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

Certificate Auto-enrollment Quick Start Guide

December 2019 (release 19.9)

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

Certificate Auto-enrollment Quick Start Guide

If you are an administrator of Centrify-managed UNIX or Linux computers, you can use this guide to help you set up a Certificate Authority with the Microsoft Windows certificate auto-enrollment feature to automatically manage certificates for UNIX and Linux computers in your domain. While there are many ways to deploy certificates, this guide describes how to use Active Directory server roles and Windows Group Policy to set up automatic enrollment.

The following topics are covered:

Working with a single Certificate Authority for UNIX computers

The Centrify agent uses the Microsoft Windows public key infrastructure (PKI) to obtain the certificates used by your Centrify-managed UNIX or Linux computers that are joined to a domain. By joining to the domain, these computers become eligible for auto-enrollment.

The most basic configuration of the Windows PKI environment utilizes a Windows server as the Certificate Authority (CA) that issues and manages security credentials and public keys through the exchange of encrypted digital certificates. The Centrify agent then uses the Microsoft Windows certificate auto-enrollment feature of the Certificate Authority to make certificates available to UNIX computers.

This section describes how to set up a basic environment that has a single, enterprise root Certificate Authority (CA). In this scenario, the Certificate Authority is a Microsoft Enterprise Certificate Server that issues all certificates. In a production environment, you may have more complex requirements that include multiple CAs configured for a domain. However, setting up this sample environment should give you enough information to extend your PKI configuration to a more complex environment.

The Centrify agent requires a Microsoft Windows Server to be configured as the Certification Authority (CA) for the Active Directory forest. Additionally, auto-enrollment is not supported for certificates issued by other public or private Certificate Authority services or organizations.

Preparing a computer to be a Certificate Authority (CA)

The first step in configuring the environment is to identify a computer to be the Certificate Authority server for the Active Directory forest. This computer must be connected to a network with a server that has Windows Server 2008 (or later) Domain Name Service installed, and it must be joined to the Active Directory domain. In most cases, the computer designated to be the CA should not be a domain controller in a live production environment. To configure the computer as a Certificate Authority, you must install Microsoft Internet Information Services (IIS) and Certificate Services.

Microsoft Internet Information Services (IIS) are required to handle Certificate Revocation List (CRL) requests made by the authentication service and to provide the virtual directories required to issue and manage certificates.

Certificate Services are required to enable the computer to act as a Certificate Authority (CA) and issue certificates to other computers that join the domain. The Application server role, which installs IIS, and the Certificate Services server role must be on the same computer. Therefore Centrify recommends that you install IIS at the same time you install Certificate Services.

What's required to install Certificate Services

Before installing Certificate Services, check that you have the following:

- Account credentials for an account that is an Enterprise Administrator and a Domain Administrator of the forest root domain of the Active Directory forest.

- A computer with Windows Server 2008 Enterprise Edition or later. Previous versions of Windows Server do not support auto-enrollment within the certificate templates. In addition, the computer must be running Enterprise Edition because Standard Edition does not support the V2 or V3 certificate templates that are required for auto-enrollment.
- Active Directory services must be installed on the Certificate Services server. If you install the Certificate Services server role on a domain controller, no further action is required. When you promote a computer to be a domain controller, the Active Directory services are installed automatically.

  Note: This guide details how to configure auto-enrollment on a computer running Windows Server 2012 R2. For information on configuring auto-enrollment for computers running other versions of Windows Server, please visit the Microsoft website.

Add the required server roles to make the computer a Certificate Authority

After you have verified that you have an appropriate account and computer configuration, you can use Server Manager to add the appropriate server roles.

To install IIS and Certificate Services on a Windows Server

1. Open the Server Manager Dashboard and click **Add Roles and Features**.

   Click **Next**.
2. For Installation Type, select **Role-based or feature-based installation**, then click **Next**.
3. Ensure that **Select a server from the server pool** is selected and highlight the server on which you would like to install roles and features. Click **Next**.
4. Select **Active Directory Certificate Services**, then click **Add Required Features** in the pop-up window.

