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.

© 2004-2018 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.
Preparing to use multi-factor authentication

Securing login access ........................................... 4
Securing privileged access .................................... 5
Previewing the preliminary steps ............................. 6
Registering for Centrify Identity Service .................. 7
Installing and configuring a connector ..................... 9
Logging on and verifying connector settings ............... 15
Preparing a group for Centrify-managed computers .... 16
Preparing a role for Centrify-managed computers in the Admin Portal ........................................... 17
Adding a user or group for MFA to a role with an Admin Portal-specified policy ........................................ 18
Preparing authentication profiles ............................. 19
Configuring roles and rights to use multi-factor authentication ........................................................................... 26
Configuration options for Linux and UNIX computers . 29
Configuration options for Windows computers .......... 33
Troubleshooting multi-factor authentication ............... 39
Customize the HTTP Proxy Configuration ................. 43
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 Infrastructure Services.

Configuration information for Centrify customers who are not using infrastructure services to manage their environment, but want to configure multi-factor authentication to log in Windows computers, should visit the following web page: https://docs.centrify.com/en/centrify/adminref/index.html?version=1482218465#page/cloudhelp%2Fwindows-agent-download.html%23

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
Securing privileged access

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. If you are configuring multi-factor authentication for UNIX and Linux computers in classic zones or in Auto Zone, the predefined **require MFA for login** role and the **Require multi-factor authentication for login** system right are not available. For multi-factor authentication on computers that are not in hierarchical zones, you need to enable and apply group policies, set configuration parameters, or use the DirectAuthorize Agent Control Panel.

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 using a Personal Identification Number (PIN) is not authenticated by multi-factor authentication.

**Securing privileged access**

If you have installed infrastructure 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.
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.
authentication when executing commands using elevated privileges (\texttt{dzdo}) or in restricted shell (\texttt{dzsh}) environments on UNIX and Linux machines, or when creating roles with elevated Windows rights.

These same preliminary steps are required to support multi-factor authentication in classic zones and in Auto Zone. However, the implementation is slightly different than in hierarchical zones, so the steps to complete the configuration on UNIX and Linux computers depend on the type of zone configuration for the computers on which you want to configure multi-factor authentication.

Registering for Centrify Identity Service

Multi-factor authentication for Centrify-managed computers relies on the infrastructure provided by the Centrify Identity platform and the Centrify identity services. The Centrify Identity service enables you to securely manage users, roles, policies, devices, and applications in the identity platform. Through the Centrify Identity service, you can 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 the Centrify Identity service if you are not already a subscriber. You can request a free trial or subscribe to the Centrify Identity service through the Centrify website.

If you don’t already have a subscription, you can start by requesting access to Centrify Identity services 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 \texttt{System Administrator} role and a unique customer
Registering for Centrify Identity Service

• Preparing to use multi-factor authentication

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 Centrify Identity 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 Centrify Identity platform with the account information in the email.

<table>
<thead>
<tr>
<th>Centrify Identity Service management:</th>
<th><a href="https://aal0287.centrify.com/manage">https://aal0287.centrify.com/manage</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Your User Name:</td>
<td><a href="mailto:admin_maya.garcia@centrifypubs.net">admin_maya.garcia@centrifypubs.net</a></td>
</tr>
<tr>
<td>Your Temporary Password:</td>
<td>hKGo!wd2N</td>
</tr>
<tr>
<td>(You’ll be asked to change this when you log in)</td>
<td></td>
</tr>
<tr>
<td>Customer ID:</td>
<td>AAEK0012</td>
</tr>
<tr>
<td>Identity Service Edition:</td>
<td>App+</td>
</tr>
</tbody>
</table>
Planning multi-factor authentication for Centrify-managed computers

The Centrify Identity 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 identity 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 the Centrify Identity service. It is separate from the role definitions and role assignments you manage using Access Manager or other infrastructure services components.

