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

Multi-factor Authentication Guide

December 2020 (release 2020.1)

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.

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

Preparing to use multi-factor authentication

This guide is intended for UNIX or Windows administrators who intend to configure multi-factor authentication for computers managed by Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service.

Configuration information for Centrify customers who are not using authentication, privilege elevation, and audit and monitoring services to manage their environment, but want to configure multi-factor authentication to log in Windows computers, should go to Downloading the Centrify Agent for Windows.

There are two separate scenarios for which you might want to require multi-factor authentication:

- **Login** access to Centrify-managed computers.
- As part of a **re-authentication** process so that users who are attempting to use Application, Network, and Desktop rights on Windows machines, or command rights with elevated privileges or in a restricted shell on UNIX machines, must provide a password and another form of authentication before they can execute the selected command.

With these two scenarios in mind, you can configure multi-factor authentication based on user roles or computer roles, for specific applications, or for individual commands. You can also skip multi-factor authentication for applications that do not support it or for other reasons on a case-by-case basis by enabling and applying group policy or by setting configuration parameters.

Securing login access

You can configure multi-factor authentication for users logging on to Centrify-managed computers to improve the security of physical or virtual data centers. You can do this by assigning the predefined `require MFA for login` role to users who are required to provide more than one form of authentication. Alternatively, for UNIX and Linux roles, you can also create custom role definitions with the **Require multi-factor authentication for login** system right selected. Because the Windows Login role can be assigned to local accounts, there is no system right for multi-factor authentication, therefore you must assign users the `require MFA for login` role.

Roles and role assignments are important when configuring multi-factor authentication for login access to Centrify-managed computers in hierarchical zones.

Before configuring multi-factor authentication, you should be aware that multi-factor authentication for Centrify-managed computers relies on the infrastructure provided by the Centrify Identity platform and the Centrify identity services.

> **Note:** For Linux and UNIX computers, logging on requires a PAM application such as `login`, `ssh`, or a desktop manager. Most programs that enable users to log in support multi-factor authentication. However, some desktop manager programs that run on older operating systems might not support multi-factor authentication.

Multi-factor authentication and Smart Card PIN login

A smart card user logging in by way of a Personal Identification Number (PIN) will not authenticated by multi-factor authentication. (Ref: CS-38641)

Securing privileged access

If you have installed authentication, privilege elevation, and audit and monitoring services, you can require multi-factor authentication when users perform operations with an elevated access right, in addition to requiring multi-factor authentication when users log in. For Linux and UNIX computers, for example, you can also create command rights that require multi-factor authentication when executing commands using elevated privileges (`dzdo`) or in restricted shell (`dzsh`) environments. For Windows computers, you can create desktop, application, and network access rights that require two-step authentication to use the elevated privileges associated with the desktop, application, or network access.

Before configuring multi-factor authentication for any type of access right, you need to perform some preliminary steps to prepare your environment.

Previewing the preliminary steps

Because multi-factor authentication for Centrify-managed computers relies on the infrastructure provided by the Centrify Identity platform, there are steps that require access to a Centrify Identity platform instance and the administrative portal. As a preview, here are the steps involved in preparing the identity platform to support multi-factor authentication for Centrify-managed computers:

- Register for the **Centrify Identity platform**.
- Install and configure at least one **Centrify connector** for communication with the Centrify Identity platform. Your machine account must have login access to the connector machine.
- Verify the users who are required to provide more than one form of authentication have valid **Active Directory accounts** that are active in the Centrify Identity platform.
- Add or select the **authentication profiles** that specify the types of authentication challenges to support.
- Create a role with the appropriate **computer members and administrative rights** for multi-factor authentication.
- Verify the **server authentication instance URL** you want to use if you have access to more than one authentication instance.

After you have completed the preliminary steps, you can assign users the predefined `require MFA for login` role or, for users of UNIX and Linux machines, a custom role with the **Require multi-factor authentication for login** system right to require two-step authentication when logging on. These preliminary steps are also required if you want to create command rights that require two-step authentication when executing commands using elevated privileges (`dzdo`) or in restricted shell (`dzsh`) environments on UNIX and Linux machines, or when creating roles with elevated Windows rights.

Registering for Privileged Access Service

Multi-factor authentication for Centrify-managed computers relies on the infrastructure provided by Privileged Access Service and authentication and privilege elevation. Privileged Access Service enables you to securely manage users, roles, policies, devices, and applications in the identity platform. You can also define the types of authentication challenges you support and where the multi-factor authentication rules apply.

Sign up and activate your account

To get started, you should register for an account in Privileged Access Service if you are not already a subscriber. You can request a free trial or subscribe to Privileged Access Service through the Centrify website.

If you don't already have a subscription, you can start by requesting access to Privileged Access Service by visiting the Centrify website.

After you register for a Centrify account with a valid email address, you will receive an "Activate Your Centrify Account" email followed by a "Your Centrify Account Is Ready - Next Steps" email with your account details. Your account details include the user name and temporary password for an administrative account that is a member of the predefined `System Administrator` role and a unique customer identifier. For example, your email message might have account details similar to the following:

Privileged Access Service management:	https://aacl0287.my.centrify.net/manage
Your User Name:	admin_maya.garcia@acme.net
Your Temporary Password:	hKGo!wd2N (You'll be asked to change this when you log in)
Customer ID:	AAEK0012

Use your account details to log in and set a new password for your administrative account.

Start or skip the wizard

After you log in successfully, you will see a Welcome to Privileged Access Service message with the option to start or skip the quick start wizard.

If you click Start the Wizard, you are prompted to manage mobile devices, add web applications, add mobile applications, add users, and invite users. You can click Next to skip any or all steps. None of the steps in the wizard are required to set up multi-factor authentication.

If you are only interested in preparing for multi-factor authentication, you can select the **Don't show this to me again** option, then click **Skip**. If you click Skip now, you can run the wizard at any time after configuring multi-factor authentication by clicking **Start Wizard** on the Getting Started dashboard.

If you have not completed these preliminary steps, stop here and verify that you have received the "Your Centrify Account Is Ready - Next Steps" email and that you can log in to the Privileged Access Service platform with the account information in the email.

Planning multi-factor authentication for Centrify-managed computers

Privileged Access Service is most often used to store information about people and devices, to identify different classes of users and devices, and to define the policies that specify what different classes of users and devices can do. To support multi-factor authentication, however, you must also add Centrify-managed computers to the access service.

Any computer that will require multi-factor authentication must also be added as a member of an identity platform-based role. This step is similar to adding computers to a zone. For multi-factor authentication, an identity platform-based role has computers as members and is managed through Privileged Access Service. It is separate from the role definitions and role assignments you manage using Access Manager or other authentication, privilege elevation, and audit and monitoring services components.

Installing and configuring a connector

The connector is a multipurpose service that enables secure communication between your internal network and Privileged Access Service. Multi-factor authentication requires at least one connector to be installed on your network inside of the firewall. The connector provides the link between your internal Active Directory forest and the Privileged Access Service platform.

You can install more than one connector for your organization to support fail-over and load balancing. You might also want to install more than one connector if you are using multiple instances of Privileged Access Service or have access to more than one customer-specific Identity platform instance URLs. In most cases, you should install at least two connectors in a production environment.

To install a connector on a domain computer

1. Open a browser and log in to the appropriate customer-specific Identity platform instance using the account information you received in your email notification.
2. In Admin Portal, **Click Settings > Network > Centrify Connectors**.
3. Click **Add Centrify Connector**.
4. Under Download, click the **64-bit** link to download the connector package.
5. Open the file you downloaded.

   If the User Account Control warning is displayed, click **Yes** to continue.
6. On the Welcome page, click **Next**.
7. Select the “I accept the terms in the license agreement” option, then click **Next**.
8. Select the components to install and verify the location for installation or click Browse to select a different location, then click **Next**.

By default, all components are selected. You must install the Centrify connector to prepare for multi-factor authentication. The other components are optional, but might be required if you want to use other features or services.