   Click **Next**.
5. Click **Next** to accept the default selections for Select Features.
6. Click **Next** on the notification that you will be unable to change the domain settings after installing Certificate Services.

7. Select **Certification Authority** and click **Next**.
8. Click **Install**.

After Windows restarts, you will see a new Role in Server Manager called AD CS. In the following procedure, you will configure this role to allow your server to act as a Certification Authority.

Configure the Certificate Authority

1. Click the notification icon in the Server Manager command bar to open the **Add Roles and Features Wizard**.
2. Click the link, **Configure Active Directory Certificate Services on the destination server**.
3. In the AD CS configuration screen, verify that you are logged on as an administrator and click **Next**.
4. Select **Certification Authority** and click **Next**.
5. Select **Enterprise CA** and click **Next**.

   Note: You must be a member of both the Enterprise Admins group and the Domain Admins group to configure an Enterprise Certificate Authority.

6. Select **Root CA** and click **Next**.
7. Select **Create a new private key** and click **Next**.
8. Accept the defaults for the cryptographic provider, key length, and hash algorithm. Click **Next**.
9. Enter a name for the Certificate Authority or accept the defaults, and click **Next.**.

   Note: After the Certificate Authority is configured, you will not be able to change the name.

10. Specify the validity period of the certificate, click **Next**.
11. Accept the default location for the certificate database and click **Next**.
12. Review your CA configuration and click **Configure**.
13. Click **Close** when the confirmation message appears, and restart the server to retrieve a certificate from the CA.

Adding a trusted root certificate to the group policy

You can use the certificate snap-in to make a copy of a certificate to use on another computer, or to create a backup copy.

In order to establish a chain of trust for your PKI environment, you identify the copy of the CA you just created as a trust anchor.

To establish the CA as a trust anchor, add the root certificate for the CA to the **Trusted Root Certification Authorities** container in the group policy object that defines the IP Security policies.

To add a trusted root certificate to the group policy object:

1. Open the Certificates (MMC) snap-in.

   If the Certificates snap-in is not available, you can run MMC and click **File > Add/Remove Snap-in** to add it.
2. Select Computer account, and click **Next**.
3. Select Local computer, then click **Next**.
4. Click **Certificates > Trusted Root Certification Authorities > Certificates**.
5. Select the root certificate generated by the CA you created in the previous procedure, then double-click it to see its Properties page.
6. Click the **Details** tab; then click **Copy to file** to start the Certificate Export Wizard. In the wizard, make the following selections:
   - **File format**: *DER encoded binary X.509 (.CER)*
   - **File Name**: Anywhere on the local server
   - **Include all certificates in the certification path**: *No*

7. Open the Group Policy Object Editor and select the group policy object that defines the IP Security policies.

   Click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.

8. Select **Trusted Root Certification Authorities**, right click, and select **Import** to open the Certificate Import Wizard.
9. Click **Next** on the **Welcome** screen.
10. Browse to find the root certificate you copied in Step 6, then click to accept the default values on each screen.
11. Click **Finish** to complete the wizard.

The root certificate is now in the Active Directory Trusted Root Certification Authorities container. Certificates in this container are downloaded to any computer that joins the domain to establish trust for the root CA.

Enabling auto-enrollment

The Centrify agent uses the Microsoft Windows certificate auto-enrollment feature to make certificates available to UNIX computers. If auto-enrollment is enabled, when a UNIX computer joins a domain, the Centrify agent requests certificates from the CA based on particular templates, and installs them on the joined computer.

To enable auto-enrollment, you must do the following:

- Enable auto-enrollment for the group policy.
- Create a certificate template with auto-enrollment enabled.

Enabling auto-enrollment for the group policy

To enable auto-enrollment for the group policy:

1. Open the Group Policy Management Editor and select the group policy object that defines IPsec policies.

   Click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Services Client - Auto Enrollment**.
2. Double-click **Certificate Services Client - Auto-Enrollment**, select Enabled, and check the following boxes:
   - **Renew expired certificate, update pending certificates, and remove revoked certificates**
   - **Update certificates that use certificate templates**
3. Click **OK** to save the auto-enrollment settings.