Installing and configuring a connector

The connector is a multipurpose service that enables secure communication between your internal network and the Centrify Identity 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 Centrify Identity 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 Centrify Identity platform services 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 identity platform 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 the Centrify Identity platform, 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 Identity platform instance URL, you can change the Identity platform authentication 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 IWS 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.
Select **Place all certificates in the following store** and click **Browse**.

Select **Trusted Root Certification Authorities** and click **OK**.

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.

7. Click **Yes** when prompted by the Security Warning.

8. Click **Save** in Connector Configuration to save your settings.

9. Restart the connector.

Connectors that are not configured to use HTTPS will not be available for IWA.

**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:

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

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 Portal click **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” on page 16, 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.
Adding a user or group for MFA to a role with an Admin Portal-specified policy

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 the Centrify Identity 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** and then click **Add**.

3 Enter a search string to locate the Active Directory group you are using for users or groups that require multifactor.
Preparing authentication profiles

With Centrify Infrastructure Services, 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 infrastructure 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.

**To create an authentication profile**

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

1. Open a browser and log on to the Centrify identity service using your customer-specific URL.
2. Switch to the administrative portal, then click **Settings** and click **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.
Preparing authentication profiles

- 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.

- Type the authentication profile name.
- Select the types of authentication to present for the first challenge.

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

- Click **OK**.

The pass-through option does not apply to Windows, Linux, or Unix MFA logins.

You should note that only the authentication challenges that are applicable for a user can be presented. For example, you might select Phone call and Email confirmation code in the authentication profile, but these challenges are only valid if users have both a phone number and email address stored for their accounts. If users only have a phone number and not an email address stored, they will receive a phone call to complete the authentication process rather than be prompted to select an authentication option. If users have both a phone number and an email address stored, they will be prompted to select which form of authentication to use.

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...
Preparing authentication profiles

between an email confirmation code, security question, or text message confirmation code.

If you have multiple challenges, Centrify Identity Services 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 Centrify Identity Services 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. Do this by performing the following steps.


2. Select Yes in the Enable authentication policy controls drop-down. Click Add Rule.

   The Authentication Rule window displays.

3. Click Add Rule on the Authentication Rule window.

4. Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access Centrify Identity Services from an IP address that is outside of your corporate IP range. Supported filters are:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The authentication factor is the computer’s IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.</td>
</tr>
<tr>
<td>Identity Cookie</td>
<td>The authentication factor is the cookie that is embedded in the current browser by the directory service after the user has successfully logged in.</td>
</tr>
<tr>
<td>Day of Week</td>
<td>The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.</td>
</tr>
</tbody>
</table>
### Filter Description

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.</td>
</tr>
<tr>
<td>Date Range</td>
<td>The authentication factor is a specific date range.</td>
</tr>
<tr>
<td>Time Range</td>
<td>The authentication factor is a specific time range in hours and minutes.</td>
</tr>
<tr>
<td>Device OS</td>
<td>The authentication factor is the device operating system.</td>
</tr>
<tr>
<td>Browser</td>
<td>The authentication factor is the browser used for opening the Centrify Identity Services user portal.</td>
</tr>
<tr>
<td>Country</td>
<td>The authentication factor is the country based on the IP address of the user computer.</td>
</tr>
</tbody>
</table>
Preparing authentication profiles

Risk Level: The authentication factor is the risk level of the user logging on to user portal. For example, a user attempting to log in to Centrify Identity Services 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.

Managed Devices: The authentication factor is the designation of the device as “managed” or not. A mobile device is considered “managed” if it is managed by Centrify Identity Services (MDM enrolled), or if it has a Centrify-trusted certificate authority (CA has been uploaded to your tenant using Admin Portal > Settings > Authentication > Certificate Authorities).

For the Day/Date/Time related conditions, you can choose between the user’s local time and Universal Time Coordinated (UTC) time.
Preparing authentication profiles

5 Click the **Add** button associated with the filter and condition.

6 Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.

7 The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option.

8 Click **OK**.

9 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.

