RSA SecurID Token Configuration for UNIX/Linux Computers

September 2020 (release 2020)

Centrify Corporation

Legal Notice

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

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

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

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

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

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

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

Contents

• • • • • •
About this guide

This document describes the steps necessary to install and configure Centrify Authentication Service and RSA SecurID to enable two factor authentication for UNIX/Linux environments.

You can configure two factor authentication with the RSA SecurID token for local users, specific Active Directory users, or Active Directory groups that have UNIX profiles in the appropriate zone.

Documentation conventions

The following conventions are used in Centrify documentation:

- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, this font indicates variables. Square brackets (`[ ]`) indicate optional command-line arguments.

- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.

- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.

- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this guide. For complete file names for the software packages you want to install, see the distribution media.

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

Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify

• • • • • •

and Centrify products and features, start by visiting the Centrify website. From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

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

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

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

Product names

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

Current Overall Product Name	Current Services Available
Centrify Identity-Centric PAM	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service

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

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	Centrify Privileged Service (CPS)		Privileged Access Service
DirectControl (DC)			Authentication Service

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
DirectAuthorize (DZ or DZwin)			Privilege Elevation Service
DirectAudit (DA)			Audit and Monitoring Service
DirectManage (DM)	Infrastructure Services		Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service
	Management Services	Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated
	User Analytics Service		Privilege Threat Analytics Service
Deployment Manager		Deployment Manager provided a centralized console for discovering, analyzing, and managing remote computers. This feature is no longer included starting with Infrastructure Services release 19.6.	

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

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

• • • • • •

Contacting Centrify

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

Getting additional support

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

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

• • • • • •

Configuring Centrify Authentication Service and RSA SecurID

Once you have installed and finished setting up your Centrify product and the RSA SecurID authentication agent, you can configure settings so that user authentication can occur for locally defined UNIX users or for Active Directory users who have UNIX profiles in the appropriate zone. In addition, specific groups of Active Directory users can be prompted for password authentication or two factor authentication.

The installation process for each agent does not interfere with or touch any configuration file used by the other product. Follow the standard installation steps for each product.

You can install the products in either order. After the Centrify DirectControl agent is installed, you need to join the computer to a domain and place it in a DirectControl Zone.

You can configure Centrify Authentication Service and RSA SecurID to work together in either of two ways:

- Configure the PAM modules to work with Centrify Authentication Service and RSA SecurID

- Configure SecurID for use with Centrify zone-based role and privilege execution

If you're using an older version of authentication service or using a version that does not include multi-factor authentication (MFA) support, you can configure the PAM modules to work with authentication service and RSA SecurID. If you've configured role definitions or command rights to require MFA, you can rename a file and create a symlink to configure RSA SecurID to work with your authentication service deployment.

• • • • • •

Prerequisites

You need to have authentication service installed, with an agent on your UNIX/Linux computer.

You need to also have the RSA SecurID authentication agent installed and configured. This guide shows you how to configure the authentication service to prompt for a SecurID token.

RSA installation prerequisites

This guide assumes that you've already installed the RSA SecurID authentication agent. You can get more information about the RSA authentication agent at the following link:

https://www.rsa.com/en-us/products-services/identity-access-management/securid/authentication-agents/authentication-agents-for-pam

Installing the RSA Authentication agent includes but is not limited to the following tasks (consult the RSA documentation for a complete list):

- RSA Secure Console is set up for use

- In the RSA Secure Console, you've added your users, computers, and generated the `sdconf.rec` file.

- You've successfully installed the RSA authentication agent on your Linux and UNIX computers (this includes installing the sdconf.rec file).

- You've successfully tested the user authentication with the RSA `acetest` command.

If you have installed the RSA Authentication agent for PAM and successfully performed a test authentication for each user, then you're ready to configure DirectControl to work with the RSA agent and SecurID token.

Installing and configuring authentication service and RSA SecurID

The installation process for each agent does not interfere with or touch any configuration file used by the other product. Follow the standard installation steps for each product.

• • • • • •

You can install the products in either order. After you install the Centrify agent, you need to join the computer to Active Directory and place it in a DirectControl Zone.

Installation overview

To install and configure authentication service and RSA SecurID (an overview):

1. Install the DirectControl agent for *NIX.

   For details, see the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service documentation.

