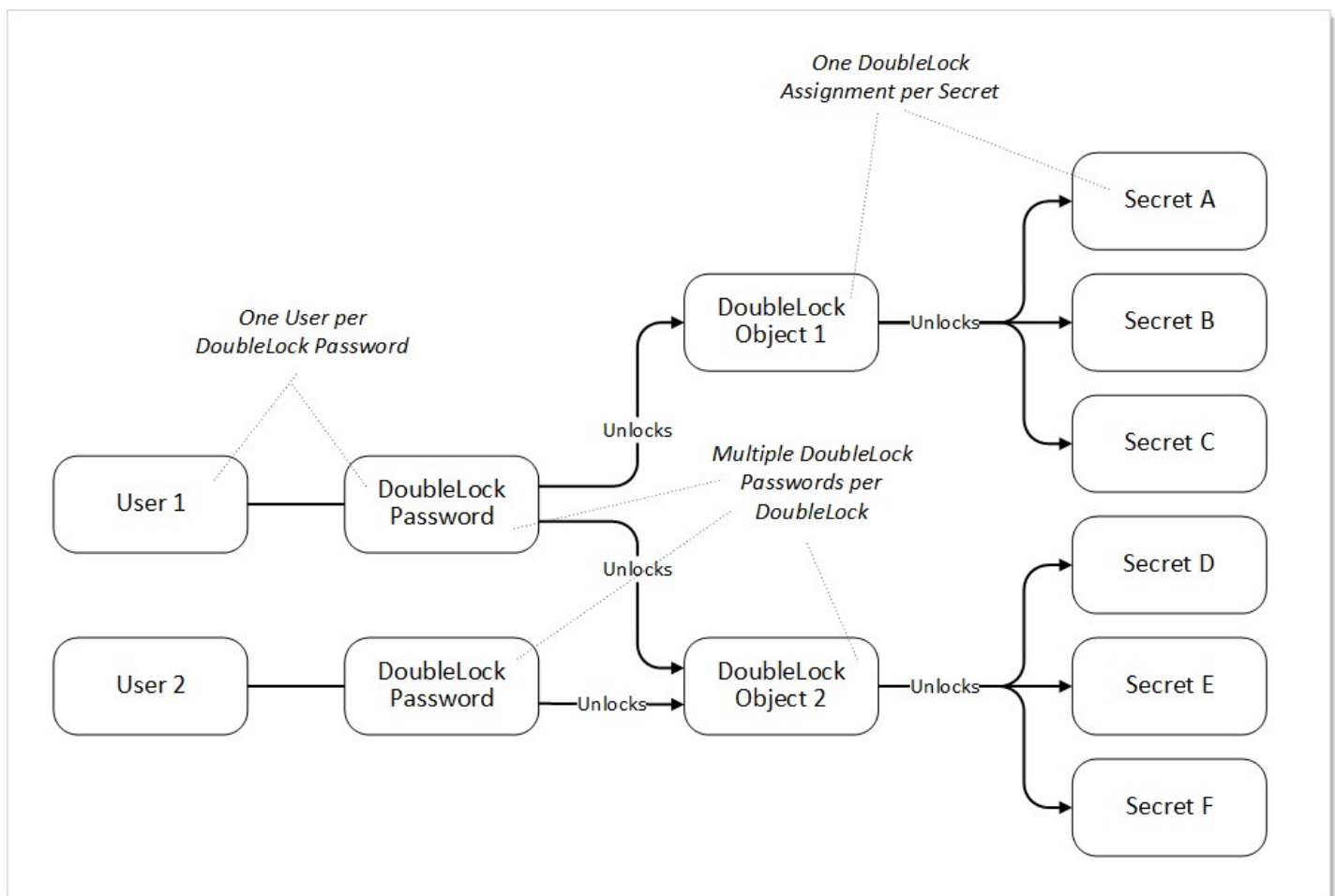
**Note:** The newly created doublelock does **not** appear on the page.

**Note:** A new doublelock and doublelock password are created at the same time. In fact, it is impossible to create a doublelock password without immediately assigning it to a doublelock. For an existing doublelock, you are assigned access to it. Upon first access, you must create a doublelock password if you do not already have one.

The doublelock system is a group of interrelated objects (see the following diagram):

- **Doublelock object:** A named object that is associated with one or more secrets and one or more users (via password objects). Doublelock objects, or simply *doublelocks*, point to secrets (what can be accessed) and doublelock password objects (who can access it).
- **Doublelock password object:** An encrypted password that is associated with one user. The same doublelock password object, or simply *doublelock password*, is used for all doublelocks to which a user has access. Once a user is assigned to a doublelock, that user has access to any secret using that doublelock, using a single password. A doublelock password has nothing to do with the user's SS access password.
- **Secret:** A secret that has a single doublelock assigned to it. Multiple secrets can have the same doublelock assigned to them.
- **User:** A SS user, which can have a single doublelock password assigned to it.

**Figure:** DoubleLock Object Relationships



Because users with access to a given doublelock each have their own separate password. Users that forget their doublelock password cannot simply ask another person using that doublelock for the password. Instead, one of the other users must reassign that forgetful user to the doublelock, and the user must choose a new password. This must occur for every doublelock the user was associated with. If no other doublelock users are available for the assignment to a given secret (there is only one associated doublelock password), the forgetful user is out of luck, and the secret will be destroyed when the user receives a new doublelock password.

When users forget their doublelock passwords, there are multiple steps and considerations. Data loss may or may not result from resetting:

1. When you forget your doublelock password, you typically come to that realization when attempting to access a secret protected by that doublelock:

DoubleLock - Mudfin Gmail

Please enter your DoubleLock password to gain access to the requested resource.


Password \*

[Forgot DoubleLock Password?](#)

Cancel Continue

2. Click the **Forgot DoubleLock Password?** link. The Reset DoubleLock Password page appears:


Reset DoubleLock Password



Resetting your forgotten DoubleLock password is irreversible and could result in permanent loss of the data. In the case you are the only user with access to the DoubleLocked Secrets, the data will be lost and the Secrets deleted. If another user has access to the Secret, they will need to re-assign you to the DoubleLock. Please review the DoubleLocks and Secrets that will be impacted on reset.

DOUBLELOCKS

Will



No one will have access to these Secret(s). The data will be permanently lost and Secrets deleted.

NAME	TEMPLATE	FOLDER	CREATED
Mudfin Gmail	Web Password	Will	2019. 05. 07.

Please enter your login password to confirm the DoubleLock reset, and acknowledge the Secrets will be lost.

Login Password \*

✓ Reset DoubleLock Password ✕ Cancel

3. At this stage, there are two possibilities:
  - You are the only one with access to the doublelocked secret: When you reset the doublelock password, the secret and its data is deleted. **This is permanent.**
  - Others have access to the secret via that doublelock: You can reset the doublelock, and you lose access to the secret, but it is not deleted. You must ask one of those others to re-assign you to the doublelock after you reset it.
4. Type your main SS password in the **Login Password** text box.

5. Click the **Reset DoubleLock Password** button. The password is reset, and if you are the only one with access to it, the secret is deleted.
6. (Optional) Ask one of the others with the doublelock password to re-assign you to the doublelock.

As an admin, to use doublelocks on a secret, you must first create complete these steps for a new doublelock:

1. One time: Create a doublelock password (one time per user). This is automatically required of you when you create a doublelock or access a secret with an existing one (that somebody else assigned to you). You can also create one manually ahead of time.
2. One time: Create a doublelock, which can be used on multiple secrets by multiple users.
3. One or more times: Assign the doublelock to a secret or secret template.
4. One time per user: Assign the user to that doublelock. Users without an existing doublelock password are required to create one.
5. Unlimited times: A user unlocks the doublelock with his doublelock password, which in turn gives the user access to the secret associated with the doublelock (every time the user wants access to the secret).

## Secret Folders

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Folders allow you to create containers of secrets based on your needs. They help organize your customers, computers, regions, and branch offices, to name a few. Folders can be nested within other folders to create sub-categories for each set of classifications. Secrets can be assigned to these folders and sub-folders. Folders allow you to customize permissions at the folder level, and all secrets within can inherit the folder's permissions. Setting permissions at the folder level ensures future secrets placed in that folder have the same permissions, simplifying management across users and groups.

**Note:** You can "favorite" a folder in the main menu by right clicking it.

If the new folder is a subfolder, you can have it use the sharing settings of its parent folder by enabling the Inherit Permissions from Parent setting for the folder.

Folders can apply one the following permissions to users or groups in the folder's Permissions table:

- **View:** Allows the user to see the folder and secrets in that folder that are inheriting permissions from their folder.
- **Edit:** Allows the user to create new folders in that folder, which forces the "Inherit Permissions from Parent" permission on the new folder, move secrets into that folder, and add new secrets into that folder.
- **Add Secret:** Allows the user to add a secret in that folder. Does not grant access to the added secret.
- **Owner:** Allows the user to create new folders in that folder without forcing inheritance, move the folder, delete the folder, rename the folder, and change the permissions and inheritance settings on the folder.

Depending on your configuration, these settings could affect the permissions of subfolders and secrets contained in this folder. Folders are not visible to users that do not have at least View permission. This allows users to create and manage their own folders without making them visible to all users.

## Personal Folders

In SS, a *personal folder* is a folder that one (and only one) individual has owner access to. No user can modify sharing permissions on these folders. A user cannot add subfolders to their personal folder. The purpose of this folder is to allow a user to securely store work-related secrets that other users do not require access to. Note that when in break-the-glass mode, an unlimited admin can access a user's personal folder in order to recover secrets if needed.

## Required Role Permissions for Managing Folders

Folder management is subject to these role permissions:

- The Administer Folders role permission allows a user to create new folders and manage folders, but specific folder permissions still apply.
- Any user with the Administer Folders role permission can create new folders; however, to create folders at the root level, the user also needs the Create Root Folders permission. They also can add new folders to any folders where they have Edit or Owner permission on that folder.
- They must have Owner permission to delete a folder.
- Users can also move folders where they have Owner permission on the source folder and Edit or Owner permission on the target folder (where they are moving it). The folder automatically inherits Permissions from its parent when it is moved, which is the same as when secrets are moved.

To setup this feature, navigate to **Administration > Folder Synchronization**. To edit the settings, you must have a role assignment with Administer ConnectWise Integration permissions.

Enabling folder synchronization requires specifying the synchronization interval in days, hours, and minutes. The "Folder to Synchronize" is the parent folder where you create the folder structure. There are two methods of Folder Synchronization, through the ConnectWise API or through a database view.

## Synchronizing with the ConnectWise API

The ConnectWise API is the recommended way to sync folders from ConnectWise. To sync:

1. Select ConnectWise API from the Folder Synchronization Method list.
2. Enter your ConnectWise site name.
3. Select a ConnectWise Integrator Secret for API Access.

### Folder Synchronization Configuration Edit

[Explain](#)

**Folder Synchronization Method**

ConnectWise API

**Synchronization Interval for Folder**

Days

0

Hours

0

Minutes

30

**Folder to Synchronize**

\Clients

Clear

**Site URL**

\* staging.connectwisedev.com

**Company ID**

\* acmeinc

**Integrator Credentials**

ConnectWise (secretserver001)
[Create New Secret](#)

**Folder Structure**

\$TYPE\STATUS

Save

Cancel

Test Connection

**Note:** The Integrator account must have access to the Company API in ConnectWise and access to all records

**ConnectWise** + Recent Chat with Support

Setup Tables > Integrator Login List > Integrator Login

**Integrator Login**

Setup Logs

Updated: 7/12/2016 2:06:55 PM by Admin1

Username: secretserver001

Password: ••••••••

Access Level: All records

**Enable Available API(s)**

- ☐ Service Ticket API
  - Service Board: [dropdown]
  - Callback URL: [text box]
  - ☐ Use legacy callback format
- ☐ Time Entry API
  - Member: [text box]
  - Callback URL: [text box]
  - ☐ Use legacy callback format
- ☐ Managed Services API
  - ☐ Enable automatic childing of Configurations (more info)
  - ☐ Allow for Configurations to be childed by the Integrator
- ☐ Contact API
  - Callback URL: [text box]
  - ☐ Use legacy callback format
- ☒ Company API
  - Callback URL: [text box]
  - ☐ Use legacy callback format

Folder structure defines how folders are named under the client's folder. By default, \$TYPE\$STATUS creates sub-folders based on the customer type in ConnectWise, then further sorted by the active status in ConnectWise. For example, the active prospect "Acme Inc" in ConnectWise would get the following folder created: Clients\Prospects\Active\Acme Inc

The supported folder structure tokens are:

- **\$COMPANYINITIAL:** First letter of company name. Use to organize companies into subfolders of A, B, C, and the like.
- **\$STATUS:** Company status, such as active, inactive, or not-approved.
- **\$TYPE:** Company type, such as competition, customer, partner, prospect, suspect, or vendor.

When configured, save and scroll down to the bottom and click **Synchronize Now** to run the synchronization

**Note:** See the [How to create a custom view for ConnectWise synchronization](#) KB article for more advanced technical information on setting up the SQL View.

## Synchronizing with a Database (Advanced)

The database synchronization method queries an on-premises database for a custom view and parse company information out of it.

Enter the SQL Server location, SQL database name, and the credential information for accessing the reference database, for example, to your ConnectWise instance. The SQL view defaults to a standard ConnectWise customer layout but can be customized to meet the desired folder Layout.

### Folder Synchronization Configuration Edit

[Explain](#)

Folder Synchronization Method

Database (Advanced) ▾

Synchronization Interval for Folder

Days

0


Hours

0

Minutes

30

Folder to Synchronize

 [No Selected Folder](#)

SQL Server Location

!

SQL Database Name

!

SQL Username

!

SQL Password

!




SQL View

☒ ConnectWise
 ☐ Custom View

[Advanced \(not required\)](#)

Days to Keep Operational Logs

30

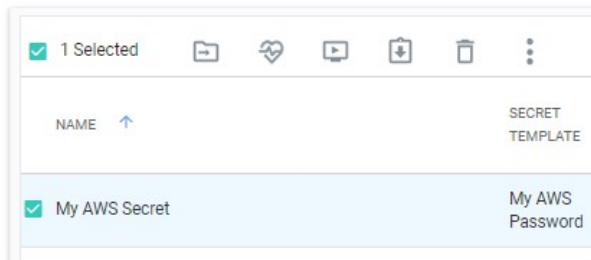
 Save
  Cancel
  Test Connection

"Days to Keep Operational Logs" sets the period to keep folder-synchronization-related logs that might contain PII. SS automatically deletes logs older than that (in days).

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Adding and Moving Secrets Between Folders

1. Consider the following before moving a secret between folders:
  - To add or move a secret to a folder, you must have Edit permission on that folder (either direct or through inheritance).
  - To move a secret from a folder, you must have Edit permission on that secret. If the secret has the "Inherit Permissions from folder" setting enabled, then you must have Owner permission to move that secret to a new folder.
  - When a secret is moved to a folder, it automatically gets the "Inherit Permissions from folder" setting even if it had specific permissions before the move.
2. Navigate to the folder containing the secret or secrets you want to move.
3. For each secret:
  1. Hover the mouse pointer over the secret. A check box appears on the left end.
  2. Click to select the check box. A command row of icons appears:

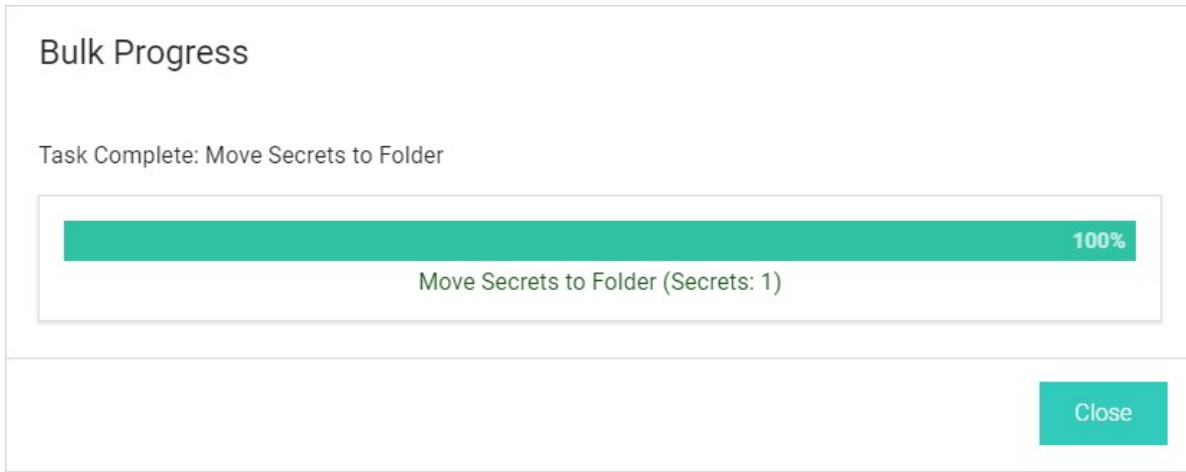


3. Click the Move to Folder icon. The move Secrets pop-up page appears:



4. Navigate to and select the target folder for the secret or secrets.

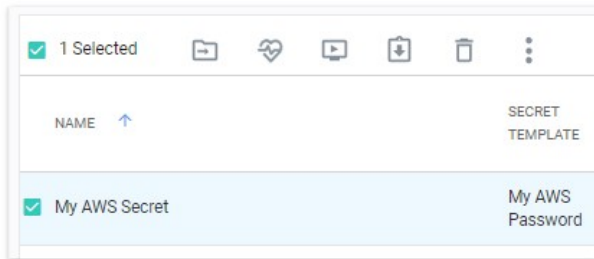
5. Click the **Move Secrets** button. The Bulk Progress popup appears:



1. The secret moves to the selected folder.

## Assigning Secret Policies to Folders

1. Navigate to the folder containing the secret you want to assign a policy to.
2. Hover the mouse pointer over the secret. A check box appears on the left end.
3. Click to select the check box. A command row of icons appears:



4. Click the Assign Secret Policy  icon. The Assign Secret Policy pop-up page appears:

### Assign Secret Policy

Secrets Selected: 1

Select the Secret Policy option to assign

Inherit Secret Policy

No

Secret Policy

None Selected

Cancel


Confirm Action

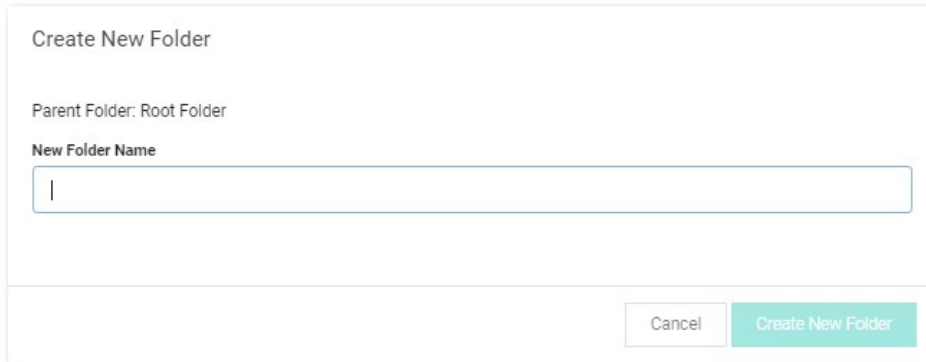
5. Click the **Confirm Action** button.

## Creating Folders

To create a folder:

**Note:** To create folders, you must have a role with the Administer Folder permission. You also must have Edit or Owner permission for the parent folder.

1. Click the parent folder for the new folder in the folder tree in the main menu. If you do not select one, the root is assumed.
2. Click the  icon and select **New Folder**. The Create New Folder pop-up page appears:

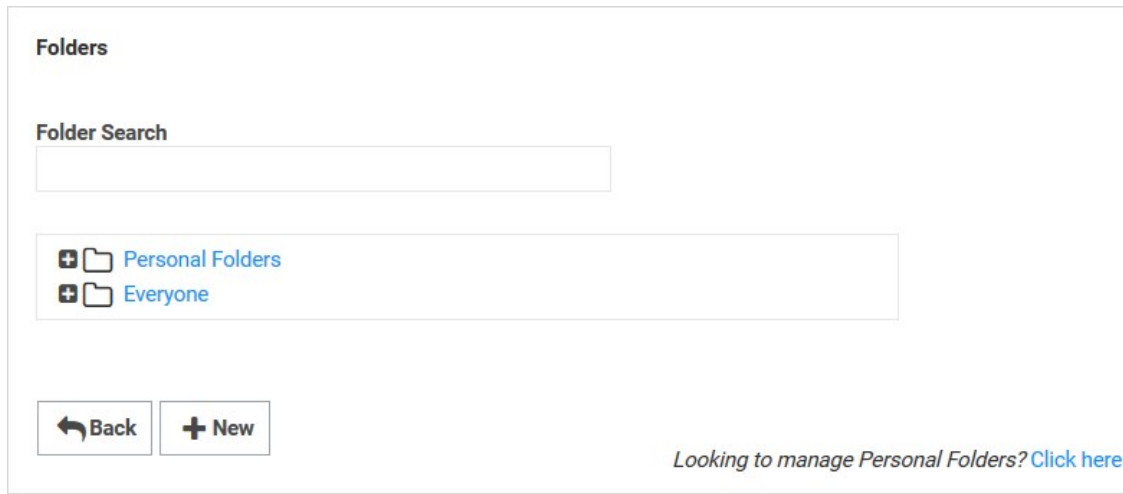


The image shows a 'Create New Folder' pop-up dialog box. It has a title bar 'Create New Folder'. Below the title bar, it says 'Parent Folder: Root Folder'. Then there is a label 'New Folder Name' followed by a text input field with a cursor. At the bottom right, there are two buttons: 'Cancel' and 'Create New Folder'.

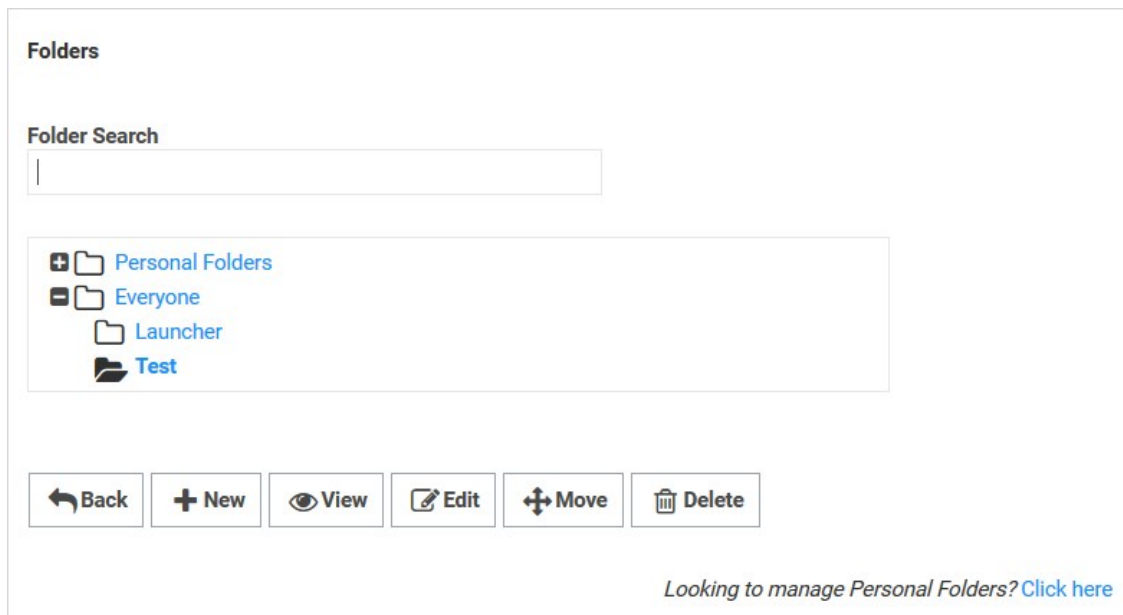
3. Type the folder name in the **New Folder Name** text box.
4. Click the **Create New Folder** button. The new folder appears in the folder tree under its parent folder.
5. Proceed to [Editing Folder Permissions](#) to customize permissions for the new folder.

## Editing Folder Permissions

1. Click **Admin** > **Folders**. The Folders page appears:



2. Navigate to or search for the desired folder.
3. Click the folder's name. The folder is bolded, which indicates it is selected, as does the appearance of several new buttons:



4. Click the **Edit** button. The unlabeled folder details and permissions page appears:

[Overview](#)
[Audit](#)

### Folder Details

Sets basic folder information including the name, folder path, secret type (template), and policies for secrets in the folder. These settings may prevent adding some secrets to the folder.

<b>Folder Name</b>	Test	<a href="#">Edit</a>
<b>Secret Policy</b>	Inherit Secret Policy - No Secret Policy	<a href="#">Edit</a>
<b>Allowable Templates</b>	All Templates	

### Folder Permissions [Edit](#)

Sets who may access the folder. This is determined by folder inheritance, as well as user and group permissions.

**Inherit Permissions** Yes

**Selected Groups**

User or Group	Folder Permission	Secret Permission
Everyone	Owner	Owner

5. To edit the folder name, click the **Edit** link next to **Folder Name**.

6. To edit the policy that is inherited by secrets in the folder:

1. Click the **Edit** link next to **Secret Policy**. The Edit Folder popup appears:

### Edit Folder

**Secret Policy**

Inherit Secret Policy - No Secret Policy

Cancel

Save

2. Click the **Secret Policy** dropdown list to select the desired policy.

3. Click the **Save** button.

7. To edit the folder permissions:

1. Click the **Edit** link next to **Folder Permissions**. The Folder Permissions section becomes editable. It is currently set to the

default, which is Inherit Permissions, so the Inherit Permissions check box is selected and the selected groups are not editable:

**Inherit Permissions** ☒

**Selected Groups**

User or Group	Folder Permission	Secret Permission
Everyone	Owner	Owner

- Click to deselect the **Inherit Permissions** checkbox. The permissions section becomes editable:

**Inherit Permissions** ☐

**Selected Groups**

User or Group	Folder Permission	Secret Permission
Everyone	Owner	Owner

[Remove](#)

**Edit**

All

- ☐ Access Control Assistance Operators
- ☐ Account Operators
- ☐ Administrators
- ☐ Allowed RODC Password Replication Group
- ☐ Backup Operators

- In the **Selected Groups** section, click the **Folder Permission** dropdown list for the desired user of group to select the desired maximum permission available to them for the folder: View (folder), Add Secret (to folder), Edit (folder), or Owner (of folder).
- In the **Selected Groups** section, click the **Secret Permission** dropdown list for the desired user of group to select the desired maximum permission available to them for secrets in the folder: List (secrets in folder), View (secrets in folder), Edit (secrets in folder), or Owner (of secrets in folder).
- If you wish to add a user or group (to set their permissions):
  - (optional) Click to select the dropdown list in the **Edit** section to filter the available list.
  - (optional) Type a desired user or group name in the **Search** text box.
  - Click the desired user or group in the **Edit** list that you want to add to the **Selected Groups** list. The user or group appears in the section.

6. To delete an entry in the **Selected Groups** section, click the **Remove** link next to the entry.

**Note:** It is possible to setup an automatically replicated folder structure from an external database, such as ConnectWise or other CRM systems. This topic is discussed later in [Folder Synchronization](#).

## Enabling Personal Folders

To use personal folders, you must first enable them:

1. Click **Admin > Configuration**.
2. Click the **Folders** tab:

**Configuration**

[General](#)
[Login](#)
[SAML](#)
[Folders](#)
[Local User Passwords](#)
[Security](#)
[Ticket System](#)
[Email](#)
[Session Recording](#)

Require View Permission on Specific Folder for Visibility	Yes
Enable Personal Folders	Yes
Personal Folder name	Personal Folders
Show user warning message	Yes
Warning message text	This folder is for work related Secrets only. Do not store personal non-work Secrets, such as your Online Banking password, in this folder.

← Back
✎ Edit

3. Click the **Edit** button:

**Configuration**

[General](#)
[Login](#)
[SAML](#)
[Folders](#)
[Local User Passwords](#)
[Security](#)
[Ticket System](#)
[Email](#)
[Session Recording](#)

Require View Permission on Specific Folder for Visibility	<input checked="" type="checkbox"/>
Enable Personal Folders	<input checked="" type="checkbox"/>
Personal Folder name	<input type="text" value="Personal Folders"/>
Show user warning message	<input checked="" type="checkbox"/>
Warning message text	<div> This folder is for work related Secrets only. Do not store personal non-work Secrets, such as your Online Banking password, in this folder. </div>

💾 Save
✕ Cancel

4. Click to select the **Enable Personal Folders** check box.
5. (Optional) Type a new folder name in the **Personal Folder name** text box to customize the root-level folder that contains all personal folders.
6. (Optional) If you want to display a warning message to users when placing secrets in their personal folders:
  1. Click to select the **Show user warning message** check box.
  2. (Optional) Edit the **Warning message text** box.
7. Click the **Save** button. A personal folder for each user is now created in a root-level folder with the personal folder name specified.

**Note:** When personal folders are enabled, a user requires the Personal Folders role permission in their role to be able to view and use their own personal folder.

## Modifying Folders with Secret Policies

You can configure secret policies to apply RPC and security settings to an entire folder of secrets.

To create a new secret policy:

1. Click **Admin > Secret Policy**. A Secret Policy page appears:

### Secret Policy

[Explain](#)

< 1 to 9 of 9 >

SECRET POLICY NAME	DESCRIPTION	ACTIVE
Checkout_Enforced		Yes
Enforced_Autochange		Yes
Privilage account		Yes
Secret_Policy_test_folder		Yes
site_Enforced		Yes
Skipped policy		Yes
Test_Policy		Yes
TestWK		Yes
Wkflow		Yes

☐ Show Inactive

← Back
+ Create New

2. Click the **Create New** button. The (new) Secret Policy page appears:

## Secret Policy

[Explain](#)

**Secret Policy Name**  \*

**Description**

**Active** ☒

SECTION	SECRET POLICY ITEM NAME	SETTING	VALUE
General	Site	< Not Set > ▼	
Remote Password Changing	Auto Change	< Not Set > ▼	

- Type a name for the new secret policy in the **Secret Policy Name** text box.
- Click the Setting dropdown list, and choose the policy's settings for each relevant section. Aside from < Not Set >, which means that the setting is not applied, there are two options:
  - Default:** The policy is applied to all secrets in the folder initially, but it **is** possible to manually change the applied secret settings as well.
  - Enforced:** The policy is applied to all secrets in the folder initially, and it **is not** possible to change those applied settings on secrets in that folder.
- Click to select the **Value** check box in that row to apply the setting. Applying the setting may enable configuration of related settings in the grid. For example, enabling Auto Change causes the Auto Change Schedule to be available for configuration:

## Secret Policy

[Explain](#)

**Secret Policy Name**  \*

**Description**

**Active** ☒

SECTION	SECRET POLICY ITEM NAME	SETTING	VALUE
General	Site	< Not Set > ▼	
Remote Password Changing	Auto Change	Enforced ▼	<input checked="" type="checkbox"/>

- Click the **Save** button to make the policy available for assignment to folders.

**Note:** To deactivate a policy that you no longer want, edit the policy and deselect the **Active** check box. For information about applying a secret policy to a folder, see [Editing Folder Permissions](#).

## Moving Folders

There are two ways to move folders. The **easiest way is to drag a folder** over another and drop it. The other way is as follows:

1. Ensure that you have edit permission for both the source and destination folders.
2. Right click the folder in the navigation pane and select **Move Folder**. The Move Folder page appears:

1568051612480

3. Navigate to and select the destination folder in the folder tree.
4. Click the **Confirm Move** button.

## Secret Heartbeats

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS's *heartbeat* feature allows secrets to have their entered credentials automatically tested for accuracy at a given interval. Using heartbeat on secrets ensures those credentials are up-to-date and can alert administrators if the credentials are changed outside of SS. Heartbeat helps manage secrets and prevent them from being out of sync.

On the **Preferences** page, the **Send Email Alerts when Heartbeat Fails for Secrets** setting can be enabled to email the user when heartbeat fails for any secret the user has view access to.

Heartbeat is configured from the secret template designer. The heartbeat interval determines how often the secret credentials are tested.

To enable heartbeat, ensure it is enabled on the **Remote Password Changing Configuration** page:

1. Navigate to **Admin > Remote Password Changing**.
2. Click the **Edit** button.
3. Click to select the **Enable Heartbeat** check box.
4. Click the **Save** button.

**Note:** Heartbeat must also be enabled on the secret template by setting the **Enable Remote Password Changing Heartbeat** setting.

The heartbeat logs for a specific secret can be accessed by clicking the **View Audit** button on the **Secret View** page and clicking to enable the **Display Password Changing Log** check box. The heartbeat logs for all secrets can be accessed by navigating to **Administration > Remote Password Changing** and scrolling down to the second set of logs.

- **Success:** The credentials in the secret authenticated successfully with the target system.
- **Failed:** The credentials in the secret failed authentication with the target system.
- **UnableToConnect:** SS was unable to contact the target system. Ensure that the domain, IP address, or hostname is correct and resolvable from the server that SS is installed on.
- **IncompatibleHost:** The most common reason for this code is an attempt to verify an account on the same server that SS is installed on. If this is not the case, ensure that the domain, IP address, or hostname is correct and resolvable from the server that SS is installed on.
- **UnknownError:** Check the Heartbeat log on the Remote Password Changing page for details, and contact [Support](#) for assistance

For the most up-to-date list of account types supported by RPC, see [this KB article](#).

Heartbeat runs in a background thread to check each secret where it is enabled. If the credential test fails, the secret is flagged as heartbeat failed and out of sync. To avoid locking out the account, heartbeat no longer runs on that secret until the secret items are edited by the user. If the machine is determined to be unavailable, the secret is flagged as heartbeat unable to connect and the secret continues to be checked on the heartbeat interval.

To manually use heartbeat to check the credentials, the **Secret View** page has a **Heartbeat Now** button. The button marks the password as heartbeat pending. The background thread processes the secret in the next 10 seconds, and when the page is refreshed the heartbeat status is updated.

**Note:** Heartbeat does not work on Windows accounts on the server that is running SS. These accounts are flagged with an "Incompatible Host" status.

To run heartbeat for a secret:

1. From **Dashboard**, click the secret you would like to test.
2. Click the **View** button. The **Last Heartbeat** field of the secret shows the last date and time that Heartbeat ran for this secret.
3. To run Heartbeat once more, click **Run Heartbeat** at the bottom of the Secret.
4. Monitor the **Last Heartbeat** field to see the updated status. This may take a few seconds to complete.

If you receive any Heartbeat status code aside from Success, you can check the Heartbeat log for details. To view the entry, Go to **Admin > Remote Password Changing** and then search for the secret name in the **Search** field of the **Heartbeat Log**.

## Secret Import and Export

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

You can export your data as XML by going to **Admin > All** and typing `export` in the search text box. Once on the Export page, click to select **XML** on the **Export Format** selection button.

You can import your data to another SS server as XML by going to **Admin > All** and typing `import secrets` in the search text box. Once on the Choose Secret Template page, click the **Upload XML File** link in the **Additional Options** section.

**Important:** Do not edit the XML file with Windows Notepad. Instead, use Notepad++, Visual Studio Code, or Atom to make your edits. Windows Notepad can add invisible characters that can prevent importation.

XML export includes:

- Folders (and their permissions)
- Secret templates
- Secrets (and their permissions)

The XML export does **not** include users, groups, launchers, configuration, and others.

**Note:** Folders and secret templates are only exportable from SS 10.0 and later.

**To ensure permissions are applied correctly, you must recreate your users and groups on the target SS before importing.**

The following secret template settings **are** transferred with the XML export or import:

- Edit Requires
- Field slug Names
- Hide on View
- Is Required?
- Keep Secret Name History
- One-time password settings
- Secret template icons
- Type descriptions
- Validate password requirements on create or edit

The following secret template settings are **not** transferred:

- Associated secrets
- Launcher settings
- Password changing settings
- Session recording enabled

**Note:** You *can* use this XML import and export to transfer between on-premises and cloud editions.

If you use XML to migrate from SS on-premises to cloud, the major release version (x.x) must be the same. Otherwise, you need to upgrade before you can migrate. Additionally, the **Allow Duplicate Secret Names** check box on the **General** tab of the **Admin Configuration** page should be disabled in Secret Server Cloud before importing.

From within the **Administration > Export** page, select the folder that needs to be exported. By default, all secrets are exported if a folder is not selected. If no folder is selected, all secrets are exported by default. The administrative password must be entered, as it is a security measure to verify the permission of the user performing the export.

**Note:** Only the secrets the user has view access to are exported.

Exports can be configured further with options to "Export with Folder Path" and "Export Child Folders." Export with Folder Path adds the full folder path to the export. Folder paths in the export file provide organizational structure if secrets need to be imported later.

By default, the option to "Export Child Folders" is active. While this option is enabled, any export of a specified folder also exports content located in folders beneath the initial selection.

Secrets are exported as a comma-separated-value (CSV) file or as XML. The CSV file can be easily handled in Excel or other spreadsheet applications. The file is grouped by secret template and each cluster of secrets has a header row that contains the template text-entry field names followed by all exported secrets based on that template.

The XML file follows the exact structure of the advanced xml import. As such, this can be useful with migrating data from one SS installation to another.

Secrets are exported in the exact structure as a secret Import. If exports are maintained, an installation of SS can be completely reproduced on a separate instance by applying the exported file.

Secret template settings for importation and exportation include:

- Is Required?
- Edit Requires
- Hide on View
- Secret template icon
- Keep Secret Name History
- Validate Password Requirements on Create/Edit
- Field Slug Name
- Type Description
- One Time Password settings

The secret template settings that do **not** transfer include:

- Launcher settings
- Password changing settings
- Session recording enabled
- Associated secrets

See the [Can I import/export data between Secret Servers?](#) (KB) for more information.

SS's importation feature simplifies integration with legacy systems and allows users to easily add large numbers of secrets from an Excel or comma-separated values (CSV) file. Secrets are batch imported by template, so multiple types of input data need to be imported in several batches. The Password Migration Tool supports easy addition of existing secrets from other third-party password-storing applications.

## Configuring Data for Importation

1. Click the  button on the Dashboard and select **Import Secrets**. The Choose Secret Template page appears:

### Choose Secret Template

What type of Secret do you want to import?

< Select >
▼
\*


↶ Back
↷ Continue

### Additional Options

[Download the Secret Server Migration Tool.](#)  
[Upload XML File](#) for an advanced import to add Folders, Secret Templates, and Secrets.

2. Click the **What type of Secret...** list box to select the type of secrets you intend to import.
3. Click the **Continue** button. The Import Secrets page appears:

### Import Secrets



Paste your Secrets directly from Microsoft Excel® or in comma/tab separated format and click 'Next'.  
 Do not include a header line.  
 Secret Name must be included but others fields can be blank.  
 Fields containing commas or tabs must be surrounded with double quotes.  
 It is permissible to include quotes if they are escaped with a \ (for example, pa\"word comes out as pa"word)  
 Fields must be in the following order:  
**Secret Name,AccessKey,SecretKey,Username,SecretId,Trigger**

↶ Back
↷ Next


☐ Allow Duplicate Secrets
 ☐ Import With Folder

4. Paste the secrets for importation from MS Excel or a CSV file directly into the text box in the **Import Secrets** page. The order of the

imported fields is based on the template selected. Consider the following:

- Do not include a header line. The field names are determined by the order, not a header line.
  - The fields **must** be in this order: Secret Name, AccessKey, SecretKey, Username, SecretId, and Trigger.
  - Secret names must be included, but other text-entry fields can be blank unless the secret template indicates that the text-entry field is required
  - Fields containing commas or tabs must be surrounded with double quotation marks
  - If you have to include double quotation marks inside your data, escape all of them with a \ character so the importer does not get confused.
- Click to select the **Allow Duplicate Secrets** check box if you wish to import a secret with the same name as an existing one.
  - Click to select the **Import with Folder** check box if you included an additional field in the importation text with a fully qualified folder name for the secret to be created in.
  - Click the **Next** button. SS displays a preview:


### Import Secrets




Paste your Secrets directly from Microsoft Excel® or in comma/tab separated format and click 'Next'.  
Do not include a header line.  
Secret Name must be included but others fields can be blank.  
Fields containing commas or tabs must be surrounded with double quotes.  
It is permissible to include quotes if they are escaped with a \ (for example, pa\"word comes out as pa"word)  
Fields must be in the following order:

**Secret Name,AccessKey,SecretKey,Username,SecretId,Trigger**

Mister Secret, sdklfjsd, sdklfjsdlk, Will, MyID1

 No, Let me change them

 Yes, Import these Secrets

☐ Allow Duplicate Secrets
☐ Import With Folder

SECRETNAME	ACCESSKEY	SECRETKEY	USERNAME	SECRETID	TRIGGER	ERROR
Mister Secret	sdklfjsd	sdklfjsdlk	Will	MyID1		

- If you are happy with what you see, click the **Yes, Import these Secrets** button.

## Importing Secrets with the Secret-Server Migration Tool

SS offers a migration utility for users wishing to import secrets from other applications. Currently, the migration tool supports to following applications:

- KeePass
- Password Corral

- Password Safe

**Note:** This is done with another exportation tool that creates a single XML file. Please contact Thycotic Support for details.

## Importing Secrets with Advanced XML Importation

Advanced importation adds folders, secret templates, and secrets based on an XML file. Permissions can be specified on the folders and secrets or the default is to inherit permissions. This import can only be done by administrators with proper role permissions.

**Note:** For details on the XML file, see [Advanced Import with XML](#).

The XML file should look like the example below, the comments are for explanation reasons only and may be removed before importing, if desired.

**Important:** Migration is **not** supported by Thycotic Technical Support.

## Notes

- Leaving the <Permissions> tag empty for a folder will cause that folder to inherit permissions from its parent folder.
- Leaving the <Permissions> tag empty for a secret will cause it to inherit permissions from its folder.
- To add a line-break within a Notes field use ##BR##.

**Note:** Please do **not** edit the XML file with Windows Notepad. Use Notepad++, Visual Studio Code, or Atom to make your edits. Using Notepad increases you chances of importation failure.

## Sample XML

```
<?xml version="1.0" encoding="utf-16"?>

<ImportFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" (http://www.w3.org/2001/XMLSchema-instance)
xmlns:xsd="http://www.w3.org/2001/XMLSchema"%3E;

  <Folders>
    <Folder>
      <FolderName>Customers</FolderName>
      <FolderPath>Customers</FolderPath>
      <Permissions>
        <Permission>
          <View>true</View>
          <Edit>true</Edit>
          <Owner>true</Owner>
          <UserName>admin</UserName>
        </Permission>
      </Permissions>
    </Folder>
    <!-- Either UserName or GroupName is required in permissions -->
    <Folder>
      <FolderName>Customer A</FolderName>
      <FolderPath>Customers\Customer A</FolderPath>
      <Permissions />
    </Folder>
    <!-- Empty Permissions will cause folder to inherit from parent -->
    <Folder>
      <FolderName>Customer A</FolderName>
      <FolderPath>Customers\Customer A</FolderPath>
      <Permissions />
    </Folder>
    <!-- Groups are optional -->
    <Groups>
      <Group>
        <GroupName>Other Administrators</GroupName>
        <GroupMembers>
          <GroupMember>
            <UserName>admin2</UserName>
          </GroupMember>
          <GroupMember>
            <UserName>DomainAdmin</UserName>
            <Domain>http://testdomain.test.com</Domain>
          </GroupMember>
        </GroupMembers>
      </Group>
      <Group>
        <GroupName>Domain Administrators</GroupName>
        <Domain>http://testdomain.test.com</Domain>
        <GroupMembers>
          <GroupMember>

```

```

    <UserName>DomainAdmin</UserName>
    <Domain>http://testdomain.test.com</Domain>
  </GroupMember>
</GroupMembers>
</Group>
</Groups>
<SecretTemplates>
<!-- You can have multiple secrettype entries -->
  <secrettype>
    <name>Windows Account</name>
    <active>true</active>
    <fields>
      <field isexpirationfield="false">
        <name>Resource URL</name>
        <mustencrypt>false</mustencrypt>
        <isurl>false</isurl>
        <ispassword>false</ispassword>
        <isnotes>false</isnotes>
        <isfile>false</isfile>
        <passwordlength>0</passwordlength>
        <historylength>0</historylength>
        <isindexable>false</isindexable>
      </field>
      <field isexpirationfield="false">
        <name>Username</name>
        <mustencrypt>false</mustencrypt>
        <isurl>false</isurl>
        <ispassword>false</ispassword>
        <isnotes>false</isnotes>
        <isfile>false</isfile>
        <passwordlength>0</passwordlength>
        <historylength>0</historylength>
        <isindexable>false</isindexable>
      </field>
      <field isexpirationfield="false">
        <name>Password</name>
        <mustencrypt>true</mustencrypt>
        <isurl>false</isurl>
        <ispassword>true</ispassword>
        <isnotes>false</isnotes>
        <isfile>false</isfile>
        <passwordlength>12</passwordlength>
      <!-- Use this number for 'All' history -->
        <historylength>2147483647</historylength>
        <isindexable>false</isindexable>
      </field>
      <field isexpirationfield="false">
        <name>Notes</name>
        <mustencrypt>false</mustencrypt>
        <isurl>false</isurl>
        <ispassword>false</ispassword>
        <isnotes>true</isnotes>
        <isfile>false</isfile>
        <passwordlength>0</passwordlength>
        <historylength>0</historylength>
        <isindexable>true</isindexable>
      </field>
    </fields>
    <expirationdays>0</expirationdays>
  </secrettype>
</SecretTemplates>
<Secrets>
  <Secret>
    <SecretName>Test Secret</SecretName>
    <SecretTemplateName>Windows Account</SecretTemplateName>
    <FolderPath>Customers\Customer A</FolderPath>
    <Permissions>
      <Permission>
        <View>true</View>
        <Edit>true</Edit>
        <Owner>false</Owner>
        <GroupName>IT Admins</GroupName>
      </Permission>
      <Permission>
        <View>true</View>
        <Edit>true</Edit>

```

```

    <Owner>true</Owner>
    <UserName>admin</UserName>
  </Permission>
</Permissions>
<SecretItems>
  <SecretItem>
    <FieldName>Resource URL</FieldName>
    <Value>10.10.0.25</Value>
  </SecretItem>
  <SecretItem>
    <FieldName>Username</FieldName>
    <Value>Administrator</Value>
  </SecretItem>
  <SecretItem>
    <FieldName>Password</FieldName>
    <Value>D*KGY#$5</Value>
  </SecretItem>
  <SecretItem>
    <FieldName>Notes</FieldName>
    <Value>Just some notes##BR##...and some more notes on a new line. </Value>
  </SecretItem>
</SecretItems>
</Secret>
<Secret>
  <SecretName>Another Test Secret</SecretName>
  <SecretTemplateName>Windows Account</SecretTemplateName>
  <FolderPath>Customers\Customer A</FolderPath>
<!-- Empty Permissions causes secret to inherit from folder -->
  <Permissions />
  <SecretItems>
    <SecretItem>
      <FieldName>Resource URL</FieldName>
      <Value>10.10.0.25</Value>
    </SecretItem>
    <SecretItem>
      <FieldName>Username</FieldName>
      <Value>JSmith</Value>
    </SecretItem>
    <SecretItem>
      <FieldName>Password</FieldName>
      <Value>DKud3()DS</Value>
    </SecretItem>
    <SecretItem>
      <FieldName>Notes</FieldName>
      <Value>This line has an empty line##BR####BR##in between this line.</Value>
    </SecretItem>
  </SecretItems>
  <SecretDependencies>
<!-- Secret dependencies are optional, and there can be multiple ones -->
    <SecretDependency>
      <Active>true</Active>
      <Restart>true</Restart>
      <Description>Some Dependency</Description>
      <MachineName>192.168.99.1</MachineName>
      <DependencyName>Some Service</DependencyName>
      <Type>Windows Service</Type>
    </SecretDependency>
  </SecretDependencies>
  <PrivilegedAccount>Some Account</PrivilegedAccount>
  <WaitBeforeSeconds>10</WaitBeforeSeconds>
</Secret>
</Secrets>
</ImportFile>

```

## Secret Launchers and Protocol Handlers

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

A secret *launcher* launches applications on end-user machines and automatically logs on using credentials stored in SS. In general, there are three types of launchers: RDP, SSH, and Custom. This provides a convenient method to open RDP and PuTTY connections, but it also circumvents users needing to know their passwords—a user can still gain access to a needed machine but it is not required to view or copy the password out of SS. A Web launcher automatically logs into websites using the client's browser.

A *protocol handler* is an application on an end-user's machine. It enables communication between SS and that client machine. It also provides the files needed by launchers. When a SS user starts a launcher:

1. The protocol handler bootstraps the client-side application.
2. The protocol handler communicates with Secret Server over HTTP(S) to ensure that it is the latest version. If not, it begins an upgrade process.
3. The protocol handler bootstraps the target launcher type and begin the process of securely logging in the user. Beyond HTTP(S) transport protection, credentials are retrieved securely from SS using signed AES-256-encrypted messages.

SS launchers, supported by protocol handlers, come in three primary types:

- **Remote Desktop:** Launches a Windows Remote Desktop session and automatically authenticates the user to the machine.
- **PuTTY:** Opens a PuTTY session and authenticates the user to a Unix system.
- **Web Password Filler:** Uses a bookmarklet or a Chrome extension to automatically log the user into a website with secret credentials.
- **Web Launcher:** An alternative method to automatically log on websites. See [Web Launchers](#).

The following instructions describe how to set up a custom launcher using SecureCRT:

## Step 1: Creating the Custom Launcher

1. Navigate to **Administration > Secret Templates**.
2. Click **Configure Launchers**. The Launcher Types page appears.
3. Click the **New** button. The Launcher page appears:

## Launcher

## GENERAL SETTINGS

Launcher Type

Process

Launches the process on the user's machine and replaces \$ parameters with values from the Secret and its associated Secret. For more information see this [KB Article](#)

Launcher Name

\*

Active



Use Additional Prompt



Launcher Image



Use Custom Image?



To prevent parameter injection in **Process Arguments** fields below, quotation marks can be inserted around custom parameters.

Example:

**\$USERNAME** becomes "**\$USERNAME**" prior to launch.

Wrap custom parameters with quotation marks



Record Multiple Windows



Record Additional Processes

## WINDOWS SETTINGS

Process Name

ex. powershell

[How do I configure process arguments?](#)

Process Arguments

ex. -user \$USERNAME -pwd \$PASSWORD -f

Run Process As Secret Credentials



Use Operating System Shell

[Advanced](#)

## MAC SETTINGS

Process Name

ex. /Applications/TextEdit.app

[How do I configure Mac process name and arguments?](#)

Process Arguments

ex. -user \$USERNAME -pwd \$PASSWORD -f



Save



Cancel

4. Click the **Launcher Type** list box and select one of the following:
  - **Process:** If you would like to use secret credentials to connect directly to the remote host.
  - **Proxied SSH Process:** If you have SSH Proxy enabled. This will prevent Secret credentials from being passed to the client by connecting to Secret Server's proxy to interact with the remote host.
5. Type the name Secure CRT Proxied Process in the **Launcher Name** text box.
6. Type the location and filename of the executable (C:\program files\acme software\clients\securecr.exe) in the **Process Name** text box in the **Windows** section. The location must be on the client machine (the machine that will run the launcher).
7. Type the following custom command-line parameters in the **Process Arguments** text box:  
`/ssh2 /AUTH keyboard-interactive /PASSWORD $PASSWORD /P $PORT /L $USERNAME $HOST`
8. Click the **Save** button. The new launcher appears:

Launcher

GENERAL SETTINGS


Launcher Name

Secure CRT Proxied Process

Active

Yes

Launcher Image



Wrap custom parameters with quotation marks

Yes

Record Multiple Windows

Yes

Record Additional Processes

< None >

WINDOWS SETTINGS

Process Name

C:\program files\acme software\clients\securecrt.exe

How do I configure process arguments?

Process Arguments

/ssh2 /AUTH keyboard-interactive /PASSWORD \$PASSWORD /P \$PORT /L \$USERNAME \$HOST

Run Process As Secret Credentials

No

Load User Profile

No

Use Operating System Shell

No

MAC SETTINGS

Process Name

How do I configure Mac process name and arguments?

