

Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

Group Policy Guide

August 2019 (release 19.6)

Centrify Corporation



Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

© **2004-2019 Centrify Corporation. All rights reserved.** Portions of Centrify software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify for Mobile, Centrify for SaaS, DirectManage, Centrify Express, DirectManage Express, Centrify Suite, Centrify User Suite, Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are registered trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

About this guide	18
Intended audience	18
Using this guide	18
Documentation conventions	19
Finding more information about Centrify products	20
Product names	20
Contacting Centrify	22
Getting additional support	23
 Group policies in Active Directory	 24
Configuring computer and user settings	24
How group policies are applied	25
Order in which policies are applied	26
How the resulting policy set is determined	27
Editing a Group Policy Object	29
Selecting computer or user settings	29
Applying policies in nested organizational units	30
Configuring group policies to be refreshed	31
 Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service group policy overview	 32
Mapping settings to a virtual registry	33
Configuring settings in administrative templates	34
Mapping computer configuration policies	35
Mapping user configuration policies	36
Editing configuration settings manually	36

Updating configuration policies manually	37
Using standard Windows group policies	38
Reporting group policy settings	39

Adding Centrify settings to Group Policies Objects 41

Adding administrative templates to a Group Policy Object	41
Installing Centrify group policy templates	42
Template file formats	42
Selecting a Group Policy Object for Centrify settings	43
Linking a Group Policy Object to an organizational unit	44
Using security filtering for group policies	44
Adding Centrify policies from XML files	46
Adding templates after an upgrade	47
Enabling Centrify policies	47
Centrify policy limitations	48

DirectControl Settings 50

Add centrifydc.conf properties	52
Enable Active Directory PAM Privilege Escalation Feature	53
Maintain DirectControl 2.x compatibility	53
Merge local group membership	53
Prefer authentication credentials source	54
Set LDAP fetch count	54
Set password cache	55
Set user mapping	56
User's initial group ID	57
Use FIPS 140-2 compliance algorithms	58
Basic requirements	58

Enabling the policy	59
Related configuration parameters	60
Account prevalidation	61
Specify allowed groups for prevalidation	61
Specify allowed users for prevalidation	62
Specify denied groups for prevalidation	62
Specify denied users for prevalidation	62
Set prevalidation service name	63
Set prevalidation update interval	64
Adclient settings	65
Add attributes to cached objects	65
Auto Zone group policies	67
Configure /etc/nsswitch.conf (Solaris, HPUX, Linux)	71
Configure /etc/{pam.conf,pam.d} (AIX, Solaris, HPUX, Linux, Mac OS X)	72
Configure /etc/security/user (AIX)	72
Configure /usr/lib/security/methods.cfg (AIX)	72
Configure Directory Services (Apple OS/X)	72
Configure dump core setting	72
Disable multi-factor authentication (MFA) on Centrify-managed computers	73
Disable nscd group and passwd caching (Solaris, Linux)	73
Disable pwgrd (HPUX)	73
Enable core dump cleanup	73
Enable logon hours local enforcement	74
Encrypt adclient cache data	74
Force domains and forests to be one-way trusted	75
Force password salt lookup from KDC	75
Map /home to /User (Mac OS X)	76
Run adclient on all processors	76

Set cache cleanup interval	76
Set the connector refresh interval	77
Set maximum number of threads	77
Set the maximum simultaneous authentication requests allowed	77
Set minimum number of threads	78
Specify low disk space interval	78
Specify low disk space warning level	78
Specify a per machine (random) delay for cache refreshed background tasks	79
Use the legal Kerberos type for cache encryption	80
Addns Settings group policies	81
Enable addns invoked by adclient	81
Set command line options used by adclient	81
Set DNS records update interval	82
Set wait response interval for update requests	82
Dzdo settings	83
Always add anchors to regex in dzdo and dzcmds	83
Enable logging of valid command execution in dzdo	83
Enable user command timeout	83
Force dzdo re-authentication when relogin	84
Force dzdo to set HOME environment variable	84
Force dzdo to set HOME environment variable when runs with '-s' option ...	85
Force per tty authentication in dzdo	85
Prompt error message if command not found by dzdo	85
Replace sudo by dzdo	86
Require dzdo command validation check	86
Require runas user for dzdo	87
Require user is logged in to a real tty to run dzdo	87
Set directory to store user timestamp by dzdo	88

Set dzdo authentication timeout interval	88
Set dzdo password prompt timeout interval	88
Set dzdo validator	89
Set environment variables to be preserved by dzdo	90
Set environment variables to be removed by dzdo	90
Set environment variables to be removed by dzdo with characters % or / ...	91
Set error message when failed to authenticate in dzdo	91
Set lecture shown by dzdo before password prompt	92
Set password prompt for target user password in dzdo	92
Set paths for command searching in dzdo	93
Set secure paths for command execution in dzdo	93
Show lecture by dzdo before password prompt	94
Use realpath to canonicalize command paths in dzdo	95
Group policy settings	96
Enable user group policy	96
Set machine group policy mapper list	96
Set group policy mapper execution timeout	97
Set user group policy mapper list	97
Set total group policy mappers execution timeout	97
Use user credential to retrieve user policy	98
Kerberos settings	99
Allow PAM to create user Kerberos credential cache	99
Allow weak encryption types for Kerberos authentication	99
Alternative location for user .k5login files	100
Disable Kerberos built-in ccselect plugins	100
Enable Kerberos clients to correct time difference	101
Force Kerberos to only use TCP	101
Generate the forwardable tickets	101

Generate Kerberos version numbers for Windows 2000	101
Manage Kerberos configuration	102
Renew credentials automatically	102
Set configuration update interval	103
Set Kerberos UDP preference limit	103
Set credential renewal interval	103
Set password change interval	104
Set password change verification interval	104
Set password change verification attempts	104
Specify credential cache type for AD users	105
Specify groups to infinitely renew Kerberos credentials	106
Specify maximum Kerberos credential cache lifetime	106
Specify users to infinitely renew Kerberos credentials	107
Specify whether CDC k5login module should ignore .k5login for SSO	107
Specify whether Kerberos PAC Checksum validation should be done	107
Strictly Enforce Default Encryption Types	108
Strictly Enforce Permitted Encryption Types	109
Use DNS to lookup KDC	109
Use DNS to lookup realms	110
Local account management settings	111
Enable local account management feature	111
Notification Command Line	111
Logging settings	113
Set Adclient audit logging facility	113
Set general audit logging facility	113
Set log message queue size	114
Set NIS audit logging facility	115
Login settings	116

Allow localhost users	116
Allow offline login when user account is locked out	117
Enabled nss emergency shell	117
Manage login filters	118
Set minimum group ID (lookup)	118
Set minimum user ID (lookup)	119
Set sync mapped users	119
Specify group names to ignore	120
Specify the certificate files to add (lookup)	120
Specify the fingerprints of certificate files to ignore (lookup)	121
Specify user names to ignore	121
Split large group membership	122
MFA Settings	123
Enable multi-factor authentication for autozone and classic zone	123
Set background fetch interval for groups that require multi-factor authentication	123
Specify Centrify Identity Platform tenant ID for multi-factor authentication	124
Specify AD users that can login when multi-factor authentication is unavailable	124
Specify AD groups that require multi-factor authentication	125
Specify AD users that require multi-factor authentication	126
Specify Centrify Identity Platform URL for multi-factor authentication	126
Network and cache settings	128
Blacklist DNS DC hostnames	128
Enable LDAP cross-forest search	128
Enable user lookup and login by CN	129
Enable user lookup and login by displayName	129
Force DNS to use TCP	130
Force DNS to rotate	130

Force switching to different domain controller in the preferred site periodically	130
Set cache negative life time	131
Set DNS cache size (deprecated)	131
Set DNS cache timeout	131
Set DNS UDP buffer size	132
Set domain DNS refresh interval (deprecated)	132
Set GC expiration	133
Set group object expiration	133
Set idle client timeout	133
Set LDAP connection timeout	133
Set LDAP response timeout	134
Set LDAP search timeout	134
Set LDAP trust timeout	134
Set LRPC response timeout	134
Set LRPC2 receive timeout	135
Set LRPC2 send timeout	135
Set maximum server connection attempts	135
Set object expiration	136
Set refresh interval for access control cache	136
Set UDP timeout	137
Set user object expiration	137
Specify AD to NTLM domain mappings	137
Specify DNS DC hostnames	138
Specify DNS GC hostnames	139
NIS daemon settings	141
Set thread number for NIS daemon	141
Specify NIS daemon update interval	141
Specify allowed NIS mapping files for NIS daemon	142

Specify disallowed NIS mapping files for NIS daemon	142
Specify allowed client machines for NIS daemon	143
Set switch delay time for NIS daemon	143
Set maximum number of mapping files allowed for NIS daemon	144
Set large group suffix for NIS daemon	144
Set large group name length for NIS daemon	145
Set domain name for NIS daemon	146
Set startup delay time for NIS daemon	146
NSS overrides	148
Specify NSS group overrides	148
Specify NSS password overrides	149
PAM settings	152
Create home directory	152
Create k5login	152
Set home directory permissions	152
Set multi-factor authentication to use an external PAM module	153
Set options for multi-factor authentication by an external PAM module	153
Set UID conflict message	154
Set UID conflict resolution	154
Set user name and UID conflict message	155
Set user name conflict message	155
Specify message for creating home directory	156
Specify NTLM authentication domains	156
Specify programs for which multi-factor authentication is ignored	157
Password prompts	158
Set account disabled error message	158
Set account expired error message	158
Set account locked message for adpasswd	158

Set adclient inaccessible message	158
Set password change disallowed message for adpasswd	159
Set invalid user or password message for adpasswd	159
Set permission denied message for adpasswd	159
Set lockout error message	159
Set error message for empty password entered	159
Set new password's mismatch error message for password change	160
Set notification text for password change	160
Set old password incorrect error message for password change	160
Set violation error message for password change	160
Set password prompt for confirming new password change	160
Set password prompt for new password change	161
Set password prompt for old password change	161
Set message text for password change	161
Set login password prompt	161
Set password expiry approaching text	161
Set workstation denied error message	162
Sudo settings	163
Forcesudo re-authentication when relogin	163

Windows Settings 165

Common Settings	165
Configure Windows authentication user privilege elevation grace period ...	165
Custom message for locked user accounts	166
Disable automatic enrollment of Windows devices	166
Disable the Centrify notification icon	166
Enable enrollment as personal device	167
Enable setup Centrify offline MFA profile	167

Enable use of alternate user's role to run an application	167
Hide command line arguments in Analytics	168
Prevent local administrators from being able to log on in rescue mode (when there are no explicit rescue users defined)	168
Re-authentication: Require smart card	169
Require justification on privilege elevation	169
Specify a list of blacklisted domains	170
Specify a list of rescue users (when the agent is not joined to a zone)	170
Specify a list of whitelisted domains	171
Specify endpoint enrollment desktop notification message	171
Specify offline MFA profile desktop notification message	171
Specify a privilege elevation validator	172
Specify whether to keep the desktop notification permanently visible	173
MFA Settings	173
Configure multi-factor authentication for logon when the agent cannot connect to the Platform	173
Configure multi-factor authentication for privilege elevation when the agent cannot connect to the Platform	174
Connect to the Centrify Identity Platform directly	174
Continue with MFA Challenges after failed Windows authentication in logon screen	174
Disable multi-factor authentication for screen unlock	175
Disable self-service password reset	175
Enable multi-factor authentication for Windows login (when the agent is not joined to a zone)	176
Force to enter explicit UPN	176
Send UUID for MFA Challenges	176
Skip client certificate authentication	176
Specify a web proxy URL	177
Specify Active Directory users that require multi-factor authentication on Windows login (when the agent is not joined to a zone)	177

Specify how frequently to check for responses to multi-factor authentication challenges	177
Specify multi-factor authentication grace period	178
Specify the authentication source for privilege elevation	179
Specify the Centrify connector URL to use	179
Specify the connection timeout for multi-factor authentication requests ...	179
Specify credential providers to exclude from the logon screen	180
Specify the Platform instance Id to use (when the agent is not joined to a zone)	180
Specify the Platform instance URL to use	181
Specify the Platform instance URL to use (when the agent is not joined to a zone)	181
Specify the timeout on skipping previously disconnected Centrify connectors	182
Specify the timeout on using the last successfully connected Centrify connector first	182
Remote Authentication Dial-In User Service (RADIUS) Service Settings	182
Enable Remote Authentication Dial-In User Service (RADIUS)	182
Specify the RADIUS connection timeout	183
Specify the RADIUS server IP address	183
Specify the RADIUS server port number	183

Audit and audit trail settings 184

Alternate location for policies installed with an ADMX template	184
Audit Trail Settings	184
Audit trail snap-in policies	185
Audit trail ADMX template policies	185
Send audit trail to Audit database	186
Send audit trail to log file	186
Audit Trail Overrides	186

Audit Trail Targets	187
Centrify Audit Settings	189
Common Settings	189
Collector Settings	192
DirectAudit advanced monitoring	193
UNIX Agent Settings	196
DirectAudit Daemon Settings	197
DirectAudit NSS Settings	208
DirectAudit Shell Settings	211
LRPC2 Client Settings	221
Spool Disk Space Settings	222
Windows Agent Settings	225

Additional group policies for UNIX services229

Common UNIX settings	229
Copy files	230
Copy files from SYSVOL	231
Sudo Rights	232
Set crontab entries	234
Specify commands to run	235
Linux Settings	236
Enforce screen locking	236
Specify basic firewall settings	238
Specify network login message settings	239
Security	239
Certificate validation method	239
Enable smart card support	240
Lock Smart Card screen for RHEL	241

Require smart card login	241
Specify applications to import system NSSDB	242
SSH (Secure shell) settings	242
Add sshd_config properties	243
Allow challenge-response authentication	243
Allow groups	243
Allow GSSAPI authentication	244
Allow GSSAPI key exchange	244
Allow users	244
Deny groups	245
Deny users	245
Enable application rights	245
Enable PAM authentication	246
Enable SSO MFA Properties	246
Match Block	247
Permit root login	248
Set banner path	248
Enable Rlogin Control SFTP	248
Enable Rlogin Control SSH	249
Specify authorized key file	249
Specify ciphers allowed for protocol version 2	250
Specify client alive interval	250
Specify log level	250
Specify login grace period	251
Specify maximum client alive count	251
Mac OS X Settings	252
Group policies and system preferences	252

Adding Mac OS X group policies	254
Installing the administrative template	254
Installing the agent and system files	255
Enabling and disabling Mac OS X group policies	255
Setting Mac OS X computer policies	256
Setting Mac OS X user policies	257

GNOME settings 260

GNOME desktop preferences	260
Adding GNOME group policy templates	261
Setting GNOME policies	261
Verifying GNOME policy settings	262
Troubleshooting GNOME policy settings	263
Using the Enable GNOME group policy	264
Creating custom GNOME settings through group policy	265

Defining custom group policies 266

Implementing custom group policies	266
Creating a custom Administrative Template	267
Defining a policy	267
Defining the user interface for a policy	269
Validating Settings	277
Adding a mapper program to the agent	280

About this guide

The *Group Policy Guide* describes the Centrify group policies that are available in Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service for cross-platform access control and privilege management. These group policies allow you to centrally manage computer and user configuration settings through the Microsoft Group Policy Objects.

Intended audience

This guide is intended for administrators who want to customize the operation of Centrify software by modifying group policies.

This guide is intended as a supplement to the main documentation set and assumes that you have a working knowledge of Centrify architecture and administration and Active Directory group policies.

Using this guide

Depending on your environment and role as an administrator or user, you may want to read portions of this guide selectively. The guide provides the following information:

- [Group policies in Active Directory](#) provides an introduction to group policies, how they are enabled, and how they are applied to Active Directory objects.
- [Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service group policy overview](#) provides an overview of how Centrify group policies work.

- [Adding Centrify settings to Group Policies Objects](#) describes how to add Centrify group policies to a Group Policy Object and how to edit group policy settings.
- [Access control and security settings](#) describes the group policies that control Centrify configuration parameters that are not related to auditing.
- [Audit and audit trail settings](#) describes the group policies that control Centrify auditing configuration parameters.
- [Additional group policies for UNIX services](#) describes the single-purpose group policies you can add to a Group Policy Object.
- [GNOME settings](#) describes the Gnome group policies you can add to a Group Policy Object.
- [Mac OS X Settings](#) provides an overview of the group policies available for Mac OS X users and computers.
- [Defining custom group policies](#) describes how to create custom administrative templates to implement your own group policies.

You'll also find an index provided for your reference.

Documentation conventions

The following conventions are used in Centrify documentation:

- Fixed-width font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, this font indicates variables. Square brackets ([]) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.
- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this guide. For complete file names for the software packages you want to install, see the distribution media.

- For simplicity, UNIX is used to refer to all supported versions of the UNIX and Linux operating systems. Some parameters can also be used on Mac OS X computers.

Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the [Centrify website](#). From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

For access to documentation for all Centrify products and services, visit the [Centrify documentation portal](#) at docs.centrify.com. From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

For details about supported platforms, please consult the release notes.

For the most up to date list of known issues, please login to the Customer Support Portal at <http://www.centrify.com/support> and refer to Knowledge Base articles for any known issues with the release.

Product names

Over the years we've made some changes to some of our product offerings and features and some of these previous product names still exist in some areas. Our current product offerings include the following services:

Current Overall Product Name	Current Services Available
Centrify Zero Trust Privilege Services	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service



Whether you're a long-time or new customer, here are some quick summaries of which features belong to which current product offerings:

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	Centrify Privileged Service (CPS)		Privileged Access Service
DirectControl (DC)			Authentication Service
DirectAuthorize (DZ or DZwin)			Privilege Elevation Service
DirectAudit (DA)			Audit and Monitoring Service
	Infrastructure Services		Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service
DirectManage (DM)	Management Services	Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated
	User Analytics Service		Privilege Threat Analytics Service

Depending on when you purchased a Centrify product offering, you may have purchased one of the following product bundles:

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
		Centrify Zero Trust Privilege Services Core Edition	Privileged Access Service and Gateway Session Audit and Monitoring	
Centrify Server Suite Standard Edition	Centrify Infrastructure Services Standard Edition	Centrify Zero Trust Privilege Services Standard Edition	Privileged Access Service, Authentication Service, and Privilege Elevation Service	
Centrify Server Suite Enterprise Edition	Centrify Infrastructure Services Enterprise Edition	Centrify Zero Trust Privilege Services Enterprise Edition	Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service (includes Gateway Session Audit and Monitoring)	
Centrify Server Suite Platinum Edition				Discontinued bundle that included DirectControl, DirectAuthorize, DirectManage, DirectAudit, and DirectSecure

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the [Centrify Technical Support Portal](#). From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrify users, ask questions, or share information, visit the [Centrify Community](#) website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

Group policies in Active Directory

This chapter provides an overview of how to use group policies configuration management in an Active Directory environment. It includes an introduction to the concept of Group Policy Objects on Windows and a summary of how group policies settings are inherited through an Active Directory structure.

The following topics are covered:

- Configuring computer and user settings
- How group policies are applied
- Editing a Group Policy Object
- Selecting computer or user settings
- Applying policies in nested organizational units
- Configuring group policies to be refreshed

Note This chapter only provides an overview of key concepts for working with group policies and Group Policy Objects. For more complete information about creating and using group policies and working with Group Policy Objects, see your Active Directory documentation. If you are already familiar with group policies and inheritance rules for Group Policy Objects, you can skip this chapter.

Configuring computer and user settings

Group policies allow you to specify a variety of configuration options and apply those settings to specific groups of computers and users through Active Directory. In a standard Windows environment, these configuration options



control many aspects of computer operation and the user experience, including the user's desktop environment, operations performed during startup and shutdown, local security enforcement, user- and computer-based settings in the local Windows registry, and software installation and maintenance services.

The configuration options available and the settings you make for those options are defined in a **Group Policy Object** (GPO) linked to an Active Directory object. Each Group Policy Object can consist of configuration information that applies to computers, configuration information that applies to users, or sections of policy specifically devoted to each.

Every Group Policy Object includes a default set of **Administrative Templates** and Software and Windows Settings that are created automatically as part of the Group Policy Object. Centrify provides additional templates to manage the Linux, UNIX, and Mac OS X computers. See [Adding Centrify policies from XML files](#) to learn how to add the Centrify templates to a group policy object.

There are two default Group Policy Objects available when you install or promote a server to be a Windows domain controller:

- Default Domain Controllers Policy
- Default Domain Policy

Your organization may have additional Group Policy Objects customized to suit your environment.

How group policies are applied

Before you can configure any settings by enabling group policies, you must create or select a Group Policy Object where the policies will apply. You can link Group Policy Objects to a specific organizational unit, domain, or site in Active Directory.

To create a new Group Policy Object

1. Open the Group Policy Management console (gpmc.msc).
2. Select a domain, organizational unit, or site, right-click, then select **Create a GPO in this domain, and Link it here.**

You must have read and write permission to access the system volume of the domain controller and the right to modify the selected site, domain, or organizational unit.

3. Type a name and, optionally, select an existing Group Policy Object to use as a model for the new Group Policy Object, then click **OK**.

Alternatively, you can select a domain, organizational unit, or site in the Group Policy Management console, right-click, then select **Link an Existing GPO** to link an existing Group Policy Object—such as the Default Domain Policy—to the selected domain, organizational unit, or site. Note that you cannot link a Group Policy Object to generic containers—such as the default Users, Computers, or Domain Controllers containers—or to containers you create.

Once you link a Group Policy Object to an organizational unit, domain, or site, the specific policies you enable are applied when computers are rebooted, when users log on, or at the next update interval if you set policies to be periodically refreshed.

Order in which policies are applied

You can link Group Policy Objects throughout the hierarchical structure of the Active Directory environment. When you have different policies at different levels, they are applied in the following order unless you explicitly configure them to block inheritance or behave differently:

- Local Group Policy Objects are applied first.
- Site-level Group Policy Objects are applied in priority order.
- Domain-level Group Policy Objects are applied in priority order.
- Organizational Unit-level Group Policy Objects are applied in priority order down the hierarchical structure of your organization, so that the last Group Policy Object used in the one that applies to the Organizational Unit the user or computer resides in.

As this set of rules suggests, a Group Policy Object linked to a site applies to all domains at the site. A Group Policy Object applied to a domain applies directly to all users and computers in the domain and by inheritance to all users and computers in organizational units and containers farther down the Active Directory tree.

A Group Policy Object applied to an organizational unit applies directly to all users and computers in the organizational unit and by inheritance to all users and computers in its child organizational units.

You can modify the specific users and computers the GPO is applied to by choosing a different point in the hierarchy, blocking the default inheritance, using security groups to create Access Control Lists, or defining WMI filters.

Note There are four group policies (run command, sudo, crontab entries and Linux firewall) that can merge the lines of different group policies to a resulting group policy. For the policies to merge, the policy in each group policy must be enforced. Policies with higher precedence will be placed lower in the resulting multi-line policy. (Ref: CS-21048a)

How the resulting policy set is determined

The order in which Group Policy Objects apply is significant because, by default, policy applied later overwrites policy applied earlier for each setting where the later applied policy was either Enabled or Disabled. Settings that are Not Configured don't overwrite anything — any Enabled or Disabled setting applied earlier is allowed to persist. You can modify this default behavior by forcing or preventing Group Policy Objects from affecting specific groups of users or computers, but in most cases, you should avoid doing so.

As an example, consider an organization with a single domain called `arcade.com` which is divided into the following top-level organizational units:

- USA
- Spain
- Korea

Each of these may be divided into lower-level organizational units, indicating major departmental or functional groupings for the top-level organizational unit. For example, the USA organizational unit may be divided into `CorporateHQ`, `Development`, and `Sales`.

A computer placed in the `CorporateHQ` organizational unit might then have several different Group Policy Objects applied to it. For example, the `arcade.com` organization might have a default domain Group Policy Object that applies to all organizational units in the domain, and each organizational unit might also have its own Group Policy Object applied.

The following table illustrates the configuration settings for two computer configuration policies—Windows Update > **Configure Automatic Updates** and Windows Media Player > **Prevent Desktop Shortcut Creation**—for the Group Policy Objects applied to the example organization `arcade.com`.

GPO name	Linked to	Sample policy configuration settings
Default Domain Policy	arcade.com	Configure Automatic Updates: Enabled with Auto download and notify for install Prevent Desktop Shortcut Creation: Enabled
USA-Specific	USA	Configure Automatic Updates: Not Configured Prevent Desktop Shortcut Creation: Enabled
All Development	CorporateHQ	Configure Automatic Updates: Not Configured Prevent Desktop Shortcut Creation: Disabled

For example, if you were managing the default domain policies used in this example, you would:

1. Start Active Directory Users and Computers.
2. Right-click the domain, `arcade.com`, then click **Properties**.
3. Click the **Group Policy** tab.
4. Select the **Default Domain Policy**, then click **Edit** to open the Default Domain Policy in the Group Policy Object Editor.
5. Click **Computer Configuration > Administrative Templates > Windows Components > Windows Update > Configure Automatic Updates** to **Enabled** and the set the **Auto download and notify for install** update option and click **OK**.
6. Click **Computer Configuration > Administrative Templates > Windows Components > Windows Media Player > Prevent Desktop Shortcut Creation** to **Enabled** and click **OK**.

When all of the policies described in the table are applied in their default order, a computer in the `CorporateHQ` organizational unit would be configured with the following policy settings:

- Configure Automatic Updates: **Enabled** with **Notify for download and notify for install**
- Prevent Desktop Shortcut Creation: **Disabled**

The User Configuration policies applied in a Group Policy Object are also determined by the organizational unit in which a UNIX user is a member. For example, if you define separate User Configuration policies in a Group Policy Object linked to the USA organizational unit, you must also add the users to this organization unit for the policies to apply. For more information, see [Applying policies in nested organizational units](#).

Editing a Group Policy Object

Any time you create a new Group Policy Object for an organizational unit, domain, or site, it includes a set of default configuration options for computers and users. Initially, all of these default configuration options are defined as “Not configured” or “Not defined” and have no effect. You can then enable the specific policies you want to use for the organizational unit, domain, or site linked to the current Group Policy Object by opening the Group Policy Object in the Group Policy Management Editor.

To edit a specific Group Policy Object

1. Open Administrative Tools, Group Policy Management (gpmc.msc).
2. Expand the Forest and Domains nodes to select a domain,
3. Expand Group Policy Objects for the domain.
4. Select an existing Group Policy Object—such as Default Domain Policy—then right-click and select **Edit**.

The default templates in Group Policy Objects do not include Centrify policies for Centrify-managed computers. For information about adding Centrify policies to Group Policy Objects, see [Adding Centrify policies from XML files](#).

Selecting computer or user settings

Group Policy Objects consist of two types of group policy settings:

- **Computer Configuration** policies define the startup and shut down operations and other computer-specific behavior. These configuration settings apply to the computers regardless of the user account that logs

on to the computer.

- **User Configuration** policies define log-on and log-off operations and other user-specific behavior. These configuration settings apply to the user account regardless of the computer the user logs on to. With these settings, users can move from computer to computer with a consistent profile.

Because the computer and user group policies contain different configuration settings, they don't affect each other directly. In planning how to implement group policies, however, you need to keep in mind which policies must be computer-based and which must be user-based. In many cases, the same group policy might be available as both a computer configuration policy and a user configuration policy. In those cases, you need to decide whether the policy is best applied to computers and all users who log on or to individual users when logging on, regardless of the computers they use.

Applying policies in nested organizational units

In many production environments, user accounts are most often defined in a parent organizational unit and computers are often placed in a child organizational unit (OU). If you have a Group Policy Object that is linked to the child organizational unit for computer policies, but the user accounts are in a parent organizational unit, the user configuration policies linked to the child organizational unit are not applied to the users when they log in to the computers in the child organizational unit. Instead, the user configuration policies linked to the child OU only apply to the users who are in that child OU.

There are two ways to apply different user configuration policies at lower levels in the organizational unit tree:

- Set the User Configuration policies at the parent level and then configure the child organizational unit to inherit the group policies from the parent.
- Enable the **User Group Policy loopback processing mode** group policy in the Group Policy Object linked to the child organizational unit to implement different user configuration policies at each level.

The **User Group Policy loopback processing mode** group policy is located under Computer Configuration, Policies, Administrative Templates, System, Group Policy. When it is enabled, Active Directory applies the Group Policy

Object settings defined for the computers in the child organizational unit to all users.

To enable the loopback policy

1. Open Administrative Tools, Group Policy Management (gpmc.msc).
2. Select the Group Policy Object linked to the child organizational unit, right-click, then select Edit.
3. Expand Computer Configuration to view policies under Group Policy.
4. Double-click **User Group Policy loopback processing mode** group policy, then select **Enabled**.

For Mode, select **Replace** if you defined a whole new set of policies or **Merge** if you are just modifying a subset of policies.

Configuring group policies to be refreshed

The computer portion of a Group Policy Object is normally applied any time you restart a computer that receives group policies. The user portion of a Group Policy Object is normally applied any time a user logs on to a computer. Both the computer and user portions of a Group Policy Object can also be configured to refresh automatically at a set interval.

To configure the refresh interval and the conditions for refreshing group policies, use the policies listed under **Computer Configuration > Administrative Templates > System > Group Policy** and **User Configuration > Administrative Templates > System > Group Policy** of a Group Policy Object.

If you configure your Group Policy Objects to refresh periodically, at the interval you specify, the computer contacts Active Directory to get the Group Policy Objects that apply and configures itself with the appropriate settings. If policies are refreshed at a set interval, users can change their configuration settings or their computers' configuration settings, but the changes will be overridden when the group policies are refreshed at the next interval.

If you configure the refresh policy settings for users or computers, the refresh policy applies to both Windows and agent-managed computers and users.

Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service group policy overview

This chapter describes how authentication, privilege elevation, and audit and monitoring services maps the policy settings defined in a Group Policy Object to configuration settings for Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computers and users.

The following topics are covered:

- Mapping settings to a virtual registry
- Configuring settings in administrative templates
- Mapping computer configuration policies
- Mapping user configuration policies
- Editing configuration settings manually
- Reporting group policy settings
- Using standard Windows group policies
- Reporting group policy settings

Use the following links to skip directly to the Centrify Settings group policy descriptions:

- Access control and security settings
- Common UNIX settings
- Linux Settings
- SSH (Secure shell) settings
- Mac OS X Settings
- GNOME settings

Mapping settings to a virtual registry

In the Windows environment, most of the configuration settings defined in a Group Policy Object are implemented through entries in the local Windows registry. For Linux, UNIX, and Mac OS X computers and users, however, local configuration details are typically defined using a set of configuration files stored in the /etc directory. In addition, the Windows, Linux, UNIX, and Mac OS X environments have different configuration requirements, and consequently require different settings to be available through group policy.

To address these differences, Centrify Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service provides its own group policies that allow administrators to use Group Policy Objects to configure settings for Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computers and users. To enable you to use Group Policy Objects to configure settings for Linux-, UNIX-, and Mac OS X-based computers and users, Privileged Access Service:

- Provides its own **administrative templates** (.xml and .admx files) that define Privileged Access Service and Linux-, UNIX-, and Mac OS X-specific configuration settings.
- Uses the `adclnt` daemon to collect configuration details from Active Directory based on the Group Policy Objects applied for the current computer or user and create a **virtual registry** of those configuration settings on the local Linux, UNIX, or Mac OS X computer.
- Runs local programs that map the configuration details in the virtual registry to the appropriate configuration file changes on the local Linux, UNIX, or Mac OS X computer.

The virtual registry is a collection of files that contain **all** of the group policy configuration settings from the group policies applied to the computer through the group policy hierarchy, including settings that apply only to Windows computers. Because the files that make up this virtual registry are not native to the Linux, UNIX, or Mac OS X environment, Privileged Access Service then uses a set of **mapping programs** to read the files, determine the settings that are applicable to Linux, UNIX, or Mac OS X computers and users, and make the appropriate changes in the corresponding Linux, UNIX, or Mac OS X configuration files to implement the configuration specified. The mapping programs ignore any Windows-specific settings that have been applied and only map the settings that are appropriate for the Linux, UNIX, or Mac OS X environment.

Note The virtual registry only supports the group policies that are implemented through registry settings. Group policies that are implemented in other ways, for example, by running an executable script on each computer, aren't supported.

The following figure provides a simplified view of the process.

As this figure suggests, the Privileged Access Service daemon, `adclnt`, retrieves policy settings from the Active Directory domain controller and starts the program `runmappers` (`/usr/share/centrifydc/mappers/runmappers`). The `runmappers` program runs the individual mapping programs that are stored in the `/usr/share/centrifydc/mappers/machine` and `/usr/share/centrifydc/mappers/user` directories. Those individual mapping programs read settings from the virtual registry and write them as the appropriate settings in application-specific configuration files.

The individual mapping programs also keep track of local changes that conflict with group policy settings, so those changes can be restored if the computer is removed from the domain, or if the configuration setting is removed from a Group Policy Object.

Configuring settings in administrative templates

Privileged Access Service administrative templates are stored as files with the `.xml` or `.admx` extension in the system volume and are used to define a specific set of configuration options. For most of the configuration settings

that apply to Linux, UNIX, or Mac OS X users or computers you must use Privileged Access Service group policy administrative templates. To apply a group policy setting, you must add the template that defines the group policy to a Group Policy Object; see [Adding Centrify policies from XML files](#).

In addition, every Group Policy Object includes a default set of Administrative Templates. The default administrative templates provide configuration options for Windows users and computers. In a few cases, however, settings you can configure in the default administrative templates do apply to Centrify Privileged Access Service-managed computers and users. For information about Windows settings that can be applied to Linux, UNIX, and Mac OS X users and computers, see [Using standard Windows group policies](#).

Mapping computer configuration policies

The Centrify agent, `adclient`, determines the group policies that apply to Centrify-managed computers using the same rules for inheritance and hierarchy that apply to Windows computers. When the Linux, UNIX, or Mac OS X computer starts or when the computer policies are refreshed, `adclient`:

- Contacts Active Directory.
- Checks for the Group Policy Objects that are linked to each organizational unit of which the local computer is a member.
- Determines all of the configuration settings that apply to the local computer, and retrieves those settings from the System Volume (SYSVOL).
- Writes all of the configuration settings to a virtual registry on the local computer.
- Starts the `runmappers` program to initiate the mapping of configuration settings using individual mapping programs for computer policies.

The mapping programs in the `/usr/share/centrifydc/mappers/machine` directory then read the virtual registry for the appropriate Linux-, UNIX-, or Mac OS X-specific computer configuration settings and locate the appropriate configuration files to change, then modify those files accordingly.

After the computer starts, the `adclient` daemon will periodically check with Active Directory to determine the current group policy settings for the computer unless you disable group policy updates.

Mapping user configuration policies

The `adcli` daemon determines the group policies that apply to Linux, UNIX, or Mac OS X users using the same rules for inheritance and hierarchy that apply to Windows users. When a user logs into an agent-managed computer, the `adcli` process detects the log-in and does the following:

- Contacts Active Directory.
- Checks for the Group Policy Objects that are linked to each organizational unit the user is a member of.
- Determines all of the configuration settings that apply to the user account, and retrieves those settings from the System Volume (SYSVOL).
- Writes all of the configuration settings to a virtual registry on the local computer.
- Starts the `runmappers` program to initiate the mapping of configuration settings using individual mapping programs for user policies.

The mapping programs in the `/usr/share/centrifydc/mappers/user` directory then read the virtual registry for the appropriate Linux-, UNIX-, or Mac OS X-specific user configuration settings and locate the appropriate configuration files to change, then modify those files accordingly.

After the user has logged on, the `adcli` daemon will periodically check with Active Directory to determine the current group policy settings for the user unless you disable group policy updates.

Editing configuration settings manually

Many of the Privileged Access Service group policies are used to modify the parameter values in the Privileged Access Service configuration file `/etc/centrifydc/centrifydc.conf`. When you make changes to a group policy setting, the change is reflected in the `/etc/centrifydc/centrifydc.conf` file on each joined Linux, UNIX, or Mac OS X computer after the following events:

- The computer is rebooted
- The computer configuration policies are refreshed at the next update

interval

- You run the `adgpupdate` command

If you enable Privileged Access Service group policies, you do not need to manually edit the configuration parameters in the `/etc/centrifydc/centrifydc.conf` file. In some rare cases, however, you may find it useful to customize these parameters on a particular computer. For example, you can use configuration parameters to temporarily disable group policies for users, computers, or both, on a computer.

For more information about customizing Privileged Access Service behavior using the Privileged Access Service configuration files and configuration parameters instead of group policies, see the *Configuration and Tuning Reference Guide*.

Updating configuration policies manually

Although there are Windows group policy settings that control whether group policies should be refreshed in the background at a set interval, Privileged Access Service also provides a UNIX command line program, `adgpupdate`, to manually refresh group policy settings at any time. With this command, you can specify whether you want to refresh computer configuration policies, user configuration policies, or both.

When you run `adgpupdate`, the `adclient` process does the following:

- Contacts Active Directory for computer configuration policies, user configuration policies, or both. By default, `adclient` collects both computer and user configuration policies.
- Determines all of the configuration settings that apply to the computer, the current user, or both, and retrieves those settings from the System Volume (SYSVOL).
- Writes all of the configuration settings to a virtual registry on the local computer.
- Starts the `runmappers` program to initiate the mapping of configuration settings using individual mapping programs for user and computer policies.
- Resets the clock for the next refresh interval.

• • • • •

For more information about using the `adgpupdate` command, see the `adgpupdate man` page.

Using standard Windows group policies

Every Group Policy Object includes default administrative templates for user and computer configuration. Most of the settings in the default administrative templates only apply to Windows computers and Windows user accounts. However, there are a few of these common Windows configuration settings that can be applied to Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computers and users. These configuration options are not duplicated in Privileged Access Service administrative templates.

You can set the following standard Windows group policy options for Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computers and users:

Select this Windows object	To set this policy
Computer Configuration > Policies > Administrative Templates > System > Group Policy	<ul style="list-style-type: none">■ Turn off background refresh of Group Policy■ Group Policy refresh interval for computers
Computer Configuration > Policies > Administrative Templates > System > Windows Time Service > Time Providers	<ul style="list-style-type: none">■ Global Configuration Settings - MaxPollInterval■ Enable Windows NTP Client <p>This policy specifies that <code>adcli</code> poll the domain NTP server to synchronize the clock of the local computer.</p> <p>This policy modifies the <code>adcli.sntp.enabled</code> parameter in the <code>centrifydc.conf</code> configuration file.</p> <p>If you disable this policy, <code>adcli</code> does not attempt to synchronize the computer with the domain NTP server. The computer uses the local NTP policies, as defined in <code>ntp.conf</code>.</p> <p>Whether you enable the policy or not, no settings</p>

Select this Windows object	To set this policy
	are changed in the <code>ntp.conf</code> file.
Computer Configuration > Policies > Administrative Templates > Windows Components > Smart Card > Allow certificates with no extended key usage certificate attribute	<ul style="list-style-type: none"> ■ Allow sctool to obtain Kerberos credentials even though the certificate does not have the extended key usage attribute.
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options	<ul style="list-style-type: none"> ■ Interactive logon: Message text for users attempting to log on ■ Interactive logon: Prompt user to change password before expiration
Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy	<ul style="list-style-type: none"> ■ Enforce password history ■ Maximum password age ■ Minimum password age ■ Minimum password length ■ Password must meet complexity requirements ■ Store passwords using reversible encryption
Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities	<ul style="list-style-type: none"> ■ Specifies the trusted root CA certificate to use
User Configuration > Policies > Administrative Templates > System > Group Policy	<ul style="list-style-type: none"> ■ Group Policy refresh interval for users

Reporting group policy settings

On Windows computers, you can use the optional Group Policy Management Console to see the results of group policy settings for a specific computer or user, including Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computers and users.