9. Click **Install**.

   If necessary, close any open applications to complete the installation.

10. Click **Finish** to open the connector configuration wizard.

By default, the configuration wizard is displayed immediately after the connector is installed.

To configure the connector

1. On the Welcome page, click **Next**.
2. Type the administrative user name and password for your Centrify account, then click **Next**.
3. Click **Next** unless you are using a web proxy server to connect to Centrify Identity platform services.

   If you are using a web proxy service, type the IP address, select the port, and specify the user name and password to use.

4. The configuration wizard performs several tests to ensure connectivity. If all of the tests are successful, click **Next**.

   As the final step, the connector registers your customer-specific identifier with Privileged Access Service, then runs in the background as a Windows service. The customer identifier that gets registered also automatically defines the default Identity platform instance URL to use for parent and child zones. If you have access to more than one customer-specific tenant URL, you can change the Privileged Access Service instance to use on a zone-by-zone basis.

5. Click **Finish** to complete the configuration and open the connector configuration panel, which displays the status of the connection and your customer-specific identifier.
6. Click the **connector** tab to view or change any of the default settings.
7. Click **Close**.

Establishing a connector identity for multi-factor authentication

In order to enable multi-factor authentication for Centrify-managed UNIX and Linux machines, the connector must validate the machine credentials using the Integrated Windows Authentication (IWA) service. To use the IWA service, your connectors must be configured to use an HTTPS-enabled port.

To configure connectors to use an HTTPS-enabled port, you must either download a host certificate issued by Centrify, or upload a host certificate issued by a Certificate Authority already trusted by your environment.

To configure Windows computers for multi-factor authentication, you must establish an initial trust relationship between the Windows machine and the Centrify connector. Since the connector accesses the IWA service through a secure HTTPS channel, you must validate the correct certificate during installation when enabling multi-factor authentication for login.

If you are operating in an evaluation environment, and cannot easily set up the required certificate trust relationship, you have the option to skip this step during installation and trust your own connector without enrolling in the IWA service. In this case, the computer is connected directly to the Centrify Identity platform, and multi-factor authentication can be enabled. Note, however, that this should only be done in an evaluation environment, as it has serious security implications in a live production environment.

If you have chosen not to establish the trust relationship, but wish to do so in the future, you can either leave and then rejoin a zone if you are joined to one, or you can disable and then re-enable multi-factor authentication for login to launch the configuration wizard.

To configure a connector to use a Centrify-issued root certificate

1. In the Admin Portal, click **Settings > Network**.
2. Select the connector you want to configure, and choose **Modify** from the **Actions** menu.
3. In **IWA Service**, click **Download your IWA root CA Certificate** to retrieve the public certificate for the tenant-specific CA certificate issued by Centrify.
4. Click **Download** to download the host certificate issued by Centrify for your connector.

You can export the `IwaTrustedRoot.cer` trusted root CA certificate issued by Centrify and manually install it on a local computer, or use group policy to distribute the certificate file as a trusted root certificate to multiple computers

Note: Centrify Express users cannot use group policies to distribute certificates in bulk to UNIX and Linux computers. To distribute the certificates, you must download and install the certificate in the appropriate directory on each computer.

To import the certificate manually to a local Windows computer

1. Right click on the certificate you downloaded in To configure a connector to use a Centrify-issued root certificate.
2. Select **Install Certificate** to start the Certificate Import Wizard.
3. Select **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Select **Trusted Root Certification Authorities** and click **OK**.
6. Click **Next** and then **Finish** to complete the Wizard.

   A Windows Security Warning may be displayed. Click Yes to finish installing the certificate.

To export the certificate for bulk Group Policy distribution

1. Select the trusted root certificate you downloaded, right-click, then click **Open**.
2. Click the **Details** tab and click **Copy to file** to start the Certificate Export Wizard, then click **Next**.
3. Select **DER encoded binary X.509 (.CER)** as the file format, then click **Next**.
4. Click **Browse** to select a location on the local server, type a file name and click **Save**, then click **Next**.
5. Click **Finish**.

To distribute the certificate using group policy

1. Open Group Policy Management to select the group policy object that defines the IP Security policies, then click **Edit**.

2. Click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
3. Select **Trusted Root Certification Authorities,** right click, and select **Import** to open the Certificate Import Wizard.
4. Click **Next** on the **Welcome** screen.
5. Browse to find the root certificate you downloaded, then click to accept the default values on each screen.
6. **Click Finish** to complete the wizard.

   The root certificate is now in the Active Directory Trusted Root Certification Authorities container. Group policy publishes all certificates in this container to computers joined to the domain. You can also run the `gpupdate` command from a command prompt to push the certificates to the computers in the domain.

Using a host certificate not issued by Centrify

If you want to use integrated Windows authentication over an HTTPS-enabled port with a certificate issued by a certificate authority (CA) that is trusted by your organization, you must upload the host certificate to the Identity platform instance to ensure the computer credentials can be validated for secure communication between the connector and the authentication server.

To use an existing host certificate for a connector

1. In the administrative portal, click **Settings > Network**.
2. Select the connector you want to configure, and choose Modify from the Actions menu.
3. Click **IWA Service**.
4. Click **Upload** and navigate to the location of the certificate trusted by your organization.

This certificate must be trusted by both the local computer and the Identity platform instance.

Note: You may get the following error while enrolling a Windows agent/machine into the cloud-based CIS with debugging enabled:

```
Failed to auto-enroll to the cloud:
System.Net.Http.HttpRequestException:

An error occurred while sending the request. --->
System.Net.WebException:

The underlying connection was closed: Could not establish trust
relationship for

the SSL/TLS secure channel. --->
System.Security.Authentication.AuthenticationException:

The remote certificate is invalid according to the validation
procedure.
```

If so, check your local machine trusted root CA. The server may not have the corresponding DigiCert Global Root CA installed. If so, export the local cert. Then import the cert to the server. After that, you should be able to enroll the server.

Verify open ports

Multi-factor authentication requires the following ports to be open for inbound communication and domain traffic:

- Port 8080 for HTTP API proxy
- Port 8443 for secure HTTP (HTTPS) connections

Installing the connector automatically sets Windows firewall rules to open these ports. However, if you are using a third-party firewall instead of the default Windows firewall, you should manually modify the port rules to allow the Centrify Agent for Windows to communicate with the Centrify connector. Both ports are required because integrated Windows authentication over HTTPS uses port 8443 to enable the connector to receive inbound connections from the agents.

Logging on and verifying connector settings

After you have installed and configured at least one connector, you can use either the Admin Portal or your default browser to log in to the Centrify Identity platform.

To log in and verify settings

1. Open a browser and log in to your customer-specific identity platform instance URL.
2. Type the user name from your account details and the password you set when you activated the service.

   If you see the Welcome message, select the “Don’t show this to me again” option, then click **Close**.

   By default, the Getting Started dashboard is displayed in the Admin Portal. The Getting Started dashboard has links to topics that explain important tasks—such as creating roles and adding users—for the Centrify Identity platform. You will perform similar steps to prepare for multi-factor authentication. However, you can skip those steps for now. For multi-factor authentication, you should first verify some settings on your connector and, if necessary, prepare a new Active Directory group for the computers where you plan to use multi-factor authentication.
3. Click **Settings > Network > Centrify Connectors**.
4. Select the connector and then select **Modify** from the Actions menu to display the connector Configuration.
5. Verify the following options are selected under IWA Service:
   - Enable Web Server

     This option is required to enable integrated Windows authentication for Centrify Agents and multi-factor authentication.
6. Click **Save**.

Preparing a group for Centrify-managed computers

After verifying connector settings, you can use Active Directory Users and Computers or other tools to prepare an Active Directory group for the computers where you plan to require multi-factor authentication. Although you can use any existing Active Directory group for this purpose, the steps in this guide assume you will use a new group specifically for multi-factor authentication.