10 Click **Save**.

11 If you have more than one authentication rule, you can prioritize them on the **Login Authentication** page.

### 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 (\texttt{dzdo}) or in a restricted shell (\texttt{dzsh}).

2. Click \textit{Save}.

## Configuring roles and rights to use multi-factor authentication

You can prepare for multi-factor authentication before or after installing infrastructure services components. 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, \texttt{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:

- \textit{Planning and Deployment Guide}
- \textit{Administrator's Guide for Linux and UNIX}
- \textit{Administrator's Guide for Windows}

For example, see the \textit{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.

You can also configure multi-factor authentication for classic zones and for Auto Zone. However, the steps for configuring multi-factor authentication for computers in those “legacy” zones are different. For information about configuring multi-factor authentication for computers in a classic zone or the Auto Zone, see “Configuring multi-factor authentication in legacy zones” on page 32.
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 for login** 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 for login** 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.

Requiring multi-factor authentication using computer roles

Computer roles 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_servers, 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_servers 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 creates 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.

**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”
Preparing to use multi-factor authentication

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.

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 passcode 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 passcode in following way:

**To set up an offline passcode**

1. Right click the Centrify notification icon in the system notification area, and select “Setup Offline Passcode”

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.

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 passcode, they will be prompted to enter the mobile passcode generated by their authentication application 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 passcode 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_consoles, 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 creates 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.

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 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 Mobile Device Management (MDM)**

After installing the *Centrify Agent for Windows* on a Windows 10, you can achieve Zero Sign-On (ZSO) by enrolling that system in Mobile Device Management (MDM).

You only need to install the Centrify Agent. You do not need to install all of the Centrify Management Services (Identity & Privilege Audit & Monitor).

When the device is enrolled, you see it on your Devices page in the Centrify user portal, along with their other personal devices.

One benefit of using MDM is that an IT administrator can track the location of your device. If the device is lost or stolen, the IT administrator can protect personal data by wiping the device.

Another key benefit is Zero Sign-On (ZSO), which makes connecting to the organization's network from outside a frictionless experience. From the device user's perspective, there is no difference between connecting from inside or outside the network. After the user signs on to the device using multi-factor authentication (MFA), they do not need to re-enter their username and password to connect to the company network. From the administrator's perspective, the mechanisms that manage the connections is different: MDM handles connections from outside, and Integrated Windows Authentication (IWA) handles connections from inside.

**Note** If a cross forest user wants to enroll their device, they must have at least one connector in the cross forest pointing the tenant in the machine specified.

In this release:

- ZSO supports Chrome, IE, and Edge browsers, but not Firefox (which we expect in the next release).
- MDM only supports Windows 10.

For administrators:
• When you add the Centrify Identity Services Platform, it enrolls the device as a corporate-owned device.
• If the service added in a previous version is upgraded, it silently enrolls the devices as corporate-owned device.
• To check whether the device is owned by the organization, the administrator uses “connect to work or school” in Windows Settings.
• To see the status of a device, use the Endpoint sections of the Admin portal.

For device users:
• To enroll a personal device, use the “enroll your device” feature.

**Note** When a machine is not connected to the Centrify Connector (for example, not in the domain network), an MFA prompt is triggered to allow the user to log in to the Centrify Cloud. Enrollment continues after a successful login.
• If you un-enroll your device, it becomes an organization-owned device.
• When your device is enrolled, Zero Sign-On (ZSO) is enabled and visible in the system tray. You can log into the Centrify user portal without entering their username/password.

**Note** Once you have enrolled your device, a desktop shortcut is added to provide you access to the Centrify User Portal.

**To configure MDM**

1. On the Windows system, install or upgrade to the latest version of Centrify Agent for Windows.
2. Enable **Centrify Identity Services Platform**.
3. Log in to the Identity platform instance, switch to the Admin Portal, and click **Core Services > Policies**.
4. Click the policy that applies to the Windows system that is running the Centrify Agent. (You can see which policies are relevant by looking under **Core Services > Policies: Login Policies >Windows Workstations**.)
5. Within Policies, expand **Endpoint Policies** and click **Device Enrollment Settings**. Set **Permit Device Enrollment** to **Yes**.

