Privileged Access Service

Installation Guide for On-Premises Deployment (Evaluation Version)

release 21.7

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

Privileged Access Service Evaluation Version

As an on-premises solution that you manage without access to the Centrify cloud, Centrify PAS replicates the infrastructure provided by the Centrify Identity Platform using computers on your network. After you install Centrify PAS, you use the Admin Portal to add, manage, and access the resources, domains, and databases and the corresponding accounts you add to the Centrify PAS.

This document describes how to install an evaluation version of the Centrify PAS on a single Windows computer. For information about installing Centrify PAS in a high availability (HA) environment containing multiple clustered computers, see the *Installation and Configuration Guide for High Availability On-premises Deployment*.

> **Note:** If you intend to eventually install Centrify PAS in an HA environment, contact Centrify for assistance.

Prerequisites

Ensure that the computer used to install Privileged Access Service meets the following hardware requirements:

- At least two CPUs.
- At least 16GB of memory.
- At least 20GB of free disk space.

Ensure that the computer where you are installing the evaluation version of Centrify PAS meets the following software requirements:

- The operating system is Windows 2012 R2 or Windows Server 2016.

  The computer has access to the internet, or—if the computer is not connected to the internet—access to installation media for required software. For example, IIS, PowerShell, and other features are required to support the Centrify PAS. If the supporting software is not already installed on the computer, it is installed automatically as part of the Centrify PAS installation. If you are using local media to install required software, connect the media to the computer before you begin the Centrify PAS installation.

  Note: If you are using a self-signed certificate, you will need Internet access to validate it during installation.

- If external access to installed services over https is necessary, port 443 must be available for TCP/IP.
- A fixed IP address.
- The Microsoft .NET Framework is updated to version 4.8.
- Permissions: You need permission to create and delete computer accounts and Full Control on cluster computer objects.
- Server requirements: only one (active) server can be run against the same database at the same time.
- Do not use the computer with Centrify customer-managed Centrify PAS installed as an App server. For instance, if you are using the Centrify Desktop App feature in the Admin Portal, which requires an App server to run Remote Desktop Services, make sure you do not run the App server on the same computer that includes the Centrify customer-managed Centrify PAS.

PostgreSQL database requirements

If you use a customer-managed PostgreSQL database, make sure it is set up to recognize the IP addresses for the server node computer in the cluster of the Centrify PAS. For instructions on how to install Centrify PAS with a customer-managed PostgreSQL database, see the procedures in Install on the primary server.

Note: Adding a load balancer to your configuration is not required as only one IIS service is running at one time. If your configuration does include a load balancer, configuration and setup is

dependent on your specific load balancer implementation and is beyond the scope of this document.

Additionally, the following are database requirements.

Database user requirements

The following is the user requirement for PostgreSQL database:

Create a new database user with `login`, `inherit`, `createdb`, and `createrole` permissions.

Database naming requirements

The default database username is "postgres" with a database name "postgres." If you change the database username, you must name the database the same name as the database username.

Database version requirements

Ensure version of the database is 9.6.9 or 10 if using SSL connection.

Create root and server certificates

To enable SSL, refer to the PostgreSQL product documentation: https://www.postgresql.org/docs/9.1/ssl-tcp.html.

Configure PostgreSQL to allow remote connection

To configure PostgreSQL server, perform the following steps:

By default, PostgreSQL service only listen to local IP addresses and allows local connections only.

1. Edit `/var/lib/pgsql/9.6/data/postgresql.conf`, and change and/or add the line below to configure PostgreSQL service to listen to all IP addresses:

```
listen_addresses = '*'
```

2. Edit `/var/lib/pgsql/9.6/data/pg_hba.conf` by adding the following to allow remote connection:

```
host all all 0.0.0.0/0 md5
```

3. Restart PostgreSQL by entering the following:

```
$ systemctl restart postgresql-9.6
```

IP addresses and DNS

Reserve an unused IP address on your network, and assign the DNS name for your Privileged Access Service web site (for example, *vault.mycompany.com*).

This is the web service URL that will be used by end users to access the Centrify PAS in a web browser (for example, *https:// vault.mycompany.com/*).

You will be prompted to specify the Centrify PAS URL/FQDN (for example, *vault.mycompany.com*) when you install the Centrify PAS on the primary server in the node.

> **Note:** You cannot change the Centrify PAS URL name after the Centrify PAS is installed and the cluster is configured.

Certificates and License Keys

- Ensure that a trusted host certificate from a public certificate authority (CA) is available on the primary server in the cluster where you are installing the Privileged Access Service. The certificate must be for the URI of the Centrify PAS web site (for example, *vault.mycompany.com*).

  In a production environment, it is likely that you already have a trusted certificate that you can use. Before installing the Centrify PAS, you should create or identify the certificate you want to use, verify that you know the location of the certificate file, and ensure that the file is available to each node computer. The certificate file must be a PKCS #12 file with both private and public keys.
- Obtain an Centrify PAS license key that is specific to your company. During installation, you will be prompted for your company name and the license key that is bound to the company name. Contact a Centrify representative if you do not have an Centrify PAS license key.

Centrify Privileged Access Service and PostgreSQL

Centrify Centrify PAS can use PostgreSQL for its database in customer-managed installations. Centrify PAS connects to the PostgreSQL instance using a customer-defined database connection string. It maintains multiple connections to its database at run-time. In the event the connections are

interrupted and dropped – for example, database failover – Centrify PAS will re-establish the connections. SSL connections to PostgreSQL are supported.