Multi-factor authentication requires computers to be members of an **identity platform role** assigned a specific **administrative right** in the Centrify Identity platform. You can add individual computers independently without using an Active Directory group. However, using an Active Directory group is the recommended approach and facilitates the deployment of computer roles that link user role assignments to computer groups.

To add an Active Directory group for multi-factor authentication

1. Open Active Directory Users and Computers.
2. Select a location, right-click, then select **New** > **Group**.

   For example, if you are using the default deployment structure, you might expand the Centrify organization unit and select Computers, then right-click to create a new group in that organizational unit.
3. Type a group name, select the group scope, and verify the group type, then click **OK**.

   For example, type `MFA-Group`, select Global for the group scope, and verify the group type is Security, then click **OK**.

Preparing a role for Centrify-managed computers in the Admin Portal

After you have prepared an Active Directory group for the computers where you plan to require multi-factor authentication, you can use the Admin Portal to prepare a role for those computers.

To prepare a role in the Admin Portal:

1. In the Admin Portalclick **Core Services**, then click **Roles**.
2. Click **Add Role**.
3. Type a role name and, optionally, a role description.

   For example, type `MFA-LinuxComputers` as the role name and `Role for multi-factor authentication of Linux Computers` as the role description, then click **Save**.
4. After naming the role, click **Members**, then click **Add**.
5. Type a search string to locate the Active Directory group you are using for computers that require multi-factor authentication.

   For example, if you created a group called Audited Servers in Preparing a group for Centrify-managed computers, you might type “aud” as the search string to locate that group. Alternatively, you can search for and add individual computers to the role if you are not using an Active Directory group. Adding individual computers to the role, however, is not a scalable approach for most organizations.

   This step creates the link between the Centrify-managed computers and the identity service. There is no change to how you manage the computers

you add to the identity service. This link is required to allow Privileged Access Service to provide authentication profiles to managed computers.

6. Select the group, then click **Add**.
7. Click **Administrative Rights**, then click **Add**.
8. Select the **Computer Login and Privilege Elevation** administrative right, then click **Add**.

   This administrative right is only applicable for the computers that are members of the identity platform role. The right does not apply to users and is ignored for any users added as members of the role. In general, you should not add users to any role that is intended for multi-factor authentication on Centrify-managed computers.
9. Click **Save**.

Adding a user or group for MFA to a role with an Admin Portal-specified policy

Offline MFA mode is not triggered during logon to the computer once the agent has successfully connected to the cloud. Logon will fail if the cloud fails to authenticate the user, the user is not allowed to perform the MFA logon, or if the user is not assigned to any profile in the portal.

To add a user or group to a role in the Admin Portal

1. Create a new role or double-click an existing role that is policy-specified.
2. Click **Members** > **Add**.
3. Enter a search string to locate the Active Directory groups or users you are using that require multi-factor.
4. Select the group or user and then click **Add**.
5. Click **Save**.

Preparing authentication profiles

With Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service, you can require multi-factor authentication for two distinct situations:

- As part of the **login** process so that users who are attempting to log in to Centrify-managed computers must provide multiple forms of authentication before they are granted access.
- As part of a **re-authentication** process so that users who are attempting to use Application, Network, and Desktop rights on Windows machines, or command rights with elevated privileges or in a restricted shell on UNIX machines, must provide a password and another form of authentication before they can execute the selected command.

To configure the types of authentication challenges allowed in each situation, you can prepare one or more **authentication profiles** in the Admin Portal. If you have already configured authentication profiles for other purposes, you can reuse those profiles for multi-factor authentication or add new profiles specifically for the computers you manage using authentication, privilege elevation, and audit and monitoring services. You can prepare one profile to use for both login access and for the use elevated privileges or you can prepare separate profiles for each situation.

Creating an authentication profile

The first step in preparing authentication profiles is to create the profile.

To create an authentication profile:

1. Open a browser and log on to Privileged Access Service using your customer-specific URL.
2. Navigate to **Settings** > **Authentication**.

Three default authentication profiles are available out-of-the-box:

- **Default New Device Login Profile**: Uses Password for the first challenge and Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client for the second challenge with a 12 hours pass-through duration.
- **Default Other Login Profile**: Uses Password for the first challenge and no secondary challenge with a 12 hours pass-through duration.
- **Default Password Reset Profile**: Gives the option for users to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client for the first challenge with a 12 hours pass-through duration.

3. Select an existing Authentication Profile or click **Add Profile**.

   The fields needed to **add new profile**.

   a. Type the authentication profile name.

   b. Select the types of authentication to present for the first challenge.

      Note: The second authentication is not needed. Challenge two is a third mechanism.

   c. Click **OK**.

The pass-through option does not apply to Windows, Linux, or UNIX MFA logins unless you specify otherwise in the policy settings.

Select the authentication mechanism(s) you require and want to make available to users. Some authentication mechanisms require additional configurations before users can authenticate using those mechanisms. See Authentication mechanisms for information about each authentication mechanism.

For example, you can require that the first challenge be the user's account password. Then for the second challenge, users can choose between an email confirmation code, security question, or text message confirmation code.

If you have multiple challenges, Privileged Access Service waits until users enter all challenges before giving the authentication response (pass or fail). For example, if users enter the wrong password for the first challenge, we will not send the authentication failure message until after users respond to the second challenge.

If users fail their first challenge and the second challenge is SMS, email, or phone call, the default configuration is that Privileged Access Service will not

send the SMS/email or trigger the phone call. Contact support to change this configuration.

Assigning Login Authentication Profiles

The next step is to assign login authentication profiles to policies. In this task, you set up a policy so that if specified conditions are met, the affected users proceed according to a specified authentication profile. If those conditions aren't met, you can specify a default authentication profile or block access entirely.

For example, you could set a policy that says that during work hours of Monday to Friday, 8:00 am to 5:00pm, users log in using an authentication profile that requires a password and a security question. For users logging in outside of those days or times, users will have to login with a password, security question, and an email confirmation code.

As a reminder, you use **authentication profiles** to define the necessary authentication methods to use. You define **authentication rules** to specify where to enforce those authentication profiles inside of a policy set.

To assign a login authentication profile to a policy set:

1. In the Admin Portal, go to **Access** > **Policies** and either click **Add Policy Set** to create a new policy or click an existing policy to edit.
2. Create or edit the policy set and assign it to the desired users or resources.

   For details, see "Creating policy sets and policy assignments" in the Privileged Access Service help.
3. In the Policy Settings area, navigate to Authentication > Centrify Server Suite Agents > and click one of the following settings:

Policy Setting	Description
Linux, UNIX and Windows Servers	For Linux and UNIX Servers or Workstations where the Centrify Agent for *NIX is installed and enabled. For Windows Servers where the Centrify Agent for Windows is installed and enabled
Windows Workstations	For Centrify-managed workstations where the Centrify Agent for Windows is installed and enabled. The operating system variant determines if it's a workstation.
Privilege Elevation	For systems where either the Centrify Agent for *NIX or Centrify Agent for Windows is installed and enabled.