• • • • •

You can also review the results of group policy settings for a Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed computer or a specific user by viewing the `gp.report` file locally on the computer. This report is automatically updated at each group policy update interval. By default, the `gp.report` for computer configuration is located in the `/var/centrifydc/reg/machine` directory and the `gp.report` for user configuration is located in the `/var/centrifydc/reg/users/username` directory.

Adding Centrify settings to Group Policies Objects

This chapter describes how to add Centrify-specific group policies to a Group Policy Object and how to set policies for Centrify-managed computers and users.

The following topics are covered:

- Adding administrative templates to a Group Policy Object
- Linking a Group Policy Object to an organizational unit
- Adding Centrify policies from XML files
- Enabling Centrify policies
- Centrify policy limitations

Adding administrative templates to a Group Policy Object

A Group Policy Object (GPO) consists of configuration information that applies to computers, configuration information that applies to users, or sections of policy specifically devoted to each. You can extend the configuration options provided by any Group Policy Object by adding Centrify-provided or custom administrative templates to the object. For example, you can add configuration settings for Centrify agents to a Group Policy Object by adding the `centrifydc_settings.xml` administrative template. Other administrative templates can be added to control other settings, such as Mac OS X system preferences, if they apply to your environment.

Installing Centrify group policy templates

When you install Access Manager using the installation wizard and you specify that all components be installed, the Centrify group policy templates are included in the installation. See “Install Access Manager and update Active Directory” in the *Administrator’s Guide for Windows* for details about using the Access Manager installation wizard.

Note For details about where the Centrify group policy templates reside after they are installed, see [Adding Centrify policies from XML files](#).

Because Centrify group policy templates and extensions are packaged separately from other Access Manager components, you have the following options if you prefer to install group policy templates and extensions separately from Access Manager:

- You can install Centrify group policy templates and extensions on any Windows domain computer without also installing Access Manager on the computer.
- You can install Access Manager on any Windows domain computer without also installing Centrify group policy templates and extensions on the computer.

The group policy template and extension package has its own .exe and .msi installer files, so that you can install group policy templates and extensions interactively through an installation wizard (by executing the .exe file) or silently from the command line (by executing the .msi file). Additionally, you can select or de-select the group policy template and extension component for installation when you run the Access Manager installation wizard.

For details about installing group policy templates and extensions separately from Access Manager, see “Install group policy extensions separately from Access Manager” in the *Administrator’s Guide for Windows*.

Template file formats

Centrify provides templates in both XML and ADMX format. In most cases, it is best to use the XML templates, which provide greater flexibility, such as the ability to edit settings after setting them initially, and in many cases contain validation scripts for the policies implemented in the template.

However, in certain cases, you may want to add templates by using the ADMX files. For example, if you have implemented a set of custom tools for the Windows ADMX-based policies, and want to extend those tools to work with the Centrify policies, you can implement the Centrify policies by adding the ADMX template files. You should note, however, that ADMX templates do not support extended ASCII code for locales that require double-byte characters. For these locales, you should use the XML templates.

Selecting a Group Policy Object for Centrify settings

Depending on the requirements of your organization and how you have linked existing Group Policy Objects to sites, domains, and organizational units in your Active Directory forest, you might want to use one of the default Group Policy Objects, use a Group Policy Object you have created specifically for your organization, or create a new Group Policy Object that is specifically for Centrify settings.

If you have created an organizational structure for Centrify objects as described in the *Planning and Deployment Guide*, creating a new Group Policy Object specifically for Centrify policies gives you the most flexibility and control over the configuration settings for managed computers and the operation of Centrify software. In deciding whether to create a new Group Policy Object or use an existing Group Policy Object, you should consider where policies should be applied. You can link Group Policy Objects to sites, domains, or organizational units to control the scope of the policies you set.

If you prefer to minimize the number of Group Policy Objects you deploy, you can add Centrify settings to one of default Group Policy Objects that are installed on the Windows domain controller:

- Default Domain Controllers Policy
- Default Domain Policy

You can add Centrify settings to any Group Policy Object regardless of whether you have any settings configured or applied to Windows users and computers. Settings that apply to Centrify-managed computers only affect computers where the Centrify agent is installed.

Linking a Group Policy Object to an organizational unit

You can link a Group Policy Object to an organizational unit, domain, or site using the Group Policy Management Console. To set group policies for a selected Active Directory site, domain, or organizational unit, you must have read and write permission to access the system volume of the domain controller and the right to modify the selected directory object.

If you have created an organizational structure for Centrify as described in the *Planning and Deployment Guide*, the most natural place to link a Group Policy Object is the top-level container of that organizational unit structure, for example, the Centrify container.

To create and link a Group Policy Object for Centrify settings:

1. Click **Start > Administrative Tools > Group Policy Management**.
2. Select the Centrify organizational unit, right-click, then select **Create a GPO in this domain, and Link it here**.
3. Type a name for the new Group Policy Object, for example, `Centrify Policy`, then click **OK**.

If you want to apply group policies to lower levels in the organizational structure, you can do so by linking Group Policy Objects to lower level organizational units. For example, if you created a separate organizational unit for zone computers, you can link a Group Policy Object to that organizational unit. However, you cannot link Group Policy Objects to containers (CN).

Using security filtering for group policies

You can use Active Directory security groups and group policy security filtering if you want to restrict the policies applied to subsets of zone computers or users. By creating an Active Directory security group and setting security filtering for a Group Policy Object, you can achieve fine-grain control over where group policies are applied within the Centrify

organizational unit structure. For example, you can create an Active Directory group called europe that has a specific set of computers in it. then restrict the application of group policies to that group.

To enable security filtering of group policies:

1. Create the Active Directory security group with the appropriate members.
2. Open the Group Policy Management Console and select the Group Policy Object for which you want to enable filtering.
3. On the Scope tab, under Security Filtering, click **Add**.
4. Be certain that 'Group' appears in **Select this object type**; if not, Click **Object Types** and select **Groups**.
5. Type all or part of the name for the group you created for filtering, click **Check Names**.
If more than one group is returned, select the appropriate group, then click **OK**.
6. Click **OK** to link the security group to scope of the Group Policy Object.

Adding Centrify policies from XML files

In most cases, you should add Centrify policies from XML templates to the Group Policy Object you are using for Centrify settings. The XML-based format is the current standard for group policy templates.

To add Centrify group policies from Centrify XML templates:

1. Click **Start > Administrative Tools > Group Policy Management**.
2. Expand the appropriate site, domain, or organizational unit to select Group Policy Object you want to use for Centrify policies, right-click, then click **Edit**.
For example, expand the top-level Centrify organizational unit to select the Centrify Policy object, right-click, then click **Edit**.
3. In the Group Policy Management Editor, expand Computer Configuration and Policies.
4. Select Centrify Settings, right-click, then click **Add/Remove Templates**.
5. In the Add/Remove Templates dialog box, click **Add**.
6. In most cases, the directory with the templates is already selected and the following Centrify templates are listed:

- centrify_gnome_settings
- centrify_linux_settings
- centrify_mac_settings
- centrify_unix_settings
- centrifydc_fips
- centrifydc_settings
- centrifyds_settings

If the templates are not listed, navigate to the group policy directory under the Access Manager installation directory. For example, if you installed files in the default location, navigate to the following directory:

```
C:\Program Files\Common Files\Centrify Shared\Group
Policy Management Editor Extension\policy
```

If you want to add templates for auditing, navigate to the Centrify Auditing and Monitoring Service installation directory. For example, if you installed files in the default location, navigate to the following directory:

```
C:\Program Files\Centrify\Audit\AuditManager
```

7. Select the Centrify templates you want to use, then click **Open**.
8. In the Add/Remove Templates dialog box, click **OK** to add the new templates.

Group policies for access control and privilege management are listed under **Centrify Settings**. You can expand this node and the categories below it to explore the group policies available.

Group policies for auditing are listed under **Centrify Audit Settings**. You can expand this node and the categories below it to explore the group policies available.

By default, all group policies are set to “Not configured.”

Adding templates after an upgrade

To make any new policies available after you upgrade Centrify software, you must add new versions of the templates you use after you upgrade the Access Manager or the auditing console. To add new versions of the templates after an upgrade, repeat [Linking a Group Policy Object to an organizational unit](#) to [Adding Centrify policies from XML files](#). If you see the message, The selected XML file already exists. Do you want to overwrite it?, click **Yes** to overwrite the old template file with the new template and make any new or modified group policies available. Overwriting the template does not affect any configuration settings that have been applied. Policies that you have enabled remain enabled.

Enabling Centrify policies

By default, all group policies, including Centrify group policies are set to Not configured. You can selectively enable the specific computer and user policies you want to use. Most of the Centrify group policies set configuration parameters on managed computers. If you choose to enable any of these

group policies, you should be familiar with the corresponding configuration parameters described in the *Configuration and Tuning Reference Guide*.

To enable and configure Centrify settings:

1. Open the Group Policy Management console.
2. Select the Group Policy Object to which you have added Centrify policies, right-click, then select **Edit**.
3. Expand **Computer Configuration > Policies > Centrify Settings**.
4. Select a policy name, right-click, then select **Properties**.
5. Click **Enabled**.

Depending on the policy, you might need to select values or provide other information to complete the configuration. For more information about the policy and how to set configuration options, click the **Explain** tab. For information about limitations to the values that you specify, see [Centrify policy limitations](#) later in this chapter.

6. Click **Apply** after making the change.

The policies you enable are applied when computers in the site, domain, or organizational units are rebooted, users next log on, or at the next update interval.

Centrify policy limitations

Some Centrify group policies allow you to select values from a list when you enable the group policy. Depending on how the list is configured, in some cases you cannot select more than 999 items from the list.

For example, if you enable the **Specify AD users allowed in Auto Zone** group policy, you are prompted to specify the names of AD users. You can specify AD user names by typing them, by specifying a file containing a predefined list of user names, or by selecting them from the list of all AD users. Because of the way in which the AD user list is configured, you cannot select more than 999 users from it. If you attempt to select more than 999 users, the following message is displayed:

```
Please enter 0 to 999 entries for User
```


• • • • •

This limitation applies to several other group policies in addition to **Specify AD users allowed in Auto Zone**.

It is generally not advisable to select 1000 or more items from a list to define a data set in a group policy. Instead, whenever possible you should use groups or a file containing a predefined list of items to define a large data set.

DirectControl Settings

The following table summarizes the group policies listed directly under **DirectControl Settings**. The full descriptions follow the table.

Select this group policy	To do this
Add centrifydc.conf properties	Add configuration parameters to <code>centrifydc.conf</code> configuration file.
Maintain DirectControl 2.x compatibility	Maintain access for legacy users or computers.
Merge local group membership	Merge local group membership from <code>/etc/group</code> into the zone group membership for groups that have the same name and GID.
Prefer authentication credentials source	Instruct <code>adcli</code> to authenticate the user using the cached credentials.
Set LDAP fetch count	Specify the number of objects to obtain in a single LDAP request.
Set password cache	Control the caching of user passwords.
Set user mapping	Map a local user account to an Active Directory account.
Use FIPS 140-2 compliance algorithms	Select the algorithms used for the authentication protocols.

Additional group policies for DirectControl Settings are organized under the following sub-nodes:

- [Account prevalidation](#)—Contains policies to manage prevalidation of users and groups for disconnected systems.
- [Adclient settings](#)—Contains policies to control certain aspects of the operation of the agent on managed computers.
- [Auto Zone group policies](#)—Contains policies to control certain aspects of the operation of the agent on machines that are joined to Auto Zone.
- [Dzdo settings](#)—Contains policies to control certain aspects of the operation of `dzdo` and `sudo`.

- **Group policy settings**—Contains policies to manage the execution of the Centrify group policy mapping programs.
- **Kerberos settings**—Contains policies to manage the Kerberos configuration. You can use these settings to control updates to the Kerberos configuration files and credential renewal.
- **Local account management settings**—Contains policies to control agent management of local users and groups.
- **Logging settings**—Contains policies to control logging policy settings. You can use these settings to specify the `syslog` facility to use for logging different `adclient` processes and to control the amount of memory to use to queue log messages.
- **Login settings**—Contains policies to control login and local account access. You can use these settings to grant or deny access to specific users and groups or to ignore Active Directory authentication for some users and groups.
- **MFA Settings**—Contains policies for configuring multi-factor authentication in classic zones and Auto Zones. You can use these settings to specify which users or groups require a two-step authentication procedure for login, define rescue users that can log in when multi-factor authentication is unavailable, and to specify a cloud URL to be used in multi-factor authentication.
- **Network and cache settings**—Contains policies to specify the maximum period for client connection time-outs and object expiration intervals. You can use these settings to determine how long to wait for a response when connecting to Active Directory and how long objects should be kept in the local cache.
- **NIS daemon settings**—Contains policies to control operation of the Centrify Network Information Service (`adnisd`) on the local host computer. The `adnisd` service provides a mechanism for the Centrify agent to respond to NIS client requests from other computers not managed by Centrify software.
- **NSS overrides**—Contains policies to specify the `passwd` or `group` override entries you want to use in place of the entries in the local `/etc/passwd` or `/etc/group` files. You can use these settings to provide fine-grain control of the users and groups who can use the computer and to

override the user ID, group ID, default shell, or home directory for specific login accounts or groups.

- **PAM settings**—Contains policies to customize the behavior of the Centrify PAM module.
- **Password prompts**—Contains policies to customize the prompts displayed when Active Directory users are prompted to provide their password. You can use these settings to change the text displayed when Active Directory users log in or change their password.
- **Sudo settings**—Contains policies to control certain aspects of the operation of sudo.
- **User's initial group ID**—Contains policies to control group numbers. You can use this setting to specify the default group identifier for new users.

Add centrifydc.conf properties

Use the **Add centrifydc.conf properties** group policy to add configuration parameters to the agent configuration file. Although you can set many configuration parameters and values by using the associated group policy, not all configuration parameters have an associated group policy. The **Add centrifydc.conf properties** group policy enables you to specify any configuration parameter and its value.

See the *Configuration and Tuning Reference Guide* for a list of all configuration parameters.

To use this group policy, select **Enabled**, then click **Add**. Enter a property name and property value. For example, to change the adnisd update interval to 10 minutes:

Property name: nisd.update.rate

Property value: 600

Be careful when adding parameters because there is no error checking. If you enter a non-existent property name or invalid value, the parameter and value will be added to the configuration file as-is. An invalid parameter name will simply be ignored but an invalid value could cause configuration problems.

Enable Active Directory PAM Privilege Escalation Feature

Use the **Enable Active Directory PAM Privilege Escalation Feature** group policy to specify if the Microsoft Privileged Access Management (PAM) Privilege Escalation feature is supported or not within the Centrify environment.

If this policy is Enabled, then, when an Active Directory user logs in, the configured privilege that's granted to the user through PAMGroup takes effect until the granted period has elapsed.

The Microsoft PAM Privilege Escalation feature specifies if Centrify DirectControl uses Microsoft PAM Privilege Escalation feature in the computer.

This group policy modifies the `microsoft.pam.privilege.escalation.enabled` setting in the agent configuration file.

Maintain DirectControl 2.x compatibility

Use the **Maintain DirectControl 2.x compatibility** group policy if you have legacy users or computers who were given access using the console, version 2.x.x.

If all of your Active Directory users are enabled for Linux, UNIX, or Mac OS X access using the console, version 3.0 or later, you should leave this policy as not configured.

This group policy modifies the `adclient.version2.compatible` setting in the agent configuration file.

Merge local group membership

Use the **Merge local group membership** policy to determine whether to merge local group membership from the `/etc/group` file into the zone group membership for groups that have the same name and GID. For example, if the agent retrieves the membership list of kwan, emily, and sam for the group profile with the group name `performx1` and GID 92531 from Active Directory and there is also a local group named `performx1` with the GID 92531 with

• • • • •

users wilson and jae, the merged group would include all five members (kwan, emily, sam, wilson, jae).

This group policy modifies the `adclient.local.group.merge` setting in the agent configuration file. By default, the parameter associated with this policy is set to `false` to prevent unexpected results.

Be careful when enabling this policy, because it violates normal NSS behavior and, therefore, may have unexpected side effects. You should analyze your environment carefully, and determine that you can safely merge local and Active Directory group profiles before enabling this policy.

Prefer authentication credentials source

Use the **Prefer Authentication against cached credentials** policy to authenticate the user using the cached credentials first, regardless of the current connectivity state with the Active Directory domain controller.

By default, the parameter associated with this policy is set to `false`. You can enable this policy to reduce traffic on slow networks. However, if the Active Directory credentials are not synchronized with the cached credentials, you run the risk of undesired side effects when the computer is online.

This group policy modifies settings in the agent configuration file. For more information about the configuration file and this configuration settings, see `adclient.prefer.cache.validation`.

Set LDAP fetch count

Use the **Set LDAP fetch count** group policy to specify the number of objects to obtain in a single LDAP request. You can use this group policy to optimize the number of objects to suit your environment.

If you select **Enabled** for this group policy, you can then set the number of objects to obtain in a single LDAP request by balancing speed and memory usage against network bandwidth and latency. As you increase the number of objects included in an LDAP request, you may improve the overall performance by decreasing the number of connections to Active Directory and reducing the overall demand on the server, but you increase the RAM used by the agent. If you decrease the number of objects included in an LDAP

request, you may reduce overall performance because of the additional network traffic, but decrease the memory used by the agent.

On faster networks, you can safely retrieve a small number of objects. On slower networks or when retrieving information for large groups (for example, groups with more than 1000 users), you may want to increase the value for this parameter.

This group policy modifies the `adclient.fetch.object.count` setting in the agent configuration file.

Set password cache

Use the **Set password cache** group policy to control the handling of user passwords. By default, the Centrify agent stores a UNIX-style MD5 hash of each user's password in the cache when the user is authenticated during login. Storing the password hash allows previously authenticated users to log on when the computer is disconnected from the network or Active Directory is unavailable.

If you select **Enabled** for this group policy, you can set the following options:

- **Allow Password storage** Allow specified users to have their password hash stored in the cache. If you set this option and specify a list of users, only those users can log on when the computer is disconnected from the network or Active Directory is unavailable. To list the specific users allowed to have their password hash stored, type the user names separated by commas or spaces, or click **List**, then **Add** to browse and select Active Directory users to add.

This option modifies the `adclient.hash.allow` parameter in the agent configuration file. By default, all users have their password hash stored.

- **Deny Password storage** Prevent specified users from having their password hash stored. If you set this option and specify a list of users, only those users are prevented from logging on when the computer is disconnected from the network or Active Directory is unavailable. To list the specific users who should not have their password hash stored, type the user names separated by commas or spaces, or click **List**, then **Add** to browse and select Active Directory users to add. This setting overrides "Allow Password storage".

This option modifies the `adclient.hash.deny` parameter in the `centrifdc.conf` agent configuration file. By default, all users have their password hash stored.

- **Cache life** Specify the number of days a password hash for any user can be stored in the cache before it expires. A value of zero (0) specifies that the password hash should never expire. When you enable this policy, a value of 7 (days) appears in the field. You can accept this value or enter a different value up to 9999.

This option setting modifies the `adclient.hash.expires` parameter in the `centrifdc.conf` agent configuration file. The default setting for this parameter is 0, which means that by default, the cache does not expire.

For more information about the configuration file and these configuration settings, see `adclient.hash.allow`, `adclient.hash.deny`, and `adclient.hash.expires` in the *Configuration and Tuning Reference Guide*.

Set user mapping

Use the **Set user mapping** group policy to map a local Linux, UNIX, or Mac OS X user account to an Active Directory account. Local user mapping allows you to set password policies in Active Directory even when a local Linux, UNIX, or Mac OS X account is used to log in. This group policy is most commonly used to map local system or application user accounts on a computer to a different Active Directory account and password, so that you can enforce password complexity rules for the account, but it can be used for any local user account.

When you select **Enabled** for the Set user mapping group policy, you can then click **Show** to add or remove user accounts.

To add mapped user accounts to the policy, click **Add**. You can then type the Linux, UNIX, or Mac OS X user account name in the first field and the Active Directory account name to which you want to map the local account in the second field, then click **OK**.

Once this policy is applied, users or services attempting to log in with the local mapped account must provide the Active Directory password for the account. For example, if you have mapped the local user `caïne` to an Active Directory account that uses the password `+shark1`, the user logging in with the `caïne` user name must provide the `+shark1` password or authentication will fail. For more information about mapping local Linux, UNIX, or Mac OS X accounts to

• • • • •

Active Directory accounts, see the *Administrator's Guide for Linux and UNIX* or the *Administrator's Guide for Mac*.

User's initial group ID

Use the group policy under **User's Initial Group ID** to specify the default group identifier (GID) to use for new users when you run the `adupdate user add` command.

Use FIPS 140-2 compliance algorithms

Use the **FIPS compliant algorithms for encryption, hashing and signing** group policy to specify the use of FIPS 140-2-compliant cryptographic algorithms for authentication protocols.

Basic requirements

Centrify supports FIPS 140-2 compliance for authentication using Kerberos and NTLM with the following requirements and caveats:

- FIPS mode is available on agent version 5.0.2 or later but only on supported operating systems. See the [NIST validation entry for the Centrify FIPS mode](#) for the current list of supported platforms.
- Domain controllers must be at Windows Server 2008 domain functional level, or later.
- The administrator must explicitly add the `centrifydc_fips.xml` or directly edit the administrative template to enable this policy.

Note Centrify recommends that you use the `centrifydc_fips.xml` template. When you do, the agent performs several checks before implementing the policy to confirm that your domain controller and joined computers meet the requirements.

- If multiple encryption types are specified only the AES128-CTS and AES256-CTS encryption type keys (with RSA for public key generation, DSA for digital signature generation and SHA1, SHA256, SHA384 or SHA512 for hashing) are generated and saved to the keytab file. However, if arcfour-hmac-md5 encryption is specified, the MD4Hash of the machine password will be generated and saved to the keytab file.

Note Which encryption types are used in each joined computer is controlled by a parameter set in each Linux, UNIX, or Mac OS X computer's configuration file. See the [adclinet.krb5.permitted.encryption.types](#) description in the Notes section on [Related configuration parameters](#) for an explanation.

- Inter-realm keys for the AES128-CTS or AES256-CTS encryption types must be established between any trusted domains to enable Active Directory users to log on to a joined computer (see the ksetup utility to set up inter-realm keys).
- FIPS mode only allows NTLM pass-through authentication over SChannel. FIPS mode is not available for NTLM authentication over SMB or SMB2.
- In some environments, offline multi-factor authentication is not compatible with FIPS mode. See the *Multi-factor Authentication Quick Start Guide* for details about this restriction.

Enabling the policy

To enforce FIPS 140-2 compliance, select the Computer Configuration > Policies > Centrify Settings > DirectControl Settings > **Use FIPS compliant algorithms for encryption, hashing, and signing** policy, open the properties, and select **Enabled**.

The policy takes effect after the next group policy update.

When you use the XML group policy template, the agent performs the following validation checks:

- It verifies that each joined computer is running a supported operating system.
- It verifies that each machine is joined to a domain at domain functional level 2008 or above. If the domain does not meet the domain functional level requirements, the agent issues the following warning:
FIPS mode is supported only on domain with 2008 domain functional level or up.

Enabling this policy with lower domain functional level may prevent adclient from working properly. Are you sure you want to enable this policy?

Respond Yes to enable the policy regardless or No to abort. However, if the current domain functional level is inadequate or FIPS mode is not supported on the host platform, the agent does not restart when the policy is applied.

For all joined computers that pass, the agent is automatically stopped and restarted. After a successful restart, the `adjoin`, `adleave`, and `adinfo` commands run in FIPS mode immediately. If a joined computer is running an unsupported platform, the computer's configuration file is not updated and the agent is not restarted.

There are several restrictions and rules governing the use of FIPS mode. The following bullets summarize the policy:

- Pre-validated groups and users that use FIPS mode to log on when disconnected must have each user's Active Directory `msDS-SupportedEncryptionTypes` attribute set to use Kerberos AES 128- or 256-bit encryption. You can set this attribute in the users' accounts using Active Directory Users and Computers or ADSI Edit.
- The value of the corresponding Windows policy to use FIPS compliant algorithms has no effect on the Windows, Linux, UNIX, or Mac OS X computers managed through the Centrify agent. You must use the Centrify policy to enable FIPS mode. The Centrify policy is only available when you add the `centrifydc_fips.xml` or `centrifydc_fips.admx` template (see [Adding Centrify policies from XML files](#)).

Related configuration parameters

The following `centrifydc.conf` configuration parameters affect FIPS operation. See the *Configuration and Tuning Reference Guide* for details about these parameters.

- `fips.mode.enable`: Enable FIPS mode on a per-computer basis. This group policy modifies the `fips.mode.enable` parameter in `centrifydc.conf`.
- `adclient.krb5.clean.nonfips.encryptypes`: If FIPS mode is enabled and this configuration parameter is set to `true`, `adclient` scans the computer's keytab file and removes all non-AES encryption keys for service principal names (SPNs) during startup. The default is `false`.
- `adclient.krb5.permitted.encryption.types`: If FIPS mode is enabled, and if you include the `arcfour-hmac-md5` encryption type in this configuration parameter, and if `adclient.krb5.clean.nonfips.encryptypes` is `true`, `adclient` generates the MD4 hash for the computer password and saves it in the keytab file.

Account prevalidation

Prevalidation enables specific users or the members of a specific group to access a Centrify-managed computer using their Active Directory credentials even if the following conditions would normally prevent them from logging on:

- The computer is disconnected from the network and unable to contact Active Directory to authenticate their identity.
- The user has not previously logged onto the computer.

Without prevalidation, only users who have previously logged on and had their password hashes stored in the local cache can be authenticated when the computer is disconnected from the network.

You can use the **Account Prevalidation** group policies to manage the users and groups who are authorized or denied access to disconnected computers.

Use the following group policies specify the users and groups that can be prevalidated:

- [Specify allowed groups for prevalidation](#)
- [Specify allowed users for prevalidation](#)

Use the following group policies specify the users and groups that cannot be prevalidated:

- [Specify denied groups for prevalidation](#)
- [Specify denied users for prevalidation](#)

Use the following group policies specify other prevalidation settings:

- [Set prevalidation service name](#)
- [Set prevalidation update interval](#)

Specify allowed groups for prevalidation

Enable this policy and enter a comma-separated list of groups to prevalidate users in the specified groups for access Centrify-managed computers. To

• • • • •

allow prevalidation for all users in the zone without any exceptions, you can enter `all@zone` in **Specify allowed groups for prevalidation**.

This group policy modifies the following setting in the agent configuration file:

```
adclient.prevalidate.allow.groups
```

Specify allowed users for prevalidation

Enable this policy and enter a comma-separated list of users to prevalidate specific users for access Centrify-managed computers. This group policy modifies the following setting in the agent configuration file:

```
adclient.prevalidate.allow.users
```

Specify denied groups for prevalidation

Enable this policy and enter a comma-separated list of groups that cannot be prevalidated for access Centrify-managed computers. If you allow any groups or users to be prevalidated, you can use this policy to define exceptions for any groups that should be prevented from prevalidation.

In most cases, you would use this policy to exclude a subset of users that are in a group that is a member of an allowed group. For example, you might want allow all users in the `admins` group to be prevalidated, except the users who are members of the nested `outsource` subgroup. To accomplish this, you would enable “Specify allowed groups for prevalidation” for the `admins` group, then use the “Specify denied groups for prevalidation” policy to deny access to users who are members of the `outsource` group.

This group policy modifies the following setting in the agent configuration file:

```
adclient.prevalidate.deny.groups
```

Specify denied users for prevalidation

Enable this policy and enter a comma-separated list of users to prevent prevalidation of specific users for access Centrify-managed computers. If you allow any groups or users to be prevalidated, you can use this policy to define exceptions for any users who should be prevented from prevalidation. In

• • • • •

most cases, you would use this policy to exclude a subset of users that are members of an allowed group.

This group policy modifies the following setting in the agent configuration file:

```
adclient.prevalidate.deny.users
```

Set prevalidation service name

Enable this policy to specify the service name to use for prevalidated users and groups. You must use the name you specify in this parameter when you register the Service Principal Name (SPN) for a user or group with the `setspn.exe` utility. The default value is `preval`.

Setting the service principal name for a user

For users or groups of users to be prevalidated, their accounts must be active accounts with permission to log on to the local computer and have a Service Principal Name (SPN) set in the form of:

```
preval/user
```

Where `preval` is the service name specified by the `adclient.prevalidate.service` parameter and `username` is the user logon name, which can be either of the following:

- the name part of the user's UPN, if the domain part matches the user's domain
- `SAMAccountName`, if the UPN is empty or the UPN's domain part is different from the user's domain

To enable prevalidation for a user, you can use the Windows `setspn.exe` utility to add a Service Principal Name for the user. For example, to register the Service Principal Name for the user `kai@arcade.com` using `preval` as the service name, you could type a command similar to the following in a Windows Command Prompt window:

```
setspn -A preval/kai kai
```

This `setspn` command registers the SPN in Active Directory for the `preval` service and the specified user account, for the Active Directory user `kai`. On the computers where this user is allowed to be prevalidated, the user can be authenticated without having logged on previously.

Setting the service principal name for group members

If you are allowing prevalidation for an administrative group, you must register a Service Principal Name for each member of the group. For example, if you are allowing prevalidation for the `admins` group and this group has five members, you would use the `setspn.exe` utility to register a Service Principal Name for each of those members.

Set prevalidation update interval

Enable this policy to specify the interval, in hours, for refreshing the credentials for prevalidated user and group accounts. The credentials for prevalidated users must be periodically refreshed to ensure they are in sync with Active Directory and that prevalidation will continue working after password changes.

The parameter value should be a positive integer. A value of 0 disables all prevalidation of users. The default is 8 hours.

This group policy modifies the `adclient.prevalidate.interval` setting in the agent configuration file.

Refreshing prevalidated credentials

Prevalidated credentials are periodically refreshed at the interval defined by the Set prevalidation update interval policy to ensure that prevalidation will continue working after password changes. In addition, the credentials for prevalidated users and groups are periodically retrieved from Active Directory whenever you do the following:

- Reboot the local computer.
- Start or restart the agent (`adclient`).
- Run the `adflush` command to clear the cache.
- Change a password from the local system.

Adclient settings

Use the group policies under **Adclient Settings** to control the operation of the agent on managed computers.

Some of these policies are platform-specific policies that control whether the agent can automatically edit specific files on the local computer. In most cases, you should enable the policies that allow the agent to maintain configuration files automatically.

If you choose to not enable any of the platform-specific policies, you must manually edit the appropriate configuration files on individual computers. For example, if not configuring files automatically through a group policy, you must manually edit the `/etc/nsswitch.conf` and `/etc/pam.d/system-auth` or `/etc/pam.d` files to include `adclient` information or authentication through Active Directory will fail and you may disable login access entirely. For more information about updating configuration files manually, see “Customizing adclient configuration parameters” in the *Configuration and Tuning Reference Guide*.

Note Several Auto Zone group policies are located within the **Adclient Settings** node. For details about Auto Zone group policies, see [Auto Zone group policies](#).

Add attributes to cached objects

Use the following group policies to add specified Active Directory attributes to the local cache:

- Add attributes to cached user objects
- Add attributes to cached group objects
- Add attributes to cached computer objects

You can use the `adquery --dump` command to see which attributes are cached by default.

These policies modify the following parameters in the `centrifdc.conf` configuration file:

```
adclient.custom.attributes.user
```

.....

adclient.custom.attributes.group

adclient.custom.attributes.computer

Auto Zone group policies

Use the **Auto Zone** group policies under **Adclient Settings** to set configuration parameters for all managed computers in the Auto Zone at once rather than configuring parameters for computers individually.

The Auto Zone group policies are defined in the `centrifdc_settings.xml` template file. These group policies and parameters have no effect on computers not joined to Auto Zone.

Auto Zone default shell

Set the default shell when joined to Auto Zone. The default value is:

- `/bin/bash` on Mac OS X and Linux computers
- `/bin/sh` on UNIX systems, including Solaris, HP-UX, and AIX

This group policy modifies the `auto.schema.shell` parameter in the `centrifdc.conf` configuration file.

Auto Zone domain prefix overrides

Specify a unique prefix for a trusted domain. The Auto Zone algorithm combines the prefix with the lower 22 bits of each user or group relative identifier (RID) to create unique Linux, UNIX, or Mac OS X numeric user (UID) and group (GID) identifiers for each user and group in the forest and in any two-way trusted forests.

Ordinarily, you do not need to set this parameter because Centrify automatically generates the domain prefix from the user or group security identifier (SID). However, in a forest with a large number of domains, domain prefix conflicts are possible. When you join a computer to a domain, if Centrify detects any conflicting domain prefixes, the join fails with a warning message. You can then set a unique prefix for the conflicting domains.

To set this parameter, select **Enabled**, then click **Add**. Type a domain name and type a prefix or use the arrows to set a prefix number. The prefix must be in the range 0 - 511. Click **OK** to enter the prefix and domain. Add as many prefixes as you need, then click **OK** to close the group policy property page.

This group policy modifies the `auto.schema.domain.prefix` parameter in the agent configuration file.

Auto Zone home directory

Specify the default home directory. If you do not enable this policy, the default home directory will be based on the platform as follows:

- Mac OS X: `/Users/{user}`
- Linux, HP-UX, and AIX: `/home/{user}`
- Solaris: `/export/home/{user}`

The variable `{user}` specifies the logon name of the user. For example, if you specify `/Users/{user}` and `jsmith` logs on to the Mac OS X computer, the home directory is set to `/Users/jsmith`.

This group policy modifies the `auto.schema.homedir` parameter in the agent configuration file.

Auto Zone remote file service (Mac OS X)

Specify the type of remote file service to use for the network home directory. The options are: SMB (default) and AFP. This group policy only applies to Mac OS X computers. When you type a path for the network home directory in Active Directory, it requires the format `/server/share/path`, but on Mac OS X computers, the format for mounting a network directory requires the remote file service type as part of the path `/type/server/share/path`. By identifying the remote file-service type, you can type the network path in the format required by Active Directory, and convert the path into the format required by Mac OS X computers.

This group policy modifies the `auto.schema.remote.file.service` parameter in the agent configuration file.

Generate new uid/gid using Apple scheme in Auto Zone

Use the Apple algorithm to automatically generate user and group identifiers. The Apple algorithm for generating identifiers is based on the `objectGuid` attribute for the user or group object. The Centrify mechanism for automatically generating UIDs and GIDs is based on the security identifier for user or group objects. Both methods ensure a globally unique and consistent identifier for the user or group.

This group policy modifies the `auto.schema.apple_scheme` parameter in the agent configuration file.

Set user's primary gid in Auto Zone

Specifies the group identifier (GID) to use as the default primary group for all users. If this policy is not configured, the primary GID for users in Auto Zone is set to one of the following platform-specific values:

- Mac: 20
- Linux, Solaris, HP-UX, AIX: -1

If you enable this group policy, you must specify an integer from -1 to 2147483647. You cannot leave the GID field blank if you enable this group policy.

If you set this group policy to -1, the primary GID is generated according to the selected scheme:

- Apple scheme
- Relative identifier (RID)
- Active Directory value

This group policy modifies the `auto.schema.primary.gid` parameter in the agent configuration file.

Specify AD Groups allowed in Auto Zone

Specify the Active Directory groups that are included in the Auto Zone. By default, all Active Directory groups are included in the Auto Zone. When you enable this policy, only the specified groups are included in the Auto Zone and assigned a GID on the computer.

You can manually enter each group name separated by a comma, or click **List**, then **Add**, to browse for groups to add. If you manually add groups, use one of the following formats:

- SAM account name
- NTLM: DOMAIN\SAMAccountName (also DOMAIN/SAMAccountName)
- UPN or SAMAccountName@domain
- Full DN: CN=commonName, ...,DC=domain_component, DC=domain_

.....

component,...

- Canonical Name : domain.com/container1/cn

You can also specify the groups in a file.

Any groups listed may be domain local, global, or universal security groups. Distribution groups are not supported. If an Active Directory user specified in “Specify AD users allowed in Auto Zone” is a member of a group that is *not* specified in the current group policy, that group is ignored.

This group policy modifies the `auto.schema.groups` parameter in the agent configuration file.

Specify AD Users allowed in Auto Zone

Specify the Active Directory users that are included in the Auto Zone and able to log in using their Active Directory account.

By default, all Active Directory users are included in the Auto Zone. When you enable this policy, only the specified users and members of the groups specified with the [Specify Groups of AD Users allowed in Auto Zone](#) policy are included in the Auto Zone and able to log in using their Active Directory account.

You can manually enter each user name separated by a comma, or click **List**, then **Add**, to browse for users to add. If you manually add users, use one of the following formats:

- SAM account name
- NTLM: DOMAIN\SAMAccountName (also DOMAIN/SAMAccountName)
- UPN or SAMAccountName@domain
- Full DN: CN=commonName, ...,DC=domain_component, DC=domain_component,...
- Canonical Name : domain.com/container1/cn

You can also specify the users in a file.

This group policy modifies the `auto.schema.allow.users` parameter in the agent configuration file.

Specify Groups of AD Users allowed in Auto Zone

Specify the Active Directory users that are included in the Auto Zone by specifying the groups whose members should be included. By default, all

Active Directory users are included in the Auto Zone. When you enable this policy, only the users listed for the [Specify AD Users allowed in Auto Zone](#) policy and members of the listed groups (including members of nested groups under these groups and users' whose primary group are set to these groups) are included in the Auto Zone.

You can manually enter each group name separated by a comma, or click **List**, then **Add**, to browse for groups to add. If you manually add groups, use one of the following formats:

- SAM account name
- NTLM: DOMAIN\SAMAccountName (also DOMAIN/SAMAccountName)
- UPN or sAMAccountName@domain
- Full DN: CN=commonName, ...,DC=domain_component, DC=domain_component,...
- Canonical Name : domain.com/container1/cn

You can also specify the groups in a file.

Any groups listed may be domain local, global, or universal security groups. Distribution groups are not supported.

This policy does not include the group in Active Directory Auto Zone, just the users in that group. This means that the group is *not* automatically assigned a GID. Use the [Specify AD Groups allowed in Auto Zone](#) group policy to include a group in the Auto Zone and assign it a GID.

Auto Zone does not support one-way trusts. Therefore, any users in the group who belong to a domain that has a one-way trust relationship to the joined domain do not become valid users on the computer.

This group policy modifies the `auto.schema.allow.groups` parameter in the agent configuration file.

Configure `/etc/nsswitch.conf` (Solaris, HP-UX, Linux)

Allow automatic editing of the Name Service Switch configuration (`nsswitch.conf`) file on **HP-UX**, **Solaris**, and **Linux** computers. This policy modifies the `adclient.autoedit.nss` setting in the agent configuration file.