Centrify PAS expects LAN-type latency (low latency) in the database connection.

Centrify PAS sees the database in the context of a database connection string. Database operations that take place above the database itself – for example, back up, log shipping, or high availability services – are effectively transparent to Centrify PAS.

This makes Centrify PAS agnostic with regards to:

- The operating system running PostgreSQL.

  Note: PostgreSQL has its own requirements for operating systems and versions.

- PostgreSQL clustering services.
- PostgreSQL high availability services.
- PostgreSQL backup services.

Hardening the system (recommended)

For security, it is recommended you secure the Privileged Access Service server (s) and their local file systems. To do this, refer to the *Centrify Centrify PAS Hardening Guide* that is delivered with the Centrify Software download package.

Installing Centrify Privileged Access Service Evaluation Version

The procedures in this section describe how to install the Centrify PAS evaluation version. Installing the Centrify PAS on a computer that will be used for evaluation purposes is performed in two stages:

- First stage—installation wizard guides you through choices for the license agreement, feature selection, optional customer-managed PostgreSQL database selection, installation location, and installation of the software.

- Second stage—PowerShell script that launches automatically, and prompts you for additional information to set up the Centrify PAS.

  Note: By default, installation logging is not enabled for the portion of the installation performed by the installation wizard. You can optionally enable installation logging prior to installing Centrify PAS so that an installation log file is created. See Creating an installation log file for details about enabling installation logging.

To convert an evaluation configuration into an HA configuration, Contact Centrify Customer Support.

Note: *For Windows Server 2016 installations:* If you are using Windows Defender, installation automatically makes and removes exclusions for the following items: Program Data directory, Application Data Directory, and the infrastructure `service_installer.exe` process. However, if you are using a third-party Antivirus, it is recommended that you add the above items to the exclusion list during installation.

To install the Privileged Access Service for evaluation:

1. On the computer that you will use to evaluate Centrify PAS, log in as an AD user with domain administrator rights.
2. Download the Centrify PAS installation file (the file is in `.exe` format).

   For backup and restoration purposes, it is recommended that you archive the Centrify PAS installation file so that—if necessary—you can restore the version and build number that you originally installed. See Backing up and restoring Privileged Access Service for more information.
3. Double-click the installation file to start the installation.

   Note: If the Microsoft .NET Framework version is not updated to version 4.8 on the computer where you are performing the installation, a dialog box stating that the Microsoft .NET Framework is required may appear. Dismiss the dialog box and then install the Microsoft .NET Framework version 4.8 according to instructions available from Microsoft.
4. When the Centrify Identity Platform installation wizard launches, follow the prompts to accept the license agreement, and provide a license key that is specific to your company name.
5. In the Feature Selection screen, select **Evaluation** and click **Next**.

6. (Optional) At the Database Option screen, select the check box to configure a customer-managed PostgreSQL database.

   If you want to use the default PostgreSQL database available with Centrify PAS, do *not* select this option and click **Next** to skip this step.

   If you select this option, make sure your customer-managed PostgreSQL database is set up to recognize the IP addresses for Centrify PAS and that the version of the database is 9.6.9 or 10 series if using SSL connection. For additional information on PostgreSQL databases, see https://www.postgresql.org/docs/9.6/static/index.html.

   Configure the following options in the Database Option screen to connect Centrify PAS to your customer-managed PostgreSQL database:

   - Host: Enter the IP address or the DNS for your custom database.

     If you are connecting to the PostgreSQL database using SSL mode, you need to enter the CN (Common Name) associated with the PostgreSQL database server certificate here (also see the Certificate field below).

   - Port: Enter the TCP/IP port number that PostgreSQL uses to listen for connections from client applications (configured during PostgreSQL installation). The default is 5432.

   - Username: Enter the name used to log in to the database.

     Note: If you are not using the default built-in PostgreSQL user, the user must be in the following (minimum) database roles:

   - Can login?
   - Create roles?
   - Create databases?
   - Inherit rights from the parent roles?

   Additionally, you must create a new database with the same username. For example: create a new database called "test1", make this the new database user, and make the "test1" user the owner of the database.

   - Password: Enter the password associated with the Username used to log in to the database.
   - Certificate: (Optional) If SSL mode is required when connecting to the PostgreSQL database, click **Browse** to upload the required certificate

to the primary computer. See the PostgreSQL documentation for more information on enabling SSL mode.

7. Click **Next**.

   If the connection to the database is successful (no errors are displayed), continue with installation.

   Note: If you intend to uninstall the Centrify PAS version with a customer-managed PostgreSQL database and reinstall it, you first need to remove the original customer-managed PostgreSQL database instances created in the customer-managed database system before reinstalling Centrify PAS.

8. In the Destination Folder screen, select an installation folder and click **Next**.
9. In the Ready to Install Centrify Identity Platform screen, click **Install** to install components.
10. After all components are installed, click **Finish** to complete the installation of the Centrify PAS software.

    Immediately after you complete the installation, a Windows PowerShell console opens, prompting you for additional information to set up the service. You must provide the information described in the following steps before you can use the Centrify PAS.

11. At the first PowerShell prompt, specify a name for a new Centrify Centrify PAS user who will have Centrify PAS administrative privileges, then press **Enter** to continue.