6. Set **Device Management Settings** to enable MDM.

7. In the Centrify Agent Configuration that opens enable the agent to connect to Centrify services that are installed on the main administrative computer. (If the agent configuration panel is not open, open the Windows **Start** menu and click **Agent Configuration**.)

8. In the agent configuration control panel, click **Add service**. This action displays all of the Centrify services that are available.

After performing these steps, the device will be able to log into the network and be managed using MDM: When the user tries to log in, Windows should present the user with the option to “Enroll your Device”. From this point forward, the device uses ZSO to connect to any ZSO-authenticated service or hardware on the network.

You can use MDM Enrollment Check to troubleshoot problems related to Mobile Device Management (MDM), as described in the following section.

**Troubleshooting multi-factor authentication**

Because multi-factor authentication for Centrify-managed computers relies on the infrastructure of the Centrify Identity platform and the Centrify Identity services, 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” on page 40.

- **Centrify Privilege Elevation Service Diagnostic Information panel (formerly the DirectAuthorize Agent Control Panel)**. The information panel is available from the Centrify Agent.
Troubleshooting multi-factor authentication

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” on page 41.

**Viewing Windows diagnostics**

The Diagnostics Tool can help you troubleshoot specific areas of multi-factor authentication.

The tests performed by the Diagnostics Tool include the following:

- **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.

- **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.

- **Centrify Identity Service 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 Service Connectivity Check.** Determines whether a connection to the cloud tenant is functional. Checks for problems with DNS, the firewall, and proxy server settings.

- **MFA Role and Permission Check.** Verifies whether role permissions are set properly in Identity Service (the Admin Portal).
- **MDM Enrollment Check.** Checks for problems related to Mobile Device Management (MDM) enrollment such as network communication problems with the identity service and operating system support for MDM.

To use the MFA Diagnostic Tool:

1. From the list of applications in the Windows Start menu, select **Agent Configuration > Centrify Identity Services Platform > Settings.**
2. Select the **Troubleshooting** tab.
3. Click **Diagnostics.**
   
The Diagnostics Tool performs several tests, and displays the results:
   
   - **Success.** The test passed.
   - **Failure.** The test did not pass due to a problem.
   - **Warning.** The test passed, but detected a problem.

4. Click the arrow to the left of each test to show more details about the test results.
5. Click the **Re-test** button to perform the diagnostic test again.
6. Click **Export** to transfer the test information to a text 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” on page 12.

**Managing Passwords**

Centrify Privilege Service (CPS) 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 CPS resource – with “Manage this password” unchecked - to log in from CPS. 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.
Disable self-service password reset

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

If this policy is set to Enabled, self-service password rest on the machine will be disabled even the cloud enabled self-service password reset.

If this policy is set to Disabled or Not Configured, self-service password reset on the machine will follow the cloud policy. (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.

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.

- **Disabled** or **Not Configured**: 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.

Customize the HTTP Proxy Configuration

Introduction

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
}
```

Where:

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

- **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 --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 local machine.

**--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.

**Command Options for --set, -S**

**--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.

**Command Options for --test**

--cip,-c <cip url>

Specify the URL of the Cloud Identity Platform.

Must be specified.
Customize the HTTP Proxy Configuration

--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.

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.

Previously, Centrify Identity Service (CIS) added this capability for Centrify Cloud users and Active Directory (AD). Now, Centrify has
added password reset to the multi-factor Authentication (MFA) for Windows, which provides strong authentication and uses the Identity Platform (CIP).

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

To reset their password, they perform the following steps:

1. On the login screen, the user clicks the "Forgot Password" link.

2. 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.)

3. The user completes the MFA challenges, which are based on the password reset profile.

4. A new prompt asks the user to enter a new password and confirm it.

5. After resetting the password, the user logs in using the normal login screen.