Centrify Server Suite 2017

Multi-factor Authentication Quick Start Guide

February 2017

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 User Suite, and Centrify Server Suite are registered trademarks and Centrify for Mobile, Centrify for SaaS, Centrify for Mac, DirectManage, Centrify Express, DirectManage Express, Centrify Identity Platform, Centrify Identity Service, and Centrify Privilege Service are 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 B2; 9,112,846; 9,197,670; 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

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 Server Suite.

Configuration information for Centrify Identity Service customers that are not using Centrify Server Suite to manage their environment, but want to configure multi-factor authentication for login on Windows machines, 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 Linux roles, you can also create custom role definitions with the **Require multi-factor authentication** 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** 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 on support multi-factor authentication. However, some desktop manager programs that run on older operating systems might not support multi-factor authentication.

Securing privileged access

If you have installed Centrify Server Suite, 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 on. 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.
- 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** 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.

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 filling out the appropriate form to request access to the Centrify identity service. Select from these editions based on the features in which you are interested:

- http://www.centrify.com/express/identity-service-form/
- http://www.centrify.com/free-trial/identity-service-form/
- http://www.centrify.com/free-trial/identity-service-form-appplus/

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:

Centrify Identity Service management:	https://aacl0287.centrify.com/manage
Your User Name:	admin_maya.garcia@centrifypubs.net
Your Temporary Password:	hKGo!wd2N (You'll be asked to change this when you log in)
Customer ID:	AAEK0012
Identity Service Edition:	App+

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

Start or skip the wizard

After you log on 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 on to the Centrify identity platform with the account information in the email.

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 DirectManage Access 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 on to the appropriate customer-specific Identity platform instance using the account information you received in your email notification.
2. Click Settings, then click **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.

The certificate configuration process is also strongly encouraged for Windows computers, but you will have the option to skip certificate validation during installation of the Centrify Agent for Windows when joining to a zone. This is because the IWA service is generally not needed for multi-factor authentication when a Windows computer is directly connected to the Centrify identity platform. However, if a computer is not directly connected to the identity platform, or errors

happen with a direct connection, the IWA service will be needed for multi-factor authentication. In this case, if you have not configured your computer to accept either the Centrify root certificate or a third party certificate, authentication will fail.

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

1. In the Admin Portal, click **Settings** and choose **Network** from the menu on the left.
2. Select the connector you want to configure.
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.
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** and choose **Network** from the menu on the left.

2 Select the connector you want to configure.

3 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.

Verify open ports

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

- Port 80 for inbound HTTP connections
- 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 on to the Centrify identity platform.

To log on and verify settings

1. Open a browser and log on 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** to display the connector Configuration.
5. Verify the following options are selected:
   - Enable Web Server

     This option is required to enable integrated Windows authentication for Centrify agents and other features.

   Note that this option is required for Centrify Server Suite multi-factor authentication.

6 Click **OK**.

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. Log on to the Identity platform instance, 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. Select 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.

   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 **Server 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**.

Preparing authentication profiles

With Centrify Server Suite, you can require multi-factor authentication for two distinct situations:

- As part of the **login** process so that users who are attempting to log on 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 Server Suite authentication or add new profiles specifically for the computers you manage through Server Suite. 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 prepare authentication profiles specifically for Server Suite authentication

1 Log on to the Identity platform instance and, if necessary, switch to the Admin Portal, then click **Settings**.

2 Under **Authentication**, click **Servers and Workstations**.

3 Select an existing Login or Privilege Elevation profile from the appropriate drop-down menu or click **Add New Profile**.

If you want to specify the authentication challenges that are presented and from which a user can select when logging on, select **Add New Profile**.

- Type the authentication profile name.
- Select the types of authentication to present for the first challenge.
- Select the types of authentication to present for the second challenge.
- Click **OK**.

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.

4 For Elevated Privileges Profile, 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 Server 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`).

5 Click **Save**.

Configuring roles and rights to use multi-factor authentication

You can prepare for multi-factor authentication before or after installing Centrify Server Suite 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, `adedit`, or Access Module for PowerShell scripts to complete most of the next steps. For more details about performing these tasks, see the core documentation for Centrify Server Suite, in particular the *Planning and Deployment Guide* and the *Administrator's Guide for Linux and UNIX* for UNIX machines, and the *Administrator's Guide for Windows* for Windows machines. For example, see the *Administrator's Guide for Linux and UNIX* for more information about creating zones, configuring role definitions, and adding command rights.

To configure multi-factor authentication

1. Install DirectManage Access 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 classic zone or Auto Zone, see "Configuring multi-factor authentication in legacy zones" on page 26.
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 on 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 on 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 on until the connection to the identity platform is restored.

Configuring secure shell (ssh) for multi-factor authentication

If you use the Centrify OpenSSH package from Centrify Server Suite 2017, or later, no configuration is required to support multi-factor authentication. However, 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 from Centrify Server Suite 2016.1, or later, 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 on 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 on Windows computers in the Group Policy Management Editor under Computer Configuration > Policies > Centrify Settings > Windows Settings > MFA Settings.

Configuring offline multi-factor authentication and rescue users

Because local accounts on Windows computers are not subject to multi-factor authentication, you can use these accounts to rescue a system that is not connected to the Centrify identity platform.

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 on 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 on 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 on to their machine if it cannot connect to the Centrify Identity platform instance.

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 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**.

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 the `adcdiag` command-line program for UNIX and Linux computers and the `dzdiag` command or Authorization Center control panel for Windows machines.

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.

For Windows machines, you can open Authorization Center by right-clicking the Centrify system notification icon and selecting **Open Authorization Center**. In the Authorization Center, you can view Login Rights, Role Assignments, the connection status of the agent, and other diagnostic information. Alternatively, you can run the `dzdiag` command from a command prompt for access to similar diagnostic information.

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.

For example, if you are using Centrify Privilege Service on-site or in a private cloud, you will be asked to specify a trusted host certificate needed for communication with the authentication service. You will have the option to specify an existing trusted host certificate or create a new, self-signed certificate. In a production environment, it is strongly recommended that you specify an existing trusted host certificate. The option to create a self-signed certificate is provided for demonstration purposes, and is not intended for production environments. Using a self-signed certificate in a production environment can leave your environment vulnerable to security breaches.

To ensure that the endpoints trust the Centrify Privilege Service host certificate, the certificate that you specify during installation should be from a known third-party certificate authority, such as GoDaddy or Verisign.

To trust the Centrify Privilege Service host certificate, locate the certificate in C:\Program Files\Centrify\Centrify Identity Platform\config and import the certificate using the steps described in “To import the certificate manually to a local Windows computer” on page 12.