    The user will be created as a Centrify Centrify PAS user, and will be the initial system administrator for the Centrify PAS. For example:

    `CISadmin@cps_eval.com`

    Note: The user name that you specify must not match an existing Active Directory user name. If you specify an existing Active Directory user name, login conflicts will occur if the Active Directory user attempts to log in to the Centrify PAS.

12. At the next PowerShell prompt, specify an email address for the administrative account, then press **Enter** to continue.
13. At the next PowerShell prompt, create a password for the administrative account, then press **Enter** to continue.

14. At the next PowerShell prompt, specify the URL (that is, a known, resolvable FQDN such as *https://vault.mycompany.com/*) for the Centrify PAS web site.

    This is the unique web site URL described earlier in IP addresses and DNS. It is used for the web service and points to the system IP address where you are installing Centrify PAS.

    The host certificate that you will specify in the next step must be for this URL. The URL that you specify here is the URL that users will specify in their web browsers or clients to connect to the Centrify PAS. After the installation finishes, you cannot change this URL name.

15. At the next PowerShell prompt, specify to use an existing certificate from a trusted certificate authority. See Certificates and License Keys for more information about how to respond to this prompt.

    Note: If you use a self-signed certificate, you must have configured your domain (or this computer) to trust the self-signed certificate root.

    The certificate file must be a PKCS #12 file with both private and public keys, and it must be issued for the Centrify PAS URL that you specified in the previous step 12.

    If necessary, you can change to a different certificate later as described in Updating or replacing a host certificate.

16. Next, you are prompted to select a folder for the service database (CisDB). Navigate to the CisDB shared disk, select a folder there, and click **Select Folder**.

17. Next, you are prompted to select a location for the service setup/recovery file (also referred to as the *cluster configuration file, clconf.zip*). Specify a secure location for the file, and click **Select Folder.**

    If you save the cluster configuration file in the default location on the server, it is located here:

    \program files\centrify\centrify identity\platform\config\clconf.zip

    The PowerShell script continues to run, displaying messages about the operations it performs. When the script finishes, you can access the Centrify PAS by opening a browser to the URL (https://vault.mycompany.com/) that you specified in step 12.

18. A Centrify login screen displays. Log in using the administrator user credentials that you specified in step 9 and step 11.

    The Centrify PAS launches, with the Centrify PAS displayed by default. The Centrify PAS is now usable, but the connector has not been installed yet.

Install the connector

After you have installed the Privileged Access Service, install the Centrify Connector, and configure the connector to use the Centrify PAS URL (*https://vault.mycompany.com/*).

> **Note:** For additional information about installing the connector, including prerequisites and permission requirements, see the doc portal.

To install the connector, you must first get the Centrify PAS Management Suite package, and then run the installation wizard.

To install a connector on a host computer:

1. Log in to the host computer located outside of the cluster, using an account that has sufficient permissions to install the connector.
2. Open Admin Portal (for example, *https://vault.mycompany.com*).
3. Click **Settings > Network > Centrify Connector > Add Centrify Connectors**.
4. Click **64-bit** in the Download pane.

   The download begins.
5. Extract the files.
6. Double-click the installation program: `Centrify Installer`

   In the file name, rr.r indicates the release version and aa indicates the processor architecture (64-bit).
7. Click **Yes** to continue if the User Account Control warning displays.
8. Click **Next** on the Welcome page.
9. Review the End User Software License and Services Agreement, accept the terms of agreement, then click **Next**.
10. Select the components to install, then click **Next**.

The default is to install all components. Use the description on the installation UI to determine what you want to install.

11. Click **Install** > **Finish** to open a second installation wizard.

    This second installation wizard initiates the connection between Active Directory and your Centrify PAS tenant.

12. Click **Next** on the Welcome page.

13. Type the administrative user name and password for your Centrify PAS account, then click **Next**.

14. Change the default URL—*https://cloud.centrify.com/*— to the Centrify PAS URL that you specified during Centrify PAS installation (*https://vault.mycompany.com/*).

15. Click **Next** unless you are using a web proxy server to connect to Centrify PAS.

    If you are using a web proxy service, select the associated check box and specify the IP address, port, user name, and password to use.

16. Specify the monitored domains and relevant credentials to synchronize deleted objects in Active Directory/LDAP with Centrify PAS, then click **Next**.

    When you delete users in Active Directory and want this deletion synchronized with Centrify PAS, you have two options:

    - You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains.
    - Delegate read permissions to the service account for the deleted objects container in the corresponding domain.

    If you do not take one of the preceding actions, users deleted in Active Directory will be listed on the Users page in the Admin Portal until you manually delete them. However, they will not have access to Centrify PAS features.

    The configuration wizard performs several tests to ensure connectivity.

17. Click **Finish** to complete the configuration and open the connector configuration panel, which displays the status of the connection and your customer ID.

18. Click **Centrify Connector** to view or change any of the default settings.

19. Click **Close**.

After you have installed and configured at least one connector, you can use either Admin Portal or your default browser to log on to Centrify PAS. The next time you log on and see the welcome page, select **Don't show this to me again**, then click **Close**.

Upgrading to a new Centrify Privileged Access Service release

This section describes how to upgrade to a new Centrify PAS release in an evaluation environment where the Centrify PAS is already installed and running.

Note: This section does not describe how to upgrade from an evaluation version of the Centrify PAS release to an HA Centrify PAS release.

