Centrify Server Suite 2016

RSA SecurID Token Configuration for UNIX/Linux Computers

May 2016

Centrify Corporation

Legal notice

Contents

Configuring DirectControl and RSA SecurID

This document describes the steps necessary to install and configure DirectControl 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.

Overview

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 DirectControl and RSA SecurID to work together in either of two ways:

- Configure the PAM modules to work with DirectControl and RSA SecurID
- Configure SecurID for use with Centrify zone-based role and privilege execution

If you're using an older version of DirectControl or using a version that does not include multi-factor authentication (MFA) support, you can configure the PAM modules to work with DirectControl 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 DirectControl deployment.

Prerequisites

You need to have DirectControl 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 DirectControl 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 DirectControl 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 DirectControl agent, you need to join the computer to Active Directory and place it in a DirectControl Zone.

Installation overview

To install and configure DirectControl and RSA SecurID (an overview):

1. Install the DirectControl agent.

   For details, see the Centrify Server Suite 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" on page 10.

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 DirectControl 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:

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

  For details, see "Configuring the /etc/pam.d/system-auth file for Linux" on page 6.

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

  For details, see "Configuring the pam.conf file for Solaris and AIX" on page 7.

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 SSH to require SecurID" on page 9.

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

After you've installed both the RSA SecurID and Direct Control 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 Centrify Direct Control.

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 DirectControl. 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/sshd_config` file and comment out the lines for the following items:

- GSSAPIKeyExchange
- GSSAPIAuthentication
- GSSAPICleanupCredentials

3 In the `/etc/centrifydc/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 DirectManage Access Manager, configure your role definitions to use multi-factor authentication:

a In DirectManage 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 **System Rights** tab.

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

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

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

a In DirectManage 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 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 DirectControl 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 DirectManage 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
  ```