Process Arguments

Back

Edit

View Audit

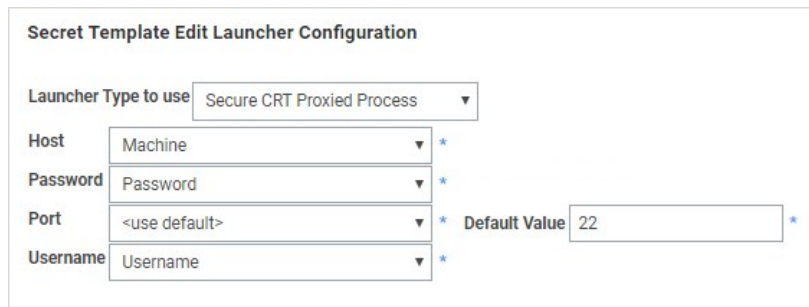
## Step 2: Creating a Custom Secret Template (optional)

See [Creating and Editing Secret Templates](#) for details on creating a custom secret template.

## Step 3: Associating the Launcher with a Secret Template

1. Navigate to **Administration > Secret Templates**.
2. Select the desired template from the drop-down menu.
3. Click **Edit**. The Secret Template Designer appears.
4. Click **Configure Launcher**. The **Secret Template Edit Launcher Configuration** page appears.

5. Click the **Add New Launcher** button.
6. For **Launcher Type to Use**, select your custom launcher.
7. Leave **Domain** set to **<blank>**.
8. For **Password** and **Username**, select **Password** and **Username**, respectively. The result should look like this:



The screenshot shows a configuration window titled "Secret Template Edit Launcher Configuration". It contains several fields for setting up a launcher:

- Launcher Type to use:** A dropdown menu with "Secure CRT Proxied Process" selected.
- Host:** A dropdown menu with "Machine" selected, marked with a red asterisk.
- Password:** A dropdown menu with "Password" selected, marked with a red asterisk.
- Port:** A dropdown menu with "<use default>" selected, marked with a red asterisk. To its right is a "Default Value" field containing the number "22", also marked with a red asterisk.
- Username:** A dropdown menu with "Username" selected, marked with a red asterisk.

9. Click the **Save** button. You can now launch SecureCRT whenever you use the launcher for secrets based off of this template.

In addition to the built in PuTTY and Remote Desktop launchers, Secret Server supports custom launchers. You can customize these process launchers to work with any application that can be started by command-line. Custom launchers pass values to the command-line from the secret text fields. For process launchers to work, the client machine needs to have the program installed and typically needs the program folder in the PATH environment variable.

**Note:** For more information on launcher arguments see [Custom Launcher Process Arguments](#).

Like the built in launchers, custom launchers run on the users machine not on the web server. Launcher Processes can be set to run either using the credentials of the logged in user or the credentials of the secret. The "Run Process as Secret Credentials" check box is used to switch between theses two options.

There are three types of custom launchers to choose from:

- **Process:** Launch a process on the client machine that connects directly to the target system from the client.
- **Proxied SSH Process:** Launch a process on the client machine that proxies its connection to the target system through SS. This applies to an SSH client other than PuTTY (which is a built-in launcher), for example, SecureCRT.

**Note:** See [Configuring SSH Proxies for Launchers](#).

- **Batch File:** Launch a batch file from the client machine that uses SS information.

## Creating Custom Launchers

**Note:** See [Custom Launcher Errors](#) if errors arise.

To create a new custom launcher:

1. Select **Secret Templates** from the **Admin** main menu item. The Manage Secret Templates page appears:

### Manage Secret Templates

Active Directory Account ▼ ☐ Show Inactive

Back

Edit

Create New

Export

View Audit

Active Templates

Password Requirements

Character Sets

Configure Launchers

Configure Secret Template Permissions

### Other Templates

Configure Dependency Templates

Configure Scan Templates

### Import Secret Templates

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

Import

2. Click the **Configure Launchers** button. The Launcher Types page appears:

Launcher Types	
LAUNCHER TYPE NAME	ACTIVE
Remote Desktop	Yes
PuTTY	Yes
Website Login	Yes
Powershell Launcher	Yes
SQL Server Launcher	Yes
Sybase isql Launcher	Yes
z/OS Launcher	Yes
IBM iSeries Launcher	Yes
<input type="checkbox"/> Show Inactive	
<div> <span>← Back</span> <span>+ New</span> </div>	

3. Click the **New** button. The Launcher page appears:

Launcher

GENERAL SETTINGS

Launcher Type

Process

*Launches the process on the user's machine and replaces \$ parameters with values from the Secret and its associated Secret. For more information see this [KB Article](#)*

Launcher Name

\*

Active

☒

Use Secret Server RDP Client


☐

Use Additional Prompt

☐

Launcher Image

☐ Use Custom Image?



WINDOWS SETTINGS

Process Name

*ex. powershell*

[How do I configure process arguments?](#)

Process Arguments

*ex. -user \$USERNAME -pwd \$PASSWORD -f*

Run Process As Secret Credentials

☐

Use Operating System Shell

☐

[Advanced](#)

MAC SETTINGS

Process Name

*ex. /Applications/TextEdit.app/Contents/MacOS/TextEdit*

[How do I configure Mac process name and arguments?](#)

Process Arguments

*ex. -user \$USERNAME -pwd \$PASSWORD -f*

Save

Cancel

The following settings are available in the General Settings section:

**Note:** Not all of the following are available for all types of launchers.

- **Launcher Type:** Select Process, Proxied SSH Process, or Batch File.
- **Launcher Name:** Name of the launcher that is displayed to the user.
- **Active:** Whether the launcher is active for use.
- **User Secret Server RDP Client:** Use the RDP client.
- **Use Additional Prompt:** User is prompted for additional information when using the launcher. When selected, the Additional Prompt Field Name text box appears.
- **Additional Prompt Field Name:** Name of the text field that is prompted for when the user uses the launcher. This value can be referenced in the process arguments with a \$ prefix.
- **Launcher Image:** Upload a custom image for the launcher.

The following settings are available in the Windows Settings section:

- **Process Name:** Name of the process that is launched. Example: powershell
- **Batch File:** As an alternative to opening a process, upload a .bat file that is downloaded and executed on the client when the user runs a launcher. The file is deleted from the client after execution.
- **Process Arguments:** Process arguments depend on the process that is being launched. View the built-in SQL Server launcher for examples on how the text-entry fields are substituted. For greater flexibility, other secrets can be linked on the Launcher tab on the secret. The text-entry field values from those secrets can also be used in the process arguments using the same prefix `$(1)[FieldName]` syntax as the SSH custom commands. There is a launcher specific token `$SESSIONKEY` that can be passed to the command line. This passes an identifier to the customer launcher that can be used to anonymously check in the secret using the `CheckInSecretByKey` Web service method. Example: `-user $USERNAME -pwd $PASSWORD -f`. See [Configuring Custom Launcher Process Arguments](#) (KB) for details.
- **Run Process as Secret Credentials:** The process authenticates with the secret credentials (username, domain, and password) instead of the current user that is using the launcher. This can be overridden at the secret level to use a privileged account to run the process.
- **Use Operating System Shell:** Use the OS shell for the launcher. Useful for processes requiring UAC confirmation.

The following settings are available in the Advanced Windows Settings section, which is accessible by clicking the **Advanced** link:

- **Escape Character:** The character to use as an escape character in passwords. Escape characters are required to allow the use of characters that are otherwise not allowed in passwords because they have special meaning to the launcher's target application.
- **Characters to Escape:** The characters that require escaping for the target application.

The following settings are available in the Mac Settings section:

- **Process Name:** Name of the process that is launched. Example: `/Applications/TextEdit.app/Contents/MacOS/TextEdit`
- **Process Arguments:** Process arguments depend on the process that is being launched. View the built-in SQL Server launcher for examples on how the text-entry fields are substituted. For greater flexibility, other secrets can be linked on the Launcher tab on the secret. The text-entry field values from those secrets can also be used in the process arguments using the same prefix `$(1)[FieldName]` syntax as the SSH custom commands. There is a launcher specific token `$SESSIONKEY` that can be passed to the command line. This passes an identifier to the customer launcher that can be used to anonymously check in the secret using the `CheckInSecretByKey` Web service method. Example: `-user $USERNAME -pwd $PASSWORD -f`. See [Custom Launcher Process Arguments](#) for details.

## Custom Launcher Errors

Common errors when creating custom launchers:

### **The process (process name) was not found**

The application has not been installed on the machine. If the application was installed, the program folder will need to be added to the path.

### **The stub received bad data (1783)**

The process is set to launch as the credentials of the secret but the username or domain is not correct on the secret or the client machine cannot find the user or domain credentials specified.

### **Error(740): The requested operation requires elevation**

When using "Run process as Secret credentials," even though the credentials have admin privileges, the process cannot be run with elevated privileges from the command prompt using runas. Instead, configure the process launcher as follows (substituting your .exe for program.exe):

- Process Name: cmd.exe
- Process Arguments: /C start /B program.exe /wait

## Custom Launcher Process Arguments

Custom launcher process arguments can use a combination of parameters from:

- A field value from the secret.
- A field value from a linked secret.
- User input obtained from a prompt prior to launching.
- \$Host and \$Port (for use with a proxied SSH process)

**Note:** For more information, see the [Dependency Token List](#).

### Syntax

Parameters are prefixed with a dollar sign \$. To obtain a value from the secret being launched, use \$FieldName. To obtain a value from a prompt, use \$PromptName. To obtain a value from a linked secret being launched, use \${n}\$FieldName (where n represents the nth linked secret). Linked secrets can be configured in the Launcher tab.

### Examples

```
-user $UserName -color ${1}$Color -Location $LocationPrompt
```

```
-ssh $UserName@$Host -pw $Password -P $Port
```

## Overview

A Common Access Card (CAC) or Personal Identity Verification (PIV) smart card is a physical card with an embedded electronic chip that uses a certificate-key pair to authenticate users. The certificate is issued by an authorized organization. The user has a PIN that should be known only to that user, which serves a second factor for two-factor authentication—access requires physical possession of the card, as well as the PIN. The user inserts the card into a card reader, which prompts for the PIN.

SS launchers can pass smart card credentials through Remote Desktop Protocol (RDP) sessions. This is useful when a user needs to authenticate through an RDP session to a resource that requires smart card authentication, for example, a secured network drive that the user attempts to open while using the RDP session.

Currently, you can enable this either globally, via user settings, or per secret:

### Enabling Globally with User Settings


1. In SS, click the user icon and select **User Preferences**. The User Preferences page appears.
2. Click the **Settings** tab.
3. In the **Launcher Settings** section, click to enable the **Allow Access to Smart Cards** toggle. The change is automatically saved.

### Enabling on a Specific Secret

1. On a Secret with an RDP launcher, click the **Settings** tab.
2. Click the **Edit** link on the **Under RDP Launcher – Personalized User Settings** title bar. The page changes to edit mode.
3. Click to select the **Allow Access to Smart Cards** check box.
4. Click the **Save** button.

## Introduction

By default, the launcher is enabled by the **Enable Launcher** setting under **Admin > Configuration**.

The launcher (protocol handler) can be deployed in two ways—with the ClickOnce (the default) or MSI-installable applications. This can also be set in the configuration settings. The latter method allows the launcher to be used in virtualized environments or any environment in which the user does not have access to a Windows Temp directory. The Protocol Handler can be downloaded by clicking the  button on the Dashboard and selecting **Launcher Tools**:

**Note:** A ClickOnce application is any Windows Presentation Foundation (.xbap), Windows Forms (.exe), console application (.exe), or Office solution (.dll) installed with ClickOnce technology in one of three ways: from a Web page, from a network file share, or from media. See [ClickOnce Security and Deployment](#) for details.

Launcher Tools

LOGIN ASSIST CHROME EXTENSION

Preferred solution for logging into websites from Chrome.

Offers similar functionality to the Web Password Filler, but for a wider range of websites.

Install the Login Assist extension by adding it to the browser from the Chrome web store:  
[Chrome Web Store - Secret Server Login Assist](#)

WEB PASSWORD FILLER

Quick, Convenient and Secure logging into Websites.

Install the Web Password Filler by adding this link to your web browser's bookmark bar:  
[Secret Server Web Password Filler](#)

- Log into most websites with a single click.
- Click while on a website.
- Automatically fill in the Username and Password.

PROTOCOL HANDLER INSTALLER


Allows launcher to function in virtualized environments. For more information [click here](#).

The MSI can be installed directly or through group policy. A reboot may be necessary on certain operating systems.

[Download Protocol Handler MSI \(64 bit\)](#)

[Download Protocol Handler MSI \(32 bit\)](#)

[Download Protocol Handler PKG \(Apple OSX\)](#)

 Back

## MSI Installer

To use the MSI installer (protocol handler installer) following steps below:

1. Go to **Admin > Configuration**.
2. Click the **General** tab.
3. Set the **Launcher Deployment Type** to "**Protocol Handler**".
4. Go to Tools > Launcher Tools to download the launcher application.
5. Click the **Download Protocol Handler MSI** link for the operating system you want to install on.
6. Run the MSI file with admin privileges.

**Note:** The session is kept in check for security reasons with the session process pinging back to SS to ensure it is still valid. This checks secret settings, such as checkout and secret access. If that check fails or the callback times out, SS errs on the side of security and kills the sessions, ensuring access is not allowed.

## Installing by Group Policy

The Protocol Handler application runs without requiring any input from the user. The installation may be pushed to your network without any special configuration. For details, see [Installing Protocol Handler through Group Policy](#) (KBA).

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Adding a Program Folder to the Windows PATH

If a launcher does not automatically add the program's folder to the Windows PATH:

1. Right click on **Computer** and go to **Properties**.
2. In the Properties window, click Advanced System Settings.
3. On the **Advanced** tab, click the **Environment Variables** button.
4. In the **System Variables** section scroll to **Path**.
5. Click **Edit** then at the very end of the text box, paste the full path to the folder where the program file is located, but make sure not to replace any existing entries. The list is semi-colon separated.
6. Click **OK** to close the dialogs.

## Common Launcher Errors

Two of the most common launcher errors:

- **The process (process name) was not found:** The application has not been installed on the machine. If the application was installed, the program folder needs to be added to the path.
- **The stub received bad data (1783):** The process is set to launch as the credentials of the secret but the username or domain is not correct on the secret or the client machine cannot find the user or domain credentials specified.

## Configuring Launchers on the Secret

Custom and SSH launchers provide additional settings on the Launcher tab of the secret for customizing authentication to the target.

- **Run Launcher using SSH Key:** If there is an SSH key set on the secret, it is used by default for authenticating to the target. Alternatively, you can specify a key from a different secret.
- **Connect As:** When an SSH secret is proxied, you can choose to connect as another user and then do an **su** to the current secret's user. This is a common practice for connecting with a lower privileged account and then switching to the root user.

## Configuring SSH Proxies for Launchers

Launchers using an SSH connection can alternatively use SS as a proxy rather than the launcher connecting directly to the target system from the machine it is being launched from. When proxying is enabled, all RD sessions are routed through SS. In SS Cloud, the Distributed Engine service also supports acting as a proxy for session launchers for greater network flexibility and offloading connections from the SS instance.

To configure this:

1. Select **Admin > SSH Proxy**:

### SSH Proxy Configuration

#### SSH PROXY SETTINGS

Enable Proxy	Yes
Enable SSH Tunneling	No
Proxy New Secrets By Default	Yes
SSH Proxy Port	22
SSH Banner	===== BE A COOL KID AND USE TERMINAL NEXT TIME =====
SSH Proxy Host Fingerprint	SHA1 - d1:0a:f6:0c:be:7c:4a:7a:7b:f1:cc:a8:b6:c2:81:5e:4e:c3:39:66 MD5 - 04:40:47:4d:51:38:72:b2:78:a9:b7:d3:34:a9:cd:ce
Enable Inactivity Timeout	No

[Advanced \(not required\)](#)

Days to Keep Operational Logs	30
-------------------------------	----

2. Scroll down and click the **Edit** button to enter your SSH proxy configuration settings. The SSH Proxy Configuration page appears:

## SSH Proxy Configuration

[Explain](#)

### SSH PROXY SETTINGS

Enable Proxy ☒

Enable SSH Tunneling ☐

Proxy New Secrets By Default ☒

SSH Proxy Port

SSH Banner

SSH Proxy Host Private Key

 Generate New SSH Key

Enable Inactivity Timeout ☐

The **SSH Proxy Settings** are:

- **Enable Proxy:** Enable or disable SSH proxying.
- **Enable SSH Tunneling:** SSH Tunneling allows Remote Desktop Sessions to be proxied using the same proxy configuration settings.
- **Proxy New secrets By Default:** This setting determines whether newly created secrets have their SSH proxy setting enabled;

secret policy takes precedence over this default.

- **SSH Proxy Port:** The default port to apply to all connections, unless another port is assigned to a specific connection.
  - **SSH Banner:** Users connecting through SS see this text banner on the SSH client.
  - **SSH Proxy Private Key:** The SS SSH private key, this can be generated using the **Generate New SSH Key** button.
  - **Enable Inactivity Timeout:** Enable or disable closing the session if there is inactivity for a defined number of seconds. When enabled, a **Timeout (seconds)** text box appears.
- **Days to Keep Operational Logs:** Sets the period to keep SSH-proxy-related logs that might contain PII. SS automatically deletes logs older than that (in days).

The **SSH Terminal Settings** are:

- **Enable Inactivity Timeout:** Enable or disable closing the SSH terminal session if there is inactivity for a defined number of seconds. When enabled, a **Timeout (seconds)** text box appears.
- **Enable Terminal:** Enable or disable the SSH terminal.
- **SSH Terminal Banner:** The text banner you want displayed when somebody opens an SSH terminal session.

**Note:** For details about connecting to SS with an SSH terminal, see the [SSH Terminal Administration Guide](#).

**Note:** To manipulate a secret via an SSH terminal, the secret's proxy setting must be enabled, and the secret must be shared with the authenticated terminal user.

1. Click the edit icon next to one of the machines in the **Nodes** section.

The **Nodes** settings are:

- **Machine Name:** The public host name of the node server.
- **SSH Public IP Address of Nodes:** The public IP that the client launcher connects to. In most cases, this can be the same as the SSH bind address; however, there may be cases where the public IP or host differs from the private IP that SS should bind to, such as NAT or an Amazon EC2 instance.

The **Sites** settings are:

- **Proxy Enabled:** Enable or disable SSH proxying for a specific site.
- **Site Name:** Site name or ID.
- **SSH Port:** The port SS listens on. The default is 22.

The **Engines** settings are:

- **Friendly Name:** Human readable site name or ID.
- **Hostname/IP Address:** The public hostname or IP that the client launcher connects to. In most cases this can be the same as the SSH Bind Address, however there may be cases where the public IP or host differs than the private IP that SS should bind to, such as NAT or an Amazon EC2 instance.
- **SSH Bind Address:** The IP Address of the network adapter that the SS SSH listener should bind to. This should not be localhost or 127.0.0.1. If you are not sure which bind IP Address to use, you may use 0.0.0.0, which binds to all IPv4 interfaces on the machine.

2. To enable secrets assigned to a site, edit the corresponding site and check the **Proxy Enabled** check box and optionally specify a custom SSH port.
3. The Distributed Engines on that site now appear in the **Engines** section, and you can configure the **Hostname/IP Address** and **SSH**

**Bind Address** text boxes on each one. The default values are the FQDN of the machine and 0.0.0.0 which should work for many internal connections but may need to be edited depending on how users are connecting to them.

**Note:** The flow for when a user proxies through a Distributed Engine, rather than SS, is the same, except that rather than the user's session launcher connecting to the public host on the node, it connects to the public host of an engine that is part of a site the secret is assigned to.

4. Once SSH Proxy has been configured, secrets using an SSH launcher have a **Show Proxy Credentials** button available. Click it to display credentials that can be used to connect through SS to the target system, that is, where a user would like to start an SSH session manually.

## Default Launcher Requirements

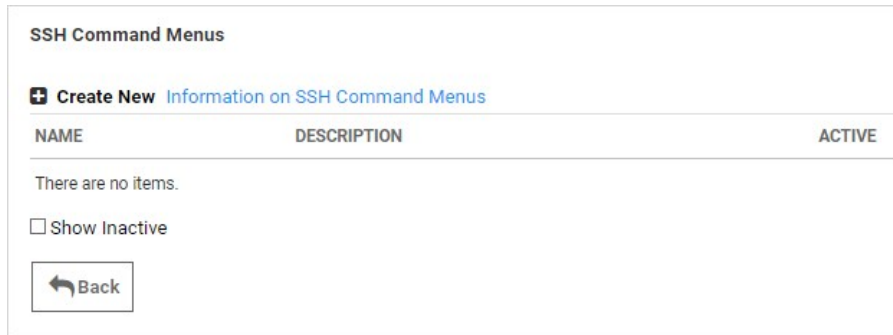
- **SQL Server Launcher:** Requires SQL Server Management Studio to be installed. When installed, the program is automatically added to the PATH.
- **PowerShell Launcher:** Requires PowerShell to be installed. When installed, the program is automatically added to the PATH.
- **Sybase iSQL Launcher:** Requires that isql.exe is installed.

## Managing Superuser Privilege

Administrators can create command menus for use with a proxied SSH connection to restrict what commands can be run by users or groups on the connected server. This feature requires an additional license. To add a command menu:

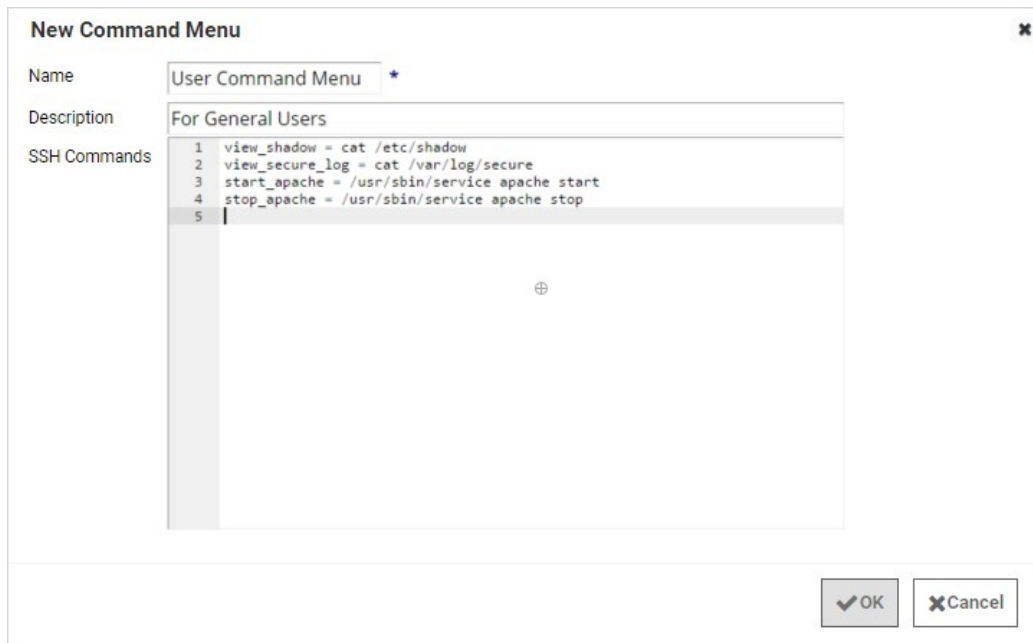
**Note:** For details, see [SSH Command Menus](#) (KB).

1. Navigate to **Admin > All**.
2. Click the **SSH Command Menus** button.



The screenshot shows the 'SSH Command Menus' page. At the top, there is a 'Create New' button and a link 'Information on SSH Command Menus'. Below this is a table with columns 'NAME', 'DESCRIPTION', and 'ACTIVE'. The table is currently empty, with the text 'There are no items.' displayed. Below the table, there is a checkbox labeled 'Show Inactive' and a 'Back' button.

3. Click the **Create New** button.
4. Type a name, description and the SSH commands:



The screenshot shows the 'New Command Menu' dialog box. It has three main input fields: 'Name', 'Description', and 'SSH Commands'. The 'Name' field contains 'User Command Menu'. The 'Description' field contains 'For General Users'. The 'SSH Commands' field contains a list of commands: '1 view\_shadow = cat /etc/shadow', '2 view\_secure\_log = cat /var/log/secure', '3 start\_apache = /usr/sbin/service apache start', '4 stop\_apache = /usr/sbin/service apache stop', and '5'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Once one or more command menus have been created, access can be controlled to individual Unix SSH secrets.

On the **Security** tab of a secret that can use a proxied PuTTY session, proxy must be enabled as well as command menu restrictions. If **Allow Owners Unrestricted SSH Commands** is enabled, any user who is an owner of the secret has unrestricted use of the PuTTY session, that is, that user is able to type in commands as in a normal session. Additionally, other groups can be assigned the Unrestricted role as well.

In the following example, the "admin" group is unrestricted, while everyone who is not in the admin group is restricted to only being able to run the commands that are enumerated in the user command menu, created above.

**SSH Unix Secret (Unix Account (SSH))**

General
Personalize
Expiration
Launcher
**Security**
Dependencies

Require Check Out

☐

Enable DoubleLock

☐

(You have not created a DoubleLock password.)

Enable Requires Approval for Access

☐

Require Comment

☐

Enable Proxy

☒

Hide Launcher Password

☐

Enable SSH Command Restrictions

☒

Allow Owners Unrestricted SSH Commands

☒

Name	SSH Command Menu		
admin	Unrestricted		
Everyone			

Add New

--Groups--

Customize Password Requirement
☐

Save

Cancel

A user who is subject to SSH Command Restrictions are presented with a screen similar to the following when connecting to an SSH session:

```
Using username "729ddaef-38d0-48e0-b9dc-d4911e76d0c1".

1. User Command Menu

    ?. Show Command Menus
    exit. Exit session
Last login: Thu Mar 17 12:38:46 2016 from 192.168.60.153
[runscripts@centostestserver ~]$
```

The user simply enters the number of the command menu to see available commands, or types "?" to display the options again.

```
Using username "729ddaef-38d0-48e0-b9dc-d4911e76d0c1".

1. User Command Menu

    ?. Show Command Menus
    exit. Exit session
Last login: Thu Mar 17 12:38:46 2016 from 192.168.60.153
[runscripts@centostestserver ~]$ 1

1. view_shadow = cat /etc/shadow
2. view_secure_log = cat /var/log/secure
3. start_apache = /usr/sbin/service apache start
4. stop_apache = /usr/sbin/service apache stop

    up. Return to Command Menu selection. You may also type ..
    ?. Show Commands
    exit. Exit session

[runscripts@centostestserver ~]$
```

Only the commands listed can be run by this user. The user can either enter the number of the command to be run, or the name of the command, which is the word to the left of the equal (=) sign. Other options are available (as shown) to navigate through the available command menus, display help, or exit the session.

## Session Recording and Launchers

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session recording works for any launcher, including PuTTY and SSH, Windows Remote Desktop, Microsoft SQL Management Studio, and custom executables. The resulting movie is viewable from the secret audit. Session recording can be toggled on or off globally on the Configuration page and set for individual secrets on the Security tab. Detailed information on supported codecs can be found in [Session Recording](#). When a user launches a session with session recording enabled, a brief message is displayed to inform the user that their actions are recorded.

**Note:** When multiple Launchers are enabled for a secret template, enabling session recording for a secret applies the setting to all launchers for that secret.

On the Secret View page, clicking the Launcher icon launches the Remote Desktop, PuTTY, or custom session directly from the browser or log into the website. The mapped text fields are passed to the launcher for automatic authentication.

If the machine is set for Remote Desktop, the console launches and allows the machine to be specified from the RDP dialog.

If the Host is set to <user>, a prompt asks for the specific machine before launching the PuTTY session.

For some browser security levels, you might need to click **Allow** for the launcher application to open.

**Note:** The View Launcher Password permission can be removed to prevent users from viewing the credentials but can still use the authentication session to access the computer.

The settings under the Launcher tab are used for secrets that are enabled for SSH and custom launchers.

You can limit the domains that a launcher connects to. If this is not set, then nothing changes—the launcher can connect to any domain. If it is set, however, Secret Server refuses to connect to any domains that are not explicitly allowed.

This setting is done via a Windows Group Policy Object (GPO) administrative template XML file (.admx). The file specifies the registry key that are changed when the GPO is edited. Download that file here: [LimitLauncherDomainPolicyDefinitions.zip](#).

For details on using these files, see [How to create and manage the Central Store for Group Policy Administrative Templates in Windows](#) on the Microsoft site. The settings are present in both user and machine configurations in the group policy editor. If both are specified, then only the machine configuration is used (the user configuration is completely ignored). This is because the user configuration is stored in part of the registry that does not require administrator access to edit, so the machine configuration should be used in most cases.

The Group Policy valid values are just domain names, like `example.com`, or IP addresses, like `192.168.1.2`. No port should be specified, and no scheme. A value like `https://example.com` is not valid, because it has `https://` in the front. Ports are also invalid, so `example.com:885` will not match. The correct value would simply be `example.com`. Wildcards are not supported, but subdomains matter, so a value of `example.com` will not match `something.example.com`.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Adding Remote Desktop Launchers

1. Click **Add New Launcher** to add a launcher to the template.
2. On the following page, select a launcher type from the drop-down menu. The text-entry fields below reflect the text-entry fields necessary to map to the launcher. In the case of a custom launcher, these text-entry fields are used to run the launcher process if the launcher is configured to run as secret credentials.
3. Choose a secret text-entry field in the drop-down menu on the right to map to each launcher value on the left. See the following section for further details on editing launcher configuration.
4. Click the **Save** button to add the launcher to the template.

## Browser Configuration

Remote Desktop (RD) launchers require the following:

- **Firefox Configuration:** Firefox requires a helper add-on application to run the RD and PuTTY launchers. The Microsoft .Net Framework Assistant add-on and .NET framework version 4.5.1 SP1 needs to be installed.
- **Chrome Configuration:** If using ClickOnce, Chrome requires a Helper Add-on application to run the RDP and PuTTY Launcher. The ClickOnce add-on for Google Chrome Add-on needs to be installed. The launcher requires .NET framework version 4.5.1 SP1 as well.
- **SSL Certificates:** SSL must be set up properly for the RD launcher to work correctly. If SS is using SSL certificates, they must be trusted at the user's computer. This is only an issue with self-created certificates.

## Editing RD Launchers

Click **Edit** to modify the settings for a launcher that has already been added to the template. For a launcher to work properly, SS requires credentials to be taken from secret text-entry fields. Fields must be assigned their corresponding credentials from the list. In addition to the secret fields, the domain can be mapped to <blank>, which passes an empty string to be used with local accounts, and the machine or host can be mapped to <user input>, which prompts the user for a specific machine to be used with domain accounts.

In cases where there are multiple endpoints to connect to, such as with a domain account, the machines can be restricted to a set list. Under the **Advanced** section of the secret template launcher configuration, enable **Restrict User Input**. When that option is on, the launcher shows a drop down of machines to connect to, based on a comma-separated list in the specified secret field.

## Setting Up Secret Templates for RD Launchers

Launchers can be accessed from any secret created from a properly configured template.

By default, the templates Windows Account, Active Directory Account, Cisco Account (SSH), HP iLO Account (SSH), Unix Account (SSH), Web Password, and SQL Server Account have the launcher configured.

Secrets can be configured for the launcher from within the Secret Template Designer page.

Clicking **Configure Launcher** displays the options available.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Web launchers are a separate login method from the Web password filler and provide a convenient click to automatically log on simpler websites. Web launchers do not work on complex login pages that rely on JavaScript. For those login pages, use the bookmarklet or browser extension for the Web password filler. By default, Web launchers are enabled on the Web Password Secret template, but they can be enabled on custom templates as well, as described in [Enabling Launchers](#).

## Configuring Web Launchers for Secrets

Once enabled on the template, a Web launcher needs to be configured for the secret. Each website login is unique and requires the secret text-entry fields to be mapped to the form controls. For a new secret the Launcher icon appears and clicking on it takes the user to a configuration screen. The user can also view and access the configuration screen from the Launcher tab. Depending on whether other secrets with the same website have been configured, the user has different options.

**Note:** Configuring the Secret for use with the Web Launcher requires the user to have Owner permission on the Secret.

First, there is the option of downloading the setting from Thycotic.com. When the Configure Web Launcher page is loaded, SS checks online at Thycotic.com for pre-approved matching websites. If any are found, they are downloaded and made available to pick from in the dropdown list.

**Note:** This functionality can be disabled in SS in the Configuration Settings.

The list displays all downloaded configurations and other secrets' configuration for the same domain that the user has permission to view. Select one from the list and click **Next** to create a copy of the settings for the secret.

There is also an option to create a configuration that allows the Web launcher to be used on most websites and not rely on published configuration settings. To use this, select the last item in the dropdown list and click **Next**. The next section discusses the create process.

## Creating a Configuration

When configuring the Web Launcher:

- **Entering the Login URL:** SS needs to know the exact URL used to login to be able to figure out the controls and perform the automatic login. Some example login URLs:

- <https://login.yahoo.com/config/login>
- <https://MyServer/Billing/login.aspx>
- <https://firewall07/login/>

**Note:** The Login URL is typically a secure site with a prefix of `https://`. If allowed to access the site, SS automatically detects if `https` should be used to ensure the credentials are passed securely.

- **Providing the Page Source:** If SS is not allowed access to sites, or the login URL is not accessible by an external site, the page source needs to be provided for the Web launcher controls to be obtained. Ensure the login URL is correct when the page source is taken. If the site can be accessed by SS the page source is automatically obtained and this step is not present.
- **Choosing the Form:** The page is read, and the exact login form needs to be identified. The page forms are listed in the list with the most likely selected. If no forms or no likely forms are found, the user needs to update the URL or page source, as configuration must have at least one textbox and one password box.
- **Wiring Up the Fields to Controls:** In most cases, SS automatically wires up the Username and Password text fields to the correct page controls. If not, the user completes the control mapping on the Launcher tab.

## Launching to a Website

The Web launcher can be used by clicking the Launcher icon on the Secret View page. The Web launcher opens a new window in the browser, which attempts to login to the site using the credentials on the secret. The launcher can also be used with the Test Launcher button on the Launcher tab. Testing the Launcher creates a dialog to offer troubleshooting help and means to upload the configuration to Thycotic.com. The uploaded configuration is reviewed and published by Thycotic for all SS customers to use with the check online feature. No secret or identifiable information is uploaded to Thycotic.com. Only the website URL and control names are sent.

## Secret Management

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

*Secrets* are individually named sets of sensitive information. Secrets address a broad spectrum of secure data, each type represented and created by a *secret template*. You can centrally manage secret security through sharing settings for each secret. Additionally, using folder structure, you can allow one or more secrets to inherit permissions from their parent folder. All secret text-entry field information is securely encrypted before being stored in the database, including a detailed audit trail for access and history.

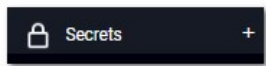
**Note:** You can "favorite" a secret in the main menu by right clicking it.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Creating Secrets

To create a secret:

1. Click the **+** on the Secrets item on the main menu:



or click the **+** icon and select **New Secret**. The Create New Secret page appears:

 The 'Create New Secret' page has a title bar. Below it, it says 'No folder selected' with a 'Change' link. Then, 'Choose a Secret Template' is followed by a search bar labeled 'Search for template name'. A scrollable list of templates includes: Active Directory Account, Amazon IAM Key, Bank Account, Cisco Account (SSH), Cisco Account (Telnet), Cisco Enable Secret (SSH), Cisco Enable Secret (Telnet), Cisco VPN Connection, Combination Lock, Contact, Credit Card, Generic Discovery Credentials, Healthcare, HP iLO Account (SSH), and IBM iSeries Mainframe. At the bottom right are 'Cancel' and 'Create Secret' buttons.

2. Click the **Choose a Secret Template** list to choose a template from which to create the secret .

**Note:** If you do not find a suitable template available, you can create a custom template.

3. Click the **Create Secret** button. A Create New Secret page appears.

**Note:** These pages differ significantly, based on the secret template you chose. For this instruction, we chose the frequently used Web Password template.

## Create New Secret

Template

Web Password [Change](#)

Folder

[Everyone](#) [Clear](#)

Name \*

URL \*

UserName \*

Password \*

Show

Generate

Notes

Auto Change Enabled

☐

Cancel

Create Secret

- Complete the text boxes and selection controls on the page.

**Note:** The password generator is governed by a password requirement, which is usually set via the secret template. However, you can override the template for this secret and set the requirement to something different in the Password Requirements section of the Security tab, after you create the secret.

- Click the **Generate** button to create a strong password that meets the requirements for that type of secret. You can also add your own. If you do, the password box will remain red until you enter a password that meets the requirements.

**Note:** The maximum password length is 1024.

The bar below the text box indicates the strength of the password you enter:

MasterPass \*

1234

Hide

Generate

qualifies, the box and bar turn green:

When you type one that

MasterPass \*
Hide
Generate

If you want to see what requirements are governing the password, hover the mouse over the password strength bar:

MasterPass \*
Hide
Generate

Password must include:

- ✓ At least 1 Lower case letters (a-z)  
abcdefghijklmnopqrstuvwxyz
- ✓ At least 1 Symbols (Symbols)  
!@#\$%^&\*()
- ✓ At least 1 Numbers (0-9)  
1234567890
- ✓ At least 1 Upper case letters (A-Z)  
ABCDEFGHIJKLMNOPQRSTUVWXYZ


- Click the **Sites** list to select a site the secret belongs to.
- (Optional) Click to select the **Auto Change Enabled** check box to enable automatic remote password changing (RPC) for the secret.
- Click the **Create Secret** button.

**Note:** It is possible to import data as secrets. See [Importing Secrets](#).

## Customizing the All-Secrets Page

On the main menu, there is a **Secrets** folder tree. When you click on the root or any subfolder, you see a list of all the secrets in that folder with multiple columns. You can customize what you see in one of three ways:

### Customizing Visible Columns

You can display additional columns on the grid by clicking the  icon. This data can be either secret metadata or template text-entry fields that have been set to be available for viewing. To select additional columns to display, click the **Advanced** link and then the **Column Selection** link. You can display the following metadata fields:

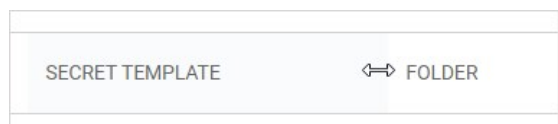
- Auto Change Enabled
- Checked out
- Checkout Enabled
- Created
- Days until Expiration
- Deleted
- Double Lock Enabled
- Expiration Field Changed
- Folder
- Inherits Permissions
- Heartbeat
- Hide Password
- Last Accessed
- Machine
- Notes
- Requires Approval
- Requires Comment
- Secret Template
- Username

### Filtering Search Results

You can filter secret search results by selecting a folder on the left, either by clicking it or using the search text-entry field above the folder tree. On the right side of the widget, secrets can be filtered further by specifying search criteria in the top text box. The Advanced section allows filtering by secret template and status, as well as the option to include secrets contained in subfolders. Advanced criteria only remain in effect while those options are expanded (visible).

### Sizing Columns

You can resize any of the columns by hovering the cursor over the border between them till it turns into a double arrow:



Click and drag to resize the column.

## Deleting and Undeleting Secrets

To delete a secret:

1. Navigate to the secret **View** page by searching or drilling down the folder tree.
2. Click the **Options** dropdown list and select **Delete**. A confirmation appears.
3. Click the **Confirm Delete Secret** button.
4. The secret is logically deleted and hidden from users who do not have a role containing the View Deleted Secrets permission.

SS uses these "soft deletes" to maintain the audit history for all data. However, deleted secrets are still accessible by administrators (like a permanent Recycle Bin) to ensure that audit history is maintained and to support recovery. A user must have the View Deleted Secrets permission in addition to Owner permission on a secret to access the secret View page for a deleted secret. For more information about these permissions, see [Roles](#) and [Sharing a Secret](#).

To undelete a secret, navigate to the secret View page and click **Undelete**.

**Note:** Secrets can also be deleted in bulk. See [Running Dashboard Bulk Operations](#).

## Duplicating Secrets

The secret duplication function allows for easier, automatic secret duplication. Any user with the Owner Secret permission on a secret can click to select **Duplicate** in the **Options** dropdown list to create a new secret with information based on the original secret. Secret text-entry field information, launcher settings, secret settings, double locks, email settings, and permissions are copied over. Audit records are written to the source secret and target secret to indicate that a copy operation took place. Currently, file attachments are not copied.

## Editing Secrets

**Note:** If using the Dashboard, see [Secret Server Dashboard](#).

To edit a secret:

1. Navigate to the secret's **View** page by searching or drilling down the folder tree.
2. Click the desired tab for the secret configuration.
3. Click the **Edit All Fields** link. All text-entry fields become editable.

**Note:** The password generator is governed by a password requirement, which is usually set via the secret template. However, you can override the template for this secret and set the requirement to something different in the Password Requirements section of the Security tab after you create the secret.

4. For passwords, you can create a random password with the **Generate** button (on the General tab). This generates a password according to the rules set at the template level (see secret templates for more information about password requirements).
5. Click the **Save** button.

## Overriding the Secret Template's Password Requirements

All secrets inherit a set of password requirements (see [Template Password Requirements](#)) from their parent secret template. After you create a secret, you can choose to use a different password requirement for this one secret, which leaves other secrets based on the template as they were. To choose a different password requirement for the secret:

1. Navigate to the secret **View** page by searching or drilling down the folder tree.
2. Click the secret to open the secret's page.
3. Click the **Security** tab.
4. Click the **Edit** Link in the **Password Requirements** subsection in the **Other Security** section. The Edit Password popup appears.
5. Click the Password Requirement dropdown list to select the password requirement you desire.
6. Click the **Save** button.

## Setting Up Password Masking

Password masking prevents over-the-shoulder viewing of your passwords by a casual observer (passwords show as \*\*\*\*\*). For security, the number of asterisks does not relate to the length of the password.

As an administrator, you can force all the secret password text-entry fields in the system when viewed to be masked. To do this, enable the **Force Password Masking** setting in the **Configuration** settings. Only secret text-entry fields marked as a password text-entry field on the secret template is masked.

There is also a user preference setting that forces password masking on all secret password text-entry fields viewed by the user. This Mask passwords when viewing secrets setting is found in the **Profile > Preference** section for each user. If the configuration setting discussed above is enabled, this user preference setting is overridden and cannot be disabled.

## Sharing Secrets

Sharing passwords is crucial for information technology teams. Due to the sensitive nature of sharing secure information, SS ensures shared passwords are tracked and guarded.

### Permissions

There are three permission levels to choose from when sharing secrets with another user or group:

- **View:** User may see all secret data, such as username and password, and metadata, such as permissions, auditing, history, and security settings.
- **Edit:** User may edit the secret data. Also allows users to move the secret to another folder unless the Inherit Permissions from Folder setting is turned on, in which case the user needs Owner permissions to move the secret.
- **List:** User may see the secret in a list, such as a list returned by running a search, but not to view any more details about a secret or edit it.
- **Owner:** User may change all the secret's metadata.

**Note:** Password text-entry fields are not visible if a secret has a launcher and the Hide Launcher Password setting is on or the user does not have the View Launcher Password role permission.

Secrets can be shared with either groups or individual users. The Secret Sharing section allows secrets to be configured for access.

### Procedure

To add or remove secret sharing:

**Note:** To simplify the sharing process, new secrets automatically inherit the settings from the folder they are stored in. That is, we enable the **Inherit Permissions from Folder** check box on the **Sharing Edit** page by default, so secrets inherit all the parent folders' sharing settings. As long as this check box is selected, you cannot set the permissions for the secret. For more on folder security, see the [Folders](#) section.

1. [View the secret](#) you want to share.
2. Click the **Sharing** tab.

The screenshot shows the 'Sharing' tab in the Delinea interface. At the top, there are tabs for 'General', 'Security', 'Audit', 'RPC', 'Dependencies', 'Sharing' (which is active), 'Settings', and an 'Options' dropdown. Below the tabs, there is a 'SHARE SECRET' section with an 'Edit' link. Underneath, the 'Inherit Permissions from folder' checkbox is checked, and the 'No' radio button is selected. Below this, there is a table with the header 'SHARED WITH' and one row with the text 'Will' and 'Owner'.

3. Click the **Edit** link. The page becomes editable:

**SHARE SECRET**

☐ Inherit Permissions from folder

SHARED WITH		
Will	Owner ▾	<a href="#">Remove</a>

**Add Groups / Users**

Search for groups or users 🔍

Cancel Save

4. Click the **Remove** link next to any share you want to delete.
5. Type any user or group you want to share with in the **Add Groups / Users** search text box.
6. When the user or group appears in the dropdown list, click to select it. The user or group appears in the **Shared with** table.
7. Click the unlabeled permission dropdown list box to select the desired permission.
8. Repeat the process for additional users or groups.
9. Click the **Save** button to commit the changes.

You can also modify sharing settings for users or groups that already have sharing enabled for the secret. If a user or group is not displayed, they do not have access to the secret.

## Viewing Secrets

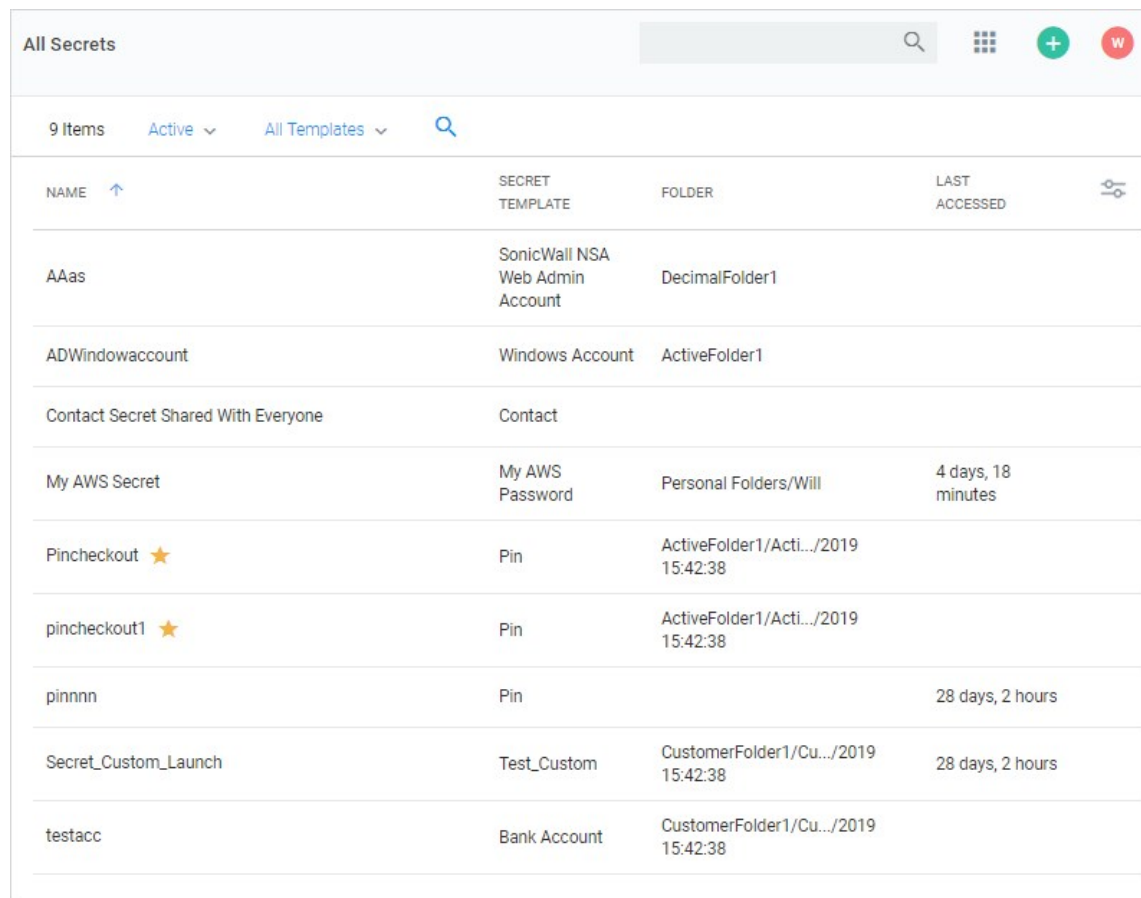
To view the information contained in a secret:

1. Locate the desired secret in one of these ways:
  - On the main menu, drill down the folders tree to select the secret.
  - Click the **Secret** menu item on the main menu and find the secret in the **All Secrets** table. You can filter the list or click the magnifying glass icon to search for the secret.
2. Click on the secret's name link. The secret's view page opens to the General tab.
3. Click the desired tab to view specific information. For example, click the General tab and go to the Expiration and Heartbeat section to see if the secret's password has expired and what its expiration interval is. You can check the history of the secret by clicking the Audit tab.
4. [Edit the secret](#) if desired.


## Searching for Secrets

To search for secrets:

1. Click the **Secrets** menu item in the main menu. The All Secrets page appears:



NAME	SECRET TEMPLATE	FOLDER	LAST ACCESSED
AAas	SonicWall NSA Web Admin Account	DecimalFolder1	
ADWindowaccount	Windows Account	ActiveFolder1	
Contact Secret Shared With Everyone	Contact		
My AWS Secret	My AWS Password	Personal Folders/Will	4 days, 18 minutes
Pincheckout ★	Pin	ActiveFolder1/Acti.../2019 15:42:38	
pincheckout1 ★	Pin	ActiveFolder1/Acti.../2019 15:42:38	
pinnnn	Pin		28 days, 2 hours
Secret_Custom_Launch	Test_Custom	CustomerFolder1/Cu.../2019 15:42:38	28 days, 2 hours
testacc	Bank Account	CustomerFolder1/Cu.../2019 15:42:38	

2. Type the secret name or other text in the unlabeled search text box at the top of the page.
3. Click the  button. The All Secrets table only displays matching secrets. Searches search for all text-entry fields that are configured as searchable on the secret's template if the extended search indexer is enabled.


**Important:** If the search indexer is not enabled, searches are only performed on the **Secret Name** text field.

## Search Indexer


The *search indexer* allows searching on all text-entry fields set to searchable on the template. To enable and configure the search indexer:

1. Click the **Admin** button on the main menu and select **See All**. The Administration page appears:

## What are you looking for?




Simplified View ▾




### Actions

Secret Server features that perform important jobs




### Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more




### Users, Roles, Access

These features help you organize users & permission settings within Secret Server



### Diagnostics, Logs, Security

Reference options for diagnostics, logs, and security features



### Tools & Integrations

Find Secret Server tools and other product integrations here

2. Type and then click Search Indexer in the Search text box. The Indexing Service page appears:

## Indexing Service

The indexing service allows searching across all fields within Secrets.

**Enabled** Yes

**Status** Idle

**Index Mode** Standard

**Indexing Separators** .,:; ,/\,\t,\n,\r,COMMA,?,!,@,#,(,),[,],{,},',"

**Progress** 100.00 %

[Advanced \(not required\)](#)

<b>Days to Keep Operational Logs</b>	30
--------------------------------------	----



Back



Edit



Rebuild Index



Refresh

## Logs

Search...	50	90 minutes	
-----------	----	------------	--

Record Count 0 Page 1 / 1 « Prev Next »



No results matching the current filter.

3. Click the **Edit** button. The page becomes editable:

## Indexing Service

The indexing service allows searching across all fields within Secrets.

Enabled

☒

Indexing Separators

Index Mode

☒ Standard
 ☐ Extended

[Explain](#)

Advanced (not required)

Days to Keep Operational Logs

Save

Cancel

- Ensure the **Enabled** check box is selected.
- Click either the **Standard** or **Extended** selection button.
  - Standard search mode* is the default and searches on whole words in a field value. For example, a field value of "My AWS Secret" would match when you search for *My AWS Secret*, *My*, or *Secret*.
  - Extended search mode* searches for whole words or a partial words by up to twelve characters. For example, a field value of "My AWS Secret" would match when you search for *My AWS Secret*, *My*, *Secret*, *WS*, or *ecret*. This is more useful, but may impact search performance and creates a larger index table.