Configure /etc/{pam.conf,pam.d} (AIX, Solaris, HP-UX, Linux, Mac OS X)

Allow automatic editing of the PAM configuration (pam.conf file or pam.d directory) on **AIX, HP-UX, Solaris, Linux, and Mac OS X** computers. This policy modifies the `adcli.ent.autoedit.pam` setting in the agent configuration file.

Configure /etc/security/user (AIX)

Allow automatic editing of the LAM user configuration files on **AIX** computers. This policy modifies the `adcli.ent.autoedit.user` setting in the agent configuration file.

Configure /usr/lib/security/methods.cfg (AIX)

Allow automatic editing of the LAM methods.cfg files on **AIX** computers. This policy modifies the `adcli.ent.autoedit.methods` setting in the agent configuration file.

Configure Directory Services (Apple OS/X)

Allow automatic editing of the Directory Service configuration on **Mac OS X** computers. This policy modifies the `adcli.ent.autoedit.dsconfig` setting in the agent configuration file.

Configure dump core setting

Specify whether the agent should be allowed to dump core. The value you set for this group policy overrides the default `u1imit` setting. When you enable this group policy, select one of the following options from the drop down menu:

- never to specify that the agent never dump core.
- once to specify that the agent should dump core only when there is no existing core dump file. Note that this setting is not valid on Mac OS X

computers. On Mac OS X, once behaves the same as always, which dumps core on every crash.

- always to specify that the agent dump core on every crash.

This policy modifies the `adcli.ent.dumpcore` setting in the agent configuration file.

Disable multi-factor authentication (MFA) on Centrify-managed computers

Enabling this policy disables multi-factor authentication on Centrify-managed computers. By default, this policy is “Not configured” which allows multi-factor authentication to be used if roles or rights are configured to require it.

This policy modifies the `adcli.ent.mfa.enabled` setting in the agent configuration file.

Disable nscd group and passwd caching (Solaris, Linux)

Do not allow editing of the name service cache daemon configuration (`nscd.conf`) on **Solaris** and **Linux** computers. Note that selecting this policy disables rather than enables automatic editing of the file. This policy modifies the `adcli.ent.autoedit.nscd` setting in the agent configuration file.

Disable pwgrd (HP-UX)

Do not allow automatic editing of the password and group hashing and caching daemon (`pwgrd`) on **HP-UX** computers. Note that selecting this policy disables rather than enables automatic editing of the file. This policy modifies the `adcli.ent.autoedit.pwgrd` setting in the agent configuration file.

Enable core dump cleanup

Specify whether to delete old core dumps generated by the agent. By default, this policy is not configured, and core dumps generated by the agent will never be deleted. If you enable this group policy, agent-generated core dumps

are kept for the number of days that you specify. The default value is 30 days, but you can specify any number of days.

On Mac OS X, the default core dump location is `/cores/`. On most UNIX systems, the core dump location is the working directory of the current process. However, the core dump location can be customized on some platforms, including RHEL, Solaris, and AIX.

If the core dump location is inside `/var/centrifydc` and you enable this policy, all old core dumps are deleted without checking the process name first. If the core dump location is somewhere other than `/var/centrifydc` and you enable this policy, only the core dumps generated by the agent processes (for example, `adclient`, `cdcwatch`, and `kcm`) are deleted.

This policy does not modify the agent configuration file.

Enable logon hours local enforcement

Specify whether you want both Active Directory and the Centrify agent to check for user logon hour restrictions, or just Active Directory. If you disable this policy, only Active Directory will check the user logon hour restrictions. By default, the configuration parameter set by this policy is set to `true`.

You might want to set this parameter to `false` if the user and Centrify agent are in different time zones, and one time zone recognizes Daylight Savings Time, while the other does not. Otherwise, the user might not be able to log on at certain times.

This group policy modifies the `adclient.logonhours.local.enforcement` setting in the agent configuration file.

Encrypt adclient cache data

Specify to encrypt the local cache of Active Directory data. If you enable this policy, all of the Active Directory data stored in the cache is encrypted and the cache is flushed each time the agent starts up. If you disable or do not configure this policy, the cache is not encrypted and is not flushed when the agent starts up.

This group policy modifies the `adclient.cache.encrypt` setting in the agent configuration file.

Force domains and forests to be one-way trusted

Use the `Force domains and forests to be one-way trusted` group policy to specify a list of two-way trusted domains that need to be treated as one-way trusted domains. This is useful when two-way trusted domains are not accessible from UNIX machines, for example, they are behind a firewall. Configuring this parameter allows x-forest users to authenticate onto the trusting machines.

To set this group policy, select **Computer Configuration > Centrify Settings > DirectControl Settings > Adclient Settings > Force domains and forests to be one-way trusted**.

The default is an empty list.

Provide the following information for the group policy:

- A list of forests or domains to be treated as one-way trusted.
Specify a list of two-way trusted forests, and domains that have two-way external trust relationship with the local domain, to be treated by DirectControl Agent as one-way trusted forests or domains.

This parameter is likely to be used together with the configuration parameters, **Specify NTLM authentication domains** and **Specify AD to NTLM domain mappings**, if these forests and domains are not accessible from UNIX machines.

- Use the group policy, **Specify NTLM authentication domains**, to specify the list of domains that use NTLM authentication instead of Kerberos authentication.
- Use the group policy, **Specify AD to NTLM domain mappings**, to map AD domains to NTLM domains.

Alternative to using this group policy, **Force domains and forests to be one-way trusted**, you can use the configuration parameter, `adclient.one-way.x-forest.trust.force`.

Force password salt lookup from KDC

Force the Centrify agent to look up the complete principal name, including the Kerberos realm used as the key salt, from the KDC. Enabling this policy is only

• • • • •

required if you remove `arcfour-hmac-md5` from the list of encryption types specified for the `adclient.krb5.tkt.encryption.types` parameter in agent configuration file and if you change a `userPrincipalName` attribute in Active Directory without changing the user's password.

Enabling this policy may cause "pre-auth required" warning messages to appear in the Active Directory event log.

This group policy modifies the `adclient.force.salt.lookup` setting in the agent configuration file.

Map /home to /User (Mac OS X)

Although this group policy is defined in the `centrifydc_settings.xml` file, not in the `mac_settings.xml` file, it applies to Mac OS X computers only. See the *Administrator's Guide for Mac* for a description of this policy.

Run adclient on all processors

Specify whether to use all processors on a multi-processor system. By default, `adclient` uses all processors.

This policy modifies the `adclient.use.all.cpus` setting in the agent configuration file. This parameter is set to `true` by default. Disable this policy to set the parameter to `false` if `adclient` becomes unstable.

Set cache cleanup interval

Specify how often the agent should clean up the local cache. At each cleanup interval, the agent checks the cache for objects to be removed or expired, and at every 10th interval, the agent rebuilds local indexes. The value should be less than the values specified for the following parameters in the Centrify agent configuration file:

`adclient.cache.negative.lifetime`

`adclient.cache.flush.interval`

`adclient.cache.object.lifetime`

The default cleanup interval is 10 minutes.

• • • • •

This group policy modifies the `adclient.cache.cleanup.interval` setting in the agent configuration file.

Set the connector refresh interval

This policy controls how frequently connections to Centrify connectors are refreshed. The refresh task is a background process that searches for and selects the nearest available connector to use for connectivity between the Active Directory forest and the identity platform service.

By default, the process runs every 8 hours. You can use this group policy to modify that interval. If the interval is set to 0, the refresh task will be suspended.

This group policy modifies the `adclient.cloud.connector.refresh.interval` parameter setting in the agent configuration file.

Set maximum number of threads

Specify the maximum number of threads the agent will allocate for processing client requests. The value should be greater than or equal to the number of pre-allocated threads specified by the Set minimum number of threads policy. If you do not enable the policy, the default value is 20 threads.

This group policy modifies the `adclient.clients.threads.max` setting in the agent configuration file.

Set the maximum simultaneous authentication requests allowed

This policy specifies the maximum number of identity platform authentication requests that can be processed simultaneously. The default is 10 simultaneous requests.

If you change this setting, you must restart the `adclient` process.

This group policy modifies the `adclient.cloud.auth.token.max` setting in the agent configuration file.

Set minimum number of threads

Specify the number of threads the agent pre-allocates for processing client requests. The value must be an integer, zero or greater. If you set the value to zero, the agent processes requests sequentially. If you do not enable this policy, the default value is 4 threads.

This group policy modifies the `adclient.clients.threads` setting in the agent configuration file.

Specify low disk space interval

Specify how frequently the agent should check the disk space available for the local cache. The default interval checks the available disk space every 5 minutes. If the disk space available at any interval is less than the value you set for the Specify low disk space warning level policy, the agent will stop saving data in the local cache and will discard any new data until you free up enough disk space for it to resume saving data in the local cache.

The value must be an integer zero or greater. A value of zero disables checking for available disk space.

Keep in mind that the value you set for this policy can affect the recovery of a system after the agent stops writing data to the local cache. If you set the value to 0, the agent will not check for available disk space so it will not return to normal operation when disk space is freed up. In addition, setting value to 0 or to a long interval may cause the agent to consume too much of the disk for its local cache and make the computer unstable or unusable. Therefore, you should keep the interval for checking the available disk space relatively short. Keeping the interval short will also help to ensure that the agent resumes normal operation and saving data to its cache at the earliest opportunity.

This group policy modifies the `adclient.disk.check.interval` setting in the agent configuration file.

Specify low disk space warning level

Generate a warning message when the disk space available for the local cache reaches a critical level. If you enable this policy, you also need to specify the

threshold for available disk space that should trigger the warning message. By default, the warning is triggered if the free disk space reaches 51200 KB. Setting the Minimum Free Disk Space to 0 KB disables the display of a warning message.

If you enable the Specify low disk space interval policy, the agent will check the availability of free disk space at the interval specified. If the disk space available at any interval is less than the KB you set for the warning level, the agent stops saving data in the local cache. At the next interval when the available disk space exceeds the KB you set for this policy, the agent resumes normal operation and saving data to its cache.

Keep in mind that the value you set for this policy can affect the recovery of a system. The agent will only resume writing data to its local cache if there is more disk space available than what you have specified to generate the warning.

This group policy modifies the `adclient.disk.check.free` setting in the agent configuration file.

Specify a per machine (random) delay for cache refreshed background tasks

This group policy allows you to specify a per machine (random) delay, in minutes, for cache refreshed background tasks.

When there are more than one machines joined to the same domain and a number of those machines schedule background tasks to frequently access AD at the same time, the convergence of these activities causes a delay in AD. If you stagger these activities, you can avoid the convergence.

Once defined, scheduling background tasks calculates a random period of time within the interval and adds the same time to the delay of the tasks. If you change the interval setting, the period of time is recalculated. This only applies to newly scheduled background tasks.

The default setting is 0 and no delay. This policy modifies the `queueable.random.delay.interval` setting in the Centrify DirectControl configuration file.

Use the legal Kerberos type for cache encryption

Specify the type of encryption to use when encrypting the local cache. The encryption type you specify must be a type supported in the Kerberos environment. For example, Windows Server 2003 Kerberos supports the following cryptographic algorithms: RC4-HMAC, DES-CBC-CRC and DES-CBC-MD5.

This group policy is only used if the Encrypt adclient cache data policy is enabled. If Encrypt adclient cache data is not enabled, this policy is ignored.

This group policy modifies the `adclient.cache.encryption.type` setting in the agent configuration file.

Addns Settings group policies

Use the group policies under **Addns Settings** to configure domain name service settings in the agent configuration file.

Enable addns invoked by adclient

Enable whether adclient automatically launches the addns command. The addns command dynamically updates the DNS records on an Active Directory-based DNS server in environments where the DHCP server cannot update DNS records automatically.

In most cases, you do not need to use the addns command if a host's IP address is managed by a Windows-based DNS server and the host obtains its IP address from a Windows-based DHCP server because the DHCP server updates the DNS record for the host automatically.

If you are not using a Windows-based DNS server, you should use nsupdate or a similar command appropriate to the operating environment of the DNS server to update DNS records.

You can set the parameters of the addns command by specifying them in the [Set command line options used by adclient](#) group policy.

The default value for Mac OS X computers is True. The default value for all other platforms is False.

This group policy modifies the `adclient.dynamic.dns.enabled` parameter in the agent configuration file.

Set command line options used by adclient

Specify the parameters to use for the addns command if it is enabled by the [Enable addns invoked by adclient](#) group policy. For example, the default setting is:

```
/usr/sbin/addns -U -m
```

• • • • •

The `-u` option creates or updates the IP address and domain name pointer (PTR) records in the DNS server for the local computer.

The `-m` option uses the local computer account's Active Directory credentials to establish a security context with the DNS server.

Note that computers that act as a gateway between networks may require you to specify the network adapter IP address in the `addns` command line. To ensure that you register the correct network address with the Active Directory DNS server, set `adclient.dynamic.dns.command` with a command line that uses the correct IP address for the network interface you want to use.

This group policy modifies the `adclient.dynamic.dns.command` parameter in the agent configuration file.

Set DNS records update interval

Specify whether or not dynamic DNS records are periodically updated for this host and, if there are updates, the interval between updates. This interval value is defined in seconds and takes an integer of 0 or greater. If you set the value to 0, the DNS update feature will be disabled. Set the value to 1 or greater to specify the number of seconds between DNS update attempts.

The default for the `is` parameter is 0.

This group policy modifies the `adclient.dynamic.dns.refresh.interval` parameter in the agent configuration file.

Set wait response interval for update requests

Specify the amount of time, in seconds, that the `addns` process waits for responses to its request for updates. The parameter value takes an integer of 0 or greater. The default value for this policy is 7 seconds.

This group policy modifies the `addns.tcp.timeout` parameter in the agent configuration file.

Dzdo settings

Use the group policies under **Dzdo Settings** to control the operation of dzdo.

Always add anchors to regex in dzdo and dzcmds

Specifies whether you want to add anchors automatically to the regular expressions you define as command rights and use in role definitions. This group policy helps to prevent matching unintended paths or commands if the regular expression pattern is not carefully set.

If you set this group policy to **Disabled**, you should carefully review all regular expressions used as command rights to identify all possible matches for the pattern defined.

This group policy modifies the `dzdo.auto.anchors` setting in the agent configuration file.

Enable logging of valid command execution in dzdo

Specify whether messages resulting from successful command execution are logged. Messages are written to the `syslog` `auth` facility or `authpriv` facility, typically located in `/var/log/secure`.

If you set this group policy to **Not configured** or **Enabled**, the dzdo program logs both valid and invalid command execution.

If you set this group policy to **Disabled**, information about only invalid command execution is logged.

This group policy modifies the `dzdo.log_good` setting in the agent configuration file.

Enable user command timeout

This group policy modifies the `dzdo.user.command.timeout` setting in the Centrify DirectControl configuration file. When this group policy is set to

Enabled, the user may specify a timeout on the dzdo command line with a -T option. If the timeout expires before the command has exited, the command will be terminated. The default setting is disabled.

Force dzdo re-authentication when relogin

Specify whether users must authenticate again with dzdo after logging out.

When a user authenticates with dzdo, a ticket is temporarily created that allows dzdo to run without re-authentication for a short period of time. If a user logs out, the ticket is reused when the user logs back in.

Enable this policy to remove the tickets when a user logs out. The user will be required to re-authenticate again when logging back in.

The default, when the policy is not set, is to not clear the tickets when users log out.

This group policy modifies the `adclient.dzdo.clear.passwd.timestamp` setting in the agent configuration file.

Force dzdo to set HOME environment variable

Specify whether privileged commands run with dzdo commands should set the HOME environment variable to the home directory of the target user (which is root by default).

If you set this group policy to **Not configured** or **Disabled**, the dzdo program does not set the HOME environment variable.

If you set this group policy to **Enabled**, the dzdo program sets the HOME environment variable. Enabling this group policy effectively implies that the -H command line option should always be used.

This group policy provides functionality equivalent to setting the `always_set_home` flag for configuring sudo operation.

This group policy modifies the `dzdo.always_set_home` setting in the agent configuration file.

Force dzdo to set HOME environment variable when runs with '-s' option

Specify whether privileged commands run with dzdo using the -s command line option should set the HOME environment variable to the home directory of the target user (which is root by default).

If you set this group policy to **Not configured** or **Disabled**, the dzdo program does not set the HOME environment variable.

If you set this group policy to **Enabled**, the dzdo program sets the *HOME* environment variable.

This group policy provides functionality equivalent to setting the `set_home` flag for configuring sudo operation.

This group policy modifies the `dzdo.set_home` setting in the agent configuration file.

Force per tty authentication in dzdo

Specify whether dzdo requires authentication once per tty rather than once per user.

If you set this group policy to **Not configured** or **Disabled**, authentication is required once per user. If you set this group policy to **Enabled**, authentication is required once per tty.

This group policy provides functionality equivalent to setting the `tty_tickets` flag for configuring sudo operation.

This group policy modifies the `dzdo.tty_tickets` setting in the agent configuration file.

Prompt error message if command not found by dzdo

Specify whether the dzdo program informs the user when it cannot find a command in the user's PATH.

• • • • •

If you set this group policy to **Not configured** or **Enabled**, the dzdo program displays an error statement indicating that the command could not be found in the user's PATH.

If you set this group policy to **Disabled**, dzdo is prevented from indicating whether a command was not allowed or simply not found.

This group policy provides functionality equivalent to setting the `path_info` flag for configuring the sudo operation.

This group policy modifies the `dzdo.path_info` setting in the agent configuration file.

Replace sudo by dzdo

Specify whether to replace sudo with dzdo.

Enable this policy to redirect sudo commands to dzdo. This policy creates a symbolic link between sudo and dzdo. When a user executes a sudo command, dzdo is executed instead. Role assignment settings for the user determine whether the user is allowed to execute the commands specified with sudo.

Be certain to set `/usr/share/centrifydc/bin` as the first search directory for the PATH variable if you enable this group policy.

This policy is only applicable if you are using zones. It is not applicable for computers that join Auto Zone.

Require dzdo command validation check

Specify whether to enforce the validation check for dzdo privileged commands.

If you set this group policy to **Enabled**, privileged commands will run only after being validated by the dzdo validator. If a command fails validation, or if the dzdo validator does not exist, is not available, or is not trusted—for example because it is not owned by root or is group or world writeable—the command will not run.

If you set this group policy to **Not configured** or **Disabled**, no attempt is made to validate privileged commands, and the commands will run without validation.

.....

This group policy modifies the `dzdo.validator.required` setting in the agent configuration file.

The dzdo validator is located and configured as described in [Set dzdo validator](#) later in this section.

Require runas user for dzdo

Specify whether a user must explicitly identify the 'runas' user when executing a command with dzdo.

If you set this group policy to **Not configured** or **Enabled**, and a user executes a command with dzdo and does not explicitly identify the user or group to run as with the `-u` or `-g` option, `adcli` assumes that the command should be run as root. If the user is not authorized to run the command as root, dzdo fails to execute the command and issues an error message.

If you set this group policy to **Disabled** and a user executes a command with dzdo that does not explicitly identify the user or group to run as, `adcli` attempts to resolve the user. If the command defines a single runas user, dzdo executes the specified command and sends a message to the log file.

If the command defines multiple runas users, dzdo cannot resolve the user to run as and attempts to run the command as root. Because the user is not authorized to run the command as root, dzdo fails to execute the command and issues an error message.

In all cases, a user can execute a command successfully with dzdo by using the `-u` option to explicitly identify the runas user. For example:

```
[u1@rh6]$dzdo -u qal adinfo
```

This group policy modifies the `dzdo.set.runas.explicit` setting in the agent configuration file.

Require user is logged in to a real tty to run dzdo

This group policy ensures a user is logged in to a valid tty to run dzdo. This policy modifies the `dzdo.requiretty` setting in the Centrify DirectControl configuration file. By default, this group policy is not configured, and you do not require a tty to run dzdo.

Set directory to store user timestamp by dzdo

Specify the directory where dzdo stores the user's login timestamp files.

If you set this group policy to **Not configured** or **Disabled**, the default directory `/var/run/dzdo` is used.

If you set this group policy to **Enabled**, you can specify a directory of your choice.

This group policy provides functionality equivalent to setting the `timestampdir` flag for configuring sudo operation.

This group policy modifies the `dzdo.timestampdir` setting in the agent configuration file.

Set dzdo authentication timeout interval

Specify the maximum number of minutes allowed between operations before prompting the user to re-enter a password.

If you set this group policy to **Not configured** or **Disabled**, the default timeout interval of five minutes is used. If you set this group policy to **Enabled**, you can specify a timeout interval of your choice.

You can set this parameter to zero (0) to always prompt for a password when users run privileged commands with dzdo. If you specify a value less than 0, the user's timestamp never expires.

This group policy provides functionality equivalent to setting the `timestamp_timeout` flag for configuring sudo operation.

This group policy modifies the `dzdo.timestamp_timeout` setting in the agent configuration file.

Set dzdo password prompt timeout interval

Specify the number of minutes before the dzdo password prompt times out.

If you set this group policy to **Not configured** or **Disabled**, the default timeout value of five minutes is used. If you set this group policy to **Enabled**, you can specify a timeout value of your choice.

• • • • •

You can set this parameter to zero (0) to have the password prompt never timeout.

This group policy provides functionality equivalent to setting the `passwd_timeout` flag for configuring sudo operation.

This group policy modifies the `dzdo.passwd_timeout` setting in the agent configuration file.

Set dzdo validator

Specify the full path of the dzdo validator. The settings in this group policy are used only when the [Require dzdo command validation check](#) group policy is enabled.

The dzdo validator is a script that runs synchronously under the user's Active Directory name. If the [Require dzdo command validation check](#) group policy is enabled, the dzdo validator runs when users attempt to execute dzdo commands. Command attempts that pass validation are allowed to run. Command attempts that fail validation are not allowed to run.

The default location of the dzdo validator is `/usr/share/centrifydc/sbin/dzcheck`. If you set this group policy to **Not configured** or **Disabled**, the validator located in this default location is used.

If you set this group policy to **Enabled**, the dzdo validator that you specify is used.

Note that the authentication, privilege elevation, and audit and monitoring services distribution package does not include a dzcheck script. Instead, a sample validator, `/usr/share/centrifydc/sbin/dzcheck.sample`, is provided for reference. To configure and enable the dzdo validator, modify the sample script or create a new script, then place that script in the default location (`/usr/share/centrifydc/sbin/dzcheck`) or use a location and script name of your choice that you specify in this group policy.

You do not need to create a dzcheck script to use dzdo. You only need to create a script if you want to modify dzdo behavior so that validation occurs when dzdo commands attempt to run.

This group policy modifies the `dzdo.validator` setting in the agent configuration file. For more information about configuring the dzdo validator, see the “dzdo.validator” section in the *Configuration and Tuning Reference Guide*.

Set environment variables to be preserved by dzdo

Specify the default list of environment variables to preserve in the user's environment. This group policy applies only if you have selected the **Reset environment variables** option for the command in Access Manager.

If you set this group policy to **Not configured** or **Disabled**, the default list of variables displayed when you run the `dzdo -v` command as root is preserved.

If you set this group policy to **Enabled**, you can specify variables to preserve in addition to the default list of variables. Variables that you specify must be formatted as a comma-separated list. For example:

```
COLORS, DISPLAY, HOME, HOSTNAME, KRB5CCNAME, LS_
COLORS, MAIL, PATH, PS1, PS2, TZ, XAUTHORITY, XAUTHORIZATION
```

This group policy provides functionality equivalent to setting the `env_keep` flag for configuring sudo operation.

This group policy modifies the `dzdo.env_keep` setting in the agent configuration file.

Set environment variables to be removed by dzdo

Specify the default list of environment variables to be removed from the user's environment. This group policy applies only if you have selected the **Remove unsafe environment variables** option for the command in Access Manager.

If you set this group policy to **Not configured** or **Disabled**, the default list of variables displayed when you run the `dzdo -v` command as root is removed.

If you set this group policy to **Enabled**, you can specify variables to remove in addition to the default list of variables. Variables that you specify must be formatted as a comma-separated list. For example:

```
IFS, CDPATH, LOCALDOMAIN, RES_OPTIONS, HOSTALIASES,
NLSPATH, PATH_LOCALE, LD_*
```

This group policy provides functionality equivalent to setting the `env_delete` flag for configuring sudo operation.

This group policy modifies the `dzdo.env_delete` setting in the agent configuration file.

Set environment variables to be removed by dzdo with characters % or /

Specify the list of environment variables that should be checked for percent (%) or slash (/) special characters. If there are environment variable values containing the special characters, dzdo removes those variables from the user's environment. Variables with % or / characters are removed regardless of whether you have selected the **Reset environment variables** option for the command in Access Manager.

If you set this group policy to **Not configured** or **Disabled**, the default list of variables displayed when you run the `dzdo -v` command as root is checked for special characters.

If you set this group policy to **Enabled**, you can specify variables to check for special characters in addition to the default list of variables. Variables that you specify must be formatted as a comma-separated list. For example:

```
COLORTERM, LANG, LANGUAGE, LC_*, LINGUAS, TERM
```

This group policy provides functionality equivalent to setting the `env_reset` flag for configuring sudo operation.

This group policy modifies the `dzdo.env_check` setting in the agent configuration file.

Set error message when failed to authenticate in dzdo

Specify the message that is displayed if a user enters an incorrect password.

If you set this group policy to **Not configured** or **Disabled**, the default message "Sorry, try again" is used. If you set this group policy to **Enabled**, you can specify a message of your choice. The message can be any text string enclosed by quotation marks. For example:

```
"The password provided is not valid."
```

This group policy provides functionality equivalent to setting the `badpass_message` flag for configuring sudo operation.

This group policy modifies the `dzdo.badpass_message` setting in the agent configuration file.

Set lecture shown by dzdo before password prompt

Specify the full path to a file containing the warning message that is displayed about using dzdo before displaying the password prompt.

If you set this group policy to **Not configured** or **Disabled**, a default message is used. If you set this group policy to **Enabled**, you can specify a file containing a message of your choice. You must specify the full path to the file. For example, to use a custom message located in the file `dzdo_warning`:

```
/etc/custom/dzdo_warning
```

This group policy provides functionality equivalent to setting the `lecture_file` flag for configuring sudo operation.

This group policy modifies the `dzdo.lecture_file` setting in the agent configuration file.

Set password prompt for target user password in dzdo

Specify the password prompt displayed when running privileged commands. This group policy serves the same function as the `dzdo -p` command.

If you set this group policy to **Not configured** or **Disabled**, the default prompt `[dzdo] password for %p:` where `%p` is `root` unless specified otherwise.

If you set this group policy to **Enabled**, you can specify a prompt of your choice. You can use the following escapes in the prompt:

`%u`—Expands to the invoking user's login name.

`%U`—Expands to the login name of the user the command will be run as. If not specified, defaults to `root`.

`%h`—Expands to the local hostname without the domain name.

`%H`—Expands to the local hostname including the domain name.

`%p`—Expands to the user whose password is asked for.

`%%`—Collapses to a single `%` character.

This group policy modifies the `dzdo.passprompt` setting in the agent configuration file.

Set paths for command searching in dzdo

Specify the search path for the dzdo program to use to look for commands and scripts that require privileges to run.

If you set this group policy to **Not Configured** or **Disabled**, no search path is set (that is, there is no default value). If you set this group policy to **Enabled**, you can specify a list of directories for the dzdo program to search for commands and scripts. The dzdo program will search in the specified directories no matter which path the command rights are configured to use in the Access Manager **System search path** option.

If command paths are configured in Access Manager using the **System search path** option and this group policy is **Disabled** or **Not Configured**, the following actions take place:

- The current user's path is used to search for the commands.
- Only the commands located under the System path are allowed to execute.

The search path that you specify can be a list of directories or the name of a file that contains the list of directories. For example, you can specify a file that contains the directories to search using the file: keyword and a file location:

```
file:/etc/centrifydc/customized_dzdo_directories
```

If you specify a file name, you should ensure that the file is owned by root and is not accessible to any other users.

This group policy modifies the `dzdo.search_path` setting in the agent configuration file.

Set secure paths for command execution in dzdo

Specify the path for the dzdo program to use when executing commands and scripts that require privileges to run.

If you set this group policy to **Not Configured** or **Disabled**, no specific path is set (that is, there is no default value). If you set this group policy to **Enabled**, you can specify the directory that dzdo uses. The dzdo program will execute only the commands and scripts that are located in the directory that you specify.

• • • • •

The path that you specify can be a list of directories or the name of a file that contains the list of directories. For example, you can specify a file that contains the directories to search using the `file:` keyword and a file location:

```
file:/etc/centrifydc/customized_dzdo_directories
```

Within the file, lines should contain paths separated by colons. For example, a file specifying two paths might look like this:

```
/etc/centrifydc/reports/exec_report_cmds:/usr/sbin/ora_cmds
```

If you specify a file name, you should ensure the file is owned by root and not accessible to any other users.

Setting this group policy and the [Set paths for command searching in dzdo](#) group policy to the same path is equivalent to setting the `secure_path` parameter in the `sudoers` configuration file.

This group policy modifies the `dzdo.secure_path` setting in the agent configuration file.

Show lecture by dzdo before password prompt

Specify whether `dzdo` displays a warning message about using `dzdo` before displaying the password prompt.

If you set this group policy to **Not configured** or **Disabled**, the message defined in the [Set lecture shown by dzdo before password prompt](#) group policy (or in `dzdo.lecture_file`) is displayed one time.

If you set this group policy to **Enabled**, you can specify whether and how often the message is displayed. The values that you can specify are:

- **once**—Display the warning message only the first time the command is run.
- **never**—Never display a warning message.
- **always**—Display the warning message every time the program is invoked.

This group policy provides functionality equivalent to setting the `lecture` flag for configuring `sudo` operation.

• • • • •

This group policy modifies the `dzdo.lecture` setting in the agent configuration file.

Use `realpath` to canonicalize command paths in `dzdo`

Specify whether `dzdo` uses command paths resolved by `realpath` when searching for commands.

If you set this group policy to **Not configured** or **Disabled**, `realpath` is not used to resolve command paths. If you set this group policy to **Enabled**, `realpath` is used to expand all symbolic links and resolve references to:

`./`

`../`

extra / characters

This group policy modifies the `dzdo.use.realpath` setting in the agent configuration file.

Group policy settings

Use the group policies under **Group Policy Settings** to manage the Centrify group policy mapping programs.

Enable user group policy

Specify whether to enable user-based group policies. If you enable this policy, user-based group policies are enabled. If you explicitly disable this group policy, user-based policies are disabled.

If you do not set this policy, the default is to enable user-based policies on Mac OS X machines and disable user-based policies on all other Linux and UNIX based computers.

When this policy is **Disabled**, all user configuration Software Settings and user configuration Windows Settings group policies set for computers in Centrify zones are not applied. You must enable this policy if you want to use any Software Settings, Windows Settings, or Centrify Settings group policies on computers in a Centrify zone.

User configuration group policies enabled in a child organizational unit do NOT apply to users logging in to computers in the child organizational unit who are not in that organizational unit (for example, they are in the parent organizational unit only). See [Applying policies in nested organizational units](#) if you need to have different user configuration policies at different levels in the organizational unit hierarchy.

This group policy modifies the `gp.disable.user` setting in the agent configuration file.

Set machine group policy mapper list

Specify the list of mapper programs to run for computer-based policies.

You can use an asterisk (*) as a wild card to match a set of program names. For example, you can specify `a*` to match all programs with names that start with the letter a.

.....

You can use an exclamation point (!) with a program name to exclude a program from the list. For example, you can specify `!mysample` to prevent the mapping program `mysample` from running.

This group policy modifies the `gp.mappers.machine` setting in the agent configuration file.

Set group policy mapper execution timeout

Specify the maximum amount of time, in seconds, to allow for a group policy mapper program to run before the process is stopped.

This group policy modifies the `gp.mappers.timeout` setting in the agent configuration file.

Set user group policy mapper list

Specify the list of mapper programs to run for user policies.

You can use an asterisk (*) as a wild card to match a set of program names. For example, you can specify `a*` to match all programs with names that start with the letter a.

You can use an exclamation point (!) with a program name to exclude a program from the list. For example, you can specify `!mysample` to prevent the mapping program `mysample` from running.

This group policy modifies the `gp.mappers.user` setting in the agent configuration file.

Set total group policy mappers execution timeout

Specify the maximum amount of time, in seconds, to allow for all group policy mapper programs to run before stopping all mapper processes.

This group policy modifies the `gp.mappers.timeout.all` setting in the agent configuration file.

Use user credential to retrieve user policy

Use this group policy to distinguish whether to use user credentials instead of machine credentials to retrieve user policy. By default, machine credentials are used to retrieve user policy. However, if a computer object does not have permission to access user group policy objects, user policy will not be applied.

If you enable this group policy, user credentials are used to retrieve user policy.

This group policy modifies the `gp.use.user.credential.for.user.policy` setting in the agent configuration file.

Kerberos settings

Use the group policies under **Kerberos Settings** to manage the Kerberos configuration.

Allow PAM to create user Kerberos credential cache

Use this policy to specify whether PAM creates the Kerberos user credential cache.

If this group policy is **Enabled** or **Not Configured**, a Kerberos user credential cache is created. The Kerberos user credential cache can be file-based or it can be a KCM in-memory cache, depending on the `krb5.cache.type` setting in `/etc/centrifydc/centrifydc.conf`.

If this group policy is disabled, the Kerberos user credential cache is not created, and any attempt to perform an SSO operation will fail.

This group policy modifies the `pam.auth.create.krb5.cache` setting in the agent configuration file.

Allow weak encryption types for Kerberos authentication

Use this group policy to specify whether to allow weak encryption types for Kerberos authentication.

By default (not configured), this policy allows the weak encryption types specified in the configuration parameters `adclient.krb5.permitted.encryption.types` and `adclient.krb5.tkt.encryption.types`.

These encryption types include:

`des-cdc-crc`

`des-cbc-md4`

`des-cbc-md5`

`des-cbc-raw`

`des3-cbc-raw`

.....

des-hmac-sha1

arcfour-hmac-exp

rc4-hmac-exp

arcfour-hmac-md5-exp

If you disable this policy, the above encryption types will not be supported. Note that setting this policy to disabled may cause authentication failures in existing Kerberos environments that do not support strong cryptography. Users in these environments should leave this policy set to **Not Configured** or **Enabled** until their environment adopts stronger cyphers.

This policy modifies the `adclient.krb5.allow_weak_crypto` parameter in the agent configuration file.

Alternative location for user .k5login files

Use this policy to specify an alternative location for user .k5login files.

If specified, this string value will be used for the `k5login_directory` in the `[libdefaults]` stanza in `krb5.conf` and the user's .k5login file will be named as `<k5login_directory>/<unix_name>`.

For security reasons the specified directory should be owned by root and writeable by root only. If the directory does not exist, adclient will create it.

This group policy modifies the `krb5.conf.k5login_directory` setting in the agent configuration file.

Disable Kerberos built-in ccselect plugins

Use this policy to specify whether adclient should disable the Kerberos built-in ccselect plugins.

If this group policy is **Enabled** or **Not Configured**, adclient will disable all ccselect built-in plugins in the **plugins** section of the `krb5.conf` file when the group policy, [Manage Kerberos configuration](#), is enabled.

If this group policy is set to **Disabled**, the ccselect plugins will **not** be disabled.

This group policy modifies the `krb5.conf.plugins.ccselect.disable` configuration parameter in the agent configuration file.

Enable Kerberos clients to correct time difference

Enable Kerberos to automatically correct for a time difference between the system clock and the clock used by the KDC. You only need to enable this group policy if your system clock is drifting and the system is not using NTP and adclient SNTP settings.

This group policy modifies the `krb5.use.kdc.timesync` setting in the agent configuration file.

Force Kerberos to only use TCP

Force all Kerberos requests to use TCP rather than UDP.

This group policy modifies the `krb5.forcetcp` setting in the agent configuration file.

Generate the forwardable tickets

Specify whether you want the Centrify agent to create forwardable Kerberos user tickets. Creating a forwardable ticket allows a user's logon ticket to be sent to another computer and used to access to additional systems and resources.

If you select **Enabled** for this group policy, service tickets can be forwarded from one service or resource to another. If you do not want tickets to be forwarded, you can uncheck this option to prevent the agent from creating forwardable tickets.

This group policy modifies the `krb5.forwardable.user.tickets` setting in the agent configuration file.

Generate Kerberos version numbers for Windows 2000

Kerberos Version Numbers (kvno), allow tickets issued with a computer's previous key to be decrypted even when the ticket was issued before the computer changed its password, but presented afterwards.

Windows 2000 does not support these kvnos, but you can enable this policy to generate version numbers that work with Windows 2000.

However, this feature requires Centrify's Kerberos libraries so older Kerberos applications may fail to understand the generated Kerberos version numbers. You can disable this policy to support older applications with the knowledge that the race condition just described may cause authentication failures.

This group policy modifies the `krb5.generate.kvno` setting in the agent configuration file.

Manage Kerberos configuration

Indicate whether you want the Centrify agent to automatically manage the Kerberos configuration files.

This group policy modifies the `adclient.krb5.autoedit` setting in the agent configuration file.

Renew credentials automatically

Specify whether to automatically reissue user credentials when they expire. If you enable this group policy, the Centrify agent keeps a hash of the user's password in memory indefinitely. If you do not enable this policy, or if you explicitly disable it, a user's credentials periodically expire and the user must be re-authenticated by re-entering a valid password.

If you enable this policy, user credentials are automatically reissued, as needed, as long as the `adclient` process continues to run even if the computer is disconnected from Active Directory. If you stop or restart `adclient`, however, the user's password hash is removed from memory. After stopping or restarting `adclient`, users must be re-authenticated by logging on with a valid user name and password.

The default value is `false`.

This group policy modifies the `krb5.cache.infinite.renewal` setting in the agent configuration file.

Set configuration update interval

Specify how frequently, in hours, the Centrify agent should update the Kerberos configuration files.

This group policy modifies the `krb5.config.update` setting in the agent configuration file.

Set Kerberos UDP preference limit

Specify the maximum size packet that the Kerberos libraries will attempt to send over a UDP connection before retrying with TCP. If the packet size is larger than this value, only TCP will be tried. If the value is set to 1, TCP will always be used. The hard UDP limit is 32700. If you enter a value larger than this, the value is reset to 32700 when you apply the policy.

This policy only takes effect if the policy Force Kerberos to only use TCP is not configured or is disabled (the configuration parameter `krb5.forcetcp` is set to `false`).

If Force Kerberos to only use TCP is enabled and the agent is managing the `krb5.conf` file, it will set `udp_preference_limit = 1`, so that the Kerberos libraries will always use TCP.

If you do not enable this group policy, the default value is 1465.

This group policy modifies the `krb5.udp.preference.limit` setting in the agent configuration file.

Set credential renewal interval

Specify how frequently, in hours, Kerberos credentials are renewed. A value of 0 disables renewal completely.

This group policy modifies the `krb5.cache.renew.interval` setting in the agent configuration file.

Set password change interval

Specify how frequently, in days, the Centrify agent should change the computer account password in Active Directory.

This group policy modifies the `adclient.krb5.password.change.interval` setting in the agent configuration file.

Set password change verification interval

Specify the interval, in seconds, that `adkeytab` waits between computer password change verification attempts.

This group policy modifies the `adclient.krb5.password.change.verify.interval` setting in the agent configuration file.

The default setting is 300 seconds (5 minutes).