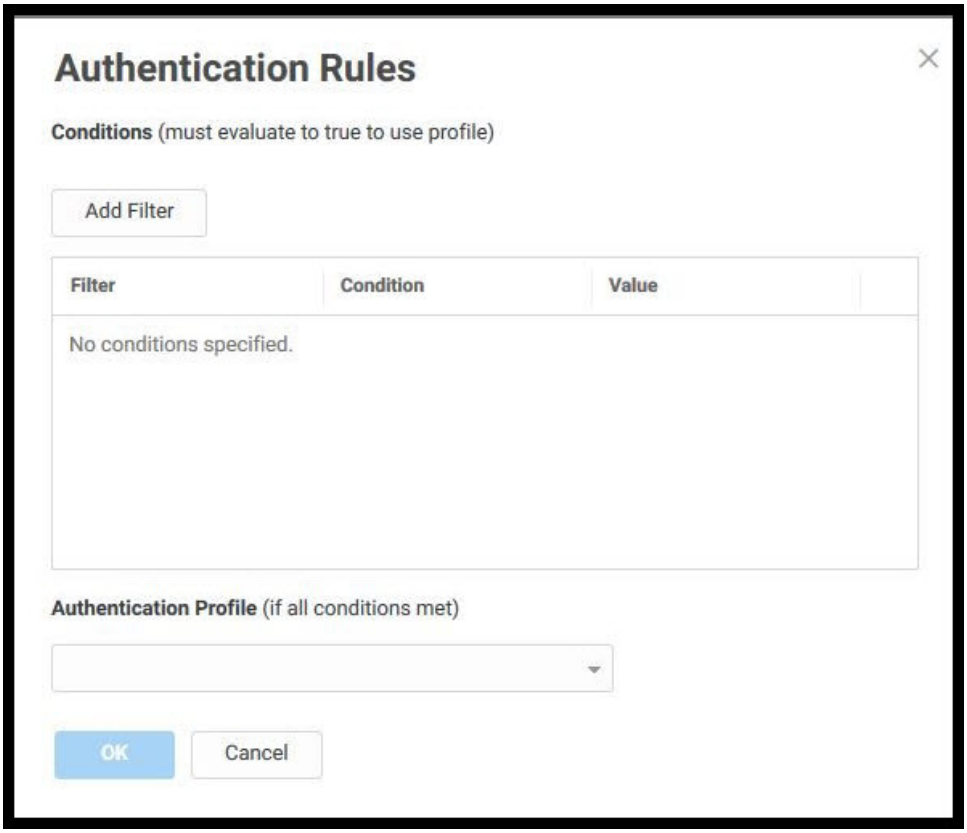
Note: For any of the above policy settings, the role assignment associated with this policy must include computer objects or groups in Active Directory and also the "Computer Login and Privilege Elevation" administrative rights.

4. Select **Yes** in the **Enable authentication policy controls** drop-down.

   The Authentication Rules section displays. You use this section to define which authentication profiles apply under which conditions.

5. (Optional) If you want to specify conditions for which different authentication rules apply, click **Add Rule**. Otherwise, proceed to step

   The Authentication Rules window displays.



6. Click **Add Filter**, and then click the same drop-down to spicy which kind of condition.

   For example, you can create a rule that requires a specific authentication method when users access Privileged Access Service from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor applies as follows: ■ For Privileged Access Service on-premise, the authentication factor is the connector's IP address when you log in. When using HTTP proxy, the authentication factor is the HTTP Proxy server's IP address when you log in. ■ For Privileged Access Service from the Centrify user portal, the authentication factor is the tenant connectors' public IP address when you log in. When using HTTP proxy, the authentication factor is the HTTP proxy server's public IP address when you log in. This option requires that you have configured the IP address range under **Settings** > **Network** > **Corporate IP Range**. **Note:** For Windows machines that can access the Internet, the authentication factor is the machine's IP address when you log in.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the directory service after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.

Filter	Description
Risk Level	Risk Level: The authentication factor is the risk level of the user logging on to Admin Portal. For example, a user attempting to log in to Privileged Access Service from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Centrify support. The supported risk level are: ■ Non Detected — No abnormal activities are detected. ■ Low — Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. ■ Medium — Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. ■ High — Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. ■ Unknown — Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.	

7. Click the **Add** button associated with the filter and condition.
8. Select the authentication profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

   The authentication profile defines which authentication methods to use. If you have not created the necessary authentication profile, select the **Add New Profile** option in the list (it's at the bottom of the list).
9. Click **OK** to close the Authentication Rules dialog box.
10. If desired, continue adding authentication rules. You can drag the rules to change the order of priority. The highest priority rule is at the top of the list.
11. Select a default profile to be applied if a user does not match any of the configured conditions in the **Default Profile (used if no conditions matched)** drop-down.

Note: If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.

12. If this policy setting is for Linux, UNIX, and Windows Servers, you have the option to configure how the pass-through duration applies. The pass-through duration is how long before the user needs to re-authenticate, and you define the pass-through duration in the authentication profile (for example, the default is 30 minutes). Select one of the following options:
    - **Never (default):** Always prompt for MFA and ignore the pass-through setting.
    - **If Same Source and Target**: Apply the pass-through duration if the user is logging in from the same system and where they're logging in to is the same system as compared to the initial login.
    - **If Same Source**: Apply the pass-through duration if the user is logging in from the same system as compared to the initial login.
    - **If Same Target**: Apply the pass-through duration if the user is logging in to is the same system as compared to the initial login.
13. If desired, you can add multiple policy settings to the same policy set.
14. Click **Save**.

Assigning Privilege Elevation (Re-authentication) Profile

Finally, you must assign privilege elevation profiles.

1. For Elevated Privileges Profile, click **Privilege Elevation Policies > Privilege Elevation**, select **Yes** for Enable authentication policy controls, and **Add Rule > Add Filter,** click **Authentication Profiles** and display the list of existing profiles and select a profile to use or click **Add New Profile**.

   You can use the same profile for server access, and to re-authenticate for roles and rights that require multi-factor authentication. However, if you want to specify different authentication challenges from which a user can select when executing UNIX commands or accessing Windows applications, select **Add New Profile**.

As with the Login Authentication Profile, you can select multiple types of authentication to present for the first and second challenges. However, only the authentication challenges that are applicable for a user can be presented when the user attempts to access privileged Windows rights or execute UNIX commands with elevated privileges (`dzdo`) or in a restricted shell (`dzsh`).

2. Click **Save**.

Configuring roles and rights to use multi-factor authentication

You can prepare for multi-factor authentication before or after installing authentication, privilege elevation, and audit and monitoring servicescomponents. The steps in this section summarize what to do to finish configuring multi-factor authentication for login access and executing commands for computers in hierarchical zones. You can use Access Manager, `adedit`, or Access Module for PowerShell scripts to complete most of the next steps.

For more information about performing these tasks, see the following documentation:

- Planning and Deployment Guide
- Administrator's Guide for Linux and UNIX
- Administrator's Guide for Windows

For example, see the *Administrator's Guide for Linux and UNIX* for more detailed information about how to create zones, configure role definitions, and add command rights for Linux and UNIX computers.

To configure multi-factor authentication

1. Install Access Manager and other components.
2. Create at least one hierarchical zone.
3. Verify the Identity platform instance URL for the zone by displaying the zone properties, then clicking the Platform tab.

   If necessary, you can click Browse to select a different Identity platform instance if you have access to more than one customer-specific Identity platform instance URL.

4. Assign the predefined `require MFA for login` role definition to the Active Directory users who have access to computers where you want to require multi-factor authentication and who are already assigned the UNIX Login or Windows Login role.

   Alternatively, you can create one or more custom UNIX or Linux role definitions that include the **Require multi-factor authentication** system right. Note that you can also use the Access Module for PowerShell to set the system right described in this step.

5. Define the rights you would like to add to the role and select the **Require multi-factor authentication** re-authentication option on the Attributes tab.

   After you create rights that require multi-factor authentication, add the rights to the appropriate role definitions and assign the roles to the appropriate Active Directory users.

   Note that you can also use the Access Module for PowerShell to require multi-factor authentication for command execution.

6. Refresh the agent.

   For a UNIX computer requiring multi-factor authentication, run `adflush -f` or restart the agent to test multi-factor authentication for login access and command execution.

   For a Windows computer requiring multi-factor authentication, run `dzrefresh` from a command prompt. Depending on your permission settings, you may need to open the command prompt using “Run as administrator.”

   Note: When you initially update or install the Centrify Agent for Windows and configure multi-factor authentication for login, there may be a slight delay while the cache refreshes. During this short period, users who are required to use multi-factor authentication to log in may only be asked for their Active Directory credentials. When they logout from their machine, the cache will have refreshed, and they will then be required to use multi-factor authentication in future login attempts.