**Note:** Indexing separators are used to split the text text-entry fields into search terms. By default, the separators are semi-colon, space, forward slash, back slash, tab (\t), new-line (\n), return (\r), and comma. Changes to the indexing separators require a full rebuild of the search index.
- Change the **Days to Keep Operational Logs** text box to set the period to keep indexing-related logs that might contain PII. SS automatically deletes logs older than that (in days).
- Click the **Save** button. The Indexing Service page reappears, and the indexing begins in the background. Depending on the size of the SS installation, it may take awhile. Progress is shown on the Progress bar.
- If you changed the indexing separators, click the **Rebuild Index** button.

## Common Configuration Options

These are the configuration options that are common to every secret:

- **Convert Template:** Change which template is being used to store and display information in this Secret.
- **Copy Secret:** Create a duplicate copy of the secret, which may also be renamed and modified.
- **Delete:** Delete the secret.
- **Edit:** Edit the secret parameters.
- **Favorite:** Click the star from the Dashboard or check this box on the Secret View page to mark the Secret as a favorite. It then displays in the Favorite Secrets widget.
- **Folder:** Folder location of the secret. The secret inherits permissions of this folder, depending on the Default Secret Permissions setting in the SS Configuration options.
- **Share:** Configure the sharing settings, or permissions, for the secret.
- **View Audit:** View the secret audit log to see which users have accessed the secret and the actions that have been performed.

## Advanced Configuration Options

These are the buttons, fields, and icons that are available for more advanced secrets:

- **Expire Now:** Expire the secret manually.
- **RDP Launcher Icon:** Click to open the Remote Desktop Protocol (RDP) Launcher. See further details in the Launcher section.
- **Run Heartbeat:** Initiate heartbeat, which attempts to verify that the secret credentials can authenticate.
- **Site:** Edit the secret to set the distributed engine site. This determines where password changing, heartbeat, and proxied sessions run from.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret expiration is a core SS feature. Any template can be set to expire within a fixed time interval. For a secret to expire, a text field must be selected as the target of the expiration. For example, a secret template for Active Directory accounts might require a change on the password text field every 90 days. If the password remains unchanged past the length of time specified, that secret has expired and appears in the Expired Secrets panel on either the Dashboard's Expired secrets widget or the Home page.

Secret expiration provides additional security by reminding users when sensitive data requires review. This assists in meeting compliance requirements that mandate certain passwords be regularly changed. When expiration is combined with RPC, SS can completely automate the process of regularly changing entire sets of passwords to meet security needs.

## Forcing Expirations

To force expiration:

1. Navigate to the **Secret View** page.
2. Click the **Expire Now** button. This forces the secret to expire immediately regardless of the interval setting. The expiration date displays "Expiration Forced."

## Resetting Expired Secrets

To reset an expired secret, you must change the text field that has expired and is required to change. For example, if the text field set to expire is the password text field and the current password is "asdf," then a change to "jklh" resets the expiration interval and thus removes the expiration text on the Secret View page.

If you do not know which text field is set to expire:

1. Go to the secret template that the secret was created from.
2. Navigate to **Admin > Secret Template**.
3. Select the template.
4. Click the **Edit** button.
5. On the next page, click the **Change** link. In the **Change Required On** text box you can see the text field that is set to expire.

## Setting up Secret Templates for Secret Expiration

To set up expiration on a secret, you must first enable expiration on the template from which the secret is created.

To enable secret expiration for a secret template:

1. Navigate to **Admin > Secret Templates**.
2. On the **Manage Secret Templates** page, select the template from the dropdown list.
3. Click the **Edit** button.
4. On the **Secret Template Designer** page, click on the **Change** link.
5. On this subsequent page, click to select the **Expiration Enabled?** check box.
6. Enter the expiration interval (every x number of days), as well as the text field on the secret you wish to expire and require to be changed.

**Note:** You can override the interval setting for individual secrets.

**Note:** Enabling expiration for a template enables expiration for all the secrets that were created using that template.

## Setting up Secrets

Once you enable expiration for the template, expiration is also enabled for secrets that were created using that template as well as secrets created in the future. The Expiration tab appears on the Secret View page and requires the user to have Owner permission on the secret.

To set a custom expiration at the secret level, you adjust the expiration interval for the secret by clicking the **Expiration** tab in the **Secret View** page. There, you can set the secret to expire using the template settings (default), a custom interval, or a specific date in the future.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Secret Dependencies Tab

The settings inside the Dependencies tab are used for secrets that have RPC enabled.

See [Manually Adding Dependencies](#) for details.

## Secret Expiration Tab

Inside the Expiration tab, the expiration period can be modified. The following options are available:

- **Template Interval:** Default expiration period configured for new secrets based on the current template.
- **Custom Interval:** A custom expiration period in days.
- **Custom Date:** A custom expiration date in month/day/year format.

**Note:** See [Secret Expiration](#) for details.

## Secret Launcher Tab

The Launcher tab appears for secrets that use either a custom launcher or Web launcher.

If a custom launcher is associated with a secret template, a secret owner can configure associated secrets or a privileged secret to run the launcher process. The associated secret can be tied in to the command line parameters on the custom launcher, and the privileged secret is the identity that kicks off the launcher process.

If a Web launcher is associated with a secret template, the launcher tab displays how the Web launcher is configured for that secret. The following options are available:

- **Edit Fields:** Modify which secret text-entry fields are mapped to the HTML input controls on the target website.
- **Reconfigure Web Launcher:** Reset the Web launcher configuration.
- **Test Launcher:** Test the current Web Launcher configuration.
- **Use Web Password Filler:** Use the Web password filler rather than the Web launcher.

**Note:** See [Web Launcher](#) for details.

## Secret Personalize Tab

These settings only apply to the user who is editing the settings. They do not apply to the other users who have View, Edit, or Owner permission to the secret.

To use the settings in the Email Notifications section, you must have email configured correctly in your configuration settings. You also need a valid email address entered for each user account to use these settings. This can be set in the **Administration > Users** section.

The following email notification settings are available:

- **Send Email When Changed:** Email the user when the secret is edited by any user.
- **Send Email When Heartbeat Fails:** Email the user when a heartbeat function fails for the secret. The email contains the secret name, error code and details.
- **Send Email When Viewed:** Email the user when the secret is viewed by any user.

The Personalize tab also contains settings that pertain to the type of launcher configured for a secret. If the launcher type is Remote Desktop Protocol (RDP), the following settings are available:

- **Connect to Console:** Remote Desktop (RD) may connect to the console session.
- **Allow Access to Printers:** RD may access local printers.
- **Allow Access to Drives:** RD may access drives connected to the local machine.
- **Allow Access to Clipboard:** RD may access the clipboard of the local machine.
- **Use Custom Window Size:** Users may specify custom window height and width. Use Preferences refer to the user's settings under **Profile > Preferences** in the **Launcher** tab.

Users may enable or disable these settings or to defer to what is configured in their user settings by selecting **Use Preferences**.

## Secret RPC Tab

The settings inside the Remote Password Changing tab are used for secrets that are Remote Password Changing (RPC) enabled:

- **Auto Change:** Enable or disable auto change for the secret.
- **Next Password:** Specify the next password

**Note:** See [Remote Password Changing](#) for details.

## Secret Security Tab

The Security tab contains settings that can be enabled to increase security for a secret. The settings listed below may or may not be visible, depending on your configuration settings:

- **Require Check Out:** Only one user at a time has access to a secret. See [Secret Checkout](#) for details.
- **Enable DoubleLock:** User must enter a doubleLock password to decrypt and view a secret.
- **Enable Requires Approval for Access:** Users must request access to view a secret.
- **Require Comment:** Users must enter a comment before being granted access to view the secret. The comment is stored in the audit log for that secret.
- **Enable Session Recording:** Record the Launcher session. This applies to secrets with a launcher associated with the secret template. See [Session Recording](#).
- **Hide Launcher Password:** Restrict users with View permission from copying passwords to the clipboard or unmasking the password text-entry field of the secret. This applies to secrets with a launcher associated with the secret template.
- **Customize Password Requirement:** Specify a password requirement for each password text-entry field.

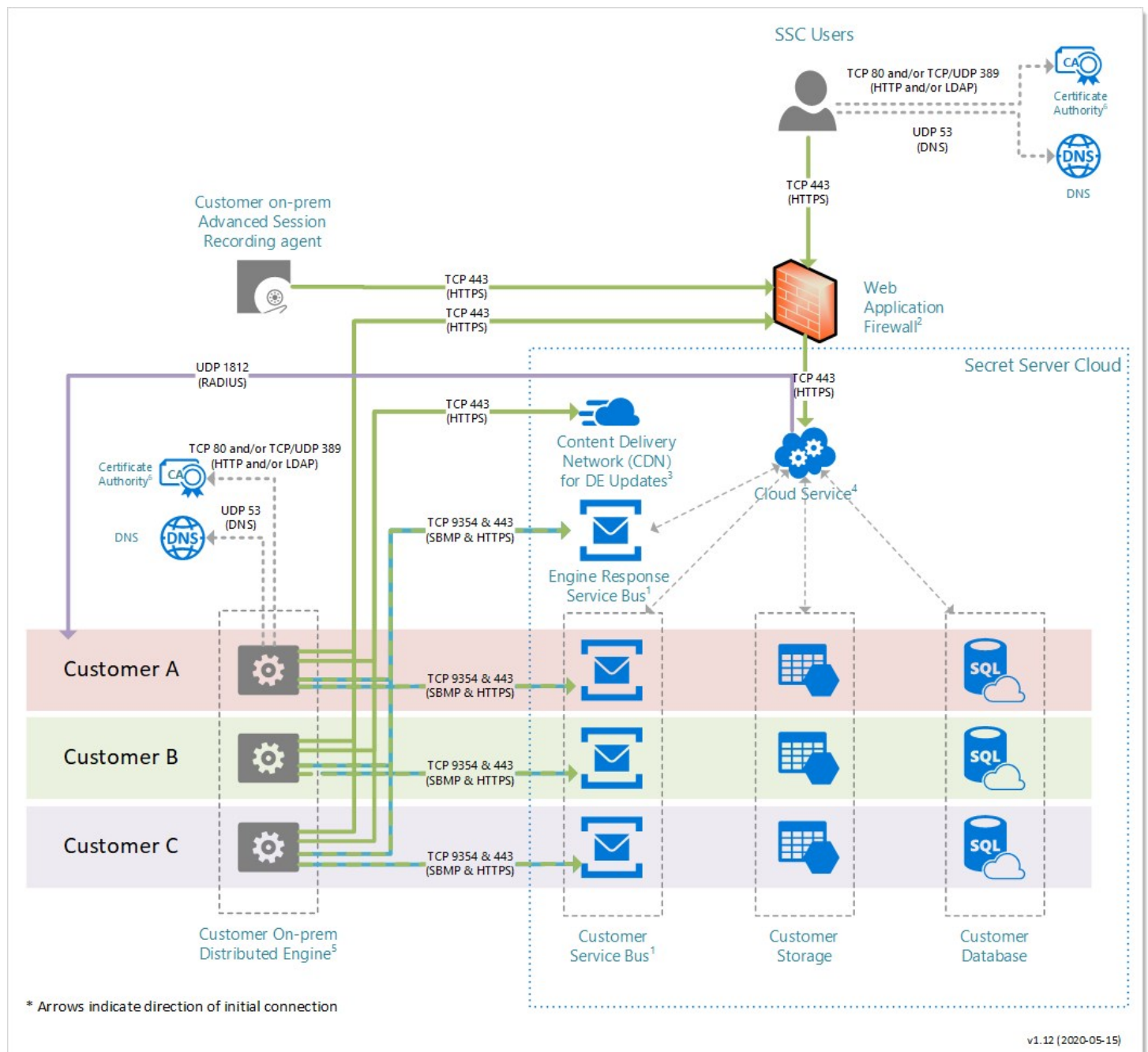
## Secret Server Cloud

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This section contains information that is exclusive to Secret Server Cloud.

## Diagram

**Figure:** Secret Server Cloud Hybrid Multi-Tenant Architecture



**Note:** Arrows indicate the direction of initial connection.

## Details

## 1: Service Buses

IP Address whitelisting is not necessary unless outbound firewall rules are in place. If IP whitelisting is necessary, Azure data center public IPs can be downloaded here:

- secretservercloud.com: <https://www.microsoft.com/en-us/download/details.aspx?id=56519> (id = ServiceBus.EastUS)
- secretservercloud.com.au: <https://www.microsoft.com/en-us/download/details.aspx?id=56519> (id = ServiceBus.AustraliaCentral)
- secretservercloud.eu: <https://www.microsoft.com/en-us/download/details.aspx?id=57064> (id = ServiceBus.GermanyCentral)
- secretservercloud.com.sg: <https://www.microsoft.com/en-us/download/details.aspx?id=56519> (id = ServiceBus.SoutheastAsia)

If you wish to restrict outbound traffic, Thycotic Support can provide you with your customer-specific service bus hostnames.

## 2: Web Application Firewall (WAF)

IP Address whitelisting is not necessary unless outbound firewall rules are in place. Public IP is based on geographical location.

IP addresses for all regions: 45.60.38.37, 45.60.40.37, 45.60.32.37, 45.60.34.37, 45.60.36.37, 45.60.104.37

## 3: Content Delivery Network (CDN)

IP Address whitelisting is not necessary unless outbound firewall rules are in place. Public IP is based on geographical location.

Edge nodes for all regions: <https://docs.microsoft.com/rest/api/cdn/edgenodes/list> (type=Standard\_Verizon)

## 4: RADIUS

Inbound whitelisting is necessary if RADIUS authentication is configured. Port 1812 needs to be open for inbound connection on the RADIUS server. The RADIUS server could either be publicly accessible or have port forwarding configured for Secret Server Cloud to be able to reach it. IP addresses:

- secretservercloud.com: 40.76.197.147, 40.121.181.52
- secretservercloud.com.au: 20.36.47.199, 20.36.45.106
- secretservercloud.eu: 51.4.141.94, 51.4.194.120
- secretservercloud.com.sg: 137.116.141.200, 137.116.143.17

## 5: Distributed Engine (DE)

If external clients must be able to connect to internal SSH or RDP endpoints, an SSH proxy can be configured on the DE. Additionally, TCP port 22 needs to be open for inbound connections on the DE server, as well as appropriate configuration to allow inbound connections from the public Internet.

## 6: Certificate CRLs

Whitelisting is not necessary unless outbound firewall rules are in place. If whitelisting is necessary, access to CRL distribution points is necessary.

secretservercloud.com:

- <http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl> (Web server)
- [<http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl>] ([http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft](http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl) IT TLS CA 5.crl) (service bus)
- [<http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl>] ([http://crl.microsoft.com/pki/mscorp/crl/Microsoft](http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%205.crl) IT TLS CA 5.crl) (service bus)

secretservercloud.com.au:

- <http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl> (Web server)
- [<http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%204.crl>]  
([http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft](http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%204.crl) IT TLS CA 4.crl) (service bus)
- [<http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%204.crl>]  
([http://crl.microsoft.com/pki/mscorp/crl/Microsoft](http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%204.crl) IT TLS CA 4.crl) (service bus)

secretservercloud.eu:

- <http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl> (Web server)
- [[ldap://directory.d-trust.net/CN=D-TRUST%20SSL%20Class%203%20CA%201%202009,O=DTrust%20GmbH,C=DE?certificaterevocationlist](http://ldap://directory.d-trust.net/CN=D-TRUST%20SSL%20Class%203%20CA%201%202009,O=DTrust%20GmbH,C=DE?certificaterevocationlist)] ([http://directory.d-trust.net/CN=D-TRUST](http://directory.d-trust.net/CN=D-TRUST%20SSL%20Class%203%20CA%201%202009,O=DTrust%20GmbH,C=DE?certificaterevocationlist) SSL Class 3 CA 1 2009,O=DTrust GmbH,C=DE?certificaterevocationlist) (service bus)
- [http://crl.d-trust.net/crl/d-trust\\_ssl\\_class\\_3\\_ca\\_1\\_2009.der.crl](http://crl.d-trust.net/crl/d-trust_ssl_class_3_ca_1_2009.der.crl) (service bus)
- [http://cdn.d-trust-cloudcrl.net/crl/d-trust\\_ssl\\_class\\_3\\_ca\\_1\\_2009.crl](http://cdn.d-trust-cloudcrl.net/crl/d-trust_ssl_class_3_ca_1_2009.crl) (service bus)

secretservercloud.com.sg:

- <http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl> (Web server)
- [<http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%202.crl>]  
([http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft](http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%202.crl) IT TLS CA 2.crl) (service bus)
- [<http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%202.crl>]  
([http://crl.microsoft.com/pki/mscorp/crl/Microsoft](http://crl.microsoft.com/pki/mscorp/crl/Microsoft%20IT%20TLS%20CA%202.crl) IT TLS CA 2.crl) (service bus)

## Secret Server End User Guide

This guide is for regular, non-administrative, users of Secret Server (SS). It is mostly a set of links to a subset of the greater corpus of SS documentation.

Secret Server is a privileged access management (PAM) system. Essentially that means it manages who can access what, when, and under whose authority—all without introducing weak points, such as weak passwords or stale user accounts, and discovering those that potentially exist. For large organizations, this is a huge undertaking. It only takes one security breach to cause huge problems, and there are seemingly countless ways for those breaches to occur. PAM systems, such as SS, are invaluable in getting this situation under control. Better still, SS can make your day-to-day work environment safer and easier to manage too.

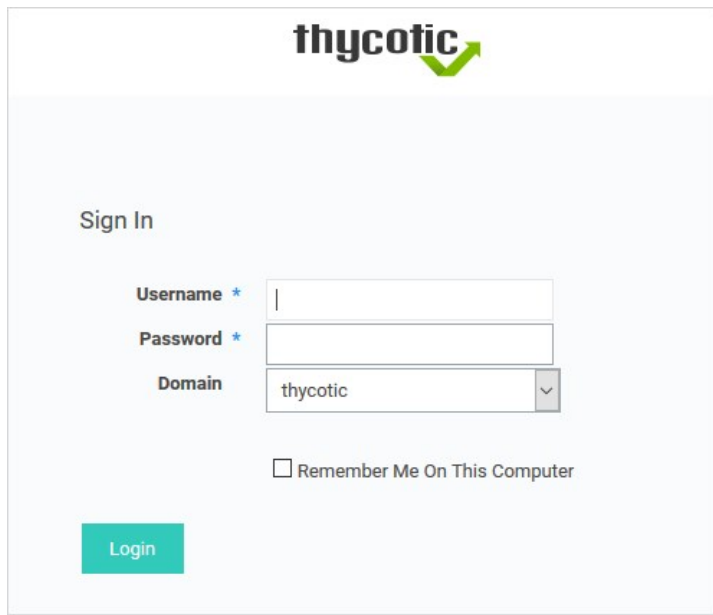
Secret Server is a powerful, advanced product with a wide range of capabilities. Even so, it is very easy to use for regular day-to-day operations for non-technical people. The key to this is knowing what to ignore and understanding the bits you do need to know. This guide is designed to help you do just that. It provides links to only what you need to know. You can add other topics later as needed.

- Technical Support: Please contact your organization's help desk.
- [Self-Help Resources](#)
- [Secret Server Glossary](#)
- [Document Conventions](#)

**Important:** When using this User Guide, it is easy to get lost in the ocean of SS documentation. To avoid that, we recommend using **<Ctrl> + click** to access the links here. That way, the page you are going to will open to a new browser window, leaving this one as is, making it much easier to get back to. You can also simply use the browser back button to return, but that can get tiresome because many pages link to others.

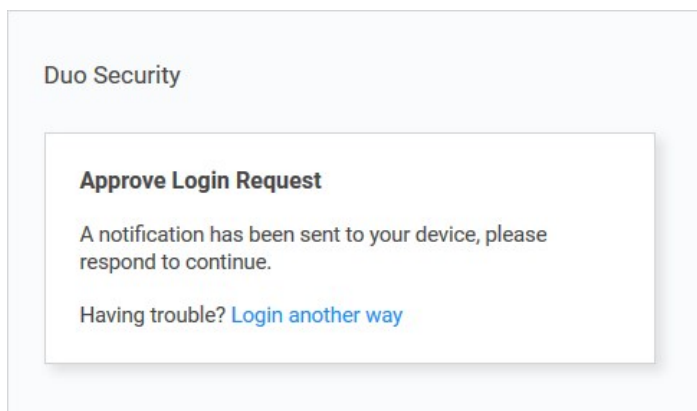
Depending on how your administrators configured SS, you can log on with either your Active Directory account or a local account.

1. In your browser, go to the URL for your organization's SS.



The screenshot shows the Thycotic Sign In interface. At the top is the Thycotic logo. Below it is the 'Sign In' heading. There are three input fields: 'Username \*', 'Password \*', and 'Domain'. The 'Domain' field is a dropdown menu currently showing 'thycotic'. Below these fields is a checkbox labeled 'Remember Me On This Computer'. At the bottom left is a teal 'Login' button.

2. On the login screen, enter your:
  - Active Directory username (or local one if you do not have one)
  - Active Directory password (or local one if you do not have one)
3. Select the your domain from the **Domain** dropdown list. If you do not have an AD domain, select **Local** instead.
4. (optional) Click to select the **Remember Me on This Computer** check box if you want to retain your username and domain on this computer.
5. Click the **Login** button. If you have Duo two-factor authentication, this appears:



The screenshot shows a 'Duo Security' dialog box titled 'Approve Login Request'. The text inside says: 'A notification has been sent to your device, please respond to continue.' Below this is a link that says 'Having trouble? Login another way'.

Your cell phone receives a notification you have to approve to access SS.

**Note:** SS also supports other two-factor authentication methods (depending on what your organization configured), such as text or email codes that SS prompts you for.

**Note:** After you log on with your local account for the first time, you are immediately prompted to change your password .

6. Click the **Login** button. The SS Dashboard appears.

*Secrets* are individually named packets of sensitive information, such as passwords. Secrets address a broad spectrum of secure data, each type represented and created by a *secret template* that defines the parameters of all secrets based on it. Secrets are very powerful and provide many ways of controlling and protecting their data, such as:

- Ensuring passwords are long, complex, and frequently changed.
- Relieving users of having to remember numerous complex passwords or when to change them. You only need to remember your password to access SS. All of your secret passwords are managed for you.
- Automatically changing passwords at set intervals with no user intervention.
- Defining who has access to the secret.
- Ensuring the person accessing SS or a secret is indeed you.
- Recording who actually accessed a secret.

All secret text-entry field information is securely encrypted before being stored in the database, including a detailed audit trail for access and history.

Some important basic information about secrets:

- [Viewing Secrets](#) (includes checking expiration and history)
- [Creating Secrets](#)
- [Secret Configuration Options](#)
- [Editing Secrets](#) (includes manually changing passwords, instead of waiting for expiration)
- [Deleting and Undeleting Secrets](#)

*Secret folders* allow you to create containers of secrets based on your needs. They help organize your customers, computers, regions, and branch offices, to name a few. Folders can be nested within other folders to create sub-categories for each set of classifications. Secrets can be assigned to these folders and sub-folders. Folders allow you to customize permissions at the folder level, and all secrets within can inherit the folder's permissions. Setting permissions at the folder level ensures future secrets placed in that folder have the same permissions, simplifying management across users and groups.

- [Creating Folders](#)
- [Adding and Moving Secrets Between Folders](#)

Please set up Web Password Filler (WPF) in the following order:

1. Ensure you can log in to SS the conventional way.
2. If necessary, create a folder in SS where the WPF secrets will reside.
3. [Install the WPF browser extension.](#)

4. [Configure WPF to point to SS.](#)
5. [Login to SS via WPF.](#)

The SS *check-out* feature grants exclusive access to a single user. If a secret is configured for check out, a user can then access it. No other user can access a secret while it is checked out, except unlimited administrators. This guarantees that if the remote machine is accessed using the secret, the user who had it checked out was the only one with proper credentials at that time. See [Secret Checkout](#) for details.

Secret Server records specific events, including expired secrets, and optionally sends you alerts when they happen. See the [Alert Notification Center](#) and [Creating Event Subscriptions](#) for details.

We created a [Getting Started Tutorial](#) for technical users. While it covers many things you do *not* need to know right now, you may later find it helpful if you want to get a deeper understanding of SS.

## Secret Server Setup

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This section contains information about installation and upgrading SS and its components.

- Components Installation
- Protocol Handler
- ASRA
- Launcher plugins
- Distributed Engines
- RabbitMQ
- SDK Client

## Understanding Licenses

SS's licensing model allows for scalability and enhanced core functionality in the form of edition enhancements (Professional, Premium Edition) and user packs. Licenses can be purchased for these items as follows:

- **Users:** SS ships with one free single user. Additional user licenses can be purchased through <https://thycotic.com> to expand an installation.
- **Support:** Support licenses allow installed instances of SS to receive all software updates. The number of support licenses and user licenses must be equivalent in order to be eligible for upgrades.

**Note:** Users must be supported in order to receive technical assistance from the SS support team.

After installation, the first thing we recommend doing is entering your licenses. You can do this in the Getting Started Wizard or from the Licenses Administration page (instructions below). This not only allows you to add more users but also enables additional features in SS.

For the Express edition, you have one license to enter. For Professional edition and higher, you have, at minimum:

- An edition license
- A user license
- A support license.

If you purchased additional licenses for sites or distributed engines, you may have more licenses to add.

**Note:** You will not have a support license if you have purchased the installed edition of SS but did not purchase support or upgrade protection.

## Activating Licenses

All non-evaluation licenses require activation after install. Activation is per license and Web server combination. Therefore, if you bring up a new Web server, it needs activation, even if your previous Web server was already activated. After installing each license, you are prompted to activate. Follow the on-screen prompts for online or offline activation. The activation process gathers the name, email, and phone number of the individual activating for internal purposes only. No other personal information is be sent to Thycotic.

To activate licenses:

1. Go to **Admin > Licenses**.
2. Click the **Install New License** button.
3. Type the **License Name** and **License Key** for one of the licenses that you received from your account manager.
4. Click the **Save** button.
5. If you have another license to add, click **Add Another License**.
6. When you have added all licenses, click **License Activation**.
7. Enter your name, email address, and phone number, then click the **Activate** button. If your server does not have outbound network access, click **Activate Offline** instead.

**Note:** For more information about license activation, see the [License Activation FAQ](#).

## Installing New Licenses

Once a license is obtained, it can be installed by copying the license name and code into the corresponding text-entry fields to a new license page. To access this page:

1. Select **Licenses** from the **Administration** menu.

2. Click **Install New License**.

## Converting from Trial Licenses

If you previously had evaluation licenses and recently purchased SS, you need to remove all evaluation licenses and install your purchased licenses. Normal trial licenses expire one month after issue. If the new licenses are not installed, users see "License has expired" error messages.

## Licensing Limited Mode

If you fail to activate, your system is be placed in limited mode, which prevents the following actions:

- AD sync
- Creating and editing secrets
- Importing secrets
- Manual RPC
- Web services (mobile applications)

## License Activation FAQ

### What happens if we find that we had more named users than licenses after activation? Will the account lock us out?

The user licenses are per named individual. You can simply disable any excess users so you are within your license count—these users can be re-enabled at a later time and all audit log information is kept.

### Why is license activation required?

Activation of license keys is standard practice in the software industry. We try to focus exclusively on implementing customer requests but occasionally we have to spend time on licensing especially as Secret Server goes into new geographical markets.

### Is there a grace period before we have to activate?

Existing customers have 30 days to activate their licenses after upgrading. New licenses have to be activated immediately on adding them to Secret Server. Evaluation licenses do not require activation.

### What will happen if we don't activate our licenses?

Secret Server will go into Limited Mode if you don't activate your licenses. Limited Mode allows you to view passwords but many other features are disabled such as creating Secrets, editing Secrets, changing permissions and using web services. Simply activate your licenses to get out of Limited Mode.

### We have several license keys. Do we need to activate each license key individually?

No, the license activation process will activate all license keys that are currently added to your Secret Server. However, additional license key for Distributed Engine may need to be activated individually if you receive the key after the other licenses.

### What if we have been using our license keys on more than one instance of Secret Server?

Secret Server software licenses (user licenses, Professional or Enterprise or Enterprise Plus edition licenses) may only be used on a **single production instance** of Secret Server. You may use your same licenses for a single testing (non-production) environment. If you have used your licenses on multiple production instances of Secret Server, please [contact us](#).

### What information is collected and sent during license activation?

License Activation is required for each web server that will be running Secret Server. The request and the response to/from [thycotic.com](https://thycotic.com) are encrypted for added security.

The following information is sent to [thycotic.com](https://thycotic.com) when you activate:

- Name (user entered)
- Phone Number (user entered)
- Email (user entered)
- All Licenses (license name, license key)
- Hardware Hash of each web server

This information is one way hashed before it is sent so it does not reveal any identifiable hardware information.

- Secret Server version
- An encrypted value to identify the instance
- This does not include any secret data or the `encryption.config` file.

- The data is gathered for the purpose of contact if there is a licensing issue and Thycotic will not sell or distribute the information provided during activation. The only information available to Thycotic staff is the contact information solely for the purposes of technical support and customer service.

## **Our Secret Server does not have outbound access to the thycotic.com Web site. Can activation be done while offline?**

Yes, there is an offline option for activating licenses. (See the Demo movie above for the offline process - also note the *offline=true* option described below if you have trouble activating offline)

To activate your Secret Server licenses when your server does not have internet access, perform the following steps:

1. Go to **Admin > Licenses**.
2. Click the **Install New License** button.
3. Type the **License Name** and **License Key** for one of the licenses that you received from your account manager.
4. Click the **Save** button.
5. If you have another license to add, click **Add Another License**.
6. When you have added all licenses, click **License Activation**.
7. Enter your name, email address, and phone number, then click the **Activate Offline** button.

Your activation is complete. If you received an error message, please take note of the error code and call the phone number contained in the message.

Secret Server may be activated on an Airgap Network for both Trials and Licensed products. Please let your Account Manager know you will be using Secret Server on an Airgap network for more information.

## **If we have trouble activating our licenses, what should we do?**

1. Please watch the demo at the top of this page to review how the process is supposed to work.
2. If your Secret Server is currently supported, that is, there is a current support license for each user license, our technical support team will be able to help you. Please [contact us](#).
3. If an error message persists after successful activation, remove expired/invalid licenses from Secret Server by clicking the license name and then Delete (the license information will remain available to you from your account at [my.thycotic.com](https://my.thycotic.com)).
4. **My Server is a VM that moves to different hardware often. Will this cause me to need to reactivate over and over?**

As of version 7.8.000000, you will not need to reactivate over and over. When you activate, you will be able to use Secret Server for a year without needing to reactivate regardless VM hardware changes. However, if your machine name changes as well as your hardware, you will need to reactivate. If you are using a version older than 7.8.000000, you will need to reactivate when the VM moves.

To upgrade SS, you need valid support licenses. To renew your support, please use our [online Web form](#) or contact sales. Once you have valid support licenses, follow the steps in [this KB article](#) to upgrade.

## Introduction

Secret Server (SS) has a built-in Web installer. The Web installer is a series of pages inside SS that allow you to download and run updates. SS is accessible by users for most of the upgrade process. You can bring down outside access to the site if you want to prevent users from making changes during the upgrade. Preventing user access makes restoring the database and site backups simpler if you decide to roll back the upgrade immediately afterward.

**Note:** You do not need to download the installer or `setup.exe`.

**Important:** Never overwrite or delete your `encryption.config` file.

**Important:** Back up your SS folder and database before performing the upgrade.

**Important:** Upgrading to SS version 10.7.000000 and above, requires SQL Server 2012 or later as the database for SS. For more information, see the [Release Notes](#).

**Important:** Upgrading to SS version 10.0.000000 and requires configuring integrated pipeline mode on the SS Application Pool. Please see [Configuring IIS for installing or upgrading to Secret Server 10](#) (KBA) for details on configuring integrated pipeline mode in IIS. If using Integrated Windows Authentication, you will also need to update IIS authentication settings as detailed in [Integrated Windows Authentication](#) (KBA). If you are at version 9.1.000000 and below, you need to first upgrade to 9.1.000001 before you can upgrade to 10.0.000000 and above.

**Important:** Upgrading to SS version 8.9.000000 and above requires Windows Server 2008 R2 or later.

**Important:** Upgrading to SS version 8.5.000000 and above, there are changes in the .NET Framework version you will need to be aware of along with some additional steps in the upgrade process. For more information, see [Secret Server Moving to .NET Framework 4.5.1](#).

## Before Beginning

1. Ensure that you have account credentials information and access for the server hosting SS *and* the SQL Server instance hosting your SS database.
2. Have a recent backup of the application files and database available.
3. If you use clustering, stop the application pools on all of the servers, except the one that is currently the primary.

## Upgrading a Clustered Environment

1. Follow the instructions in [Upgrading Secret Server](#) (KBA) or [Upgrading Secret Server Without Outbound Access](#) as applicable to upgrade your primary server.
2. Once upgraded and working, copy the Web application folder (without the `database.config` or the `encryption.config` files) to all secondary servers, and replace the content of the existing Web application folder with the new.
3. If Thycotic Management Server (TMS) is installed and clustered, you need to copy the TMS directory to the secondary servers as well. The TMS directory is included by default for new installs of SS 10.2 and above. TMS is used by advanced session recording and Privilege Manager. If the TMS folder and site does not exist in IIS, then no additional actions are needed beyond copying the SS directory.
4. Start secondary servers and confirm they still work.

## EFS and DPAPI Encryption

When upgrading, after the initial cluster configuration, you do not need to copy the `database.config` or `encryption.config` files to the other servers. If you need to copy those files because the database configuration changed and are using DPAPI, disable DPAPI encryption in SS by going to

**Admin > Configuration** and click **Decrypt Key to not use DPAPI** on the **Security** tab before copying those files to secondary servers.

**Note:** EFS encryption is tied to the user account running the SS application pool, so it is not machine specific. Copying EFS encrypted files between SS instances will not result in errors, but is not needed.

## Upgrading Database Mirroring

1. If there is more than one Web server running SS, ensure all instances are pointing to the primary database.
2. Stop all but the Primary web server.
3. Perform the upgrade on that single instance.
4. Once upgraded and working, copy the Web application folder to all secondary servers.
5. Start the secondary servers, and confirm they work.
6. Ensure all instances are properly activated.
7. Ensure that the primary database changes have been replicated to the mirror database.
8. If the secondary Web server was pointing originally to the secondary database, adjust it to point back to the secondary database.

## Upgrading Remote DR Instances

1. Perform the upgrade on the primary instance.
2. Backup the primary instance.
3. Copy the database backup to the remote DR instance.
4. Restore the database.
5. Once the primary instance is upgraded and working, copy the Web application folder (but not the `database.config` OR `encryption.config` files) to the remote DR instance (overwriting the existing files).
6. Restart IIS or recycle the application pool running SS on the remote DR instance.
7. Confirm that the remote DR instance is working correctly.

## Error Conditions

Two errors that may arise:

- Encryption configs don't match: See [Encryption key doesn't match error](#) (KBA).
- Version does not match: If a secondary node is not properly updated from the primary node after an upgrade, that node will not run because the application version does not match the database. The solution is to copy the application folder (minus the `database.config` OR `encryption.config` files) to replace the files on the secondary server.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Please [review our prerequisites](#) and then select either our [basic \(automatic\)](#) or [advanced \(manual\)](#) installation.

## Enabling SQL Server Encryption

Administrators can enable end-to-end encryption with the SQL database by using an Encrypted connection. This is a feature that is built into Microsoft SQL Server and Secret Server supports. To enable encryption:

1. Go to **Admin** > **See All**. The admin panel appears.
2. Type Database in the **Search** text box and select **Database**. The Database Configuration page appears:

### Help

Secret Server supports Microsoft SQL Server versions 2012, 2014, 2016, 2017, and Express.

View [Collation Requirements](#). Need help installing or configuring SQL Server? View [Installing and Configuring SQL KB Article](#).

### Database Configuration

#### SQL SERVER LOCATION

Server Name	QA-CUST-SQL-01
Database	SS_Playground

#### SQL AUTHENTICATION

☒ Windows Authentication using Application Identity (GAMMA\ss\_iis\_svc) - **Recommended**  
*(Advanced Setting. Windows Authentication requires a Service Account and advanced IIS setup. Detailed in [Windows Authentication KB](#).)*

☐ SQL Server Authentication *(SQL Authentication requires Mixed Mode. See setup in [SQL Authentication KB](#).)*

**[+] ADVANCED (NOT REQUIRED)**

Edit

View Audit

3. Click the **Edit** button.
4. Click the **Advanced (Not Required)** link. A new section appears:

[-] ADVANCED (NOT REQUIRED)

SSL Encryption ?

☐ Enable

Trust Server Certificate

☐ Enable

Failover Partner ?

(Requires SQL Server Configuration change)

Multi-Subnet Failover

☐ Enable

(Enabling Multi-Subnet Failover for AlwaysOn Availability Groups requires SQL Server 2012 and higher with AlwaysOn enabled)

Connection Timeout (in seconds)

15

Save Database Connection Settings

Cancel

- Click to select the **SSL Encryption** check box.
- Click the **Save Database Connection Settings** button.

**Note:** SQL Server must be pre-configured to support encryption. This [Microsoft TechNet article](#) explains how to configure the SQL Server environment for encryption. The SSL encryption used for communicating with SQL Server is either 40 or 128 bit, depending on the Windows operating system used.

**Note:** Using this setting can adversely affect [performance](#) (KBA). See this [TechNet article](#) for additional information.

## Manual IIS Installation

IIS is an internal part of the Windows operating system, and only needs to be enabled. If IIS is not found, the Thycotic Installer will install it for you. If you would prefer to install IIS manually, please refer to the instructions listed below for example steps in the Windows Server 2016 Operating System. For the most up-to-date setup instructions, see [Microsoft's Technical Documentation](#). Navigate to **Docs > Internet Information Services > Install**.

### Roles and Features

Thycotic products recommend the following roles and features to be installed on the SS IIS Server for maximum security and functionality options:

#### Roles

- Web Server (IIS)
- Web Server (IIS)\Web Server
- Web Server (IIS)\Web Server\Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
  - HTTP Redirection
- Web Server (IIS)\Web Server\Health and Diagnostics
  - HTTP Logging
- Web Server (IIS)\Web Server\Performance
  - Static Content Compression
  - Dynamic Content Compression
- Web Server (IIS)\Web Server\Security
  - Request Filtering
  - Windows Authentication
- Web Server (IIS)\Web Server\Application Development
  - .NET Extensibility 4.6
  - ASP.NET 4.6
  - ISAPI Extensions
  - ISAPI Filters
- Web Server (IIS)\Web Server\Management Tools

- IIS Management Console

## Features

- .NET Framework 4.x Features
  - .Net Framework 4.x
  - ASP.NET 4.x
- WCF Services
  - HTTP Activation
  - TCP Activation
  - TCP Port Sharing
- PowerShell
  - Windows PowerShell 5.1

## Step One: Windows Server 2012–2019 IIS Installation

To install Internet Information Services (IIS) Manager on Windows Server 2016, you will need to give your server the Web Server (IIS) role using the following procedure:

**Note:** If this is *not* the first time you have run the wizard (that is, when first installing IIS), the Web Server Role (IIS) and Role Services windows will not appear, and the wizard order changes a bit. Instead, role services are selectable in the Server Roles window.

1. Click the **Server Manager** button on your server. The Server Manager Dashboard appears.
2. Click the **Add Roles and Features** button. The Add Roles and Features Wizard on the Before You Begin window appears.
3. Click the **Next** button. The Select Installation Type window appears.
4. Click to select **Role-based or feature-based installation** selection button.
5. Click the **Next** button. The Select Destination Server window appears.
6. Ensure the **Select a Server from the Server Pool** selection button is selected.
7. In the **Server Pool** section, click to select your server.
8. Click the **Next** button. The Select Server Roles window appears.
9. Click to select the **Web Server (IIS)** check box.
10. Click the **Next** button. The Select Features window appears.
11. In the **Features** list, Click to select the following checkboxes (If necessary, click the **Add Features** button when prompted):
  - .NET Framework 4.x Features > WCF Services > **HTTP Activation**
  - .NET Framework 4.x Features > WCF Services > **TCP Activation**
12. Click the **Next** button. The Web Server Role (IIS) window appears.

13. Click the **Next** button. The Select Role Services Window appears.

14. In the **Roles** list, click to select the following check boxes:

**Note:** Leave all the auto-selected check boxes as is.

- Web Server (IIS) > Web Server > Common HTTP Features > **HTTP Redirection**
- Web Server (IIS) > Web Server > Performance > **Dynamic Content Compression**
- Web Server (IIS) > Web Server > Security > **Windows Authentication**

15. Click the **Next** button. The Confirmation window appears

16. Confirm your installation details.

17. Click the **Install** button. Wait for the installation to complete. The Results window appears.

18. Click the **Close** button. An IIS tile should now appear on your server.

**Note:** We recommend you run [Windows Update](#) to install the latest security patches for IIS once you have IIS installed.

## Step Two: Configure the IIS Website

Follow these steps to configure a website in IIS for SS:

1. Extract the SS files into C:\inetpub\wwwroot\SecretServer or your location of choice.
2. Open Internet Information Server (IIS) Manager: On the taskbar, click **Server Manager > Tools > Internet Information Services (IIS) Manager**.
3. In the Connections pane, expand the server name.
4. Click on the **Application Pools** node. The Application Pools window appears.
5. Click the **Add Application Pool** link. The Add Application Pool dialog box appears.
6. Type SecretServer in the **Name** text box.
7. Click to select **4.x** in the **.NET Framework Version** dropdown list.
8. Click to select **Integrated** in the **Managed Pipeline Mode** dropdown list.
9. Click the **OK** button to save the new application pool. The dialog box closes.
10. (optional) Customize the Windows account SS runs as:
  1. Right click the new application pool and select **Advance Settings...**
  2. Click the **Identity** setting in the **Process Model** section to select the desired account. Using this, you can, for example, set SS to use IWA to connect to SQL.
11. Expand the **Sites** node on the **Connections** tree.
12. Click on the Default Web Site node.
13. In the **Actions** pane, click **Bindings** to set your desired website. The Edit Bindings dialog box appears.
14. Edit or add bindings as desired. We recommend using HTTPS with a real SSL certificate.

15. Click the **Close** button.
16. In the **Connections** tree, expand the **Default Website** node.
17. **Either**, If you see the default folder, **SecretServer**, which you created earlier:
  1. Right click the **SecretServer** folder and select **Convert to Application**. The Add Application dialog box appears.
  2. Click the **Select...** button to choose the pool you created earlier for SS.**Or**, If you used a custom location instead:
  1. right click the Default Website. The Add Application dialog box appears.
  2. Type SecretServer in the **Alias** text box.
  3. Click **Select...** and pick the app pool created for SS.
  4. Type the path where you extracted the SS files in the **Physical Path** text box.
18. Click the **OK** button.

### Step Three: Ensure IIS Does Not Stop the Worker Process

When using IIS version 7.0 and above, by default, the worker process terminates after an inactive period. If SS is in its own application pool, that application pool will stop after a period of no requests. To ensure this does not happen, perform the following procedure. Additionally, by default, IIS launches a worker process when the first request for the Web application is received, so if the SS application takes a long time to start, issues can result. Thus, we recommend launching the SS application pool worker process as soon as IIS starts by setting the start mode to "AlwaysRunning."

Procedure:

1. Open **Internet Information Server (IIS) Manager**:
  - If you are using Windows Server 2012 or Windows Server 2012 R2: On the taskbar, click **Server Manager > Tools > Internet Information Services (IIS) Manager**.
  - If you are using Windows Server 2008 or Windows Server 2008 R2: On the taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name.
3. Click **Application Pools**.
4. Determine which application pool SS is running as:
  1. Expand **Sites** at the left.
  2. Find the website SS is running on.
  3. Click on the SS website or virtual directory (if it is running on one).
  4. Click **Basic Settings** on the right panel. This indicates SS's application pool.
5. Right-click the application pool and select **Advanced Settings...** The Advance Settings dialog appears.
6. In the **General** section, set **Start Mode** to **AlwaysRunning**.
7. In the **Process Model** section, set **Idle Time-out (minutes)** to **0**.

8. In the **Recycling** section, set **Regular Time Interval (minutes)** to **0**.
9. In the **Recycling** section, click the › next to **Specific Times** to ensure there are no times set. If there are, click the ... to clear them.
10. Leave IIS Manager open—we will return to it below.

#### **Step Four: Ensure the User Profile Always Loads**

As of version 10.2, SS requires its application pool "Load User Profile" setting enabled. Otherwise, SS reports a critical alert to system admins.

**Note:** Even without the setting enabled, SS loads to give access to secrets but many internal operations may malfunction, so we recommend resolving this issue as soon as possible.

Procedure:

1. Right-click the SS application pool in IIS Manager and select **Advanced Settings...** The Advance Settings dialog appears.
2. Go to the **Process Model** section in the **Advanced Settings** dialog.
3. Set **Load User Profile** to **True**.
4. Preform an `iisreset` on the server (in an administrator command prompt).

## Running the IIS Application Pool As a Service Account

### Overview

We recommend setting up a domain service account that can both access the Thycotic product's SQL database and 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. Granting the service account access to the SQL Server database.
3. Assign the service account as the identity of the application pool or pools in IIS.
4. Grant folder permissions for the service account on two folders.
5. Configure User Rights Assignment to the service account.

### Procedure

**Note:** You must have IIS installed on your Web server before completing these steps.

#### Task 1: Creating a Domain Service Account

1. Create a local or domain user account (or identify one to use).
2. Open IIS (**Search > inetmgr**) on your Web server.
3. Open the **Active Directory Users and Computers** link from **Administrative Tools**.
4. Click to open the directory where you want to assign this account, such as testlab.com.
5. Select **Service Accounts**.
6. Right click and select **New > User**. The "New Object - User" wizard dialog box appears.
7. Type a name and logon name for the service account.
8. Click the **Next** button. The wizard advances to the next dialog box (same name).
9. Type a password in the Password and Confirm Password text boxes.
10. If necessary, click to deselect the **User must change password at next login** check box.
11. Click to select the **Password never expires** check box. Failing to do this could lock the account out of SS.
12. " Check **Password never expires** or the account could lock you out of SS.
13. Click **Next** button.
14. Click the **Finish** button. You can now give the account access to the database server and the application server.

#### Task 2: Granting Access to the SQL Database

**Note:** You must have SQL installed on your database server before completing these steps.

Grant access:

1. Open the SQL Management Studio on your database server.
2. Connect to your Thycotic product's SQL database using an administrator account.
3. Click to select the Security folder in the Object Explorer.
4. Right-click the same folder and select **New > Login...** A log on dialog box appears.
5. Ensure the **Windows Authentication** radio button is selected.
6. Click the **Search...** button. The "Select User, Service Account, or Group" dialog box appears.
7. Ensure that your domain or AD server appears in the **From this location** text box. If not, click the **Locations...** button and select it.
8. Type the login name you created for your Thycotic service account, such as svc\_thycotic, in the **Enter the object name to select** text box.

9. Click the **Check Names** button.
10. Click to select the correct account.
11. Click the **OK** button. The dialog box closes, returning you to the Login - New dialog box.
12. **Either**, if you have already created the database for your Thycotic product:
  1. Click **User Mapping** in the **Select a page** list box.
  2. Click to select the check box for the database in the **Users mapped to this Login** list.
  3. Click to select the **db\_owner** check box in the **Database role membership...** list.
13. **Or**, if you have not yet created the database:
  1. Click **Server Roles** in the **Select a page** list box.
  2. Click to select the **db\_creator** check box.
14. Click the **OK** button.

### Task 3: Assigning the Identity of Application Pools

1. Click the **Applications** node under the server name in the **Connections** tree.
2. Right-click the node and select **Advanced Settings...** The Advance Settings dialog box appears.
3. Click the ... button for the **Identity** entry in the **Process Model** section. The Application Pool Identity dialog box appears.
4. Click to select the **Custom Account** selection button.
5. Click the **Set...** button. The Set Credentials dialog box appears.
6. Type your service account's name, such as test and password.
7. Click the **OK** button. The dialog box closes.
8. Open the command console as an Admin.
9. Change the directory to your .NET framework installation directory using the "cd" command, for example,  
C:\Windows\Microsoft.NET\Framework\v4.0.30319.
10. Type `.aspnet_regiis -ga <domain name>\<username>`, replacing <domain name> and <username> with your information. For local accounts omit the domain name parameter.

### Task 4: Granting Folder Permissions

**Note:** You must have the Thycotic product application files installed (on your Web server) before completing this section.

Following the steps below, you give the service account "Modify" access to **two** folders:

- C:\Windows\TEMP
- The folder where your Thycotic product's application files are located, such as C:\inetpub\wwwroot\SecretServer

Procedure (for each folder):

1. In a file manager, navigate to the SS application folder.
2. Right-click the folder and select **Properties**. The Properties dialog box appears.
3. Click the **Security** tab.
4. Click the **Advanced** button.
5. Click the **Add** button. A permissions panel appears.
6. Click the **Select a Principal** link. The "Select User, Computer, Service Account, or Group" dialog box appears.
7. Ensure that your domain or AD server appears in the **From this location** text box. If not, click the **Locations...** button and select it.
8. Type the login name you created for your Thycotic service account, such as svc\_thycotic, in the **Enter the object name to select** text box.
9. Click the **Check Names** button.
10. Click to select the correct account.
11. Click the **OK** button. The dialog box closes, returning you to the permissions panel.
12. Click to select the **Modify** check box in the **Basic Permissions** section. Your service account should have the **Modify, Read & Execute, List folder contents, Read**, and **Write** permissions selected for this folder
13. Click the **OK** button.

14. Click the **Apply** button.

**Note:** If a Windows Security pop-up appears, click the **Yes** button. 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.

## Task 5: Configuring User Rights

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 or locally on your IIS Web server using the Local Security Policy Console. See [User Rights Assignment](#) to learn more.

### Option 1: Setting User Rights Assignment on the Domain

**Note:** This is an example of how to create a Group Policy Object (GPO), we recommend consulting with your organizational group policy administrator to create this policy.

**Note:** This overwrites any configuration in the local security policy. The local security policy is a safer option if you are not sure about usage across your domain.

1. Open the Group Policy Management Console.
2. Right-click the desired GPO folder (under the domain node) in the **Group Policy Management** Tree, and select **New**. The New GPO dialog box appears.
3. Type the name, such as “Thycotic User Rights Assignment,” in the **Name** text box.
4. Click the **OK** button. The dialog box closes.
5. Right-click the GPO you just created and select **Edit**. The Group Policy Object Editor appears.
6. On the **Computer Configuration** node, click to expand **Policies > Windows Settings > Security Settings > Local Policies**.
7. Click to select the **\*\*User Rights Assignment\*\*** folder.
8. Repeat the following procedure for the “Log on as a batch job” and “Impersonate a client after authentication” permissions (for this instruction we show the former):
  1. In the list on the right, right-click **Log on as a batch job** and select **Properties**. The “Log on as a batch job Properties” dialog box appears.
  2. Ensure that the **Define these policy settings** check box is checked.
  3. Click the **Add User or Group** button. A dialog box appears.
  4. Add your Thycotic service account.
  5. Click the **OK** button. The dialog box closes. The new policy appears in the list.
  6. Click the **Apply** button.
9. Link your new GPO to the OU where your Thycotic product machine accounts exist, that is, the Web and database servers.

### Option 2: Setting User Rights Assignment Locally

1. On the Web server hosting IIS and your Thycotic Application files, open the “Local Security Policy Console” as an administrator (Run as administrator).
2. On the Local Policies node, click to expand **Local Policies > User Rights Assignment**.
3. Click to select the **\*\*User Rights Assignment\*\*** folder.
4. Repeat the following procedure for the “Log on as a batch job” and “Impersonate a client after authentication” permissions (for this instruction we show the former):
  1. Right-click on **Log on as a batch job** in the list on the right and select **Properties > Add User or Group**.
  2. Click to select your Thycotic service account.

3. Click the **OK** button.

**Note:** If you get a "Service Unavailable" error after applying "Log on as a batch job" permissions, try updating your group policy settings: Open the **Command Console**, type in `gpupdate /force**`, and restart the **Windows Process Activation Service**.