To upgrade to a new Privileged Access Service release:

1. Start the installation by double-clicking the installation file (.exe file).

   Note: If the Microsoft .NET Framework version is not updated to version 4.8 on the computer where you are performing the installation, a dialog box stating that the Microsoft .NET Framework is required may appear. Dismiss the dialog box and then install the Microsoft .NET Framework version 4.8 according to instructions available from Microsoft.

   The Centrify Identity Platform installation wizard launches, and detects the existing Centrify PAS installation.

2. In the **Ready to Update Centrify Identity Platform** wizard screen, click **Update**.

   System messages display as the new release is installed.

3. When the installation wizard finishes, click **Finish** at the prompt.

   A Windows PowerShell console opens, prompting you for additional information to set up the service.

4. Follow the prompts to complete installation.

   The Centrify PAS upgrade is now complete.

Note: If upgrading on an instance where the Centrify Connector is installed on the same machine as the Centrify PAS server, remember to restart the connector service.

Uninstalling the Centrify Privileged Access Service Evaluation

To uninstall Privileged Access Service from your computer:

1. On a computer where the Centrify PAS is installed, log in as an AD user with domain administrator rights.
2. Launch the installation wizard by double-clicking the installation file.
3. Follow the prompts displayed until you reach the prompt giving you the choice to change, repair, or remove Centrify Identity Service. Select **Remove**.
4. After the installation wizard finishes removing files, click **Finish**.
5. Reboot the computer to complete the removal of the Centrify PAS software.

   Note: If you do not have access to the Centrify PAS installation file, you can use the Windows **Programs and Features** control panel to uninstall Centrify Identity Platform. Uninstalling Centrify Identity Platform also uninstalls Centrify PAS.

   Note: If you uninstall an Centrify PAS version with a customer-managed PostgreSQL database and plan to reinstall it, you first need to remove the original customer-managed PostgreSQL database instances created in the customer-managed database system before reinstalling Centrify PAS.

Performing post-installation tasks

If any of the following tasks were not performed when you originally installed Privileged Access Service, perform them now.

• • • • • •

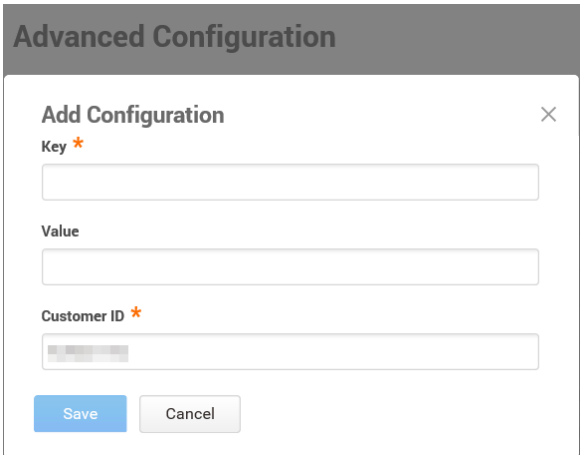
To perform post-installation tasks:

1. In the Admin Portal, manually configure services and features as described in Enabling services and features after installation.
2. In the Admin Portal, set up additional Centrify PAS accounts and resources as described in the Centrify PAS online help, and the Centrify PAS *Getting Started Guide*.
3. In the Admin Portal, enroll devices as described in the following Admin Portal help topics:
    - In the Admin Portal Dashboards page, select **Getting Started** from the dashboard drop-down list. In the left-hand pane, select **Enrolling mobile devices**.
    - In any Admin Portal page, click the Help icon to open the online help system. In the table of contents in the left-hand pane, select either **Commonly used How To scenarios > How to enroll devices** or **Managing devices > Enrolling a device**.

    Note: The issuer of host certificate must be trusted by mobile devices for device enrollment to succeed. The certificate is trusted by a device if it is issued by a public certificate authority. Also note that for device enrollment to succeed, you need disable certificate pinning (see To disable certificate pinning in the Admin Portal:).

To disable certificate pinning in the Admin Portal:

1. In the Admin Portal, click **Settings > Customization > Advanced Configuration** and then click **Add.**
2. At the Add Configuration screen, enter the following values:
    - Key field—`HostCertificatePinningDisabled`
    - Value field—`True`



3. Click **Save**.

   Note: If the `HostCertificatePinningDisabled` key is not configured as `true`, you must disable Cert Pinning in **Settings** > **Server Authentication** > **Enable Cert Pinning** when enrolling devices.

Creating an installation log file

You can optionally use the native Windows installation logging facility to save information about your Privileged Access Service installation session.

To save installation session information using the Windows installation logger:

1. In a command prompt window, launch the installation with logging enabled.

   For example, you would issue the following command to perform an installation using the `Centrify_Infrastructure_Service-18.6.exe` file, and save the log information in a file named `cps.log`:

   ```
   Centrify_Infrastructure_Service-18.6.exe /l cps.log
   ```

   You can also use the `-log`, `/log`, or `-l` option to specify a log file.

   If you do specify a file, log information is saved in the file `Centrify Identity Platform` version_timestamp`.log` in your computer's temporary file folder. For example:

   ```
   C:\Users\Administrator\AppData\Local\Temp\Centrify Identity
   Platform 18.6.125_20171205022113.log
   ```

2. Install Centrify PAS as described in Installing Centrify Privileged Access Service Evaluation Version .

3. When the installation finishes, review the log file to verify that it saved the log events from the installation session.