Creating a certificate template

To configure a template with auto-enrollment:

1. Open the MMC Certificate Template snap-in.

   Another way to open the Certificate Template console is to open the Certification Authority console, right-click **Certificate Templates**, and select Manage.

2. Select a template, then right-click and select **Duplicate Template** to create a new template that you can modify.

   For example, select the Workstation Authentication template.

3. On the Properties page for the new template, do the following:
   a. Select the **General** tab and enter a name for the template.
   b. Select the **Security** tab and select **Domain Computers**. Then select **Read** and **Autoenroll** permissions.
   c. Select the **Subject Name** tab. For **Subject name format**, select **Fully distinguished name**.
   d. Select the **Extensions** tab. Then select **Application Policies**.
   e. Click **Edit**. **Client Authentication** should already be shown.
   f. Click **Add**, then scroll and select **Server Authentication**.
   g. Click **OK**.
4. Click **OK** to save the new template.

Assigning the certificate template to the CA

You can now assign the newly created template to the Certificate Authority. Whenever a computer joins the domain, the CA issues a certificate based on the template, and the Centrify agent downloads the certificate to the computer.

To assign the template to a CA:

1. Open the Certification Authority console.
2. Click **Certification Authority > CA_*name* > Certificate Templates**, where CA_*name* is the container for the CA you set up earlier in Preparing a computer to be a Certificate Authority (CA).
3. Right-click and select **New > Certificate Template to Issue**. Select the template you just created and click **OK**.

The root CA is now set up to issue certificates based on the template you created.

Retrieving certificate revocation lists (CRLs)

Generating a certificate revocation list (CRL) is the method a Certificate Authority (CA) uses to maintain the validity of the certificates that it issues. A CRL contains a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid, and therefore should not be relied upon. The agent retrieves CRLs from CAs after specific events (such as joining a domain) and at specific intervals to determine which certificates, if any, have been revoked, and thus whether to request new certificates.

Note: The current version of the Centrify agent only supports complete certificate lists, not delta CRLs, which only describe the updates since the complete list was published.

Generating a certificate revocation list (CRL)

A CRL is generated by a CA and contains a list of certificates to revoke from the list of certificates that the CA has issued.

Typically, a CA automatically generates a CRL at a specified interval, anywhere from two hours to one year, at which point the new CRL with the list of revoked certificates is available for clients to request.

The CRL itself contains the interval period, which allows clients, such as Centrify Authentication Service, to determine when to request a new CRL. See Retrieving a certificate revocation list and verifying certificates for information about retrieving CRLs.

In addition to automatic generation of a CRL, an administrator can use specific Active Directory utilities that allow them to manually revoke certificates and publish a CRL on the CA. In this case, the CRL-publishing interval is reset so the

next automatic publishing operation will occur in the appropriate amount of time.

Retrieving a certificate revocation list and verifying certificates

At specific times (when the UNIX system joins a domain, the administrator issues the `adgpupdate` command, or the group policy refresh interval occurs), the Centrify agent performs certain tasks, including determining whether to retrieve a CRL. Specifically, the agent does the following:

- Identifies the CA that issued certificates for the system.
- Looks at the refresh interval in the current CRL to determine whether to retrieve a new CRL.
- If the interval has expired, retrieves a new CRL by using the IIS Web Server for the CA.
- Verifies the currently issued certificates against the CRL and requests new certificates for certificates that have been revoked.

  Note: When you manually revoke a certificate, it is possible that the certificate will appear as valid even after running the `adgpupdate` command to trigger an IPsec update. When you revoke a certificate, the Centrify agent first looks at the current CRL to determine the validity of the certificates that have been issued. In this case, the newly revoked certificate still appears as valid. Immediately afterwards, because of the IPsec update, the agent requests a new CRL. The new CRL shows that the certificate in question is invalid, but the agent will not look at the new CRL until the next scheduled update, or until you run the `adgpupdate` command again. Therefore, to be certain to have current information, if you manually revoke certificates, you can issue the `adgpupdate` command twice in sequence.