2. Install and set up the RSA SecurID agent.

   For details, see the RSA document, "*RSA Authentication Agent 7.1 for PAM--Installation and Configuration Guide for RHEL.*" The document is included in the agent download package.

3. Run the RSA `acetest` command to verify that the user login credentials work.

   For details, see the RSA documentation.

4. If you have configured role definitions or command rights to require multi-factor authentication (MFA), you create a symlink to point to the RSA SecurID authentication file instead of the file for DirectControl. For details, see Configuring SecurID for use with Centrify zone-based role and privilege execution.

   With MFA enabled for role definitions or command right definitions, you don't have to manually configure each authentication module to use RSA SecurID.

5. If you use Centrify Authentication Service but you don't use role definitions or command right definitions configured for MFA:

   a. Modify the PAM authentication files for Linux, Solaris, or AIX:

      a. For Linux: Configure the /etc/pam.d/system-auth file:

         For details, see Configuring the /etc/pam.d/system-auth file for Linux.

      b. For Solaris and AIX: Configure the pam.conf file:

● ● ● ● ● ● ●

For details, see Configuring the pam.conf file for Solaris and AIX.

b. (Optional) Configure the system to use the SecurID for authentication for specific users or groups.

> **Tip:** It may be a good idea to disable SecurID authentication for the root user, at least initially, so that you don't get locked out of the computer entirely.

c. (Optional, as needed) Configure SSH or other authentication services to use SecurID. For details on configuring SSH, see Configuring the pam.conf file for Solaris and AIX.

Configuring the PAM modules for use with DirectControl and SecurID

This section includes the following topics:

- Configuring the /etc/pam.d/system-auth file for Linux
- Configuring the pam.conf file for Solaris and AIX
- Requiring token authentication for specific groups or local users
- Configuring SSH to require SecurID

Configuring the /etc/pam.d/system-auth file for Linux

After you've installed both the RSA SecurID and Centrify agents on a Linux computer, you'll also need to insert a line in the `/etc/pam.d/system.auth` file. This change will make it so that the system prompts users for their SecurID token.

Just so that you know, this file will already have some lines at the top that were inserted by the authentication service.

• • • • • •

To configure the Linux system authentication file so that users are prompted for the RSA token:

- Add the following line to the beginning of the `/etc/pam.d/system.auth` file:

  ```
  auth  required  pam_securid.so
  ```

  You should restart any services that you plan to use with RSA. For example, if you're using SSH, you should restart the SSH service.

Configuring the pam.conf file for Solaris and AIX

For Solaris and AIX computers, you need to edit the `/etc/pam.conf` file.

To configure the Solaris or AIX system authentication file so that users are prompted for the RSA token:

In the `/etc/pam.conf` file, add the following code snippet to the end of the file:

```
# Support for Kerberos V5 authentication and example
configurations can
# be found in the pam_krb5(5) man page under the "EXAMPLES"
section.
sshd-kbdint auth     required     pam_securid.so
sshd-kbdint auth     sufficient   pam_centrifydc.so     unix_cred
sshd-kbdint auth     requisite    pam_centrifydc.so     deny
sshd-kbdint account  sufficient   pam_centrifydc.so     unix_cred
sshd-kbdint account  requisite    pam_centrifydc.so     deny
sshd-kbdint session  required     pam_centrifydc.so
sshd-kbdint password sufficient   pam_centrifydc.so     ry_first_
pass
sshd-kbdint auth     requisite    pam_authtok_get.so.1
sshd-kbdint auth     required     pam_dhkeys.so.1
sshd-kbdint auth     required     pam_unix_cred.so.1
sshd-kbdint auth     required     pam_unix_auth.so.1
sshd-kbdint account  requisite    pam_roles.so.1
sshd-kbdint account  required     pam_unix_account.so.1
sshd-kbdint session  required     pam_unix_session.so.1
sshd-kbdint password required     pam_dhkeys.so.1
sshd-kbdint password requisite    pam_authtok_get.so.1
sshd-kbdint password requisite    pam_authtok_check.so.1
sshd-kbdint password required     pam_authtok_store.so.1
```

You should restart any services that you plan to use with RSA. For example, if you're using SSH, you should restart the SSH service.

• • • • • •

Requiring token authentication for specific groups or local users

RSA supports the ability to require RSA token authentication for specific groups of users. This feature is supported when using Centrify Authentication Service. You can specify Active Directory groups as the required group. Local groups work as well.