Administering and Troubleshooting Centrify Privileged Access Service

In general, this chapter describes how to perform basic Centrify Privileged Access Service administration and troubleshooting tasks. It is assumed that you have already installed and logged in to the Centrify PAS.

Enabling services and features after installation

The following services and features are available by default in the cloud-based version of the Centrify Privileged Access Service, but are not available by default in the on-premises version of the Centrify PAS:

- SMTP server for email support.
- Twilio account for SMS.
- Google Maps.
- 42Matters.

To make these services and features available, you must enable them manually as described in the following sections after installing the Centrify PAS.

Enabling an SMTP server for email support

You must configure an SMTP server for email features to be available. If you do not configure an SMTP server, the following capabilities that require email support are not available in the Centrify Privileged Access Service:

- Invite new users to log on.
- Use email as an authentication option in multi-factor authentication.
- Request and approve access to applications through workflows.
- Request and approve password checkout and login access requests through workflows.
- Receive email notification about the results of password migration jobs.
- Receive email notification about the results of provisioning jobs.
- Receive directory synchronization reports.

To enable an SMTP server for email support:

1. In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.
2. In System Configuration, select the check box for **Use custom SMTP server settings**.
3. Provide an SMTP user name and password, the name or address of the SMTP server, and the server port number.
4. Click **Save** when you are finished.

Enabling a Twilio account for SMS support

You must configure a Twilio account for SMS features to be available. If you do not configure a Twilio account, features that require SMS support are not available in the Admin Portal.

To enable a Twilio account for SMS support:

1. In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.
2. In System Configuration, select the check box for **Use custom Twilio account settings**.
3. Specify an account SID, an authentication token, and a From Number or sender ID.

   Note: Both Programmable Voice and Programmable Messaging services are needed to run phone calls and SMS for MFA.

Enabling Google Maps

You must configure Google Maps for maps to be available. If you do not configure Google Maps, the map widget in the Admin Portal will indicate that maps are not available.

To enable Google Maps:

1. In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.
2. In System Configuration, select the check box for **Use custom Google API settings**.
3. Specify a Google client ID or API key (such as an ID or key from a Google or gmail account).

Enabling 42Matters

You must configure 42Matters to enable searching for mobile applications. If you do not configure 42Matters, the mobile application UI is hidden in the Admin Portal.

To enable 42Matters to support mobile application searching:

1. In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.
2. In System Configuration, select the check box for **Use custom 42Matters.com settings**.
3. Specify a 42Matters API key.

Executing scripts provided with Centrify Privileged Access Service

The Centrify Privileged Access Service provides several scripts, some of which you can execute manually to perform various configuration and administration tasks after the Centrify PAS is installed. If the Centrify PAS is installed in the default location, the scripts reside in this folder:

- - - - - -

```
C:\Program Files\Centrify\Centrify Identity Service\scripts
```

Log diagnostic information

A PowerShell script (`capture_diagnostics.ps1`) is provided with the Centrify Privileged Access Service to record information about the following areas:

- The product registry hive from `HKLM\Software\Centrify`.
- The `cisdb` database.
- Centrify log files for the connector, lrnode, web, and installation log4net.

To save Centrify Privileged Access Service diagnostic information using the capture_diagnostics.ps1 script:

1. Open a PowerShell console window as Administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the Centrify PAS installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. Run the `capture_diagnostics.ps1` script:

   ```
   .\capture_diagnostics.ps1
   ```

   When the script finishes, output is saved in a file named `diag-gid-date.zip`.

Bypassing Admin Portal lockout

If you get locked out of the Admin Portal, you can run the `launch_manageportal.ps1` script to log in to the Admin Portal using the default admin account and a one-time token to authenticate.

To run the launch_manageportal.ps1 script

1. Open a PowerShell console window as Administrator.
2. In the PowerShell console, change to the Centrify Privileged Access Service `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the Centrify PAS installation. If the default installation

location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.

3. Run the `launch_manageportal.ps1` script:

   ```
   .\launch_manageportal.ps1
   ```

When the script finishes, it launches the Admin Portal automatically.

Updating or replacing a host certificate

This section describes how to use the `update_host_cert.ps1` script to update an expired host certificate or change to a different host certificate.

Note: The procedure described here applies only to the evaluation version Centrify Privileged Access Service installations (that is, installations in which the database host and web host are installed on the same computer). If you have installed additional web hosts or a backup database host in a distributed (HA) environment, you cannot update or replace the host certificate.

To update or replace a host certificate:

1. On the computer where the Centrify PAS is running and the host certificate resides, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the Centrify PAS installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. Execute the `update_host_certificate.ps1` script:

   ```
   .\update_host_cert.ps1
   ```
4. When the script runs, you are prompted for the following information:
   - The location of the host certificate.
   - Whether a host certificate password is required.
   - The password for the host certificate, if a password is required.

Restoring administrator access

This section describes how to use the `rescueuser.ps1` script to restore administrator access to the Centrify Privileged Access Service in the event that the administrator account becomes locked out.

While it is possible to reset the password for any user that is listed as a cloud user in the Admin Portal, the `rescueuser.ps1` script is intended to be used specifically to restore the Centrify PAS administrator account (such as the administrator account that was created when the Centrify PAS was originally installed). To see which users can have their password reset, switch to the Admin Portal, open the **Users** tab, and select **Cloud Users** in the **Search** field.