Set password change verification attempts

Specify the number of times that `adkeytab` attempts to verify password changes after an initial, failed attempt.

Some environments, such as those using a read-only domain controller (RODC), can experience replication delays that may prevent Kerberos password changes to be verified through `adclient`. As a result of this delay, the new password may not be saved to the keytab file.

Increasing the number of verification attempts can address replication delays that may result from having a read-only domain controller.

This group policy modifies the `adclient.krb5.password.change.verify.retries` setting in the agent configuration file.

The default setting is 0, which means that `adkeytab` does not attempt additional password verification attempts after the initial failure.

Specify credential cache type for AD users

Specify the type of Kerberos credential cache that `adcli`ent will create when an Active Directory user logs in. You can specify a file-based or in-memory-based credential cache.

Note The use of in-memory credential caches is not supported on Mac OS X computers, therefore applying this group policy setting to a Mac OS X computer has no effect.

To specify the type of cache to create, click **Enabled**, then select the type of cache from **Kerberos credential cache type**.

If you select **File-based credential cache**, the Centrify agent creates a file-based credential cache for each Active Directory user in `/tmp` when the user logs in. A file-based credential cache persists until the file is deleted.

If you select **In-memory credential cache provided by Centrify-KCM service**, the Centrify agent creates an in-memory credential cache for each Active Directory user when the user logs in. The `centrify-kcm` service, run as root, manages in-memory credential caches. When the `adcli`ent process starts up, if the policy is configured for an in-memory credential cache, `adcli`ent starts the KCM service. If you change the setting from file-based to in-memory while `adcli`ent is running, `adcli`ent starts the KCM service the next time it is forced to reload configuration parameters, for example, if you run the `adgupdate` command to update group policy settings, or if a user opens a new session.

Setting this parameter affects new users only — not users who have already logged in. For example, if you change from a file-based, to an in-memory credential cache, Direct Control will continue to use the file-based credential cache for any user who was logged in at the time of the change. If a logged in user opens a new session, or a new user logs in, the agent will use an in-memory cache for them.

An in-memory credential cache ends as soon as the `centrify-kcm` service is stopped.

This group policy modifies the `krb5.cache.type` setting in the agent configuration file.

Specify groups to infinitely renew Kerberos credentials

Specify a list of Active Directory groups whose members' Kerberos credentials require infinite renewal even after the users have logged out. Groups that you specify must be Active Directory groups, but do not need to be zone enabled. However, only zone enabled users in a group will have their credentials automatically renewed.

If this group policy is **Enabled**, group member's credentials are renewed automatically. You must use the following format to specify groups when you enable this group policy:

```
sAMAccountName@domain
```

For example:

```
test_group_sam@example.com
```

By default, this group policy is disabled.

This group policy modifies the `krb5.cache.infinite.renewal.batch.groups` setting in the agent configuration file.

Specify maximum Kerberos credential cache lifetime

Specify whether adclient deletes credentials from the Kerberos cache if they are the specified number of days old.

If this group policy is **Enabled**, the credentials will be cleared for all users whether or not they are logged on, have active processes running, or are specified in the following group policy lists:

- [Specify groups to infinitely renew Kerberos credentials](#)
- [Specify users to infinitely renew Kerberos credentials](#)

You can configure this group policy by enabling it and setting the value to the age of the credential cache to be cleared, in days.

The default value for the group policy is 0 days, which means that this group policy does not clear any credential caches.

This group policy modifies the `krb5.cache.clean.force.max` setting in the agent configuration file.

Specify users to infinitely renew Kerberos credentials

Specify a list of users whose Kerberos credentials require infinite renewal even after the users have logged out. Users that you specify must be zone enabled (that is, mapped users are not supported). If this group policy is enabled, user credentials are renewed automatically.

You can use any of the following formats to specify user names:

unixName

userPrincipleName

sAMAccountName

sAMAccountName@domain

For example:

`test_user`

`test_user@example.com`

`test_user_sam`

`test_user_sam@example.com`

By default, this group policy is disabled.

This group policy modifies the `krb5.cache.infinite.renewal.batch.users` setting in the agent configuration file.

Specify whether CDC k5login module should ignore .k5login for SSO

Specify whether the k5login module should ignore .k5login for SSO.

The default value is `false`.

This group policy modifies the `krb5.sso.ignore.k5login` setting in the agent configuration file.

Specify whether Kerberos PAC Checksum validation should be done

This group policy specifies whether or not to verify that the user's PAC (Privilege Authorization Certificate) information is from a trusted KDC (Key

Distribution Center) so as to prevent what's referred to as a "silver ticket" attack.

When performing credential verification, a service ticket is fetched for the local system. After the credential is verified, the local system uses the PAC information in the service ticket.

This group policy takes effect when the policy is enabled or when DirectControl is using the user's PAC from a service ticket. This setting does not apply to retrieving the PAC by way of the S4U2Self protocol.

There are 3 possible values for this policy:

- `disabled` (default): NO PAC validation will be done at all.
- `enabled`: If PAC Validation fails, the PAC information is used and the user login is allowed.
- `enforced`: If PAC Validation fails, the PAC information is discarded and the user login is denied.

Setting this group policy to enabled or enforced will have significant impact on the user login and user's group fetch performance.

Strictly Enforce Default Encryption Types

This parameter specifies if DirectControl should add or replace the default encryption types listed in the settings, `default_tgs_etypes` and `default_tkt_etypes` in `krb5.conf` with the types specified in the setting `adclient.krb5.tkt.encryption.types` in `centrifdc.conf`.

- When this group policy is not set (default) —No change in behavior. It means DirectControl adds any additional encryption types.
Default encryption types from `centrifdc.conf` are added, if they were not already listed. Other items that were already in `default_tgs_etypes` and `default_tkt_etypes` are left alone and not removed.
- When this group policy is set—DirectControl replaces the encryption types listed in the settings, `default_tgs_etypes` and `default_tkt_etypes` in `krb5.conf` to match exactly with the encryption types listed in the setting, `adclient.krb5.tkt.encryption.types` in `centrifdc.conf`.

Default encryption types from `centrifdc.conf` are added, if they were not already listed. Other items that were already in `default_tgs_enctypes` and `default_tkt_enctypes`, and not in `centrifdc.conf`, are removed.

This group policy is set as follows: **Computer Configuration > Centrify Settings > DirectControl Settings > Kerberos Settings > Control if strictly enforce the encTypes.**

Strictly Enforce Permitted Encryption Types

This parameter specifies if DirectControl should add or replace the permitted encryption types listed in the setting, `permitted_enctypes` in `krb5.conf` with the types specified in the setting, `adclient.krb5.permitted.encryption.types` in `centrifdc.conf`.

- When this group policy is not set (default) —No change in behavior. it means DirectControl adds any additional encryption types.

Permitted encryption types from `centrifdc.conf` are added, if they were not already listed. Other items that were already in `permitted_enctypes` are left alone and not removed.

- When this group policy is set—DirectControl replaces the setting, `permitted_enctypes` in `krb5.conf` to match exactly with encryption types listed in the setting, `adclient.krb5.permitted.encryption.types` in `centrifdc.conf`.

Permitted encryption types from `centrifdc.conf` are added, if they were not already listed. Other items that were already in `permitted_enctypes`, and not in `centrifdc.conf`, are removed.

This group policy is set as follows: **Computer Configuration > Centrify Settings > DirectControl Settings > Kerberos Settings > Control if strictly enforce the permitted_encTypes.**

Use DNS to lookup KDC

Allow the agent to use DNS to locate the Kerberos Key Distribution Center (KDC).

• • • • •

This group policy modifies the `krb5.use.dns.lookup.kdc` setting in the agent configuration file.

Use DNS to lookup realms

Allow the agent to use DNS to locate Kerberos realms.

This group policy modifies the `krb5.use.dns.lookup.realm` setting in the agent configuration file.

Local account management settings

Use the group policies under **Local Account Management** to control whether local accounts are managed by the agent, and other aspects of local account management by the agent.

Enable local account management feature

Specify whether the agent manages local users and groups on the computer where the agent is installed.

When this group policy is **Enabled**:

- The agent gets the local user and local group profiles from the zone, and updates the local password and local group files using the information defined in the zone.
- You can view and manage local users and groups in Access Manager as described in the *Administrator's Guide for Linux and UNIX*.

By default, this group policy is disabled (unless you upgraded from a authentication, privilege elevation, and audit and monitoring services release in which it was enabled), and the agent does not manage local users and groups.

This group policy modifies the `adclient.local.account.manage` setting in the agent configuration file.

Notification Command Line

Define a command to process changes to local account profiles after the agent synchronizes local user and group profiles with profiles defined in a zone.

For example, if new local users are added, removed, or have their enabled/disabled status changed locally, the command that you define in this policy is executed. Typical activities that this command might perform include setting the password for new or updated local accounts, or notifying

• • • • •

password vault about changes to local accounts and defining actions to take regarding those accounts.

When this policy is **Enabled**, the agent invokes the defined command in another process and passes a comma separated UNIX name list to the command for further processing.

By default, this policy is not configured (that is, no command is defined).

This group policy modifies the `adclient.local.account.notification.cli` setting in the agent configuration file.

This policy takes effect only when local account management is enabled through the **Enable local account management feature** group policy, or through the `adclient.local.account.manage` configuration parameter.

Logging settings

Use the group policies under **Logging Settings** to control the following aspects of a computer's logging facilities:

- Set Adclient audit logging facility
- Set general audit logging facility
- Set log message queue size
- Set NIS audit logging facility

Set Adclient audit logging facility

Specify the syslog facility to use for logging adclient auditing messages. You can separately enable syslog facilities for logging general adclient messages, adclient auditing messages, and adnisd messages.

Select a value for this group policy from the list box, which contains a list of valid syslog facilities, for example, auth, authpriv, daemon, security, user, local n, and so on. The available facilities may vary depending on the operating system. The default value is auth.

If this group policy is not enabled, the audit messages are logged in the facility defined for the Set general audit logging facility policy.

This group policy modifies the `logger.facility.adclient` setting in the agent configuration file.

Rather than using the policy to set the facility, you can edit the agent configuration file to set the `logger.facility.adclient` parameter to any valid syslog facility. For example, you can set this parameter to log messages to one of auth, authpriv, daemon, security, local n facilities, and so on.

Set general audit logging facility

Specify the syslog facility to use for logging general adclient activity. You can separately enable syslog facilities for logging general adclient messages, adclient auditing messages, and adnisd messages.

Select a value for this group policy from the list box, which contains a list of valid `syslog` facilities, for example, `auth`, `authpriv`, `daemon`, `security`, `user`, `local n`, and so on. The available facilities may vary depending on the operating system. The default value is `auth`.

This group policy modifies the `logger.facility.*` setting in the agent configuration file.

Rather than using the policy to set the facility, you can edit the agent configuration file to set the `logger.facility` parameter to any valid `syslog` facility. For example, you can set this parameter to log messages to one of `auth`, `authpriv`, `daemon`, `security`, `localn` facilities and so on.

You may also edit the agent configuration file to specify other process names for logging, or use an asterisk (*) to specify the default facility to use for all agent processes. For example, you can specify `logger.facility.*: auth` in the configuration file to direct all agent processes send messages to the `auth` facility of `syslog`.

Set log message queue size

This policy controls the maximum size in KB to use for queued log messages. The messages in the queue are sent to `syslog` asynchronously. During normal operation, if the size of the message queue reaches the value set for this parameter, no new messages are added until the size of the queue decreases below the maximum size you have specified. If the logging level is set to `DEBUG`, however, this policy's value is automatically multiplied by a factor of 4 to allow additional messages to be logged.

The value must be a positive integer. For example: 256

Setting this parameter to zero (0) disables the message queue, and causes all log messages to be written to the `syslog` facility synchronously. In most cases, disabling the message queue degrades system performance, and in extreme cases, may cause a dead lock with the `syslog` daemon during log rotations. Therefore, Centrify recommends that you never set this parameter value to 0.

This group policy modifies the `log.queue.size` setting in the agent configuration file. If this parameter is not defined in the configuration file, its default value is 256 KB.

Set NIS audit logging facility

Specify the `syslog` facility to use for logging `adnisd` operations.

You can separately enable `syslog` facilities for logging general `adclient` messages, `adclient` auditing messages, and `adnisd` messages.

Select a value for this group policy from the list box, which contains a list of valid `syslog` facilities, for example, `auth`, `authpriv`, `daemon`, `security`, `user`, `local n`, and so on. The available facilities may vary depending on the operating system. The default value is `auth`.

If this group policy is not enabled, the audit messages are logged in the facility defined for the Set general audit logging facility policy.

This group policy modifies the `logger.facility.adnisd` setting in the agent configuration file.

Rather than using the policy to set the facility, you can edit the agent configuration file to set the `logger.facility.adnisd` parameter to any valid `syslog` facility. For example, you can set this parameter to log messages to one of `auth`, `authpriv`, `daemon`, `security`, `local n` facilities, and so on.

Login settings

Use the group policies under **Login Settings** to control the following login and local account configuration options:

- Allow localhost users
- Allow offline login when user account is locked out
- Enabled nss emergency shell
- Manage login filters
- Set minimum group ID (lookup)
- Set minimum user ID (lookup)
- Set sync mapped users
- Specify group names to ignore
- Specify the certificate files to add (lookup)
- Specify the fingerprints of certificate files to ignore (lookup)
- Specify user names to ignore
- Split large group membership

Allow localhost users

Specify user names that should be allowed to authenticate locally when logging in.

This group policy is used to ensure that an account mapped to an Active Directory user can still access a system locally if there are problems with the network, the Active Directory server, or the agent.

If you select **Enabled** for this group policy, the users you specify can log in locally by appending `@localhost` to the user name. For example, if you specify the root user, you would log in as `root@localhost`.

This group policy modifies the `pam.allow.override` setting in the agent configuration file.

Note This group policy and the `pam.allow.override` configuration parameter are not supported on AIX computers. There is no equivalent policy or parameter for controlling local access on AIX computers.

Note If you are using a Solaris machine with the Name Switch Cache Daemon (NSCD) running, you will not be able to log in as an override user using `<username>@localhost`.

Allow offline login when user account is locked out

Use this group policy to specify whether to allow a user to log in to a machine that is in disconnected mode if their account is locked.

If this policy is set to **Disabled**, or **Not configured**, by default, users with locked accounts cannot access a disconnected machine.

This group policy modifies the `secdit.system.access.lockout.allowofflinelogin` parameter in the agent configuration file.

Enabled nss emergency shell

Use this group policy to specify whether to use the default login shell when a user or group attempting to access the computer is not allowed to log on.

The default no-login shell and its location is typically platform-specific. For example, on Red Hat Linux the default shell for users who are denied access is:

```
/sbin/nologin
```

If this policy is **Disabled** or **Not configured**, by default, the `nologin` shell specified in the agent configuration file by the configuration parameter, `nss.shell.nologin`, is returned.

This group policy modifies the `nss.shell.emergency.enabled` parameter in the agent configuration file.

Manage login filters

Specify the users and groups allowed to log in to the system. With this policy, you can explicitly list either:

- Users and groups who are allowed to log in (all other users and groups are denied)
- Users and groups who should be denied access (all others are allowed)

When you enable this policy, you can select either the **allow** or **deny** option, then specify a list of user names, a list of group names, or both.

You can specify a list of users or groups in either of these ways:

- Enter a comma-separated list of users, groups, or both in the appropriate text boxes.
- Click the **List** button, then **Add**, to browse for and select users or groups to allow or deny.

Depending on your selections when you configure this group policy setting, the policy can modify any of the following configuration parameters in the agent configuration file:

`pam.allow.groups`

`pam.allow.users`

`pam.deny.groups`

`pam.deny.users`

Note This group policy does not support one-way, cross-forest groups.

Set minimum group ID (lookup)

Specify the lowest group ID that is looked up in Active Directory.

Note This group policy does not apply to agent versions 4.1 or later. If you are using 4.1 or later, use the [Specify group names to ignore](#) group policy to explicitly identify user groups that are always treated as local.

This group policy modifies the `nss.mingid` setting in the agent configuration file.

Set minimum user ID (lookup)

Specify the lowest user ID that is looked up in Active Directory.

Note This group policy does not apply to agent versions 4.1 or later. If you are using 4.1 or later, use the [Specify user names to ignore](#) group policy to explicitly identify user names that are always treated as local.

This group policy modifies the `nss.minuid` setting in the agent configuration file.

Set sync mapped users

Synchronize the Active Directory password for local mapped users. When you enable this policy for a mapped user, if the user changes their Linux, UNIX, or Mac OS X password with the `passwd` command, or with a similar command, PAM changes the password to match in the local Linux, UNIX, or Mac OS X account. In this way, if there are problems with the network, Active Directory, or `adclient`, local users can still log into the machine.

Note This policy has no effect on Mac OS X computers.

To log in as a local user, append `@localhost` to the username. For example, log on as:

```
root@localhost
```

After enabling this policy, click **Browse** to search for users to add.

For this policy to work:

- The specified user must be a mapped user configured in `centrifdc.conf` with the `pam.mapuser` parameter.
- Either the Centrify or Microsoft password synchronization service must be installed on all domain controllers.
- The zone to which the machine belongs must be configured to support agentless clients.
- The Active Directory user to whom the local user is mapped must have a profile in the zone configured for agentless authentication.

This group policy modifies the `pam.sync.mapuser` setting in the agent configuration file.

Specify group names to ignore

You can enter the list of local group names that aren't stored in Active Directory and separate each name with a space. The service will then use this list to disable looking up Active Directory account information for the specified groups. Ignoring this list of groups results in faster name lookups for system user accounts, such as tty and disk.

You can also specify a file that lists the usernames by entering the file: keyword and a file location. For example:

```
file:/etc/centrifydc/group.ignore
```

When you enable this policy, you can select the location where the group name list is populated. The default setting is "Populate group names to centrifydc.conf".

If you select "Populate group names to centrifydc.conf", this group policy modifies the nss.group.ignore setting in the Centrify DirectControl configuration file (centrifydc.conf).

If you select "Populate group names to group.ignore", this group policy modifies the nss.group.ignore setting in centrifydc.conf as "file:/etc/centrifydc/group.ignore", and populates all configured group names to the group.ignore file. If you enter the file: keyword and a file location instead of the list of group names, this policy restores the ignore file /etc/centrifydc/group.ignore with the default list.

Note: The selection of the populating location was added after Centrify DirectControl Agent version 5.6. If you're using version 5.5 or earlier, the agent ignores the population location setting and populates the user names to centrifydc.conf.

Specify the certificate files to add (lookup)

Define a list of certificate files which will be included in the certgp.pl install, if found.

It can be a list of certificates to be added. For example:

```
gp.mappers.certgp.pl.additional.cafiles: <ca-file> <ca-  
file> ...
```


.....

It can also point to a file that contains a list of certificate files to be added. For example:

```
gp.mappers.certgp.pl.additional.cafiles:  
file:/etc/centrifydc/cert_included.list
```

The default value is empty.

This group policy modifies the `gp.mappers.certgp.pl.additional.cafiles` setting in the agent configuration file.

Specify the fingerprints of certificate files to ignore (lookup)

Define a certificate list which will be excluded from the `certgp.pl` install, if matched.

It can be a list of fingerprints of the certificates to be excluded. For example:

```
gp.mappers.certgp.pl.exclude.cacerts: <fingerprint>  
<fingerprint> ...
```

It can also point to a file that contains a list of fingerprints of the certificates to be excluded. For example:

```
gp.mappers.certgp.pl.exclude.cacerts:  
file:/etc/centrifydc/cert_excluded.list
```

The default value is empty.

Specify user names to ignore

You can enter the list of local user names that aren't stored in Active Directory and separate each name with a space. The service will then use this list to disable looking up Active Directory account information for the specified users. Ignoring this list of users results in faster name lookups for system user accounts, such as `tty` and `disk`.

You can also specify a file that lists the usernames by entering the file: keyword and a file location. For example:

```
file:/etc/centrifydc/user.ignore
```

• • • • •

When you enable this policy, you can select the location where the user name list is populated. The default setting is "Populate user names to centrifydc.conf".

If you select "Populate user names to centrifydc.conf", this group policy modifies the `nss.user.ignore` and `pam.ignore.users` settings in the Centrify DirectControl configuration file (`centrifydc.conf`).

If you select "Populate user names to user.ignore", this group policy modifies the `nss.user.ignore` and `pam.ignore.users` settings in `centrifydc.conf` as `"file:/etc/centrifydc/user.ignore"`, and populates all configured user names to the `user.ignore` file. If you enter the `file:` keyword and a file location instead of the list of user names, this group policy restores the ignore file `/etc/centrifydc/user.ignore` with the default list.

Note: The selection of the populating location was added after Centrify DirectControl Agent version 5.6. If you're using version 5.5 or earlier, the agent ignores the population location setting and populates the user names to `centrifydc.conf`.

Split large group membership

Specify whether you want to split up or truncate large groups. In operating environments that don't support large groups, commands that return group information may fail or return incomplete results when a group has a membership list that exceeds the maximum size allowed. Typically, the maximum size allowed for groups is 1024 bytes, which is roughly equivalent to 125 users. If you have large groups that exceed the 1024-byte limit, you can set this parameter to `true` to have those groups automatically split into multiple groups when they reach the maximum size.

The default value is `true` for Solaris, HP-UX, and IRIX but `false` for all other operating environments.

Note This policy has no effect in Mac OS X environments.

This group policy modifies the `nss.split.group.membership` setting in the agent configuration file.

MFA Settings

Use the group policies under **MFA Settings** to control the following multi-factor authentication configuration options.

Enable multi-factor authentication for autozone and classic zone

Specify whether multi-factor authentication is **Enabled** for a classic zone or an Auto Zone. If you enable this policy, you can specify which Active Directory users and groups require multi-factor authentication to log on to their computers or to use privileged commands using the following group policies:

- Specify AD users that require multi-factor authentication
- Specify AD groups that require multi-factor authentication

This policy does not affect multi-factor authentication settings in hierarchical zones.

Before enabling this policy, you should be aware that multi-factor authentication relies on the infrastructure provided by the Centrify identity platform and the cloud-based Centrify identity service.

Multi-factor authentication is disabled by default.

This group policy modifies the `adclient.legacyzone.mfa.enabled` configuration parameter in the agent configuration file.

Note that on computers running Centrify Express agents, you must set this policy using the configuration parameter. Group policies are not supported for Express agents.

Set background fetch interval for groups that require multi-factor authentication

Use this group policy to specify how often the Centrify agent updates the cache with the list of users and groups in classic zones and Auto Zones that require multi-factor authentication, as well as the list of rescue users.

• • • • •

This is a background process that updates the cache periodically according to the interval specified (in minutes).

To disable this process, set the interval value to 0.

The default policy value is 30 minutes.

Note On computers running Centrify Express agents, you must set this policy using the configuration parameter. Group policies are not supported for Express agents.

This group policy modifies the `adclient.legacyzone.mfa.background.fetch.interval` configuration parameter in the agent configuration file.

Specify Centrify Identity Platform tenant ID for multi-factor authentication

Use this policy to specify the Centrify Identity Platform tenant ID for multi-factor authentication.

This policy applies to Auto Zones and classic zones only.

You can get the Centrify Identity Platform tenant ID from your service registration.

This policy modifies the `adclient.legacyzone.mfa.tenantid` setting in the agent configuration file.

Specify AD users that can login when multi-factor authentication is unavailable

Use this policy to specify rescue users who can log on to computers in a classic zone or an Auto Zone when multi-factor authentication is required, but the agent cannot connect to the Centrify cloud service.

You should specify at least one user account for this policy to ensure that someone can access the computers in the event that multi-factor authentication is unavailable.

If you enable this policy, you can specify users by name in the following formats:

- SAM account name: sAMAccountName
- SAM account name of a user in a different domain: sAMAccountName@domain
- User Principal Name: name@domain
- Canonical Name: domain/container/cn
- Full DN: CN=commonName,...,DC_domain_component, DCdomain_component
- An asterisk (*), which includes all Active Directory users

By default, this policy does not specify any rescue users.

This group policy modifies the `adclient.legacyzone.mfa.rescue.users` configuration parameter in the agent configuration file.

Specify AD groups that require multi-factor authentication

Specify the Active Directory groups in classic zones or Auto Zones that are required to use multi-factor authentication to log on or use privileged commands.

For example, if you want to require all members of the Qualtrak Admin group to use multi-factor authentication when they log on to computers that host sensitive information, you can specify that group in this policy. Groups specified in this parameter must be security groups. Distribution groups are not supported.

If you enable this policy, you can specify groups by name in the following formats:

- sAMAccountName
- sAMAccountName@domain
- domain/container/cn

By default, no groups are required to authenticate using multi-factor authentication.

Note On computers running Centrify Express agents, you must set this policy using the configuration parameter. Group policies are not supported for Express agents. This group policy modifies the

Note `adclient.legacyzone.mfa.required.groups` configuration parameter in the agent configuration file.

Specify AD users that require multi-factor authentication

Specify the Active Directory users in classic zones or Auto Zones that require multi-factor authentication to log on or use privileged commands.

If you enable this policy, you can specify users by name in the following formats:

- `SAMAccountName`
- `SAMAccountName@domain`
- `userPrincipalName@domain`
- `domain/container/cn`
- `CN=commonName,...,DC=domain_component,DC=domain_component`
- An asterisk (*), which includes all Active Directory users

By default, no users are required to authenticate using multi-factor authentication.

Note On computers running Centrify Express agents, you must set this policy using the configuration parameter. Group policies are not supported for Express agents.

This group policy modifies the `adclient.legacyzone.mfa.required.users` configuration parameter in the agent configuration file.

Specify Centrify Identity Platform URL for multi-factor authentication

Specify which Centrify identity platform instance URL the agent will access in order to implement multi-factor authentication for users in classic zones and Auto Zones.

Enable this policy if you have access to more than one instance URL. If you have multiple instance URLs and do not specify which one the agent should use for multi-factor authentication, MFA will fail.

If you only have a single platform instance URL for all of the connectors in your Active Directory forest, the agent will use this URL for multi-factor authentication by default, and you do not need to enable this policy.

• • • • •

When specifying a cloud URL, the URL should be in the following format:

```
https://tenantid.domainfqdn:port/
```

For example:

```
https://abc0123.mydomain.com:443/
```

Note that on computers running Centrify Express agents, you must set this policy using the configuration parameter. Group policies are not supported for Express agents.

This group policy modifies the `adclient.legacyzone.mfa.cloudurl` configuration parameter in the agent configuration file.

Network and cache settings

Use the group policies under **Network and Cache Settings** to control connection timeout and object expiration intervals.

Blacklist DNS DC hostnames

Specify a list of domain controllers to filter out when resolving the domain controller for the agent to contact through DNS. Set this policy to prevent the agent from attempting to contact a domain controller that you know is inaccessible, for example, because it resides behind a firewall, or from contacting a domain controller that is inappropriate because of its physical location, or because it is no longer a valid domain controller for the site.

To specify a domain controller, select **Enabled**, then click **Add** and enter the fully qualified name of a domain controller. For example:

```
wink2-admin13@ajax.com
```

You may enter only one controller at a time. To remove a controller from the list, select it and click **Remove**.

This group policy modifies the `dns.block` setting in the agent configuration file.

Enable LDAP cross-forest search

Specify whether to allow the Centrify agent to query trusted domains and forests for transitive trust information. If you enable this policy by selecting the **LDAP Cross-Forest Search** box, the agent generates a `krb5.conf` that includes information from all trusted forests and can be used to authenticate cross-forest users to Kerberos applications. If you disable this policy, the agent does not query external trusted domains or forests for information.

By default, the configuration parameter set by this policy is **Enabled**.

Querying external trusted forests can take a significant amount of time if the other forests are blocked by firewalls. You may want to set this parameter to

• • • • •

false if your trust relationships, network topology, or firewalls are not configured properly for access.

This group policy modifies the `adclient.ldap.trust.enabled` setting in the agent configuration file.

Enable user lookup and login by CN

Specify whether you want to allow users to be found by their common name (cn) attribute.

By default, Centrify allows users to login using their Linux, UNIX, or Mac OS X profile name. In addition, Linux and Unix users can use their Active Directory `displayName` or Active Directory `cn` attribute (default value is disabled for Mac OS X users). Allowing users to log on using these additional attributes can require the agent to perform multiple searches to locate a user account in Active Directory. In environments with domain controllers under heavy load or with large user populations, searching Active Directory multiple times may negatively impact performance.

If you want to prevent the Centrify agent from attempting to access to user information by the common name, you can disable this policy.

This group policy modifies the `adclient.user.lookup.cn` setting in the agent configuration file.

Enable user lookup and login by displayName

Specify whether you want to allow users to be found by their display name (`displayName`) attribute.

By default, Centrify allows users to login using their Linux, UNIX, or Mac OS X profile name. In addition, Linux and Unix users can use their Active Directory `displayName` or Active Directory `cn` attribute (default value is disabled for Mac OS X users). Allowing users to log on using these additional attributes can require the agent to perform multiple searches to locate a user account in Active Directory. In environments with domain controllers under heavy load or with large user populations, searching Active Directory multiple times may negatively impact performance.

• • • • •

If you want to prevent the Centrify agent from attempting to access to user information by the display name, you can disable this policy.

This group policy modifies the `adclient.user.lookup.display` setting in the agent configuration file.

Force DNS to use TCP

Force all DNS requests to use TCP rather than UDP. The initial size of the buffer is determined by the Set DNS UDP buffer size group policy (if you have enabled it), but the size will be increased, if necessary, for a specific response.

This group policy modifies the `dns.forcetcp` setting in the agent configuration file.

Force DNS to rotate

Force all DNS queries to rotate through the list of servers in the `/etc/resolv.conf` file.

This group policy modifies the `dns.rotate` setting in the agent configuration file.

Force switching to different domain controller in the preferred site periodically

This group policy specifies whether to force LDAP binding to be refreshed even if the current binding is to a local (preferred) Active Directory site. Under some conditions, binding to a different site can help facilitate load balancing between servers. However, in environments with many machines joined to a large domain, binding to a new domain controller can cause serious performance problems because the agent must entirely rebuild the cache.

If you set this policy to **Enabled**, the agent will attempt to connect to another local domain controller when the period specified in the configuration parameter, `adclient.binding.refresh.interval` expires.

• • • • •

If this policy is set to **Disabled** or **Not configured**, by default, the agent will not attempt to connect to another domain controller if it is already connected to a preferred Active Directory site.

This group policy modifies the `adclient.binding.refresh.force` parameter in the agent configuration file.

Set cache negative life time

Specify the maximum time, in minutes, a negative object should remain in the cache. A negative object is returned when an object is not found in a search result. This policy determines how long that negative result should remain in the cache, regardless of the object type or object expiration time. By storing this negative result in the cache, the agent does not need to connect to Active Directory to look for an object that was previously not found.

The default period of time for keeping negative results is 5 minutes. Setting the policy value to 0 keeps negative objects in the cache indefinitely.

This group policy modifies the `adclient.cache.negative.lifetime` setting in the agent configuration file.

Set DNS cache size (deprecated)

Use this group policy with agent versions earlier than 4.5. This feature was deprecated starting with agent version 4.5.

Specify the unique number of DNS requests that can be cached by `adclient`. Set this value to approximately 10 times the number of unique domains in the forest.

This group policy modifies the `adclient.dns.cache.size` setting in the agent configuration file.

Set DNS cache timeout

Use this group policy with agent versions 4.5 and later. With agent versions earlier than 4.5, use the **Set DNS cache timeout (deprecated)** group policy.

• • • • •

Specify the maximum time, in seconds, before a cached DNS response expires. The default value is 300 seconds.

This group policy modifies the `dns.cache.timeout` setting in the agent configuration file.

Set DNS cache timeout (deprecated)

Use this group policy with agent versions earlier than 4.5. This feature was deprecated starting with agent version 4.5. With agent versions 4.5 and later, use the **Set DNS cache timeout** group policy.

Specify the maximum time, in seconds, before a cached DNS response expires. The default value is 300 seconds.

This group policy modifies the `adclient.dns.cache.timeout` setting in the agent configuration file.

Set DNS UDP buffer size

Specify the maximum size of a UDP request in bytes. If the response is larger than this size, switch to TCP. If you have set the Force DNS to use TCP policy (`dns.forcetcip` parameter), the value you set here for the UDP buffer is the initial size of the TCP request buffer; the size will automatically be increased, if necessary, for a specific response.

The default value is 4096; the minimum is 512.

This group policy modifies the `dns.max.udp.packet` setting in the agent configuration file.

Set domain DNS refresh interval (deprecated)

Use this group policy with agent versions earlier than 4.5. This feature was deprecated starting with agent version 4.5.

Specify the number of minutes between DNS updates. Specify a positive integer. The default value is 15 minutes.

This group policy modifies the `adclient.dns.update.interval` setting in the agent configuration file.

Set GC expiration

Specify the maximum time, in seconds, that Distinguished Names are kept in the global catalog cache.

This group policy modifies the `adclient.cache.expires.gc` setting in the `centrifydc.conf` configuration file. By default, this parameter is set to 3600 seconds (1 hour).

Set group object expiration

Specify the maximum time, in seconds, that a group object is kept in the local cache.

This group policy modifies the `adclient.cache.expires.group` setting in the agent configuration file. By default, this parameter is not defined in the configuration file, in which case, the value is determined by the [Set object expiration](#) group policy. If Set object expiration is not enabled, the default value is 3600 seconds (1 hour).

Set idle client timeout

Specify the maximum time, in seconds, to wait before the agent closes a connection to an inactive client.

Note You must restart `adclient` for this policy to take effect.

This group policy modifies the `adclient.client.idle.timeout` setting in the agent configuration file.

Set LDAP connection timeout

Specify the maximum time, in seconds, for the agent to wait for a connection to an LDAP server to be established.

This group policy modifies the `adclient.ldap.socket.timeout` setting in the agent configuration file.

Set LDAP response timeout

Specify the maximum time, in seconds, for the agent to wait for a response from an LDAP server.

This group policy modifies the `adclient.ldap.timeout` setting in the agent configuration file.

Set LDAP search timeout

Specify the maximum time, in seconds, that the Active Directory Client Service will wait for a search response from an LDAP server.

This group policy modifies the `adclient.ldap.timeout.search` setting in the agent configuration file.

Set LDAP trust timeout

Specify the maximum number of seconds to wait for responses from external forests and trusted domains when attempting to determine trust relationships. If your trusted domains and forests are widely distributed, have slow or unreliable network connections, or are protected by firewalls, you may want to increase the value for this parameter to allow time for the agent to collect information from external domains and forests. The default value, if you do not set this policy, is 5 seconds.

This group policy modifies the `adclient.ldap.trust.timeout` setting in the agent configuration file.

Set LRPC response timeout

Specify the maximum time, in seconds, for an LRPC client to wait for a response.

This group policy modifies the `lrpc.timeout` setting in the agent configuration file.

Set LRPC2 receive timeout

Specify the maximum time, in seconds, for the agent to wait to receive data coming from a client request.

The default value is 30 seconds.

This group policy modifies the `adclient.lrpc2.receive.timeout` setting in the agent configuration file.

Set LRPC2 send timeout

Specify the maximum time, in seconds, for the agent to wait for reply data to be sent in response to a client request.

This group policy modifies the `adclient.lrpc2.send.timeout` setting in the agent configuration file.

Set maximum server connection attempts

Specify the maximum number of servers per domain the agent should attempt to connect to before going into disconnected mode. This policy is used if the agent is unable to connect to its primary domain controller to enable it to query DNS for a list of other domain controllers and try each server in the list up to the maximum number of servers you specify. For example, if you have a large number of replica domain controllers for a given domain, you may want to use this policy to limit the number of servers for the agent to try in order to limit network traffic and improve performance.

The value should be a positive integer or 0. Setting the value to 0 means that the agent attempts to connect to every server in the list until successful.

The default value is 0.

This policy is ignored if you have defined a master domain controller for the zone to which the computer belongs because the computer only connects to that domain controller.

This group policy modifies the `adclient.server.try.max` setting in the agent configuration file.

This setting is deprecated for versions of `adcli` from 4.4.3 to 5.0.x. It is available in version 5.1.0 and later.

Set object expiration

Specify the maximum time, in seconds, before an object in the local cache expires. This expiration period applies to any object for which you have not set an object-specific expiration time, except [Set GC expiration](#), which has its own default value.

This group policy modifies the `adcli.cache.expires` setting in the agent configuration file. The default is 3600 seconds (1 hour).

Set refresh interval for access control cache

Specify the maximum number of minutes to keep information from the authorization store cached before it expires.

The authorization store is an Active Directory object that stores the rights, roles, and role assignments that the privilege elevation service uses to control access to `dzdo` privileged commands, `dzsh` restricted environments, and PAM-enabled applications. Because the agent handles connecting to and retrieving information from Active Directory, this configuration parameter controls how frequently `adcli` retrieves the privilege elevation service set of information from Active Directory if any such data has been modified in Active Directory.

If local account management is enabled, this group policy also specifies how often `etc/group` and `etc/passwd` are updated on UNIX and Linux computers, based on the local group and local user settings that you configure in Access Manager.

If this policy is not **Enabled**, the default is 30 minutes.

Starting with agent version 5.1.3, this group policy modifies the `adcli.refresh.interval.dz` setting in the agent configuration file.

Note Prior to agent version 5.1.3, this group policy modified the `adcli.azman.refresh.interval` setting. That setting was deprecated in version 5.1.3.

Set UDP timeout

Specify the maximum number of seconds to allow to complete UDP binding. The agent will attempt to bind twice. If the first bind request is not complete within the period specified by this policy, the agent sends a second request with a timeout period that is double the setting of this policy. If both bind requests fail to complete within the allotted time, the agent sets its status to disconnected.

For example, if you set this policy to 10 seconds and the bind request is not complete within 10 seconds, the agent sends a second bind request and waits a maximum of 20 seconds for the bind to complete before assuming the computer is disconnected from the network or Active Directory is unavailable.

The default value for this policy is 15 seconds.

This group policy modifies the `adclient.udp.timeout` setting in the agent configuration file.

Set user object expiration

Specify the maximum time, in seconds, that a user object is kept in the local cache.

This group policy modifies the `adclient.cache.expires.user` setting in the agent configuration file. By default, this parameter is not defined in the configuration file, in which case, the value is determined by the [Set object expiration](#) group policy. If Set object expiration is not enabled, the default value is 3600 seconds (1 hour).

Specify AD to NTLM domain mappings

Use the `Specify AD to NTLM domain mappings` group policy to manually map Active Directory domain names to NTLM domains. This parameter is useful when you need to use NTLM authentication and:

- firewalls prevent Kerberos authentication
- firewall constraints prevent the automatic discovery of Active Directory to NTLM domain mapping

To set this group policy, select **Computer Configuration > Centrify Settings > DirectControl Settings > Network and Cache Settings > Specify AD to NTLM domain mappings**.

Provide the following information for the group policy:

- One or more pairs with ActiveDirectory domain name and NTLM domain name.
- Optionally, provide a file with a list of AD to NTLM domain name pairs. Include the file location. Use separate lines for each pair in the file. For example:

```
AJAX.ORG:AJAX
FIREFLY.COM:FIREFLY
HR1.FIREFLY.COM:HR1
```

After you defined the mapping of Active Directory domains to NTLM domains, you can specify the list of domains that use NTLM authentication instead of Kerberos authentication. Use either the group policy, **Specify NTLM authentication domains** or the configuration parameter, [pam.ntlm.auth.domains](#).