## Advanced (Manual) Installation

### Procedure

#### Step 1: Downloading the Secret Server Application Files

**Important:** Ensure you have the IIS, .NET Framework, and SQL Server prerequisites installed before following the steps below.

Go to the [download page](#) to get a .zip file that contains both Secret Server and Privilege Manager files in the manual installation section. Use this .zip file for the instructions below.

#### Step 2: Creating Folders and Extracting Contents

1. Extract the contents of the .zip file downloaded above (Right-click, **Extract All...**). The original file is named with the latest version number for SS.
2. Extracting this file reveals a nugetCache folder, as well as another zipped folder named ss\\_update. For a SS-only install, you will not need the contents of the nugetCache folder.
3. Create a folder called SecretServer in the location C:\inetpub\wwwroot\.
4. Extract the contents of the ss\\_update.zip file (Right-click, **Extract All...**) to C:\inetpub\wwwroot\SecretServer.

#### Step 3: Configuring IIS

Open Internet Information Services (IIS) Manager\* and create a new application pool:

**Note:** Our IIS installation sets the .NET trust level to "Full (internal)", which may affect other applications on the server.

1. Right-click **Application Pools** and select **Add Application Pool...**
2. Type a name (for example, SecretServerAppPool).
3. Ensure that the highest .NET CLR version is selected.
4. Ensure the Managed pipeline mode is set to **Integrated**.
5. Click the **OK** button.

**Note:** The SS installer sets the application pool to default to the system Network Service account. Follow [these instructions](#) if you selected Windows Authentication Mode during the SQL Installation process. To use Windows Authentication you must use an Active Directory service account to run the application pool in IIS. We recommend this as a security best practice.

6. Follow [these instructions](#) to set the Idle Timeout and Regular Timeout settings to 0 for the application pool in IIS.
7. Install SS as either a virtual directory (4a) or as a website (4b):

#### Step 4a: Installing Secret Server as a Virtual Directory

1. Right-click **Default Web Site** and select **Add Virtual Directory...**
2. Select an alias for your Secret Server. The alias is appended to the website, and it is best to name it the name of your earlier unzipped folder. For example, SecretServer becomes https://myserver/SecretServer.
3. Select the physical directory for where you unzipped SS, for example, C:\inetpub\wwwroot\SecretServer.
4. Click the **OK** button.

5. In the tree, right-click the new virtual directory and select **Convert to Application**.
6. Set the **Application Pool** to the same one you created in the Manual Installation section, for instance, SecretServerAppPool. Secret Server is now ready for installation. Skip to Step 5.

#### Step 4b: Installing Secret Server as a Website

1. In IIS, right-click **Sites** and select **Add Website...**
2. Type a site name.
3. Click **Select...** and choose the application pool you created in the Manual Installation section.
4. Click the **OK** button.
5. Click the ... button beside the **Physical path** field and select the directory containing the unzipped SS files, for example  
C:\inetpub\wwwroot\SecretServer.
6. Click the **OK** button.
7. Click the **OK** button at the bottom of the **Add Website** window to save your settings. Secret Server is now ready for installation.

#### Step 5: Completing Secret Server Installation from the Website

Your SS advanced installation is now ready to complete:

1. Open a browser and navigate to where your Secret Server is located, such as <http://localhost/secretserver>. You should arrive at a page that says "Secret Server (Not Installed or Unable to Access the Database)."
2. Click the **Install Secret Server** button.
3. On the **SQL Server Location** page, specify the server name of your SQL Database Server, `DatabaseMachineName\InstanceName` and then the database name that you created in SQL for SS.
4. If you are using Windows authentication mode to access SQL (recommended), ensure the correct service account is listed.
5. If you selected mixed mode during the SQL install, select **SQL Server Authentication** and enter the SQL username and password you created for the SQL account. For information about adding a SQL Server user, see the [Adding a SQL Server User](#) (KB).
6. Click the **Install Secret Server** button. Secret Server verifies it is able to successfully create the SS database. If an error occurs no database changes will be made.

**Note:** Secret Server attempts to download and install the latest version from the Internet. If you do not have an active Internet connection on your Web server, SS will continue to install the version from your downloaded application files.

7. The install may take a few minutes to complete. Once successful, click the **Return to Home** button.
8. Create a username and password for the administrator account for SS and store these credentials in a safe location.
9. Click the **Create User** button and log on after entering the username and password.
10. Once logged on SS, you are prompted with the Getting Started wizard. The wizard guides you through adding your Licenses, setting up an email server, and creating your first group.

**Note:** If you skipped the wizard and would like to return, go to **HELP > Getting Started** from the top menu.

SS is now installed. See our [Getting Started Tutorial](#) or contact Thycotic Support about training.

#### Troubleshooting Notes

- If the database name you provide does not yet exist in the specified instance of SQL Server, SS attempts to create the database using the SQL or Windows account you have specified. For that account to create a database, it needs to have the dbcreator server role in

SQL Server.

- If using Windows authentication mode (recommended) you need to use a service account to run SS's application pools with appropriate permissions. See [this article](#) if you have not already done so.

## Basic (Automatic) Installation

### Introduction

This is the installation guide for Windows Server 2016 and Windows 10. For other operating system installation guides, [contact Thycotic Support](#).

### Secret Server Is an ASP.NET Website

Secret Server is installed as an ASP.NET website. The setup.exe file sets up the website with the correct permissions and creates the settings in IIS.

### SQL Server Is Usually Required

Secret Server requires an instance of SQL Server for the database backend and is 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.

### Administrative Access

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

### Review the Prerequisites

**Important:** Except for the operating system, the following prerequisites are installed automatically by our installer. If you already have some of them installed or wish to install them yourself, the installer will skip over them.

If this is the first time you are installing Secret Server, please take the time to review the [full list of system requirements and recommendations](#).

### System Requirements Overview

- Windows Server 2016 operating system
- Microsoft SQL Server 2008 or greater (any edition)
- Microsoft Internet Information Services (IIS)
- Microsoft .NET Framework 4.6

**Note:** Windows Server 2016 and Windows 10 come with the .NET Framework 4.6 already installed.

### Additional Recommendations

We suggest you:

- Use an SSL certificate for Secret Server.
- Run [Microsoft Update](#) on your server to make sure all components are up to date.

### Procedure

#### Step 1: Downloading the Latest Version of Secret Server

The latest version of SS is available for [download](#). A setup.exe file is downloaded to your machine. We recommend running setup.exe as an administrator.

## Step 2: Running the Installer

### Welcome Page

The first installer page you are presented is the Welcome Page. The installer should detect whether the machine has SS or Privilege Manager for Windows and will declare which of those products it will install.

### Database Page

The Database page allows you to choose to install SQL Express or connect to an existing SQL Server. If you select SQL Express, the installer requires Internet access to download the installation for SQL Server Express.

If Internet access is not available, a link to download SQL Server Express is presented. You are expected to install SQL Server Express and then restart the installer.

If Internet access is available, SQL Server Express is installed.

### Pre-Requisites Page

The Pre-Requisites page ensures everything that is required to install SS is setup correctly. Everything on this page *can* be installed outside of the installer. If not, the installer installs and configures them for you. This page is primarily for third party server configuration. If there are issues, please refer to support for the specific non-Thycotic vendors.

### Database Connection Page

The Database Connection page contains the connection information that Secret Server (and Privilege Manager) uses. You must click the **Test Connection** button and have a successful result before installation can continue.

### Create User Page

The Create User page is where you enter the information for the initial SS user.

### Email Server Page

Enter connection information for the email server on this page. This is also optional and you can skip it and set it up later in SS. This page will configure email for both Secret Server and Privilege Manager for Windows.

### Review Page

Review the, mostly default, settings on the Review page, and change them if needed. Some of the settings are validated before the install can begin.

### Install Page

The Install page shows the status from log files as both Secret Server and Privilege Manager are installed.

## Step 3: Reviewing the Log Files (Optional)

After the applications are installed, the installer opens a Web browser to the Secret Server log on page. At this point, everything is installed to start using both Secret and Privilege Manager. If the installation failed or you wish you view the logs from the installation, click the **View Log Files** button.

## Step 4: Opening Secret Server

If the setup.exe did not automatically open a browser, navigate to where SS is located, for example: <http://localhost/secretserver>.

## **Step 5: Learning Secret Server**

See our [Getting Started Tutorial](#) or contact Thycotic Support about training.

## Installing and Configuring SQL Server

For step-by-step instructions on how to install SQL 2016, see our example [SQL 2016 Installation guide here](#).

Secret Server requires Microsoft SQL Server as the back-end database. All editions including the Express version of 2012–2017 are supported.

Setting up SQL Server requires:

- Installing SQL Server
- Creating a SQL Account
- Configuring database access in Secret Server
- Installing SQL Server

**Note:** If you are using SQL Express make sure to get the edition with tools that will include SQL Management Studio. Follow the link in the KB article [Download SQL Express with Tools](#).

### Creating a SQL Account

#### SQL Authentication

The fastest method to get started with Secret Server is to create a SQL Authentication account. Follow the instructions in the Database section of the [Installation Guide](#).

For troubleshooting and configuring SQL installation on a different server than the application server see [SQL Authentication Configuration](#) article.

#### Windows Authentication

A more advanced way to have Secret Server access the SQL server would be through a service account and using Windows Authentication. Because of the requirement of a service account and added IIS settings, we only recommend this for non-evaluation setups. See instructions in [Accessing MS SQL Server with IWA](#).

### Configuring Database Access in Secret Server

Once the account has been created and SQL server installed with the MSI. The third step of the Web installer will ask for database access information.

#### SQL Location

- **Server Name or IP:** If it is a local machine the server name will be (local) or localhost for the default instance, or if a named instance such as SQL Express it would be localhost\SQLEXPRESS. If you are unsure, copy the value from the "Server name" text box when connecting through SQL Management Studio.
- **Database Name:** If you have created a database, enter the name. If you have given the SQL account dbCreator permission, enter a database name for Secret Server to create.

#### SQL Authentication

- **SQL Server Authentication:** Implies a SQL account has been created that exists only with SQL Server. The account will need to be dbOwner on the database or need dbOwner permission to create the database. This is recommended for quickest setup. For more detailed information and troubleshooting see [SQL Authentication Configuration](#) article.
- **Windows Authentication:** The identity of the application pool will access the database. This requires a domain Service account that has been granted access to run ASP.Net and the database. This is an advanced setting that is not recommended for evaluations.

Follow the instructions on using a service account in [Accessing MS SQL Server with IWA](#).

## Installing RabbitMQ

### Overview

#### What is RabbitMQ?

RabbitMQ is a robust message queuing software package that Secret Server uses to communicate with its distributed engines. For detailed information about RabbitMQ go to <https://www.rabbitmq.com/>

#### Why do you need to install it?

RabbitMQ is an enterprise-ready alternative to MemoryMQ. While MemoryMQ is sufficient for basic and prototyping installations, RabbitMQ is the preferred messaging framework when the need for greater reliability and clustering arises.

#### RabbitMQ and Encryption

All data sent from or read by Secret Server from RabbitMQ is encrypted. If you would like to add SSL despite the data already being encrypted, please follow the "Advanced installation of RabbitMQ with TLS" use case. Please note that Thycotic Support can help with non-SSL installations. For SSL installation, configuration, troubleshooting, and RabbitMQ clustering, please contact [Thycotic Professional Services](#) to learn more about our Professional Services rates.

#### Prerequisites

**Important:** Secret Server only supports RabbitMQ on Windows operating systems.

RabbitMQ requires:

##### General

- Windows Server 2008 or higher with PowerShell v3 support
- Nodes hosting RabbitMQ need a minimum of 2 GB RAM
- Nodes hosting RabbitMQ should have at least 128 MB of memory available at all times
- Disk space is not an issue, but it should not go below 50 MB (default value), especially if you host RabbitMQ on the same server as SS
- Minimum 2 vCPUs
- Ports 5672 (non-SSL) or 5671 (SSL) opened on the machine and firewall

##### SSL Certificate

- A server certificate PFX type and a root certificate authority certificate CER type.
- The PFX certificate should have:
  - A name that matches the RabbitMQ Fully qualified machine name
  - If you plan on making a RabbitMQ cluster, add DNS names (SANs) to your certificate
  - Your certificate must be an RSA certificate. CNG is not supported and will cause the installation to fail.
- If you do not have an internal PKI and prefer not to use a public certificate, you can use a self-signed certificate.

**Note:** Thycotic will not assist with creating or troubleshooting self-signed certificates.

### Installation

#### Task 1: Secret Server

In Secret Server UI

1. Navigate to **Admin > Distributed Engine**.
2. Click the **Manage Site Connectors** button. The Manage Site Connectors page appears:

### Manage Site Connectors

< 1 to 2 of 2 >

SITE CONNECTOR	ACTIVE	VALIDATED	QUEUE TYPE	HOST	VERSION
Default MemoryMq Service	Yes	No	MemoryMq	QA-CUST-01	5.0.0.40
RMQ_for_BUG169089	Yes	No	RabbitMq	EARTH.solar.local	Unknown

☐ Show Inactive

← Back
+ New Site Connector

3. Click the **+ New Site Connector** button. The Site Connector Details page appears:

### Site Connector Details

Queue Type

Memory MQ

Name

Active

☒

Use SSL

☐

Host Name

Port

8672

Save


Cancel


4. Click to select **Rabbit MQ** in the **Queue Type** dropdown list.
5. Type a name for your new site connector in the **Name** text box.
6. Click to select the **Active** check box.
7. Type the host name of the machine where you plan to install RabbitMQ in the **Host Name** text box.

**Note:** The Engines need to be able to resolve this host name or the connection will fail. Also, inbound firewall rules must be created on the machine that is hosting the connector.

8. Type either port 5672 (non-SSL) or 5671 (SSL) in the **Port** text box.
9. Click the **Save** button.
10. After the site connector is created, click the site connector's link. The Site Connector Details page appears:

### Site Connector Details


Connectivity has not been validated.


To be included in the mailing list about updates to MemoryMq, please send an email to [MemoryMQ@thycotic.com](mailto:MemoryMQ@thycotic.com).

Queue Type MemoryMq





Name Default MemoryMq Service


Active Yes

Use SSL No

Host Name QA-CUST-01


Port 8672


 Back
 Edit
 View Credentials
 Download Site Connector Installer


 Validate Connectivity


- Click the **View Credentials** button to retrieve the automatically generated credentials. The Site Connector Credentials popup appears. You can ignore the informational message that the connectivity has not been validated for now as you will be doing so after you install RabbitMQ on the host you have selected.

### Site Connector Credentials


These credentials are automatically used by the Site Connector and by Engines that use this Site Connector.

User Name  eFAQUJzHtIHUtdnD05YME0ZOLxF8qggv09OqAVfJudDpxJVIBEr0gAzGG-7nz5F

Password  FHkdCq6gSRlt3OL4Vcb1x9EZDyggqJe8rho5R1hDjtxaitnaTYoya4HQQu4M3U0

 OK

- Click the copy icons to copy both the **User Name** and **Password**, and store them for use in the next section.
- Click the **OK** button.

## Task 2: RabbitMQ Host

- Download the [Thycotic RabbitMQ Helper](#).
- Install the Thycotic RabbitMQ helper by running the downloaded MSI.
- Review the supported [installation scenarios](#).
- Navigate to the installation folder in %PROGRAMFILES%\Thycotic Software Ltd\RabbitMq Helper
- Launch the Thycotic.RabbitMq.Helper.exe, which opens the Windows PowerShell.
- Then, issue a cmdlet command from the scenario that applies to your need.
- After installation completes, the helper opens a Web browser to the RabbitMQ management console. There is no need to interact with the site at this time, so you can minimize or close the page for now.
- Return to SS, and go to the site connector you created in the previous section.
- Click the site connector's link. The Site Connector Details page appears.

10. Click the **Validate Connectivity** button.
11. If everything is set up correctly, you will see "Validation Succeeded."
12. If you see "Validation Failed," do the following:
  1. Ensure the RabbitMQ Windows service is running.
  2. Check the logs found under C:\Program Files\Thycotic Software Ltd\RabbitMq Site Connector\log.
  3. Check the SS system log for a full error report.

## Troubleshooting

Please refer to [RabbitMQ Helper](#).

## SQL Server 2014 Express Edition Installation

### Overview

**Important:** Thycotic recommends using SQL Express in sandbox or trial environments **only** due to size and performance limitations.

SQL Express is a free edition of SQL and is available for use with Thycotic products. The following steps walk you through setup and configuration for SQL Server 2014 Express Edition as an example. For the most up to date resources on installing SQL see [Microsoft SQL Technical Documentation](#) for more information.

At the completion of this article you will have:

- Installed a basic stand-alone instance of SQL Server 2014 Express with the minimum features necessary for SQL Server. This includes SQL Server Management Studio and other tools.
- Created a database in SQL for your Thycotic product
- Created a new SQL Server user login for your SQL database

**Note:** This document uses Thycotic's Secret Server product as example in the instructions, but the same steps apply for Privilege Manager advanced installs.

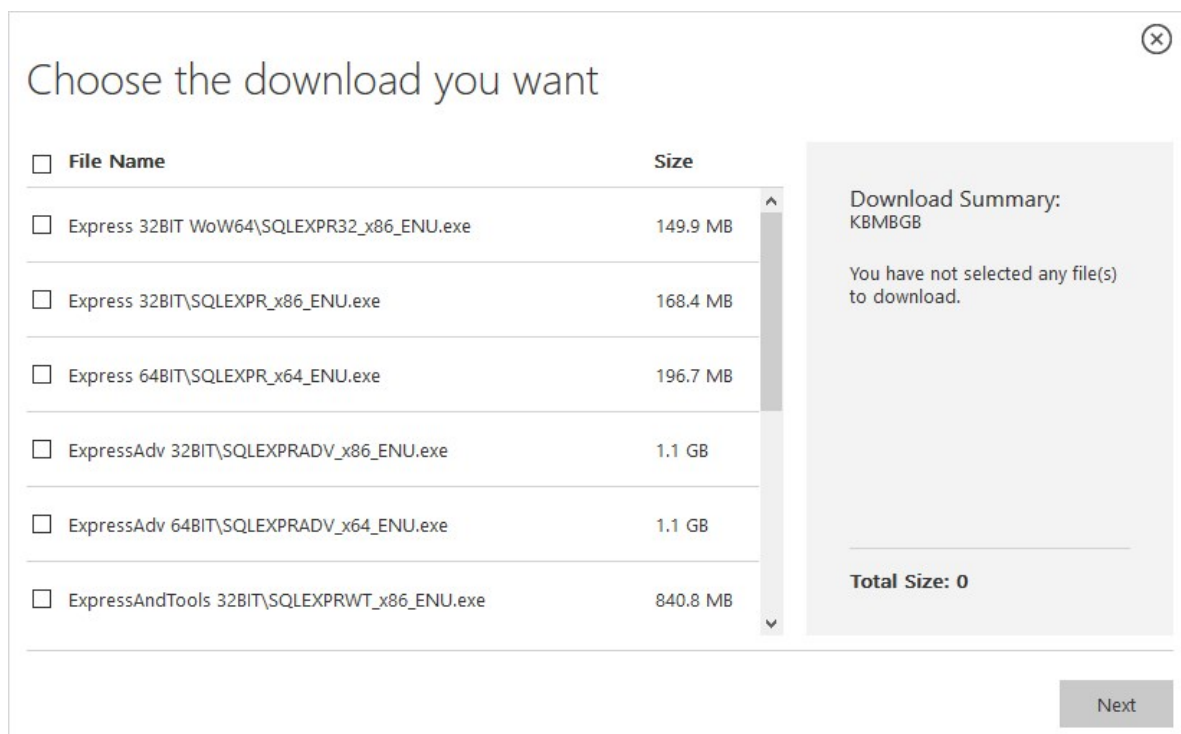
### Procedures

#### Downloading SQL Server Express with Tools

If you plan to use SQL Server Express, we strongly recommend downloading the package that includes **Tools**. This also installs SQL Server Management Studio that allows you to connect to the database directly and gives access to server settings.

Procedure:

1. Go to the [SQL Server 2014 Express download page](#).
2. Click the **Select Language** list box and select **English**.
3. Click the **Download** button. A popup page appears:



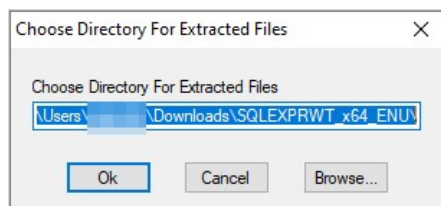
4. Click to select the following check boxes (you may need to scroll down):

- **ExpressAndTools 64BIT\SQLEXPRWT\_x64\_ENU.exe**
- **MgmtStudio 64BIT\SQLManagementStudio\_x64\_ENU.exe**

5. Click the **Next** button. SQLEXPRWT\_x64\_ENU.exe and SQLManagementStudio\_x64\_ENU.exe\* download to your computer.

## Installing SQL Server Express 2014

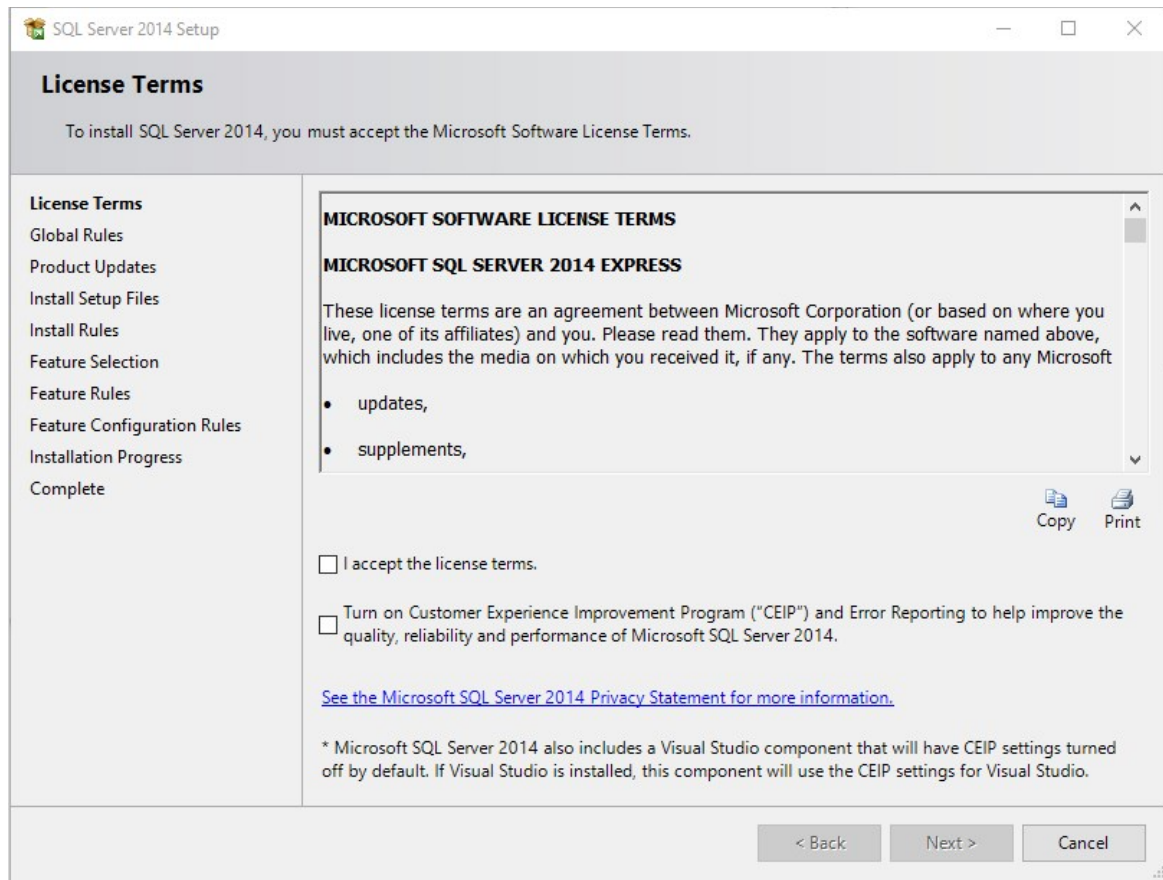
1. If necessary, download and install the latest version of .NET Framework. See [Microsoft .NET Framework 4.8 offline Installer for Windows](#) for the latest version as of when this topic was written. If you have already installed Secret Server, you have already done this.
2. Double click the SQLEXPRWT\_x64\_ENU.exe you downloaded to run it. The User Account Control appears.
3. Click the **Yes** button. The Choose Directory... dialog box appears:



4. Click the **OK** button. The files are extracted to that location, and the SQL Server Installation Center appears:

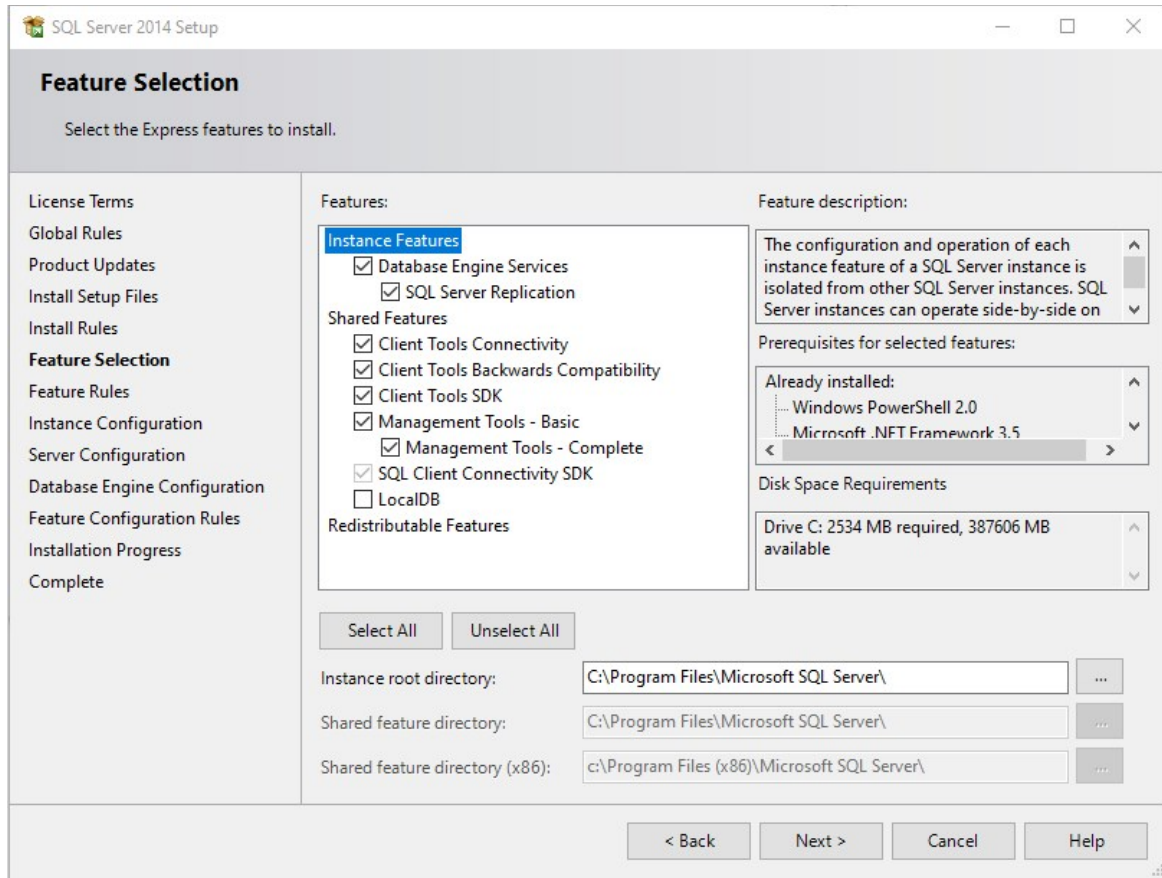


5. Click the **New SQL Server stand-alone...** link. The License Terms wizard page appears:



6. Click to select the **I accept the license terms** check box.

7. Click the **Next >** button. The installation processes four pages with no input from you and stops on the Feature Selection page:



8. Ensure that the **Database Engine Services** and **Management Tools – Basic** check boxes are selected. Leave the others as is.

**Note:** A SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

**Note:** Management tools include Management Studio support for the database engine and SQL Server Express, SQL Server CLI (SQLCMD), SQL Server PowerShell provider, and the distributed replay administration tool.

9. Click the **Next >** button. The installation processes one page with no input from you and stops on the Instance Configuration page:

**SQL Server 2014 Setup**

## Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

License Terms  
Global Rules  
Product Updates  
Install Setup Files  
Install Rules  
Feature Selection  
Feature Rules  
**Instance Configuration**  
Server Configuration  
Database Engine Configuration  
Feature Configuration Rules  
Installation Progress  
Complete

☐ Default instance

☒ Named instance:

Instance ID:

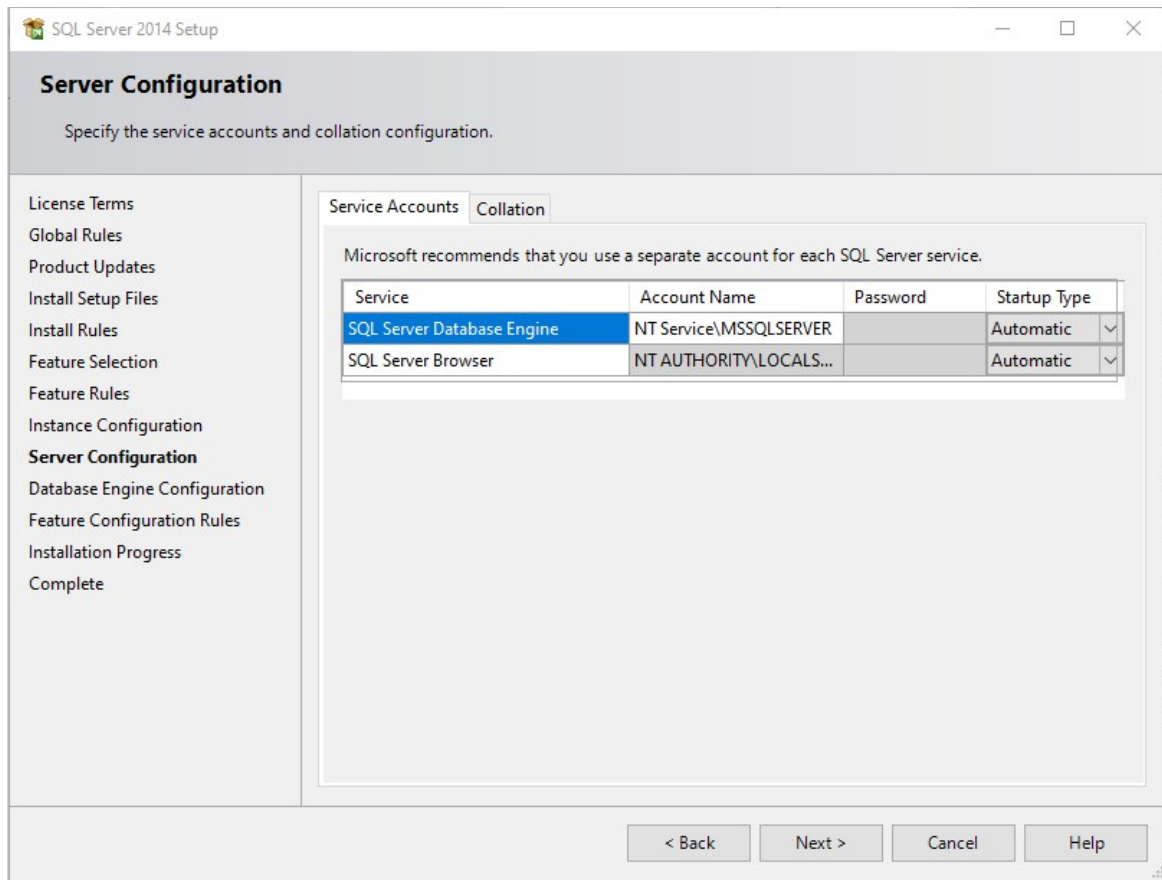
SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL12.

Installed instances:

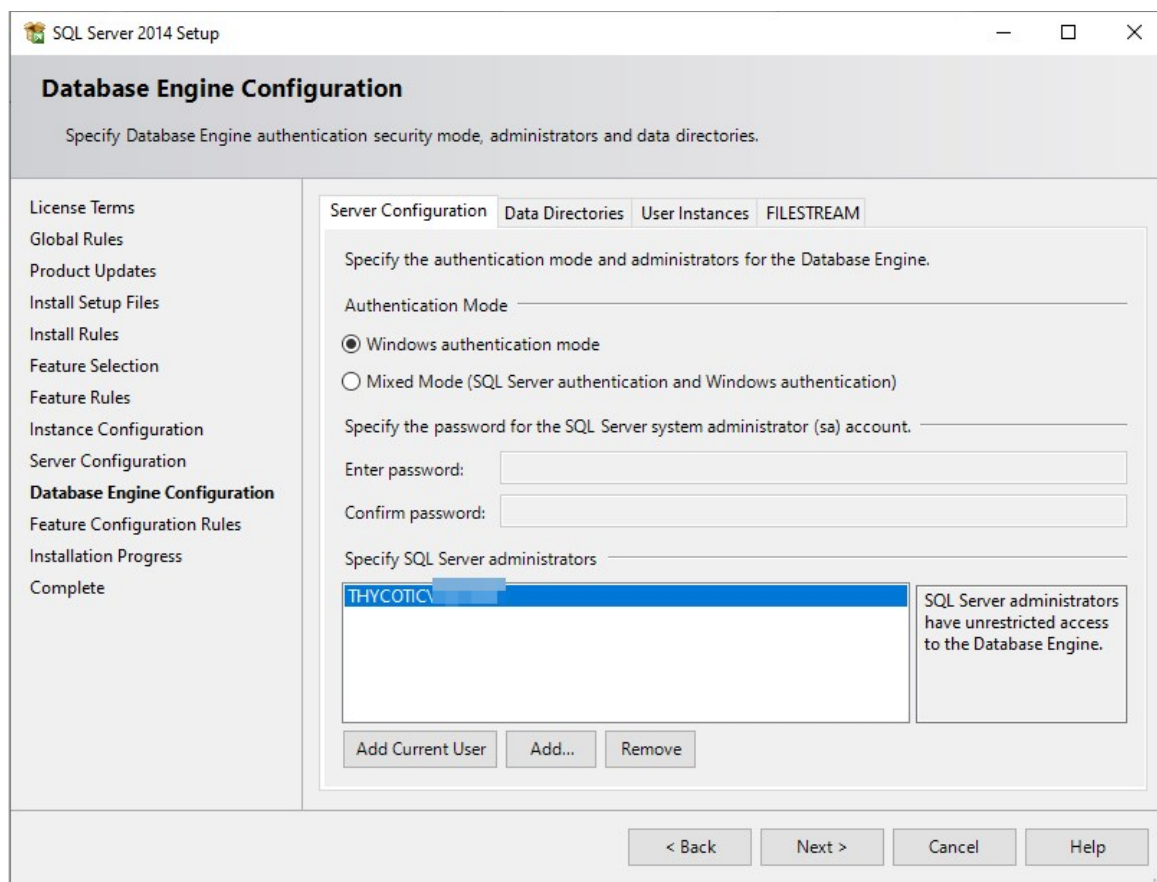
Instance Name	Instance ID	Features	Edition	Version
SQLEXPRESS	MSSQL14.SQLEXPRESS	SQLEngine_VNext	Express	14.0.2027.2

< Back   Next >   Cancel   Help

10. **Ether** click to select the **Default instance** selection button, which uses an already present instance called SQLEXPRESS.
11. **Or** type your desired name in the **Named instance** text box.
12. Type your instance ID in the **Instance ID** text box. We chose MySQLInstance. The instance ID will become part of the installation path.
13. Click the **Next >** button. The Server Configuration page appears:



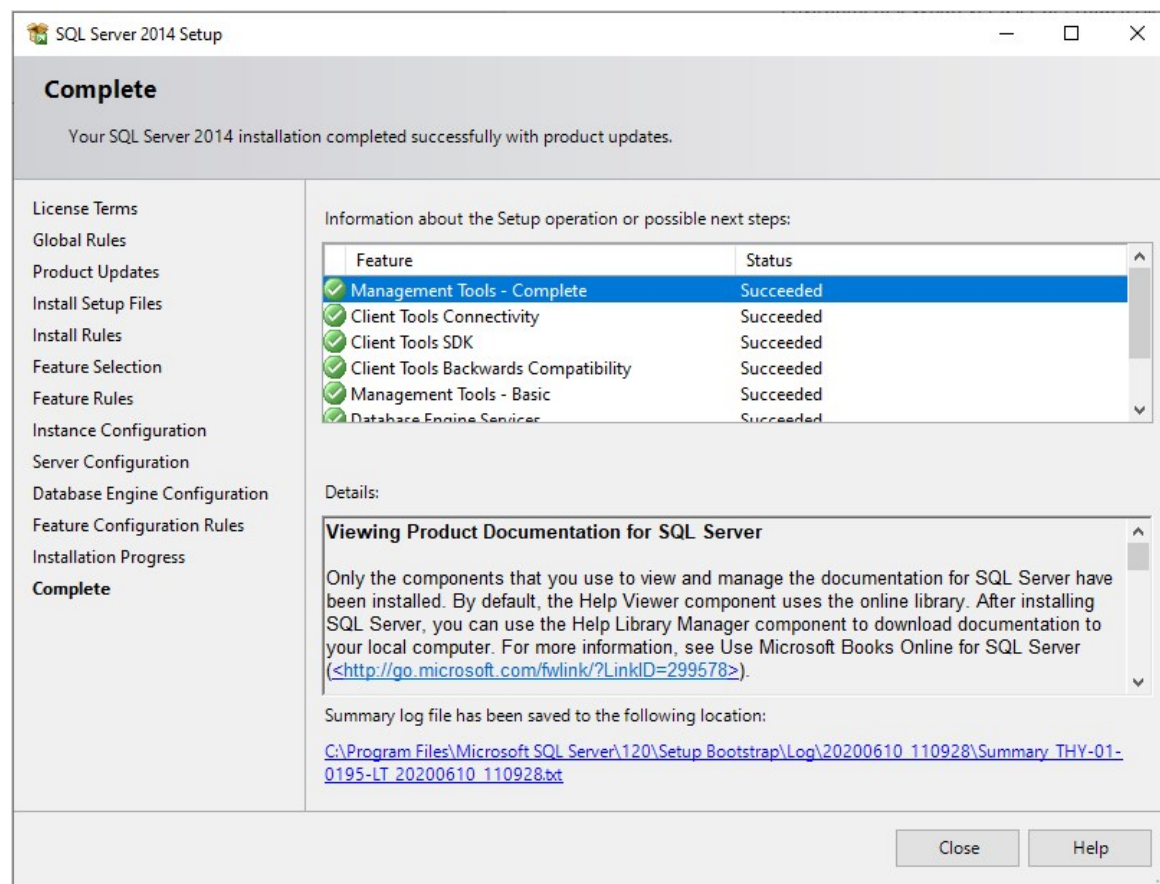
14. Leave the page as is, and click the **Next >** button. The Database Engine Configuration page appears:



15. You have the choice to select either **Windows Authentication Mode** or **Mixed Mode**. Click to select the option that works best for your environment:
  - **Mixed Mode (for easiest configuration)**: This mode is required if you intend on using a SQL Server account to authenticate Secret Server to your SQL Server instance. **We recommend using mixed mode if you are setting up a test or demo environment.** Selecting this option will also require you to set a password for the SQL Server system administrator (sa) account. See [Adding a SQL Server User](#) (section below) for instructions on adding more users.
  - **Windows Mode (recommended for best security)**: This mode prevents SQL Server account authentication. We recommend using Windows mode for production environments. Whatever user or group assigned will have administrative access to your SQL instance. According to best security practices, limit this number to as few users as possible. Only choose this if you have experience and require this for a specific issue—we do **not** recommend SQL Server Express for production accounts.

**Note:** If choosing **Windows Mode** you will also need to [run the IIS application pool as a service account](#) later in the installation process.
16. If you selected mixed mode, which you almost certainly did, type your SQL Server system administrator (sa) account password in the **Enter password** and **Confirm password** text boxes. The password must meet Microsoft's definition of a strong password. Click the **Help** button and search for "Database Engine Configuration - Account Provisioning" if you want to find out what that is. A 16 character mixture of lower and uppercase letters and numerals works fine.
17. Your user account should already be shown in the **Specify SQL Server administrators** text box. If not, click the **Add Current User** button.
18. Click the **Next >** button. The Installation Progress page appears and SQL Server Express is installed. This can take awhile. Eventually,

the Complete page appears:



19. Click the **Close** button.

## Creating the SQL Server Database

To install SS, the Thycotic installer creates the SQL database for you if it does not exist and if the user account has permission to create a new database, which requires the dbcreator server role.

If not using the Thycotic Installer, use the following steps to create a database manually through SQL Server Management Studio:

1. Open SQL Server Management Studio.
2. Connect to your SQL Server instance.
3. Right click the **Databases** folder and select **New Database...** The New Database page appears.
4. Type a name for your database in the **Database Name** text box.
5. Click the **OK** button.

## Adding a SQL Server User

According to security best practices, limit the number of users with access to your SQL database as much as possible. Use the following instructions to add a SQL Server account for SS to use to access the SQL database:

1. Open SQL Server Management Studio.
2. Connect to your SQL Server Database.

3. Expand the **Security** folder.
4. Right-click the **Logins** folder and select **New Login...**
5. Select a method of authentication:
  - **SQL Server Authentication:** Use this option to create a new SQL Server account (this requires mixed mode to be enabled). To create the account, enter a new username and password and then deselect the **Enforce Password Policy** check box to prevent the account from expiring.
  - **Windows Authentication:** Use this option to add access to SQL Server for an existing Windows account. To add the account, enter the login name or click **Search** to find the account. It is recommended to use a domain account rather than a local Windows account.
6. Click **User Mapping** in the left menu.
7. Click to select the check box next to your SS database.
8. In the **Database Role Membership** window, click to select the **db\_owner** check box.
9. Click the **OK** button.

## SQL Server 2016 Standard Edition Installation

### Overview

The following steps walk you through setup and configuration for SQL Server 2016 Standard Edition as an example. For the most up to date resources on installing SQL see [Microsoft SQL Technical Documentation](#) for more information.

At the completion of this article you will have:

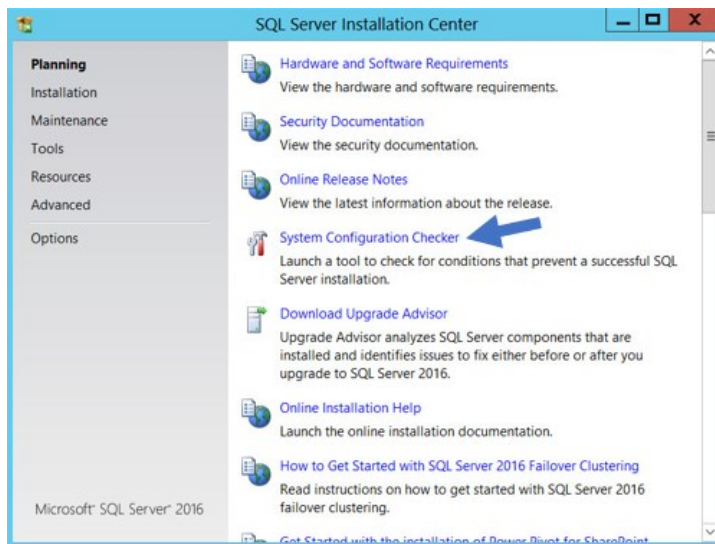
- Installed a basic stand-alone instance of SQL Server 2016 Standard with the minimum features necessary for SQL Server.
- Installed SQL Server Management Studio for managing the local database.
- Created a database in SQL for your Thycotic product
- Created a new SQL Server user login for your SQL database

**Note:** This document uses Thycotic's Secret Server product as example in the instructions, but the same steps apply for Privilege Manager advanced installs.

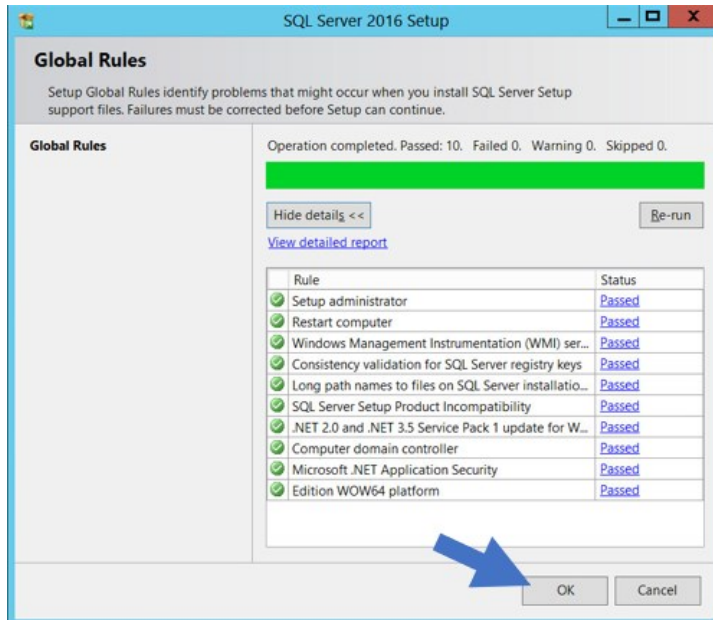
### Procedures

#### Installing SQL Server 2016

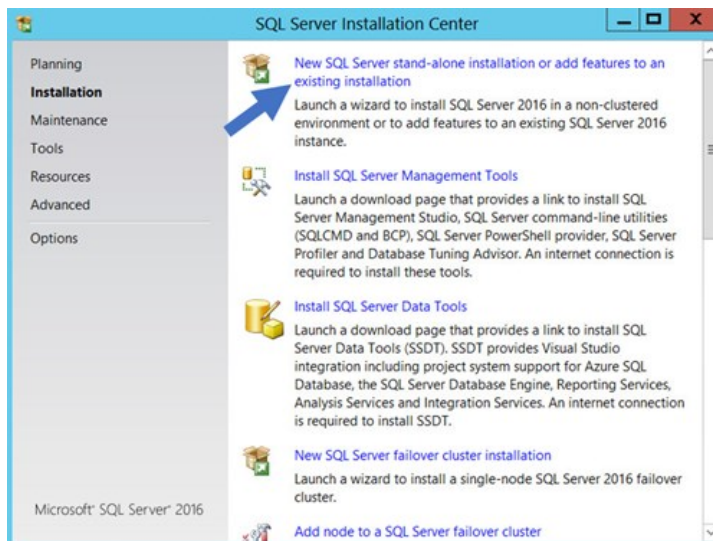
1. Launch the SQL Server installer from CD or file download. The SQL Server Installation Center opens to the Planning window:



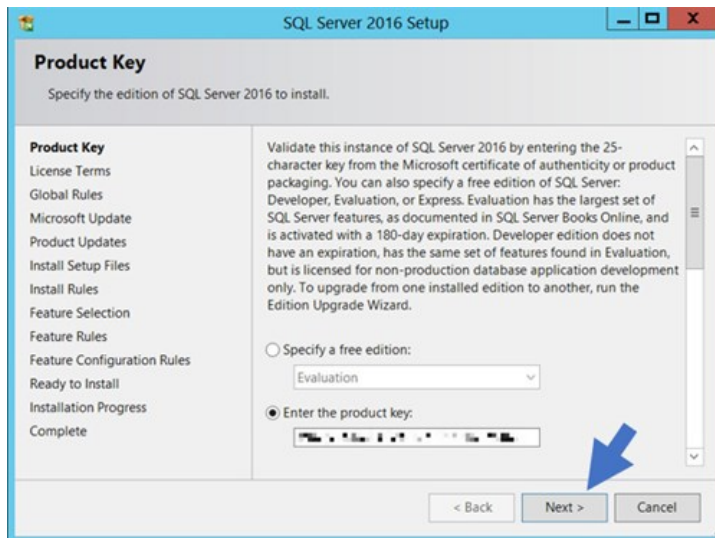
2. Click the **System Configuration Checker** link. This runs a tool that checks for conditions on your server that could prevent SQL Server from installing.
3. When the tool launches, click the **Show details** button. A successful scan should look like the one shown below. If you encounter any issues, look at the detailed report, resolve the reported issues, and rerun the scan.