You can also configure the agent so that specific groups are not prompted to authenticate with the RSA SecurID token. Group members excluded from SecurID authentication can authenticate using UNIX credentials or by way of another PAM module; you can configure this

> **Note:** The ability to require RSA SecurID token authentication for specific groups does **not** work with AIX. There is a bug in the AIX OS that prevents the SecurID agent from iterating Active Directory groups.

> **Note:** Be sure to exclude any users that you do not want to authenticate with the RSA SecurID token. Once you've enabled users or groups for token authentication, then all users will be challenged for a token even if they weren't assigned on. This situation can cause some users to be locked out of the computer that they're trying to log in to. When you are testing this functionality, it's a good practice to exclude the root user to avoid any complications.

To require SecurID token authentication for specific groups or users:

1. Edit the `sd_pam.conf` file and add the following lines:

   ```
   #VAR_ACE :: the location where the sdconf.rec, sdstatus.12
   and securid files will go
   VAR_ACE=/opt/RSA
   ```

2. To specify specific groups to authenticate using the RSA token, first enable group support by setting the `ENABLE_GROUP_SUPPORT` parameter to 1, as shown below:

   ```
   #ENABLE_GROUP_SUPPORT :: 1 to enable; 0 to disable group
   support
   ENABLE_GROUP_SUPPORT=1
   ```

3. To specify the list of groups that will use the RSA token, include them in

the `LIST_OF_GROUPS` parameter, as shown below:

```
#LIST_OF_GROUPS :: a list of groups to include or
exclude...Example
#LIST_OF_GROUPS=other:wheel:eng:othergroupnames
LIST_OF_GROUPS=sampleadgroup
```

4. To exclude groups from requiring the RSA token, include them in the `INCL_EXCL_GROUPS` parameter, as shown below:

```
#INCL_EXCL_GROUPS :: 1 to always prompt the listed groups for
securid
# authentication (include)
# :: 0 to never prompt the listed groups for securid
# authentication (exclude) INCL_EXCL_GROUPS=1
```

5. (Optional) To configure what happens when an excluded user tries to authenticate, modify the `PAM_IGNORE_SUPPORT` parameter, as shown below:

```
#PAM_IGNORE_SUPPORT :: 1 to return PAM_IGNORE if a user is
not SecurID
# authenticated due to their group membership
# :: 0 to UNIX authenticate a user that is not SecurID
# authenticated due to their group membership
PAM_IGNORE_SUPPORT=1
```

6. To specify specific users to authenticate using the RSA token, first enable user support by setting the `ENABLE_USERS_SUPPORT` parameter to 1, as shown below:

```
#ENABLE_USERS_SUPPORT :: 1 to enable; 0 to disable users
support
ENABLE_USERS_SUPPORT=1
```

7. To specify the list of users that will use the RSA token, include them in the `LIST_OF_USERS` parameter, as shown below:

```
#LIST_OF_USERS :: a list of users to include or
exclude...Example
LIST_OF_USERS=localuser1:aduser2
```

8. To exclude users from requiring the RSA token, include them in the `INCL_EXCL_USERS` parameter, as shown below:

```
#INCL_EXCL_USERS :: 1 to always prompt the listed users for
securid
# authentication (include)
# :: 0 to never prompt the listed users for securid
# authentication (exclude) INCL_EXCL_USERS=1
```

9. (Optional) To configure what happens when an excluded user tries to authenticate, modify the `PAM_IGNORE_SUPPORT_FOR_USERS` parameter.

You can also consult the RSA SecurID documentation for more details about configuring token authentication for groups, users, excluding users, and so

• • • • • •

forth. There are more configurations available than are presented in this document.

Configuring SSH to require SecurID

When setting up the SecurID product you must make some configuration changes to the sshd configuration files.

If you are using the Centrify openSSH product you must make some configuration changes to support token authentication. The Centrify openSSH is configured to attempt Kerberos single sign-on whenever a user logs in. This means that the user is not prompted for their user name or password. This capability must be disabled if you want to prompt users for token authentication.