Alternative to using this group policy, **Specify AD to NTLM domain mappings**, you can use the `adclient.ntlm.domains` configuration parameter.

Specify DNS DC hostnames

Specify the domain controller host names if your DNS is not configured to use Active Directory. In most cases, you should not use this group policy in a production environment because Active Directory automatically updates DNS with fail-over and replica servers optimized for the Active Directory site configuration. This group policy is used primarily for configuring an evaluation environment when the DNS server is on a Linux, UNIX, or Mac OS X computer and can't provide the `_ldap` service records.

The domain controller name must be resolvable using either DNS or in the local `/etc/hosts` file. Therefore, you must add entries to the local `/etc/hosts` for each domain controller you want to use if you are not using DNS or if the DNS server cannot locate your domain controllers.

To specify DC host names:

• • • • •

After enabling this group policy, click **Add**, then enter the following information:

Domain: The domain name, for example, acme.com.

DC hostnames separated by space: One or more hostnames in the domain, for example, qa1-winxp, admin-winxp

Click **OK** to add the specified hostnames.

You can click **Add** again to add hosts from a different domain.

When you are done, click **OK**.

Once you've added one or more hostnames, you can select an existing domain and click **Edit** or **Remove** to edit or remove the specified hosts.

This group policy modifies the `dns.dc.domain_name` setting in the agent configuration file.

Specify DNS GC hostnames

Specify the domain controller used as the global catalog if your DNS is not configured to use Active Directory. In most cases, you should not use this group policy in a production environment because Active Directory automatically updates DNS with fail-over and replica servers optimized for the Active Directory site configuration. This group policy is used primarily for configuring an evaluation environment when the DNS server is on a Linux, UNIX, or Mac OS X computer and can't provide the `_gc` service records.

The domain controller name must be resolvable using either DNS or in the local `/etc/hosts` file. Therefore, you must add entries to the local `/etc/hosts` for each domain controller you want to use if you are not using DNS or if the DNS server cannot locate your domain controllers.

To specify GC hostnames:

After enabling this group policy, click **Add**, then enter the following information:

Domain: The domain name, for example, acme.com.

• • • • •

GC hostnames separated by space: One or more hostnames in the domain, for example, qa1-winxp, admin-winxp

Click **OK** to add the specified hostnames.

You can click **Add** again to add hosts from a different domain.

When you are done, click **OK**.

Once you've added one or more hostnames, you can select an existing domain and click **Edit** or **Remove** to edit or remove the specified hosts.

This group policy modifies the `dns.gc.domain_name` setting in the agent configuration file.

NIS daemon settings

Use the group policies under **NIS daemon** to control the operation of the Centrif Network Information Service (`adnisd`) on the local host computer. The Centrif Network Information Service provides a mechanism for the agent to respond to NIS client requests from computers not managed by Centrif agents.

Set thread number for NIS daemon

Specify the number of threads that may run simultaneously for the Centrif Network Information Service (`adnisd`) on the local computer.

After enabling the policy, type a number or use the arrow keys to select a value. You must specify an integer between 1 - 200 inclusive. If you type a value outside this range, it is automatically reset to a valid number when you click **OK** or **Apply**.

The default value is 4 threads.

This group policy modifies the `nisd.threads` setting in the agent configuration file.

Specify NIS daemon update interval

Specify the interval, in seconds, that the `adnisd` daemon waits between connections to Active Directory. At each interval, the `adnisd` daemon connects to Active Directory, gets the latest NIS maps for the local computer's zone, and updates its local NIS map data store.

The value must be an integer equal to or greater than zero. If the value is zero, then the update interval is disabled and the local NIS map data store is not updated. For example, to set the interval for getting NIS maps to 1 hour:

3600

If this group policy is not enabled, the default interval is 30 minutes (1800 seconds).

• • • • •

This group policy modifies the `nisd.update.interval` setting in the agent configuration file.

Specify allowed NIS mapping files for NIS daemon

Specify the name of the NIS maps currently available for NIS service. When the `adnisd` daemon connects to Active Directory, it retrieves the list of NIS maps available for the local computer's zone, creates a local map data store, and updates this configuration parameter, if necessary, to indicate the maps retrieved. If any NIS client requests a map that is not in the list specified by this group policy, the daemon refuses the request.

Enter a list of valid NIS map names, separated by spaces. You must explicitly specify the base maps and the derived maps. For example, to make the `netgroup` maps available but no other maps, enable this group policy and specify the following maps:

```
netgroup netgroup.byhost netgroup.byuser
```

If this group policy is not defined, all NIS maps found in Active Directory are retrieved and available for service.

This group policy modifies the `nisd.maps` setting in the agent configuration file.

Specify disallowed NIS mapping files for NIS daemon

Specify the name of the NIS maps you want to prevent the NIS service from using in response to NIS clients. This group policy enables you to exclude specific maps rather than explicitly specifying the maps you want to make available. For example, if you have a large number of `automount` maps or other network information that you want to make available to NIS clients but do not want to use agentless authentication, you can use this parameter to exclude the `passwd` and `group` maps but respond to `automount` or `netgroup` requests.

Enter a list of valid NIS map names, separated by spaces. Note that this policy excludes the named map and all derived maps; for example:

```
group passwd
```

• • • • •

If you do not enable this group policy, all NIS maps found in Active Directory are retrieved and available for service. This group policy overrides the setting of the Specify allowed NIS mapping files for NIS daemon.

This group policy modifies the `nisd.exclude.maps` setting in the agent configuration file.

Specify allowed client machines for NIS daemon

Specify a list of one or more subnets from which the daemon will accept NIS requests. You enable this group policy to restrict access to the Centrify Network Information Service by IP address. NIS requests that do not come from the IP addresses specified in this group policy are refused by the `adnisd` daemon.

You do not need to specify the local IP address for this group policy. The Centrify Network Information Service will always accept local NIS client requests.

The value must include both the specific IP address or subnet and the subnet mask, separated by a forward slash. For example:

192.168.111.0/255.255.255.0

You can specify multiple IP addresses by separating each IP address-subnet mask pair with a comma or a space. For example:

192.68.11.0/255.255.255.0,192.147.10.0/255.255.255.0

If this group policy or the parameter it modifies is not defined in the configuration file, only local NIS client requests are accepted by the `adnisd` process. When you enable this group policy, the default value is 0/0 to allow all machines.

This group policy modifies the `nisd.securenets` setting in the agent configuration file.

Set switch delay time for NIS daemon

Specify how long, in seconds, to wait before loading maps from a backup domain controller when the connection to the primary domain controller is lost. If the Centrify Network Information Service is unable to connect to its

• • • • •

primary Active Directory domain controller, it will respond to NIS client requests using information in the local cache until the switch to the backup domain controller is complete.

The value must be an integer equal to or greater than zero. If the value is zero, then the delay is disabled. For example, to set the delay period to 2 hours, enter:

7200

If group policy is not enabled, the default delay for switching to the backup domain controller is ten minutes (600 seconds).

This group policy modifies the `nisd.server.switch.delay` setting in the agent configuration file.

Set maximum number of mapping files allowed for NIS daemon

Specify the number of alternate sets of NIS maps to retain. A new set of NIS maps is normally created when `adnisd` switches to an alternate domain controller. Keeping these alternate sets of maps allows Centrify Network Information Service to more efficiently switch between domain controllers.

You must specify an integer value greater than zero. The default is 2 map sets.

This group policy modifies the `nisd.maps.max` setting in the agent configuration file.

Set large group suffix for NIS daemon

Specify the suffix string or character to use in group names when automatically splitting up a group with a large number of members.

Because `group.bygid` and `group.byname` NIS maps often contain membership lists that exceed the 1024 limit of NIS data that can be served to clients, the `adnisd` process automatically truncates the membership list when this limit is reached. When you enable this group policy, the Centrify Network Information Service automatically splits a large group into as many new groups as needed to deliver the complete membership list.

When a group's data size exceeds the 1024 data limit, a new group is created. The new group name is formed using the original group name, followed by the

• • • • •

string defined for this policy, and ending in a number that represents the numeric order of the new group created.

For example, for a large group named `performix-worldwide-corp`, a suffix string defined as `-all`, and the maximum length for group names as 10, the `performix-worldwide-corp` group membership is split into these multiple groups:

```
performix-worldwide-corp-all1
performix-worldwide-corp-all2
performix-worldwide-corp-all3
performix-worldwide-corp-all4
```

All of the new groups have the same group identifier (GID) as the original group. If the new group names would exceed the maximum length for group names on a platform, you can use the `Set large group name length for NIS daemon group policy` to set the maximum length for the new groups created.

If this policy is not enabled, the `adnisd` process truncates the group membership list such that each group entry is under 1024 characters.

This group policy modifies the `nisd.largegroup.suffix` setting in the agent configuration file.

Set large group name length for NIS daemon

Specify the maximum number of characters to use in group names when groups with a large number of members are split into multiple new groups. Because some devices that submit NIS requests have limitations on the length of group names, you can use this parameter to specify the maximum length for group names.

When the `adnisd` process splits the group membership for a large group into multiple smaller groups, it truncates the original group name as needed to append the suffix defined in the `Set large group suffix for NIS daemon group policy` and not exceed the number of characters specified by this group policy. For example, if you have a large group named `worldwide-all-corp`, and have defined the suffix string as `-all` and the maximum length for group names as 10, when the `worldwide-all-corp` group membership is split into multiple groups, the groups are named as follows:

```
world-all1
```

.....

world-all2

world-all3

world-all3

If this group policy is not enabled, the maximum group name length is 1024 characters by default.

This group policy modifies the `nisd.largename.length` setting in the agent configuration file.

Set domain name for NIS daemon

Specify the NIS domain name for the `adnisd` process to use when communicating with NIS clients.

If you do not enable this group policy, the zone name is used by default.

This group policy modifies the `nisd.domain.name` setting in the agent configuration file.

Set startup delay time for NIS daemon

Specify the maximum time (in seconds) that `adnisd` will wait before answering NIS requests. If this policy is not enabled, `adnisd` begins answering requests only after all maps have been loaded or created, or when the default value, 180 seconds is reached, whichever comes first. If you set this policy, `adnisd` will begin answering NIS requests no later than the specified delay, as follows:

Before the delay time is reached, if all maps have not been loaded or created, requests are blocked waiting for the specified delay.

Once the delay time is reached, requests are answered whether all maps are loaded or not. Be aware that clients may receive partial or empty answers to their requests.

If all maps are loaded or created before the delay time is reached, `adnisd` will immediately begin answering requests.

Specify a value between 0 and 100000. If you enable the policy and do not change the value, the default is 180 seconds.

• • • • •

This group policy modifies the `nisd.startup.delay` setting in the agent configuration file.

NSS overrides

Use the group policies under **NSS Overrides** to override entries in the local `/etc/passwd` or `/etc/group` files. These group policies provide additional access control and account configuration options on the computers where the policies are applied.

Specify NSS group overrides

Specify the group override entries you want to use in place of the entries in the local `/etc/group` file. You can use these settings to provide fine-grain control of the groups that can use the computer and to override the group ID for specific group accounts.

This group policy modifies the `nss.group.override` setting in the agent configuration file.

This group policy allows define filters to control the groups that can access a local computer. You can also use the override controls to modify the information for specific fields in each group entry on the local computer. For example, you can override the group ID or member list for a specific group on the local computer without modifying the group entry itself.

The syntax for overriding group entries is similar to the syntax used for overriding NIS. You use `+` and `-` entries to allow or deny access for specific groups on the local computer. Additional fields correspond to the standard `/etc/group` fields separated by colons (`:`).

Note If you don't specify override information for a field, the information from the local `/etc/group` file is used. You cannot specify override information for the password hash field, however. Any changes to this field in the override file are ignored and do not affect Centrify user passwords.

If you select **Enabled** for the **Specify NSS group overrides** group policy, you can type a comma-separated list of the override entries you want inserted into the override file, `group.ovr`, using the following format for each entry:

```
+zone_group_name:group_name:group_password:group_id:member_list
```

• • • • •

```
-zone_group_name:group_name:group_password:group_id:member_
list
```

For example, you can specify entries similar to the following:

```
+users:::
+admins:::jdoh,bsmith,frank
+ftusers:ftp::300:
-webusers
+:::
```

For more information about overriding group entries, see the sample group override file `/etc/centrifydc/group.ovr`.

Specify NSS password overrides

Specify the `passwd` override entries you want to use in place of the entries in the local `/etc/passwd` file. You can use these settings to provide fine-grain control of the users and groups who can use the computer and to override the user ID, group ID, default shell, or home directory for specific login accounts.

This group policy modifies the `nss.passwd.override` setting in the agent configuration file.

This group policy allows you to define filters to control access to a local computer. You can also use override controls to modify the information for specific fields in each `/etc/passwd` entry on the local computer. For example, you can override the user ID, primary group ID, default shell, or home directory for specific login accounts on the local computer without modifying the account entry itself.

The syntax for overriding `passwd` entries is similar to the syntax used for overriding NIS. You use `+` and `-` entries to allow or deny access for specific users on the local system. Additional fields correspond to the standard `/etc/passwd` fields separated by colons (`:`).

Note If you don't specify override information for a field, the information from the local `/etc/passwd` file is used. You cannot specify override information for the password hash field, however. Any changes to this

.....

field in the override file are ignored and do not affect Centrify user passwords.

If you select **Enabled** for the **Specify NSS password overrides** group policy, you can type a comma-separated list of the override entries you want inserted into the override file, `passwd.ovr`, using the following format for each entry:

```
+zone_username:username:password:uid:gid:GECOS:home_
directory:shell

-zone_username:username:password:uid:gid:GECOS:home_
directory:shell
```

For example, you can specify entries similar to the following:

```
+mike:::::::::/usr/local/ultrabash
+jane@arcade.org:jdoe::300:300::
+@sysadmins::::::::
-ftp
+@staff::::::::
+@rejected-users:::767:767:::/sbin/nologin
```

In the example above, the @ symbol denotes an Active Directory name. The name can be an Active Directory group name, a Centrify zone name, or some other container name. You can also specify an Active Directory user principal name (UPN) instead of the zone name.

Entries in the override file are evaluated in order from first to last with the first match taking precedence. This means the system will only use the first entry that matches a particular user. For example, if the user `cruz` is a member of both the `staff` group and the `rejected-users` group and you have defined the override entries as listed in the example above, the `cruz` user account is allowed to log on to the computer because the `staff` entry is evaluated and matched before the `rejected-users` entry. If the order were reversed in the override file, the `cruz` account would be flagged as a `rejected-users` account and denied access.

It is important, therefore, to consider the order in which you list the override entries in the group policy configuration. The order you use to specify the entries in the group policy is the order used when the entries are inserted into the override file.

• • • • •

Changes to the NSS password override entries only affect the entries inserted through the group policy. You can also manually create or update override entries in the override file on any local computer, if needed. Changes made to manually inserted or edited entries do not affect the entries maintained through the NSS Overrides group policies.

For more information about overriding passwd entries, see the sample password override file `/etc/centrifydc/passwd.ovr`.

PAM settings

Use the group policies under **Pam Settings** to control a computer's PAM configuration.

Create home directory

Control whether a home directory should be created automatically when a new user logs on to a system for the first time.

This group policy should not be applied to computers that use NFS to mount home directories. By default, if this group policy is not configured, home directories are automatically created when new Active Directory users log on to a system for the first time except on Solaris computers.

If you do not want the Centrify agent to automatically create user home directories, select **Disabled**. This group policy modifies the `pam.homedir.create` setting in the agent configuration file.

Create k5login

Create a `.k5login` file automatically in a user's home directory the first time the user logs on.

The `.k5login` file is used to enable Kerberos authentication and single sign-on in PAM-aware applications.

If you want Centrify agent to automatically create the `.k5login` file in the user's home directory, select **Enabled**. This group policy modifies the `pam.create.k5login` setting in the agent configuration file.

Set home directory permissions

Set the default read, write, and execute permissions on new home directories.

• • • • •

This group policy specifies the default permissions to assign a user's home directory if a new home directory is created for the user on the local computer.

If you want to set the permissions on the user's home directory, select **Enabled** then specify an octal value. For example, to give read, write, and execute permissions on the home directory to the user and no other permissions, type:

```
0700
```

This group policy modifies the `pam.homedir.perms` setting in the agent configuration file. The default value is 0755 on Mac OS X computers and 0700 on all other platforms.

Set multi-factor authentication to use an external PAM module

This policy specifies the PAM application you want to use for multi-factor authentication if you are not using the Centrify PAM module and Centrify Privileged Access Services

By default, the Centrify PAM module and Centrify Privileged Access Services are used to provide multi-factor authentication. This group policy allows you to specify the name of another PAM module if you would prefer to use a different multi-factor authentication provider.

This group policy modifies the `pam.mfa.module.name` setting in the agent configuration file.

Set options for multi-factor authentication by an external PAM module

Specify the options to use if multi-factor authentication is done by an external PAM application.

Note Parameters must be separated by a space.

This group policy modifies the `pam.mfa.module.options` setting in the agent configuration file.

Set UID conflict message

Specify the message displayed if a user identifier (UID) conflict is detected during login. This message is displayed if there is a local user with the same UID but a different user name than the Active Directory user logging on.

When the message is displayed, the %d token in the message string is replaced with the UID of the conflicting local account. The message string you define must contain exactly one %d token, and no other string replacement (%) characters.

For example:

```
Account with conflicting UID (%d) exists locally
```

This group policy modifies the `pam.account.conflict.uid.mesg` setting in the agent configuration file.

For information about what to do when local conflicts are detected, see [Set UID conflict resolution](#).

Set UID conflict resolution

Control how the Centrify agent responds if a user logs on with an Active Directory account and either the Active Directory user name or Active Directory UID conflicts with a local user account.

The purpose of detecting a duplicate user name or duplicate UID is to prevent an Active Directory user from signing on and receiving privileges to modify files created by a different local user.

If you select **Enabled** for this group policy, you can choose one of the following options:

- **ignore** — Do not report duplicate user names or UID conflicts. If detected, log the conflict at the info level if logging is enabled.
- **warn** — Warn the user of the user name or UID conflict after a successful login. Log the conflict at warning level if logging is enabled. This is the default value.
- **error** — Report UID conflict to user after user name is entered. Don't accept password. Don't allow log in. Log conflict at error level.

• • • • •

This group policy modifies the `pam.uid.conflict` setting in the agent configuration file.

Set user name and UID conflict message

Specify the message displayed if there are both user name and user ID conflicts detected during login. This message is displayed if there are two local account conflicts. For example, this message is displayed if there is a local user and the Active Directory user that have the same UID but different user names, and there is also another local account with the same user name as the Active Directory user but the two accounts have different UID values.

When the message is displayed, the `%s` token in the message string is replaced with the name of the first conflicting local account, and the `%d` token is replaced with the UID of the second conflicting local account. The message string you define must contain exactly one `%s` token and exactly one `%d` token, in that order, and no other string replacement (`%`) characters.

For example:

```
Accounts with conflicting name (%s) and UID (%d) exist  
locally
```

This group policy modifies the `pam.account.conflict.both.mesg` setting in the agent configuration file.

For information about what to do when local conflicts are detected, see [Set UID conflict resolution](#).

Set user name conflict message

Specify the message displayed if a user name conflict is detected during login. This message is displayed if there is a local user with the same user name but a different UID than the Active Directory user logging on.

When the message is displayed, the `%s` token in the message string is replaced with the name of the conflicting local account. The message string you define must contain exactly one `%s` token, and no other string replacement (`%`) characters.

For example:

```
Account with conflicting name (%s) exists locally
```

• • • • •

This group policy modifies the `pam.account.conflict.name.msg` setting in the agent configuration file.

For information about what to do when local conflicts are detected, see [Set UID conflict resolution](#).

Specify message for creating home directory

Specify the message to display when a user's home directory is created.

For example:

```
Creating home directory ...
```

This group policy modifies the `pam.homedir.create.msg` setting in the agent configuration file.

Specify NTLM authentication domains

Use the `Specify NTLM authentication domains` group policy to specify the list of domains that use NTLM authentication instead of Kerberos authentication.

This group policy enables you to authenticate users behind a firewall when the Kerberos ports are blocked, but a trust relationship exists between domains inside and outside the firewall.

For example, use this group policy to specify that the Active Directory domains `AJAX.ORG` and `FIREFLY.COM`, which are outside of the firewall with a one-way trust to the forest inside the firewall, use NTLM authentication.

To set this group policy, select **Computer Configuration > Centrify Settings > DirectControl Settings > Pam Settings > Specify NTLM authentication domains**.

Provide the following information for the group policy:

- One or more fully-qualified Active Directory domain names.
- The Active Directory domain names that are mapped to NTLM domain names.

These can be mapped automatically or manually:

- automatically, if the firewall does not prevent the mapping from being discovered.
- manually, if the firewall prevents the mapping from automatically being discovered, by modifying the contents of the `/etc/centrifydc/domains.conf` file.

To manually configure the mapping use either the group policy, **Specify AD to NTLM domain mappings**, or the configuration parameter, `adclient.ntlm.domains`.

Alternative to using this group policy, **Specify NTLM authentication domains**, you can use the configuration parameter, `pam.ntlm.auth.domains`.

Specify programs for which multi-factor authentication is ignored

Specify which PAM applications are exempt from multi-factor authentication.

For example, if you have a role with the login-all PAM application right and have selected the “Multi-factor authentication required” system right, you can use this group policy to bypass multi-factor authentication for programs that don’t support it. You can also add program names to this list to skip multi-factor authentication when you want to make specific exceptions to the MFA requirement.

By default, programs which are known to be unable to support multi-factor authentication are included in the list. For example, multi-factor authentication is ignored by default for the `xscreensaver` and `vsftpd` programs.

Note Program names must be separated by a space.

This group policy modifies the `pam.mfa.program.ignore` setting in the agent configuration file.

Password prompts

Use the group policies under **Password Prompts** to customize the prompts displayed when Active Directory users are prompted to provide their password.

Set account disabled error message

Customize the text displayed during login if a user is denied access because the user's account is disabled. This group policy modifies the `pam.account.disabled.mesg` setting in the agent configuration file.

Set account expired error message

Customize the text displayed during login if a user is denied access because the user's account has expired.

This group policy modifies the `pam.account.expired.mesg` setting in the agent configuration file.

Set account locked message for adpasswd

Customize the text displayed by the `adpasswd` program when users cannot change their password because their account is locked. This group policy modifies the `adpasswd.account.disabled.mesg` setting in the agent configuration file.

Set adclient inaccessible message

Customize the message displayed during password change, for a local Linux, UNIX, or Mac OS X user who is mapped to an Active Directory account, when the agent (`adclient`) is not accessible. This group policy modifies the `pam.adclient.down.mesg` setting in the agent configuration file.

Set password change disallowed message for adpasswd

Customize the text displayed by the adpasswd program when users are not allowed to change their password because password change for these users has been disabled in Active Directory. This group policy modifies the `adpasswd.password.change.disabled.mesg` setting in the agent configuration file.

Set invalid user or password message for adpasswd

Customize the text displayed by the adpasswd program when a user enters an account name that is not recognized or an invalid password. This group policy modifies the `adpasswd.account.invalid.mesg` setting in the agent configuration file.

Set permission denied message for adpasswd

Customize the text displayed by the adpasswd program when a user cannot change another user's password because of insufficient permissions. This group policy modifies the `adpasswd.password.change.perm.mesg` setting in the agent configuration file.

Set lockout error message

Customize the text displayed when a user account is locked out. This group policy modifies the `pam.account.locked.mesg` setting in the agent configuration file.

Set error message for empty password entered

Customize the text displayed when a user enters an empty password. Empty passwords are not allowed. This group policy modifies the `pam.password.empty.mesg` setting in the agent configuration file.

Set new password's mismatch error message for password change

Customize the text displayed during password change when the new passwords entered do not match. This group policy modifies the `pam.password.new.mismatch.mesg` setting in the agent configuration file.

Set notification text for password change

Customize the text displayed when Active Directory users attempt to change their password. This group policy modifies the `pam.password.change.mesg` setting in the agent configuration file.

Set old password incorrect error message for password change

Customize the text displayed during password change when the old password entered is incorrect. This group policy modifies the `pam.auth.failure.mesg` setting in the agent configuration file.

Set violation error message for password change

Customize the text displayed during password change if the operation fails because of a domain password policy violation. For example, if the user attempts to enter a password that doesn't contain the minimum number of characters or doesn't meet complexity requirements, this message is displayed. This group policy modifies the `pam.policy.violation.mesg` setting in the agent configuration file.

Set password prompt for confirming new password change

Customize the text displayed when Active Directory users are prompted to confirm their new password. This group policy modifies the `pam.password.confirm.mesg` setting in the agent configuration file.

Set password prompt for new password change

Customize the text displayed when Active Directory users are prompted to provide their new password. This group policy modifies the `pam.password.new.mesg` setting in the agent configuration file.

Set password prompt for old password change

Customize the text displayed when Active Directory users are prompted to provide their old password. This group policy modifies the `pam.password.old.mesg` setting in the agent configuration file.

Set message text for password change

Customize the text displayed when Active Directory users enter the correct password but must change the password immediately. This group policy modifies the `pam.password.change.required.mesg` setting in the agent configuration file.

Set login password prompt

Customize the text displayed when Active Directory users attempts to log in. This group policy modifies the `pam.password.enter.mesg` setting in the agent configuration file.

Set password expiry approaching text

Customize the text displayed when the account password is approaching the expiration date. The message is displayed when the expiration date is within the limit defined by the `pam.password.expiry.warn` parameter. In the message, use the `%d` token for the number of days until expiration.

This group policy modifies the `pam.password.expiry.warn.mesg` setting in the agent configuration file.

• • • • •

Set workstation denied error message

Customize the text displayed during login if a user is denied access because of a workstation restriction. This group policy modifies the `pam.workstation.denied.mesg` setting in the agent configuration file.

Sudo settings

Use the group policies under **Sudo Settings** to specify whether users must re-authenticate with sudo after logging out.

Forcesudo re-authentication when relogin

Specify whether users must authenticate again with sudo after logging out.

When a user authenticates with sudo, a ticket is temporarily created that allows sudo to run without re-authentication for a short period of time. If a user logs out and the ticket is not cleared, the ticket is reused when the user logs back in, and the user does not need to re-authenticate. If a user logs out and the ticket is cleared, the user must re-authenticate with sudo when logging back in.

Starting with release 2015, the way that you configure whether re-authentication is required depends on the `tty_tickets` parameter in the sudoers configuration file (`/etc/sudoers.conf`). In some situations, re-authentication requirements are also controlled by this policy. Details are as follows:

- If `tty_tickets` is enabled, tickets are always removed when a sudo user logs out, regardless of whether this policy is enabled or disabled. That is, when `tty_tickets` is enabled, this policy has no effect, and sudo users must always re-authenticate.
- If `tty_tickets` is disabled, the requirement for sudo users to re-authenticate is controlled by this policy and the `adclient.sudo.clear.passwd.timestamp` setting in the agent configuration file.

Tickets are cleared and sudo re-authentication is required in the following scenarios:

- The `tty_ticket` parameter in the sudoers configuration file is enabled (it is enabled by default)
- The `tty_ticket` parameter in the sudoers configuration file is disabled and this group policy is enabled

• • • • •

- The `tty_ticket` parameter in the `sudoers` configuration file is disabled and the `adclient.sudo.clear.passwd.timestamp` parameter is set to `true`

Tickets are not cleared and `sudo` re-authentication is not required in the following scenarios:

- The `tty_ticket` parameter in the `sudoers` configuration file is disabled and this group policy is disabled
- The `tty_ticket` parameter in the `sudoers` configuration file is disabled and the `adclient.sudo.clear.passwd.timestamp` parameter is set to `false`

By default, this policy clears tickets in the `/var/run/sudo` directory. To clear tickets in a different directory, use the `adclient.sudo.timestampdir` parameter in the agent configuration file as described in the *Configuration and Tuning Reference Guide*. This group policy modifies the `adclient.sudo.clear.passwd.timestamp` setting in the agent configuration file.

Windows Settings

Use the group policies under **Centrify Settings > Windows Settings > Common Settings** to control the configuration of Centrify agents on Windows computers.

Common Settings

Use the group policies under **Centrify Settings > Windows Settings > Common Settings** to control Centrify-managed Windows computers.

Configure Windows authentication user privilege elevation grace period

You can use this group policy to configure the Windows authentication grace period (in minutes) for user privilege elevation, such as run as role, run with privilege, new desktop, and switch desktop.

This per-session grace period starts when the user performs a successful privilege escalation in the session and the grace period is restarted. If the group policy is set to:

- **Enabled:** the grace period for privilege elevation is configured in the group policy.
- **Disabled:** the grace period for privilege elevation is disabled.
- **Not Configured:** the grace period for privilege elevation is not enabled and a local policy can override the setting.

Custom message for locked user accounts

Use the Custom message for locked user accounts policy to customize the message that will be shown to the user when the user tries to log into a locked user account.

- If this policy is set to **Enabled**, an administrator can specify the message that will be shown to the user when the user tries to log into a locked user account. The credential provider shows the message if the message is specified (not empty).
- If this policy is set to **Disabled** or **Not Configured**, you will see the same message as the windows credential provider.

The group policy "Custom message for locked user accounts" only changes the message for the console logon or remote logon without Network Level Authentication (NLA). If you log on remotely with NLA, Remote Desktop Client will block logon with its message.

Disable automatic enrollment of Windows devices

You can use this group policy to disable the otherwise automatic enrollment of Windows devices with the Centrify Identity Services Platform.

There are two settings for this group policy:

- By default, when this policy is **Disabled** or **Not Configured**, it will automatically enroll the device with Centrify Identity Services Platform as a corporate-owned device.
- When this policy is **Enabled**, it does not automatically enroll the device with the Centrify Identity Services Platform.

Note If this policy is set to Enabled, you can't enroll a personal device as such even if the Enable enrollment as personal device group policy is set to Enabled.

Disable the Centrify notification icon

Disable the Centrify icon in the notification area of the Windows task bar for users that are not assigned any roles, or for machines that are not joined to a

• • • • •

domain.

Enable enrollment as personal device

You can use this group policy to enable devices to be enrolled as a personal device.

There are two settings for this group policy:

- By default, when this policy is **Disabled** or **Not Configured**, users cannot enroll the computer or device as a personal device.
- When this policy is **Enabled**, users can enroll the computer or device as a personal device.

Note If the Disable automatic enrollment of Windows devices group policy is enabled, then this policy has no effect and users cannot perform enrollment as a personal device.

Enable setup Centrify offline MFA profile

Use this group policy to enable setup of Centrify offline MFA profile.

There are two settings for this group policy:

- When this policy is **Enabled** or **Not Configured**, you can set up the passcode for multi-factor authentication. A passcode can be used to fulfill multi-factor authentication in the event the computer cannot connect to the Centrify Identity Platform.
- When this policy is **Disabled**, you cannot setup an offline MFA profile.

Enable use of alternate user's role to run an application

You can use this group policy to use an alternate user's role to run an application. The alternate user's credential is required when you use an alternate user's role. This policy does not apply to the `runasrole` command-line interface.

There are two settings for this group policy:

- By default, when this policy is **Disabled** or **Not Configured**, the user can run an application with only their user role.
- When this policy is **Enabled**, the user can use another user's role to run an application.

Hide command line arguments in Analytics

You can use this group policy to hide command line arguments from Analytics Data (RunWithPrivilege Events)

There are two settings for this group policy:

- By default, when this policy is **Enabled** or **Not Configured**, the Analytics Data does not show the command line arguments.
- If this policy is set to **Disabled**, the Analytics Data shows the command line arguments.

Prevent local administrators from being able to log on in rescue mode (when there are no explicit rescue users defined)

Use this policy to prevent local administrators that are not defined rescue users from logging in to a machine that is running in rescue mode or Windows Safe Mode.

If you set this policy to **Enabled**, you should add users and groups to the rescue user list by issuing them the rescue user role, or a custom role with the rescue user system right selected.

If you are not joined to a zone (because your computers are not managed by Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service), you can enable the group policy, [Specify a list of rescue users \(when the agent is not joined to a zone\)](#), and add users to the rescue user list.

By default, if this policy is set to **Disabled** or **Not Configured**, all local administrators are able to log in without multi-factor authentication when the machine is running in rescue or safe mode.

Re-authentication: Require smart card

Enable this policy to require Windows users to re-authenticate using a smart card.

By default, this setting is disabled.

Require justification on privilege elevation

You can use this group policy to require any user to provide a reason when they operate with elevated privileges, such as run with privilege, run as role, and new desktop.

This group policy works in conjunction with the [Specify a privilege elevation validator](#) policy. If you only set one of these policies, any affected user is prompted to provide a reason for privilege escalation.

There are two settings for this group policy:

- By default, when this policy is **Disabled** or **Not Configured**, users can run with elevated privileges as normal.
- When this policy is **Enabled**, the agent prompts the user with a justification dialog box, where the user can provide a reason category and a text string for the reason.

Also, if you've configured your system to work with a ticketing system such as ServiceNow, you can use the [Specify a privilege elevation validator](#) group policy to validate the ticket number that the user enters.

You can view the reason information that users enter in the audit trail event.

You can use this group policy with loopback mode, so that you can apply the policy based on the computer that a user logs into. For more details about loopback mode, see the Microsoft documentation, such as the following page:

<https://support.microsoft.com/en-us/help/231287/loopback-processing-of-group-policy>

Specify a list of blacklisted domains

Enable this group policy to specify a list of domains that will be ignored by the Centrify Agent.

After enabling this policy, enter one or more domain names, separated by a comma, in the following format:

`domain1.com, domain2.com, ..., domainN.com`

If the root domain of a trusted forest is specified in this list, all of its leaf domains will also be ignored.

By default, if this policy is set to **Not configured**, no domains are blacklisted.

Specify a list of rescue users (when the agent is not joined to a zone)

If the agent is not joined to a zone (because your computers are not managed by Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service), use this policy to specify a list of users who can log in without using multi-factor authentication if the machine is running in rescue mode or Windows Safe Mode.

The user name can be specified in any of the following formats:

- `SAMAccountName`
- `SAMAccountName@domain` (if the account is not in the current domain).
- `UserPrincipalName@domain`
- An asterisk (*), which includes all Active Directory users.

You can enter the list of users separated by a comma, for example:

`joe, janedoe, user1, user2@domain.com.`

By default, if this policy is set to **Disabled** or **Not configured**, only local administrators can log on in rescue mode or safe mode. However, if you enable [Prevent local administrators from being able to log on in rescue mode \(when there are no explicit rescue users defined\)](#), and do not enable this policy, no one will be able to log in if the computer is running in these modes.

Specify a list of whitelisted domains

Enable this group policy to specify a list of domains that will be trusted and processed by the Centrify Agent. If you enable this policy, **only** these domains will be trusted.

After enabling this policy, enter one or more domain names, separated by a comma, in the following format:

```
domain1.com, domain2.com, ..., domainN.com
```

You must specify the root domain on this list if you specify any of its leaf domains.

By default, if this policy is set to **Not configured**, all domains are trusted and processed by the Centrify Agent.

Specify endpoint enrollment desktop notification message

You can use this group policy to specify the endpoint enrollment desktop notification message.

There are two settings for this group policy:

- **Enabled** or **Not Configured**: The default endpoint enrollment desktop notification message appears.
- **Disabled**: When this policy is disabled, the endpoint enrollment desktop notification message will not appear.

Specify offline MFA profile desktop notification message

Use this group policy to specify conditions for the offline MFA profile desktop notification message.

There are two settings for this group policy:

- **Enabled** or **Not Configured**: The user-specified offline MFA profile desktop notification message appears.
- **Disabled**: The offline MFA profile desktop notification message does not appear.

Specify a privilege elevation validator

You can use this computer configuration group policy to validate ticket information that a user enters when she provides a ticket number along with a privilege elevation reason. You can validate ticket information using a customized PowerShell script against a ticketing system, such as ServiceNow.

If you enable this policy, here are some important things to know:

- Centrify provides a sample script that you can use as a starting point for your own script. At the minimum, you need to enter your ServiceNow URL for the `$url` parameter. You can get the sample script from github: in the `centrify-agent-windows` repo, go to `Samples > ITSM validation > servicenow`.
- If the ticket ID is not validated successfully, the user's request for elevated privilege is rejected.
- The custom PowerShell script must be available and accessible on each Windows computer where the validation occurs. If you're not running the PowerShell script on a local computer, be sure to allow remote PowerShell access for the script.
- This group policy works in conjunction with the [Require justification on privilege elevation](#) policy. If you only set one of these policies, any affected user is prompted to provide a reason for privilege escalation.
- If the script cannot validate the ticket entry within the specified timeout duration, then the validation fails. By default, the timeout value is 2 minutes.

Please consult the group policy explain text for more details.

There are two settings for this group policy:

- By default, when this policy is **Disabled** or **Not Configured**, users can run with elevated privileges as normal.
- When this policy is **Enabled**, you specify the PowerShell script filename and users entries are validated against the third-party ticketing system before granting privileged access.

You can view the reason information that users enter in the audit trail event.

Specify whether to keep the desktop notification permanently visible

Use this group policy to specify whether to keep the desktop notification message visible at all times.

The desktop notification message shows what roles are currently being used by the user and may be helpful to remind those using privileged desktops which elevated privileges they are authorized to use for that desktop. Select **Enabled** to keep the message visible.

If this policy is **Disabled**, or **Not configured**, by default, the notification message will fade a few seconds after clicking the Centrify icon in the system notification tray.

MFA Settings

Use the group policies under **Centrify Settings > Windows Settings > MFA Settings** to control multi-factor authentication on Centrify-managed Windows computers.

Configure multi-factor authentication for logon when the agent cannot connect to the Platform

You can use this group policy to configure offline multi-factor authentication for users that are required to use multi-factor authentication to log on to their computers in the event that the agent cannot connect to the Centrify Identity Platform.

There are three configuration possibilities:

- If an offline MFA profile is setup, prompt for offline MFA. Otherwise don't allow to proceed.
- If an offline MFA profile is set up, prompt for offline MFA. Otherwise, allow to proceed and remind user to set up the offline MFA profile.
- Allow to proceed. Don't prompt for offline MFA.

If this policy is set to **Disabled** or **Not Configured**, the default is the second option.

Configure multi-factor authentication for privilege elevation when the agent cannot connect to the Platform

You can use this group policy to configure offline multi-factor authentication for users that are required to use multi-factor authentication to use elevated roles in the event that the agent cannot connect to the Centrify Identity Platform.

There are three configuration possibilities:

- Only users who have set up an offline MFA profile will be prompted for offline multi-factor authentication for privilege elevation. Users who have not set up an offline passcode will not be able to proceed.
- If an offline MFA profile is set up, prompt for offline MFA. Otherwise, allow the user to proceed and remind them to set up the offline MFA profile.
- Users can use elevated rights or roles when their machine is offline without multi-factor authentication.

If this policy is set to **Disabled** or **Not Configured**, the default is the first option.

Connect to the Centrify Identity Platform directly

Connect to the Centrify identity platform directly without using a web proxy or a connector as a web proxy. If you enable this policy, you must configure the client to be able to connect to the cloud service.

Continue with MFA Challenges after failed Windows authentication in logon screen

Configuring this policy setting allows you to continue with MFA challenges, even with a failed Windows authentication.