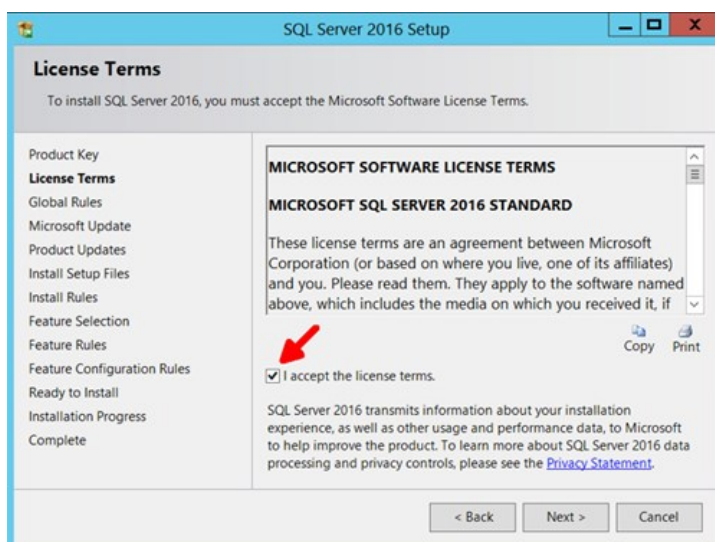
- Click the **OK** button when done to return to the "SQL Server Installation Center" window.
- In the SQL Server Installation Center window, click the **Installation** link. The Installation Window appears:



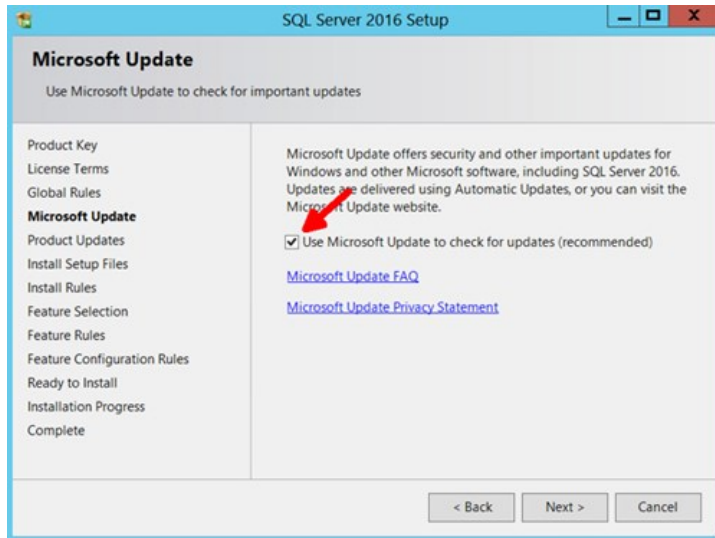
- Click **New SQL Server stand-alone installation...** link. The Product Key page appears:



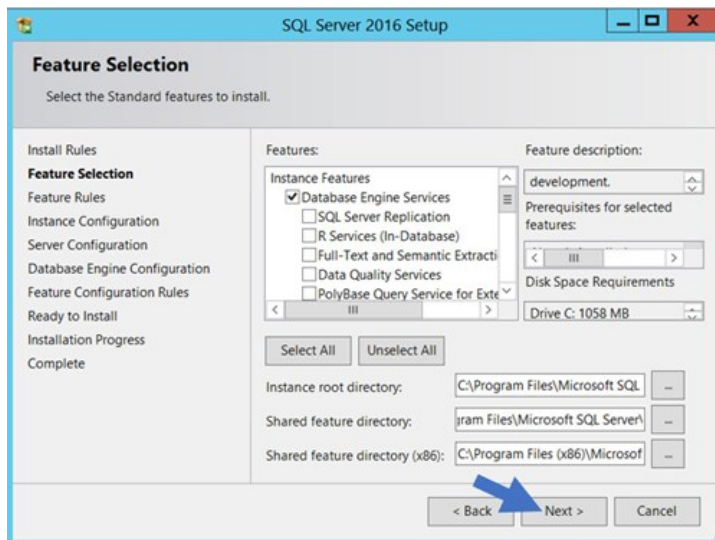
7. Click to select the **Enter the Product Key** selection button.
8. Type your product key in the the **Enter the Product Key** text box.
9. Click the **Next >** button. The License Terms page appears:



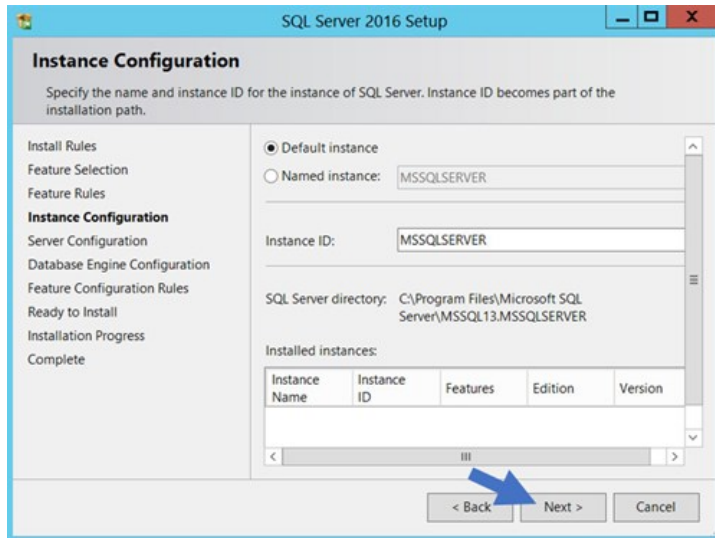
10. Click to select the **I accept the license terms.** check box.
11. Click the **Next >** button. The Global Rules page appears (not shown) after the rule check runs.
12. Click the **Next >** button. The Microsoft Update page appears:



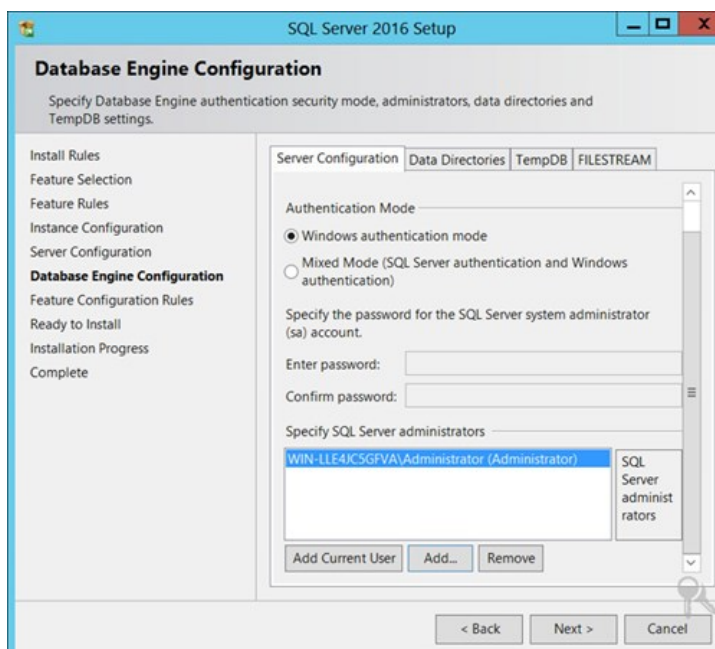
13. Click to select the **Use Microsoft Update...** check box to check for updates (recommended), unless your software update process does not use automatic updates from Microsoft
14. Click the **Next >** button twice to bypass the Product Updates page. The Install Setup Files page appears.
15. Wait for the installation to complete.
16. Ensure that all operations pass.
17. Click the **Next >** button twice to bypass the Install Rules page. The Feature Selection page appears:



18. Ensure the **Database Engine Services** check box is selected. This is the only feature necessary for Secret Server. Unless you are using Geo-Replication, you can leave everything else unchecked. Leave the directory locations unchanged.
19. Click the **Next >** button twice to bypass the Feature Rules page. The Instance Configuration page appears:



20. Ensure the **Default Instance** selection button is selected.
21. Type a name for your SQL Instance in the **Instance ID** text box.
22. Click the **Next >** button twice to bypass the Server Configuration page. The Database Engine Configuration page appears:

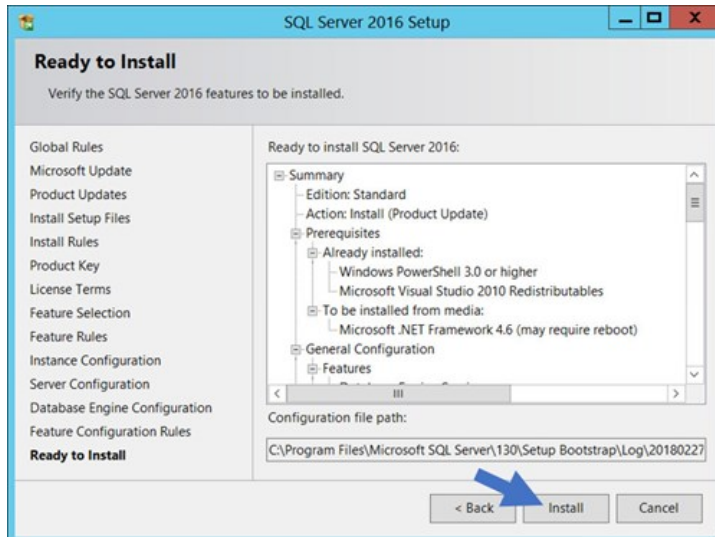


23. You have the choice to select either **Windows Authentication Mode** or **Mixed Mode**. Select the option that will work best for your environment:
  - **Mixed Mode (for easiest configuration)**: This mode is required if you intend on using a SQL Server account to authenticate Secret Server to your SQL Server instance. We recommend using mixed mode if you are setting up a test or demo environment. Selecting this option will also require you to set a password for the SQL Server system administrator (sa) account. See [Adding a SQL Server User](#) (section below) for instructions on adding more users.

- **Windows Mode (recommended for best security)**: This mode prevents SQL Server account authentication. We recommend using Windows mode for production environments. Whatever user or group assigned will have administrative access to your SQL instance. According to best security practices, limit this number to as few users as possible.

**Note:** If choosing **Windows Mode** you will also need to [run the IIS application pool as a service account](#) later in the installation process.

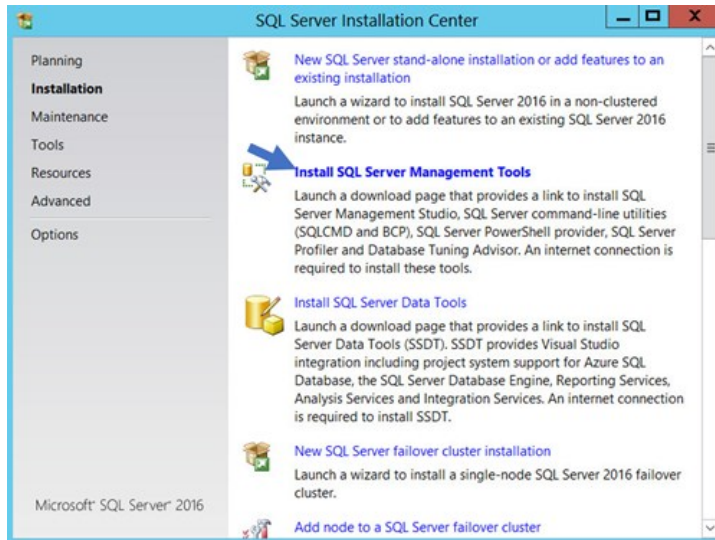
24. You can leave the options in the remaining tabs at their default values or change the file locations in the **Data Directories** and **TempDB** tabs if you wish to store the database and log data in a different drive or directory.
25. Click the **Next > button** twice to bypass the Feature Configuration Rules page. The Ready to Install page appears:



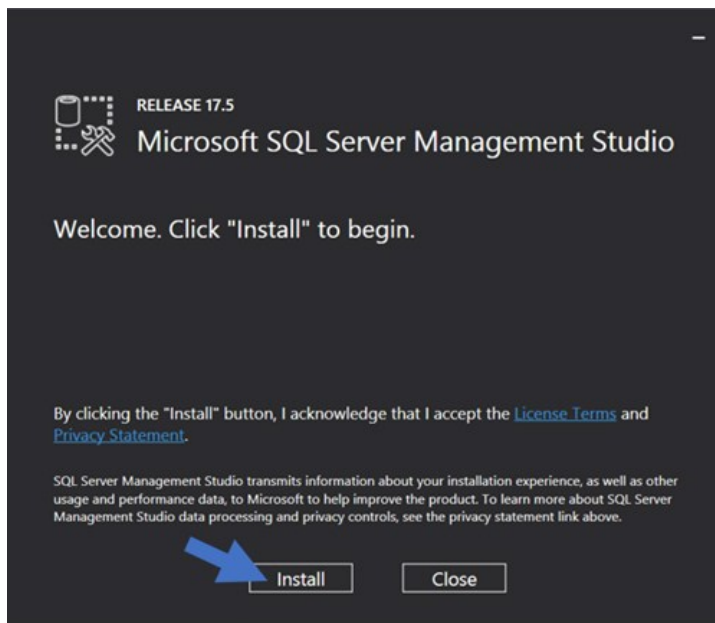
26. Click the **Install** button.
27. Wait for installation to complete. This may take several minutes.
28. Click the **Close** button.

## Installing SQL Server Management Studio

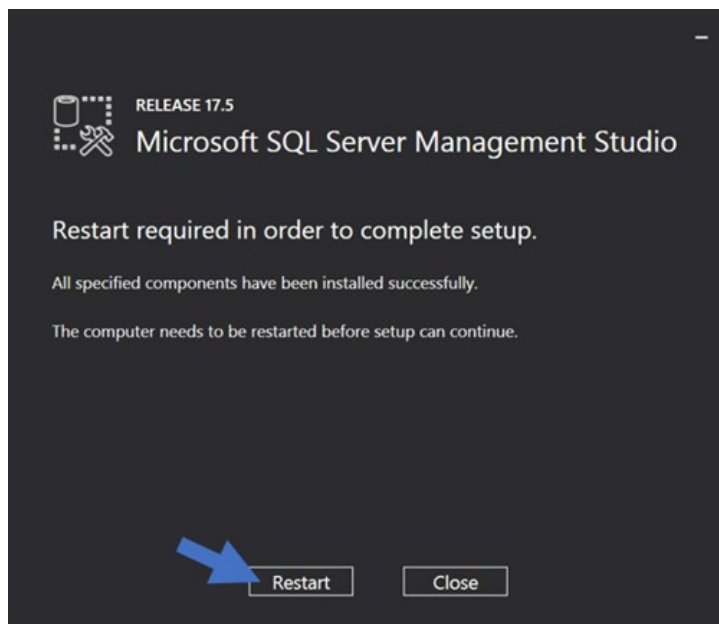
1. In the "SQL Server Installation Center" window, click the **Installation** menu item. The Installation page appears:



2. Click the **Install SQL Server Management Tools** link.
3. Wait for the Web page to load then click the **Download SQL Server Management Studio...** link. A file downloads.
4. Run the downloaded file (varies by browser). The SQL Server Management Studio installer starts.



5. Click the **Install** button.
6. Wait for the installer to complete. This may take several minutes.



7. Click the **Restart** button if prompted. Otherwise, click the **Close** button.
8. Close "SQL Server Installation Center."

## Creating the SQL Server Database

To install SS, the Thycotic installer creates the SQL database for you if it does not exist and if the user account has permission to create a new database, which requires the dbcreator server role.

If not using the Thycotic Installer, use the following steps to create a database manually through SQL Server Management Studio:

1. Open SQL Server Management Studio.
2. Connect to your SQL Server instance.
3. Right click the **Databases** folder and select **New Database...** The New Database page appears.
4. Type a name for your database in the **Database Name** text box.
5. Click the **OK** button.

## Adding a SQL Server User

According to security best practices, limit the number of users with access to your SQL database as much as possible. Use the following instructions to add a SQL Server account for SS to use to access the SQL database:

1. Open SQL Server Management Studio.
2. Connect to your SQL Server Database.
3. Expand the **Security** folder.
4. Right-click the **Logins** folder and select **New Login...**
5. Select a method of authentication:
  - **SQL Server Authentication:** Use this option to create a new SQL Server account (this requires mixed mode to be enabled). To create the account, enter a new username and password and then deselect the **Enforce Password Policy** check box to

prevent the account from expiring.

- **Windows Authentication:** Use this option to add access to SQL Server for an existing Windows account. To add the account, enter the login name or click **Search** to find the account. It is recommended to use a domain account rather than a local Windows account.

6. Click **User Mapping** in the left menu.
7. Click to select the check box next to your SS database.
8. In the **Database Role Membership** window, click to select the **db\_owner** check box.
9. Click the **OK** button.

## System Requirements

Please review the detailed [System and Memory Requirements for Secret Server](#). The *Minimum Requirements* are for trial, sandbox, and POC environments. The *Recommended Requirements* are for production deployments.

## Hardware Requirements

SS can be installed on a physical server or virtual machine.

If you would like to set up front-end (application) clustering, you need to have two or more servers available.

For testing of high availability for the SQL Server, you can use either existing Microsoft AlwaysOn infrastructure or database mirroring. If you choose to test this, this is something your database team needs to prepare in advance.

## Software Requirements

### Checklist

- Windows Server 2012 or newer (recommended) (one server, minimum)
- SQL Server (one instance, minimum)
- Application server prerequisites
- SSL certificate

### SQL Server

You can create the SQL database in an existing SQL instance, or a new installation of SQL Server. For high availability, this needs to be a paid edition of SQL Server (not SQL Express). If you are using a new installation of SQL Server, please have this installed beforehand.

Detailed instructions for installation and configuration of SQL Server are included in one of the installation guides below (choose the guide matching the OS that SQL server will be installed on).

### Application Server

We recommend installing SS on Windows Server 2012 or greater. Include IIS, ASP.NET and .NET Framework. Refer to the System Requirements KB above to view prerequisite details.

**Important:** Please read the notes at the bottom of this article.

## Minimum Requirements for Basic Deployments

2 CPU Cores	2 CPU Cores
4 GB RAM	4 GB RAM
25 GB Disk Space	50 GB Disk Space
Windows Server 2012	Windows Server 2012
IIS 7 or newer (64-bit applications only)	SQL Server 2012-2019
.NET 4.5.1 or newer	Collation SQL_Latin1_General_CP1_CI_AS

## Recommended Requirements for Basic Deployments

**Note:** Environments budgeting for over 10,000 secrets require a scoping call with a Thycotic engineer

4 CPU Cores	4 CPU Cores
16 GB RAM	16 GB RAM
25 GB Disk Space	100+ GB Disk Space
Windows Server 2012-2019	Windows Server 2012-2019
IIS 7 or newer (64-bit applications only)	SQL Server 2012-2019
.NET 4.6.1 or newer	Collation SQL_Latin1_General_CP1_CI_AS

## Minimum Requirements for Advanced Deployments

Recommended for organizations deploying discovery, session recording, or increased numbers of distributed engines:

**Note:** Also see feature-specific guides listed below.

8 CPU Cores	8 CPU Cores
16 GB RAM	16 GB RAM

25 GB Disk Space	100+ GB Disk Space
Windows Server 2012-2019	Windows Server 2012-2019
IIS 7 or newer (64-bit applications only)	SQL Server 2012-2019
.NET 4.6.1 or newer	Collation SQL_Latin1_General_CP1_CI_AS

4 CPU Cores	4 CPU Cores
4 GB RAM	4 GB RAM
25 GB Disk Space	40 GB Disk Space

**Note:** Further adjustments to system requirements for both RabbitMQ and distributed engines are at the discretion of Thycotic Professional Services engineers.

## Recommended Requirements for Specific Features

[Session Recording Requirements: Basic and Advanced](#)

[Ports Used By Secret Server](#)

## Notes

- Secret Server requires Microsoft SQL Server and its database be set to the collation SQL\_Latin1\_General\_CP1\_CI\_AS. See [Microsoft SQL collation requirements](#) and check your server collation settings before upgrading.
- System Requirements apply to both physical and virtual machines.
- For best performance, we recommend using dedicated (clean) servers for hosting Thycotic products.
- If .NET 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, we highly recommend upgrading 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>.
- **Installing Secret Server with Azure SQL:** Currently, we do not recommend using SS with Azure SQL when the Web host and the Azure SQL instance are in different datacenters. According to Microsoft, applications, such as SS, that use frequent, high-volume, ad hoc queries use substantial response time on network communication between the application and Azure SQL database tiers. Thus, network latency with many data access operations across datacenters can become an issue.
- **Unsupported Web Servers:** Small Business Server (SBS), The Essentials Edition, Any client OS, domain controllers, SharePoint servers.
- Secret Server Cloud requires an on-premise machine to use a distributed engine.
- SQL launchers do not support SSMS 18.0 or higher.
- Discovery scanning for Windows Server 2016 scheduled tasks requires that either the SS node or the distributed engine that is executing the scan must run on Windows Server 2016 or later. This is due to changes in Windows Server 2016 API used for scheduled task dependency scans.
- AWS RDS: Currently, we do not recommend using SS with AWS Relational Database Service when the Web host and the SQL instance

are in different datacenters. Applications, such as SS, that use frequent, high-volume, ad hoc queries depend on fast network communication response time between the application and SQL database. Thus, network latency with many data access operations across datacenters can become an issue.

- Secret Server (SS) requires the application pool to have the “load user profile” setting enabled. Secret Server will report a critical alert to notify admins if this setting is not enabled.

**Important:** Upgrading to Secret Server version 8.9.000000 and above will require **Windows Server 2008 R2 or greater**.

**Important:** Upgrading to Secret Server version 8.5.000000 and above, there are changes in the .NET Framework version you will need to be aware of along with some additional steps in the upgrade process. For more information, see [Secret Server Moving to .NET Framework 4.5.1](#).

**Important:** Upgrading to Secret Server version 10.0.000000 and above will require configuring integrated pipeline mode on the Secret Server Application Pool. Please see [this KB](#) for details on configuring integrated pipeline mode in IIS. If using Integrated Windows Authentication you will also need to update IIS authentication settings as detailed in [this KB](#). If you are at version 9.1.000000 and below, you will need to first upgrade to 9.1.000001 before you can upgrade to 10.0.000000 and above.

## How Upgrades Work

Secret Server periodically polls our update server to detect updates. If your Secret Server is on an internal network that has no outbound access or goes through a proxy, Secret Server will not be able to perform updates automatically, therefore, outbound access to the below connections on your firewall is needed if you want to perform updates automatically:

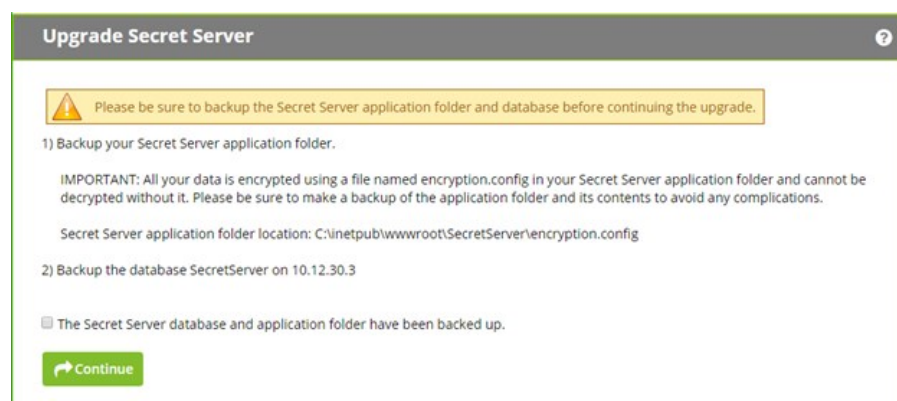
- d36zgw9sidnotm.cloudfront.net:443
- updates.thycotic.net:443
- updates.thycotic.net:80

The steps below can be used to perform an upgrade for versions 7.1.000015 and higher. If you have an older version of Secret Server, please contact Thycotic technical support for assistance.

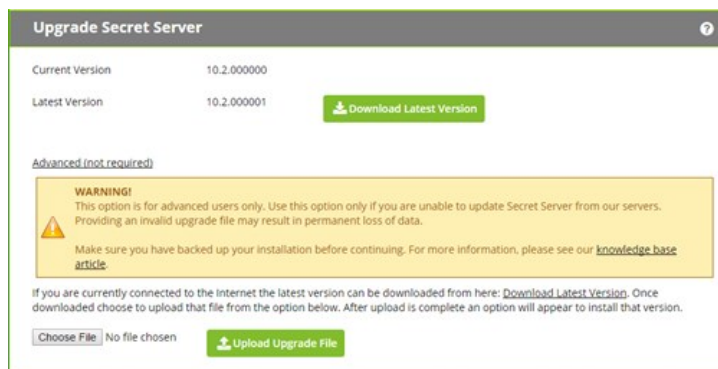
## Procedure

### Step 1: Open the Upgrade Secret Server Wizard

1. From a computer that does have outbound network access and Secret Server access, go to the Secret Server Upgrade page by browsing to: `http://<yourinstance>/Installer.aspx?patch=true` (filling in your Secret Server URL for <yourinstance>). The wizard appears:



2. Backup your Secret Server application folder and your Secret Server database.
3. Click to select the **The Secret Server database...** check box on the page.
4. Click the **Continue** button. The next page appears:



## Step 2: Get and Upload the Latest .zip File

1. Download the latest version .zip file by clicking the **Download Latest Version** button on the installer page. The file name will appear something like Version\_10\_2\_000000.zip. Note where you save it.

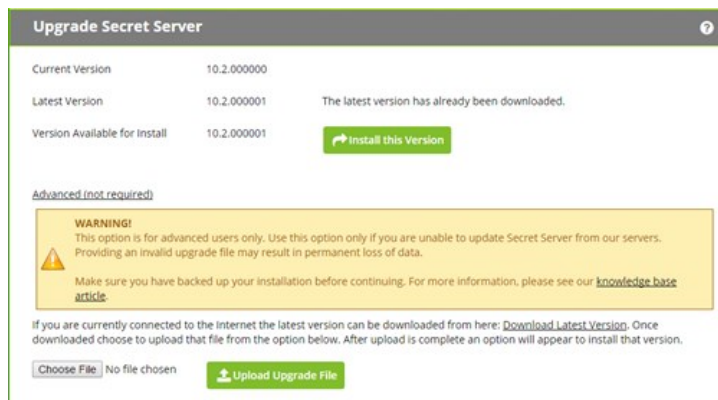
**Note:** You also can find the downloadable update files in our [Secret Server Offline Update File KB here](#) (KBA).

2. Click the **Choose File** button to select the Secret Server .zip file you just downloaded.

**Note:** You can [verify the file hashes for the latest version using the posted hash values](#) (KBA).

**Note:** You should **not** use the fresh install SecretServer.zip or setup.exe that is first downloaded from [thycotic.com](#). Only use the Get Latest Version link—there is a difference between the upgrade file and fresh install zip.

3. Click the **Upload Upgrade File** button. You see a message confirming the file was successfully uploaded, and the Install This Version button appears.



4. Click the **Install this Version** button. The Upgrade Secret Server page appears (not shown).

## Step 3: Upgrade Secret Server

1. Click the **Upgrade** button. The upgrade automatically processes and once it has finished you will see a confirmation page.
2. Click **Return to Home** to return to the dashboard.

## Secret Templates

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Secret templates are used to create secrets and allow customization of the format and content of secrets to meet company needs and standards. Examples include: Local Administrator Account, SQL Server Account, Oracle Account, Credit Card and Web Password. Templates can contain passwords, usernames, notes, uploaded files, and drop-down list values. New Secret templates can be created, and all existing templates can be modified.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Activating and Deactivating Templates

If a template is no longer relevant or outdated, it can be inactivated. This can be done from the specific template's Secret Template Edit page.

Templates can also be inactivated in bulk from the Manage Secret Templates page. Click the **Active Templates** button to navigate to the Set Active Secret Templates page. This screen displays all the secret templates in SS. Each secret template can be set as active or inactive. Once the secret templates are chosen as active or inactive, then saving changes brings the secret templates into effect immediately. Inactivating a secret template does not inactivate any secrets using that secret template—those secrets still exist, but users are not able to create new secrets using an inactivated secret template.

## Changing a Secret's Template

To convert secrets from one secret template to another:

1. View a secret and click on the **Convert Template** button.
2. Click to select the target template from the **Secret Template** list.
3. Map each text-entry field to a new field:
  1. Go through each list and select the target text-entry field for each source text-entry field on your secret.
  2. If you want to remove the value for a text-entry field instead of converting it, then select the <Remove> option on the list for that text-entry field.
  3. When you are done selecting, you can choose a folder.
4. Click **Save**.

The Convert Template button is only available to users and groups with the "Owner" permission to the secret.

**Note:** To preserve audit data, when a secret is converted from one type to another, the old secret is deleted, and a new secret is created. An admin can view old secret by searching for deleted secrets on the dashboard. A user needs "Add Secret," "Edit Secret," "Delete Secret," and "Own Secret" role permissions in order to convert a secret to a new template.

## Configuring Secret Template Permissions

As of SS 10.3 it is possible to assign users and groups to specific secret templates so they can either manage or create secrets based on those templates. This allows you to have more granular control over what secret templates are seen by users and groups when they are managing the templates or creating secrets. To configure permissions:

1. Select **Admin > Secret Templates**. The Manage Secret Templates page appears:

**Manage Secret Templates**

Active Directory Account ☐ Show Inactive

[Back](#)
[Edit](#)
[+ Create New](#)
[Export](#)
[View Audit](#)
[Active Templates](#)
[Password Requirements](#)

[A Character Sets](#)
[Configure Launchers](#)
[Configure Secret Template Permissions](#)

**Other Templates**

[Configure Dependency Templates](#)
[Configure Scan Templates](#)


**Import Secret Templates**

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

[Import](#)

2. Click the **Configure Secret Template Permissions** button. The Secret Template Permissions page appears:

## Secret Template Permissions



The [Everyone] group has Create Secret permission on all Secret Templates by default. To change this, remove those permissions from the [Everyone] group and assign them to another Group or User

**Group/User:**

Select a user or group to change their Secret Template permissions.

Back
View Audit
Edit

- Select a group or user by typing in the **Group/User** text box. The page changes:

**Group/User:**

Select a user or group to change their Secret Template permissions.

Back
View Audit
Edit


- Click the desired user or group in the **Group/User** dropdown list that appeared.

- Click the **Edit** button. A drop-down list appears:

**Group/User:**

*View Effective Permission report for [Users](#)*

PERMISSIONS FOR



No Secret Template permissions are directly assigned. To see all the Secret Template permissions that this User/Group has, click the report link listed above.

Save
Cancel

- Click to select a secret template you wish to assign them to. You may either assign "Template Create secret" or "Template Owner" to a user or group.

- Template Create secret allows a user or group to create secrets based on the selected secret template.
- Template Owner allows a user or group to edit a secret template and create secrets based on the selected secret template. By default, the Everyone group that targets all users of SS can create secrets based on any secret template.

**Note:** Users' secret Template permissions are based on the permissions directly assigned to them, as well as the permissions assigned to all of the groups they are a member of. If a user or group does not have Template Create secret or Template Owner permissions, they are unable to create a secret based on that secret template or see that it exists in SS.

7. Click the **Save** button.

## Creating or Editing Secret Templates

Select **Admin > Secret Templates**. The Manage Secret Templates page appears:

**Manage Secret Templates**

Active Directory Account ☐ Show Inactive

[Back](#)
[Edit](#)
[+ Create New](#)
[Export](#)
[View Audit](#)
[Active Templates](#)
[\\* Password Requirements](#)

[A Character Sets](#)
[Configure Launchers](#)
[Configure Secret Template Permissions](#)

**Other Templates**

[Configure Dependency Templates](#)
[Configure Scan Templates](#)

**Import Secret Templates**

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

[Import](#)

If editing an existing template:

1. Click to select that template in the unlabeled secret template dropdown list.
2. Click the **Edit** button. The Secret Template Designer page appears (see below).

If creating a new template:

1. Click the **Create New** button. The Create New Secret Template pop-up page appears:

**Create New Secret Template**

Name of the New Secret Template? \*

[+ Create](#)
[X Cancel](#)

2. Type the name of the new template in the text box.

3. Click the **Create** button. The Secret Template Designer page appears:

Secret Template Designer

SETTINGS

Secret Template Name

My Secret Template

Secret Template Icon

Active?

Expiration Enabled?

Validate Password Requirements On Create?

Validate Password Requirements On Edit?

Field Displayed on Basic Home

Folder Name

Edit

FIELDS

FIELD NAME	FIELD DESCRIPTION	FIELD TYPE	IS REQUIRED?	HISTORY	SEARCHABLE	EDIT REQUIRES	HIDE ON VIEW	EXPOSE FOR DISPLAY
* <div></div>	<div></div>	<div>Text</div>	<input type="checkbox"/>	<div><div></div><div>All</div></div>	<input type="checkbox"/>	<div>Edit</div>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Show Inactive Fields

Back

Configure Password Changing

Configure Launcher

Configure Extended Mappings

View Audit

Copy Secret Template

There is/are 0 My Secret Template Secret(s).

The Secret Template Designer page provides all the options for configuring a secret template, as well as which text-entry fields appear on any secret created from that template.

Add template fields as desired. See [Secret Template Settings](#).


Click the **Edit** button to customize the template general settings. The Secret Template Designer appears:


## Secret Template Designer

Secret Template Name

\* My Secret Template

Secret Template Icon


Change



You can use a naming pattern to enforce a standardized name for this Secret Template.  
The naming pattern uses **Regular Expressions**.  
For example, the expression `"\w+\\\\\w+$"` would allow "NTDOMAIN01\USER3454" but not "USER3454 on NTDOMAIN01".

Name Pattern

Name Pattern Error Message

Description

Active?

☒

Keep Secret Name History?

☐

Expiration Enabled?

☐


Validate Password Requirements On Create?



☐

Validate Password Requirements On Edit?

☐

Field Displayed on Basic Home

Folder Name 

 Save
 Cancel

These settings are available:

- **Secret Template Name** check box.
- **Secret Template Icon** link: Click to change the icon displayed for the template.
- **Name Pattern** text box. See [Template Naming Patterns](#).
- **Name Pattern Error Message** text box. See [Template Naming Patterns](#).
- **Keep Secret Name History?** check box: If Keep Secret Name History is enabled, SS keeps the specified number of entries for viewing. This feature creates a record of every name used when a new secret is created.
- **Expiration Enabled?** check box: Secret templates allow expiration on certain text-entry fields. When the check box is selected, an expiration time interval can be specified for a selected text-entry field using the dropdown menu. With this option enabled and a time duration specified, SS begins providing alerts if the secret text-entry field is not changed within the specified expiration requirements.
- **Validate Password Requirements on Create?** check box: Ensure requirements are met on secret creation.
- **Validate Password Requirements on Edit?** check box: Ensure requirements are met when editing secret.
- **Field Displayed on Basic Home** dropdown list box: Choose the field that appears on the Basic Home view.




Click the **Save** button. The Secret Template Designer page reappears.

Select the following buttons to further configure the secret template:

- **Edit Passwords Button:** Only visible for templates that contain a text-entry field that is of the password type. It is used to alter the minimum password length, as well as the character set used, for the auto-generation of the secret's password. See [Creating Secrets](#) for further details on password auto-generation.
- **Configure Password Changing Button:** Used to enable RPC on these secrets. For details, see [Remote Password Changing](#).
- **Configure Launcher Button:** Used to enable Remote Desktop or PuTTY Launcher or custom launchers on these secrets. For details, see [Secret Launchers](#).
- **Configure Extended Mappings Button:** Extended Mappings allows you to tie a text-entry field value to a SS defined system type for additional functionality. For example, you may have a generic password secret template that has a username and password text-entry field. For purposes of looking up credentials, such as a ticket system authentication secret, SS needs to know that actual type of the text-entry fields since the text-entry field name can be custom. Extended mappings available are:
- **SSH Private Key:** Defines which text-entry fields make up the SSH Key components of Private Key, Private Key Passphrase, and Public Key.
- **Username and Password:** Defines which text-entry fields contain the username and password.
- **Remote Server SSH Key for Validation:** Ensures the machine SHA1 digest for validating the machine connected to is correct.
- **OATH Secret Key:** For password changing on the Amazon Root Account using the Web Password Changer. If you enter the OATH secret for two factor, SS generates the one-time password (OTP) automatically for password changing and heartbeat, allowing you to automate that while enforcing two-factor authentication on the AWS root credential.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

The secret template designer provides several settings to customize secret template text-entry fields:

- To add a secret text-entry field, fill out the values and click the **+** button.
- To delete a text-entry field, click the  icon. There is a confirmation dialog box before deletion takes place.
- To edit a text-entry field, click the  icon. Click either the  icon to save or the **X** icon to discard the changes.

## Field Slug Names

A *field slug name* in SS is a unique human-readable identifier for a data field in a SS template. The field slug name is available for integrating with third-party applications via API calls. Slug names are programmatically available for API calls but are not visible to users of the template (those creating secrets) but are display in the secret templates for references.

**Note:** If you are not planning to access SS with an API, slug field names are not for you—leave the suggested name as is.

**Figure:** Field Slug Name in a Secret Template

FIELDS		
FIELD NAME	FIELD SLUG NAME	FIELD DESCRIPTION
Public Key	public-key	The SSH public key.
Private Key	private-key	The SSH private key.
Private Key Passphrase	private-key-passphrase	The passphrase for decrypting the SSH private key.
Notes	notes	Any additional notes.
*   <input type="text"/>	* <input type="text"/>	<input type="text"/>

Field slug names are automatically generated, based on the field name, when the field is created. For example, "User Name" became "user-name." Characters that are potentially problematic for programming, such as spaces, are swapped out. The automatically generated name is unchangeable by human users, unlike the field name. If API calls were based on the field name, human users with access to the template could break those calls, simply by changing the name.

With SS 10.7.X+, The generated field slug names are now user-definable. You can edit the generated names to:

- Conform to a naming convention used in your API calls.
- Maintain the same name for a field across secret templates to simplify coding by developers.

The only requirement is that each slug field name is unique to that template.

**Note:** If you are wondering how SS internally uniquely identifies fields, there is an internal ID that is not accessible by users or APIs. It is not available read-only (for API use) because we want to futureproof integrations from internal changes to SS.

**Note:** The user-definable field slug names are also automatically generated when you upgrade from a version of SS that did not have user-defined field slug names. If there are two fields with the same field name, the second (and later) generated field slug name has an incremented number appended to it.

## Secret Template Field Types

Template text-entry fields can be specified as one of several different types to enhance customization:

- **Text:** Single-line text-entry field.
- **Notes:** Multi-line text-entry field.
- **URL:** Clickable hyperlink.
- **Password:** Password type text-entry field.
- **File:** File attachment link. File attachments are stored in the Microsoft SQL Server database.


## Secret Template Text-Entry Field and Control Settings

The settings available for text-entry fields are:

- **Field Name:** Name of the text-entry field. This name is used for the Create New drop-down list on either the Dashboard's Create Secret Widget or Home page.
- **Field Description:** Description of the text-entry field.
- **Field Type:** Type of the text-entry field. See below for a description of the different text-entry fields.
- **Is Required:** Whether the text-entry field should require a value. These check boxes are checked for correct content when the user attempts to create this secret. A validation error is displayed if not entered correctly.
- **History:** Number of values to keep in the text-entry field's history of values.
- **Searchable:** Whether that text-entry field should be indexed for searching. By default, passwords are not indexed. File attachments and history cannot be indexed for searching.
- **Edit Requires:** Minimum permissions on the secret needed in order to edit the value on the secret. The options are Edit, Owner and Not Editable. This enables the secret text-entry field to be locked down at a more granular level than other text-entry fields on the template.
- **Hide on View:** If checked, this text-entry field is not displayed to users when viewing the secret. The text-entry field is only be displayed when the secret is in Edit mode.
- **Expose for Display:** If checked, this text-entry field is available to be displayed as a Custom Column on the SS Dashboard.

**Note:** All text-entry fields that are set to "Expose for Display" are **not** encrypted in the database. Only check this value if the secret text-entry field data is not considered privileged information.

The order of the text-entry fields in the Template Designer grid is the same as those that appear when the user views or edits a secret created from the template. The order can be modified through the up and down arrows on the grid.

Default values can be specified on each text-entry field by clicking the edit defaults  button . These added values appear as a list on any secret created from this template.

With this SS feature, admins can use private SSH keys for PuTTY launcher sessions as well as for RPC tasks (configurable through password changer settings) and Unix and Linux discovery. Passphrases can additionally be stored, if necessary, to decrypt the private keys for additional security. The Unix Account (SSH) secret template includes text-entry fields for the private key and passphrase by default:

The SSH Key template is included by default and can be used to store SSH keys that can later be selected for use in RPC, discovery or launcher authentication for other secrets:

**Note:** Starting with version 10.1.000000, SS also supports SSH key rotation on secrets.

The **Unix Account (SSH Key Rotation)** and **Unix Privileged Account (SSH Key Rotation)** secret templates use password changers that change the public key in the account's `authorized_keys` file as well as change the password on the account. SS ships with a password changer and custom command sets that allow an account to change its own public key and password, and a password changer and custom command sets that changes a user's public key and password using a privileged account. These scripts can be customized for different Unix environments.

For more information about SSH Key Rotation, see the [SSH Key Rotation](#) (KBA) and [SSH Key Rotation Quick Start](#) (KBA).

Character sets are a collection of distinct characters that are used in password requirements and password rules. Custom sets can be created, and both ASCII and Unicode are supported. For more information on setting up compliance checks and password generation standards, see [Password Requirements](#). The five standard character sets are:

- Lower Case (a-z)
- Upper Case (A-Z)
- Numeric (0-9)
- Non-Alphanumeric (!@#\$%^&\* ( ))
- Default – Includes all the above

To manage character sets, click the **Character Sets** button on the **Administration > Secret Templates** page. Only character sets which are not currently used by a password requirement can be deleted.

SS supports naming patterns for secret templates. Naming patterns are a way for administrators to maintain consistency for secret names and can help ease both browsing and grouping secrets by name. Patterns are created using regular expressions. Regular expressions are a formal set of symbols commonly used to match text to patterns. For example, the regular expression `^\\w+\\\\w+$`, allows `NTDOMAIN01\\USER3454` but not `USER3454` on `NTDOMAIN01`.

**Note:** Regular expressions are beyond the scope of this document. They are very powerful and can get quite complex—books have been written on the topic. Microsoft offers a good overview at their [Regular Expression Language Quick Reference](#) Web page.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Set requirements on a password text-entry field to validate user-entered passwords or make auto-generated passwords conform to set specifications.

A password requirement is made up of a minimum and maximum length, a set of characters, and optional rules such as "At least three upper-case characters" or "The first character must be lower-case". The default password requirement is 12 characters from the default character set, with at least one upper-case, lower-case, numeric, and symbol character.

Create or edit password requirements by clicking the **Password Requirements** button on the **Administration > Secret Templates** page.

Click the **Character Sets** button next to the Password Requirements button to create or delete character sets.

## Creating a Custom Password Requirement

To create a new password requirement:

1. Go to **Admin > Secret Templates**. The Manage Secret Templates page appears:

### Manage Secret Templates

Active Directory Account
Show Inactive

Back
Edit
+ Create New
Export
View Audit
Active Templates

\* Password Requirements
A Character Sets
Configure Launchers

Configure Secret Template Permissions

### Other Templates

Configure Dependency Templates
Configure Scan Templates

### Import Secret Templates

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

Import

2. Click the **Password Requirements** button. The Password Requirements page appears:


**Password Requirements**

NAME	DESCRIPTION	MINIMUM LENGTH	MAXIMUM LENGTH	DEFAULT
Default	The default password requirement, which uses the alpha-numeric character set and requires one lowercase, one uppercase, one number, and one symbol.	12	12	Yes
SAP	SAP Password Requirement	12	12	No
Mainframe	Mainframe Password Requirement	8	8	No

 Back Create New

3. Click the **Create New** button.

## Password Requirement Edit


**Example:**

Name

Description

Is Default

☐

### GENERATE PASSWORD

Prevent Username In Password

☐

Length between

\*

and

\*

.

Using

Default

▼

[Character Set.](#)

### Password Rules

Minimum of


▼


1


from

Select...

▼



 Save

 Cancel

[Show Usages](#)

4. Type the name and description.
5. If you want the requirement to become the new default, click to select the **Is Default** check box.
6. Set the general options for the requirement in the **Generate Password** section.
 

**Note:** You can also create a custom character set by clicking the Character Set link.
7. Add one or more password rules:
  1. Click to select the type of rule in the first dropdown list in the **Password Rules** section.
  2. Set that type's parameter in the following text box.
  3. Click to select the character set from the "from" dropdown list.
  4. Click the **+** icon to save the rule.

8. Click the **Save** button.

**Note:** To set a custom password requirement for a specific secret, use the "Customize Password Requirement" in the Security tab of a secret.

**Note:** You can enable or disable the validation of manually entered passwords at the secret template level via the "Validate Password Requirements on Create" and "Validate Password Requirements on Edit" settings.

**Note:** The "What Secrets Do Not Meet Password Requirements" report shows secrets containing a password that does not meet the password requirements set for its secret template.

**Note:** Password requirements cannot include rules with overlapping character sets. For example, if an attempt is made to add both a "Minimum of 1 upper-case" rule and a "Minimum of 3 Default" rule to a new password requirement, an error displays.

## Setting the Password Requirement for a Secret Template

To set the password requirement for a text-entry field for a secret template:

1. Go to **Admin > Secret Templates**. The Manage Secret Templates page appears:

### Manage Secret Templates

Active Directory Account
Show Inactive

Back
Edit
Create New
Export
View Audit
Active Templates

Password Requirements
Character Sets
Configure Launchers

Configure Secret Template Permissions

### Other Templates

Configure Dependency Templates
Configure Scan Templates

### Import Secret Templates

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

Import

2. Click to select the desired template in the unlabeled dropdown list.
3. Click the **Edit** button. The Secret Template Designer page appears:

## Secret Template Designer

### SETTINGS

Secret Template Name

Test Template

Secret Template Icon

Active?

☒

Expiration Enabled?

☐

Validate Password Requirements On Create?

☒

Validate Password Requirements On Edit?

☐

Field Displayed on Basic Home

Folder Name

Edit

### FIELDS

FIELD NAME	FIELD DESCRIPTION	FIELD TYPE	IS REQUIRED?	HISTORY	SEARCHABLE	EDIT REQUIRES	HIDE ON VIEW	EXPOSE FOR DISPLAY	
MasterPass	Master Password	Password	<input checked="" type="checkbox"/>	All	<input type="checkbox"/>	Edit	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="text"/>	<input type="text"/>	<input type="text" value="Text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Edit"/>	<input type="checkbox"/>	<input type="checkbox"/>	

☐ Show Inactive Fields

Back

Assign Password Requirement

Configure Password Changing

Configure Launcher

Configure Extended Mappings

View Audit

Copy Secret Template

There is/are 1 Test Template Secret(s).

- Click the **Assign Password Requirement** button. The Secret Template Passwords page for that template appears:

## Secret Template Passwords

### Passwords for Test Template.

FIELD NAME	PASSWORD REQUIREMENT	
MasterPass	Default	

Back

- Click the pencil edit icon for the field you desire. The password requirement turns into a dropdown list.
- Click to select the desired password requirement.
- Click the **Save** icon to save the changes.

## Secret Workflow Templates

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Starting in 10.6, SS introduced *access-request workflow templates*. These allow users to build more complex interactions based on events within SS than currently possible. The first release of workflows offers access requests. Workflow templates define the series of steps and reviewers required for an access request. You can assign workflow templates to secrets or secret policies.

With Access-Request Workflow Templates, you can:

- Require that multiple people approve a request before access is granted
- Require multiple workflow steps, each with different reviewers and number of required approvers, if desired.
- Select "Owners" as a review group

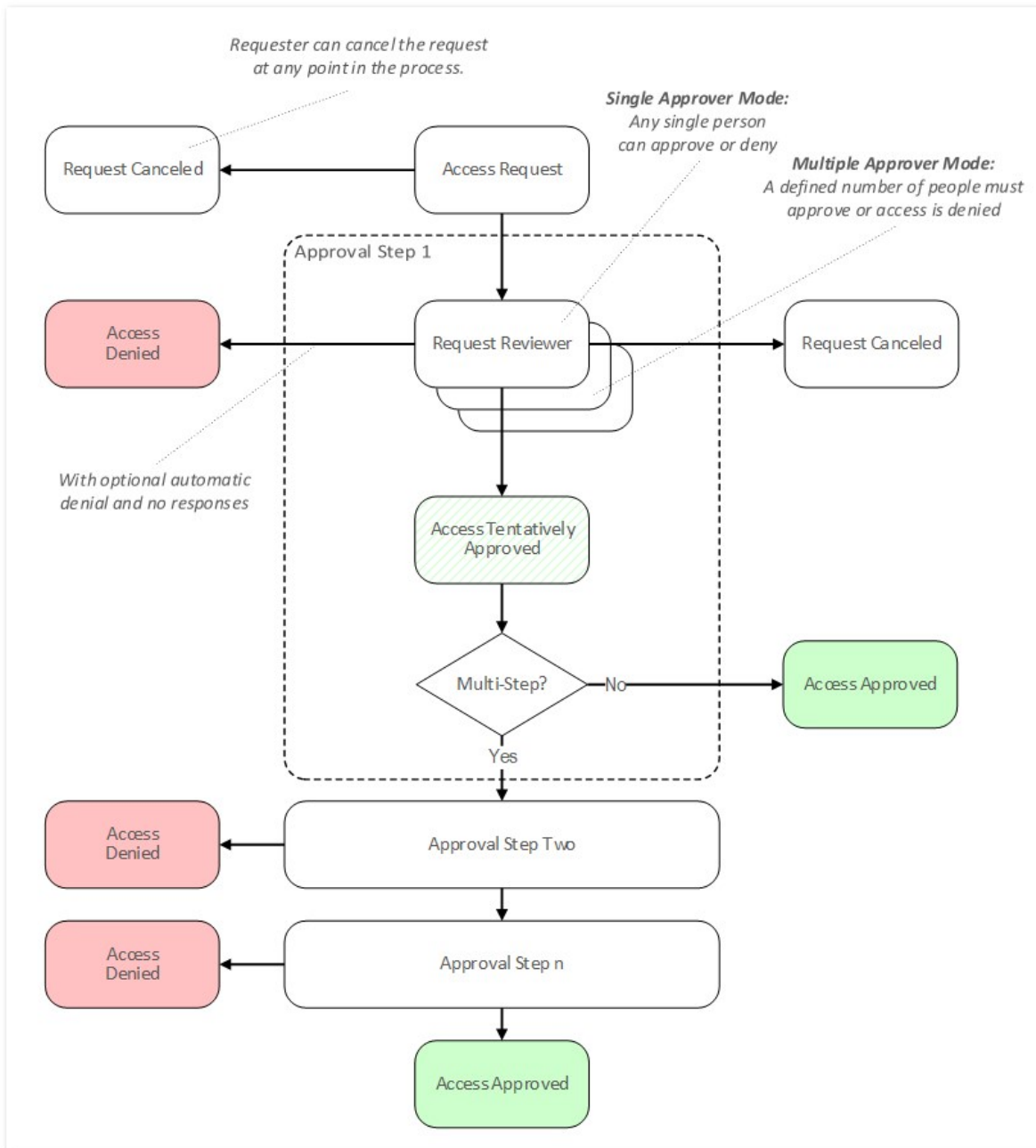
**Note:** Access Requests already existed in SS, but with 10.6 they become much more powerful. Previously, if access requests enabled on a secret, requests were granted after a single reviewer approved the request. Now, approval workflows can require multiple approvers, and multiple approval levels.

The original access requests are one level or step—anyone approving approves the request—no other input is required. Workflows allow up to 15 approval steps where approval by reviews in step 1 moves the request to step 2, approval at step 2 moves it to step 3 and so forth. Denial at any step denies the request.

The new workflow feature can be configured where one approver at a given step is not enough. In effect, approvers in each step can "vote" for approval—you stipulate how many approvers at a step must approve for the approval to move on to the next step.

The following diagram is the entire process summarized:

**Figure:** The Approval Process Workflow



In general, "simple access requests," the only type available to older versions of SS, are the same as a one-step stepped approval. The major exception is that with stepped requests, once a workflow access request has been approved, denied, or canceled, its status cannot be changed. In contrast, simple, non-workflow, access requests retain the original behavior of allowing a request to be approved after it has been denied or denied after it has been approved.

To access workflow templates:

1. Go to **Admin > Workflows**. The Workflow Template page appears:

Workflow Templates

Create Workflow Template

52 Items

Show Inactive ☐

1 of 4

Workflow Template Name	Type	Active	
workflow_test_01	Access Request	Yes	
workflow_Step	Access Request	Yes	
workflow_Policy	Access Request	Yes	
workflow_group	Access Request	Yes	
Workflow_Del	Access Request	Yes	
Workflow_01	Access Request	Yes	
Workflow Template 2 Step - Marrio - Barry	Access Request	Yes	
Workflow Template 1-Step Barry	Access Request	Yes	
WK01	Access Request	Yes	
Will Workflow 01	Access Request	Yes	
WFT_001	Access Request	Yes	
WF_template01	Access Request	Yes	
testWF	Access Request	Yes	

The page lists all active workflow templates.

2. (Optional) Click to enable the **Show Inactive** toggle button, under the **Create Workflow Template** button, to show both active and inactive templates. When the toggle button is disabled, it only shows active workflow templates.
3. Click any workflow template in the list to go to the designer page for that workflow:

Admin > Workflow Templates > Will Workflow 01

Duplicate

Delete

Designer

Audit

WORKFLOW DESIGNER

EDIT

Workflow Name

Will Workflow 01

Description

One step approval (Barry)

Step 1

Step 1

APPROVERS

Barry

Include owners as reviewers

No

Needs at least 1 users(s) in this step to approve

1. Click **Admin > Secret Policy**. The Secret Policy page appears:

## Secret Policy

[Explain](#)

< 1 to 6 of 6 >

Secret Policy Name	Description	Active
<a href="#">Default</a>		Yes
<a href="#">policy</a>		Yes
<a href="#">policy_flow_1</a>		Yes
<a href="#">Policy Workflow</a>		Yes
<a href="#">test</a>		Yes
<a href="#">Test Access Policy</a>		Yes

☐ Show Inactive

← Back
+ Create New

2. For this instruction, we are going to create a new policy.
3. Click the **+ Create New** button. Another Secret Policy page appears:

## Secret Policy

[Explain](#)

Secret Policy Name \*

Description

Active ☒

Section	Secret Policy Item Name	Setting	Value
General	Site	< Not Set > v	

4. Type the new policy name in the **Secret Policy Name** text box.
5. Scroll down the page to the **Security Settings**:

Security Settings	Enable Requires Approval for Access	< Not Set > ▾
Security Settings	Request Access Approvers <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾
Security Settings	Request Access Workflow <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾
Security Settings	Editors also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾
Security Settings	Owners and Approvers also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾

- Click the **Enable Requires Approval for Access** list and select **Enforced**.
- Click to select the check box next to the list. The Assign Approvers popup page appears:

### Assign Approvers

Select the users or groups to be approvers.

Name
------

User/Group < Select > ▾

- Click the **Cancel** button. The other access approval setting become enabled:

**Note:** You cannot set approvers and use a workflow at the same time. The intent of the next few instructions is avoid attempting to do so, which causes an error.