Configuration options for Linux and UNIX computers

After you have completed the basic steps to enable multi-factor authentication, you might want to customize the configuration to suit your environment or to address specific scenarios. For example, you might want to enable group policies or set configuration parameters if you want to modify the default multi-factor authentication operations.

For more information on setting group policies for multi-factor authentication, please see the *Centrify Group Policy Guide*. For information on setting configuration parameters, see the *Centrify Configuration and Tuning Reference Guide*.

The next sections discuss the most common customization scenarios.

Adding rescue rights

You should have at least one role with the “rescue” system right for the UNIX and Linux computers in hierarchical zones where you are requiring multi-factor authentication. This system right enables selected users to log in in cases where multi-factor authentication cannot be completed. For example, if a UNIX computer where multi-factor authentication is required is disconnected from the network and cannot access the Centrify Identity platform, only users with the “rescue” right will be able to log in until the connection to the identity platform is restored.

Configuring secure shell (ssh) for multi-factor authentication

If you are planning to require multi-factor authentication for secure shell (ssh) sessions and you want to use a native secure shell package, you should review

the settings in the secure shell configuration file (`sshd_config`) to be sure that the `ChallengeResponseAuthentication` option is set to `yes`.

You can edit the file manually or enable the “Allow challenge-response authentication” group policy to automatically configure this setting. You can find this group policy in the Group Policy Management Editor under Computer Configuration > Policies > Centrify Settings > SSH Settings. For more information about adding, enabling, and applying Centrify group policies and the other group policies you can use for secure shell sessions, see the *Group Policy Guide*.

Enforcing multi-factor authentication for single sign-on login access

If you use the Centrify OpenSSH package, you can require multi-factor authentication for secure shell connections even for single sign-on access to remote computers. In this scenario, users must respond to the authentication challenges to open the secure shell connection then be silently authenticated to additional services and computers. Note that this scenario is only supported if you are using the Centrify version of the OpenSSH package and not supported for native secure shell packages. To enable multi-factor authentication for single sign-on using secure shell sessions, you must enable and apply the Enable SSO MFA group policy. You can find this group policy in the Group Policy Management Editor under Computer Configuration > Policies > Centrify Settings > SSH Settings. For more information about adding, enabling, and applying Centrify group policies and the other group policies you can use for secure shell sessions, see the *Group Policy Guide*.

If you are not enabling and applying group policies for Centrify-managed computers, you can manually enforce multi-factor authentication for single sign-on by setting the secure shell configuration parameter `SSOMFA` to `yes` in the `/etc/centrifydc/sshd/sshd_config` file.

If you enable the group policy or set the parameter and auditing is set to required, users who access a Centrify-managed computer using `ssh` or PuTTY are prompted to respond to the multi-factor authentication challenges before starting the shell session. Securing the shell session with multi-factor authentication prevents unauthorized users from using the secure shell session to connect to remote services and computers.

Requiring multi-factor authentication for PAM applications

If you select the “Multi-factor authentication required” system right in a role definition, the PAM applications you add to the role will require users to provide a secondary form of authentication to log in successfully. You define the forms of authentication available and presented to the user in the **authentication profile** you have configured in the Centrify Identity service using the administrative portal.

Note that some applications do not support multi-factor authentication and users might be denied access to applications that they would otherwise be able to use. For example, if a specific version of an application that you want to use only supports a single layer of authentication—such as a password challenge—users would be prevented from logging on and using the service even if they are assigned to a role with the predefined `login-all` PAM application right.

If you want to grant access to applications that only support one layer of authentication in roles where you are generally using the “Multi-factor authentication required” system right, you must add those applications to the list of applications for which you want to skip multi-factor authentication. You can update the list of applications for which to skip multi-factor authentication by enabling and modifying the “Specify programs for which multi-factor authentication is ignored” group policy or setting the `pam.mfa.program.ignore` configuration parameter in the `centrifydc.conf` file.

Before assigning roles with multi-factor authentication required to users, you should test access to all of the applications you expect users to access to verify they won’t be unexpectedly denied access simply because multi-factor authentication isn’t supported. Because the applications that don’t support multi-factor authentication will depend on the platforms and the versions of the applications you plan to support, testing in your own environment is the only way to determine which applications to add to the `pam.mfa.program.ignore` configuration parameter.

The most common applications that are known to only support a single password challenge and response for authentication are ignored for multi-factor authentication by default. For example, some versions of `vsftpd`, `java`, and `httpd` do not support multi-factor authentication and are ignored by default.

Additionally, while some platforms support multi-factor authentication for all PAM applications, they may not allow you to require multi-factor authentication for GUI log in. For example, for users running AIX, Solaris, and HP-UX, multi-factor authentication for GUI login is not supported.

Configuring multi-factor authentication in legacy zones

If you want to configure multi-factor authentication for UNIX and Linux computers in classic zones or in Auto Zone, you must follow different steps than in hierarchical zones. For multi-factor authentication on computers in the "legacy" types of zones, you must either enable and apply group policies or set configuration parameters.

You can find these group policies in the Group Policy Management Editor under Computer Configuration > Policies > Centrify Settings > DirectControl Settings > MFA Settings. For more information about adding, enabling, and applying Centrify group policies, see the *Group Policy Guide*. For more information about setting configuration parameters, see the *Configuration and Tuning Reference Guide*.

Configuration options for Windows computers

The following sections describe multi-factor authentication configuration options for Centrify-managed Windows computers. In addition to these options, you can use group policies to customize basic operations for connecting to the Centrify Identity platform and multi-factor authentication on Windows computers. For more information on these group policies, please see the *Group Policy Guide*.

You can find the group policies for multi-factor authentication and the grace period on Windows computers in the Group Policy Management Editor under **Computer Configuration > Centrify Settings > Windows Settings > MFA Settings**.

To set the grace period, use the following group policies:

- Configure multi-factor authentication lock screen grace period. This group policy enables the grace period for lock screen.
- Configure multi-factor authentication user privilege elevation grace period This group policy allows the administrator to set the grace period for privilege elevation for users.

Reset Password

Password reset is a very popular self-service capability for Identity and Access Management solutions: It reduces calls to the help-desk and enables users to become productive quickly. The system allows the user to make a limited number of reset password requests within a specified period.

Note: This feature does not enable the user to unlock their account.

• • • • • •

To reset your password (user instructions):

1. On the login screen, click the **Forgot Password** link.

   A prompt appears asking the user name. (If the user already entered their username using the login screen, it appears in this user name field.)

2. Complete the MFA challenges, which are based on the password reset profile.

3. A new prompt asks you to enter a new password and confirm it.

   After resetting the password, you can log in using the normal login screen.

Disable self-service password reset

Configuring this policy setting allows the administrator to force disable the 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.

Configuring offline multi-factor authentication and rescue users

When a Windows computer that is running a Centrify Agent is not configured to use multi-factor authentication, you can use a local account to rescue that system when it cannot connect to the Centrify Identity platform.

Local users do not require MFA challenge. For non-safe mode in Windows Operating System:

- With **Centrify Privilege Elevation Service** (zone mode) a local user can log in without MFA whenever they cannot connect to Centrify Identity Platform. The exception is that the local user does not assign roles for either "Window login permit" or "rescue user."
- Without **Centrify Privilege Elevation Service** (zoneless mode) a local user is allowed to log in without MFA.

For safe mode in Windows Operating System, a local user can only log in as a rescue user. To set a rescue user for zone mode, go through the Access Manager to assign roles. To set a rescue user for zoneless mode, go through Group Policies to configure.

If a computer that is joined to a zone starts in Safe Mode, only users who are assigned a Login role with the system rescue right selected will be able to access the machine. These users will not be required to use multi-factor authentication.

Users who are required to use multi-factor authentication to log in to their Windows workstations can set up an offline MFA profile to use as a second form of authentication in the event that their machine cannot connect to the Centrify Identity platform. These users will see a system notification urging them to set up this passcode each time they log in to their machine until they configure it.