Note The following is recommended for PCI DSS or NIST 800-53 guidelines for multi-factor or multi-step authentication.

If this policy is set to **Enabled**, authentication on the Windows logon screen continues with MFA challenges with the wrong password or use of expired/locked out/disabled accounts.

Note Specify multi-factor authentication grace period is disabled when this policy is enabled.

If this policy is set to **Disabled** or **Not Configured**, authentication on Windows logon screen fails immediately when you enter the wrong password and the MFA challenges are not triggered. To continue to the second MFA challenge when previous challenge response failed, use the policy "Continue with additional challenges after failed challenge" in the Centrify Portal.

Disable multi-factor authentication for screen unlock

Use this policy to disable multi-factor authentication for the Windows lock screen. When multi-factor authentication is required to log on to a Windows machine, by default, users must also use multi-factor authentication to unlock the Windows lock screen. If this policy is set to **Enabled**, users that require multi-factor authentication to log on will not have to use multi-factor authentication to unlock the Windows lock screen.

If this policy is set to **Disabled** or **Not configured**, the default is to require users to use multi-factor authentication to unlock the Windows lock screen.

Disable self-service password reset

You can use this group policy to allow the administrator to force disabling of the password reset feature. There are two settings for this group policy:

- **Enabled:** If this policy is set to **Enabled**, the self-service password reset feature on the machine is disabled, including the cloud-enabled self-service password reset.
- If this policy is set to **Disabled** or **Not Configured**, the self-service password reset feature on the machine follows the cloud policy setting (cloud policy settings can be found at: **Policy Settings > User Security Policies > Self Service > Password Reset**). The cloud policy settings are accessed through the Centrify Administrator Portal.

Note The admin portal is available after you log in to a Centrify identity platform instance.

Enable multi-factor authentication for Windows login (when the agent is not joined to a zone)

Use this policy to enable multi-factor authentication for Windows login when the agent is not joined to a zone.

If this policy is set to **Disabled** or **Not configured**, the default is that no user is required to use multi-factor authentication to log in.

Force to enter explicit UPN

Configure this policy setting to force all users that require MFA to log in to the machine using the UPN format of: user@domain.com. There are two settings for this group policy:

- If this policy is set to **Enabled**, all users that require MFA must log in using the UPN format, otherwise an error message appears "Invalid User. Please use format user@domain.com and try again."

Note All users that do not require MFA can log in using either the UPN format or NT account format.

- If this policy is set to **Disabled** or **Not Configured**, all users can log in using either the UPN format or NT account format.

Send UUID for MFA Challenges

Configure this group policy to enable the DirectAuthorize Agent to send user UUID with the user UPN for the MFA challenges.

- If this policy is set to **Enabled**, DirectAuthorize Agent sends the user UUID as addition field with the user UPN for the MFA challenges.
- If this policy is **Disabled** or **Not Configured**, DirectAuthorize Agent sends only the UPN for the MFA Challenges.

Skip client certificate authentication

Use this group policy to skip client certificate authentication to the Centrify Identity Platform if client certificate authentication is disabled or blocked by

enterprise policies or proxy settings.

If you enable this policy, you must configure the client to be able to connect directly to the Centrify Connector for multi-factor authentication.

If this policy is set to **Disabled** or **Not configured**, client certificate authentication is required for multi-factor authentication.

Specify a web proxy URL

Specify a web proxy to use to connect to the Centrify identity platform. If you have enabled the client to connect to the cloud service directly, without using a connector or web proxy, enabling this policy has no effect.

Specify Active Directory users that require multi-factor authentication on Windows login (when the agent is not joined to a zone)

Use this policy to specify the Active Directory users that are required to use multi-factor authentication to log on to Windows computers. If you enable this policy, you can specify users by name in the following formats:

- SAMAccountName
- SAMAccountName@domain
- userPrincipalName@domain
- An asterisk (*), which includes all Active Directory users

Use quotes for names containing spaces, for example, "Krusty T. Clown".

By default, no users are required to authenticate using multi-factor authentication.

Specify how frequently to check for responses to multi-factor authentication challenges

Set the polling interval in seconds for checking whether a user has responded to a multi-factor authentication challenge. Some authentication challenges require the client to wait for the user to respond to the challenge.

This value defines how frequently the client checks with the cloud service for a user's challenge response. The lower the value, the faster the client responds.

The minimum value you can specify is 1 second and the maximum value is 300 seconds. If you enable this policy, the default value is 3 seconds.

Specify multi-factor authentication grace period

Use the group policies under **Windows Settings > MFA Settings** to control the multi-factor authentication grace period.

There are two group policies that affect the multi-factor authentication grace period.

- Configure multi-factor authentication lock screen grace period
- Configure multi-factor authentication user privilege elevation grace period

The *Configure multi-factor authentication lock screen grace period* group policy allows the administrator to configure the multi-factor authentication grace period (in minutes) for the lock screen. If the group policy is set to:

- **Enabled:** the grace period for lock screen is enabled and it is configured in the group policy. If this value is configured to 0, it means no grace period for MFA in the lock screen.
- **Disabled:** the grace period for lock screen is disabled.
- **Not Configured:** the grace period for lock screen is not enabled and a local policy can override the setting.

The *Configure multi-factor authentication user privilege elevation grace period* group policy allows the administrator to configure the multi-factor authentication grace period for user privilege elevation, such as run with privilege and add new desktop. This per-session grace period starts when the user performs a successful MFA challenge in the session and the grace period is restarted. If the group policy is set to:

- **Enabled:** the grace period for privilege elevation is configured in the group policy.
- **Disabled:** the grace period for privilege elevation is disabled.

- **Not Configured:** the grace period for privilege elevation is not enabled and a local policy can override the setting.

Specify the authentication source for privilege elevation

Use this policy to specify the authentication source for privilege elevation. You can choose either multi-factor or RADIUS authentication.

If this policy is set to Enabled, agents will use the configured source for privilege elevation multi-factor authentication.

If this policy is set to Disabled, you cannot use another authentication source for privilege elevation multi-factor authentication.

If this policy is set to Not Configured, you can configure another authentication source locally on the agent.

Specify the Centrify connector URL to use

Specify the Centrify connector to use.

You should specify the URL with a fully-qualified domain name and port number. For example, if using a secure HTTP (HTTPS) connection, type an entry similar to the following:

```
https://acme.example.com:8080/
```

If you enable and apply this policy, you must also enable and apply the policies to specify the cloud instance URL and, if applicable, the web proxy URL.

If you don't configure this policy, the cloud instance URL will automatically locate an available connector to use by default.

Specify the connection timeout for multi-factor authentication requests

Use this group policy to set the connection timeout for multi-factor authentication requests. This policy defines the number of seconds to wait before the request times out.

.....

If you enable this policy, the minimum value you can specify is 1 second, and the maximum value is 100 seconds.

If this setting is set to **Not Configured**, the default value is 15 seconds.

Specify credential providers to exclude from the logon screen

Use this group policy to list specified credential providers to exclude from the login options on the Windows login screen when users access the machine remotely.

You must list the Class Identifiers (CLSID) for the providers you would like to exclude. For example, to exclude the Windows Password Provider and the Smartcard Credential Provider on machines running Windows 8 or later and Windows Server 2012 or later, you would enter the following:

```
{60b78e88-ead8-445c-9cfd-0b87f74ea6cd},{8FD7E19C-3BF7-489B-A72C-846AB3678C96}
```

To find the CLSIDs for installed credential providers, navigate to the following location in the HKEY_LOCAL_MACHINE registry:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
```

If this policy is set to **Disabled** or **Not configured**, only the Windows Password credential provider will be disabled by default.

Specify the Platform instance Id to use (when the agent is not joined to a zone)

Use this policy to specify the Centrify Identity Platform instance Id (also called a tenant ID) to use when the agent is not joined to a zone.

In most cases, this policy is only required if you have access to multiple platform Ids and want to explicitly specify which platform instance to connect. For example: AAH0305

You can get the Centrify Identity Platform tenant ID from your service registration.

• • • • •

If you're using a version of Access Manager prior to 19.6 and you upgrade your connectors to a version of 19.5 or later, please make sure you manually update the tenant URL to use the .net domain extension after the connector upgrade. Otherwise, MFA will not work and the Centrify Identity Services Platform won't be listed in the agent configuration.

If you're already using a version of Access Manager of 19.6 or later, you can set the tenant ID on the zone. Then when you upgrade your connectors, the agent gets the new tenant URL automatically.

Specify the Platform instance URL to use

Specify the Centrify platform instance URL to use. In most cases, this policy is only required if you have access to multiple cloud instances and want to explicitly specify which instance to connect to.

You should specify the URL using the customer-specific identifier for the cloud instance and a fully-qualified domain name and port number.

For example, if using a secure HTTP (HTTPS) connection, type an entry similar to the following:

```
https://ht150.my-test.centrify.com:443/
```

Specify the Platform instance URL to use (when the agent is not joined to a zone)

Use this group policy to specify which platform instance URL the agent will access for users of computers that are not joined to a zone.

Enable this policy if you have access to more than one instance URL.

If you only have a single authentication server URL for all of the connectors in your Active Directory forest, the agent will use this URL by default, and you do not need to enable this policy.

When specifying a URL, the URL should be in the following format:

```
https://customerid.domainfqdn:port/
```

For example:

```
https://abc0123.mydomain.com:443/
```

Specify the timeout on skipping previously disconnected Centrify connectors

Specify the length of time, in seconds, for the agent to ignore previously disconnected connectors while attempting to connect to the cloud for an authentication request.

You can avoid connection delays by specifying a longer timeout period for previously disconnected connectors. The agent will not attempt to connect with these connectors until the timeout period ends. The minimum value you can specify is 0 seconds and the maximum value is 86400 seconds. The default value is 1800 seconds.

Specify the timeout on using the last successfully connected Centrify connector first

Specify the length of time, in seconds, for the agent to attempt to connect to the cloud using the last successful connector.

The lower you set this value, the faster the agent will try other connectors during the next authentication request. The minimum value you can specify is 0 seconds and the maximum value is 86400 seconds. The default value is 600 seconds.

Remote Authentication Dial-In User Service (RADIUS) Service Settings

Use the group policies under **Centrify Settings > Windows Settings > MFA Settings > Remote Authentication Dial-In Service (RADIUS) Settings** to control Radius multi-factor authentication on Centrify-managed Windows computers.

Enable Remote Authentication Dial-In User Service (RADIUS)

Use this policy to enable Remote Authentication Dial-In User Service (RADIUS) for privilege elevation.

• • • • •

If this policy is set to Enabled, you can use RADIUS for privilege elevation multi-factor authentication.

If this policy is set to Disabled, you cannot use RADIUS for privilege elevation authentication.

If this policy is set to Not Configured, you can enable RADIUS locally on the agent.

Specify the RADIUS connection timeout

Use this policy to specify the connection timeout in seconds for the RADIUS server.

If this policy is set to Enabled, agents will use the configured timeout for authentication.

If this policy is set to Disabled or Not Configured, you can configure the connection timeout locally on the agent.

Specify the RADIUS server IP address

Use this policy to specify the RADIUS server IP address.

If this policy is set to Enabled, agents will use the configured RADIUS server for authentication.

If this policy is set to Disabled or Not Configured, you can configure the RADIUS server IP address locally on the agent.

Specify the RADIUS server port number

Use this policy to specify the RADIUS server port number.

If this policy is set to Enabled, the agent will use the configured port for authentication.

If this policy is set to Disabled or Not Configured, you can configure the RADIUS server port number locally on the agent.

Audit and audit trail settings

This chapter describes the audit-related group policies that are located under **Centrify Audit Trail Settings** and **Centrify Audit Settings**.

Group policies located under **Centrify Audit Trail Settings** allow you to specify both category-specific and global audit trail targets. These group policies are located in subfolders under **Centrify Audit Trail Settings**. See [Audit Trail Settings](#) for details about these group policies.

Group policies located under **Centrify Audit Settings** allow you to configure the auditing agent installation, and platform-specific auditing features. These group policies are located in subfolders under **Centrify Audit Settings**. See [Centrify Audit Settings](#) for details about these group policies.

Alternate location for policies installed with an ADMX template

If Audit Trail group policies are installed using an ADMX template instead of the plugin that the Auditing installer uses, the group policies are installed in this location in GPOE:

Computer Configuration > Policies > Administrative Templates Policy definitions (ADMX files) > Centrify Audit Trail Settings

All of the Audit Trail group policies are located in this folder, including the **Set global audit trail targets** policy.

Audit Trail Settings

There are two locations of audit trail settings:

- Some group policies are located under **Computer Configuration > Centrify Audit Trail Settings**. These policies are provided by the Centrify snap-in extension.
- Additional group policies are located under **Computer Configuration > Administrative Templates > Centrify Audit Trail Settings**. They are in an ADMX template.

Audit trail snap-in policies

For the policies located in Computer Configuration > Centrify Audit Trail Settings:

- There is a subfolder for each category of items that generate an audit trail. For example, Audit Analyzer Settings, Audit Manager Settings, and so forth.
- For global settings, the Centrify Global Settings subfolder contains group policies that affect all settings.
- Within each subfolder, there are 2 group policies:
 - [Send audit trail to Audit database](#)
 - [Send audit trail to log file](#)

You can configure each of these group policies to "Not configured", "Enabled", or "Disabled".

Audit trail ADMX template policies

For the policies located in Computer Configuration > Administrative Templates > Centrify Audit Trail Settings:

- There is one group policy for each category of items that generate an audit trail. For example, "Set audit trail targets for category "Audit Analyzer."
- For global settings, use the "Set global audit trail targets" policy.
- You can configure each of these group policies to to "Not configured", "Enabled", or "Disabled".
- If you enable one of these policies, you also need to specify the value for Audit trail targets and Audit trail targets override. The audit trail targets

and targets override is set within each of the policies (they're not separate policies).

Send audit trail to Audit database

Enable this group policy to specify that audit events for this component — **Audit Analyzer**, **Audit Manager**, and so on—are sent to the active audit store database.

See the **Explain** tab in the group policy for details about which parameter each group policy sets in the agent configuration file.

Send audit trail to log file

Enable this group policy to specify that audit events for this component—such as **Audit Analyzer**, **Audit Manager**, and so on—are sent to the local logging facility (syslog on UNIX systems, Windows event log on Windows systems).

See the **Explain** tab in the group policy for details about which parameter each group policy sets in the agent configuration file.

Audit Trail Overrides

This setting specifies whether to override the global audit trail targets. If this parameter is set, the system uses the targets value in the current component; otherwise, the system uses the global configured value.

There are two target settings that can be overridden:

- Whether the system sends the audit trail information to DirectAudit or not
- Whether the system sends the audit trail information to the local logging system or not. On UNIX systems, the local logging system is syslog and on Windows systems it's the Windows event log.

For this setting, you specify a single numeric value to represent where the system will send the audit trail information. (Setting one value to signify two settings is called a bit mask.) The possible settings are as follows:

Value	Override whether the audit trail information is sent to DirectAudit?	Override whether the audit trail information is sent to the local logging system?	Description
0	No	No	There is no override to the audit trail target of the current component. The system uses the global audit trail target value.
1	Yes	No	The system overrides just the audit trail target for DirectAudit. This capability is supported by DirectAudit version 3.2 and later.
2	No	Yes	The system overrides just the audit trail target for the local logging system. If you're using a DirectAudit version prior to version 3.2, this is the default setting.
3	Yes	Yes	The system overrides both the audit trail targets for DirectAudit and the local logging system. If you're using DirectAudit version 3.2 or later, this is the default setting.

This group policy modifies the `audittrail.<product>.<component>.overrides` settings in the agent configuration file. Each category has its own setting in that file.

Audit Trail Targets

This setting specifies how to calculate where the system sends the audit trail information for a particular component if you have also set the corresponding [Audit Trail Overrides](#) setting.

There are two kinds of audit trail targets that can be specified:

- Whether to enable the DirectAudit audit trail target for the component or not
- Whether to enable the local logging system audit trail target or not. On UNIX systems, the local logging system is syslog and on Windows systems it's the Windows event log.

For this setting, you specify a single numeric value to represent which audit trail targets are enabled for the component. (Setting one value to signify two settings is called a bit mask.) The possible settings are as follows:

Value	Enable the DirectAudit audit trail target for the component?	Enable the local logging audit trail target for the component?	Description
0	No	No	Neither the DirectAudit nor the local logging target are enabled for the component. This is the default setting for the group policy
1	Yes	No	Enable only the DirectAudit audit trail target for the component. This capability is supported by DirectAudit version 3.2 and later.
2	No	Yes	Enable only the local logging audit trail target for the component.
3	Yes	Yes	Enable the audit trail targets for both DirectAudit and the local logging system.

The system calculates the final audit trail targets for a component based on the following information:

- If the Audit Trail Targets Override is not specified, the system uses the global audit trail target value
- If Audit Trail Targets Override is specified, for each target (DirectAudit and local logging), whether the audit trail information will be sent to this target is determined by the following:
 - If the setting is not overridden in with Audit Trail Targets Override, the system uses the global audit trail target value

- If the target is overridden by Audit Trail Targets Override and enabled by Audit Trail Targets, the system sends the audit trail information to this target

This group policy modifies the `audittrail.<product>.<component>.targets` settings in the agent configuration file. Each category has its own setting in that file.

Centrify Audit Settings

Centrify Auditing and Monitoring Service group policies are located in the following subfolders:

- [Common Settings](#)—Contains policies pertaining to the audit installation. See [Common Settings](#) for details about the policies in this node.
- [Collector Settings](#)—Contains policies pertaining to the collector service. See [Collector Settings](#) for details about the policies in this node.
- [DirectAudit advanced monitoring](#)—Contains policies pertaining to advanced monitoring configuration. See [DirectAudit advanced monitoring](#) for policy details.
- [UNIX Agent Settings](#)—Contains sub-nodes for policies pertaining to the Centrify UNIX Agent. See [UNIX Agent Settings](#) for details about the policies in these sub-nodes.
- [Windows Agent Settings](#)—Contains policies pertaining to user lists used by the Centrify agent for Windows. See [Windows Agent Settings](#) for details about the policies in this node.

Common Settings

Use the group policies under **Common Settings** to configure basic operations for the auditing service.

Installation

Use the Installation group policy to specify which installation agents and collectors are part of. By enabling the Installation group policy, you can

prevent local administrators from configuring a computer to be part of an unauthorized installation.

Note After applying the settings through the "Centrify Auditing and Monitoring Service Settings" group policy, you must restart the target agent machine(s) for the policy to take effect.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab of the dialog box, select **Enabled**.
3. Click **Browse** to select the installation you want to secure, then click **OK**.

See the *Auditing Administrator's Guide* for more information about installing and managing installations of the auditing infrastructure.

Set maximum missed status update tolerance

Use the Set maximum missed status update tolerance group policy to specify how many times the auditing agent will fail to connect to a collector before sending a notification that the agent is not joined to a collector. The interval between attempts is 5 minutes.

This group policy modifies the `agent.max.missed.update.tolerance` setting in the agent configuration file.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. Click **Edit**.
3. Select **Enabled**.
4. Enter the value.
For example, enter 3 if you would like the agent to notify you after 3 failed attempts to join a collector.
5. Click **OK**.

If this group policy is Disabled or Not Configured the default value is 4.

This group policy can be used with the [DirectAudit Daemon Settings](#) group policy which allows you to specify the amount of time, in seconds, that the agent waits during each connection attempt before it determines that it cannot connect to a collector.

Set the preferred Audit Store

Use this group policy to specify the preferred audit store that auditing will use in the event that your UNIX or Linux computer has IP addresses that match the criteria for multiple audit stores.

If you have this type of installation and you do not enable this policy and specify the preferred audit store, the collector may not connect to the correct audit store.

This group policy modifies the parameter `preferred.audit.store` in the agent configuration file.

Set video capture auditing of user activity

Use the Set video capture auditing of user activity group policy to specify any agents for which you want to change the video capture settings. This setting can be useful in cases where the user output should not be recorded because of security audit rules. For example, if you have enabled video capture auditing for your entire auditing installation, you can disable video capture for one or more specific agents.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab of the Properties dialog box, select **Enabled**.
3. In the Set video capture auditing section, select one of the following options:
 - **Enable Video Audit:** Select this option to turn on video capture. This setting overrides your installation-wide video capture setting.
 - **Disable Video Audit:** Select this option to turn off video capture. This setting overrides your installation-wide video capture setting.
 - **Use Installation-Wide Setting:** Select this option to make sure that

this agent uses the same setting as what you have set for the entire auditing installation.

4. Click **OK** to save the change.

Use the host name specified by the agent

Enable this group policy to display the real host name of audited computers in the Audited Systems node in Audit Manager instead of the host name resolved by the collector through DNS.

This configuration parameter is useful in configurations where the DNS servers used by the collectors cannot reliably resolve host names from IP addresses. The most common scenarios that might require you to use this configuration parameter are when the agents are in a virtual environment using network address translation (NAT) or in a perimeter network outside of a firewall.

If this group policy is enabled, the host name for the agent is determined by the agent. If this group policy is not enabled, the collector determines the agent's host name based on its IP address. If this group policy is not configured, this setting will be disabled by default.

This group policy modifies the agent . send . hostname setting in the auditing configuration file.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. Click the Edit policy setting link above the policy's Description.
3. Select **Enabled**.
4. Click **OK**.

Collector Settings

Use the group policies under Collector Settings to configure the collector service.

Do not audit output of specified UNIX commands

Use this group policy to specify one or more UNIX commands whose output you do not want to save to in the audit store database.

You can use this group policy to prevent the output from specific UNIX command that you do not want to capture or review from being saved. For example, common UNIX commands, such as the "top" and "tail" commands, might display output that you do not want to capture and store for auditing purposes. To prevent auditing the output for these types of commands, enable this group policy, click Add, then type the command.

The command string you specify must be an exact match. For example, to prevent auditing output of "cat filename", you must specify "cat filename" as the command string in this group policy.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **Add**, type the exact command you want to skip for auditing purposes, then click **OK**.
4. Repeat Step 3 for each command to skip when auditing session activity until you are finished adding commands, then click **OK**.

DirectAudit advanced monitoring

Use the following group policies to generate advanced monitoring for program and process execution on audited machines.

Enabling these group policies will allow you to generate reports that monitor programs and process that are run individually, as part of a script, or within other commands.

You can also configure a file monitor report which details user interaction with sensitive files.

Note You must first enable the group policy, [Enable advanced monitoring](#) to enable any of the other Advanced Monitoring policies.

Enable advanced monitoring

Use this group policy to enable Advanced Monitoring.

If this policy is **Not configured**, by default, Advanced Monitoring is not enabled.

Set monitor of program execution for audit sessions

Use this group policy to enable recording for all programs executed in an audited session. You can export these monitoring events when reviewing a session and they are also recorded in the Detailed Execution reports.

If this policy is **Not configured**, by default, this feature is not enabled.

This group policy modifies the `event.execution.monitor` parameter in the agent configuration file.

Set monitored programs list

Use this group policy to specify a list of programs that will generate an audit trail event when executed by users.

If you enable this policy, all users executing the listed programs will generate an audit trail event, whether they are audited or not, unless the user is specified in [Set skip users for monitored program executions](#).

Note that all commands must be specified with full paths.

If this policy is set to **Disabled** or **Not configured**, by default, no executed programs will generate an audit trail event for any user.

This policy modifies the `event.monitor.commands` parameter in the agent configuration file.

Set monitoring of system configuration files

Use this group policy to enable monitoring of changes made to the system configuration files in the following directory trees:

- `/etc`
- `/var/centrify`
- `/var/centrifyda`
- `/var/centrifydc`

By default, if this policy is set to **Not configured**, or if you enable this policy, all changes made to these system configuration files **will** be monitored.

Set processes that are skipped for system configuration file monitoring

Use this group policy to specify programs that modify configuration files which you do not want to be monitored when [Set monitoring of system configuration files](#) is enabled.

When you enable this policy, you can specify a list of trusted programs that can modify any system configuration files or directories without causing an audit trail event.

If this policy is **Not configured**, `/usr/sbin/daspool` is skipped by default, along with all `adcli`ent and `dad` processes and subprocesses.

Set skip users for monitored program executions

Use this group policy to specify a list of users who can run programs and commands without generating an audit trail event.

Users listed in this policy can run commands without generating an audit trail, even if those commands are listed in [Set monitored programs list](#).

If this policy is **Disabled** or **Not configured**, by default, all users will generate an audit trail event when executing monitored commands.

This policy modifies the `event.monitor.commands.user.skiplist` parameter in the agent configuration file.

Set users that will be skipped for program execution monitoring

Use this group policy to specify a list of audited users that will not generate an audit trail event record, for use in Detailed Execution reports, when they execute programs listed in [Set monitored programs list](#) when it is enabled.

If this policy is **Not configured**, by default, no users are added to this list.

Set users who will be skipped for system configuration file monitoring

Use this group policy to specify a list of users who can modify any system configuration file and directory without generating an audit trail event when [Set monitoring of system configuration files](#) is enabled.

If this policy is set to **Not configured**, by default, only `root` is added to this list.

• • • • •

This policy modifies the `event.file.monitor.user.skiplist` parameter in the agent configuration file.

UNIX Agent Settings

Use the group policy under **UNIX Agent Settings** to set auditing configuration options.

Add `centrifyda.conf` properties

Use this group policy to specify any configuration parameters you want to add to the `centrifyda.conf` configuration file. You can specify any configuration parameter name and its value by using this group policy.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **Add**, type a property name and a property value, then click **OK**.
For example, to change the configuration parameter `autofix.nss.conf` from the default value of `true` to `false`, you would type the following:
 - Property name: `autofix.nss.conf`
 - Property value: `false`
4. Repeat [Collector Settings](#) for each configuration parameter you want to set until you are finished adding property values, then click **OK**.

In typing property names and values, you should note that the agent does not perform any validation or error checking. If you specify an invalid property name or value, the parameter and value are added to the configuration file as entered. In most cases, invalid parameter names are simply be ignored. However, an invalid parameters value might cause unexpected problems when the auditing service runs.

Additional group policies for UNIX Agent Settings are organized under the following sub-nodes:

- **DirectAudit Daemon Settings**—Contains policies that pertain to the auditing service dad process. See [DirectAudit Daemon Settings](#) for details about the policies in this sub-node.
- **DirectAudit NSS Settings**—Contains policies that pertain to authentication requests that are processed or ignored by the Centrify name service switching (NSS) module. See [DirectAudit NSS Settings](#) for details about the policies in this sub-node.
- **DirectAudit Shell Settings**—Contains policies that pertain to the audited shell (cdash). See [DirectAudit Shell Settings](#) for details about the policies in this sub-node.
- **LRPC2 Client Settings**—Contains policies that pertain to LRPC2. See [LRPC2 Client Settings](#) for details about the policies in this sub-node.
- **Spool Disk Space Settings**—Contains policies that pertain to offline database settings. See [Spool Disk Space Settings](#) for details about the policies in this sub-node.

Enable DirectAudit session auditing properties

Use this group policy to enable and disable DirectAudit session auditing.

DirectAudit Daemon Settings

Use the group policies under DirectAudit Daemon Settings to control operations for the auditing service.

Set allow to dump core

Use this group policy to specify whether the dad process is allowed to dump core. If this group policy is enabled, the dad process is allowed to dump core. If this group policy is disabled or not configured, the dad process is not allowed to dump core.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.

2. On the Policy tab of the Properties dialog box, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dad.dumpcore` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Set audit level of ignored user

Use this group policy to specify the audit level of users who are on the ignored user list. Values that you can set in this policy are:

- 0 — Audit if possible.
- 1 — Do not audit.

If this group policy is disabled or not configured, a default value of 0 is used, meaning that the audit level is “audit if possible.” If you enable this group policy is enabled, you can specify a value of 0 or 1.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Set the ignored user audit level to 0 or 1.
4. Click **OK** to save settings in this policy.

This group policy modifies the `user.ignore.audit.level` setting in the `/etc/centrifida/centrifida.conf` configuration file.

Set cache live time

Use this group policy to specify the length of time entries should remain valid in the name service cache. You can specify the maximum number of seconds cached query result should be available in the cache. This policy is applicable only if the `set cache the query results` policy is enabled.

If this group policy is disabled or not configured, a default value of 600 seconds is used. If this group policy is enabled, you can specify the number of seconds.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds that cached information remains valid.
4. Click **OK** to save settings in this policy.

For example, to increase the number of seconds that query results are available in the cache on an audited computer, enable this policy and specify a value of your choice that is greater than 600 seconds.

This group policy modifies the `cache.time.to.live` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set cache the query results

Use this group policy to specify whether the dad process caches name service query results about users and groups.

- If this group policy is disabled, query results are not saved and must be retrieved whenever they are needed.
- If this group policy is enabled or not configured, the dad process stores query results—for example, from user lookup requests—in memory for better performance.
- If this group policy is enabled, you can use the `set max cache size` and `set cache live time` policies to control the number and duration of entries in the cache.
- If this group policy is enabled, you can also use the `daflush` command to clear the cache manually when you want to ensure you get updated information. For example, if you remove the UNIX Login role for an Active Directory user, some information for that user might remain in the cache and be returned when you run a command such as `getent passwd`. You can run `daflush` to ensure that the user is removed completely from the local computer cache, including the auditing name service cache.

To use this group policy:

• • • • •

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `cache.enable` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set check NSS configuration file timeout

Use this group policy to specify how frequently (in seconds) the dad process checks the `/etc/nsswitch.conf` file for changes.

If this group policy is disabled or not configured, a default value of 60 seconds between checks is used. If this group policy is enabled, you can specify the number of seconds between checks.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds between checks.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.timer.monitor.nss.conf` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set client idle timeout

Use this group policy to specify how long (in seconds) the dad client can be idle before timing out. If this group policy is disabled or not configured, a default value of 1800 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.

3. Specify the number of seconds that the dad client can be idle before timing out.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.client.idle.timeout` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Set codepage of audit client

Use this group policy to specify the code page used for character encoding by the auditing service. Supported values are UTF8 and ISO8859-1.

If this group policy is disabled, not configured, or set to a value that is not supported, a default code page of UTF8 is used. If this group policy is enabled, you can specify a supported code page.

This group policy modifies the `lang_setting` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Set connect to collector timeout

Use this group policy to specify the amount of time, in seconds, the agent waits during each connection attempt before it determines that it cannot connect to a collector.

If this group policy is disabled or not configured, the default value is 60 seconds. This group policy modifies the `dad.connect.collector.timeout` configuration parameter.

You can use this parameter with the [Common Settings](#) group policy which allows you to specify the number of unsuccessful attempts that the agent can make to connect to a collector before notifying the user that it is not connected to a collector.

Set fix NSS configuration file automatically

Use this group policy to specify whether to enable the dad process to fix `/etc/nsswitch.conf` automatically if anything goes wrong.

If this group policy is disabled, `/etc/nsswitch.conf` is not updated. If this group policy is enabled or not configured, `/etc/nsswitch.conf` is updated automatically by the dad process.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `autofix.nss.conf` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set max cache size

Use this group policy to specify the maximum number of entries that can be stored in the name service cache. Entries store query results about users and groups. This group policy is applicable only if the [Set cache the query results](#) group policy is enabled.

If this group policy is enabled, the query results are stored in memory up to the value that you specify, resulting in better performance. If this group policy is disabled or not configured, a default value of 80,000 entries is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the maximum number of entries to cache.
4. Click **OK** to save settings in this policy.

This group policy modifies the `cache.max.size` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set resource monitor check interval

Use this group policy to specify how often (in seconds) the resource monitor checks dad resource usage.

If this group policy is disabled or not configured, a default value of 600 seconds is used. If this group policy is enabled and set to 0 seconds, monitoring is disabled.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds for the interval.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.timer` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set resource monitor CPU limit

Use this group policy to specify the maximum percentage of CPU cycles that dad can consume.

If this group policy is disabled or not configured, a default value of 50 percent is used. If this group policy is enabled and set to 0 percent, dad CPU usage is unlimited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the maximum CPU usage percentage.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.cpuLimit` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set resource monitor CPU limit tolerance

Use this group policy to specify (in seconds) how long the maximum percentage of dad CPU cycles can be exceeded before dad is restarted. If this group policy is disabled or not configured, a default value of 5 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds that the maximum percentage of dad CPU cycles can be exceeded.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.cpuLimit.tolerance` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Set resource monitor file descriptor limit

Use this group policy to specify the maximum number of file descriptors that dad can open.

If this group policy is disabled or not configured, a default value of 1024 is used. If this group policy is enabled and set to 0, the number of file descriptors is unlimited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the maximum number of file descriptors.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.fdLimit` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Set resource monitor memory limit

Use this group policy to specify the maximum number of bytes that can be allocated to dad.

If this group policy is disabled or not configured, a default value of 104857600 bytes (100 MB) is used. If this group policy is enabled and set to 0, dad memory allocation is unlimited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the maximum number of bytes that can be allocated to dad.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.memlimit` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set resource monitor should restart dad

Use this group policy to specify whether the resource monitor should restart dad if resource usage exceeds the limits set in other group policies or configuration parameters.

If this group policy is enabled, dad is restarted if resource usage exceeds specified limits. If this group policy is disabled or not configured, dad is not restarted if resource usage exceeds specified limits.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dad.resource.restart` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set seal over a secure GSSAPI connection collector

Use this group policy to specify whether the auditing service seals network communications with the collector using a secure GSSAPI connection.

If this group policy is enabled or not configured, the network connection is sealed and cannot be read. If this group policy is disabled, the connection is not sealed and is human-readable.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dad.gssapi.seal` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set sign over a secure GSSAPI connection with collector

Use this group policy to specify whether the auditing service signs network communications with the collector over a secure GSSAPI connection.

If this group policy is enabled or not configured, the network connection is signed. If this group policy is disabled, the network connection is not signed.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dad.gssapi.sign` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set soft limit of open files

Use this group policy to specify the number of file descriptors that can be used for audited sessions.

For some UNIX platforms, such as Solaris, the default number of available file descriptors for each process is insufficient of auditing sessions, because the Centrify agent requires two descriptors per session.

Use this policy to increase the number of file descriptors available.

This policy modifies the `dad.process.fdlimit` parameter in the agent configuration file.

Set update agent status timeout

Use this group policy to specify how often (in seconds) the agent status in the audit store database is updated.

If this group policy is disabled or not configured, a default value of 300 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds between agent status updates.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.timer.update.agent.status` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set verification of spool disk space timeout

Use this group policy to specify the number of seconds between checks of disk space when the disk space reserved for offline storage is less than the percentage specified in the `set minimum percentage of disk space` group policy. At each check, a warning message is written to the log file.

If this group policy is enabled, disk space is checked at the interval that you specify. If this group policy is disabled or not configured, a default value of 360 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds between disk space checks.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dad.timer.diskspace` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

DirectAudit NSS Settings

Use the group policies under **DirectAudit NSS Settings** operations for the name switching service.

Override audit level for a list of users

Use this group policy to specify individual user names and audit levels or a file that contains the list of user names for which you want to override the default audit level. For more information about the how this group policy affects user auditing in classic and hierarchical zones, see the discussion of the `nss.user.override.userlist` parameter in the *Configuration and Tuning Reference Guide*.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Type each user name and audit level using the following format:

```
user_name[:audit_level]
```

Alternatively, you can type the name of a file that contains a list of user names and audit levels.

4. Click **OK** to save your settings.

Set audit level for conflict user

Use this group policy to specify the audit level to use if there is a conflict caused by a user being included in the ignores users list and having a `use_sysrights` audit level defined.

To use this group policy:

• • • • •

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Select the audit level to use when there is a conflicting audit level defined for a user.
4. Click **OK** to save your settings.

Set audit level for users listed in `uid.ignore`

Use this group policy to specify the audit level for users who are listed in the `user.ignore` or `uid.ignore` file. For more information about the how this group policy affects user auditing in classic and hierarchical zones, see the discussion of the `nss.user.override.auditLevel` parameter in the *Configuration and Tuning Reference Guide*.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Select the audit level to use for users listed in the ignored user list.
4. Click **OK** to save your settings.

Set ignored programs

Use this group policy to list the programs that should not look up account information in Active Directory. If this group policy is not enabled or not configured, the following programs that are used for local account management are ignored by default:

`useradd`

`userdel`

`adduser`

`usermod`

`mkuser`

`rmuser`

• • • • •

`chuser`

If you enable this group policy, you must specify the list of programs to be ignored separated by spaces.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Type program names separated by spaces.
4. Click **OK** to save your settings.

Set no-login shells

Use this group policy to specify the shells that are treated as no-login shells.

If this group policy is disabled or not configured, the shells `/sbin/nologin` and `/bin/false` are treated as no-login shells. If this group policy is enabled, specify one or more shells in a space-separated list.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Type one or more shell names, separated by spaces, in the **No-login shells** field.
4. Click **OK** to save your settings.

This group policy modifies the `nss.nologin.shell` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set override audit level for non-Hierarchical zone users

Use this group policy to specify the default audit level to use if a specific audit level is not defined for users in a classic zone. For more information about the how this group policy affects user auditing in classic zones, see the discussion

of the `nss.alt.zone.auditlevel` parameter in the *Configuration and Tuning Reference Guide*.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Select the default audit level to use in classic zones.
4. Click **OK** to save your settings.

DirectAudit Shell Settings

Use the group policies under **DirectAudit Shell Settings** to configure shell operations for an audited shell.

Defining information pattern in custom format to obfuscate sensitive information

Use this group policy to specify information that is not displayed in auditing results. You specify the information to omit from display by defining a pattern in the group policy. Information that matches the pattern is not displayed in auditing results.

If this group policy is not configured or disabled, all information is displayed in auditing results. By default, this group policy is not configured.

If you enable this group policy, you must define a pattern as follows for information that is not displayed.

- Type the pattern that will not be displayed in auditing results. For example:
`nnnn-nnnn-nnnn-nnnn`
- Each single character in a pattern corresponds to one character in actual session data.
- If you define more than one pattern, separate the patterns with spaces.

For example:

nnnn-nnnn A-nnnn

Supported characters in a pattern are as follows:

a	Any lower case letter.
A	Any upper case letter.
d	Any character.
D	Any letter.
n	Any decimal digit character.
Symbols, such as the following:	
s	~ ` ! @ # (space) \$ % ^ & * (- _ =
	+ [{] } \ : ; ' < , > . ? /
-	Separator for exact matching in session data.
_	Separator for exact matching in session data.
(Separator for exact matching in session data.
)	Separator for exact matching in session data.
,	Separator for exact matching in session data.
.	Separator for exact matching in session data.

This group policy modifies the `dash.obfuscate.pattern` setting in the `centri fyda.conf` configuration file.

Defining information pattern in regex format to obfuscate sensitive information

Use this group policy to specify information that is not displayed in auditing results. You specify the information to omit from display by defining a regular expression in the group policy. Information that matches the regular expression is not displayed in auditing results.

If this group policy is not configured or disabled, all information is displayed in auditing results. By default, this group policy is not configured.

If you enable this group policy, you must define a regular expression as follows for information that is not displayed.

- Type a regular expression to define the information that will not be displayed in auditing results. For example:

[A-Z] [0-9] { 6 } \ \ ([0 - 9 A - Z] \ \)

- If you define more than one regular expression, separate the regular expressions with spaces. For example:

```
[0-9] - [0-9] [a-z] - [0-9]
```

This group policy modifies the `dash.obfuscate.regex` setting in the `centrifda.conf` configuration file.

Set always allowed unix user name list

Use this group policy to specify UNIX users who are allowed to use a session even if the computer cannot be audited due to environment setup issues.

If this group policy is disabled or not configured, root is the only user allowed to use an unaudited session. If you enable this group policy, you must specify a space-separated list of UNIX user names.

This group policy modifies the `dash.user.alwaysallowed.list` setting in the `centrifda.conf` configuration file.

Set audit all invocations

Use this group policy to specify whether to audit all shell invocations.

If this group policy is **Enabled**, all login and non-login shells are audited.

If this group policy is **Disabled** or **Not Configured**:

- Only login shells and login sub-shells are audited.
- Invoked shells are not audited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dash.allinvoked` setting in the configuration file `/etc/centrifda/centrifda.conf`.

Set audit commands

Use this group policy to specify commands to audit.

If this group policy is enabled, you can create a command list and specify whether each command in the list is audited. Commands in the command list that have an action of **Enable** are audited by the auditing agent. Commands in the command list that have an action of **Disable** are not audited by the auditing agent.

If this group policy is disabled or not configured, commands to be audited must be configured manually on each UNIX computer.

When you add a command to the list, you must specify the full path to the command. You cannot add a link, shell, or wrapper script to the command list.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **Add** to add a command to the Audit Commands list.
4. Specify the full UNIX path name of the command.
5. In the Action field, select whether to enable or disable auditing for the command.
6. Click **OK** in the Set audit commands dialog box.
7. Click **OK** in the Set audit commands Properties dialog box to save settings in this policy.

Set audit STDIN data

Use this group policy to specify whether the auditing agent captures standard input (stdin).

If this group policy is enabled or not configured, the auditing service records all session input and output, including standard input (stdin).

If this group policy is disabled, the auditing service records all session activity to standard output, but does not capture standard input data.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dash.auditstdin` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set continue working without dad

Use this group policy to specify whether the audited shell (cdash) continues to run if the dad process is not running.

If this group policy is enabled or not configured, the audited shell continues to run when the dad process is not running. If this group policy is disabled, the audited shell stops running when the dad process stops running, and the user is prompted to restart the dad process.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dash.cont.without.dad` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set except auditing password strings

Use this group policy to specify strings that the auditing agent should ignore when capturing standard input data. For security, typed passwords are always ignored by default.

If this group policy is enabled, specify strings to ignore using regular expressions that do not include quotes. Leading and trailing spaces are ignored, spaces in the middle are not affected. For example:

```
dash.auditstdin.except: (prompt1|prompt2)
```

will match strings like these:

• • • • •

This is prompt1:

Prompt2 asks for password:

If this group policy is disabled or not configured, this mandatory string pattern is applied:

```
(password[[:alnum:]][[:blank:]][[:punct:]]*:[[:space:]]*$) |  
(verify[[:alnum:]][[:blank:]][[:punct:]]*:[[:space:]]*$)
```

The default value is empty to ignore only the passwords that users enter.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Type a regular expression that defines the string to ignore.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.auditstdin.except` setting in the configuration file `/etc/centrifyda/centrifyda.conf`. For more information about specifying exceptions, see the comments in the `centrifyda.conf` file.

Set force audit list

Use this group policy to specify one or more session binary files to audit.

If this group policy is enabled, the binary files that you specify are audited. You can separate entries in the list of binary files by typing a space or a comma. You can escape spaces or commas in file names using the backslash character (`\`).

If the group policy is disabled or not configured, no binary files are audited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.

• • • • •

3. Type one or more binary file names in the list.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.force.audit` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set not audited ssh command list

Use this group policy to specify a space-separated list of ssh commands that are not audited.

If the group policy is disabled or not configured, the commands `scp`, `rsync`, and `sftp-server` are not audited. If this group policy is enabled, the commands that you specify are not audited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Type one or more commands in the list, separated by spaces.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.ssh.command.skiplist` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set parent process skip list

Use this group policy to specify a list of parent processes that are not audited. If the name of a process's parent is in this list, the audited shell (`cdash`) will drop out without auditing.

If this group policy is disabled or not configured, the following processes are not audited by default:

```
sapstartsrv  
gdm-binary  
gdm-session-wor  
kdm  
sdt_shell
```

• • • • •

If you enable this group policy, you must specify a space-separated list of process names.

This group policy modifies the `dash.parent.skipList` setting in the `centrifya.conf` configuration file.

Set reconnect to dad timeout

Use this group policy to specify the number of seconds to wait after restarting the dad process before cdash attempts to reconnect to the auditing service.

If this group policy is enabled, the timeout that you specify is used. If this group policy is disabled or not configured, a default value of 1 second is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds to wait.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.reconnect.dad.wait.time` setting in the configuration file `/etc/centrifya/centrifya.conf`.

Set reconnect to dad times

Use this group policy to specify how many times cdash attempts to connect to the auditing service after the dad process has started.

If this group policy is enabled, the number of attempts that you specify is used. If this group policy is disabled or not configured, a default value of 3 attempts is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.

.....

3. Specify the number of attempts.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.reconnect.dad.retry.count` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set record login entry

Use this group policy to specify whether the auditing service should add utmp entries for the cdash pseudo terminals (pty). The setting of this group policy affects the results of `whoami` and `who` commands.

If this group policy is enabled, the auditing service adds utmp entries for cdash pty processes. Under this scenario, the `whoami` command in an audited shell works as expected, but the `who` command lists logged-in users twice.

If this group policy is disabled or not configured, the auditing service does not create additional utmp entries. Under this scenario, the `whoami` command in an audited shell cannot determine complete user information.

Workaround: on some operating systems, the `who --lookup` command works, but the `who` command lists users only once.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **OK** to save settings in this policy.

This group policy modifies the `dash.loginrecord` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set SHELL to actual user shell

Use this group policy to specify whether cdash sets the SHELL environment variable to the user's actual shell or to the audit shell.

If this group policy is enabled or not configured, the default value is true, and the SHELL environment variable is set to user's actual shell. If you disable this group policy, the SHELL environment variable is set to the DirectAudit audit shell.

• • • • •

This group policy modifies the `dash.shell.env.var.set` setting in the `centrifida.conf` configuration file.

Set skip auditing userlist

Use this group policy to specify the names of UNIX users and Active Directory users with a UNIX login who should not be audited. You can separate user names by typing a space or a comma. For example:

```
dash.user.skiplist: Mae kelly,dmorris,Booker
```

If this group policy is enabled, the users on the list are not audited. If this group policy is disabled or not configured, all users are audited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Create a list of users to audit.
4. Click **OK** to save settings in this policy.

This group policy modifies the `dash.user.skiplist` setting in the configuration file `/etc/centrifida/centrifida.conf`.

Show actual user running an audited command

Use this group policy to specify whether command-based auditing records will display the actual user account that executed the audited command, rather than just the run-as user account. Enable this policy to show both the run-as user account and the actual user account in command-based auditing records.

By default, this policy is not enabled, and only the run-as account used to run the privileged command is shown in auditing records. To enable this policy, set the parameter to `true`.

This group policy modifies the `dash.cmd.audit.show.actual.user` setting in the agent configuration file.

LRPC2 Client Settings

Use the group policies under **LRPC2 Client Settings** to control timeout and reconnect settings for the auditing service.

Set contact with dad timeout

Use this group policy to specify the number of seconds that cdash and dainfo wait before timing out while trying to contact the dad process.

If this group policy is enabled, the timeout that you specify is used. If this group policy is disabled or not configured, a default value of 30 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify the number of seconds to wait.
4. Click **OK** to save settings in this policy.

This group policy modifies the `lrpc2.timeout` setting in the configuration file `/etc/centrifyda/centrifyda.conf`.

Set contact with dad timeout for rebinding collector

Use this group policy to specify the number of seconds that dareload (-b) waits before timing out while trying to contact the dad process.

If this group policy is enabled, the timeout that you specify is used. If this group policy is disabled or not configured, a default value of 300 seconds is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. Select **Enabled**.

• • • • •

3. Specify the number of seconds to wait.
4. Click **OK** to save settings in this policy.

This group policy modifies the `lrpc2.rebind.timeout` setting in the configuration file `/etc/centrifda/centrifda.conf`.

Spool Disk Space Settings

Use the group policies under **Spool Disk Space Settings** to configure spool disk limits.

Set maximum disk space for DB file size

Use this group policy to specify maximum disk space (in bytes) to allocate to the offline storage database.

If this group policy is enabled, the file size that you specify is used. If this group policy is disabled or not configured, a default value of 0 bytes is used. A value of 0 bytes specifies unlimited file size.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify a file size.
4. Click **OK** to save settings in this policy.

This group policy modifies the `spool.maxdbsize` setting in the configuration file `/etc/centrifda/centrifda.conf`.

Set minimum percentage of disk space

Use this group policy to specify the minimum volume of disk space required on the partition containing the offline spool file before spooling stops.

You can set this value as a percentage of the disk space, or you can set it as an exact size. To set the value as an exact size, specify the unit value after the number value. The unit values are not case-sensitive.

• • • • •

You can specify the following unit values:

- B (byte)
- KB (kilobyte)
- MB (megabyte)
- GB (gigabyte)
- TB (terabyte)

The default value for this group policy is 10 percent of disk space.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify a value.
4. Click **OK** to save settings in this policy.

This group policy modifies the `spool.diskspace.min` parameter in the agent configuration file.

Set soft limit percentage of disk space

Use this group policy to specify the minimum volume of disk space that should be available for the offline storage file before warnings are posted to the log file. If available disk falls below the level specified in this group policy, a warning is logged and auditing will continue until disk space falls below the level specified in the [Set minimum percentage of disk space](#) group policy.

You can set this value as a percentage of the disk space, or you can set it as an exact size. To set the value as an exact size, specify the unit value after the number value. The unit values are not case-sensitive.

You can specify the following unit values:

- B (byte)
- KB (kilobyte)
- MB (megabyte)

.....

- GB (gigabyte)
- TB (terabyte)

If this group policy is enabled, the volume that you specify is used. The default value is 12 percent.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify a value.
4. Click **OK** to save settings in this policy.

This group policy modifies the `spool.diskspace.softlimit` parameter in the agent configuration file.

Set threshold percentage of disk space to reset log state

Use this policy to specify a threshold percentage of disk space that is added to the minimum percentage of disk space (set in the [Set minimum percentage of disk space](#) group policy) that determines when the information/warning/error log state is reset. Message logging resumes only after the log state is reset.

When disk space drops below the minimum percentage (for example, 10%), a warning is logged. Additional warnings are not logged until disk space has risen above the minimum percentage + threshold percentage (for example, $10\% + 2\% = 12\%$), and then drops again to below the minimum percentage (10%).

Setting a threshold percentage is useful to prevent unnecessary log messages when disk space hovers near the minimum percentage and would otherwise trigger a log message every time the minimum percentage is crossed.

If this group policy is enabled, the percentage that you specify is used.

If this group policy is disabled or not configured, a default value of 2 percent is used.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Specify a percentage.
4. Click **OK** to save settings in this policy.

This group policy modifies the `spool.diskspace.logstate.reset.threshold` setting in the configuration file `/etc/centri fyda/centri fyda.conf`.

Windows Agent Settings

Use the group policies under **Windows Settings** to configure settings for agents on audited Windows computers.

Allow selected administrative users to stop the auditing service

Use this group policy to specify which users and groups can stop the auditing service on a local Windows computer using the DirectAudit Agent Control Panel.

If this policy is disabled or not configured, no users or groups can stop the auditing service through the control panel.

To use this group policy:

1. Double click the group policy in the right pane of the Group Policy Management Editor.
2. On the **Policy** tab, select **Enabled**.
3. Click **Add**.
4. In the Select Users or Groups dialog, specify the users or groups who will be able to stop the auditing service using the DirectAudit Agent Control Panel.
5. Click **OK** in the Select Users or Groups dialog.
6. Click **OK** in the group policy **Policy** tab to save your changes.

Audited user list

Use this group policy to specify which users and groups are audited. When you enable this group policy, only the users and groups you specify in the policy are audited. Be aware that this group policy takes precedence over the audit level set for a role.

If this policy is not configured, all users and groups are audited.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **Add** and identify specific users and groups to audit.
4. Click **OK** to save the list of users and groups.

See the *Auditing Administrator's Guide* for more information about the effect of choosing to enable this policy, the [Non-audited user list](#) policy, or a combination of both policies.

Non-audited user list

Use this group policy to specify which users and groups are not audited. When you enable this group policy, only the users and groups you specify in the policy are not audited. If this policy is not configured, all users and groups are audited. If you enable both the [Audited user list](#) and the [Non-audited user list](#) policies, the users you include in the Non-audited user list take precedence over the Audited user list. Be aware that this group policy takes precedence over the audit level set for a role.

To use this group policy:

1. Double click the policy in the right pane of the Group Policy Management Editor.
2. On the Policy tab, select **Enabled**.
3. Click **Add** and identify specific users and groups to exclude from

auditing.

4. Click **OK** to save the list of users and groups.

See the *Auditing Administrator's Guide* for more information about the effect of choosing to enable the [Audited user list](#) policy, the [Non-audited user list](#) policy, or a combination of both policies.

Set maximum recorded color quality

You can use this group policy to set the maximum color quality of recorded sessions. If this group policy is disabled or not configured, a default value of Low (8bit) is used.

To use this group policy:

1. Double click the group policy in the right pane of the Group Policy Management Editor.
2. Select **Enabled**.
3. Select one of the following options:
 - Native color
 - Low (8bit)
 - Medium (16bit)
 - Highest (32bit)
4. Click **OK** to save settings in this policy.

Set maximum size of the offline data file

You can use this group policy to specify the maximum percentage of disk space that the offline data file uses. If this group policy is disabled or not configured, the default is 10%.

To use this group policy:

1. Double click the group policy in the right pane of the Group Policy Management Editor.
2. Select **Enabled**.

• • • • •

3. Specify the maximum disk space percentage.
4. Click **OK** to save settings in this policy.

Set update agent status timeout

Use this group policy to specify how often (in seconds) the agent status in the audit store database is updated. If this group policy is disabled or not configured, a default value of 300 seconds is used.

To use this group policy:

1. Double click the group policy in the right pane of the Group Policy Management Editor.
2. Select **Enabled**.
3. Specify the number of seconds between agent status updates.
4. Click **OK** to save settings in this policy.

Additional group policies for UNIX services

Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service provides additional group policies that control the configuration of specific Linux, UNIX, and Mac OS X services. This chapter describes these additional group policies.

The following topics are covered:

- [Common UNIX settings](#)
- [Linux Settings](#)
- [SSH \(Secure shell\) settings](#)

Common UNIX settings

Some of the **Common UNIX Settings** group policies—such as [Copy files](#), [Sudo Rights](#), and [Copy files from SYSVOL](#)—are implemented with a dynamic link library (.dll) rather than an administrative template. Policies that are implemented with .dll plug-ins are always available on computers where the Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service Group Policy Management Extension is installed.

Other Common UNIX Settings policies—such as [Set crontab entries](#) and [Specify commands to run](#)—are available only after you add the `centrify_unix_settings.xml` or `centrify_unix_settings.admx` template to the Group Policy Management Extension. You can add or remove the group policies from the `centrify_unix_settings` administrative template independent of the policies implemented in .dll plug-ins.

Note The Centrify agent no longer supports the ADM administrative template in versions 2016 and later. All administrative templates must be formatted in either XML or ADMX.

Copy files

Use this group policy to automatically copy a set of one or more files from the domain controller to each Linux, UNIX, and Mac OS X computer that joins the domain.

Note For the **Origin** domain in the **Source** file, you can only list out trusted domains in the current forest.

To enable and configure Copy files:

1. Create the files to copy in either of two locations:
 - sysvol on the domain controller.
 - A shared folder

The sysvol location is assumed to be:
`\\domainController\sysvol\domainName\gpdata`

If the gpdata directory does not exist, create it first. Files to copy can be text or binary.
2. Select the Group Policy Object and click Edit to open the Group Policy Object Editor.
3. Select **Computer Configuration > Centrify Settings > Common Unix Settings**, then double-click **Copy files**.
4. In **Copy file policy setting**, select **Enabled**.
5. Click **Add**, then provide the following information:
 - Select a trusted domain or type a server name. For example, select `acme.com` or type a name `admin1.acme.com`.
 - Type the name of a file to copy or click **Browse** to browse to a directory and select a file. You can only add one file name at a time. To add multiple files, you must click **Add** for each one.
 - Type the name of a directory on the Centrify-managed computer,

such as, /etc.

- Select **Use destination file ownership and permissions** to apply permissions to the file based on the directory to which it is copied or select **Specify permissions and ownership** to manually apply permissions. When you select this button, you must enter permission data in the next three fields.
 - Enter file permissions using octal notation. Use `man chmod` for information.
 - Enter the UID for the file owner or click **Browse** to browse Active Directory for a user. The UID of the user you select is entered in this field.
 - Enter the GID for the user's group, or click **Browse** to browse Active Directory for a group. The GID of the group you select is entered in this field.
 - Select **Copy as binary file** to copy the file as binary. By default, files are copied as text files.
6. Click **OK** to add the specified file to the list.
 7. Click **Add** to add another file to be copied.
 8. When you are finished adding files, click **OK** to apply the policy with the files you have selected.
 9. At any time, to remove a file, select it and click **Remove**. You may also select a file and click **Edit** to make changes to the information for the file, such as where to copy it or file permissions.

Note If you change the policy from *enabled* to *not configured*, all files are removed from the list. However, files are not removed if you change from *enabled* to *disabled*.

Copy files from SYSVOL

Use this group policy to automatically copy a set of one or more files from the domain controller to each Centrify-managed computer that joins the domain.

Note This group policy is still supported but has been deprecated in favor of [Copy files](#).

• • • • •

The steps to enable and configure the Copy Files from SYSVOL group policy are the same as [Copy files](#) except that the files must be located in sysvol directory on the domain controller.

The sysvol location is assumed to be:

```
\\domainController\sysvol\domainName\gpdata
```

You can create the gpdata directory if it does not exist, then put the files you want to copy in the directory. For more information, see [Copy files](#).

If you change the policy from *enabled* to *not configured*, all files are removed from the list. However, files are not removed if you change from *enabled* to *disabled*.

Sudo Rights

Use this group policy to centrally control which users can run commands as another user and the specific commands that can be run as that user. This policy configures the sudoers file with the appropriate lines when a user who has this policy applied logs on. When the user logs off, the lines applied for the user are removed and the sudoers file is restored to its previous state.

Note In order to work properly, the sudo Rights group policy requires that the sudo package, including vi sudo and the sudoers file, is installed on the Centrify-managed computer.

When you select **Enabled** or **Disabled** for the sudo Rights group policy, you can then add or remove user names and commands.

You add items to the text box just as you would to the sudoers file; that is, you type entries as you want them to appear in the sudoers file.

Note It is important to use the proper syntax for entries in the sudoers file. If the syntax isn't valid, the sudo command interprets the sudoers file as corrupt and no users are allowed to run commands using sudo rights. Therefore, in addition to the **Explain** tab, which describes the sudoers grammar in Extended Backus-Nauer Format (EBNF), this policy provides several other ways to help you enter and verify the correct syntax for your entries:

- The **Sample** tab shows sample sudoers file entries.
- A right click menu provides templates for inserting alias entries, as well as the ability to browse for users.
- Validation code verifies that there are no syntax errors in your entries before writing the entries to the sudoers file.

For example, the following procedure shows you how to create a command alias (for the `rm` command) and how to permit a user to simulate running as root to run the `/usr/sbin/backup` command:

1. In the Group Policy Editor, open the Sudo Rights policy properties and select **Enabled** or **Disabled**. Right-click and select **Insert Alias > Cmnd**. The following text is inserted in the box:

```
Cmnd_Alias <alias>=<command>
```

2. Replace `<alias>` with `DEL` and `<command>` with the full path to the `rm` command:

```
Cmnd_Alias DEL=/bin/rm
```

3. Click **Apply** to enter the command alias and verify that the syntax is correct.

4. On the next line, enter the following:

```
jsmith ALL = /usr/bin/backup
```

This entry gives `jsmith` all privilege on the Linux, UNIX, or Mac OS X computer to run the `backup` command. The user, `jsmith`, still needs to enter a password to run this command. You can use the context menu to change the entry and remove the password requirement.

5. After the '=' sign, insert a space, then right-click and select **Insert Value > Cmnd > NOPASSWD:** and `NOPASSWD:` is added to the entry.

The entry now should now look like this:

```
jsmith ALL = NOPASSWD /usr/bin/backup
```

6. Click **Apply** or **OK** to save the entry.

When a user to whom this policy applies logs in, the appropriate lines are added to the sudoers file. For example, when the user `jsmith` logs on to the computer `machine1`, the following is added to the sudoers file:

```
jsmith ALL = NOPASSWD /usr/bin/backup
```

.....

```
Cmnd_Alias DEL=/bin/rm
```

If any of your entries have improper syntax, you will see an error message. Click **Details** to get information about the syntax error, then click **Cancel** and make corrections.

Note The right-click context menu also allows you to browse for user names. Right-click and select **Insert Value > Browse**, then enter search criteria. Select a name and click **OK**, and that name is added to the entry. In addition, as you add aliases, they are added to the context menu. For example, if you right-click and select **Insert Value > Cmnd**, you should see the **DEL** alias that you created in the previous procedure.

For more information about using sudo and the syntax to use in the sudoers file, see the man pages for sudo and sudoers appropriate to your operating environment.

Set crontab entries

Use the **Set crontab entries** group policy to manage crontab entries for individual users or for an entire computer. The management of computer-level crontab entries is performed as the root user. User-specific crontab entries run under the user's account.

Select the **Computer Configuration > Centrify Settings > Common UNIX Settings > Set crontab entries** group policy to configure computer-based policies for the root user.

Select the **User Configuration > Centrify Settings > Common UNIX Settings > Set crontab entries** group policy to configure user-based policies for individual users.

Both Set crontab entries group policies are defined in the `centrify_unix_settings.xml` administrative template.

If you select **Enabled** for either group policy, you can then click **Show** to add or remove entries in the `/etc/crontab` file.

To add crontab entries to the policy, click **Add**. You can then type the entry to be added to the file using the appropriate format for the local computer's operating environment, then click **OK**.

The standard format for entries in this file is:

• • • • •

Minute Hour DayOfMonth Month DayOfWeek User Command

For the Minute field, the valid values are 0 through 59. For the Hour field, the valid values are 0 through 23. For the Day of the Month field, the valid values are 1 through 31. For the Month of the Year field, the valid values are 1 through 12. For the Day of the Week field, the valid values are 0 through 6, with 0 representing Sunday. An asterisk (*) can be used in any of these fields to indicate all valid values.

For the Command field, you should type the entire command line to be executed at the specified times.

For example, to remove core files every weekday morning at 3:15 am, you could type an entry similar to this:

```
15 3 * * 1-5 find $HOME -name core 2>/dev/null | xargs rm -f
```

Specify commands to run

Use the **Specify commands to run** group policy to configure one or more commands to run any time a computer is rebooted and at the computer group policy refresh interval when applied to a computer, or when a user logs on and at the user group policy refresh interval when applied to user accounts.

Select the **Computer Configuration > Centrify Settings > Common UNIX Settings > Specify commands to run** group policy to configure computer-based policies that run when a computer restarts and at the computer group policy refresh interval.

Select the **User Configuration > Centrify Settings > Common UNIX Settings > Specify commands to run** group policy to configure user-based policies that run when users log on.

Both **Specify commands to run** group policies are defined in the `centrify_unix_settings.xml` administrative template.

If you select **Enabled** for either group policy, you can then click **Show** to add or remove commands.

• • • • •

To add commands to the policy, click **Add**. You can then type the commands to be added to the file using the appropriate format for the local computer's operating environment, then click **OK**.

For computers, the commands you specify should be general computer commands.

For user accounts, the commands you specify should be user-specific. The user account that is used to run the command is recorded in the \$ENV variable in the `RunCommand.pl` script. An entry in `/var/log/centrifydc.log` identifies the user. For example:

```
The commands are invoked for user: wtest2
```

Linux Settings

Use the group policies under **Linux Settings** to configure the following basic settings:

- Enforce screen locking
- Specify basic firewall settings
- Specify network login message settings

Use the policies under **Linux Settings > Security** to configure the following computer configuration settings:

- Certificate validation method
- Enable smart card support
- Lock Smart Card screen for RHEL
- Require smart card login

Use the policies under **Linux Settings > Security** to configure the following user configuration settings:

- Specify applications to import system NSSDB

Enforce screen locking

Use the **Enforce screen locking** group policy to control the screen lock enforcement and the time out value for all users logging on to a computer or

for individual users. Select the **Computer Configuration > Centrify Settings > Linux Settings > Enforce screen locking** group policy to configure computer-based screen locking. Select the **User Configuration > Centrify Settings > Linux Settings > Enforce screen locking** group policy to configure user-based screen locking.

Both Enforce screen locking group policies are defined in the `centrify_unix_settings.xml` administrative template. The mechanism used to control screen locking is specific to Linux-based computers, however, so the policies are listed under the Linux Settings category.

The most common way to handle screen locking on Linux computers is through the `xscreensaver` program. Although the `xscreensaver` program has a default configuration file, this centralized configuration file is automatically overridden if users have a local `.xscreensaver` file in their home directory. To enforce a centralized screen locking policy, this group policy creates a directory in the user's home directory that is owned by root and places a file that is also owned by root in this directory, so that the file cannot be removed by the user. When the `xscreensaver` program tests to see if there is a regular file in the user's home directory and does not find it, it uses the system configuration file.

Note If the user home directory is NFS-mounted, with the `root-squash` option set, this policy will not work as intended because the group policy (running as root) cannot create the un-deletable `$HOME/.xscreensaver` directory. As a workaround, the user may manually create the `.xscreensaver` directory with a `umask` of `0700` in the user home directory on the NFS server to prevent the user from changing `.xscreensaver`.

If you select **Enabled** for this group policy as a computer configuration policy, you can make the policy the default screen locking behavior for all users of the computer and set the default number of minutes to wait before locking the screen, but users are free to override the default.

To enforce this policy for individual users, you should enable the screen locking policy as a user configuration policy. However, enabling the user configuration screen locking group policy prevents users from changing their screen locking parameters.

Specify basic firewall settings

Use the **Specify basic firewall settings** group policy to set up a simple exclusionary firewall on targeted computers using `iptables`. If you select **Enabled** for this group policy, the firewall will allow all outgoing traffic but block any inbound traffic, except `ssh` and `ping`, by default. To customize the firewall settings, select **Enabled**, then click **Show** to add or remove entries.

The Specify basic firewall settings group policy is defined in the `centrify_linux_settings.xml` administrative template.

To modify the default behavior of the policy, click **Add**. You can then type the appropriate entries to set up the `iptables` using the following format:

Name:Type:Protocol:Port>Action

where

- Name is an identifying string.
- Type is either `INPUT` or `OUTPUT` (caps are mandatory). Use `INPUT` to block incoming requests on the specified port and `OUTPUT` to block the computer from sending on that port.
- Protocol should be one of `tcp`, `udp`, `icmp`, or `all`.
- Port is the port number.
- Action is either `ACCEPT` or `DROP`.

For example, to allow connections to the computer that acts as a web server:

`HTTP:INPUT:tcp:80:ACCEPT`

The following example would prevent the computer from sending mail:

`SMTP:OUTPUT:tcp:25:DROP`

When you are finished setting up the `iptables`, click **OK**.

This group policy does not incorporate any Linux distribution or release-specific configurations to enable broad use of the policy.

Any existing tables are purged and new tables are built from the data pushed to the computer through the group policy.

Specify network login message settings

Enable the **Specify network login message settings** group policy to display the same welcome messages for both remote and local users. This group policy creates a symbolic link between the files `/etc/issue.net` and `/etc/issue`. If you disable the policy, the symbolic link is removed and `/etc/issue.net` is restored, if it existed originally.

The Specify network login message settings group policy is defined in the `centrify_linux_settings.xml` administrative template.

Security

Use the group policies under **Security** to configure the following computer settings:

- Certificate validation method
- Enable smart card support
- Lock Smart Card screen for RHEL
- Require smart card login

These computer configuration policies are only applicable for Red Hat Enterprise Linux and Mac OS X. See the release notes for information about the smart card manufacturers and models supported. If you are setting group policies for Mac OS X, see the *Administrator's Guide for Mac* for additional group policies available only for this platform.

Use the group policy under **Security** to configure the following user settings:

- Specify applications to import system NSSDB

Certificate validation method

Use this group policy to configure the certificate validation method.

For **Certificate Revocation List**, select one of the following settings:

- **Off:** No revocation checking is performed.
- **Best attempt:** The certificate passes unless the server returns an indication of a bad certificate. This setting is recommended for most environments.
- **Require if cert indicates:** If the URL to the revocation server is provided in the certificate, this setting requires a successful connection to a revocation server as well as no indication of a bad certificate. Specify this option only in a tightly controlled environment that guarantees the presence of a CRL server. If a CRL server is not available, SSL and S/MIME evaluations could hang or fail.
- **Require for all certs:** This setting requires successful validation of all certificates. Use only in a tightly controlled environment that guarantees the presence of a CRL server. If a CRL server responder is not available, SSL and S/MIME evaluations could hang or fail.

Enable smart card support

Use this group policy to enable users to log in with smart cards. Enabling this policy automatically enables the Group Policy Settings [Enable user group policy](#) policy.

To remove smart card support after it has been enabled, you need to set this policy to Disabled. Changing the policy to Not configured after being Enabled does not remove the smart card requirement.

Specifying the PKCS #11 module

Optionally, after enabling this policy, you can specify the PKCS #11 module to be used by smart card components. By default, smart card components use the Centrify Coolkey PKCS #11 module. However, Coolkey does not support all smart cards so you can specify a different module if necessary by specifying the absolute path to your PKCS #11 module in **PKCS #11 Module**. For example:

```
PKCS #11 Module    /usr/$LIB/pkcs11/opensc-pkcs11.so
```

This field supports the use of the \$LIB environment variable in the path, which allows a single group policy to work for 32-bit and 64-bit systems. At run time on 32-bit systems \$LIB resolves to lib, while on 64-bit systems it

.....

resolves to `lib64`. When you specify a PKCS #11 module, the group policy sets the following parameter in the Centrify configuration file to the specified path:

```
rhel.smartcard.pkcs11.module
```

After you enable this policy, it does not go into effect until you join the computer to the domain (if not already joined) and run the `adgpupdate` command.

Lock Smart Card screen for RHEL

Use this group policy to lock the computer screen when the smart card is removed from the reader. Note that the [Enable smart card support](#) policy must be enabled in order for this policy to take effect.

To remove lock screen support after it has been enabled, you need to set this policy to Disabled. Changing the policy to Not configured does not remove this feature.

After you enable this policy, it does not go into effect until you join the computer to the domain (if not already joined) and reboot the computer.

Require smart card login

Use this group policy to require all users to log in with a smart card. When this policy is enabled, no users can log in to the machine simply with a user name and password.

The [Enable smart card support](#) policy must be enabled in order for this policy to take effect. After you enable this policy, it does not go into effect until you join the computer to the domain (if not already joined) and reboot the computer.

If you don't want to require smart card login for all users, you can use the Active Directory account option to require smart card login for a specific user. For example:

- In Active Directory Users and Computers select the user's account and open the Properties.
- Click the Account tab, scroll down the list of Account options and select the **Smart card is required for interactive logon** option.

Specify applications to import system NSSDB

Use this group policy to specify one or more locations to import the NSS database that resides in `/etc/pki/nssdb`. This policy synchronizes the individual NSS application databases with the system NSS database. Enabling this policy gives these applications access to the most current certificates and CRLs. Many applications, including Firefox and Thunderbird have their own NSSDB for the user. This feature enables a mapper that parses the `profiles.ini` file at the location you specify and imports the certificates and CRLs to the location specified in the profile.

If you are using Firefox, you must run Firefox at least once before enabling this policy. Firefox creates the user-specific preference folder on first usage.

Enable this policy and click the **Add** button to specify the application directory in which to import the system NSS database. For each application, enter the location of its `profiles.ini` file. The entry must be in relation to the home directory of the user; that is, the path should start with `~/`. For example, the entry for the default location of the Firefox `profiles.ini` file would be `~/mozilla/firefox`.

To discontinue using this policy after it has been enabled, you need to set it to Disabled. Changing the policy to Not configured does not discontinue the import.

Once enabled, this group policy takes effect dynamically at the next group policy refresh interval.

SSH (Secure shell) settings

Use the group policies **SSH Settings** to manage different aspects of secure shell (ssh) authentication. The SSH Settings group policies are defined in the `centrify_unix_settings.xml` administrative template.

When you set SSH Settings group policies, parameters are set in the secure shell configuration file, `/etc/centrifydc/ssh/sshd_config`, not in the Privileged Access Service configuration file. You might have other ssh configuration files stored in other default locations, depending on the operating system. Privileged Access Service first checks the `/etc/centrifydc/ssh` directory for configuration files, then looks for the

configuration file in the `/usr/local/etc` directory on AIX computers, and `/etc/ssh` on AIX, SunOS, IRIX/IRIX64, and Linux computers.

Add sshd_config properties

Use this group policy to configure secure shell properties defined in the `sshd_config` file by group policy.

There are two settings for this group policy:

- If the group policy is **Enabled**, you can click **Add** to add new properties as name/value pairs or edit and/or remove secure shell properties defined in the `sshd_config` file.
- If it is **Disabled**, or **Not Configured**, you can not add new properties as name/value pairs or edit and/or remove secure shell properties defined in the `sshd_config` file.

Allow challenge-response authentication

Use this group policy to specify whether challenge and response authentication is allowed. Enabling this group policy sets the `ChallengeResponseAuthentication` option in the `/etc/centrifydc/ssh/sshd_config` file to `yes`. This setting is required to use multi-factor authentication for secure shell sessions. For more information about preparing to use multi-factor authentication, see the *Multi-factor Authentication Quick Start Guide*.

Allow groups

Use this group policy to specify a list of groups whose members are allowed to log on through `sshd`. You can use wildcards (`*` and `?`) to identify the groups to allow. Separate multiple names by spaces. Users whose primary or supplementary group membership matches any of the specified groups will be allowed to log on using a secure shell `sshd` session.

You cannot use numeric group identifiers (GID) to identify groups. By default, log in is allowed for all groups.

• • • • •

This group policy modifies the `AllowGroups` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Allow GSSAPI authentication

Use this group policy to allow authentication based on GSSAPI, either as the result of a successful key exchange, or through GSSAPI user authentication.

Be certain that you are using a version of OpenSSH that supports GSSAPI authentication. Otherwise, setting this policy will render the OpenSSH server unable to start.

This group policy modifies the `GSSAPIKeyExchange` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Allow GSSAPI key exchange

Use this group policy to allow key exchanged based on GSSAPI. Note that GSSAPI key exchange does not rely on ssh keys to verify host identity.

This policy applies to protocol version 2 only.

This group policy modifies the `GSSAPIAuthentication` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Allow users

Use this group policy to specify a list of users who are allowed to log on through sshd. You may use wildcards (`*` and `?`) to identify the users to allow. Separate multiple names by spaces.

You may also specify a host name to allow a user or users only from particular hosts. For example, `mbradley@oak.com`.

You may not use numerical group IDs to identify users.

This group policy modifies the `AllowUsers` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Deny groups

Use this group policy to specify a list of groups whose members are not allowed to log on through sshd. You may use wildcards (* and ?) to identify the groups to disallow. Separate multiple names by spaces. Log on through sshd is not allowed for users whose primary or supplementary group list matches any of the specified groups.

You may not use numerical group IDs to identify groups.

By default, log in is allowed for all groups.

This group policy modifies the `DenyGroups` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Deny users

Use this group policy to specify a list of users who are not allowed to log on through sshd. You may use wildcards (* and ?) to identify the users to disallow. Separate multiple names by spaces.

You may also specify a hostname to disallow a user or users only from particular hosts. For example, `mbradley@oak.com`.

You may not use numerical group IDs to identify users.

By default, log in is allowed for all users.

This group policy modifies the `DenyUsers` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Enable application rights

Use this group policy to enable SSH application rights. Depending upon the user's role settings, this allows applications to grant rights such as password log in and allow normal shell. You configure and assign rights in zone manager.

This feature is supported in Centrify OpenSSH 4.5.4 or later. Setting this property on an unsupported version renders OpenSSH unable to start.

This group policy adds the following `ServiceAuthLocation` parameter to the `/etc/centrifydc/ssh/sshd_config` file for all computers to which the group policy object applies. It sets the path to the `dzsshchk` command which verifies the rights for users when they log in with SSH:

```
ServiceAuthLocation /usr/share/centrifydc/libexec/dzsshchk
```

This policy is disabled by default

Enable PAM authentication

Use this group policy to enable PAM authentication, account processing, and session processing. When you enable this policy, PAM authentication is implemented through the `ChallengeResponseAuthentication` mechanism.

Depending on your PAM configuration, enabling this policy may bypass the `sshd` settings of `PasswordAuthentication`, `PermitEmptyPasswords`, and `PermitRootLogin without-password`.

If you just want the PAM account and session checks to run without PAM authentication, then enable this policy but disable the `ChallengeResponseAuthentication` mechanism in `sshd`.

Be certain that you are using a version of OpenSSH that supports PAM authentication. Otherwise, setting this policy will render the OpenSSH server unable to start.

This group policy modifies the `UsePAM` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Enable SSO MFA Properties

Use this group policy to enable multi-factor authentication for users after they authenticate through single sign-on using Centrify OpenSSH.

This group policy is only supported by OpenSSH versions 5.3.1 and later. If you attempt to enable this policy while running an earlier version of OpenSSH, the OpenSSH server will not start.

By default, this group policy is not enabled.

This group policy modifies the `SSOMFA` setting in the `/etc/centrifydc/ssh/sshd_config` file

Match Block

You can use the Match Block group policy to add or edit match criteria so that you can match users using a variety of sub-directives.

For example, you can use this group policy if you want to set different kinds of combinations of key/value pairs to match conditions, such as the following general examples to set:

- A key/value to match a condition (key/value)
- Multiple keys/values to match a condition (key/value)
- The same keys/values to match multiple conditions (keys/values)
- Multiple keys/values to match multiple conditions (keys/values)
- Multiple conditions (keys/values) (This has the same effect as setting the policies (keys/values) individually)

For example, you could use the Match Block group policy to fulfill the following use case:

"Any user with an account login ending with *-adm will not be able to use PubkeyAuthentication"

For this example, you would set "Match User *-adm" in the match directives and set "PubkeyAuthentication no" in it's sub-directives.

The arguments to Match are one or more criteria-pattern pairs or the single token All which matches all criteria. The available criteria are User, Group, Host, LocalAddress, LocalPort, and Address.

The match patterns may consist of single entries or comma-separated lists and may use the wildcard and negation operators.

The patterns in an Address criteria may additionally contain addresses to match in CIDR address/masklen format, such as "192.0.2.0/24" or "3ffe:ffff::/32". Note that the mask length provided must be consistent with the address - it is an error to specify a mask length that is too long for the address or one with bits set in this host portion of the address. For example, "192.0.2.0/33" and "192.0.2.0/8" respectively.

Check the group policy explain text for details on which keywords can be used.

Permit root login

Use this group policy to specify whether and how root can log in using ssh. When you enable the policy, select one of the following options from the drop-down list:

- yes — Allow root to log in using ssh.
- without password — Disable password authentication for root. It is still possible for root to log in using another form of password authentication, such as keyboard-interactive PAM.
- forced commands only — Allow root log in with public-key authentication, but only if the command option has been enabled. All other authentication methods are disabled for root.
- no — Do not allow root to log in through ssh.

This group policy modifies the `PermitRootLogin` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Set banner path

Use this group policy to identify a file on the Linux, UNIX, or Mac OS X computer to be sent to a remote user requesting authentication. Typically, the file contains a warning about authentication to provide legal protection to the company.

This group policy modifies the `Banner` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Enable Rlogin Control SFTP

Use the `Enable Rlogin Control Sftp` group policy to allow remote sftp login to AIX machines when `rlogin=false` for the non-root users in `/etc/security/user` file.

This group policy overrides the `rlogin=false` setting in the `/etc/security/user` file.

Set `RloginControlSftp` in `/etc/centrifydc/ssh/sshd_config`. Default is yes. The setting term yes or no applies to whether to respect the `rlogin` setting or not.

- `RloginControlSftp=yes`, respects the `rlogin=false` setting, and denies the remote login. This is the default.
- `RloginControlSftp=no`, overrides the `rlogin=false` setting for the user, and allows remote sftp login.

Enable Rlogin Control SSH

Use the Enable Rlogin Control SSH group policy to allow remote ssh login to AIX machines when `rlogin=false` for the non-root users in `/etc/security/user` file.

This group policy overrides the `rlogin=false` setting in the `/etc/security/user` file.

Set `RloginControlSsh` in `/etc/centrifydc/ssh/sshd_config`. Default is yes. The setting term yes or no applies to whether to respect the `rlogin` setting or not.

- `RloginControlSsh=yes`, respects the `rlogin=false` setting, and denies the remote login. This is the default.
- `RloginControlSsh=no`, overrides the `rlogin=false` setting for the user, and allows remote ssh login.

Specify authorized key file

Use this group policy to specify the file that contains the public keys that can be used for user authentication.

If you enable this policy, specify the file in the authorized keys file box. The file specification is interpreted as an absolute path or a path relative to the user's home directory. To specify multiple files, separate each entry with a space.

The default file specification is `.ssh/authorized_keys`. In addition, if there are backward compatibility issues, `.ssh/authorized_keys2` is checked.

Specify ciphers allowed for protocol version 2

Use this group policy to specify the ciphers allowed for SSH protocol version 2. If you enable this policy, you can add or delete ciphers to increase the speed of SSO.

Multiple ciphers must be separated by commas. If you want to add a cipher to the list, use the '+' character at the beginning of the name. If you enter the name only, you will replace the existing ciphers with the new cipher.

The order of the cipher list will determine the order that sshd uses the ciphers. For example, if you want to increase the speed of SSO, you can place the cipher, aes128-ctr, at the beginning of the list.

When this policy is disabled, the default cipher list, which is the most secure grouping, is used, but may cause delays in SSO.

To enable this group policy, you must be running Centrify OpenSSH 5.3.0 or later.

This group policy modifies the `ciphers` setting in the following file:
`/etc/centrifydc/ssh/sshd_config`

Specify client alive interval

Use this group policy to specify a timeout interval, in seconds, for requesting a response to client alive messages. If sshd does not receive a response from the client to client alive messages within the timeout interval, it sends a message through the encrypted channel requesting a response.

The default is 0, indicating that these messages are not sent to the client.

This group policy modifies the `ClientAliveInterval` setting in the following file: `/etc/centrifydc/ssh/sshd_config`

Specify log level

Use this group policy to specify the log level for messages from sshd. When you enable the policy, you can select the level from a drop-down list.

.....

The default level is INFO. DEBUG and DEBUG1 are equivalent. Logging with any of the DEBUG levels violates users privacy and is not recommended for general use.

This group policy modifies the `LogLevel` setting in the `/etc/centrifydc/ssh/sshd_config` file

Specify login grace period

Use this group policy to specify the time, in seconds, after which the server disconnects if a user has failed to log in. The default is 120 seconds.

Use 0 to specify no time limit.

This group policy modifies the `LoginGraceTime` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Specify maximum client alive count

Use this group policy to specify the maximum number of client alive messages that may be sent by the secure shell daemon (sshd) without receiving a response from the client.

When the policy is enabled, the default setting is three messages.

If the threshold is reached while sshd is sending a client alive message, sshd disconnects the client, terminating the session.

This group policy modifies the `ClientAliveCountMax` setting in the `/etc/centrifydc/ssh/sshd_config` file.

Mac OS X Settings

Privileged Access Service group policies allow administrators to extend the configuration management capabilities of Windows Group Policy Objects to managed Mac OS X computers and to users who log on to Mac OS X computers. This chapter provides a high-level overview to using the group policies that can be applied to Mac OS X computers and users. For details on individual policies, see the *Administrator's Guide for Mac*.

The following topics are covered:

- [Group policies and system preferences](#)
- [Adding Mac OS X group policies](#)
- [Enabling and disabling Mac OS X group policies](#)
- [Setting Mac OS X computer policies](#)
- [Setting Mac OS X user policies](#)

Group policies and system preferences

Windows administrators who have Mac OS X computers in their organization often want to manage settings for all of their computers and users using a standard set of tools. In a Windows environment, the standard method for managing computer and user configuration settings is through group policies applied to the appropriate site, domain, or organizational unit (OU) for computer and user accounts.

The Centrify administrative template for Mac OS X (`centrify_mac_settings.xml` or `centrify_mac_settings.admx`) provides group policies that can be applied to control the behavior of Mac OS X computers running supported versions of the Mac OS X operating system, and the configuration settings for the users who log on to those computers. By adding the

administrative template for Mac OS X to a Group Policy Object, Windows administrators can access and set native Mac OS X system preferences.

This chapter provides an overview of the group policies you can enable under **Mac OS X Settings** if you add the administrative template. These group policies control the following types of Mac OS X system preferences:

- Accounts
- Appearance
- Desktop & Screen Saver
- Dock
- Saver
- Security
- Sharing
- Software Update

When you Enable a group policy in a Windows Group Policy Object, you effectively set a corresponding system preference on the local Mac OS X computer where the group policy is applied.

For example, if you enable the group policy **Computer Configuration > Policies > Centrify Settings > Mac OS X Settings > Security & Privacy > Require password to unlock each secure system preference**, it is the same as opening the Security & Privacy system preference on a local Mac OS X computer, clicking **Advanced**, and setting the **Require an administrator password to access locked preferences** option.

On the local Mac OS X computer, the corresponding option is checked:

Note Not all group policies apply to all versions of the Mac OS X operating environment or all Mac computer models. If a particular system preference doesn't exist, isn't applicable, or is implemented differently on some computers, the group policy setting may be ignored or overridden by a local setting. Use the information in this chapter as a general guideline to group policies for Mac OS X. Refer to *Administrator's Guide for Mac* for detailed group-policy information for all Mac OS X versions.

Once the administrative template for setting Mac OS X group policies is installed as described below, the Windows administrator can use Group Policy

Management and Group Policy Management Editor to define, link, and enforce these policies on Mac OS X computers that are joined to an Active Directory domain.

For more information about using Active Directory Users and Computers or Group Policy Management to create and link Group Policy Objects to sites, domains, or OUs, see the [Adding Centrify settings to Group Policies Objects](#). You can also refer to that chapter for more information about how to add Privileged Access Service administrative templates to a Group Policy Object.

Adding Mac OS X group policies

Centrify group policies for Mac OS X consist of two components:

- An administrative template (.xml or .admx file) that describes the policy to the Group Policy Object Editor which runs on Windows.
- A system executable and its associated configuration files that reside on the Mac and determine the policy for the local computer or for the user who is logged into the local computer and implement the policy.

Installing the administrative template

By default, the .xml file for Mac OS X group policies (centrify_mac_settings.xml) is installed in the c:\Program Files\Centrify\Access Manager\group_policy\policy directory when you select **Group Policy Editor Extension** in the Privileged Access Service setup program. To use any of the policies, you must add centrify_mac_settings.xml to a group policy object.

Centrify provides templates in both XML and ADMX format. In most cases, it is best to use the XML template. The ADMX template file, centrify_mac_settings.admx, resides in a different directory than the .xml file.

To install the administrative template for Mac OS X group policies:

1. Create or edit an existing Group Policy Object linked to a site, domain, or OU that includes Mac OS X computers.

For more information about creating and linking a Group Policy Object, see the Active Directory documentation or [Adding Centrify settings to Group Policies Objects](#).

2. In the Group Policy Object Editor, expand Computer Configuration, then right-click Centrify Settings and select **Add/Remove Templates**.
3. Click **Add**, then navigate to the directory that contains the Centrify `centrify_mac_settings.xml` administrative template. By default, administrative templates are located in the local `C:\Program Files\Centrify\Access Manager\group policy\policy` directory.
4. Select the `centrify_mac_settings.xml` file, click **Open** to add this template to the list of Current Policy Templates, then click **Close**.

You should now see the administrative template for the Mac OS X group policies listed as **Mac OS X Settings** under **Centrify Settings** in the Group Policy Object Editor.

Installing the agent and system files

To install the Centrify agent and the configuration files for group policy on a Mac OS X computer, run the package installer for Mac OS X and follow the instructions displayed. For more information about installing the agent or joining the domain on a Mac OS X computer, see the *Administrator's Guide for Mac*.

Enabling and disabling Mac OS X group policies

Like other group policies, policies for Mac OS X users and computers are organized into categories within the Windows Group Policy Object Editor under **Computer Configuration > Centrify Settings** or **User Configuration > Centrify Settings**. These categories typically map to Mac OS X system preferences and individual policy settings map to specific system preferences settings.

Once enabled, policies get applied at the next group policy refresh interval, after the user logs out and logs back in, or after the computer has been

rebooted. The description of each group policy indicates whether the policy can be applied “dynamically” at the next refresh interval or requires a re-login or a reboot.

Note The system preference updated on an individual computer must be closed, then reopened for the group policy setting to be visible.

In most cases, group policies can be Enabled to activate the policy or Disabled to deactivate a previously enabled policy. Changing a policy to Not Configured has no effect for any Mac OS X group policies. Once a group policy is set on a local computer, it remains in effect even if the computer leaves the Active Directory domain. The administrator or users with an administrative account can change settings manually at the local computer, but any manual change are overwritten when the group policy is applied.

Setting Mac OS X computer policies

The following table lists the categories of group policies you can set for Mac OS X computers. These group policies are in the Privileged Access Service Mac OS X administrative template (`centrify_mac_settings.xml`) and accessed from **Computer Configuration > Centrify Settings > Mac OS X Settings**.

Use this policy	To do this
802.1X Settings	Create computer profiles for wireless network authentication. The profiles you specify with these group policies are created in the Network system preferences pane.
Accounts	Control the look and operation of the login window on Mac OS X computers. These group policies correspond to Login Options in the Accounts system preference.
App Store Settings (Deprecated)	This policy was intended to control access to the App Store, however, it has been deprecated and no longer has any effect when enabled. It is provided to allow an administrator to disable the policy if it was set in an earlier version of Privileged Access Service or the agent.
Custom Settings	Specify whether to use the Custom payload to specify preference settings for applications that use the standard plist format for their preference files. You can use this group policy to add keys and values to an existing preferences plist file.
Energy Saver	Control sleep and wake-up options on Mac OS X computers. These group policies correspond to settings in the Hardware: Energy Saver

Use this policy	To do this
	system preference.
Firewall	Control the firewall configuration on Mac OS X computers. These group policies correspond to settings in the Firewall pane of the Sharing system preference.
Internet Sharing	Manage Internet connections on Mac OS X computers. These group policies correspond to settings in the Internet pane of the Sharing system preference.
Network	Control DNS searching and proxy settings. These group policies correspond to settings in the TCP/IP and Proxies panes of the Network system preference.
Remote Management	Control Apple Remote Desktop access for zone users. These group policies correspond to the Manage > Change Client Settings options in Apple Remote Desktop.
Scripts	Deploy login scripts when an Active Directory user or local user logs on to a Mac OS X computer.. You. create the scripts and store them in the Active Directory domain's system volume (sysvol). They are transferred to the Mac OS X computer when the group policies are applied and executed when a user logs on.
Security & Privacy	Control security settings on Mac OS X computers. These group policies correspond to settings in the Personal: Security & Privacy system preferences.
Services	Control access to various services on Mac OS X computers. These group policies correspond to settings in the Services pane of the Sharing system preference.
Software Update Settings	Control the options for automatic software updates on Mac OS X computers. These group policies correspond to settings in the Software Update system preference.

For details on the individual group policies in each category and how to configure specific policies, see the *Administrator's Guide for Mac*.

Setting Mac OS X user policies

The following table lists the categories of group policies you can set for Mac OS X users. These group policies are in the Privileged Access Service Mac OS X

administrative template (centrify_mac_settings.xml) and accessed from **User Configuration > Centrify Settings > Mac OS X Settings.**

Use this policy	To do this
802.1X Settings	Create user profiles for wireless network authentication. The profiles you specify with these group policies are created in the Network system preferences pane.
Automount Settings	Automatically mount network share's and the Windows home directory when a user logs in. .
Application Access Settings	Control the specific applications users are either permitted to use or prohibited from using. These group policies correspond to Applications preferences set in the Workgroup Manager.
Desktop Settings	Control the desktop and screen saver options for users on Mac OS X computers. These group policies correspond to settings in the Desktop & Screen Saver system preference.
Dock Settings	Control the look and operation of the Dock displayed on the user's desktop. These group policies correspond to Dock preferences set in the Workgroup Manager.
Finder Settings	Configure Finder commands, preferences and views.
Folder Redirection	Redirect specified folders from a network home directory to the local machine.
Import Settings	Import plist files to customize your preferences.
Login Settings	Specify frequently used items, such as applications, folders, or server connections to automatically open when a user logs in.
Media Access Settings	Control the specific media types users are either permitted to use or prohibited from using. These group policies correspond to Media Access preferences set in the Workgroup Manager.
Mobility Settings	Control the synchronization rules applied for users access services from mobile devices. These group policies correspond to Mobility preferences set in the Workgroup Manager.
Printing Settings	Specify a list of printers for a user.
Scripts (Login/Logout)	Specify login and logout scripts that run when Active Directory users log on or log out.
Security Settings	Control the secure login options for users on Mac OS X computers.

Use this policy	To do this
	These group policies correspond to settings in the Security system preference.
System	Control the specific system preferences displayed for users.
Preference Settings	These group policies correspond to System Preferences set in the Workgroup Manager.

For details on the individual group policies in each category and how to configure specific policies, see the *Administrator's Guide for Mac*.

GNOME settings

Privileged Access Service provides a set of GNOME group policies that control the configuration of GNOME user preferences on Linux computers. This chapter provides a high-level overview to using the group policies that can be applied to user preferences for the GNOME desktop environment.

The following topics are covered:

- GNOME desktop preferences
- Adding GNOME group policy templates
- Setting GNOME policies
- Verifying GNOME policy settings
- Troubleshooting GNOME policy settings
- Using the Enable GNOME group policy

GNOME desktop preferences

GNOME is a commonly used desktop environment for Linux computers. GNOME provides a configuration system, GConf or GSettings, to store and manage GNOME user preferences. Many settings are pre-configured and stored as user preferences in the file system. The tools you use to get and set desktop preferences depend on the version of GNOME you are using. The Centrify GNOME group policies enable you to set preferences from a central location and a single interface instead of using the native tools for configuring settings. For information about setting GNOME preferences using native tools, see the [documentation provided on the GNOME website](#).

Adding GNOME group policy templates

Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service provides a set of GNOME group policies that implement a majority of the GNOME desktop user preferences. When enabled, these group policies use the `gconftool-2` or `dconf/gsettings` to get and set configuration settings on Centrify-managed Linux computers.

The Centrify GNOME group policies are defined in the `centrify_gnome_settings.xml` and `centrify_gnome3_settings.xml` template files or in `centrify_gnome_settings.admx` and `centrify_gnome3_settings.admx` template files. Group policy template files are installed automatically on the local computer if you run the setup program on a domain controller. To apply any GNOME group policy settings, you must first add one or both templates to a Group Policy Object. See [Adding Centrify policies from XML files](#).

Setting GNOME policies

After you add template files to a Group Policy Object, you can enable and apply the policies to computer as described in the following procedure.

To apply GNOME group policies:

1. Open the Group Policy Management Editor.
2. Open **User Configuration > Policies > Centrify Settings > GNOME Settings**.

The right pane displays a list of folders for GNOME setting categories that correspond to the GConf settings folders on a Linux computer, and one policy, Enable GNOME group policies. By default, all group policies are set to 'Not configured'.

3. Open category folders to find the policies you want to set.

You may need to open several layers of sub-folders. For example, to enable the policy to show hidden files in the GNOME desktop, open **desktop > gnome > file_views** to locate the **Whether to show hidden files** policy.

You can click the **Explain** tab in any policy to review a brief explanation of the policy and its default value.

4. Double-click the policy, select **Enabled**, then click **OK** to set the policy.

Note In most cases, you should set all of the GNOME policies you want to deploy before performing the next step.

5. Enable the top-level Enable GNOME group policies.

No changes to individual GNOME policies take effect until you enable this policy. This policy allows you to set GNOME user preferences exactly as you want, then implement them all at one time, rather than implement them one at a time as you set them. See [Using the Enable GNOME group policy](#) for more information about this policy.

6. Expand **Computer Configuration > Policies > DirectControl Settings > Group Policy Settings**.
7. Double-click **Enable user group policy**, then select **Enabled** and click **OK**.

By default, on Linux and computers, user-based group policies are ignored until you explicitly enable them with this policy.

Verifying GNOME policy settings

After setting GNOME policies, you can verify the settings on any managed Linux machine by using the `gconftool-2` or `dconf/gsettings` command.

To verify GNOME policy settings on Linux computers:

1. Set one or more GNOME group policies.
2. Enable the “Enable GNOME group policies” master policy.
3. On a managed Linux computer, run `adgupdate` to apply group policies with the updates you have made.

The agent updates group policies at a regularly specified interval. Running `adgupdate` applies the new policies immediately.

4. Run `gconftool-2` or use `dconf/gsettings` and pipe it to `grep` to view specific settings; for example, to see the local GNOME setting for hidden files:

• • • • •

```
[user1@qa1 ~]$gconftool-2 -R /desktop |grep -i hidden
show_hidden_files = true
```

If you are using GNOME 2, you can run `gconftool-2 -R` to see all of your GNOME desktop settings. For example:

```
[user1@qa1 ~]$gconftool-2 -R /desktop
/desktop/gnome:
/desktop/gnome/file_views:
tabs_enable = true
tabs_open_position = end
show_hidden_files = true
icon_theme = crux_teal
show_backup_files = false
/desktop/gnome/applications:
/desktop/gnome/applications/component_viewer:
exec = nautilus %s
/desktop/gnome/applications/help_viewer:
needs_term = false
accepts_urls = true
exec = nautilus
```

To see all system settings, you can run:

```
gconftool-2 -R /system
```

or all desktop gnome application settings:

```
gconftool-2 -R /desktop/gnome/applications
```

Troubleshooting GNOME policy settings

The GNOME group policies handle GConf settings for common applications that are installed on most Linux platforms. If one of these common applications is not installed on a user's computer, it won't be possible to set the group policies for that application. If group policy debug is enabled in the `centrifdc.conf` configuration file, you will see a message such as:

```
Can not get schema: user [***] gconf_key [***]
```

If none of the GNOME policies are taking effect, you should enable debug tracing and check the log file, for example, by executing the `addebug` command:

```
addebug set TRACE
```

In order to enable GNOME settings, `sudo` must be able to run without a TTY. If you see a message such as the following:

```
sudo: sorry, you must have a tty to run sudo
```

you need to edit the `sudoers` file on the Linux computer to allow `sudo` execution without a TTY.

To allow `sudo` execution without a TTY to allow enabling GNOME settings

1. Log in as root on the Linux computer.

2. Edit the `sudoers` file; for example:

```
visudo
```

3. Find the text `requiretty`; for example:

```
Defaults requiretty
```

4. Disable `requiretty` for all users or a specific user by using the `!` symbol, as follows:

```
Defaults !requiretty
```

```
Defaults: userName !requiretty
```

5. Save and close the file.

Using the Enable GNOME group policy

Because GNOME group policies affect users' desktops, it is best to apply all the policies you set at once, rather than one at a time. To support this, you can use Enable GNOME group policies as a master policy. No changes to other GNOME policies take effect until you set the master policy to Enabled. After you enable the set of policies you want to deploy, you set this policy to have all of the policies deployed at the same time.

Similarly, you can disable all previously-enabled policies at once by disabling the master policy. For example, if you want to change some existing settings, you can temporarily disable all policies, then re-enable Enable GNOME group policies when you have made all your changes.

When you disable the master Enable GNOME group policies policy, the settings on each Linux machine revert to the local GNOME settings that were in effect before you deployed group policies. The Centrify GP mapper first saves the current GNOME settings as local values on the Linux client and before it applies the Centrify GNOME settings. If you disable GNOME group policies, the Centrify GP mapper restores the local GNOME settings that were previously saved.

Creating custom GNOME settings through group policy

If you need to use group policy to configure GNOME settings that are not controlled by the default set of GNOME 3 group policies, you can use the **Custom Gnome 3 settings** group policy to do so.

If you enable the **Custom Gnome 3 settings** group policy, you specify a GNOME schema, key, and data that are implemented by the group policy. You specify the information in the group policy as follows:

- **Gnome schema:key** field: *schema id: keyname*

For example:

```
org.gnome.desktop.sound:theme-name
```

- **Data** field: *datastring*

For example:

```
freedesktop
```

Note If you define custom settings in this group policy that are already defined in a default GNOME 3 group policy, the settings in the default group policy take precedence, and the settings in this group policy are not implemented.

Defining custom group policies

This chapter describes how to create custom group policies and administrative templates for your Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service-managed systems.

The following topics are covered:

- [Implementing custom group policies](#)
- [Creating a custom Administrative Template](#)
- [Adding a mapper program to the agent](#)

For more detailed information about creating custom group policies and administrative templates for Windows computers, see the Microsoft Web site or your Windows documentation.

Implementing custom group policies

You can define your own custom group policies for Centrify Privileged Access Service-managed computers and users and add these custom group policies to existing or new Group Policy Objects. Custom group policies consist of:

- A custom administrative template (.xml) file that describes how to set the policy within the Group Policy Object Editor. For example, the Administrative Template describes the user interface presented to the administrator on Windows computer.
- A program or script that makes the appropriate settings for the computer or the user logging on. For example, you can create a Perl script that reads the group policy settings and modifies the appropriate UNIX configuration file to reflect those settings.

Creating a custom Administrative Template

The administrative template enables you to specify the following for a group policy:

- The policy settings, including registry settings, type of configuration (computer or user), category, and help text for the policy.
- The user interface to set the policy.
- Validation code for user-interface fields.

Note The custom Administrative Template is not strictly required if you do not need to make the settings visible and available to the Active Directory or Windows administrator, but in most cases, you should create one using a standard text editor or the Privileged Access Service.

Once you create your custom .xml file, you should copy the file to the C:\Program Files\Centrify\Access Manager\group policy\policy directory on a computer that has the Group Policy Object Editor (normally a domain controller) or any other accessible directory. You can then add the custom .xml file to a new or existing Group Policy Object in the same way you add any other administrative template.

Defining a policy

Extensible Markup Language (XML) files, like a custom administrative template file, are structured documents that contain a set of supported elements enclosed in opening and closing angle (< >) brackets. The elements can be required or optional depending on the requirements of the application.

For each group policy, an administrative template provides elements to do the following:

- Place the policy in the computer configuration, in the user configuration, or in both
- Place the policy in a category
- Define the registry key entries and values to be set
- Provide explanatory text for the policy-setting page

The following example illustrates the basic file format:

.....

```
<class type="Machine">

    <category title="DirectControl Settings"
    keynameid="CentrifyDCPolicyRegistrySettings">

        <category title="Pam Settings"
        keynameid="CentrifyDCPolicyRegistryPam">

            <policy title="Set UID conflict resolution"
            valuenam="pam.uid.conflict.enabled">

                <page>

                    <!--
                        UI Definition
                    -->
                    .
                    .
                    .

                </page>

                <explainpage textid="CentrifyDCPamUidConflict_
Explain" />

            </policy>

            <policy title="Create k5login"
            valuenam="pam.create.k5login">

                <valueon value="true" />

                <valueoff value="false" />

                <explainpage textid="CentrifyDCPamCreateK5Login_
Explain" />

            </policy>

        </category>

    </category>

    .
    .
    .

</class>
```

Use the following keywords to define the policy:

For this type	You can specify
class	Specifies the node in which to place the policy. Use one of the following with the type keyword: Machine: Computer Configuration node User: User Configuration node Both: Computer and User Configuration nodes
category	Specifies the folder for the policy. You can place a set of related policies in a single category. You can also nest categories by placing subfolders within a folder. Use title or titleid to name a category folder.
keyname keynameid	Specifies the registry setting. You can define the registry key at different levels, including category, policy, policy page or UI control, and it applies to all child levels. You can also override the setting at any child level. You should determine whether to use an existing registry key or create a new, custom key. See Defining the user interface for a policy for a discussion of when to use keynameid instead of keyname .
policy	Defines the policy. Use title or titleid for the display name, keyname or keynameid to specify the registry key, and page to define the property page user interface.
explainpage	Provides a page on which you can provide an explanation or instructions for the policy. The best practice is to provide a textid string for the page, and define the content (the explanatory text) of this and other strings in a separate section of the file. See Defining the user interface for a policy for more information.
page	Defines the property page for the policy. Use title or titleid for the page title. See Defining the user interface for a policy for a description of the tags you can use within page tags to define the property page.

Defining the user interface for a policy

You define the user interface for a group policy property page using the **page** tag. The template provides a number of tags that enable you to define a variety of controls, buttons, and dialogs for finding and entering Active Directory information to set group policies. Place any of the following tags within the **page** /**page** tags to define the user interface:

Note This chapter is not intended as a complete reference to the xml schema for a Privileged Access Service administrative template file, but rather shows how tags are commonly used to define a policy. For example, the current section shows how to construct the user interface to a group policy property page; specifically, it shows the tags used to create the user interface of the group policy property page. A complete reference would also show all the elements that could go into creating a dialog box, but this is not generally relevant to creating a property page and hence is not covered in this chapter.

For this type	You can specify
text	Defines a text label control. Use <code>text</code> or <code>textid</code> to define the text to be displayed in the text label.
groupbox	Groups a set of UI controls on a policy page. Use <code>text</code> or <code>textid</code> to provide a name for the box. Use <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level.
	Creates a box in which a user can enter text. It requires the <code>valuenam</code> keyword and <code>value</code> . The <code>value</code> should be the name used in the registry, if applicable. You can also use the following with <code>edittext</code> : <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>default</code> to display a default value when the policy is first enabled. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level.
edittext	<ul style="list-style-type: none"> ■ <code>maxlength value</code> maximum length of the string ■ <code>charcas</code>ing to specify whether to leave the case of characters in the box as is or convert them to lowercase or uppercase. The default is to leave them as is (<code>Normal</code>). ■ <code>required</code> to require a value be set. ■ <code>readonly</code> to specify whether the value can be changed. The default is to allow the value to be changed (<code>false</code>). ■ <code>button</code> to define a button to be displayed after the text control box. ■ <code>validation</code> to define validation for user input.

For this type	You can specify
numeric	<p>Creates a numeric text box control that allows a user to adjust a numeric value up or down. It requires the <code>valuenam</code> keyword and <code>value</code>. The <code>value</code> should be the name used in the registry, if applicable. You can also use the following with <code>numeric</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level. ■ <code>valuetype</code> to display the type of the value in the registry setting. ■ <code>default</code> to display a default value when the policy is first enabled. ■ <code>min value</code> to set the minimum value allowed. ■ <code>max value</code> to set the maximum value allowed. ■ <code>spin</code> to define the amount to increment or decrement on each button click. The default increment is 1. ■ <code>decimalplaces</code> to specify the number of decimal places for the value to be filled in. The default is 0. ■ <code>required</code> to specify that the user must enter a value. The default is <code>false</code>, that is, the field is not required. ■ <code>validation</code> to define validation for user input.
listbox	<p>Provides a list view in which a user may add, remove, or edit setting values. Use <code>dialog</code> to associate a dialog box that enables a user to add a new entry or edit an existing entry in the list box. Specify the type of the listbox (<code>listboxtype</code>) to specify the kind of values the listbox generates:</p> <ul style="list-style-type: none"> ■ <code>single</code> The box contains one column and generates a single value that is a concatenation of values from all rows separated by the <code>separator</code> attribute. ■ <code>Prefix</code> The box contains one column and generates a list of registry values. The registry value name is defined by the <code>prefix</code> attribute and with a row number appended to the prefix name. ■ <code>Explicit</code> The box contains two columns and generates

For this type	You can specify
	<p>a list of registry values. The first column contains the registry value name while the second column contains the registry value.</p> <p>You can also use the following with <code>ListBox</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level. ■ <code>prefix</code> to define the prefix of the value name of the registry setting. Use this attribute with a <code>listtype</code> of <code>Prefix</code>. ■ <code>separator</code> to separate values when the <code>listtype</code> is <code>Single</code>. ■ <code>min</code> to set the minimum number of rows allowed. ■ <code>max</code> to set the maximum number of rows allowed. ■ <code>sort</code> to specify whether sorting is enabled in the list box.
checkbox	<p>Boolean values. This keyword requires the <code>valuenam</code> keyword and <i>value</i>, and the <code>valuetype</code>. The <i>value</i> should be the name used in the registry, if applicable. You can also use the following with this <code>checkbox</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level. ■ <code>checked</code> to set the check box to checked when the policy is first enabled. Without this keyword, the check box is not checked by default. ■ <code>valueon</code> to define the registry setting when the check box is checked. ■ <code>valueoff</code> to define the registry setting when the check box is not checked.
radiogroup	<p>Defines a set of two or more radio buttons (<code>radiobutton</code>) from which a user must make a single choice. This keyword requires the <code>valuenam</code></p>

For this type	You can specify
	<p>keyword and <code>value</code>, and the <code>valuetype</code>. The <code>value</code> should be the name used in the registry, if applicable.</p> <p>You can also use the following with <code>radiogroup</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level. ■ <code>radiobutton</code> to define radio buttons for the control. Use <code>checked=true</code> to specify the default radio button.
<code>radiobutton</code>	<p>A list of suggestions to allow the user to select or type a value. It requires the <code>valuenam</code> keyword and <code>value</code>. The <code>value</code> should be the name used in the registry, if applicable. You can also use the following with <code>combobox</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>checked</code> to define the default state for the radio button. The default is <code>false</code> (not checked). ■ <code>valueon</code> to specify a value to be written to the registry when the radio button is checked.
<code>dropdownlist</code>	<p>A list of suggestions to allow the user to select a value. It requires the <code>valuenam</code> keyword and <code>value</code>. The <code>value</code> should be the name used in the registry, if applicable. You can also use the following attributes with <code>dropdownlist</code>:</p> <ul style="list-style-type: none"> ■ <code>valuetype</code> to define the type of value in the registry setting. ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>keyname</code> or <code>keynameid</code> to specify the registry setting. Setting the registry key at this level overrides any setting at a higher level, for example, at the category level. ■ <code>editable</code> to specify whether the value in the dropdown list may be edited. The default is <code>false</code> (cannot be edited). ■ <code>required</code> to require a value be set. ■ <code>sort</code> to specify whether sorting is enabled in the dropdown list box.

For this type	You can specify
	<p>You can use the following tags within <code>dropdownlist</code>:</p> <ul style="list-style-type: none"> ■ <code>listitem</code> to define an item in the drop-down list. ■ <code>validation</code> to define validation for user input.
<code>button</code>	<p>Creates a button for a text field defined by <code>edittext</code>.</p> <p>Use the <code>dialog</code> or <code>adbrowse</code> tags with <code>button</code> to define a dialog box to be shown when a user clicks the button.</p> <p>You can also use the following attributes with <code>button</code>:</p> <ul style="list-style-type: none"> ■ <code>text</code> or <code>textid</code> to display a name for the box. ■ <code>valueid</code> to identify the value returned from the dialog box that is launched by clicking the button.

For this type	You can specify
dialog	<p>Provides a dialog box. You associate a dialog box to a button or to a <code>listbox</code>. Use <code>title</code> or <code>titleid</code> to specify the title for the dialog.</p> <p>You can use the following child tags to define a dialog box:</p> <ul style="list-style-type: none"> ■ <code>groupbox</code> to define a group box control in the dialog. ■ <code>text</code> to define a text control in the dialog. ■ <code>edittext</code> to define a text edit box control in the dialog. ■ <code>numeric</code> to define a numeric up down control in the dialog. ■ <code>listbox</code> to define a list box control in the dialog. ■ <code>checkbox</code> to define a check box control in the dialog. ■ <code>radiogroup</code> to define a group of radio button controls in the dialog. ■ <code>dropdownlist</code> to define a drop down list control in the dialog. ■ <code>validation</code> to define the validation on the user inputs in the dialog.
adbrowse	<p>Provides a dialog box for browsing. You associate an <code>adbrowse</code> dialog box to a button or to a <code>listbox</code>. Use <code>text</code> or <code>textid</code> to specify the title for the dialog.</p> <p>To browse Active Directory, use <code>adbrowse type</code> to identify the type of browsing:</p> <ul style="list-style-type: none"> ■ <code>FindADUser</code> ■ <code>FindADGroup</code> ■ <code>FindUnixUser</code> ■ <code>FindUnixGroup</code> ■ <code>FindComputer</code> <p>Use <code>multiselect</code> to define whether a user can select multiple search results in the Active Directory browse dialog.</p> <p>Use <code>separator</code> to specify the separator for multiple results.</p> <p>You can use the following child tags to define an <code>adbrowse</code> dialog box:</p> <ul style="list-style-type: none"> ■ <code>groupbox</code> to define a group box control in the dialog.

For this type	You can specify
	<ul style="list-style-type: none"> ■ <code>text</code> to define a text control in the dialog. ■ <code>edittext</code> to define a text edit box control in the dialog. ■ <code>numeric</code> to define a numeric up down control in the dialog. ■ <code>listbox</code> to define a list box control in the dialog. ■ <code>checkbox</code> to define a check box control in the dialog. ■ <code>radiogroup</code> to define a group of radio button controls in the dialog. ■ <code>dropdownlist</code> to define a drop down list control in the dialog.

Using string IDs

When entering strings, such as text, keynames, and titles, you have the choice of using strings or string IDs. String IDs offer several advantages, such as a cleaner, more modular design, and the ability to customize the text if you plan to port to different languages.

The best practice is to put the string IDs in a 'Strings' section of the template file, which makes them easy to locate and modify in case of porting to other languages.

For example, the following segment from a template file shows how the `explainpage` tag specifies a string ID to attach explanatory text for a policy to the policy dialog box, while the actual text is defined in a 'Strings' section at a different place in the template:

```
- <!--
        Set login password prompt
    -->
- <policy title="Set login password prompt"
        valuenam="pam.password.enter.enabled">
- <page>
    - <edittext text="Set login password prompt"
        valuenam="pam.password.enter.mesg"
        maxlength="1024" default="Password:">
    </edittext>
```

.....

</page>

<explainpage textid="CentrifyDCPasswordPrompt_Explain" />

</policy>

- <!--

.

.

.

- <!--

=====

Strings

=====

<string id="CentrifyDCPasswordPrompt_Explain">The prompt that is displayed when an Active Directory user attempts to log in. Environment variables may be used in the form \$VARNAME if a '\$' character is desired, escape it: \\${</string>

<string id="CentrifyDCPasswordChangeNotify_Explain">The message that is displayed to an Active Directory user when they attempt to change their password. Environment variables may be used in the form \$VARNAME if a '\$' character is desired, escape it: \\${</string>

.

.

.

Validating Settings

You can write validation scripts to check individual settings. The validation scripts are run after a user enters settings but before the settings are saved.

You can use any of the following languages to write validation scripts:

.....

- VBScript
- JScript
- C#
- VB.net

Use the `validation` tag to apply a validation script to a setting. Use `method` to define the validation method name. Use `param` to define a parameter value to pass to the method or `paramval` to pass a registry setting value to the method. The validation result is returned by the method's return value. Use either `dotnetscript` to define a .net script (C# or VB.net), or `script` to define a script (VBScript or JScript) to do the validation.

The following segment from an administrative template file illustrates how to call a validation method:

```
- <validation>
    <method name="Validation.CheckUser" />
- <dotnetscript language="C#">
    - <code>
        - <![CDATA[
public class Validation
{
    public static string[] CheckUser
(string value)
    {
        return Utility.CheckUnixNames
(value, new
        char[] { }, "Unix user name");
    }
}

]]>
    </code>
</dotnetscript>
</validation>
```

.....

You place the code to call the method within a CDATA tag. Likewise, place the validation code itself within a CDATA tag, as in the following example:

```
- <dotnetscript language="C#">
  - <code>
    - <!--
      Validation Utility
    -->
  - <![CDATA[
      using System;
      using System.Text;
      public class Utility
      {
        .
        .
        .
        /// <summary>
        /// Check for a list of Unix names separated by
seps
        /// </summary>
        /// <param name="value"></param>
        /// <param name="seps"></param>
        /// <param name="displayText"></param>
        /// <returns></returns>
        public static string[] CheckUnixNames(string
value, char[]
        seps, string displayText)
        {
          .
          .
          .
        }
      }
    ]>
  - </code>
- </dotnetscript>
```

.....

```
        }  
    }  
]]>  
</code>  
</dotnetscript>
```

Adding a mapper program to the agent

To implement group policies for UNIX computers and users, you need to create the custom scripts or programs that modify the appropriate UNIX configuration files or settings. You can create the programs or scripts using the programming or scripting language of your choice. Most of the Privileged Access Service policies use Perl scripts and you can use those scripts for models if you choose to use Perl.

Once you create a program or script to implement a group policy, you need to:

- Place the program or script in the `/usr/share/centrifydc/mappers/machine` directory if it is a computer configuration group policy, or in the `/usr/share/centrifydc/mappers/user/user_name` directory if it is a user configuration group policy.
- Make the program or script an executable file.
- Use the `runmappers` command to test that the program or script works as expected and updates the appropriate configuration file.

By default, when you use the `runmappers` command, it executes all of the programs in both the `/usr/share/centrifydc/mappers/machine` and the `/usr/share/centrifydc/mappers/user/user_name` directories. Optionally, you can run the command to only execute your custom program. For example, if you have created an executable script called `setport.pl` as a UNIX computer configuration policy and placed the file in the `/usr/share/centrifydc/mappers/machine` directory, you could use a command similar to the following to execute the script along with the other computer configuration mapper programs and test its behavior:

• • • • •

```
runmappers machine map
```

Note To run the mapping programs for a user, you must specify the user's UNIX login name to identify which user's group policies should be mapped or unmapped. For example, to run the mapping programs for the UNIX user account `jgarcia` in the `/usr/share/centrifydc/mappers/user/jgarcia` directory, you could use a command similar to the following:

```
runmappers user jgarcia map
```