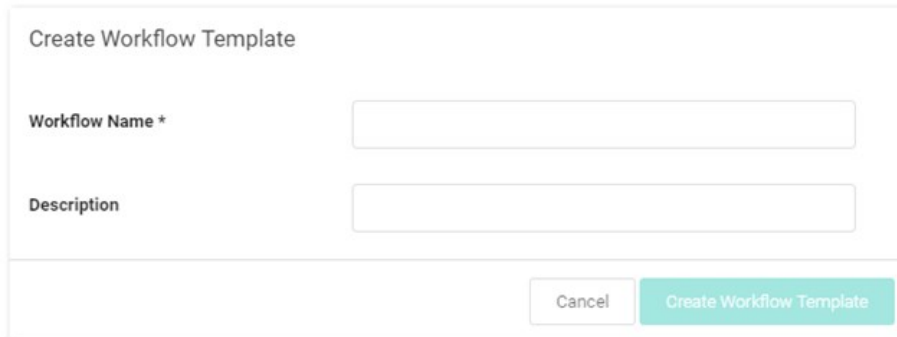
Security Settings	Enable Requires Approval for Access	Enforced ▾ <input checked="" type="checkbox"/>
Security Settings	Request Access Approvers <i>(Dependent on: Enable Requires Approval for Access)</i>	Enforced ▾ < None >
Security Settings	Request Access Workflow <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾
Security Settings	Editors also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾
Security Settings	Owners and Approvers also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > ▾

- Click the **Request Access Approvers** list and select **Not Set**.

10. Click the **Request Access Workflow** list and select **Enforced**. A new list appears alongside.
11. Click the new unlabeled list and select the access template workflow to associate with the policy.
12. Click the **Save** button at the bottom of the page. The policy is now available for assignment to secrets and folders, just like any other policy.

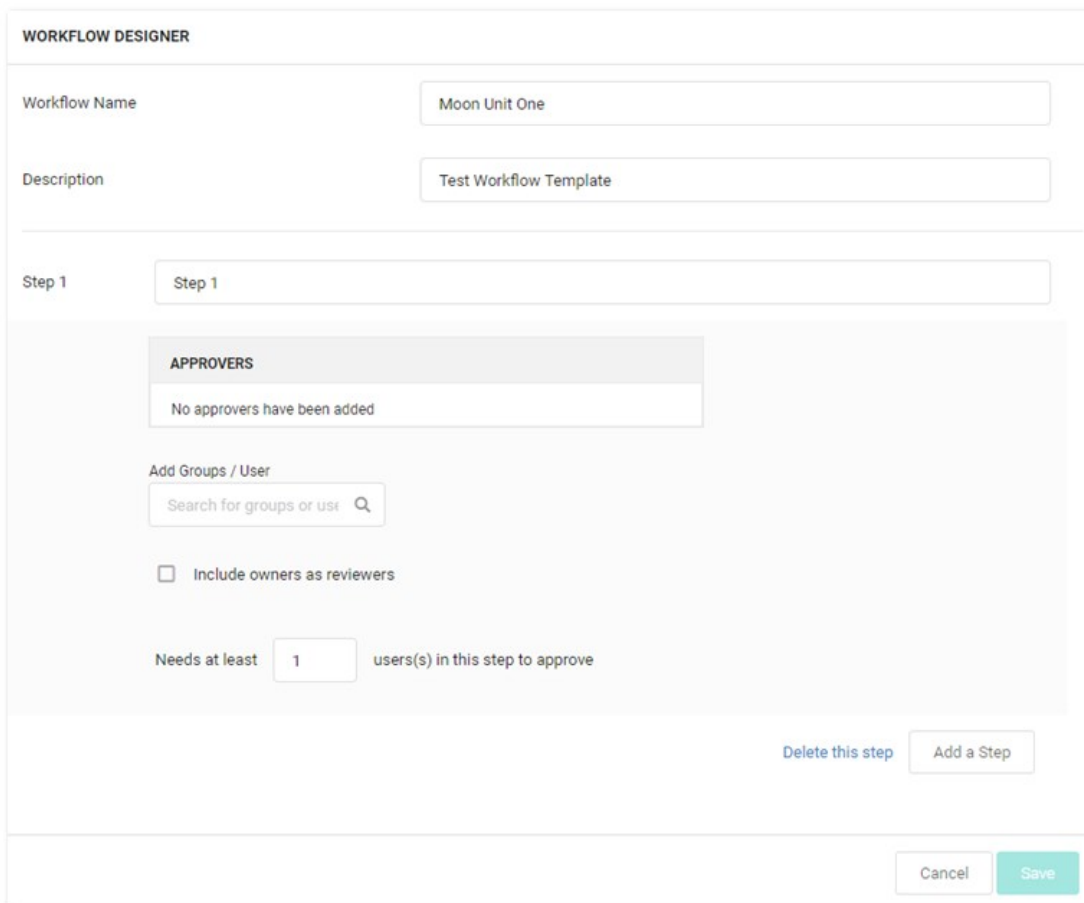
## Task 1: Access the Workflow Designer:

1. Click the **Create Workflow Template** button.



A dialog box titled "Create Workflow Template". It contains two text input fields: "Workflow Name \*" and "Description". At the bottom right, there are two buttons: "Cancel" and "Create Workflow Template".

2. Type the workflow template's name and descriptions in their text boxes. Once you type the name, the Create Workflow Template button becomes enabled.
3. Click the **Create Workflow Template** button. The Edit page for the new workflow template appears.

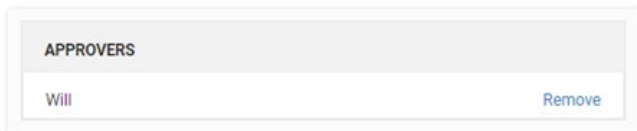


The "WORKFLOW DESIGNER" edit page. It features a header "WORKFLOW DESIGNER". Below it are two text input fields: "Workflow Name" (containing "Moon Unit One") and "Description" (containing "Test Workflow Template"). A section titled "Step 1" contains a text input field with "Step 1". Below this is a section titled "APPROVERS" with a message "No approvers have been added". Underneath is a search bar labeled "Add Groups / User" with the placeholder text "Search for groups or user" and a magnifying glass icon. Below the search bar is a checkbox labeled "Include owners as reviewers". At the bottom of the approvers section, it says "Needs at least" followed by a text input field containing "1" and the text "users(s) in this step to approve". At the bottom right of the main content area are two buttons: "Delete this step" (in blue text) and "Add a Step". At the very bottom right of the page are two buttons: "Cancel" and "Save".

A new workflow template has only one empty step by default.

## Task 2: Set up the first step:

1. (Optional) Type a name for the first step in the **Step 1** text box, such as "Line Managers."
2. Click the **Add Groups / Users** (search) text box.
3. Type the name of the user or group you desire as approvers, options appear in the dropdown.
4. Click the desired user or group. It appears in the Approvers table:

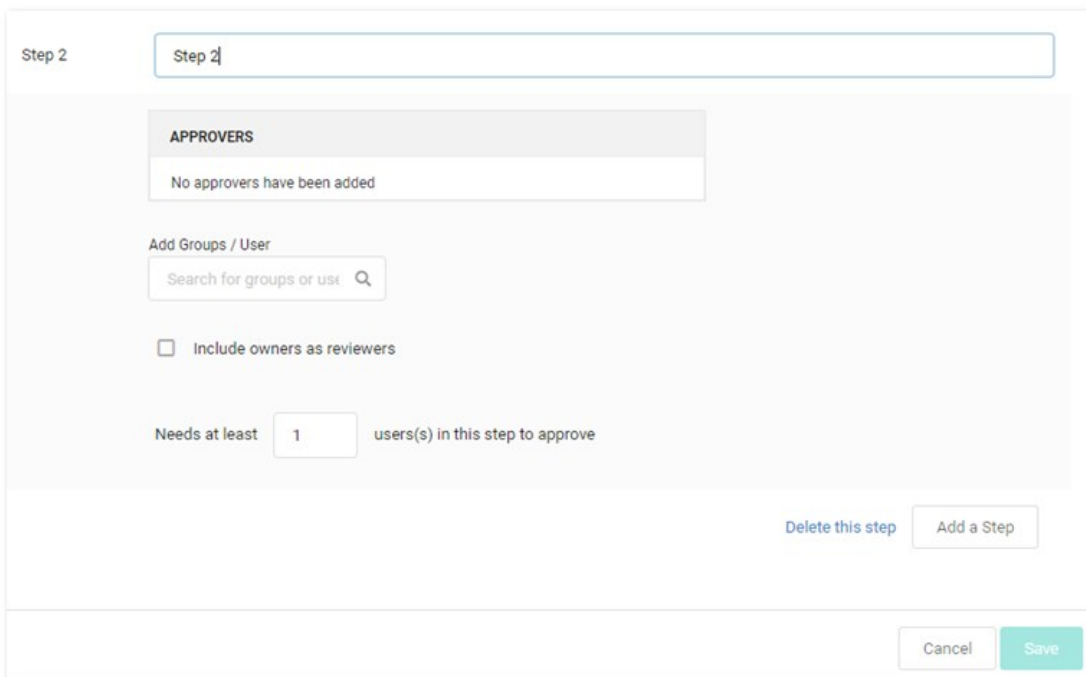


APPROVERS
Will <span>Remove</span>

5. Repeat as desired.
6. (Optional) To automatically include the owner of the secret the template is assigned to, click to select the **Include owners as reviewers** check box.
7. (Optional) If you wish to have multiple approvers required on the step, type the minimum required in the **Needs at least...** text box.

## Task 3: (Optional) Add more steps:

1. Click the **Add a Step** button. A new step appears below the first one:



Step 2

Step 2

APPROVERS

No approvers have been added

Add Groups / User

Search for groups or users

☐ Include owners as reviewers

Needs at least

1

users(s) in this step to approve

Delete this step

Add a Step

Cancel

Save

2. Repeat the process for step one.
3. (Optional) Keep adding steps till satisfied.
4. Click the **Save** button to create the access-request workflow template. The template exits editable mode:

Designer

Audit

WORKFLOW DESIGNER

EDIT

Workflow Name

Line Manager Approval

Description

Step 1

Line Managers

APPROVERS

Will

Barry

Include owners as reviewers

No

Needs at least

1

users(s) in this step to approve

- Click the **Workflow Templates** link on the top of the page to return to the table.

To delete a workflow template:

1. Access the Workflow Designer:

WORKFLOW DESIGNER

Workflow Name

Will Workflow 01

Description

One step approval (Barry)

---

Step 1

Step 1

APPROVERS

Barry

Remove

Add Groups / User

Search for groups or use

☐

Include owners as reviewers

Needs at least

1

users(s) in this step to approve

Delete this step

Add a Step

Cancel

Save

2. Click the workflow template you want to copy in the **Workflow Templates** table. That template appears:

Admin > Workflow Templates > Will Workflow 01

Duplicate Delete

**Designer**  
 Audit

**WORKFLOW DESIGNER** [EDIT](#)

Workflow Name Will Workflow 01

Description One step approval (Barry)

---

Step 1 Step 1

**APPROVERS**

Barry

Include owners as reviewers No

Needs at least 1 users(s) in this step to approve

3. Click the **Delete** button. A confirmation popup page appears.

4. Click the **Yes, Delete** button.

**Note:** Because workflows based on the template may still be in play, the template is not completely deleted. Instead, it is inactivated. You can reactivate the template later. See [Accessing the Workflow Designer](#)."

If you need to create a new workflow template that is like one you already have, you can save time by copying the similar template and then making the any changes:

1. Access the Workflow Templates page:

Workflow Templates

Create Workflow Template

52 Items

Show Inactive ☐

1 of 4 ◀ ▶

Workflow Template Name <span>↓</span>	Type	Active	
workflow_test_01	Access Request	Yes	
workflow_Step	Access Request	Yes	
workflow_Policy	Access Request	Yes	
workflow_group	Access Request	Yes	
Workflow_Del	Access Request	Yes	
Workflow_01	Access Request	Yes	
Workflow Template 2 Step - Marrio - Barry	Access Request	Yes	
Workflow Template 1-Step Barry	Access Request	Yes	
WK01	Access Request	Yes	
Will Workflow 01	Access Request	Yes	
WFT_001	Access Request	Yes	
WF_template01	Access Request	Yes	
testWF	Access Request	Yes	

2. Click the workflow template you want to copy in the **Workflow Templates** table. That template appears:

Admin > Workflow Templates > Will Workflow 01

[Duplicate](#) [Delete](#)

**Designer**  
Audit

**WORKFLOW DESIGNER** [EDIT](#)

Workflow NameWill Workflow 01

DescriptionOne step approval (Barry)

Step 1Step 1

**APPROVERS**

Barry

Include owners as reviewersNo

Needs at least 1 users(s) in this step to approve

- Click the **Duplicate** button. The new template appears, filled in the same as the original, including the name:

**WORKFLOW DESIGNER**

Workflow Name

Will Workflow 01

Description

One step approval (Barry)

Step 1

Step 1

**APPROVERS**

Barry

Remove

Add Groups / User

Search for groups or users

☐ Include owners as reviewers

Needs at least

1

users(s) in this step to approve

Delete this step

Add a Step

Cancel

Save

4. Change the name and edit as desired.
5. Click the **Save** button when finished.

To edit the template:

1. Click the blue **Edit** button. The Workflow Designer page becomes editable:
2. At this stage the process is nearly identical to creating a new workflow template. The only difference is many of the parameters and additional steps are already completed. Change them as desired. If you want to eliminate an entire step, click the **Delete This Step** link for that step.

**Note:** You cannot make any changes to the behavior of a workflow template if there are active requests using that template without cancelling those requests. An active request is any unexpired request that has not been approved, denied, or canceled by the user. If you do make an alteration, any requests are canceled and those affected are notified by email so they can resubmit their requests. Any user editing the template is notified when he or she tries to save changes on the canceled request.

Consider the following when setting up an access-request workflow template:

- Use multiple-step approval workflows when you need to have different people (such as different departments) sign off on an approval request.
- We do not recommend assigning equally important approvers or groups to multiple steps. Having a single step with multiple approvers works better. Remember, steps are best used for hierarchical approval--an approval chain.
- A reviewer can only respond to a request once. If you have the same user as a reviewer in multiple steps, that approver cannot respond if he or she already responded on an earlier step. In addition, the reviewer's earlier approval does **not** count towards the number of approvals required in later steps. Thus, if you want to assign the same user as a reviewer in multiple steps, make sure that you have enough reviewers in each step to approve without that user.
- A well-crafted workflow template design ensures there are enough approvers in a group to satisfy the multiple approver (x of n reviewers must approve) requirement, but group membership can change after the workflow is created. Thus, if you remove members from groups used by workflows, ensure there are still enough members in those groups to approve requests.

## Security and Hardening

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Overview

There are 3 reasons for Thycotic products to call home—when:

- Checking for available updates
- Activating licenses
- Reporting anonymized usage metrics

Each of these communications is explained below and can be disabled or avoided.

## Checking for and Downloading Updates

Frequency: Once per day

The software checks for available updates and sends the following information to Thycotic's update server:

- .NET Framework version
- IP address of the installed instance
- Microsoft SQL Server version
- Microsoft Windows version
- Product version

Checking for updates and sending this information will only occur if both of the following are true:

- The server has outbound network access, which you can block at a firewall.
- The "Allow Automatic Checks for Software Updates" check box is enabled at Admin > Configuration (see below).

No sensitive data is sent during the check. Its only purpose is to alert administrators if a software update is available. The queried website is also used to download new software versions during the upgrade process. If you wish to whitelist the specific servers involved, they are:

- d36zgw9sidnotm.cloudfront.net:443
- updates.thycotic.net:443
- updates.thycotic.net:80
- tmsnuget.thycotic.com/nuget/

## License Activation

Frequency: when a new license is activated.

The software also sends contact and license-key information, provided by the administrator, to Thycotic during online license activation. The same information is sent via another computer for offline activation.

## Reporting Anonymized Usage Metrics

**Note:** This section only applies to Secret Server and Secret Server Cloud versions 10.6 and above.

Thycotic collects anonymized usage data to help guide future research and development plans so that product improvements can provide the greatest benefit to customers.

Frequency: Once per day

Secret Server returns anonymized metrics across several categories:

- A unique identifier number that allows Thycotic to correlate metrics from the same server over time but does not contain any information that identifies the customer.
- License information, including edition information and the number of licensed users but not license keys or other identifying data.
- Product configuration and usage, such as number of secrets stored and product feature status, not including any identifying data.
- Product environment, including host operating system and SQL server version, not including any identifying data.

Reporting of anonymized metrics only occurs if:

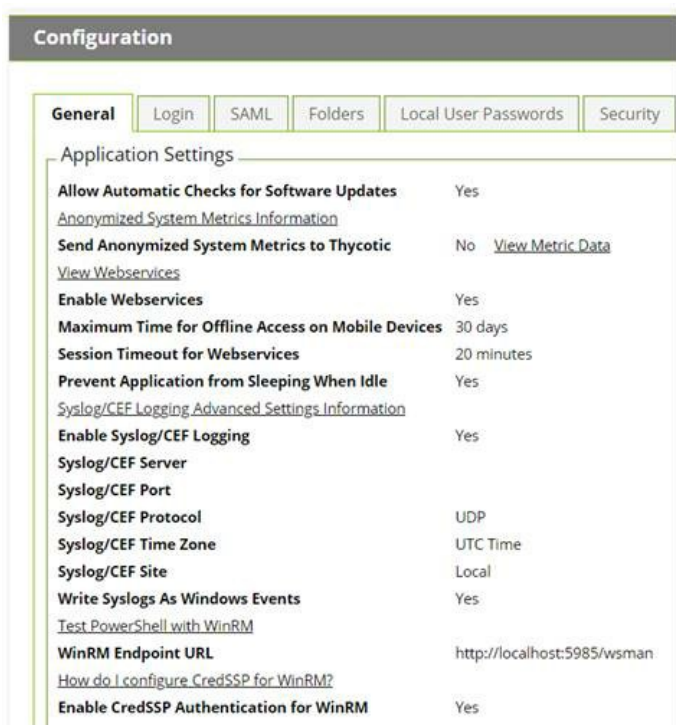
- The server has outbound network access (you can block your server at a firewall if desired)
- The "Send Anonymized System Metrics to Thycotic" setting under Admin > Configuration is enabled (see below).

You can allow for the metrics reporting on your firewall by whitelisting: <https://telemetry.thycotic.net:443>.

## Setting and Viewing Secret Server Telemetry

To set or view telemetry:

1. Click **Admin > Configuration**. The Configuration page on the General tab appears:



The screenshot shows the 'Configuration' page with the 'General' tab selected. The page has a header 'Configuration' and a sub-header 'Application Settings'. Below this, there are several settings with their current values and links to view more information.

Setting	Value	Link
Allow Automatic Checks for Software Updates	Yes	
<a href="#">Anonymized System Metrics Information</a>		
Send Anonymized System Metrics to Thycotic	No	<a href="#">View Metric Data</a>
<a href="#">View Webservices</a>		
Enable Webservices	Yes	
Maximum Time for Offline Access on Mobile Devices	30 days	
Session Timeout for Webservices	20 minutes	
Prevent Application from Sleeping When Idle	Yes	
<a href="#">Syslog/CEF Logging Advanced Settings Information</a>		
Enable Syslog/CEF Logging	Yes	
Syslog/CEF Server		
Syslog/CEF Port		
Syslog/CEF Protocol	UDP	
Syslog/CEF Time Zone	UTC Time	
Syslog/CEF Site	Local	
Write Syslogs As Windows Events	Yes	
<a href="#">Test PowerShell with WinRM</a>		
WinRM Endpoint URL	http://localhost:5985/wsman	
<a href="#">How do I configure CredSSP for WinRM?</a>		
Enable CredSSP Authentication for WinRM	Yes	

2. (Optional) To view the JSON file for the possible sent metrics, click the **View Metric Data** link. The file appears:

```
{
  "identifier": "cef588896e3e9718d59ccdd0f9e77568",
  "licenses": [],
  "features": [
    {
      "name": "Remote Password Changing",
      "enabled": true,
      "count": 0,
      "countDescription": "Secrets with AutoChange enabled"
    },
    {
      "name": "Heartbeat",
      "enabled": true,
      "count": 614,
      "countDescription": "Secrets with Heartbeat enabled"
    },
    {
      "name": "Checkout",
      "enabled": true,
      "count": 5,
      "countDescription": "Secrets with Checkout enabled"
    },
    {
      "name": "Checkout Change Password",
      "enabled": false,
      "count": 0,
      "countDescription": "Secrets with Checkout change password enabled"
    },
    {
      "name": "DoubleLock",
      "enabled": true,
      "count": 0,
      "countDescription": "Secrets with DoubleLock enabled"
    },
    {
      "name": "Request Access",
      "enabled": true,
      "count": 104,
      "countDescription": "Secrets with Request Access enabled"
    },
    {
      "name": "Request Access Editors need approval",
      "enabled": true,

```

3. Scroll down and click the **Edit** button. The tab changes to edit mode:

**General** | Login | SAML | Folders | Local User Passwords | Security

Application Settings

**Allow Automatic Checks for Software Updates** ☒

[Anonymized System Metrics Information](#)

**Send Anonymized System Metrics to Thycotic** ☐ [View Metric Data](#)

[View Webservices](#)

**Enable Webservices** ☒

[Maximum Time Offline Explanation](#)

**Maximum Time for Offline Access on Mobile Devices**

Days	30
Hours	0

4. Click to select or deselect the **Send Anonymized System Metrics to Thycotic** check box.

5. Click the **Save** button.

To secure your ASP session and forms authentication cookies, perform the following steps:

1. Ensure that there is an SSL certificate installed for the instance.
2. Log in to Secret Server using HTTPS.
3. Navigate to the **Admin > Configuration** page
4. Click on the **Security** tab.
5. Click the **Edit** button
6. Check the **Force HTTPS/SSL** check box
7. Click the **Save** button.
8. Open the `web-cookie.config` file in the application installation folder.
9. Set `requireSSL` to `true`.

Save and Close the file.

10. Open the `web-auth.config` file in the application installation folder.
11. Set `requireSSL` to `true` . If the attribute does not exist, add it to the `forms` tag.

Save and Close the file.

12. Recycle the Secret Server's application pool.

**Important:** If you later migrate Secret Server to a new server, SSL must be configured on the new server before you can log in due to these settings. If you want to log in prior to configuring SSL, reverse steps 8 through 13 and recycle the application pool.

## Introduction

This document outlines security hardening for securing your Secret Server (SS) instance, whether it be installed on a single server or in a multi-clustered environment.

**Note:** Throughout this guide, many references are made to "configuration" settings. Unless otherwise specified, this refers to the settings found by selecting **Configuration** from the **Admin** menu in SS.

## Overview

It is critical to secure your SS implementation. That needs to include a layered approach to security (defense in depth), including the operating system, software updates, physical access, protocols, system settings, backups, and personnel procedures. This section of the guide links to other sections and knowledge base articles (KBAs) containing more details.

## Best Practices

### General

- **Keep Windows up-to-date:** Microsoft regularly releases security patches that resolve vulnerabilities in Windows operating systems.
- **Backup at least daily:** Consider your disaster recovery plan. Review the [Business Continuity and Disaster Recovery Planning](#) KBA for more information.
- **Review system log for errors:** Periodically check the system log (Admin > System Log) for recurring errors. Also do so after any upgrades.
- **Whole-disk encryption:** Use whole disk encryption, such as [BitLocker](#), with a trusted platform module (TPM) to prevent those with physical access from removing disks to gain access to your SS application by circumventing OS and application authentication.
- **Security Hardening Standards:** Consider security hardening standards that apply to either the operating system or applications, such as IIS or Microsoft SQL. Our application does not currently have full compatibility with third party standards such as CIS Level 1 hardening or the Microsoft Published Security Baselines. We are compatible with CIS Level 2 hardening and have STIG compatibility.

**Note:** Attaining full security-hardening standards compatibility is a Thycotic priority.

### Active Directory

On Active Directory domain controllers, there is a set of unsafe default configurations for LDAP channel binding that allow LDAP clients to communicate with them without ensuring LDAP channel binding and LDAP signing. This can open the controllers to privilege vulnerabilities. See [2020 LDAP channel binding and LDAP signing requirements for Windows](#) for details.

### Database

- **Limit access to your Secret Server database:** When you create your SS database, limit access to as few users as possible. We recommend you disable the "sa" account in the SQL instance that contains SS.
- **Limit access to other databases:** When you create a database account for SS, you should ensure it only has access to the SS database.
- **Use Windows Authentication for database access:** Windows authentication is much more secure than SQL authentication. See [Choose an Authentication Mode](#) (TechNet article) for details. To use Windows authentication in SS, you need to create a service account. See the [Using Windows Authentication to access SQL Server](#) KBA for details.
- **Limit access to your database backups:** Database backups are critical for disaster recovery, but they also carry a risk if

someone gains access. The SS database is encrypted, but you should still limit access to ensure maximum security. Limit access to database backups to as few users as possible.

- **Don't share a SQL instance with less secure databases:** Putting the database on a server with less-secure database instances can expose vulnerabilities. For example, an attacker could use SQL injection on another application to access your private SS database. If you intend to put SS on a shared SQL instance, ensure that the other databases are classified internally as sensitive as SS and have similar security controls in place.
- **Review Microsoft's recommendations for SQL security:** See the [Securing SQL Server](#) article in Microsoft's documentation.

**Note:** SS also supports SQL Server Transparent Data Encryption (TDE) for further protection of the database files. This can have a slight performance impact on the environment and can increase the complexity of the database configuration. Please review this page for more information: [Transparent Data Encryption \(TDE\)](#).

## Application Server

- **Use SSL (HTTPS):** We require using Secure Sockets Layer (SSL) encryption to ensure that all communication between the Web browser and SS is secure. We recommend you install a third-party certificate, domain certificate, or self-signed certificate on your website. For information on creating and installing a self-signed certificate, please see the [Installing a Self-Signed SSL/HTTPS Certificate](#) KBA.
- **Force SSL (HTTPS):** Even after you install an SSL certificate, users may still be able to access SS through regular HTTP. To that, enable the "Force HTTPS/SSL" option in SS at Admin > Configuration on the **Security** tab.
- **Limit access to your Secret Server directory.** This contains the SS encryption key, as well as the database connection information (these values are encrypted but remember "defense in depth." Try to grant access to as few users as possible).
- **Limit logon rights to the application server.** Administrators accessing the Application Server directly could attempt to monitor memory in use on the server. SS does several things to protect application memory but the best safeguard is to limit access to the Application Server to as few users as possible.
- **Protect your encryption key.** The encryption key for SS is contained in the encryption.config file, which resides in your SS directory. This file is obfuscated and encrypted, but "defense in depth" would require limiting access to the file. [Using DPAPI to encrypt your encryption.config file](#) is one option. This will use machine-specific encryption to encrypt the file. Make sure you back up the original file before enabling this option. To further protect the file, you can enable EFS encryption. EFS (Encrypting File System) is a Microsoft technology that allows a user or service account to encrypt files with login passwords. For more details, read [Protecting Your Encryption Key Using EFS](#) in this same article. The most secure option is to use a Hardware Security Module (HSM) to protect the SS encryption key. For more information see the [HSM Integration Guide](#).

## Application Settings

- **Use doublelock for your most sensitive secrets:** DoubleLock is a feature in SS that allows secrets to be protected with additional AES256 encryption keys. Each user gets their own public and private key set when using doublelock. Their private key is protected by an additional password (user-specific, not a shared password) that each user must enter when using doublelock. DoubleLock protects from situations where you accidentally assign someone to the wrong AD group or an attacker gains full access to both your database and Web server - they still will not be able to access doublelocked secrets. For more information, refer to [Using DoubleLock](#) (KB).
- **Secure the local admin account:** When you create the first user in SS, it is a privileged admin account that you can use when your domain is down. We recommend that you choose a non-obvious name for this account and protect it with a very strong password. This password should be stored in a physical safe with limited access (there is no need to use this account except in emergencies where other accounts are not working if AD is down or some other reason).
- **Review activity reports:** It is a good practice to regularly review the activity and permissions reports. This can help find anomalies in secret permissions and login failures.

- **Use event subscriptions or SIEM to notify of any security anomalies:** Use event subscriptions to send email alerts on various events in the system, and syslog can send events to a SIEM tool for correlation. For example, this could be used to notify administrators if there are failed login attempts or if certain secrets are viewed.

## Security Hardening Report

SS contains a built-in security hardening report to provide a basic checklist of recommendations that can improve the security of SS and the data it houses. The items in this report range from common tasks, such as ensuring SSL is configured, to more advanced options like DPAPI encryption of the encryption key. To find this report, click the **Reports** on the dashboard, and then select the **Security Hardening** tab.

**Figure:** Security Hardening Report:

□

An X denotes a failure, and a checkmark denotes a pass. An exclamation point is a warning. Typically, SS could not detect a setting or all aspects of a check were not completed. For example, TLS 1.0 was disabled but TLS 1.1 was not.

You will find the following items in the report:

**Note:** The individual items below are in alphabetical order, not the order they are in the Hardening Report. The sections are in the same order as the report. This was because the report name does not always match the name of the corresponding label on the configuration UI control. In addition, the controls are not in the same order in the UI as their equivalents in the report.

### Configuration Section

#### Allow Approval for Access from Email

Recommendation: Off

Allow Approval For Access from Email is a convenience option that allows users to approve or deny a secret access request by clicking a link in the request email sent by SS. Allow Approval From Email does not require a user to authenticate with SS when approving access to a secret. This can be a security concern if the approver's email account becomes compromised, which could allow an attacker to mitigate MFA in some cases to complete an approval. Turn Allow Approval From Email off to get a pass result.

To disable this setting, find the **Permission Options** section of the **Configuration Settings** page and disable **Allow Approval for Access from Email**.

#### Browser AutoComplete

Recommendation: Off

Browser autocomplete allows Web browsers to save the login credentials for the SS login screen. These credentials are often kept by the Web browser in an insecure manner on the user's workstation. Allowing Autocomplete also interferes with the security policy of your SS by not requiring the user to re-enter their login credentials on your desired schedule.

To prevent the autocomplete feature, navigate to the **Configuration Settings** page and disable the **Allow AutoComplete** option on the **Login** tab.

#### File Attachment Restrictions

Recommendation: On

**Note:** Labeled **Enable File Restrictions** in the UI.

File attachment restrictions allows administrators to configure what kind of file attachments can be uploaded to secrets. This helps protect users from being tricked into downloading a malicious secret attachment. The file extension and maximum file size can be specified, such as:

\*.7z, \*.bmp, \*.ca-bundle, \*.cer, \*.config, \*.crt, \*.csr, \*.csv, \*.dat, \*.doc, \*.docx, \*.gif, \*.gz, \*.id-rsa, \*.jpeg, \*.jpg, \*.json, \*.key, \*.lic, \*.p7b, \*.pcf, \*.pdf, \*.pem, \*.pfx, \*.pkey, \*.png, \*.ppk, \*.pub, \*.tar, \*.tif, \*.tiff, \*.tpm, \*.txt, \*.vdx, \*.vsd, \*.vsdx, \*.xls, \*.xlsx, \*.xml, \*.zip

This security check will fail if the file attachment restrictions is not enabled. This check will return warnings if a potentially dangerous file extension is allowed, maximum file size is not specified, or maximum file size is greater than 30 MB.

Go to **Admin > Configuration > Security tab > File Restrictions section** to change these settings.

## Frame Blocking

Recommendation: On

**Note:** Labeled **Enable Frame Blocking** in the UI.

Do not allow SS to be opened in a <iframe> HTML tag on another, potentially malicious, site. This adds the HTTP header X-Frame-Options: DENY. This deters clickjacking and spreading potential XSS vulnerabilities.

Go to **Admin > Configuration > Security tab > Frame Blocking section** to change this setting.

## Force Password Masking

Recommendation: On

Setting: Same

Password masking prevents over the shoulder viewing of your passwords by a casual observer (passwords show as \*\*\*\*\*). Note the number of asterisks does not relate to the length of the password for added security.

As an administrator, you can force all the secret password fields in the system to be masked when viewed. To do this, enable **Force Password Masking** on the **Configuration Settings** page. Only secret fields marked as a password type field on the secret template will be masked. There is also a user preference setting which will force password masking on all secret password fields viewed by the user.

This **Mask passwords when viewing Secrets** setting is found in the **Tools > Preferences** section for each user.

**Note:** If the "Force Password Masking" configuration setting discussed above is enabled, this user preference setting will be overridden and cannot be disabled.

## Login Password Requirements

Passwords used by local users to log onto SS can be strengthened by requiring a minimum length and using a variety of character sets. We recommend a minimum password length of eight characters. In addition, all character sets (lowercase, uppercase, numbers, and symbols) are required to get a pass result.

Turn on these login password settings on the **Local User Passwords** tab of the **Configuration Settings** page.

## Maximum Login Failures

Recommendation: Reference the lockout policy for your organization. Most often, this setting will mirror the AD GPO lockout policy.

The maximum number of login failures is the number of attempts that can be made to log into SS as a user before that user's account is locked. A user with the administer users role permission will then be required to unlock the user's account. The maximum failures allowed should be set to five or less to get a pass result.

Change the **Maximum Login Failures** setting on the **Login** tab of the **Configuration** settings.

## Remember Me

Recommendation: Off

**Note:** Labeled **Allow Remember Me** in the UI.

"Remember Me" is a convenience option that allows users to remain logged onto SS for up for a specific period. This setting can be a security concern because it does not require re-entry of credentials to gain access to SS.

Disable **Allow Remember Me** on the **Login** tab of the **Configuration** page to get a pass result. It must be set to be valid for 1 day or less to not get a fail result.

**Note:** Closing a browser completely (all tabs) will log the user out of SS, regardless of this setting.

## Secure Session and Forms Auth Cookies

**Note:** Secure Session and Forms *Authentication* Cookies.

Recommendation: See KBA

Cookies contain potentially sensitive information that can allow users to log onto application. By default, cookies are not marked with the secure attribute. That is, **they are transmitted unencrypted when a user accesses SS through HTTP instead of HTTPS**.

For more information about how to secure your cookies, see [Secure ASP Session and Forms Authentication Cookies](#) (KBA).

## Markdig.Syntax.Inlines.EmphasisInline

**Note:** Labeled **Allow HTTP Get** in the UI.

Recommendation: Off

Web service HTTP get requests are allowed. Allowing HTTP GET requests allows REST-style calls to many SS Web service methods. This can be a security concern because simply clicking a link to the Web service, created by a malicious user, would cause it to be executed.

Disable **Allow HTTP Get** under the **Security** tab of the **Configuration** settings to pass.

## Zero Information Disclosure Error Message

Recommendation: On

Replace all error messages with a custom "contact your admin" message. Error messages can be very helpful when diagnosing installation and configuration issues. However, having errors displayed to a potential attacker can provide him or her with the critical information they need to perform a successful attack.

To hide error messages from the end user, add the ZeroInformationDisclosureMessage application setting to the web-appSettings.config file. This file is located in directory containing the SS application files. Add the key below to this file in between the <appSettings> tags. The contents of that tag is displayed as a message that appears to the user whenever an error occurs in the system. For example:

```
<add key="ZeroInformationDisclosureMessage" value="An error occurred in the application. Please contact your administrator." />
```

**Note:** This setting is enabled by default in SS 10.7.26+.

## Database Section

### SQL Account Using Least Permissions

Use the fewest SS permissions as possible in the SQL Account used to access the database. We recommend using a least permission

approach where the account only has dbOwner. See [Installing and Configuring SQL Server](#).

## SQL Server Authentication Password Strength and Username

**Note:** This section addresses two separate but closely related settings: "SQL Server Authentication Password Strength" and "SQL Server Authentication Username."

Recommendation: Change settings as needed

SQL Server authentication requires a username and a strong password. Strong passwords are eight characters or longer and contain lowercase and uppercase letters, numbers, and symbols. In addition, the SQL Server authentication username should not be obvious. Using "sa", "ss" or "secretserver" is not accepted.

You can change the credentials of a local SQL account through SQL Server Management Studio, where the SS database is located. The SQL Server authentication credentials used by the application can then be changed by going to the installer `installer.aspx` page and changing them on step three. Using Windows authentication to authenticate to SQL Server is allowed.

For details about creating or modifying a SQL account for SS, see the [Installation Guide](#).

## Windows Authentication to Database

Recommendation: Configure

**Note:** If the SQL instance is *solely* using Windows authentication, this check will pass. If using mixed mode, it will fail—even you are using both Windows authentication plus SQL authentication.

Windows authentication takes advantage of Windows security to provide secure authentication to SQL Server. The SQL Server authentication options can be changed by going to the installer (`installer.aspx`) and changing them.

**Note:** See the [Installation Guide](#) for instructions on configuring Windows authentication to SQL Server.

## Environment Section

### Application Pool Identity

Recommendation: Check configuration

The Application Pool identity appears to be a member of the administrators group on the system. This puts the system at risk by giving more access than necessary.

Check the identity of the application pool used by SS in IIS. The Application Pool should be configured to use a service account and not be given unrestricted access to the server or domain.

### DPAPI or HSM Encryption of Encryption Key

Recommendation: On

Encrypt your SS encryption key, and limit decryption to that same server. Data Protection API (DPAPI) is an encryption library that is built into Windows operating systems. It allows encryption of data and configuration files based on the machine key. Enabling DPAPI Encryption in SS protects the SS encryption key by using DPAPI, so even getting access to the SS encryption key is not enough to be useful—the machine key is required. If you enable this option, back up your encryption key first, as a DPAPI encrypted file can only be used by the machine it was encrypted on.

To enable DPAPI encryption, to to **Admin > Configuration > Security tab** and click the **Encrypt Key Using DPAPI** button.

**Note:** This check also passes if Hardware Security Module (HSM) integration is enabled.

## SSL Section

### Require SMTP SSL

Recommendation: On

**Note:** Labeled **Use SSL** (on the Email tab) in the UI.

**Note:** We strongly recommend enabling this setting.

SMTP SSL is required to ensure that all communication between SS and the email server is encrypted. Enable the "Use SSL" option in Secret Server to get a pass result.

Go to **Admin > Configuration > Email tab > Use SSL** to enable the setting.

### Require SSL

**Note:** Labeled **Force HTTPS/SSL** in the UI.

Recommendation: On

**Note:** We **strongly** recommend using SSL for SS.

Only use SSL (HTTPS) for SS access. Secure Sockets Layer (SSL) is required to ensure that all communication between the Web browser and SS is encrypted. To do so, you need an SSL certificate. You may use an existing wildcard certificate, create your own domain certificate, or purchase a third-party SSL certificate for the SS website. For testing, you can use a self-signed certificate. See [Installing a Self-Signed SSL/HTTPS Certificate](#) (KB) for more information.

Once the SSL certificate is installed, enable **Force HTTPS/SSL** on the **Security** tab of the **Configuration** page to force users to only access SS over HTTPS and to receive a pass in the report.

### SSL/TLS Hash

Recommendation: Confirm or remediate

Check the digest algorithm of the certificate. If the algorithm is SHA1, this check returns a warning because SHA1 is being phased out. If the digest algorithm is MD2, MD4, or MD5, the check will fail because they are not secure. SHA256, SHA384, and SHA512 will pass. This check fails if SS cannot be loaded over HTTPS.

Example warning:

"The digest algorithm is sha1RSA, which is considered weak. The algorithm is being phased out and should be replaced with a better algorithm when it comes time to renew the SSL certificate."

Go to the browser's certificate information when logged onto SS. This is usually a button next to the URL text box.

### SSL/TLS Key

Recommendation: Confirm or remediate

Check the key size of the HTTPS certificate used. If it is RSA or DSA, the key must be at least 2048-bit to pass. If the signature algorithm of the certificate is ECDSA, the key size must be at least 256-bit to pass. If the algorithm of the certificate is unknown, the result shows "unknown". This check fails if SS cannot be loaded over HTTPS.

Go to the browser's certificate information when logged onto SS. This is usually a button next to the URL text box.

## SSL/TLS Protocols

Recommendation: Confirm or remediate

Check for legacy SSL or TLS protocols, which should not be used in a secure environment. If the server accepts SSLv2 or SSLv3 connections, this check will fail. SSLv2 is not considered secure for data transport, and SSLv3 is vulnerable to the POODLE attack. If this server does not support TLSv1.1 or TLSv1.2, this check will give a warning because they are recommended. The SSL certificate used may affect what protocols can be used, even if they are enabled. This check will fail if SS cannot be loaded over HTTPS.

**Note:** You can check and modify these settings in the Window registry. See [Transport Layer Security \(TLS\) Registry Settings](#) in Microsoft's documentation.

Example warning:

"The server supports the accepts SSLv2 or SSLv3 connections protocol, which are weak. Consider disabling these protocols."

## Using HTTP Strict Transport Security

**Note:** Labeled **Enable HSTS** in the UI.

HTTP Strict Transport Security (HSTS) is an additional security layer for SSL. HSTS allows SS, Password Reset Server, or Group Management Server to inform browsers that it should only be accessible over HTTPS. With this setting enabled, visitors are automatically redirected by their browser to the HTTPS-enabled site.

When the **Force HTTPS/SSL** option is enabled on the **Security** tab of the **Configuration** page, the **Enable HSTS** check box will be displayed. After the option is turned on, you can click **Advanced** to specify the maximum age in seconds for how long the policy should be in effect before re-evaluating. The default value is 25200 seconds (7 hours). We recommend setting this as high as possible, up to a year, if the site, should never be accessed without TLS or SSL.

For details about this, see [Securing with HTTP Strict Transport Security \(HSTS\)](#) (KB).

## Security Settings Not in the Hardening Report

### Apply TLS Certificate Chain Policy and Error Auditing

Recommendation: Confirm or remediate

Add audits for TLS certificate validation. Auditing will apply to all Active Directory domains using LDAPS and Syslog using TLS. Certificate policy options, including ignoring certificate revocation failures, apply to syslog using TLS only. The default is the most strict so the certificate chain policy may need to be updated. TLS errors will be logged to Security Audit Log found on the Administration page.

Disable the **Admin > Configuration > Security tab > Apply TLS Certificate Chain Policy and Error Auditing** setting.

TLS errors are logged to the **Security Audit** log at **Admin > See All > Security Audit Log**.

### Enable FIPS Compliance

Recommendation: Off

Only allow FIPS-compliant encryption schemes. FIPS (Federal Information Processing Standards) is a set of standards for government entities. It covers many things, including encryption. For businesses, FIPS can be counter productive because it restricts them from using newer or improved existing encryption methods. In addition to enabling this setting, several other tasks are required to meet this standard, including enabling it for Windows itself. For more information, see [Enabling FIPS Compliance in Secret Server](#) (KBA) for details.

Go to **Admin > Configuration > Security tab > FIPS Compliance** to change this setting.

## Key Rotation

Recommendation: Review KBA

**Note:** Key rotation is not a setting but an activity. It is included here for completeness (the entire Configuration Security tab)

Secret key rotation changes out the encryption key for secret data and re-encrypts that data with a new key. This helps you to meet compliance requirements mandating that encryption keys are changed on a regular basis. See [Secret Key Rotation](#) (KBA) for details.

## Two-Factor Authentication

Users must authenticate to SS at least once using either local SS credentials or their Active Directory credentials. In addition, you can protect SS by enabling two-factor authentication (2FA). 2FA is an additional security layer, such as a text message PIN code sent to your smart phone. The following options are supported by SS for 2FA:

### SAML

SS supports the Security Assertions Markup Language (SAML), which provides a more centralized method of adding 2FA to the SS log on. Please see the [Secret Server SAML Configuration Guide](#).

### Email

Using email for 2FA means that after authenticating with their password, the user receives an email containing a one-time PIN code to enter. For this to work, an SMTP server must be configured in SS and each user must have a valid email address associated with their account. For Active Directory users, the email address will be synced automatically from their domain account.

Check user email addresses at **Admin > Users**.

### Soft Tokens

Soft tokens using the Time-based One-time Password (TOTP) algorithm, such as Google Authenticator and Microsoft Authenticator, are supported by SS 2FA. Users are prompted to enter a token displayed on their mobile device each time they log onto SS. The time-based token changes on a regular interval (such as 30 seconds).

### RADIUS

One option is to use a Remote Authentication Dial-In User Service (RADIUS)-compliant device, such as an RSA or CryptoCard token, as the second form of authentication. The user is prompted to enter his or her RADIUS password after initial authentication is done with their SS or AD password.

To set this up, you first need to configure SS to integrate with your RADIUS server, and then you can enable it for individual users or for by domain.

See [Enabling RADIUS Two-Factor Authentication](#) for details.

### Duo Security

Using this method requires that you have an active account for Duo Security. Duo Security provides several options for 2FA. The API hostname, integration key, and secret key values are required for SS to authenticate Duo users.

See [Configuring DUO for Two Factor](#) for details.

## Enabling Two-Factor Authentication

### Enabling for Users

To enable two-factor authentication for a user or several users at once, select **Users** from the **Admin** menu and then select the users in the grid. Use the bulk operation drop-down menu to choose the type of authentication to enable.

**Note:** If prerequisite settings are not configured, the 2FA option may be disabled or will not appear as an option. See the descriptions above for information about prerequisites for each type of two-factor authentication.

## Enabling per Domain

Two-factor authentication can also be enabled per domain if you are syncing users from Active Directory. To do so, select **Active Directory** from the **Admin** menu and then click **Edit Domains**. Click the domain name and then click **Advanced (not required)** to reveal the **Auto-Enable Two Factor for New Users** setting. Select this checkbox and click **Save and Validate**.

## Roles

SS uses role-based access control, which allows administrative and user capabilities to be partitioned by role. This can allow for granular control over which areas of the application a user has access to, for example, allowing someone the rights to manage licenses and view reports in SS but nothing else.

## Controlling Access to Features Using Roles

### Limiting Role Access to the Export Permission

Exporting secrets from your SS as text is very helpful for meeting regulations in certain industries (secrets can then be printed to paper and locked in a physical safe). It can also be used as another disaster recovery option, but access to exporting data from the SS should be tightly controlled. You could create a separate role with just the export permission for anyone needing to export secrets.

### Unlimited Administration Mode

Unlimited administration mode allows any role with the "unlimited administrator permission" to see all secrets in the SS. This mode is very helpful for recovering passwords in emergencies or when staff are terminated. You can tightly control access to this feature by splitting out the role permissions for "administer configuration unlimited admin" and "unlimited administrator" into two different roles. This allows you to create the "two-key effect" for access to the mode. See [Using Two Roles for Access to Unlimited Administration Mode](#) (#Using\_Two\_Roles\_for\_Access\_to\_Unlimited\_Administration\_Mode), below, for details.

### Limiting Role Access to Secret Templates

Anyone with access to modify your secret templates can change the definitions of the data being stored, and this access should be tightly controlled. Your secret templates are unlikely to need changing once you have defined them, so limiting access to a select number of individuals is typically sufficient.

### Monitoring Roles with Event Subscriptions

Another option when protecting roles is to configure event subscriptions to notify appropriate staff in the event that Roles are changed or assigned. Event subscriptions are email alerts that can be sent to users, groups or specific email addresses, based on different events in SS. There are also events available around the "unlimited administrator" role to further protect it from misuse.

### Using Two Roles for Access to Unlimited Administration Mode

We recommend determining which role permissions should or should not be combined for users before assigning roles and allowing users access to the application. Part of that is planning access to the "unlimited administration" mode. Users with the "administer configuration unlimited admin" role permission can enable that mode. Once the system is in the mode, users with the "unlimited administrator" role permission can view all secrets in SS and access all configuration settings. So a user with both permissions can enable the "unlimited

administration" mode and then view all the secrets or make any configuration change.

To prevent a single person from having that much access, the two role permissions should be given to two different roles and only those roles, and nobody should have access to both of the roles. That enforces accountability and requires the cooperation of two people to enter "unlimited administration" mode.

A solution is to create the two roles, each containing one of the permissions, and then take those two permissions out of the day-to-day administrator role and any other roles besides the two. You can then assign either one of those roles to trusted people with no single person having both roles.

Thus, the access procedure is:

1. User A with the role with the "administer configuration unlimited admin" permission puts the system into "unlimited administration" mode. Not having the correct role, user A cannot make any changes requiring the "unlimited administrator" permission.
2. User B with the role with the "unlimited administrator" permission performs any configuration or accesses secrets only available to that role.
3. When User B is finished, user A takes the system out of "unlimited administration" mode.
4. User B can no longer make any changes requiring the "unlimited administrator" permission because roles with that permission can only be accessed in "unlimited administration" mode. User A cannot make any changes either because User A does not have the role with the "unlimited administrator" permission.

Additional safeguards included:

- Enabling or disabling "unlimited administration" mode is audited, and a comment should be provided each time it is enabled.
- When "unlimited administration" mode is enabled, a banner appears at the top of every SS page notifying users that their secrets can currently be viewed by an unlimited administrator.
- Event subscription notifications should be set up to send an email to a specified user, group of users, or other email address whenever "unlimited administration" mode is enabled or disabled.
- All actions that are normally audited, such as secret views, edits, or permissions changes, are still audited while "unlimited administration" mode is enabled.

## Encryption

### DPAPI Encryption

#### Overview

The Data Protection API (DPAPI) is an option that provides an additional layer of security for the SS encryption key. The SS encryption key is contained within a file that is decrypted and used by the application to encrypt or decrypt the sensitive data that is stored in the SS database. Using the DPAPI option in SS ensures that the encryption key file is also encrypted with a key that only Windows knows and is only be usable on same server it was encrypted on. Anybody trying to configure SS on another server using that DPAPI-encrypted key is blocked from doing so.

**Important:** The encryption key file, `encryption.config`, should be backed up and stored in a secure location before turning on DPAPI encryption. This allows you to restore a backup of the application on another server in a DR scenario. The file is in the SS application directory.

#### Enabling and Disabling DPAPI

To turn on DPAPI encryption of the file, select **Configuration** from the **Admin** menu. Select the **Security** tab, click **Encrypt Key Using DPAPI**, and then type your password and acknowledge the warning before clicking **Confirm**. To decrypt the key, navigate to the same tab and click **Decrypt Key to not Use DPAPI**.

## Using Clustering with DPAPI

You can use DPAPI while clustering is enabled for SS, however there are a few things to take into consideration:

- Backup the encryption key before using this option, otherwise disaster recovery could prove impossible, should the server fail.
- You must initially transfer the un-encrypted key that DPAPI will encrypt to each SS node.
- You must enable DPAPI for SS by accessing each server locally (browse to SS while on the server it is installed on, and then enable DPAPI encryption).
- During upgrades, to avoid turning off DPAPI, you can copy all files over to secondary nodes *except* for `database.config` and `encryption.config`.

For more information about clustering SS, see [Setting up Clustering](#) (KBA).

## Protecting Your Encryption Key Using EFS

Encrypting File System (EFS) is a Microsoft technology that allows a user to encrypt files with their password. This means that only the user who encrypted the file will be able to access it, even if it is assigned to other users. If an administrator resets the password on this account and the account does not change its own password, then the file is not recoverable.

You can use EFS to protect your SS encryption key. This allows only a single service account to access the file, and no other user can read the key unless they know the service account password. Below are the steps for encrypting your `encryption.config` and `database.config` files with EFS:

1. Backup your `encryption.config` and `database.config` files to a secure location. This is very important for DR recovery purposes.

**Important:** This step is critical—If you lose access to your service account or the server fails, you will be unable to recover your secrets without these backup files.

2. Create a new service account or select an existing one. The service account should initially have privileges to log on a computer.
3. If you have already installed SS and are using Windows authentication for database access, make sure the service account has access to the database.
4. Run the SS application pool as this service account. See [Running the IIS Application Pool As a Service Account](#).
5. Give the service account full access to your SS directory through Windows Explorer if it does not have it already.
6. Log on your server as the service account.
7. For both the `encryption.config` and `database.config` files (this instruction uses the former):
  1. Locate the `encryption.config` file in your SS directory (usually `C:\inetpub\wwwroot\SecretServer`).
  2. Right-click the file and select **Properties**.
  3. Click the **General** tab.
  4. Click the **Advanced** button.
  5. Click to select the **Encrypt contents to secure data** check box.
  6. Click the **OK** button.
  7. Click the **Apply** button.
  8. If prompted, select the **Encrypt the file only** option.
  9. Click the **OK** button.
8. Log out of Windows and log back in as an administrator.
9. Confirm that the application still works by performing an IIS Reset (`IISReset` command at the command prompt) or recycling the application pool.
10. Ensure you can still log in and view your secrets.

## SSL (TLS) and HSTS

We strongly recommend employing SSL (TLS) for SS. Taking SSL a step further, SS also supports HTTP Strict Transport Security (HSTS). HSTS is supported by modern browsers and tells the browser that a site is only accessible by SSL with a valid certificate, period. Even if there is a man-in-the-middle attack with a trusted, but different, SSL certificate, the browser will reject the SSL certificate. Consequently, this setting is very useful for protecting against forged SSL certificates or man-in-the-middle attacks.