Users set up their offline MFA profile in following way:

To set up an offline MFA profile:

1. Right click the Centrify notification icon in the system notification area, and select **Setup Offline MFA Profile**.
2. Click **Next** to begin the Offline Authentication Wizard.
3. Select one of the following methods to create a authenticator account profile on your mobile device:
    - **Scan barcode**

      If you select this option, a QR code is displayed for you to scan using your mobile authenticator application. You can use either the Centrify application or a third-party authenticator application.
    - **Manual entry**

      If you select this option, you must manually enter the displayed account profile information into your authenticator application.

- **Program YubiKey**

  If you select this option, you can use a YubiKey as the second form of authentication. You'll then need to select which slot on the YubiKey to use, and whether or not to use Yubikey's touch-to-sign feature.

4. Enter the passcode that is generated after you have created your authenticator profile. Click **Next**.
5. Click **Finish** to exit the Wizard.

After a user has set up their offline MFA profile, they will be prompted to enter the mobile passcode generated by their authentication application or YubiKey as the second form of authentication when they attempt to log in to their machine if it cannot connect to the Centrify Identity platform instance.

Note: If you have already set up your offline MFA profile and want to reconfigure (override) it, you will be prompted for multi-factor authentication. That profile is set in the MFA Login Policy.

Requiring multi-factor authentication using computer roles

Computer roles can enable you to group and provide access to computers through role assignments. One strategy you might find useful is to use computer roles to control where multi-factor authentication should apply. For example, you might have several computers with highly sensitive material where you want to ensure all user access will require multi-factor authentication. To accomplish this goal, you can configure a computer role, then add and remove computers with sensitive information to control whether multi-factor authentication is required.

To require multi-factor authentication based on a computer role

1. Open Access Manager.
2. Expand Zones and the individual parent or child zones required to select the zone name that will contain the new computer role.
3. Expand Authorization to select Computer Roles, right-click, then click **Create Computer Role**.

4. Type the role name and, optionally, a role description, then select **<Create group>** for the Computer group to create a new Active Directory group for computers.

   For example, to create a new Active Directory security group for the computers with sensitive information, click **Browse** to select the Active Directory location for the new group. If you are using the default deployment structure, you would browse to a location similar to `centrify.pubs.org/Centrify/Computer Roles` then type a group name such as `mfa_required_consols`, select a scope, and click **OK**.

5. Click **OK** to save the new computer role.

6. Add the computers that require multi-factor authentication for access to the `mfa_required_consoles` Active Directory security group.

   As you add computers to the Active Directory security group, the computers are listed as Members of the computer role.

7. Expand the computer role you created in Step 4, select Role Assignments, right-click, then select **Assign Role**.

   For example, if you created a new computer role with the role name `CR_MFA_required`, expand that computer role name to select Role Assignments, right-click, then select **Assign Role**.

8. Select the predefined `require MFA for login` role definition, then click **OK**.

9. Select **All Active Directory accounts**, then click **OK**.

Using multi-factor authentication when there are selective cross-forest trusts

If you have domains in different forests that have a two-way selective trust relationship, any computer or user accounts that are used to log on to the remote forest must be granted the “Allowed to authenticate” right on the domain controllers in both forests to get role information.

In addition to granting the “Allowed to authenticate” right to users and to computers with the Centrify Agent for Windows installed, the right must also be granted to computers that host your Centrify connectors.

After you grant these computers and users the “Allowed to authenticate” right for the domains in both forests, users that are assigned a role with a multi-

factor authentication right for login and privilege elevation will be able to authenticate using any of the authentication mechanisms that you have assigned to them.

If a connector is not allowed to authenticate on the remote domain controller, some multi-factor authentication mechanisms may fail to authenticate users.

Configuring MFA with RADIUS for Centrify Privilege Elevation Service for Windows checklist

This document provides a configuration checklist for 3rd party multi-factor authentcation providers such as Duo, Okta, SecurID (or any other vendor that provides a RADIUS service) to provide identity validation with the Centrify Privilege Elevation Service in the Microsoft Windows platform.

If you have an identity service provider (such as Duo, Okta, SecureID, and so forth) that you use for MFA logins, you can integrate authentication and privilege elevation with your identity provider and the RADIUS protocol to require MFA for privilege elevation tasks, such as Run with Privilege and New Desktop.

Make sure that you work with your RADIUS expert along with your network and directory services lead administrators during the design and configuration tasks.

The checklist below includes links to documented procedures.

Note: If you use Privileged Access Service, although you can enable MFA with RADIUS, the recommended practice is that you use the native integration.

Step#	RADIUS Configuration Step	Notes
	RADIUS requirements	
1	Gather the following settings for your RADIUS service: ■ IP address or fully qualified domain name ■ Port ■ Timeout settings ■ Pre-shared secret	

Step#	RADIUS Configuration Step	Notes
2	Verify that you can generate a RADIUS one-time password successfully.	
3	Verify that identity authentication is working correctly with your RADIUS system.	
4	Have access to someone who is knowledgeable about your RADIUS system and can answer questions or help troubleshoot issues, if needed.	
	Windows and Active Directory requirements for RADIUS configuration	
5	A Windows computer to use as a RADIUS client for initial testing, including: ■ Client name ■ Client IP address	
6	Make sure that client systems can reach the RADIUS server over the network (check your firewall settings). You may need help also from your network team if your RADIUS cluster has a load-balancer in the front end.	
7	You have administrative access to the designated Windows computer so that you can install software and do configurations.	
8	You have Active Directory account access so that you can modify group policies that apply to the target computer.	
9	You have access to the Group Policy Management Console.	
10	Your Active Directory expert must decide how the group policy layout and scope will be designed so that the group policies are applied to the clients based on their RADIUS service availability.	
	Centrify Authentication and Privilege Elevation Services Requirements for RADIUS configuration	

Step#	RADIUS Configuration Step	Notes
11	Access Manager console is installed on the client computer.	For details, see "Run the setup program on a Windows computer" in the *Administrator's Guide for Windows*.
12	The Centrify Agent for Windows is installed on the client system, you've configured the system to work with Centrify Privilege Elevation Service, including joining the computer to a zone.	For details, see "Install Centrify agents for Windows" in the *Administrator's Guide for Windows*.
13	You have administrative access to Access Manager so that you can manage roles and rights.	
14	The Centrify group policy templates from release 19.6 or later are installed. For RADIUS configuration, you need at least the Centrify Windows settings group policies.	For details, see "Install group policy extensions separately from Centrify Access Manager" in the *Administrator's Guide for Windows*.
15	If you want to capture the RADIUS events in your SIEM system, make sure the Audit trail is configured to go to the local log file.	In GPME, go to computer Configuration > Policies > Centrify Audit Trail Settings > Centrify Global Settings > Send audit trail to log file (this is not configured by default). For details, see "Send audit trail to log file" in the *Group Policy Guide*. For details, see "Send audit trail to log file" in the *Group Policy Guide*.
16	You have a role and user to test with. Make sure the role has rights for privilege elevation, such as New Desktop rights or Run as Role.	Make sure that you can elevate privileges successfully for that user and role before you try to configure RADIUS authentication.
	Configure a system to use RADIUS for privilege elevation (using group policies)	

Step#	RADIUS Configuration Step	Notes
17	Enable and configure the RADIUS group policies.	Configure the following group policies: Windows > MFA Settings > Specify the authentication source for privilege elevation : set this policy to RADIUS Authentication. Windows > MFA Settings > Remote Authentication Dial-In User Service (RADIUS) Settings > ■ Enable Remote Authentication Dial-In User Service (RADIUS): enable this policy. ■ Specify the RADIUS connection timeout: Configure to match your RADIUS timeout setting. ■ Specify the RADIUS server IP address: enter your RADIUS IP address. ■ Specify the RADIUS server port number: enter your RADIUS port number (the default is 1812). For details, see "Remote Authentication Dial-In User Service (RADIUS) Service Settings" in the *Group Policy Guide*. For details, see "Remote Authentication Dial-In User Service (RADIUS) Service Settings" in the *Group Policy Guide*. After you update the policies, do a group policy update on the Windows client computer.
18	Configure the role to require re-authentication using multi-factor authentication.	For example: 1. Right-click your test role and choose Properties. The Role Properties dialog box opens. 2. Click the Run As tab. 3. Select Re-authenticate current user and then select Require multi-factor authentication. 4. Click OK to apply the changes.