To reset a user password:

1. On the computer where the Centrify PAS is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the Centrify PAS installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. From the `scripts` folder, run the `rescueuser.ps1` script. When the script runs, it prompts you for the name of the user whose access you are restoring, and a new password for that user.
4. Once complete, issue the `iisreset` command to restart IIS.

   For example, to reset the password for an Centrify PAS user named `CISadmin@cps_demo.com`, you would issue the `rescueuser.ps1` command and respond to prompts as follows and then issue the iisreset command:

   ```
   .\rescueuser.ps1
   username: CISadmin@cps_demo.com

   New password for CISadmin@cps_demo.com: **********

   Verify new password: **********

   User reset OK

   iisreset
   ```

Backing up and restoring Privileged Access Service

Use the scripts as described in this section to save data regularly to a secure location, and to recover data that was lost unexpectedly. The following scripts are provided for HA and evaluation Privileged Access Service configurations:

- `pg_backup.ps1`
- `pg_restore.ps1`

Data that is backed up and restored includes the Centrify Identity Service database, and additional configuration information such as application templates, the `config` folder (which retains the certificates necessary to configure the system, as well as encryption keys), and so on.

The information that you back up is specific to the Centrify PAS release and build in which the data was created. You cannot use backup data from one release to restore data in another release, nor can you use backup data from one build to restore data in a different build of the same release. For example, if you back up data in Centrify PAS release 18.5, you cannot restore that data in any release other than 18.5. Also, for example, if you back up data in Centrify PAS build 18.5-190, you cannot restore that data in any build other than 18.5-190. Because of these restrictions, it is recommended that you save the Centrify PAS installation file so that you can restore the version and build number that you originally installed.

Note: The following backup and restore procedures do not apply to configurations that have a customer-managed PostgreSQL database. If your configuration includes a customer-managed PostgreSQL database, you will need to provide your own backup and restore strategy. Be sure to have the name of the customer-managed PostgreSQL database saved during the backup procedure available, as you will need to provide that same name during the restore procedure.

Evaluating Centrify Privileged Access Service

To back up the evaluation version of Centrify Privileged Access Service:

Note: The Centrify PAS must be stopped (and is therefore unavailable) during backup and restore operations.

1. On the computer where evaluation Centrify PAS is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The `scripts` folder is located in the installation folder that was specified during Centrify PAS installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Platform`.
3. From the `scripts` folder, run the `pg_backup.ps1` script, using the `-DestDir` option to specify the folder where the backup file is saved.

   Note: Do not specify the folder where the database resides as the location for the backup file. The folder containing the database is not a supported backup file location. For example, to back up Centrify PAS data and save the backup file in the `D:\Backups` folder, and do so in verbose mode, you would issue the following command:

   ```
   .\pg_backup.ps1 -DestDir D:\Backups -Verbose
   ```

4. At the *Select location of config zip file* screen, navigate to the location of the clconf.zip file and then click **Open**.

   If you saved the cluster configuration file in the default location on the server, it is located here:

   ```
   \ProgramData\Centrify\Centrify Identity
   Platform\data\clconf.zip
   ```

To restore the evaluation version of Centrify Privileged Access Service:

Note: The Centrify PAS must be stopped (and is therefore unavailable) during backup and restore operations.

1. On the computer where the evaluation version of Centrify PAS is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The scripts folder is located in the installation folder that was specified during Centrify PAS installation. If the default installation location was selected, the `scripts` folder is in `C:\Program Files\Centrify\Centrify Identity Platform`.
3. From the `scripts` folder, run the `pg_restore.ps1` script, using the `-SourceDir` option to specify the folder where the backup resides.

For example, to restore Centrify PAS from `D:\Backups\`, you would issue the following command:

```
.\pg_restore.ps1 -sourcedir D:\Backups -initdb -verbose
```

4. After `pg_restore.ps1` finishes, you need to start the IIS service manually on the computer where you performed the restore operation.

Migrating from standalone to primary node

The following describes how to migrate a standalone Centrify Privileged Access Service configuration to a High Availability (HA) primary node. For additional information on creating an HA/clustered configuration, review Create and configure a cluster.

The following two database (DB) environments are available:

- LifeRaft (customers with Centrify PAS for High Availability On-premises Deployment version 17.6 or earlier).
- Postgres (customers with Centrify PAS for High Availability On-premises Deployment version 17.7 or later).

Previously, if you had a standalone configuration and you upgraded from version 17.6 or earlier, you were required to retain the LifeRaft DB. For example, if you started with 17.6 and you upgraded your Centrify PAS version to 18.3, you would retain the LifeRaft DB. The Centrify PAS High Availability On-premises Deployment LifeRaft database configuration does not allow for an update to Centrify PAS HA (cluster features).

In order to convert your standalone configuration to an HA/clustered environment, you need to upgrade the LifeRaft database to a Postgres database first, and then convert the standalone node to a primary node to support clustering.

High Availability upgrade overview

The following steps assume you are starting with a Centrify PAS standalone version 17.6, running LifeRaft DB.

- Upgrade the standalone Centrify PAS instance to 17.7 or later.
- Run the `upgrade_database_engine.ps1` script to move the LifeRaft DB to standalone Postgres DB.
- Run the `make_primary.ps1` script to convert the Centrify PAS standalone node to a Centrify PAS primary node.
- Run the `uninstall_connector.ps1` script to remove the connector on what was the standalone Centrify PAS computer.
- Add secondary nodes.