For more information about configuring SSL certificates, see [Creating 2048-bit Domain SSL Certificate](#) (KB) and the [Installation Guide](#). You can view additional information about HSTS in [Securing with HTTP Strict Transport Security \(HSTS\)](#) (KBA).

## SSH Key Validation

Host SSH Key verification is supported for use with heartbeat, proxied launchers, password changers, and discovery. Host SSH key verification can help ensure that the machine you are connecting to is a trusted host. Host SSH key verification will not pass credentials to the target machine unless the public key digest matches the SHA1 digest that SS has on file. This helps prevent man-in-the-middle attacks.

## Mapping an SHA1 Digest to Secrets

To configure host SSH key verification:

1. Navigate to **Secret Templates** from the **Admin** menu.
2. And add a field for the host's SSH key digest.
3. Click **Configure Extended Mappings**.
4. Add a **Server SSH Key** mapping to your newly created SSH key digest field.
5. On your secrets, add the SSH key digest of the hosts to your digest field. Verification takes effect the next time you connect to the host.

## Validating SHA1 Digests for Unix Account Discovery

To validate SHA1 server digests for Unix account discovery, create a file named `KeyDigests.txt` in the root of the SS website. Each line should contain an IP address or other computer identifier, a comma, and the SHA1 digest, for example:

```
192.168.1.5,7E:24:0D:E7:4F:B1:ED:08:FA:08:D3:80:63:F6:A6:A9:14:62:A8:15  
apollo,7A:25:AB:38:3C:DD:32:D1:EA:86:6E:1C:A8:C8:37:8C:A6:48:F9:7B
```

When the file exists and has data, all scanned machines must match one of the SHA1 hashes in the file before scanning. Any computers that do not match will still show up on the "Discovery Network View" page, but authenticated scanning will not take place. That is, no credentials will be passed to the machine, and accounts will not be retrieved from the machine.

## Disabling IIS HTTP Headers

### Introduction

This section describes plugging some potential, minor but significant, information leaks by the Secret Server (SS) Web server. Web applications, such as SS, may unintentionally disclose information about their underlying technologies through headers, error messages, version numbers, or other identifying information. An attacker can use that information to research vulnerabilities in those technologies to attack the application to breach the system.

### Procedure

First, **hide the IIS version**. The HTTP header "X-Powered-By" reveals the version of IIS used on the server. To stop this, remove the header:

1. Open the IIS Manager.
2. In the **Connections** tree, select the website that SS is running under.
3. Click the **HTTP Response Headers** button on the right. The HTTP Response Headers panel appears.
4. Click to select the **X-Powered-By** HTTP header.

5. Click the **Remove** button in the **Actions** panel. The header disappears.

Second, **hide the ASP.NET version**. The HTTP header "X-ASPNET-VERSION" reveals the version of ASP.NET being used by the SS application pool. To stop this, remove the header:

1. Open the `web.config` file for SS, which is located in the root directory for the website.
2. Inside the `<system.web>` tag, add the tag `<httpRuntime enableVersionHeader="false"/>`.
3. Save the file.

Third, **hide the server type**. The header line `Server: Microsoft-HTTPAPI/2.0` is added to the header by the .NET framework. To remove that information, you must update the Windows Registry:

**Important:** Do not simply remove the Server header variable—it will cause parts of SS to malfunction.

1. Open the Windows Registry Editor.
2. Navigate to `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters`.
3. Change the `DisableServerHeader` (REG\_DWORD type) registry key from 0 to 1.

**Note:** There are other ways to hide the server type. We strongly recommend this one.

## Additional Resources

- [Secret Server – Security Hardening webinar](#)
- [Thycotic Knowledge Base](#)
- [Secret Server Best Practices Guide](#)
- [Thycotic.com](#)

## Session Recording

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

**Note:** macOS Catalina requires additional configuration to use basic session recording. See [macOS Catalina Security](#).

Basic session recording is a licensed feature in SS. It relies on the protocol handler configured on client machines through SS's launcher. Using the launcher, SS captures second-by-second screenshots on the client machine during a user's recorded session. These images of the user's screen are compiled into a video that can be downloaded and played back for auditing and security purposes. Activity recorded in the session is based on screen changes only.

Session monitoring allows administrators with the Session Monitoring permission to view all active launched sessions within SS. If session recording is enabled on the secret, an administrator can watch the user's session in real time.

Admins can search through active and ended sessions. To review and search through sessions go to **Admin > Session Monitoring**.

Searching across sessions can search the following data. To select what data is searched across check the options on the search filters on the left-hand side.

## Session Playback Search

### Search Filters

Search Across

Secret Name

Secret Items

Username

Proxy Session Client Data

RDP Keystroke Data

Date

Last 30 Days

Status

All

Launcher Type

All

Users

Groups

Secrets

Folder

< All Folders >

Back

Search for Sessions

Search

10.0.0.243\winuser2 - Accessed By ssadmin Remote Desktop 4/11/2017 05:46 PM · 0:10:03 win-h0ko2iq58no · ssadmin <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop 4/11/2017 05:41 PM · 0:00:59 win-h0ko2iq58no · user282 <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop 4/11/2017 05:35 PM · 0:01:44 win-h0ko2iq58no · user282 <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop 4/11/2017 05:35 PM · 0:00:11 win-h0ko2iq58no <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop 4/11/2017 05:33 PM · 0:00:00 win-h0ko2iq58no <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop 4/11/2017 05:19 PM · 0:00:32 win-h0ko2iq58no · user282	

Some search filters require additional components to be installed or configured:

- **Proxy Session Client Data:** Search within keystroke data of proxied SSH sessions. Requires that the SSH proxy is enabled and SSH sessions are using it.
- **RDP Keystroke Data:** Requires the RDP Session Monitoring Agent be installed on the target.
- **RDP Application Name:** Requires the additional RDP Session Monitoring Agent be installed on the target.

To view a recording, click the camera icon on the session. The Watch Session Recording page appears:

## Watch Session Recording

### Session Summary

**Session Secret:** [10.0.0.243\winuser2](#)  
**Machine:** win-h0ko2iq58no

**Session User:** Andrew Smithson  
**Launcher Used:** Remote Desktop

**Session Start:** 3/30/2017 11:10 PM  
**Session End:** 3/30/2017 11:10 PM

### Search Session Activity

Activity Type: All    Keyword:

Elapsed	Type	Activity	Jump To
00:00:00	explorer		
00:00:00	rdpinput		
00:00:00	TSTheme		
00:00:00	rdpclip		
00:00:00	Thycotic.SessionRecorder		
00:00:00	taskhostx		
00:00:00	explorer		
00:00:04	TSTheme		
00:00:04	powershell		
00:00:04	conhost		
00:00:04	powershell		
00:00:06	hello		
00:00:08	echo		

If there is logged session activity, such as keystroke or application data from the RDP agent or SSH proxy then you can search through session activity and jump to points within the video playback. The playback also displays an activity map to show points of high activity, such as screen changes, keystrokes, and processes started and stopped.

Selecting an activity in the grid also shows additional details below such as the full folder path where the application started and the user that performed the operation.

**Note:** SSH Keystroke data is shown in one-minute segments. In a short session of less than minute, the "jump to" only goes to the beginning of the video.

For active sessions, there are two actions that can be taken:

- **Watch Live:** When session recording is turned on for the secret and admin can view and replay the user's activity.
- **Terminate:** Sends a message to the end user or terminates their session. The end user sees an alert dialog pop up on their machine with the message. Session recording does not need to be enabled for this to work. For ended sessions admins can watch the recorded video and view the SSH log if session recording was turned on for the secret.

Advanced Session Recording (ASR) is a licensed feature of SS that adds capabilities to those offered by basic session recording. You install the Advanced Session Recording Agent (ASRA), which uses the Remote Desktop Protocol, on any client machine where you want more information from the sessions recorded.

**Note:** ASR is not available to those using our Mac launcher.

**Note:** Older ASRAs (earlier than 7.7) only work if a distributed engine configuration is enabled with RabbitMQ or MemoryMQ installed.

ASR enhances the launcher sessions, which typically only include screenshots, keystrokes, and process activity. ASR features include:

- **Screen Capture:** The SS launcher records second-by-second screen images compiled into a playback video of the user's session. This is essentially the same as basic session recording.
- **Logged Processes:** The ASRA logs all processes started and stopped during a user's session.
- **Recorded Key Strokes:** The ASRA records all user keystrokes during the session, which can be disabled.

In addition to those, ASR includes these enhanced video playback features:

- **Searchable Video:** You can search video activity to find locations where specific activities, such as specific keystrokes or ran processes.
- **Enhanced Playback:** Sessions recorded using ASR display additional data on playback, such as the current active window, the used processes, and keystrokes in the session.
- On-demand video processing
- Recording all sessions
- Inactivity timeout
- Maximum session-length protection

**Note:** The Windows protocol handler encodes your session in WEBM format in real time and sends the recording to SS. There is now an "Enable On-Demand Video Processing" option in SS which leaves the recordings in WEBM format, which Chrome and Firefox can playback without any further processing, saving server processing time. If an on-demand recording is viewed with Internet Explorer or Edge (which do not support WEBM playback), you can click a "Request Video Processing" button and the video will be converted to H.264/MP4, which they can then play. If "Enable On-Demand Video Processing" is not checked, then all sessions recorded by the Windows protocol handler will be automatically converted to H.264/MP4.

**Note:** The Mac protocol handler does not yet support this feature, so any recordings created with it are converted to the chosen legacy video codec format. We recommend H.264/MP4. You can set the advanced session recording agent to "Record All Sessions." If someone logs into a server directly without launching from SS, or even logs in at the console, the full session is recorded, including metadata.

**Note:** See [Secret Server Advanced Session-Recording Agent Installation](#) (KBA) for details.

The Session Recording tab contains the following configuration options:

- **Enable Deleting:** After the "Days Until Deleting" value, SS deletes the videos from disk.
- **Enable Moving to Disk:** After the "Days Until Moved to Disk" value, SS can move videos from the database to an archive path on disk.
- **Enable Session Recording:** Enable session recording for launched sessions.
- **Save Videos To:** By default, videos are stored in the database, SS can also store them directly to a network share. This network share must be accessible from all Web servers that SS is installed on.
- **Video Code:** Specify the codec to use to create the videos from the launcher screenshots. This codec must be installed on the Web server (or servers if clustering is enabled) that SS is installed on.

**Note:** The Microsoft Video 1 codec is for testing only and does not support in browser playback. Sessions encoded with Microsoft Video 1 can still be downloaded for review.

For details on the settings in the Login and "Local User Passwords" tab, see [Configuring Users](#).

## General

System requirements apply to both physical and virtual machines.

- Thycotic does not support these Web servers:
- Any Client OS
- Domain Controllers
- SharePoint Servers
- Small Business Server (SBS)
- Windows Server Essentials
- For best performance, we recommend using dedicated (clean) servers for hosting Thycotic products.
- If .NET and IIS features are not already installed on the Web server, the Thycotic Installer adds and configure them automatically.

## Database

- Database disk storage depends directly on how many recorded videos are stored to disk. For active users, we recommend you **use a 1 TB shared or local drive for archival or storage space**. For light users, we recommend beginning with 300 GB. Monitor your disk space usage closely, and tailor it for best results.
- **Carefully consider how quickly your allotted storage might be exhausted.** Once again, it is highly variable, but you might expect around 15 hours of recording per GB of storage. Using the example of encoding capacity used in the Session Recording section, if you wanted to record one year of usage by your 60 8-hour users, you would need around 11 TBs of storage (given vacations and holidays). Our recommended 1 TB would last nearly a month in that scenario. A session retention policy using the automatic deletion feature is likely your best option.
- If MS SQL Server is not already installed on your database server, the Thycotic Installer can setup SQL Express on the Web server; however, **SQL Express is only for trials and sandbox environments**. Though Thycotic supports SQL Express, your users will likely experience performance issues due to memory and product limitations. If experiencing performance issues while using SQL Express, we highly recommended upgrading to MS SQL Server prior to contacting Thycotic Support.

**Note:** Please see Microsoft documentation on SQL Express at: <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017>

## Network Bandwidth and Video

- For SS 10.6 ASR requires around 300 Kbps. Older versions of Session Recording require 1-3 Mbps.

**Note:** Our Mac launcher uses the older bit rate.

- Session recording bandwidth requirements vary widely based on monitor resolution and image complexity--higher resolutions and more complex images (simpler screen images compress better) use more bandwidth. For example, with a 1024×768 screen resolution, the required network bandwidth is typically between 0.1 Mbps and 1 Mbps.
- If your connection cannot support the needed bandwidth, the session data is still transmitted, but it takes longer to process each session.
- If a user tries to cancel the transmission, this activity appears in the audit record for the Session Recording Secret.

- All sessions are recorded at 1080p.

**Note:** Before SS 10.6, session recordings 1080p or higher were not supported due to a limitation in Microsoft IIS. The session video would be recorded but may have been corrupted.

- Sessions are recorded using the H.264 MPEG-4 codec.

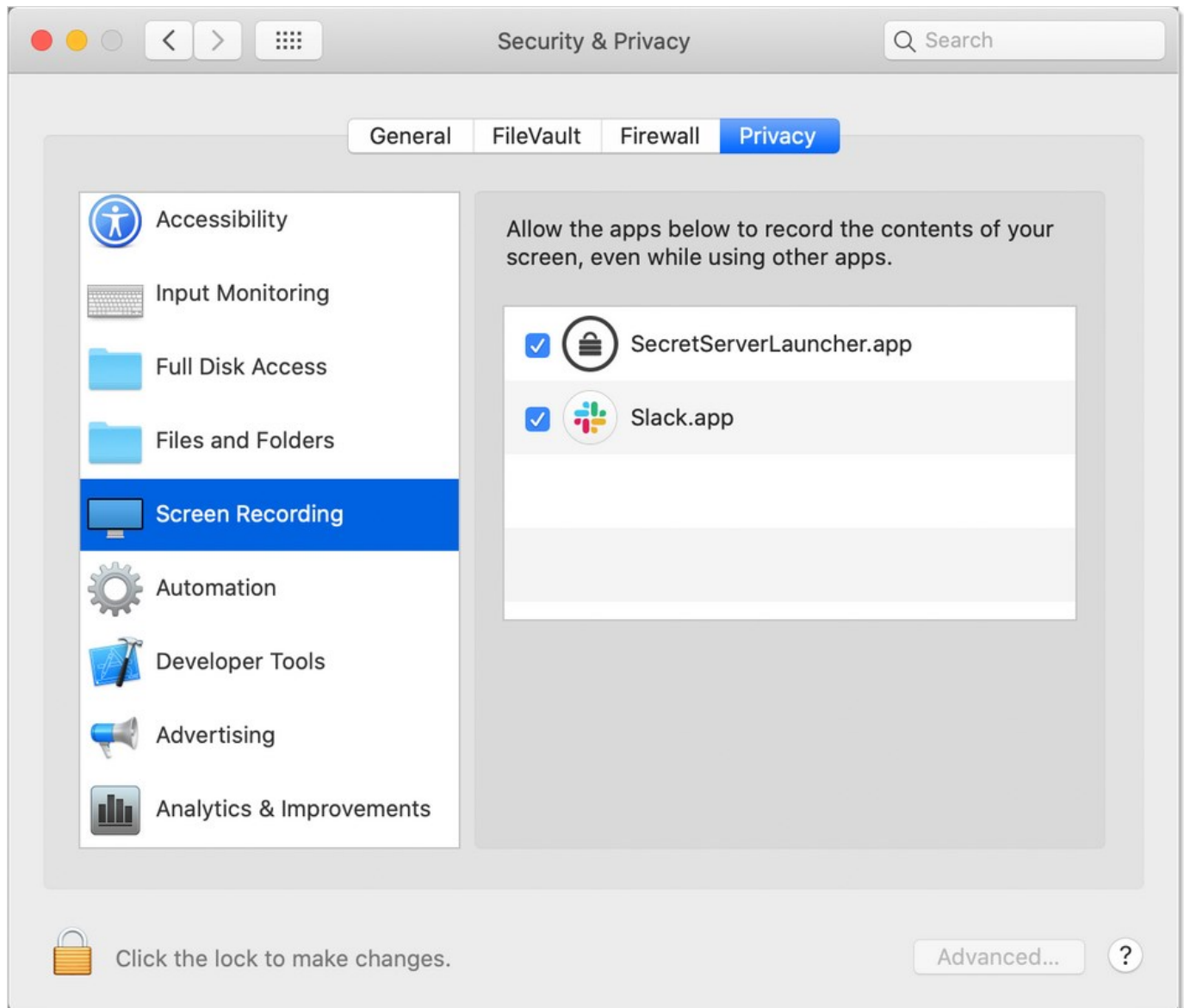
## Session Recording

- Server hosting session recording requires fixed RAM and disk space. We strongly recommend that you **do not apply dynamic settings**.
- **Do not record more sessions than you can encode.** If more concurrent sessions are recorded than the system can process, the sessions wait in a queue and are processed when enough server resources become available, which could be in a very long time or perhaps never if your storage is overwhelmed.
- The frame rate we can encode varies dramatically based on many factors, so **testing what encoding rate your session recording configuration can sustain is a must**. From there, you can get an idea of what is possible. For example, let us say you found that we can process 20 FPS on average on your Xeon processors. Given that rate, we could encode around 1 minute of a session recording in 3 seconds, or 1 hour in 3 minutes, or 1 day in 72 minutes--giving you perhaps 480 session hours per day. You could then parse that figure based on your typical usage to arrive at a maximum potential usage, for example, 60 people doing 8-hours of session recording.
- Typically, you can record **up to one hundred sessions at a time per web node**, load balanced, which should handle large use cases.
- CPU usage during video processing varies depending on concurrent users and recording length. We recommend that you **closely monitor CPU percentages on your web server** during video processing, as well on your client machines during recording, to increase CPU count for machines, if needed.
- We recommend that you **set up RabbitMQ as the backbone service bus** in session recording environments. To setup RabbitMQ. See: [Secret Server: How to install RabbitMQ](#) (KBA).

## macOS Catalina Security

macOS Catalina enforces security policy around screen recording. To use the session recording feature of the Thycotic launcher on MacOS Catalina, you must first:

1. Go to **System Preferences > Security & Privacy > Screen Recording** on your Mac.
2. Allow recording for the SecretServerLauncher.app:



## Overview

Session recording allows you to record an RDP or PuTTY session, with optional metadata, and play it back in Secret Server (SS).

The Windows protocol handler encodes your session in WebM format in real time and sends the recording to SS. There is an "Enable On-Demand Video Processing" option in SS which leaves the recordings in WebM format, which Chrome and Firefox can playback without any further processing, saving server processing time. If an on-demand recording is viewed with Internet Explorer or Edge (which do not support WebM playback), you can click the "Request Video Processing" button and the video is converted to H.264/MP4, which they can then play. If "Enable On-Demand Video Processing" is not checked, then all sessions recorded by the Windows protocol handler are automatically converted to H.264/MP4.

**Note:** The Mac protocol handler does not yet support this feature, so any recordings created with it are converted to the chosen legacy video codec format. We recommend H.264/MP4.

You can set the advanced session recording agent to "Record All Sessions." If someone logs into a server directly without launching from SS, or even logs in at the console, the full session is recorded, including metadata.

## Configuration

1. Go to **Admin > Configuration > Session Recording**.
2. On the **Session Recording** tab, click the **Edit** button.
3. Ensure the **Enable Session Recording** check box is selected.

**Note:** For testing and proof of concept deployments, SS's [Unexpected Link Text](#) is sufficient for session recording. For production deployments we strongly recommend [RabbitMQ](#) for a more-robust message queue.

## Using Legacy Video Codecs

You can select a legacy video, but it will only apply to sessions recorded by the Mac protocol handler. Thycotic recommends the H.264 codec, which was available starting in SS 10.5.000003 because it produces the highest quality videos and requires no additional installation. If you want a different legacy codec, ensure that the codec you select is correctly installed on the same machine as SS. It does not need installation on any client machines, where the session recording is occurring.

Available legacy codecs:

**Note:** On Windows Server 2008 and above, you can install Window Media Player by adding "Desktop Experience" from the features of Server Manager.

- Microsoft Video 1 (testing only): Microsoft Video 1 is deprecated in favor of Microsoft Video 9 and should not be used for production. Microsoft Video 1 does not support browser-based playback of sessions.
- Microsoft Video 9: High compression level and quality. Requires Windows Media Player. This option produces comparable video sizes to Xvid for moderate activity in an RDP session.
- VP8: High compression level and quality. VP8 is bundled with SS. This option produces comparable sized video to Xvid for moderate activity in an RDP session.
- Xvid: Provides similar quality and compression to DivX and is freely available. This option produces approximately 20 MBs of video for 1 hour of moderate activity in an RDP session. See <https://www.xvid.com/>

## Enabling Session Recording on Secrets

You must enable session recording on the Security tab for each secret. Once session recording is enabled, SS records that session when the launcher is used.

To view the recorded session after it is completed, click the **View Audit** button on the secret screen and then the **View Session Recording** link in the **Details** column.

You can also search recordings from the Session Monitoring page under **Admin > Session Monitoring**.

The Session Monitoring page lets users search and filter sessions based on session data, secrets, users, groups, launcher type, date, and folders. This page is also where any recordings appear when using the Record All Sessions option (see below), because such recordings are not tied to a specific secret.

**Note:** Browser playback is only supported in SS 10.2 and higher. Older versions of SS prompt the user to download the recording.

To view a session, click the camera icon to the right of it. This takes you to the Web playback interface. The video playback shows an activity map to quickly skip to sections of higher usage.

As noted above, if using the "On-Demand Video Processing" option, Chrome and Firefox can play the video. If you try to view an on-demand video using Internet Explorer or Edge, a warning message appears.

If you click the **Request Video Processing** button, the recording is converted from WebM to H.264 as soon as possible, allowing IE/Edge to play it back.

## Extending Session Recording with Custom Launchers

You can configure SS with custom launchers to run arbitrary programs, which can then be recorded by session recording. To do so:

1. Define a custom launcher:
  1. Go to **Admin > Secret Templates > Configure Launchers**. The Manage Launcher Types page appears.
  2. Click the **New** button.
  3. Leave the **Launcher Type** dropdown list set to **Process**.
  4. Type a name for the custom launcher in the **Launcher Name** text box.
  5. Type a process name in the Process Name text box.
  6. (optional) Type process arguments in the Process Arguments text box.
  7. Customize other Options as needed.
  8. Click the **Save** button.
2. Associate the launcher with a secret template:
  1. Go to **Admin > Secret Templates**. The Manage Secret Templates page appears.
  2. Click the template dropdown list and select the desired template.
  3. Click the **Edit** button.
  4. Click the **Configure Launcher** button. The Secret Template Edit Launcher Configuration page appears.
  5. Click the **Add New Launcher** button.
  6. In the **Launcher Type to use** dropdown list, select your custom launcher.
  7. Customize any other options as needed.

Secret Server 10.8 added two new options to custom launchers:

### Record Multiple Windows Option

If this option is not checked, only the main window of the main launcher process will be recorded (this was always the behavior prior to Secret Server 10.8). If it is checked, multiple windows as well as child processes are recorded.

Without this enabled, the main window of the main process sometimes does not show anything useful, depending on the application, resulting in a blank recording. With this enabled, recordings are generally more accurate. This also applies to applications that can open or undock separate windows or those that launch additional processes, such as an application launching PowerShell and then launching other applications from the command prompt.

#### **Record Additional Processes Option**

Here you can type an optional comma-separated list of processes to record if found, running under your same user account, that are not started or terminated by the custom launcher. "Record Multiple Windows" must be enabled for this option to be available.

In the example above of launching PowerShell and then opening Notepad, if "Record Multiple Windows" is enabled, both PowerShell and Notepad would be recorded automatically, because the OS can tell that Notepad is a child process of PowerShell. This even works multiple levels deep—for example, launching PowerShell, then the command prompt, and then launching in PowerShell again, finally followed by Notepad.

In some cases, though, you may wish to record an additional process that was already running before the custom launcher was launched or may want to start running one later. To this end, any process names specified in this option are checked for periodically, and recording is attempted on them as well.

#### **Example**

If you wanted to run an X11 server such as Xming and then PuTTY with X11 forwarding, you could configure a custom launcher with these values:

Process Name: C:\Program Files\PuTTY\putty.exe Process Arguments: -X -ssh \$MACHINE -l \$USERNAME -pw \$PASSWORD Record Additional Processes: Xming.exe

In this case, Xming should already be running before the launcher was used and would remain running after the session has ended. It would have no parent/child relationship with PuTTY at all. However, while the launcher session was active, any windows it spawns would still be recorded, allowing the X11-forwarded applications to be recorded, not only the PuTTY window.

#### **Advanced Session Recording**

##### **Metadata Recording**

By default, session recording creates videos of the launched session. SS supports logging additional metadata, such as keystrokes for RDP and SSH sessions. When these options are enabled, users can search for keystrokes or applications across sessions, and the session playback interface shows additional activity information.

Remote Desktop session metadata requires SS 10.6 and the advanced session recording feature, which in turn requires an installation of an advanced session recording agent (ASRA) on the target servers. See [Advanced Session Recording Agent](#).

SSH keystroke data relies on the Secret Server SSH Proxy. This can be enabled under **Admin > SSH Proxy**. See [SSH Proxy Configuration](#) (KBA) for more information. Once proxying is enabled recorded SSH sessions will log SSH traffic which can be searched and is displayed in the session playback interface.

##### **Record All Sessions**

As of SS 10.6.26, you can configure the ASRA to record all sessions. This causes it to record video and metadata for anyone logging into the server, even when not using SS, including logging into the console. Since these recordings are not tied to any specific secret, you must go to the **Admin > Session Monitoring** page to view them.

## Session Recording Settings

Under **Admin > Configuration > Session Recording** there are several settings for configuring how SS handles session recordings:

### Hide Recording Indicator

When viewing a secret, the launcher icon normally indicates if the session will be recorded or not via the recording icon. When launched into, a notification window also informs the user that their session is being recorded. If "Hide Recording Indicator" is checked, users cannot tell which secrets have recording enabled based on the icons, and if they launch a recorded session, they will not be warned that their session is being recorded.

### Enable On-Demand Video Processing

The Windows protocol handler encodes the recording on the fly in WebM format and streams the video to SS. Once the session has ended, SS reconstructs the video and leaves it in WebM format, which Chrome and Firefox can natively play back.

**Note:** WebM is an audiovisual media file format that is a royalty-free alternative to HTML5 audio and video.

Internet Explorer and Edge currently have issues playing back WebM videos, so if you are using those browsers and try to view an on-demand recording, you are presented with a "Request Video Processing" button, which converts the video to H.264/MP4, as soon as possible, which IE or Edge can then play back.

If this option is not checked, all sessions recorded by the Windows protocol handler are converted to H.264/MP4 automatically. If you have many IE or Edge users, Thycotic recommends leaving this option unchecked, but this will increase the processing time of videos and increase the load on your SS servers that have the Session Recording role enabled.

This setting has no effect on sessions recorded with the Mac protocol handler, which is always encoded using your legacy video codec choice.

### Enable Inactivity Timeout (Minutes)

If enabled, if a session appears idle, users are given a five-minute warning that they will be disconnected. A prompt appears that lets them choose to disconnect immediately or to continue the session. If no response is received, the session is disconnected five minutes later.

**Note:** This feature was added in SS 10.6.26 and is currently only supported in the Windows protocol handler (not Mac).

### Max Session Length (Hours)

This sets a hard limit to how long a recorded session may last. This includes both launched from SS, as well as recorded sessions if using ASRA and the "Record All Sessions" option. This option helps prevent accidental recordings over the weekend, or even longer, if someone forgets to disconnect their session.

**Note:** This feature was added in SS 10.6.26 and is supported by both the Windows and Mac protocol handlers.

### Use Hardware Acceleration

If enabled, when processing H.264/MP4 files, this setting makes SS attempt to use hardware acceleration for video processing if possible (GPU or CPU). Thycotic recommends this setting is always enabled because SS will fall back to not using hardware acceleration if necessary.

**Note:** This feature was added in SS 10.6.0.

### Save Videos to

This configuration includes:

- **Database:** Stores the information from a recorded session as encrypted data to your database.
- **Disk:** Stores the recorded session as a video file directly to the specified folder path.

#### Archive Location Dependent on Site

If you save recordings to disk, enabling this option lets you pick a separate path for each of your sites. This is useful in large environments that need many recordings spread out across multiple devices and locations.

**Note:** See below for a note about using network shares for storage.

#### Folder Path

If you save recordings to disk, this is where they are saved. If you use the "Archive Location Dependent on Site" option, this is the default storage location for newly added sites, until you customize their folder path to something else.

**Note:** See below for a note about using network shares for storage.

#### Encrypt Archive on Disk

This setting encrypts the session videos when stored on disk. Videos stored on disk are played back through the SS UI but cannot be viewed directly from the file system.

#### Enable Archiving to Disk

After the specified number of days have passed, all recorded session information in your database is transferred to the specified folder path as video files and cleared from the database.

#### Enable Deleting

After the specified number of days have passed, all recorded videos in your database will be cleared and video files in your archive path will be deleted.

#### Setting Notes

- To use "Save Videos to Disk" or "Archive to Disk," the Application Pool service account must have write permission to the specified file path.
- To delete videos from the archive path, the Application Pool service account must have "modify" permissions.
- After saving a change to **Configuration > Session Recording**, the configurations for "Save Videos To Disk" and "Enable Deleting" will immediately be applied to all existing session recordings.

#### Using Network Share Path

In a clustered environment SS needs to use a network path when saving the files to disk. All nodes need access to the path to read the videos back to the user.

To archive or save to a file path that is a network share, instead of a local folder:

- The SServer IIS application pool must be running as a service account. See [Running Secret Server IIS Application Pool with a Service Account](#).

- You must grant access to the network share (using Windows ACLs) to the account running the SS IIS application pool.

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

## Advanced Session Recording

**Note:** This applies to ASRA and SS. See below for additional details.

**Table: Advanced Session Recording Requirements**

8 CPU Cores	8 CPU Cores	2 CPU Cores
32 GB RAM	32 GB RAM	16 GB RAM
50 GB Disk Space	100+ GB Disk Space	25 GB Disk Space
Windows Server 2012 or newer	Windows Server 2012 or newer	Windows XP (>5.1) or newer MacOS 10.11 (El Capitan) or newer
IIS 7 or newer	SQL Server 2012 or newer	
.NET 4.6.1 or newer		

Basic Session Recording

**Note:** See below for additional details.

**Table:** Basic Session Recording Requirements

8 CPU Cores	8 CPU Cores
16 GB RAM	16 GB RAM
25 GB Disk Space	100+ GB Disk Space
Windows Server 2012 or newer	Windows Server 2012 or newer
IIS 7 or newer	SQL Server 2012 or newer
	.NET 4.6.1 or newer

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

The latest ASRAs use more-reliable durable message exchanges, which are not compatible with earlier (already deployed) ASRAs. Version 7.7+ of the ASRA only requires HTTP connectivity to SS—the distributed engine response-bus site connector is no longer required.

To prevent this from breaking older ASRS, exchanges remain permanently transient. Newer ASRAs use HTTP uploads, which do not use the message queue. Thus, older versions of ASRAs continue to function as they have, and newer ASRA versions do not use the message queue and will have "durable" behavior over HTTP. We recommend updating your ASRA to version 7.7 or later as soon as feasible.

## Enabling Inactivity Timeout

If enabled, if a session appears idle, users are given a five-minute warning that they will be disconnected. A prompt appears that lets them choose to disconnect immediately or to continue the session. If no response is received, the session is disconnected five minutes later.

**Note:** This feature was added in SS SP2 and is currently only supported in the Windows protocol handler (not Mac).

## Enabling On-Demand Video Processing

As described above, this feature was added in SS 10.6.24 to greatly improve session recording performance.

The Windows protocol handler now encodes the recording on the fly in WEBM format and streams the video to SS. Once the session has ended, SS reconstructs the video and leaves it in WEBM format, which Chrome and Firefox can natively play back.

Internet Explorer and Edge currently have issues playing back WEBM videos, so if you are using those browsers and try to view an on-demand recording, you are presented with a "Request Video Processing" button, which converts the video to H.264/MP4, as soon as possible, which IE or Edge can then play back.

If this option is not checked, all sessions recorded by the Windows protocol handler are converted to H.264/MP4 automatically. If you have many IE or Edge users, Thycotic recommends leaving this option unchecked, but this will increase the processing time of videos and increase the load on your SS servers that have the Session Recording role enabled.

This setting has no effect on sessions recorded with the Mac protocol handler, which is always encoded using your legacy video codec choice.

## Record All Sessions

As of SS SP2, you can configure the ASRA to record all sessions. This causes it to record video and metadata for anyone logging into the server, even when not using SS, including logging into the console. Since these recordings are not tied to any specific secret, you must go to the **Admin > Session Monitoring** page to view them.

## Recording Metadata

By default, session recording creates videos of the launched session. SS supports logging additional metadata, such as keystrokes for RDP and SSH sessions. When these options are enabled, users can search for keystrokes or applications across sessions, and the session playback interface shows additional activity information. Remote Desktop session metadata requires SS 10.6 and the advanced session recording feature, which in turn requires an installation of an advanced session recording agent (ASRA) on the target servers. See [Secret Server Advanced Session-Recording Agent Installation](#) (KBA). SSH keystroke data relies on the Secret Server SSH Proxy. This can be enabled under Admin > SSH Proxy. See the SSH Proxy configuration KB article for more information. Once proxying is enabled recorded SSH sessions will log SSH traffic which can be searched and is displayed in the session playback interface.

**Note:** This applies to both ASR and basic session recording. See below for details.

**Table: Session Recording Capacities**

Dedicated for session recording	4	2 hours	10 minutes
Shared for front-end processing and session recording	2	2 hours	20 minutes

**Note:** The "Maximum Concurrent Session Conversions per Node" setting can be increased. See <https://thycotic.force.com/support/s/article/Configuring-Number-of-Max-Concurrent-Sessions-Per-Web-Node-Session-Recording>.

## Thycotic Support

**Important:** Please see our [Support Services Guide](#) for details about our support policy. This page is a high-level summary of portions of that guide.

Before you contact Support, gather the following information:

- Your Thycotic Support username and password
- The email account already associated with your account (if using email)
- Your company name
- The technical contact name
- The technical contact phone number
- The product name
- Issue symptoms and details
- Any other relevant details, such as hours the technical contact is present

The support PIN validates that your license includes support, and you must provide the PIN in your email or when you call. The PIN also makes it easier for Thycotic Support to locate your customer records and give you better support.

To get your PIN:

1. Get the log on credentials you received when you became a Thycotic customer.
2. Log on the [Support Portal](#) using your credentials.
3. On the main page, click the large blue **PIN** bar to get your PIN.
4. Record your PIN.
5. If you want to use our ticketing system for support, leave the browser tab open, and return for step four.

Thycotic customers have access to support by phone, email, and our support ticketing system (best for issue tracking). In all cases, **you must first obtain a support PIN**.

**Important:** For Severity 1 issues you **must** use phone support. Otherwise, use the method you prefer. Severity 1 means a critical problem that has caused *complete loss of service* and work cannot reasonably continue at your worksite.

Using one of the below methods, contact Thycotic Support.

### Phone Support

Thycotic delivers support by phone worldwide. Select the applicable number from this list:

AMERICAS	all	+1 202 991 0540
EMEA	UK	+44 20 3880 0017

	Germany	+49 69 6677 37597
APAC	Australia	+61 3 8595 5827
	Philippines	+63 2 231 3885
	New Zealand	+64 9-887 4015
	Singapore	+65 3157 0602

## Email Support

Send your email to [support@thycotic.com](mailto:support@thycotic.com) **with the PIN number as part of the subject line** of your email. For example: PIN 345 Workflow Stopped Unexpectedly. Include all the information listed in step one.

**Important:** You must send your email using an email address already noted in your account with Thycotic. Otherwise, it might delay our response.

## Ticketing System Support

Open a support ticket and track your issue to resolution.

- Visit the [Support Portal Login Page](#) using the credentials you received when you became a customer.
- After logging on, click the **Cases** tab, and then click **Create a Case**.
- Follow the instructions to complete your case.

## Ticketing System Integration

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS can allow users to enter a ticket number when viewing a secret. This number can be validated through a regular expression, and can also be marked as required, if needed. SS can integrate with third party ticket systems. For more information on the ticket system integration, see [Ticket System Integration with SS](#) (KBA).

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS can integrate with BMC Remedy's Incident and Change Management. This integration includes validating ticket numbers, their status, and adding work detail items to the request.

The integration with BMC Remedy leverages the out-of-the-box, SOAP-based Web services that are installed with the ITSM product installation. These services must be installed on your mid-tier BMC Remedy server to allow for this integration if they are not already installed and configured.

## Configurable Settings

### Validating Ticket Status

When a BMC Remedy request number is entered into SS, the status of that request is retrieved to ensure that it is an open state. For example, if an incident number is entered that is in the "Closed" state, the user is informed that the ticket is closed.

Incident Management: Service Incident request cannot be closed or canceled. Change Management: Change management requests cannot be complete, closed, or canceled.

### View Ticket URL Template

The format of the URL to be used for viewing the ticket. This is placed in the audit log so you can easily view the corresponding ticket from SS. For details on this format, see [View Ticket URL Template Format](#) (KBA). Depending on your version of BMC Remedy, the URL to link directly to a request may be slightly different.

Incident management:

```
https://<midtier_server>/arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Incident Number'%3D%22$TICKETID%22
```

Change management:

```
https://<midtier_server>/arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Change Number'%3D%22$TICKETID%22
```

### Ticket Number Format Pattern (Regex)

Before even making a call to the BMC Remedy Web service, you can have SS validate that the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure users enter the prefix. Some sample expressions to validate the ticket number are listed below:

Incident management: ^INC\_CAL\_[d]{7}\$

Change management: ^CRQ\_CAL\_[d]{7}\$

### Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

### Service Endpoint URL

This is the URL for the SOAP-based Web services. Below are some samples for what is expected. You can find the actual endpoint using BMC Remedy Developer Studio and accessing the correct application from the AR System Navigator and viewing the Web services section of the application.

Incident management: HPD\_IncidentInterface\_WS

Change management: CHG\_ChangeInterface\_WS

### System Credentials

Select or create a secret that contains the username and password for a user that has access to execute the SOAP Web services. The username and password are added to the authentication header for the SOAP request.

### Authentication

If your installation of BMC Remedy uses an authentication server, enter it in this text-entry field. Most installations allow this text-entry field

to be blank.

## **Add Comments to Ticket**

Check this box if you want the comment that a user enters to be added to the request in BMC Remedy. This adds information such as the secret for which access is requested, who requested access, and the requester's comments.

## **Comment Work Type**

When a comment is added to a request as a work item, the Work Item type is required. "General Information" is selected by default, but all default Work Type options are supported.

## Requirements

- BMC Remedy SOAP Web Services enabled
- A username and password that has access to execute the Web services. This can be set up in the developer studio by accessing the application in the navigator and viewing Permissions for the CHG\_ChangeInterface\_WS or HPD\_IncidentInterface\_WS. This user should also have access to query requests and add work items to requests for the appropriate module.
- SS environment needs to be able to connect to the BMC Remedy Web services via port 80 or 443. SSL is highly recommended because the SOAP messages contain a username and password.

## Testing Your Integration Setup

After configuring the ticket system (see configurable settings below), use the **Test Validation** button to verify that SS can successfully access BMC Remedy. This button opens a dialog in which you can enter a ticket number from BMC Remedy. This validation process returns success or an error code. BMC Remedy may not return much detail in the error message so you need to look at the BMC Remedy API log to see a detailed error message, see [BMC Remedy Error Messages](#) (KBA).

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS can integrate with your ticketing system via PowerShell. This integration includes validating ticket numbers, their status, and adding comments. In our example we are connecting to a ServiceNow instance.

**Note:** See [Creating and Using PowerShell Scripts](#) (KBA).

## Configurable Settings

### View Ticket URL Template

You can configure the view ticket URL if you have a web based ticketing system to allow easy access to link to your ticketing system from Secret Server.

### Ticket Number Validation Pattern (Regex)

Before making a call to the PowerShell script you can have Secret Server validate the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure they enter this prefix. See [Regex KB](#).

### Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern Regex.

### The PowerShell RunAs Credentials

In Secret Sever a domain credential is required to execute the PowerShell script. This is a required field.

### System Credentials

The system credentials are specific to your ticketing system. Any secret using the Username and Password extending mapping can be used as your system credential. Additional arguments can be populated from field on this secret and reference in your script.

## Validating Ticket Status

### Overview

To validate tickets you will need to create a PowerShell script to retrieve and validate the ticket. The integration will use arguments to pass custom values to your script. By default we will map certain fields to the first set of arguments. The ticket number will be collected by user input and assigned to the first parameter. When you have your ticketing system credentials mapped to a secret and assigned to the "System Credentials" field in the ticketing system setup, SS inserts UserName and Password as the second and third parameters.

Therefore, for the sample script below, the Ticket Status Script Arguments text box should be only contain \$url (which is also retrieved from the System Credentials secret), as \$ticket, \$user and \$password are supplied automatically by the system.

### Sample Script

```
$ticket = $args[0]
$user = $args[1]
$password = $args[2]
$url = $args[3]
$validStatus = "2"
$fields = "state"
$P = $password | ConvertTo-SecureString -AsPlainText -Force
```

```
$credentials = New-Object System.Management.Automation.PsCredential($user,$p)
$getStatusMethod = "$url/api/now/table/incident?sysparm_limit=10&sysparm_query=number=$ticket&sysparm_display_value=&sysparm_fields=$fields"
$response = Invoke-RestMethod $getStatusMethod -Method Get -ContentType 'application/json' -Credential $credentials
if($response.result.state -ne $validStatus)
{
    throw "Invalid State"
}
```

## Adding Comments to Tickets

To add a comment to tickets, create another script to do so. Example:

```
$ticket = $args[0]
$comment = $args[1]
$user = $args[2]
$password = $args[3]
$url = $args[4]
$p = $password | ConvertTo-SecureString -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PsCredential($user,$p)
$restEndpoint = "$url/api/now/table/incident?sysparm_limit=10&sysparm_query=number=$ticket&sysparm_display_value=&sysparm_fields=sys_id"
$response = Invoke-RestMethod $restEndpoint -Method Get -ContentType 'application/json' -Credential $credentials
$id = $response.result.sys_id
$updateObject = @{'work_notes'=$comment}
$body = $updateObject | ConvertTo-Json
$addComment = "$url/api/now/table/incident/$id"
$response = Invoke-RestMethod $addComment -Method Put -ContentType 'application/json' -Credential $credentials -Body $body
```

## Adding Comments to a General Audit Log

In addition to adding comments to specific tickets, you may want general audit entries made in your ticket system. The arguments are passed in the following order.

```
$comment = $args[1]
$user = $args[2]
$password = $args[3]

## custom script here
```

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS can integrate with ServiceNow's Incident and Change Management service. This integration includes validating ticket numbers, their status, and adding Work Detail items to the request. The integration with ServiceNow leverages the out-of-the-box REST-based Web services.

## Configurable Settings

### View Ticket URL Template

The format of the URL to be used for viewing the ticket. This appears in the audit log so you can easily view the corresponding ticket from SS. For details on this format, see [View Ticket URL Template Format](#) (KBA).

Incident management: `https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sysparm_query=number=$TICKETID`

Change management: `https://<instance name>.service-now.com/nav_to.do?uri=change_request.do?sysparm_query=number=$TICKETID`

### Ticket Number Format Pattern (Regex)

Before even making a call to the ServiceNow Web service you can have SS validate the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure they enter this prefix. Some sample expressions to validate the ticket number are listed below:

Incident management: `^INC\d{7}$`

Change management: `^CHG\d{7}$`

### Ticket Number Validation Error Message

The error message to display to the user when their entered ticket number fails the validation pattern regex.

### Instance Name

This is the name of your instance in the format `https://<instance name>.service-now.com`.

### System Credentials

Select or create a secret that contains the username and password for a user that has access to execute the REST Web services. SS uses these credentials to authenticate to ServiceNow.

### Add Comments to Ticket

Check this box if you want the comment that a user enters to be added to the request in ServiceNow. This adds information such as the Secret to which access is requested, who requested access, and their comments. The comment is added as a work note in the activity section of the request.

## Requirements

- ServiceNow instance running the Eureka version or later with REST services enabled.
- A username and password that has access to execute the REST services, specifically GET and MODIFY on the following tables: Change Request and Incident.
- The SS environment needs to be able to connect to the ServiceNow Web services via port 80 or 443. SSL is highly recommended because the REST messages authenticate with a username and password.

## Testing your Integration Setup

After configuring the ticket system (see configurable settings below), use the **Test Validation** button to verify SS can successfully access ServiceNow. This button opens a dialog in which you can enter a ticket number from ServiceNow. This validation process either succeeds or shows an error code.

SS can require users to enter a ticket number when viewing a secret. Admins can track access to secrets based on an external ticket system. On the **Ticket System** tab of the **Configuration** page, an administrator can enter the settings to match the ticket system.

After the ticket system is enabled in SS, a user can enter a ticket number on the Comment screen or the Request Access screen.

The secret needs to have Require Comment or Requires Approval for Access enabled to allow the user to enter a ticket number. When a ticket number is required, this secret setting is displayed as "Require Comment/Ticket Number" on the Security tab.

Configurable settings:

- **Auditing:** The ticket number appears in the audit log and can be queried in reports. If the **View Ticket URL** has been set, the log shows the ticket number as a hyperlink linking to the external ticket system. Information on setting the URL can be found in [View Ticket URL Template Format](#) (KB).
- **View Ticket URL Template:** The format of the URL to be used for viewing the ticket. This is placed in the audit log so you can easily view the corresponding ticket from SS. For details on this format, see [View Ticket URL Template Format](#) (KB).
- **Ticket Number and Reason Options:** This option allows fine-grained control of what the user must enter when Require Comment is enabled and ticket system integration is turned on.
  - **Reason Only Required:** Ticket number is optional, reason is required.
  - **Both Required:** Ticket number and reason are required.
  - **Ticket Number or Reason Required:** Either ticket number or reason must be entered.
  - **Ticket Number Only Required:** Ticket number is required, reason is optional.
- **Ticket Number Format Pattern (Regex):** A regular expression to use for validating the ticket number entered. This can help prevent typos in the number. For details on creating this expression, see the [Setting a Ticket Pattern Regex](#) (KB).
- **Ticket Number Label:** The text that displays next to the Ticket Number box on the Comment or Request Access page.
- **Ticket Number Validation Error Message:** The error message to display to the user when their entered ticket number fails the validation pattern regex.

You can add multiple ticket systems from the **Ticket System** tab. To add a new system, click **New Ticket System**.

You can make a select ticket system be SS's default ticketing system by clicking on the link of the desired system, then clicking **Set as Default**.

## Troubleshooting and Notices

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

This section contains common troubleshooting issues, workarounds, and technical notices.

**Note:** This section is a work in progress. It does **not** contain a complete set of SS troubleshooting and workaround articles.

## Overview

When using IIS version 7.0 and above, by default, the worker process terminates after a period of inactivity. If SS is in its own application pool, the application pool will stop after a period of no requests. To make sure that the application pool associated with SS does not stop when idle:

- Set the idle time-out to 0 minutes.
- Set the regular time interval to 0.
- Ensure there are no specific times scheduled for recycling.

Additionally, by default, IIS launches a worker process when the first request for the Web application is received. So if the SS application takes a long time to start, we recommend launching the worker process as soon as IIS is started by setting the start mode to AlwaysRunning to launch the worker process for the SS application pool as soon as IIS is started.

## Procedure

To change IIS advanced settings:

1. Open **Internet Information Server (IIS) Manager**: On the taskbar, click **Server Manager**, click **Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name.
3. Click **Application Pools**.
4. Locate the application pool SS is running as. To determine this:
  1. Expand **Sites** at the left, then find the website SS is running on.
  2. Click on the SS website or virtual directory (if it is running on one).
  3. Click **Basic Settings** on the right panel. This indicates Secret Server's application pool.
5. Right-click the application pool, and select **Advanced Settings**. The Advanced Settings panel appears.
6. Go to the **(General)** section.
7. Set **Start Mode** to **AlwaysRunning**.
8. Go to the **Process Model** section.
9. Set **Idle Time-out (minutes)** to **0**.
10. Go to the **Recycling** section.
11. Set the **Regular Time Interval (minutes)** to **0**.
12. Select **Specific Times**.
13. **Either** click the > expander arrow to see if there is time specified below. **Or** click the ... to see if there are any values in the **TimeSpan Collection Editor** dialog box. If so, clear it out.
14. Click the **OK** button. The dialog closes.
15. Click the **OK** button.

An HTTP 404.2 error code is received when ISAPI/CGI Restrictions are preventing the .NET Framework 4.5.1 from running.

## Resolution

1. Open Internet Information Services.
2. Select the Server in the left tree view.
3. In the **IIS** section, open ISAPI and CGI Restrictions.
4. For all items beginning with **ASP.NET v4.0**, right-click the item and select **Allow**.

## Error

After upgrading Secret Server (SS) and changing the CLR version, when attempting to load SS, you receive the following error in Internet Explorer:

HTTP Error 404.17 - Not Found The requested content appears to be script and will not be served by the static file handler

## Resolution

This error can be caused by ASP.NET 4.5 not being correctly registered on the server. To correct this:

### Windows Server 2012 or 2012 R2

Use the Server Manager to install ASP.NET 4.5.

1. Open the Server Manager.
2. Select **Manage > Add Roles and Features**. The Add Roles and Features wizard appears.
3. Click the **Next** button. The Select Installation Type page appears.
4. Click to select the **Role-based or feature-based installation for your server** selection button.
5. Click the **Next** button twice. The Select Server Roles page appears.
6. Click to select the **Web Server (IIS)** check box in the **Roles** list.
7. Click the **Next** button until you arrive at **Role Services** under **Web Server (IIS)**.
8. Drill down to **Web Server > Application Development** in the **Role Services** list.
9. Click to select the **ASP.NET 4.5** check box.
10. Click the Next button until you arrive at the final page.
11. Click the **Install** button.
12. Once installed, follow the resolution instructions in [HTTP Error 404.2 - ISAPI and CGI Restrictions](#) (KBA) to ensure ASP.NET 4.0 is allowed to execute in IIS.

Secret Server (SS) requires the application pool to have the "load user profile" setting enabled. Secret Server will report a critical alert to notify admins if this setting is not enabled.

**Note:** The site will load to give access to secrets but many internal operations will not function correctly so we recommend fixing the issue as soon as possible.

**Note:** This applies to version 10.2 and later.

Steps to enable the "load user profile" setting:

1. On each Web server that is running Secret Server, open IIS Manager.
2. Under the **Application Pool** node on the left, select **Secret Server**.
3. On the right-hand panel, select **Advanced Settings** to get to the full properties.
4. Scroll to the **Load User Profile** setting in the **Process Model** section.
5. Set **Load User Profile** to **True**.
6. Click the **OK** button.
7. Perform an iisreset on the server:
  1. Open a Windows command prompt as an administrator.
  2. Type iisreset.
  3. Press the **<Enter>** key.

## Relevance

This Thycotic **technical issue** knowledge base article is relevant to:

- Product(s): Secret Server using jQuery 3.2.1
- Version(s): 10.7
- Edition(s): All

## Technical Issue

Secret Server 10.7 uses jQuery 3.2.1, which is listed as vulnerable to the jQuery CVE-2019-11358 security issue on the [Common Vulnerabilities and Exposures \(CVE\) list](#).

## Resolution

Thycotic removed the jQuery vulnerability from Secret Server's copy of jQuery v3.2.1 by applying a patch (see [Related Articles and Resources](#)).