Step#	RADIUS Configuration Step	Notes
19	Run dzflush to make sure that the agent has the changes from Access Manager.	For details, see "Using dzflush" in the *Administrator's Guide for Windows*.
20	Set the RADIUS shared secret.	The RADIUS secret is unique to each system and will match the secret that the RADIUS server has. You can set the pre-shared secret by either of the following methods on the client computer: ■ Run the Set-CdmRadiusSecret cmdlet to set the RADIUS shared client secret. For details, see the DirectAuthorize PowerShell cmdlet help. ■ Use the Agent Configuration settings dialog box to configure the RADIUS server, including the pre-shared secret. For details, see "Configuring agent settings for the Identity Services Platform" in the *Administrator's Guide for Windows*.
	TEST AND VERIFY	
21	Verify that a user can elevate privileges by entering the RADIUS one-time password.	For example, if your role has New Desktop rights: 1. Right-click the System Tray and select New Desktop. 2. In the dialog box that appears, select your test role and click OK. 3. If the RADIUS authentication has been configured successfully, you are prompted to enter a password for RADIUS authentication. Enter the password and click Next to continue. 4. You can also view the audit trails for the successful authentication in the system's event log.
22	Verify that a user cannot elevate privileges after entering an incorrect RADIUS one-time password.	

Troubleshooting multi-factor authentication

Because multi-factor authentication for Centrify-managed computers relies on the infrastructure of the Privileged Access Service, troubleshooting the configuration of your environment and potential connectivity issues can be challenging. To help you test and verify the proper configuration of an integrated environment, Centrify provides several diagnostic tools.

The following Centrify diagnostic tools are available on Windows computers:

- **Diagnostics Tool.** The diagnostics tool is available through the Centrify Agent Configuration service, and is described in Viewing Windows diagnostics.
- **Centrify Privilege Elevation Service Diagnostic Information panel** (formerly the DirectAuthorize Agent Control Panel) The information panel is available from the Centrify Agent Configuration service, and is described in the Centrify *Administrator's Guide for Windows*.
- **The dzdiag command.** The command is available from the Windows command prompt, and is described in the Centrify *Administrator's Guide for Windows*.

The following Centrify diagnostic tool is available on UNIX and Linux computers:

- **The adcdiag program.** The program is available from the UNIX or Linux command line, and is described in Viewing UNIX and Linux diagnostics.

Viewing Windows diagnostics

The Centrify Agent for Windows provides logging and diagnostic services. If you have administrative access on a local computer, you can generate diagnostic information about the operation of the Centrify agent for Windows and view and save the current content of the log file from the agent configuration panel. For example, you can generate diagnostic information

about user sessions, user roles, desktops, and elevated account access, as well as detailed information about auditing from the agent configuration panel.

There are three different types of diagnostics information available:

- **Centrify Audit & Monitoring Service** provides the diagnostic information related to the auditing and monitoring service.
- **Centrify Identity Services Platform** provides the diagnostic information related to Privileged Access Service, such as for MFA. This diagnostics tool runs the following tests:
  - **Agent Service Connectivity Check:** Checks to see if the agent is in service, and if the agent is running in a normal state. Also determines whether the agent is in a zone, or is configured to use zoneless mode.
  - **Centrify Connector Connectivity Check:** Determines whether all connectors in the network can be connected properly.
  - **Centrify Identity Services Platform Certificate Validation Check:** Checks whether the certificates (IWA and cloud) have been installed properly. Also determines whether the agent can be connected without a trusted certificate problem.
  - **Centrify Identity Services Platform Connectivity Check:** Determines whether a connection to the cloud tenant is functional. Checks for problems with DNS, the firewall, and proxy server settings.
  - **MFA Configuration Check:** Determines whether the local computer has been configured properly. If the computer is in a zone, the test also checks whether MFA complies with the configuration defined in the zone.
  - **MFA Role and Permission Check:** Verifies whether role permissions are set properly in the Privileged Access Service Admin Portal.
  - **Offline MFA Provisioning Check:** Determines if the computer has been configured with an offline MFA profile or not.
  - **RADIUS Configuration Check:** If RADIUS authentication is enabled, this check determines if the RADIUS settings are configured correctly or not.
  - **RADIUS Connectivity Check:** If RADIUS authentication is enabled, this check determines if the agent can connect to the RADIUS server or not.

- **Centrify Privilege Elevation Service** provides the diagnostic information related to privilege management.

You can view these diagnostics tools either from the Windows system tray or from the agent configuration panel.

For more details, see the Administrator's Guide for Windows.

To view diagnostics from the Windows system tray:

1. Log on to a computer where the Centrify Agent for Windows is installed.
2. In the Windows system tray, right-click the Centrify icon and click **Troubleshooting**, then select the service for which you want to view diagnostic information (your options may vary depending on what services are enabled on the computer):
    - **Centrify Audit & Monitoring Service** opens a dialog box with a text-based summary of diagnostic auditing and monitoring information.
    - **Centrify Identity Services Platform** runs a series of connectivity tests and lists out the results of each test.
    - **Centrify Privilege Elevation Service** opens a dialog box with a text-based summary of diagnostic privilege elevation information.

To generate diagnostics or view the log file from the agent configuration panel:

1. Log on to a computer where the Centrify agent for Windows is installed.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Select the service for which you want to view information:
    - **Centrify Audit & Monitoring Service** opens a dialog box with a text-based summary of diagnostic auditing and monitoring information.
    - **Centrify Identity Services Platform** runs a series of connectivity tests and lists out the results of each test.
    - **Centrify Privilege Elevation Service** opens a dialog box with a text-based summary of diagnostic privilege elevation information.
4. Click **Settings**.
5. Click the **Troubleshooting** tab.
6. Click **Diagnostics** to generate diagnostic information.

7. Select the Diagnostic Information displayed, right-click, then select **Copy** to copy and paste the output to a file for further analysis.
8. Click **View Log** to display the current log file for the local agent.
9. Click **Options** to see or change the location of the log file or the level of detail recorded in the log file.

Viewing UNIX and Linux diagnostics

The `adcdiag` program performs a set of tests to check for access to a Centrify server authentication instance, the availability of one or more Centrify connectors, whether the computer is joined to an Active Directory domain, and whether the connector you are attempting to use is configured to use integrated Windows authentication.

To perform the set of tests to verify a UNIX or Linux computer can be configured to use multi-factor authentication, run the following command:

```
/usr/share/centrifydc/bin/adcdiag
```

By default, the command displays the test results in standard output (stdout) and generates a diagnostic report in the `/var/centrify/tmp` directory with a dated time stamp similar to the following:

```
adcdiagCheckingReport_20160307_151128.log
```

If any of the tests returned errors or warnings, you can check the diagnostic report for additional information, including suggestions for resolving any issues found. For details about the command-line options available for the `adcdiag` command, see the `man` page for the command.

Addressing certificate errors

Depending on how your Windows environment is set up, you may have to specify a trusted host certificate in order to enable multi-factor authentication. If you do not do this, you will see an error message during installation and configuration.

In a production environment, it is strongly recommended that you specify an existing trusted host certificate from a known third-party certificate authority, such as GoDaddy or Verisign. Using a self-signed certificate in a production environment can leave your environment vulnerable to security breaches.

For details about importing a trusted host certificate, see To import the certificate manually to a local Windows computer.

Managing Passwords

Centrify Privileged Access Service (PAS) cannot manage the password for a user if multi-factor authentication is required for the user to log in. You can still add a multi-factor authentication-required user account to a PAS resource – with “Manage this password” unchecked - to log in from PAS. However, you may see the status as “Failed” due to system delay. If the operation is successful, then no status will be shown for this user.