Running required scripts

The following scripts are required to upgrade from Centrify Privileged Access Service standalone to Centrify PAS HA/Clustered. All scripts are checked into the codebase in Perforce in this location:

`//depot2/Cloud/OnPrem/dev_scripts/`

- `upgrade_database_engine.ps1` (migration script)
- `make_primary.ps1` (conversion script)
- `uninstall_connector.ps1` (remove connector script)

Note: You need the latest version of the Centrify PAS software.

Migration script

`upgrade_database_engine.ps1`

The migration script migrates the Centrify PAS DB from LifeRaft to Postgres.

Once you migrate to Postgres DB, your Centrify PAS instance is still in a standalone configuration. The next step is to convert Centrify PAS from a standalone instance to a Centrify PAS primary node. This allows you to apply the Centrify PAS clustering features.

Conversion script

`make_primary.ps1`

The conversion script takes an Centrify PAS standalone Postgres instance and converts it to an Centrify PAS primary node instance (for Centrify PAS versions 17.7 or above). It also:

- Shuts down the connector.
- Creates a file called “clconf.zip” for cluster/recovery support.
- Moves the database to a shared storage location that you specify.

Uninstall connector script

`uninstall_connector.ps1`

The uninstall connector script uninstalls the connector service on the Centrify PAS standalone computer. In an HA environment, the connector should not be installed on any of the computers in the HA cluster.

Migrating Centrify Privileged Access Service with a LifeRaft database

To migrate Centrify Centrify PAS with a LifeRaft database, perform the followings steps:

1. In the Centrify Admin Portal, navigate to the **About** window, check the version on the standalone Centrify PAS instance. It must indicate version 17.6. (LifeRaft DB configurations end with Centrify Centrify PAS 17.6) as shown below:

   Note: Once you have verified the Centrify PAS version, perform a backup of the system (by reviewing Backing up and restoring Privileged Access Service). This will also back up the LifeRaft DB.

2. Upgrade the Centrify PAS software to version 17.7 or later.

   Note: The web site URL has already been defined in your installation. Use the web site URL that you use to access the

service, instead of the `vault.mycompany.com` from the installation instructions. During installation, if you need to find the web site URL, you can go to IIS manager in **Administrative Tools** and under sites locate **Centrify** and click **Browse website to see the URL**.

3. Once installation is complete, check the version in the Centrify Admin Portal > **About** window to make sure the version is updated.

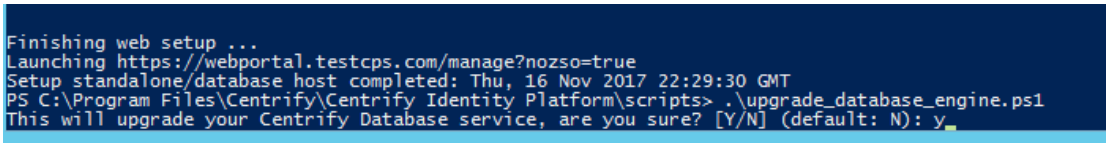
4. Under **Windows Task Manager** > **Services**, locate a service called **Centrify Identity Platform Database**. Centrify Identity Platform Database indicates that Centrify PAS is running on the LifeRaft database.

5. Copy the following scripts to the following directory: `C:\Program Files\Centrify\Centrify Identity Platform\scripts` on the computer you are upgrading:

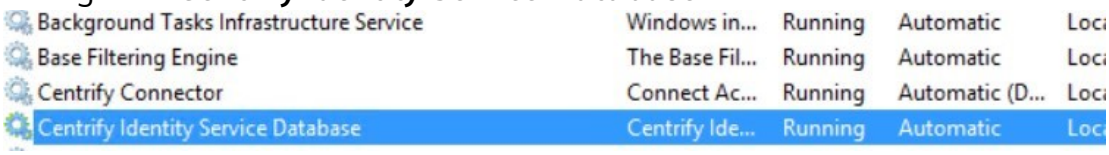
   - `upgrade_database_engine.ps1`
   - `make_primary.ps1`
   - `uninstall_connector.ps1`

   If you do not have the scripts, see Running required scripts for information on where you can download the scripts.

6. Right-click the script then run with PowerShell or open PowerShell and navigate to the scripts directory to run `upgrade_database_engine.ps1`. Be sure to be logged in as administrator.

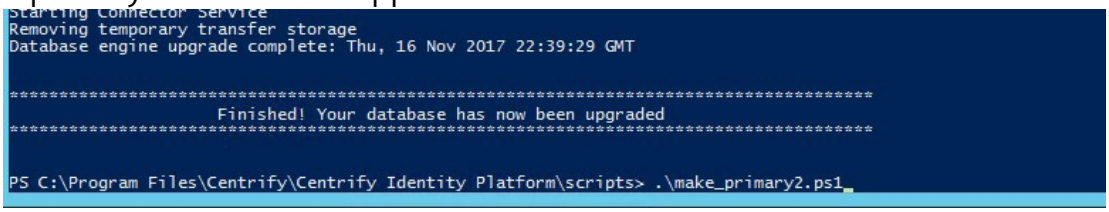


7. Enter Y to upgrade the database from LifeRaft to Postgres.
8. In the **Windows Task Manager** > **Services** tab verify that the service name changed to **Centrify Identity Service Database**.