To verify the fix:

1. Navigate to `https://<your_secret_server_URL>/assets/libs/jquery-3.2.1.js`
2. Open the file in a text editor.
3. Search for the string `proto` in the code: ...

```
// Prevent Object.prototype pollution
// Prevent never-ending loop
if ( name === "__proto__" || target === copy ) {
  continue;
}
```

4. If the string appears, the patch has been applied.

## Related Articles and Resources

- [NIST website for CVE-2019-11358](#)
- [GitHub commits on the fix](#)

**Note:** The commit shows two files, the top file is the security fix, and the bottom file is a unit test for the fix. Secret Server does not ship with any jQuery unit tests as found in that second file.

- [Common Vulnerabilities and Exposures \(CVE\) list](#)

## Relevance

This Thycotic **technical issue** knowledge base article is relevant to:

- Product(s): Secret Server using jQuery 3.2.1
- Version(s): 10.8.000004
- Edition(s): All

## Technical Issue

Secret Server 10.8.000004 uses jQuery 3.2.1, which is listed as vulnerable to the jQuery CVE-2020-11022 security issue on the [Common Vulnerabilities and Exposures \(CVE\) list](#).

## Resolution

Thycotic removed the jQuery vulnerability from Secret Server's copy of jQuery v3.2.1 by applying a patch (see [Related Articles and Resources](#)).

To verify the fix:

1. Navigate to `https://<your_secret_server_URL>/assets/libs/jquery-3.2.1.js`
2. Open the file in a text editor.
3. Search for the string `htmlPrefilter` in the code (line 5919):

```
jQuery.extend( {  
  htmlPrefilter: function(html) {  
    return html;  
  }  
}
```

4. If the string appears, the patch has been applied.

## Related Articles and Resources

- [NIST website for CVE-2020-11022](#)
- [GitHub commits on the fix](#)

**Note:** The commit shows multiple files, the top file is the security fix, and the bottom files are unit tests for the fix. Secret Server does not ship with any jQuery unit tests.

- [Common Vulnerabilities and Exposures \(CVE\) list](#)

This topic discusses resolving the "The specified domain is not a valid domain" error.

## Troubleshooting Procedure

1. Verify that you are entering the fully qualified domain name in the domain field and that the domain username and password fields are correct.
2. Ensure that the ports used for LDAP (389) or LDAPS (636) are open. For more information about the ports used by Secret Server, see [Ports Used by Secret Server](#).
3. Ensure that your server is connecting to the correct DNS server:
  1. Open the command console as an administrator (**Start > Run > cmd**).
  2. Type `ipconfig /all`.
  3. Press **<Enter>**.
  4. Find your primary ethernet adapter and look in the **DNS Servers** section. Verify that the DNS server is correct.
4. If the DNS server is incorrect, then follow these steps to configure the DNS server:
  1. Open up your control panel (**Start > Control Panel**).
  2. Click on **Network and Sharing Center**.
  3. Click **Manage Network Connections** on the left.
  4. Right click on your primary network adapter and select **Properties**.
  5. Click **Internet Protocol Version 4 (TCP/IPv4)**.
  6. Click **Properties**.
  7. Click to select the **Use the following DNS server addresses selection** button.
  8. Type your primary DNS server in the first row.
  9. If you have a secondary DNS server, put it in the second row.

**Important:** Both DNS servers must contain the SRV record for your domain controller.
5. Check that your server is retrieving domain controller DC records correctly:
  1. Open up your control panel (**Start > Control Panel**).
  2. Type `nslookup`.
  3. Press **<Enter>**.
  4. Type `set q=srv`
  5. Press **<Enter>**.
  6. Type `_ldap._tcp.dc._msdcs.<Fully_Qualified_Active_Directory_Domain_Name>`.
  7. Press **<Enter>**.

8. If you get a result that looks like:

```
_ldap._tcp.dc._msdcs.<Fully_Qualified_Active_Directory_Domain_Name> SRV service location: priority = 0 weight = 100 port = 389 svr hostname =
*Domain_Controller_Host_Name*
```

Then you are retrieving the DNS record correctly. Otherwise, your DNS records are not correctly configured.

## Configuring the DNS Record on Your Server

1. If you are **not** using a Windows DNS server, contact your vendor to ask how to add SRV records. You will need to add a SRV record pointing `_ldap._tcp.dc._msdcs.<Fully_Qualified_Active_Directory_Domain_Name>` to your primary DNS server.
2. Connect to your Windows DNS server.
3. Open the DNS control panel (**Start > Administrative Tools > DNS**).
4. Expand the node corresponding to your server.
5. Expand the **Forward Lookup Zones** node.
6. Expand the node corresponding to your domain.
7. Delete the **\_msdcs** node if it exists.
8. Right click on the domain node and select **New Domain...**
9. Type `_msdcs` as the name.
10. Right click on the new **\_msdcs** node, and select **New Domain...**
11. Type `dc` as the name.
12. Right click on the new **dc** node and select **Other New Records...**
13. Select **Service Location (SRV)** as the record type.
14. Click the **Create Record** button.
15. Select **\_ldap** as the service.
16. Select **\_tcp** as the protocol.
17. Type 389 as the port.
18. Type the fully qualified host name of your DC or the IP address in the **Host offering this service:** text box.
19. Click the **OK** button.
20. Click the **Done** button.
21. Open up the services console (**Start > Run > services.msc**)
22. Right click on the **DNS Server** service and select **Restart**. Your domain DNS record should now be set up.

## Resolving Other DNS Issues

Secret Server requires that the DNS is correctly configured to add a domain. For additional tips on tracking down DNS Issues, see this [Troubleshooting Active Directory Installation Wizard Problems](#).

Also ensure the domain controller is using the appropriate DNS. The `ipconfig /registerdns` command (as per the link above) is frequently helpful for entering the correct DNS entries in for a given domain.

## Overview

Beginning with Windows 10 version 1607 (Creator's Update) and Windows Server 2016, the default GPO security descriptor denies users [remote access to Security Account Manager \(SAM\)](#) with non-domain credentials, and therefore prevents remote heartbeat and password changes made by otherwise-authenticated local user accounts. Affected Windows local account secrets return "Access Denied" on a heartbeat or remote password change.

This article provides a script and instructions to address these "access denied" errors. The script modifies the default local group policy remote SAM access security descriptor to allow all local users on a specified machine remote SAM access after authentication. This script requires elevated PowerShell permissions.

**Note:** Adding an account to the local computer's Administrators group does not solve the problem.

On most systems, the Administrators group on the local machine is part of the "Network Access: Restrict clients allowed to make remote calls to SAM" security policy setting. Through testing, we determined that Windows currently treats this group as only the built-in administrator account for this configuration. Therefore, if you add another user to the Administrators group on the machine, that user will be unable to heartbeat since it is not the built-in administrator account. In addition, the built-in object, "Local account and a member of Administrators" does not allow a local account that is a member of Administrators to heartbeat for any account other than the built-in administrator account.

## Additional Requirements

For heartbeat to work correctly, make sure that the local or authenticated users are:

- *Not* in the "Deny access to this computer from the network" security policy
- *In* the "Access this computer from the network" security policy

## Remediation Options

**Option 1:** Creating a custom group and adding users to it (this is what the script does for users on the endpoint) then adding that group to the security setting to allow the user to heartbeat successfully. New local users need to be added to the custom group if they are created in the future.

**Option 2:** Adding a user individually to the security setting to allow the user to heartbeat successfully.

**Option 3:** Modifying the Default GPO: Adding "allow authenticated or local users" to the security setting. This allows all local users or all users who are authenticated to the machine to bypass this setting. This does require the PowerShell Script below. The drawback is that this allows all users to remotely access SAM, so long as they are authenticated.

**Option 4:** Create a heartbeat workaround for GPO "Network Access: Restrict Clients Allowed to Make Remote Calls to SAM." This is addressed in the last section. This is for situations where the GPO needs to be completely bypassed.

## Option 3: Modifying the Default GPO

### PowerShell Script Description

This script adds a local non-privileged user group to the machine (a custom group name can be specified with the `-GroupName` parameter), adds all local users to the group, and then adds this group to the "Network Access: Restrict clients allowed to make remote calls to SAM" local group policy. This allows all local users within the group remote access to SAM after authentication, which is required for SS heartbeat and password changing.

## Download

Extract the .ps1 script found here: [https://updates.thycotic.net/secretserver/support/PowerShell\\_Win10-HB-RPC-Fix/Win10-HbFix.zip](https://updates.thycotic.net/secretserver/support/PowerShell_Win10-HB-RPC-Fix/Win10-HbFix.zip) Run in an elevated PowerShell ISE session.

## Script Argument Help

### Command Prompt Help

For full help text, run:

```
> Get-Help C:\Script\Win10-HbFix.ps1 -Examples
```

### Parameters

#### **-ComputerNames (string)**

Specifies the computers on which the script runs (comma separated). If unspecified, the default is the local computer.

#### **-Username (string)**

Specifies a username of an account that has administrative permissions on the computer to add a local user group and modify the local group policy. You will be prompted for a password. Examples: Administrator Or TestDomain\AdminUser.

#### **-GroupName (string)**

Specifies a name for the SAM access local user group. If unspecified, the default group name is "Secret Server Remote SAM Access"

#### **-ForceGPUUpdate**

Specifies whether a group policy update should be forced for immediate effect following the script. (Otherwise Group Policy changes may take up to 120 minutes to take effect by default).

### Examples

> C:\Script\Win10-HbFix.ps1 This example gives remote SAM access to all local users on the current machine. The current PowerShell credentials would be used for authentication.

> C:\Script\Win10-HbFix.ps1 -LogDir "D:\Win10-HbFix\log" This example changes the default output log path to D:\Win10-HbFix\log (default is [user temp directory]\log).

> C:\Script\Win10-HbFix.ps1 -ComputerNames "WINSERVER","TestDomain\SOMEMACHINE" -Username "TestDomain\Administrator" This example gives remote SAM access to all local users on the WINSERVER and TestDomain\SOMEMACHINE remote computers. The domain user "TestDomain\Administrator" credentials will be used. You would be prompted for a password.

> C:\Script\Win10-HbFix.ps1 -ComputerNames "D:\Win10MachineList.txt" -Username "TestDomain\Administrator"

This example gives remote SAM access to all local users on the remote computers listed in D:\Win10MachineList.txt (one machine per line). The domain user "TestDomain\Administrator" credentials will be used. You would be prompted for a password.

> C:\Script\Win10-HbFix.ps1 -ComputerNames "WINSERVER" -GroupName "Secret Server Group"

This example gives remote SAM access to all local users on the WINSERVER remote computer. The local group created will be named "Secret Server Group". Current PowerShell credentials would be used for authentication.

> C:\Script\Win10-HbFix.ps1 -ComputerNames "WINSERVER" -ForceGPUUpdate -Verbose This example gives remote SAM access to all local users on the WINSERVER remote computer, with verbose output. The current PowerShell credentials will be used for authentication. Group policy update

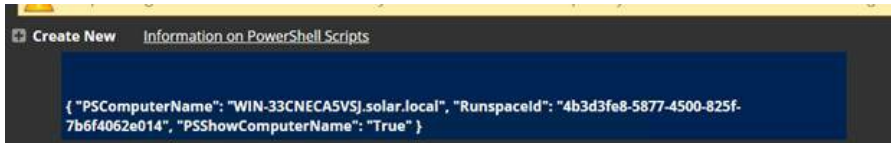
will be forced on WINSERVER for immediate effect.

## Related Articles and Resources

[Network access: Restrict clients allowed to make remote calls to SAM](#)

## Option 4: Creating a Heartbeat GPO Workaround

1. Make sure that **Admin > Scripts** is functional. Once you have it working, download, unzip, and run this script [HBWorkAroundScripts.zip](#).
2. Go to **Admin > Scripts**.
3. Add the HBWorkAroundScript and the HBWorkAroundPasswordChange scripts.
4. Test the first script. Add the appropriate `args[]` as needed. Add arguments 0-4 with no quotes or commas. Spaces are the argument separator and are required.
5. You should get a return of "True," such as this:



```
{ "PSComputerName": "WIN-33CNECA5VSJ.solar.local", "RunspaceId": "4b3d3fe8-5877-4500-825f-7b6f4062e014", "PSShowComputerName": "True" }
```

6. Navigate to **Admin > Remote Password Changing**.
7. Click the **Configure Password Changers** button. The Password Changers Configuration page appears.
8. Click the **New** button at the bottom.
9. Click the **Base Password Changer** dropdown list to select **PowerShell Script** as your password changer.
10. Type a name in the **Name** text box.
11. Click the **Save** button. The password change command page appears:

Test PC

Verify Password Changed Commands

Testing of PowerShell Scripts can be performed at Admin -> Scripts.

PowerShell Script

<select>

Script Args

Save

Hide Advanced Settings

SETTING	VALUE
Heartbeat Unknown Error to Unable to Connect Translation (regex)	
Attempt Password Change with new password when error contains (regex)	

Back

Configure Scan Template

View Audit

Password Change Commands

Testing of PowerShell Scripts can be performed at Admin -> Scripts.

PowerShell Script

<select>

Script Args

Save

12. Click the **PowerShell Script** dropdown list in the **Password Change Commands** section to select the script you ran earlier.

13. Add the appropriate tokens in the **Script Args** text box.

**Note:** See [Dependency Tokens](#) for a complete list.

12. Click the **Save** button. Your configuration should look like this:

HBWorkAroundChangerSAM

Verify Password Changed Commands

Testing of PowerShell Scripts can be performed at Admin -> Scripts.

PowerShell Script

HBWorkAroundScript

Script Args

`\${1}\$Username \${1}\$Password \$Machine \$Username \$Password

Password Change Commands

Testing of PowerShell Scripts can be performed at Admin -> Scripts.

PowerShell Script

HBWorkAroundPasswordChange

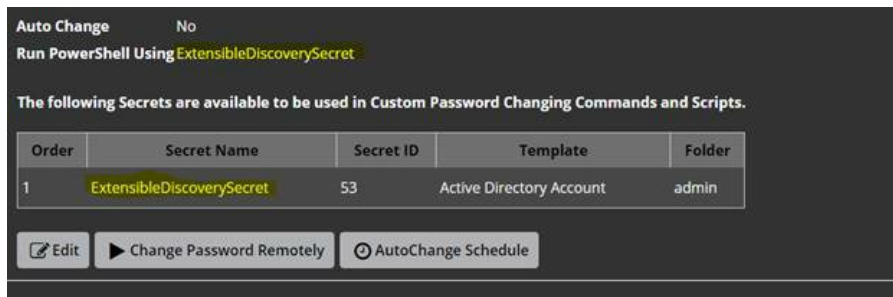
Script Args

`\${1}\$Username \${1}\$Password \$Machine \$Username \$NewPassword

13. Go to **Admin > Secret Templates**.

14. Select **Windows Account**.

15. Click the **Edit** button.
16. Click the **Copy Secret Template** button.
17. Click the **Configure Password Changing** button.
18. Click the **Edit** button.
19. Click the **Password Type to Use** dropdown list to select the password change you created earlier.
20. Create your windows secret using the custom template.
21. Once it is created, add your privileged and associated secret to the RPC tab as seen below. In that example we use the same one for the privileged and associated secret.



22. Run a heartbeat to confirm it works as desired.

## User Groups

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS allows administrators to manage users through *user groups*. Users can belong to different groups and receive the sharing permissions, as well as roles, attributed to those groups. This setup simplifies the management of the permissions and roles that can be assigned to a user. Additionally, groups can be synchronized with Active Directory to further simplify management.

Group Administrators can also set another group or user as the group owners for a SS local group. Group owners can manage membership just for that group. To assign the group owner:

1. Navigate to the **Groups** page:

Admin > Groups

Groups Audit

Manage Active Directory Groups View Group Assignment Create Group

Groups: 65 All Domains  Include Disabled

GROUP NAME	ENABLED	CREATED
Access Control Assistance Operat...	Yes	8/9/2019 02:08 pm
Account Operators	Yes	8/9/2019 02:08 pm
Administrators	Yes	8/9/2019 02:08 pm
Allowed RODC Password Replicati...	Yes	8/9/2019 02:08 pm
Backup Operators	Yes	8/9/2019 02:08 pm
Cert Publishers	Yes	8/9/2019 02:08 pm
Certificate Service DCOM Access	Yes	8/9/2019 02:08 pm
Cloneable Domain Controllers	Yes	8/9/2019 02:08 pm
Cryptographic Operators	Yes	8/9/2019 02:08 pm

2. Click the desired group in the list. The Group's page appears:

Group

Group Name

Test Group

Enabled

Yes

Created

8/12/2019

IP Address Restrictions

None

Group Owners

NAME

gamma.thycotic.com\Developers

admin

gamma.thycotic.com\Jonathan Thompson

gamma.thycotic.com\Roberto Hernandez

gamma.thycotic.com\Jonathan Lohoff

Jon Thompson

Mark

Christopher

Rob Hernandez

Jonathan Lohoff

Members

There are no members.

Back

Edit

Change IP Restrictions

Configure Secret Template Permissions

View Audit

View Group Assignment Audit

View IP Address Audit

3. Click the **Edit** button. The Group Edit page appears:

## Group Edit

Group Name

Enabled
☒

Managed By

### Members

### All Users

admin  
appaccount1  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con  
gamma.thycotic.con

<<

<

>

>>

Save

Cancel

4. Click the **Managed By** dropdown list to select the owner.

5. Click the **Save** button.

**Note:** Very commonly, the group owner is managed by Active Directory, not SS:

Q

Group

Group Name	gamma.thycotic.com\Administrators
Enabled	Yes
Created	8/9/2019
IP Address Restrictions	None
Group Owners	Managed by Active Directory

Members

| Show All < 1 to 15 of 17 >

NAME
gamma.thycotic.com\David Lindberg
gamma.thycotic.com\Thomas Thomsen
gamma.thycotic.com\Christopher Taylor
gamma.thycotic.com\Robert Nichols
gamma.thycotic.com\David Hoffmann

Back

Change IP Restrictions

Configure Secret Template Permissions

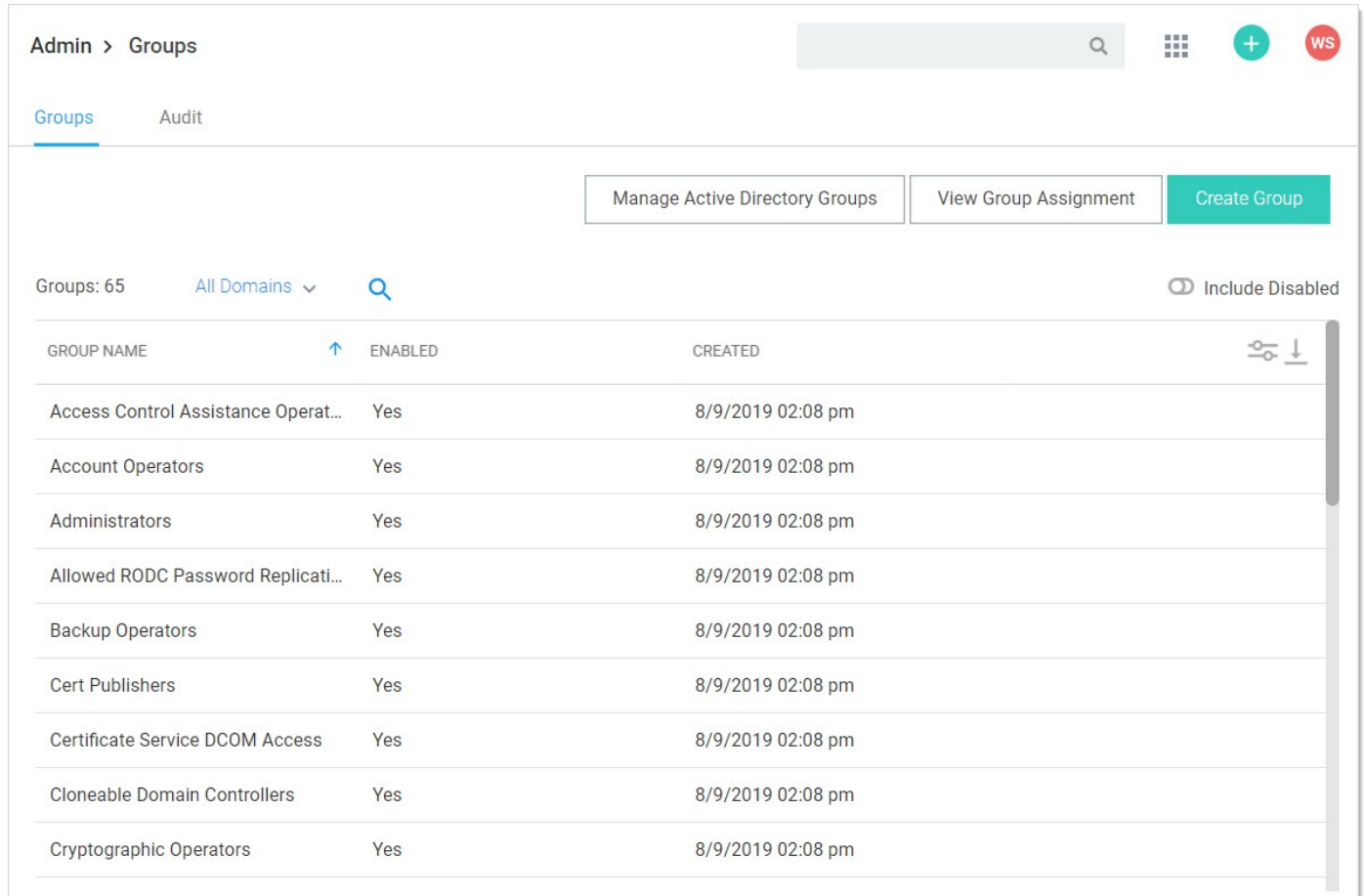
View Audit

View Group Assignment Audit

View IP Address Audit

On the Group Assignment page, users can be added and removed from the group.

1. Navigate to the **Groups** page:



Admin > Groups

Groups Audit

Manage Active Directory Groups View Group Assignment Create Group

Groups: 65 All Domains  Include Disabled

GROUP NAME	ENABLED	CREATED
Access Control Assistance Operat...	Yes	8/9/2019 02:08 pm
Account Operators	Yes	8/9/2019 02:08 pm
Administrators	Yes	8/9/2019 02:08 pm
Allowed RODC Password Replicati...	Yes	8/9/2019 02:08 pm
Backup Operators	Yes	8/9/2019 02:08 pm
Cert Publishers	Yes	8/9/2019 02:08 pm
Certificate Service DCOM Access	Yes	8/9/2019 02:08 pm
Cloneable Domain Controllers	Yes	8/9/2019 02:08 pm
Cryptographic Operators	Yes	8/9/2019 02:08 pm

2. Click the **View Group Assignment** button. The Group Assignment page appears:

## Group Assignment

[By Group](#)
[By User](#)

Group
Duo Approvers

Assigned

Unassigned

<<

<

>

>>

← Back

- Use the arrow buttons to move users into and out of the current group. When you have finished with your changes, click the **Save Changes** button and your new group members are added.

Alternatively, you can click the By User tab and manage the groups for a single user:

## Group Assignment

By Group By User

User

### Assigned

### Unassigned

Duo Approvers  
Test Group  
TJWForWorkflow



 Back

**Note:** If the group was created using Active Directory synchronization, this group is not be editable. See [Active Directory Synchronization](#).

You can create and edit groups from the Groups page. You can get to the Groups page by navigating to **Admin > Groups**

Admin > Groups

+

WS

Groups

Audit

Manage Active Directory Groups

View Group Assignment

Create Group

Groups: 65

All Domains

Q

☐ Include Disabled

GROUP NAME	↑	ENABLED	CREATED	
Access Control Assistance Operat...		Yes	8/9/2019 02:08 pm	
Account Operators		Yes	8/9/2019 02:08 pm	
Administrators		Yes	8/9/2019 02:08 pm	
Allowed RODC Password Replicati...		Yes	8/9/2019 02:08 pm	
Backup Operators		Yes	8/9/2019 02:08 pm	
Cert Publishers		Yes	8/9/2019 02:08 pm	
Certificate Service DCOM Access		Yes	8/9/2019 02:08 pm	
Cloneable Domain Controllers		Yes	8/9/2019 02:08 pm	
Cryptographic Operators		Yes	8/9/2019 02:08 pm	

By either selecting an already existing group from the list, or clicking **Create Group**, you can modify or add the group.

**Note:** To add groups and the users inside them from your Active Directory setup, you can use Active Directory synchronization (see [Active Directory Synchronization](#)).

## User Teams

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

With SS teams, administrators can create special groups called *teams* to restrict what users can see. A team bundles users and groups to assign them the same rules as to what other users and sites are visible to them. For example, a managed service provider could isolate their customers from seeing other customer's user accounts or a large company could "firewall" their users by department. Site visibility can also be restricted by teams.

**Note:** Teams are designed for shared secrets and do not apply to SS administration as a whole.

**Note:** Users *without* any team-related permissions are subject to team restrictions. The Unrestricted by Teams permission must be present to remove them. That is why the User role comes with that permission by default. See [Team-Related Permissions](#).

**Note:** Team restrictions are designed for regular users so granting additional administrative permissions can override the restriction. This applies to group owners, so if a user is assigned as a group owner, that user will be able to see all users when assigning members.

Team visibility and management are controlled by user roles. Those roles, and by extension users, are governed by the following team-related role permissions:

- **Administer Teams:** Users can create, edit, and view all teams.
- **No Teams-related Permissions:** Users can only view other users within their team.
- **Unrestricted by Teams:** Users can view all users, groups, and sites, regardless of Team affiliation. Essentially, teams do not exist for the users with this permission, and the Teams page is not available to them. The default user role has this permission.
- **View Teams:** Users can view all teams. This is essentially a read-only Administer Teams.

To set up SS to use the team management feature:

1. Create a new role called *Team Limited User*.
2. Assign all permissions of the standard user role except *Unrestricted by Teams*.
3. Assign users you want restricted by teams this role.
4. Remove the User role from their account.

**Note:** If you want all new users restricted by team, you can configure SS to assign the Team Limited User role as the default upon creation of a new user.

1. Navigate to **Admin** > **See All**. The Administration page appears:

What are you looking for?

Search for an admin option



[Simplified View](#) ▾



## Actions

Secret Server features that perform important jobs



## Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more



## Users, Roles, Access

These features help you organize users & permission settings within Secret Server



## Diagnostics, Logs, Security

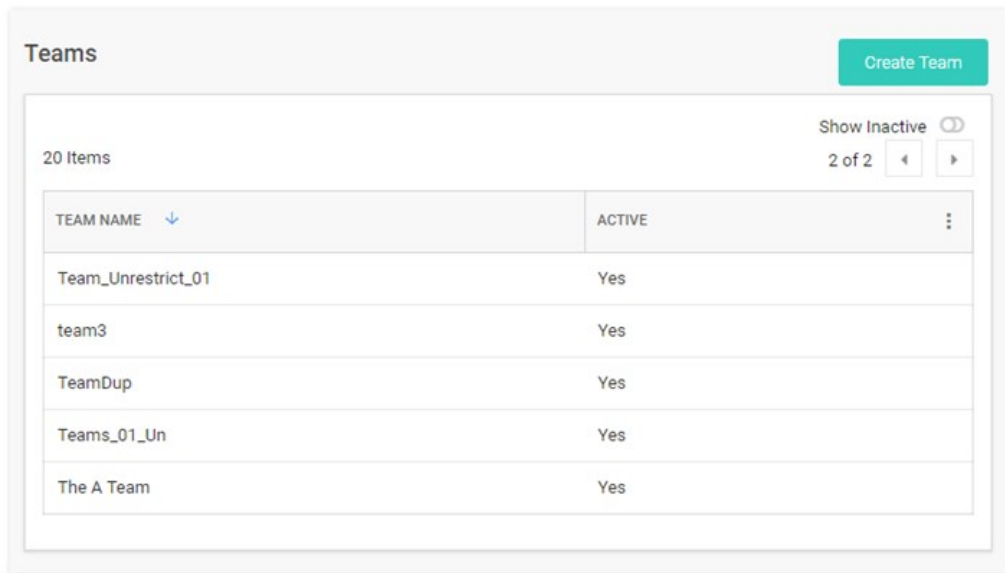
Reference options for diagnostics, logs, and security features



## Tools & Integrations

Find Secret Server tools and other product integrations here

2. Type and then click **Teams** in the list. The Teams page appears:



- Click the **Create Team** button. The Create Team popup page appears:

The screenshot shows the 'Create Team' popup form. It has two text input fields: 'Team Name \*' and 'Team Description'. At the bottom right, there are two buttons: 'Cancel' and 'Create Team'.

- Type the name for the new team in the **Team Name** text box.
- (Optional) Type a description in the **Team Description** text box.
- Click the **Create Team** button. The new team appears on the Teams page:

The screenshot shows the 'Teams' page with the newly created team 'Accounting' added to the list. The table has two columns: 'TEAM NAME' and 'ACTIVE'. The table contains the following data:

TEAM NAME	ACTIVE
Accounting	Yes

- Click the table row for the newly created team. That team's page appears:

Teams > Accounting

**General**

Sites

Audit

Members

**TEAM** [EDIT](#)

**Team Name \*** Accounting

**Description** Accounting leads

**Active** Yes

8. Click the **Sites** button on the left. The Sites page appears:

Teams > Accounting

General

**Sites**

Audit

Members

**SITES** [EDIT](#)

**Should Restrict Sites** No

9. Click the **Edit** button. The page becomes editable:

**SITES**

**Should Restrict Sites** ☐

[Cancel](#) [Save](#)

10. Click to select the **Should Restrict Sites** check box. A Site dropdown list appears:

**SITES**

**Should Restrict Sites** ☒

**SITE**

Site

Select one ▼

[Cancel](#) [Save](#)

- Click the **Site** list to select a site to restrict the team to. The selected site appears in the Site table:

**SITES**

Should Restrict Sites ☒

**SITE**

Local

Site

Select one ▼

Cancel Save

- Click the **Save** button.
- Click the **Members** button on the left. The Members page appears:

**MEMBERS** EDIT

USERS AND GROUPS

- Click the **Edit** button. The page becomes editable:

**MEMBERS**

USERS AND GROUPS

Add Groups / User

Search for groups or use 🔍


Cancel Save

- Type the name of the desired user or group to add in the **Add Groups / User** search box. When you begin typing, a list of available groups and users appear below. Select one. The user or group appears in the Users and Groups table:

**MEMBERS**

**USERS AND GROUPS**

Will [Remove](#)

**Add Groups / User**  
 

Cancel

Save

16. Click the **Save** button. The member appears on the Members page:

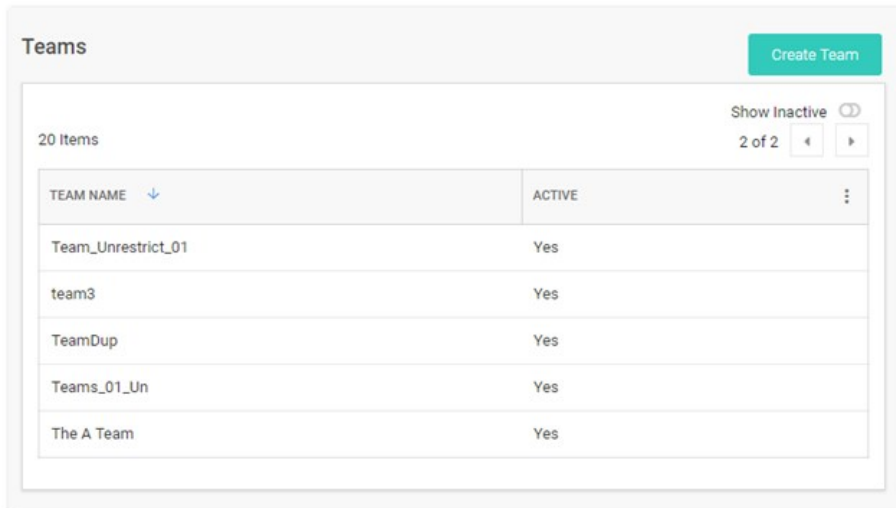
**MEMBERS** [EDIT](#)

**USERS AND GROUPS**

Will

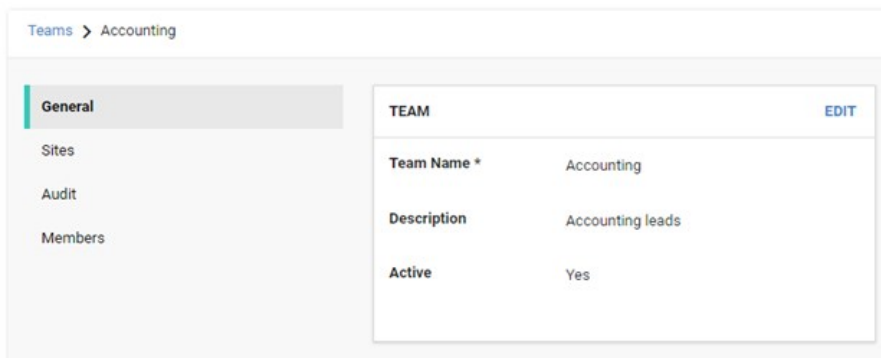
**Note:** You cannot delete teams because of auditing restrictions.

1. In SS, click the **Admin** menu item. The Administration page appears.
2. Click the **Teams** button in the list. The Teams page appears:



TEAM NAME	ACTIVE
Team_Unrestrict_01	Yes
team3	Yes
TeamDup	Yes
Teams_01_Un	Yes
The A Team	Yes

3. Click the table row for the desired team. That team's page appears:



TEAM	
Team Name *	Accounting
Description	Accounting leads
Active	Yes

4. On the **General** page, click the **Edit** button. The tab becomes editable:

**TEAM**

Team Name \*

Accounting

Description

Accounting leads

Active

☒

Cancel

Save

5. Click the **Active** check box to deselect it.
6. Click the **Save** button. The team is deactivated.

1. In SS, click the **Admin** menu item. The Administration page appears.
2. Type and then click **Teams** in the list. The Teams page appears:

Teams

Create Team

20 Items

Show Inactive ☐

2 of 2 ◀ ▶

TEAM NAME <span>↓</span>	ACTIVE	
Team_Unrestrict_01	Yes	
team3	Yes	
TeamDup	Yes	
Teams_01_Un	Yes	
The A Team	Yes	

3. Click the table row for the desired team. That team's page appears:

Teams > Accounting

General

Sites

Audit

Members

TEAM

EDIT

Team Name \*

Accounting

Description

Accounting leads

Active

Yes

4. On the **General** page, click the **Edit** button to change:
  - The team name
  - The team's description
  - The team's status
5. To restrict the visible sites:
6. Click the **Sites** button on the left. The Sites page appears

Teams > Accounting

General  
**Sites**  
Audit  
Members

SITES [EDIT](#)

Should Restrict Sites	No
-----------------------	----

- Click the **Edit** button. The page becomes editable:

SITES

Should Restrict Sites
☐

Cancel
Save

- Click to select or deselect the **Should Restrict Sites** check box. If you enabled it, a Site dropdown list appears:

SITES

Should Restrict Sites
☒

SITE

Site

Select one ▼

Cancel
Save

- Click the **Site** list to select a site to restrict the team to. The selected site appears in the Site table:

**SITES**

Should Restrict Sites ☒

**SITE**

Local

**Site**

Select one ▼

Cancel Save

10. Click the **Save** button.

11. To edit the team's member users or groups:

1. Click the **Members** button on the left. The Members page appears:

**MEMBERS** EDIT

**USERS AND GROUPS**

2. Click the **Edit** button. The page becomes editable:

**MEMBERS**

**USERS AND GROUPS**

**Add Groups / User**

Search for groups or use 🔍

Cancel Save

3. Type the name of the desired user or group to add in the **Add Groups / User** search box. When you begin typing, a list of available groups and users appear below. Select one. The user or group appears in the Users and Groups table:

MEMBERS

USERS AND GROUPS

Will

Remove

Add Groups / User

Cancel

Save

- Click the **Save** button. The member appears on the Members page:

MEMBERS

EDIT

USERS AND GROUPS

Will

- View events for the team using its audit trail:

- Click the **Audit** button on the left. The Audit page appears:

Audit

3 Items

DATE <span>↓</span>	DISPLAY NAME	ACTION	NOTES	
01/14/2019 02:54 pm	Will	Edit	ShouldRestrictSites: false to true;	
01/14/2019 02:54 pm	Will	UPDATE SITE MAP	+ Local	
01/14/2019 02:33 pm	Will	Create		

- Audit events occur when:

- The team is created

- General tab: name, description, or active status is changed
- Sites tab: restrictions are added, removed, or changed
- Members: users or groups are added or removed

Users can view other users not in their teams if that user already had a connection, such as a shared secret, with the other user prior to setting up the team restrictions.

The API does not restrict who can be assigned if they use the known group ID of a user or group not in their team. This is designed so secret permissions can be saved across teams without removing the permissions of another team.

1. Navigate to **Admin** > **See All**. The Administration page appears:

What are you looking for?

Search for an admin option



[Simplified View](#) ▾



## Actions

Secret Server features that perform important jobs



## Setup & System Maintenance

Setup your Secret Server system and keep it running with Licensing, Backups, Imports, Networking options, and more



## Users, Roles, Access

These features help you organize users & permission settings within Secret Server



## Diagnostics, Logs, Security

Reference options for diagnostics, logs, and security features



## Tools & Integrations

Find Secret Server tools and other product integrations here

2. Type and then click **Users** in the search text box. The View User page appears:

## View User

User Name	[REDACTED]
Display Name	[REDACTED]
Email Address	[REDACTED]@thycotic.com
Domain	Local
Two Factor	< None >
Enabled	Yes
Locked Out	No
Application Account	No

### IP Address Restrictions

None

Restricted By Team	No
--------------------	----

You can see if the user belongs to a team, and if so, what teams the user belongs to. If the Restricted by Team line says *No*, it means the user has been granted the Unrestricted by Teams permission, which means the user can view all users, groups, and sites.

## Users

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

Bulk operations on users can also be performed from the **Users** page. Select one or more users using the check boxes beside the **User Name** column, or select all or none by toggling the check box in the header row. Once the appropriate users have been selected, use the Bulk Operation list at the bottom of the grid to select an action. Bulk operations on users currently include enabling or disabling user access, as well as configuring users for email or RADIUS two-factor authentication.

User settings can be modified by clicking the username in the **User Name** column on the **Users** page. Search for users using the search bar at the top of the grid. To show users that are marked inactive, check the **Show Inactive Users** box below the grid.

To manually create a single user, navigate to **Administration > Users** and click the **Create New** button. On the subsequent page, you can enter the relevant information for a user.

**Note:** To add many users from your Active Directory setup, you can use Active Directory synchronization (see [Active Directory Synchronization](#)).

You cannot delete users per se because of auditing requirements; however, deactivating the user from the [User Settings page](#) accomplishes the same thing. See [Removing Deactivated User PII](#) for eliminating all traces of a deactivated user.

The following settings are found in the **Administration > Configuration** page, inside the **Local User Passwords** tab. These settings apply to users that were created manually, not users brought into SS through Active Directory synchronization:

- **Allow Users to Reset Forgotten Passwords:** If enabled, the "Forgot your password?" link appears on all users' login screens. Clicking on this link prompts the user to enter the email address that is associated with the user's SS account. If the email address is found, then an email containing a link for password reset is sent. Note that this only works for local user accounts and not for Active Directory accounts.
- **Enable Local User Password Expiration:** When enabled, SS forces a password change for a user after a set interval. After the interval time has elapsed, the next time the user attempts to log in, they are prompted for the old password, a new password, and a confirmation of the new password. The new password is validated against all the password requirements. Newly created local users are also be prompted to change their password upon logging into SS for the first time when this setting is enabled.
- **Enable Local User Password History:** If enabled, this prevents a user from reusing a password. For example, if set to "20 Passwords", this would prevent the user from using a password they have used the previous 20 times. This in conjunction with "Enable Minimum Local Password Age" helps ensure that users are using a new and unique password frequently rather than recycling old passwords.
- **Enable Minimum Local User Password Age:** If enabled, the value for this setting reflects the minimum amount of time that needs to elapse before a password can be changed. This prevents a user from changing their password too frequently, which allows them to quickly re-use old passwords.
- **Local User Password is valid for:** If enabled, this is the interval that a local user password is valid before it must be changed (see "Enable Local User Password Expiration" setting for details). If this setting is disabled, the entered value displays as "Unlimited".
- **Lowercase Letters Required for Passwords:** Force all user SS login passwords to contain at least one lowercase letter.
- **Minimum Password Length:** Force all user SS login passwords to contain a set minimum number of characters.

**Note:** The maximum number of characters is 1024.

- **Numbers Required for Passwords:** Force all user SS login passwords to contain at least one number.
- **Symbols Required for Passwords:** Force all user SS login passwords to contain at least one symbol, such as !@#%&^\*.
- **Uppercase Letters Required for Passwords:** Force all user SS login passwords to contain at least one uppercase letter.

## Overview

General Data Protection Regulation (GDPR) adherence raises the possibility that SS users may make a data removal claim against a SS administrator. This requires removing any personally identifiable information (PII) in SS for that individual.

To address this, SS has a button that automatically removes most PII for any deactivated user.

## Removing the PII

1. Remove the user from Active Directory (AD). See [Active Directory Considerations](#) below.
2. In SS, go to **Admin > Users**. The Users page appears.
3. Click the user name link for the desired user. The View User Page appears.
4. Click the **Remove Personally Identifiable Information** button. A confirmation dialog box appears.

**Important:** Once you confirm, the user cannot log on to SS. Click the Cancel button if you are not positive this is what you want to do.

Clicking the **OK** button will change these to random values:

- Username
- Display name
- Password
- Personal folder name
- Personal group name
- RADIUS username

In addition:

- The user's AD GUID is cleared
- The user's email address is removed from their record
- The user's name is replaced with "<redacted>" in event audits where it can be clearly identified.
- The PII removal is recorded in the user's audit

5. Click the **OK** button. The removal begins. Once complete, the Remove PII button disappears for that user.
6. (Optional) Run a query that scans the entire SS database for the removed strings. You may want to do this because the process cannot find *all* potential instances of USER PII throughout SS, such as that in secret names or notes.

**Note:** You can create an Event Subscription to "remove user PII" events.

## Active Directory Considerations

We recommend removing the user from AD before removing the PII. If you remove the PII without first removing the user from AD, the user is reintroduced into SS on subsequent AD synchs. This creates a new user account in SS, which might require you to to disable this new user account and remove its PII too (after removing the AD user).

If a user fails their login too many times (specified in the **Local User Passwords** section of the configuration page), their account is locked out and they are not be able to log in.

To unlock the account:

1. Log on as an administrator.
2. Click on **Admin > Users**.
3. Click on the user who is locked out.
4. Click **Edit**.
5. Click to deselect the **Locked out** check box.
6. Click **Save**.

SS users can be set up with many different login requirements. For example, you can force strong Login passwords by requiring a minimum length and the use of various character sets.

The following settings are available under the **Administration > Configuration** page, inside the **Login** tab:

- **Allow AutoComplete:** AutoComplete is a feature provided by most Web browsers to automatically remember and pre-fill-in forms for you. This can be a great security concern since they typically do not save the data in a secure manner. You can enable or disable Web browser pre-fill on the login screen by using this option.
- **Allow Remember Me:** This option enables the Remember Me checkbox on the Login screen. When a user chooses to use remember me, an encrypted cookie is set in their browser. This enables the user to revisit SS without the need to log in. This cookie is no longer valid when the remember me period has expired. They then have to enter their login information again. This option allows users to remain logged in for up to a specific period (specified in the "Remember Me Is Valid for" setting mentioned below). This option can be a security concern as it does not require re-entry of credentials to gain access to SS.

**Note:** "Remember me" is only visible if the "Allow Remember Me" setting is enabled. This is the period that the remember me cookie mentioned above is valid. For example: if set to one day, then users taking advantage of "remember me" have to log in at least once a day. To set a time value (minutes, hours, or days), uncheck the Unlimited checkbox.

- **Enable RADIUS Integration:** Allow for RADIUS server integration with your user login authentication. Other RADIUS settings appear upon enabling this option. These settings are discussed in [RADIUS Authentication](#).
- **Maximum Concurrent Logins Per User:** This setting allows a user to log into SS from multiple locations at once without logging out their sessions at other locations.
- **Maximum Login Failures:** Set the number of login attempts allowed before a user is locked out of their account. Once locked out, they need a SS administrator to reset their password and enable their account. For details on how to reset a locked account, see [Creating Users](#).
- **Require Two Factor for these Login Types:** This setting specifies which types of login require two-factor authentication:
  - Website and Web service Log on
  - Website log on only
  - Web service log on only
- **Visual Encrypted Keyboard Enabled:** This setting enables a visual keyboard for logins.
- **Visual Encrypted Keyboard Required:** This setting requires a visual keyboard for logins.

User Administrators can also set another group or user as the *user owner* for a SS local user. User owners can manage and edit just that user. For example, a developer might need to unlock or reset the password for an application account but should not have access to all users. Set **Managed by to User Owners** on a user and then select **Groups** or **Users**. Note that Unlimited Administrator mode can still be used to manage groups with user owners assigned.

**Note:** Users can set their preferences by hovering on their profile icon in the top right and selecting preferences.

## General Tab

The following configuration settings are available for users under the General tab:

- **Date Format and Time Format:** Date and time format displayed for a user in SS.
- **Language and My Theme:** Customize the look of SS on a per user basis. For details, see [Themes](#).
- **Mask passwords when viewing Secrets:** When enabled, this masks the Password text box for a secret. There is a configuration setting that forces this to be enabled for all users. For details on password masking, see [Setting Up Password Masking](#).
- **Send email alerts when dependencies fail to update:** Enables emails to be sent when dependencies fail to update.
- **Send email alerts when Heartbeat fails for Secrets:** When enabled, the user is emailed when a heartbeat fails for any secret the user has view permission to.
- **Send email alerts when Secrets are changed:** Enables emails to be sent on all changes of any secret that the user has view permission. There is a limit of one mail per five minutes per edit of the same user. For example, if user "User1" edits the secret twice within this grace period, only one email is sent.
- **Send email alerts when Secrets are viewed:** Enables emails to be sent on all views of any secret that the user has view permission. There is a limit of one email per five minutes per view of the same user. For example, if user "User1" views the secret twice within this grace period, only one email is sent.
- **Show the full folder path on search results:** Enables the full path to be displayed in the Folder column on the Home page.
- **Use the TreeView control for search on the home screen:** Enables the TreeView control for the Search tab on the Legacy Home screen. This option does not apply to the Dashboard.

## Launcher Tab

The following configuration settings are available to users on the Launcher tab:

- **Allow Access to Printers, Allow Access to Drives, Allow Access to Clipboard:** Allow access to various items when using the launcher.
- **Connect to Console:** Allows you to connect to remote machines using the Remote Desktop launcher and connects as an administrator. This is the equivalent of using the `/admin` or `/console` switch when launching Remote Desktop.
- **Use Custom Window Size:** Checking this box displays Width and Height text boxes for the user to specify a custom window size for an RDP launcher.

The following restriction settings are available:

- **Enable Login Policy:** If enabled, this simply displays the policy. To force the acceptance of the policy.
- **Force Inactivity Timeout:** This setting is the time limit on idle SS sessions. Once a session expires, the user must login again with their username and password.
- **Force Login Policy:** This setting forces the checking of the "I accept these terms" checkbox before allowing the user to login to SS.
- **IP Restrictions:** This setting can be entered by going to **Administration > IP Addresses**. In there, you can enter the IP ranges you wish your users to use. To configure a user to use the ranges, navigate to the **User View** page and click the **Change IP Restrictions** button. In the subsequent page, you can add all the ranges you want your user to use.
- **Login Policy Agreement:** The Login Policy Agreement is displayed on the login screen. You can change the contents of the Login Policy Statement by editing the file `policy.txt`. By default, this is not enabled. The settings to enable this are accessed by first navigating to **Administration > Configuration** and going into the **Login** tab. Then click the **Login Policy Agreement** button.

Below is a brief explanation of each text-entry field or control:

- **Display Name:** Text that is used throughout the user interface, such as in audits.
- **Domain:** If a drop-down list is visible, selecting a domain from the list is one way to set the expected domain of the user. However, a more dynamic way to have this text-entry field (and all the other text-entry fields) set is through Active Directory synchronization.
- **Email Address:** Email address used for Request Access, email two-factor authentication, and the like.
- **Email Two-Factor Authentication:** On a login attempt, the user has an email sent to the email address entered above. This email contains a pin code that the user needs to log into the account. See [Email Two-Factor Authentication](#) for details.
- **Enabled:** Disabling this control removes the user from the system. Effectively, this is the way to delete a user. SS does not allow complete deletion of users due to auditing requirements. To re-enable a user, navigate to the **Administration > Users page**, check the **Show Inactive Users** checkbox just under the **Users** grid, and edit the user to mark them enabled (see [Configuring Users](#)).
- **Locked Out:** If checked, then this user has been locked out of the system due to too many login failures. To remove the lock, uncheck the check box. For more details on locking out users, see Maximum Login Failures setting described in the Login Settings section.
- **Password:** Login password for the user. For the various login settings, see Login Settings section.
- **RADIUS Two-Factor Authentication:** This text-entry field only appears if RADIUS authentication is enabled in the configuration. On a login attempt, the user must enter the RADIUS token sent from the RADIUS server. See [RADIUS Authentication](#).
- **RADIUS User Name:** This text-entry field only appears if the above RADIUS Two Factor Authentication setting is enabled. This is the username the RADIUS server is expecting. See [RADIUS Authentication](#).
- **User Name:** Login name for the user.

**Note:** A new user is assigned the User role by default. For more information on roles, see "Roles."

## Webservices

**Note:** Please click the table of contents on the left to see any sub-pages to this one. Click the table of contents on the right to see headings on this page.

SS provides a suite of webservices which can be used to retrieve and update secrets, and folders. The webservices allow SS to be accessed using the mobile apps as well as custom built integrations. The webservices are secure and require authentication in the same manner as regular access to SS. All actions that involve data are also logged, such as secret views, updates, and adds.

Webservices can be enabled at the **Administration > Configuration** general tab. Enabling webservices simply makes the ASP.NET webservices built into SS available. They are found under `/webservices/sswebservice.asmx` in your SS directory. They run on the same port as the Web application. You can view them with a browser to see the functionality that is offered. Specific webservice functionality is documented in the SS Webservice API guide.

SS also provides a webservice that uses integrated Windows authentication instead of a username and password. This webservice can be used in an application or script to access SS and retrieve secrets without storing the login credentials in the application or configuration file.

**Note:** See the [Windows Integrated Authentication Webservice](#) (KBA) article for more advanced technical information on using this webservice.

SS can set up a Java Console API to retrieve values from SS without embedding a password. This allows scripts to retrieve passwords from SS while keeping both the password and credentials to SS secure. The SS Java Console is setup using a user in SS, but the password is changed and hardware-specific, so copying the jar file to other machines does not allow it to access SS. As a user in SS, an admin can share only specific secrets with the account running the Java Console. As a Java implementation, this can be used on any OS including Windows, Mac, Linux and Unix. For installation instructions and examples see the [Application API Guide](#).

## Secret Server Release Notes

**Note:** As of Secret Server 10.8, Secret Server Cloud release notes are included in the main release notes.

**Note:** Scroll down for legacy Secret Server Cloud.

### [Secret Server 10.8.000004](#)

- [Secret Server 10.8.000000](#)
- [Secret Server 10.7.000059](#)
- [Secret Server 10.7.000002](#)
- [Secret Server 10.7.000000](#)
- [Secret Server 10.6.000027](#)
- [Secret Server 10.6.000026](#)
- [Secret Server 10.6.000001](#)
- [Secret Server 10.6.000000](#)
- [Secret Server 10.5.000003](#)
- [Secret Server 10.5.000001](#)
- [Secret Server 10.5.000000](#)
- [Secret Server 10.4.000000](#)
- [Secret Server 10.3.x](#)
- [Secret Server 10.2.x](#)
- [Secret Server 10.1.x](#)
- [Secret Server 10.0.x](#)
- [Secret Server 9.x](#)
- [Secret Server 8.x](#)
- [Secret Server 7.x](#)
- [Secret Server 6.x](#)
- [Secret Server 5.x](#)
- [Secret Server 4.x](#)

- [Cloud Release December 21, 2019](#)
- [Cloud Release September 21, 2019](#)
- [Cloud Releases prior to September 21, 2019](#)

### [Documentation Changelog](#)