Customize the HTTP Proxy Configuration

Typically, a Unix/Linux system running the Centrify Agent is located on a private network. By default, the Centrify Agent uses the Centrify Cloud Connector as a HTTP proxy server for connecting to the Centrify Identity Platform (CIP) to, for example, perform multi-factor authentication.

However, you may prefer to reconfigure the Centrify agent to use a different proxy server. The following sections explain how to do that.

Requirements

The configuration described in these sections require the following conditions:

- The HTTP proxy server is used only for communication between the Centrify Agent and the Centrify Identity Platform (CIP). It does not provide proxy services for another purpose.
- All of the Agents must use the same proxy server.
- You have installed Centrify DirectControl (CDC) on the system.

Also note the following points:

- All of the agents use a single proxy server configuration (multiple configurations not supported)
- The machine password keytab must contain at least two versions of the key.
- This proxy server configuration supports all zone types.
- The information in the following sections does not apply to Mac OS X.

Configure the Agent to Use a Custom HTTP Server

To configure the Agent to use a custom HTTP server, use the following command syntax to set the custom HTTP proxy server:

```
adwebproxyconf --set,-S [--username,-u <username>]
[--password, -p <password>]  [--machine,-m]
[--server,-s <servername:port|"">]
[--authreq,-r <true|false|"">] [--authtype, -t <type>],
'--version,-v','--help,-h' and '--verbose,-V'
```

For example, enter the following command (replacing the angle brackets and placeholders with actual values):

```
adwebproxyconf --set --username <username>
--password <password> --server <servername:port>
--authreq <true> --authtype <type>
```

Change the value of `adclient.cloud.direct.connection` to `false`.

Verify that the new configuration works. Enter:

```
adwebproxyconf --test --cip <cip url>
--server <servername:port>
```

For more information, see Command Reference.

HTTP Proxy Credential Local Storage

This section describes how the HTTP proxy credentials are stored locally on the Unix/Linux system that's running the Centrify Agent.

The HTTP proxy credentials are be stored only in the local kset file: `/var/centrifydc/httpproxy.cred`

This `httpproxy.cred` file is only readable and write-able by root.

For security, remove `httpproxy.cred`. from the system when you remove the system from the domain.

For security, the proxy user's password is encrypted before being stored in `httpproxy.cred`.

Password Encryption

The proxy user's password is encrypted using the system's principal key, which is normally stored in `/etc/krb5.keytab`.

It should use the latest key to do encrypt the password. By default, it uses AES256-CTS-HMAC-SHA1-96 encryption.

If the key for a particular encryption type is not available, the Agent uses the next preferred and available encryption type that has a key in the system's keytab file.

When the system password changes, the agent uses it to re-encrypts the proxy server password. The system keytab file keeps the two latest versions of key.

If the Centrify Agent on the Unix/Linux system has FIPS Mode enabled, only a FIPS-compliant encryption type is allowed to encrypt the proxy credential password.

If a password is encrypted with non-FIPS-compliant encryption type, even if the machine keytab contains a valid key, the agent will not be able to decrypt it. If that happens, set the proxy password again so that it is encrypted using a FIPS-compliant encryption type.

Encrypted Password Storage

The encrypted password and relevant information is represented in ASN.1 as shown below and is encoded using ASN.1 Basic Encoding Rule (BER) as defined in Section 5.1 of the RFC 4511 LDAP Protocol (https://www.ietf.org/rfc/rfc4511.txt):

```
PROXY_USER_CRED ::= SEQUENCE {
username      STRING,
kvno          UInt32,
etype         Int32,
cipher        OCTET_STRING
}
Int32          ::= INTEGER (-2147483648..2147483647) -- signed
values re-presentable in 32 bits
UInt32         ::= INTEGER (0..4294967295)           -- unsigned 32
bit values
```

Where:

- `username`: The proxy user's name.
- `kvno`: The version number of the key under which the data is encrypted

- `etype`: The encryption type used to encrypt the cipher. The encryption type number MUST be a type that is supported by the Kerberos protocol.
- `cipher`: The encrypted password

Local Machine Account Support

In some cases, the current system account's Kerberos credentials should be configured, the username be S-1-5-18, and the cipher part must contain an octet string with 0 length.

Command Reference

adwebproxyconf

The `adwebproxyconf` command configures the HTTP proxy server settings and credentials on the local system. Typical use cases are:

- Set up the HTTP proxy credential to be used by agent.
- Delete the HTTP proxy credentials.
- Get information about the HTTP proxy credentials.
- Test the proxy connection using the configured credentials
- Test the proxy connection using the supplied credentials

Requirements

- Only root can run this command.
- To run, the system must have joined a zone.

Synopsis

```
adwebproxyconf --set,-S [--username,-u <username>]
[--password, -p <password>]  [--machine,-m]
[--server,-s <servername:port|"">]
[--authreq,-r <true|false|"">]
[--authtype,-t <basic|digest|ntlm|negotiate|anyauth|"">],
'--version,-v','--help,-h' and '--verbose,-V'
```

```
adwebproxyconf --delete,-D
adwebproxyconf --list,-L
adwebproxyconf --test,-T <--cip,-c <cip url> >
[--server, -s <servername:port>]
[--username,-u <username>]
[--password, -p <password>]  [--machine,-m]
```

Command options

`--set,-S`

Set the HTTP proxy server and credentials for the local system. After using `adwebproxyconf -S`, use `adreload` to force the Centrify agent process (adclient) to reload its configuration files.

the configuration properties in the /etc/

centrifydc.conf file and in other files in the /etc/

centrifydc directory.

`--delete,-D`

Delete the HTTP proxy credentials from the local computer and reset the HTTP Proxy configurations in `centrifydc.conf`:

- HTTP Proxy Server
- HTTP Proxy authentication type
- HTTP Proxy authentication required

`--list,-L`

List the HTTP proxy username and server from the configuration on the local system.

`--test,-T`

Test the HTTP proxy credential using configured or supplied settings.

`--username,-u <username>`

Proxy username. If a username is not supplied but `--password` is supplied, the username defaults to `Administrator`'

`--password, -p <password>`

Proxy user's password, if not provided, will be prompted

`--machine,-m`

- - - - - -

Use local machine account for proxy authentication, and SPNEGO authentication is used.

This option cannot be used with `-u`, `-p`, or `-t`.

`--authreq,-r <true|false|"">`

Specify if HTTP Proxy authentication is required in centrifydc.conf, Optional.

Can use individually or with other options.

`--authtype,-t <basic|digest|ntlm|negotiate|anyauth|"">`

Specify if HTTP Proxy authentication authentication type in centrifydc.conf. Optional.

Please refer to above section for valid values.

Can use individually or with other options.

`--server, -s <servername:port|"">`

Specify HTTP Proxy Server to use to update to centrifydc.conf. Optional.

Empty string unsets the value in centrifydc.conf.

Can use individually or with other options.

`--version,-v`

Specify the version.

`--help,-h`

Get command line help.

`--verbose,-v`

Get additional details while the settings are being applied.

`--cip,-c <cip url>`

Specify the URL of the Cloud Identity Platform.

Must be specified.

`--server, -s <servername:port>`

Specify HTTP Proxy Server to test.

If not specified, get it from centrifydc.conf

`--username,-u <username>`

Proxy username.

If not specified, get it from proxy cred file.

- - - - - -

`--password,-p <password>`

Proxy user's password.

If username is specified, but password is not, prompt for it.

If both username and password are not specified, get it from proxy cred file.

`--machine,-m`

Use local machine account for proxy authentication, and SPNEGO auth type is used.

This option cannot be used with `-u`, `-p`, or `-t`.

This test option always use the proxy credential to check the connection to CIP thru the specified HTTP Proxy server.

You can also use the `adcdiag` command to check HTTP proxy server settings.