Centrify Identity Service Database indicates that Centrify PAS is now running on the Postgres database. Although the Centrify PAS is running the Postgres database, it is still in standalone mode.

9. Run `make_primary.ps1` from the scripts directory to convert the node into a primary node for HA support.



10. At the prompt, select new folder for the service database, enter a location for the Centrify PAS Postgres database.

    Note: The location should be a shared storage location between primary and secondary nodes. Make sure the new location follows Centrify Centrify PAS's clustering prerequisites (review Prerequisites for more information).

11. Select a location to save the `clconf.zip` file (cluster configuration file). The file is used for cluster/recovery support and is typically saved in `\program files\centrify\centrify\identity\platform\config\clconf.zip`. The location where you save the file can be a local or shared location, however - it should not be the shared drive where the Centrify Centrify PAS Postgres DB is located.
12. Run the `uninstall_connector.ps1` script to uninstall the connector service.

    Note: In an HA environment, the connector cannot be installed on any of the HA nodes.

13. In **Admin Portal** > **Settings** > **Network**, select the connector you want to remove and then click **Delete** from the Actions menu to remove the connector.
14. Continue with the Centrify PAS cluster configuration to complete the following steps:
    - Install the Centrify PAS software on secondary nodes and create and configure the cluster using the Windows Failover Cluster Manager. Review sections: Install on secondary servers and Create and configure a cluster.
    - Install Centrify Connectors (you will need to install and configure new connectors onto computers that are not part of HA cluster).
    - Perform another backup of the primary node. Since you have a new database configuration, it is a good idea to perform another backup. Be sure to label it so that it is clear it is the backup with Postgres DB. The LifeRaft BD will no longer work. See Backing up and restoring Privileged Access Service for more information.

Troubleshooting and log information

For troubleshooting and log information, review the following:

- The log diagnostic information section of the *Centrify Privileged Access Service Installation and Configuration Guide for High Availability On-premises Deployment Guide*. Additionally, it instructs you on how to run the `capture_diagnostics.ps1 script.`
- The windows failover logs.

Debugging failover clustering issues

The following steps detail how to troubleshoot failover issues with the cluster.

Note: For additional information on cluster log related commands, see https://docs.microsoft.com/en-us/powershell/module/failoverclusters/get-clusterlog?view=win10-ps.

1. On the computer where the Centrify Centrify PAS is running on the primary node, open a PowerShell console window as Windows administrator.
2. At the prompt, issue the following commands to create log files with information regarding the current failover cluster:

```
Get-cluster > .\Clusterlist.txt
Get-clusterNode > .\ClusterNode.txt
Get-ClusterResource -Verbose > .\ClusterResource.txt
```

3. Enter the following command to change the default logging level for the size and level of detail captured in the cluster log (default is 3): `Set-clusterlog -Level 5`
4. Trigger a cluster failover using the Failover Cluster Manager to reproduce the failover issue.
5. At the prompt, issue the following commands to create a log file with cluster information after triggering a failover.

```
Get-ClusterResource -Verbose > .\ClusterResource_After.txt
```

6. Issue the following command to collect the cluster log:

```
Get-clusterlog -UseLocalTime -TimeSpan 20 -Destination .
```

Note: There is a full stop '.' at the end of the command. This command collects the last 20 minutes of cluster log files with the local timestamp and stores the files in the current directory.

7. Revert the logging level back to the default (default level is 3).

```
Set-clusterlog -Level 3
```

8. Upload the following files and send them to Centrify Support for further investigation.

- `Clusterlist.txt`
- `ClusterNode.txt`
- `ClusterResource.txt`
- `ClusterResource_After.txt`
- `<FQDN of cluster>_cluster.log`

Enabling certificate authentication by smart card and tenant CAs

The `setup_certauth.ps1` script is provided with the Centrify Privileged Access Service to enable certificate authentication when client certificates are issued by Centrify or by your own certificate authority.

After you execute `setup_certauth.ps1`, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page is enabled. In the Certificate Authorities page, you can configure authentication by

smart card and by certificates issued by your PKI infrastructure. If you do not execute `setup_certauth.ps1`, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page remains disabled, and is not visible.

Before you can execute `setup_certauth.ps1`, you must ensure that the following prerequisites are met:

- A CNAME record that points the DNS host to the Centrify PAS host has been created within your DNS infrastructure. After the CNAME record is created, it can take up to 15 minutes for the CNAME to resolve the IP addresses of the DNS host and the Centrify PAS host.
- A certificate from a trusted certificate authority has been issued for the DNS host. When the `setup_certauth.ps1` script runs, you will be prompted to specify the path to this certificate.

The `setup_certauth.ps1` script validates these prerequisites during runtime. If either prerequisite is not met, `setupcertauth.ps1` aborts.

To enable authentication by smart card and tenant CAs:

1. On the computer where the Centrify PAS is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the Centrify PAS `scripts` folder. The scripts folder is located in the installation folder that was specified during Centrify PAS installation. If the default installation location was selected, the `scripts` folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. From the `scripts` folder, run the `setup_certauth.ps1` script:

   ```
   .\setup_certauth.ps1
   ```
4. When the script prompts you to verify that the prerequisites are satisfied, type **Y** and press **Enter**.
5. The script validates prerequisites, and prompts you for the path to the DNS host certificate. Type the path to the certificate and press **Enter**.

When the script finishes, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page is enabled.