To configure SSH to require a SecurID token:

1. Edit the `/etc/centrifydc/ssh/ssh_config` file and comment out the lines for the following items:

   - GSSAPIAuthentication

   - GSSAPIKeyExchange

   - GSSAPIDelegateCredentials

   For example:

   ```
   # Configuration for Centrify DirectControl: Host *
   #GSSAPIAuthentication yes
   #GSSAPIKeyExchange yes
   #GSSAPIDelegateCredentials yes
   ```

2. Edit the `/etc/centrifydc/ssh/sshd_config` file and comment out the lines for the following items:

   - `GSSAPIKeyExchange`

   - `GSSAPIAuthentication`

   - `GSSAPICleanupCredentials`

3. In the `/etc/centrifydc/ssh/sshd_config` file, be sure that the `PrintMotd` and `UsePam` settings are set as followings:

   ```
   PrintMotd no
   UsePAM yes
   ```

4. Restart `sshd` to ensure the changes take effect.

• • • • • •

Configuring SecurID for use with Centrify zone-based role and privilege execution

For the users that you want to use the SecurID pass code for login, you modify the affected role definitions to require multi-factor authentication. For the commands where you want users to provide a SecurID pass code, you configure the command right for re-authentication using multi-factor authentication.

To configure RSA SecurID for use with Centrify zone-based role definitions and command rights:

1. In Access Manager, configure your role definitions to use multi-factor authentication:

   a. In Access Manager, locate the role definitions for which you want to require use of the SecurID pass code.

      For example, navigate to your zone, then go to **Authorization** > **Role Definitions**, and then select the rights definition in the right pane.

   b. For each role definition, right-click the role definition and select **Properties**.

   c. Click the **Authentication** tab.

   d. Select **Require multi-factor authentication for login**.

   e. Click **OK** to save the changes.

2. In Access Manager, configure your command rights to use multi-factor authentication:

   a. In Access Manager, locate the command rights definitions for which you want to require use of the SecurID pass code.

      For example, navigate to your zone, then go to **Authorization** > **UNIX Right Definitions** > **Commands**, and then select the rights definition in the right pane.

   b. For each command right, right-click the command right and select **Properties**.

   c. Click the **Attributes** tab.

   d. Select **Re-authenticate current user**.

● ● ● ● ● ●

     e. Select **Require multi-factor authentication**.

     f. Click **OK** to save the changes.

3. Make sure that you've installed the DirectControl agent for *NIX on the UNIX or Linux computer where you want users to use the RSA SecurID pass code.

4. On the Linux or UNIX computer where you want users to use the SecurID pass code, locate the `pam_centrifydc_cloud.so` file.

5. Rename the `pam_centrifydc_cloud.so` file.

6. Create a symlink for the `pam_centrifydc_cloud.so` file to point to the `pam_securid.so` file instead.

   For the affected users on the affected UNIX or Linux computers, those users will now need to enter their RSA SecurID pass code in order to log in to those computers.

Verifying the Installation

To verify the authentication service and SecurID setup:

1. On the RSA Administration Server, add and configure a UNIX user.

2. Confirm that the local UNIX user can log in using the SecurID token by running the RSA acetest command.

3. In Access Manager, create a UNIX profile for a user in the zone where the UNIX machine is registered.

4. On the RSA Administration Server, register the UNIX profile user and assign them a SecurID token.

5. On the UNIX computer, log in with the new user.

       Tip: Use the UNIX login user name, not the Active Directory user name, when logging in to the UNIX computer.

Controlling Machine Access with DirectControl

If you need to disable a user's access to a particular computer, you can do so by one of three ways:

• • • • • •

- Disable the user's Active Directory Account.

- Remove the user from the DirectControl Zone.

- Deselect the "Enable user access to this zone" option in the user's Centrify Profile tab.

Known Issues

- For `sshd_config`, you should explicitly set the following parameter to `Yes`. Even though the parameter is defaulted to this value, it sometimes is not correctly set. Without this parameter, you will not receive prompts for events like New Pin, and so forth.

  `ChallengeResponseAuthentication Yes`

- Even though the user authenticates with their SecurID token, they may be prompted to reset their Active Directory password if it has expired in the domain. After the user logs in, they will be presented with the "Change Password" prompts from Active Directory.

- When a user authenticates with a SecurID token, they are granted access to the UNIX machine, but they are not authenticated to the Active Directory Domain. As a result, they will not have Kerberos Credentials or single sign-on capability to other systems. After signing on, the user may type the following and then enter their Active Directory password to authenticate to Active Directory.

  `>kinit`