Centrify Privilege Service

Getting Started Guide

April 2015

Centrify Corporation

Legal notice

Contents

Getting started with Centrify Privilege Service

Welcome to the Centrify Identity Platform and Centrify Privilege Service. Centrify Privilege Service lets you securely store user name and password combinations for local **accounts**. You can then use those accounts to log on securely to the servers, switches, and routers you identify as **resources**.

To get here, you have most likely already completed a few key steps:

1 You have requested a free trial or subscription to the Centrify privilege service.

If you did not download this guide as part of a free trial or subscription, you should start by filling out the following form to request access to the Centrify privilege service:

http://www.centrify.com/free-trial/privilege-service-form/

2 You have registered for a Centrify account with a valid email address and have received an "Activate Your Centrify Account" email followed by a "Your Centrify Account Is Ready - Next Steps" email with your account details.

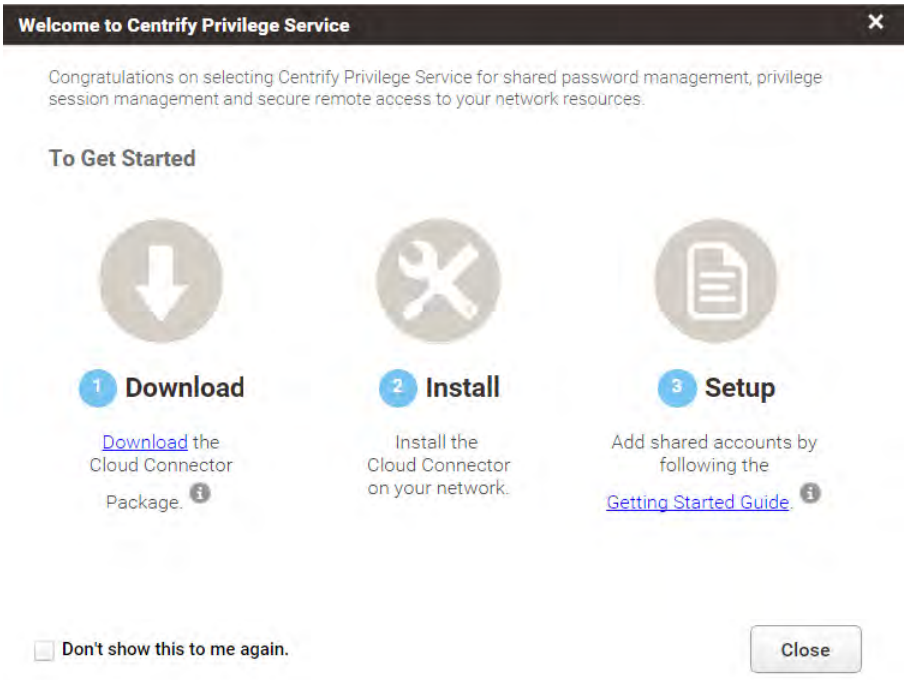
Your account details include the user name for an administrative account that is a member of the `sysadmin` role and a unique customer identifier. For example, your email might have account details similar to the following:

Centrify privilege service management:	https://cloud.centrify.com/resources
Your User Name:	admin_maya.garcia@centrifypubs.net
Your temporary password:	hKGo!wd2N (You'll be asked to change this when you log in)
Customer ID:	AAE0012

Members of the built-in `sysadmin` role have access to all Centrify cloud-based services and can grant access rights to other users.

3 You have logged on using your account details and set a new password for your administrative account.

Logging on displays the following welcome message:



If you have not completed these preliminary steps, stop here and verify that you have received the "Your Centrify Account Is Ready - Next Steps" email and that you can log on to the Centrify cloud with the account information in the email.

Add a cloud connector

The cloud connector is a multipurpose service that enables secure communication between your internal network and the Centrify cloud. The Centrify privilege service requires at least one cloud connector to be installed on your network inside of the firewall.

You can install more than one cloud connector for your organization to support fail-over and load balancing. You might also want to install more than one cloud connector if you are using multiple Centrify cloud-based services. In most cases, you should install two cloud connectors in a production environment.

To install a cloud connector on a domain computer

1 Click Download on the welcome page to download the cloud connector.

2 Open the file you downloaded.

If the User Account Control warning is displayed, click Yes to continue.

3 On the Welcome page, click Next.

4 Select I accept the terms of the license agreement, then click Next.

5 Select the components to install, then click Next.

By default, all components are selected. You must select Centrify Cloud Connector to use the Centrify privilege service. Other components are optional for the Centrify privilege service, but might be required if you want to use other cloud-based services.

6 Click Install.

7 Click Finish to open the cloud connector configuration wizard.

To configure the cloud connector

1 On the Welcome page, click Next.

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

3 Click Next unless you are using a web proxy server to connect to Centrify cloud-based services.

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

4 The configuration wizard performs several tests to ensure connectivity. If all of the tests are successful, click Next.

As the final step, the cloud connector registers your customer identifier with your tenant, then runs in the background as a Windows service.

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

6 Click the Cloud Connector tab to view or change any of the default settings.

7 Click Close.

Logging on after adding a cloud connector

After you have installed and configured at least one cloud connector, you can use either Cloud Manager or your default browser to log on to the Centrify cloud service.

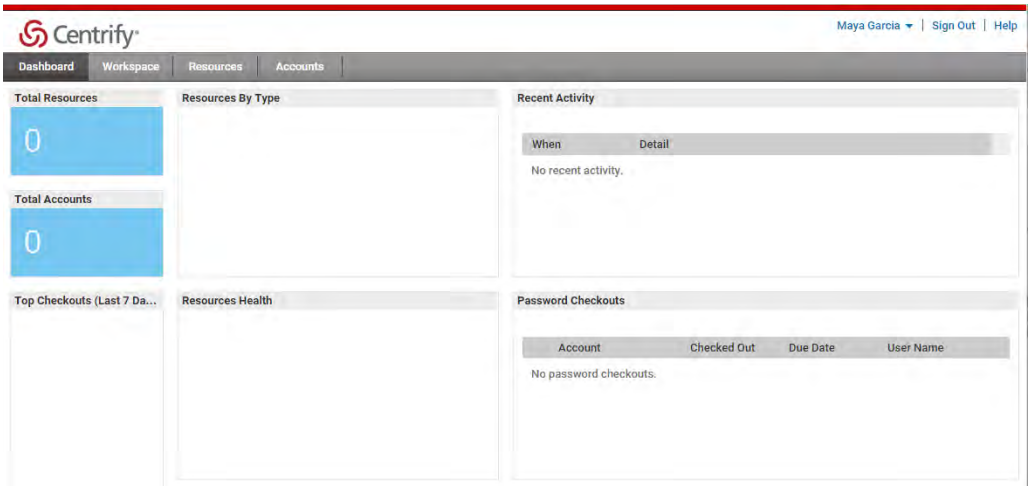
To log on

1 Go to the `cloud.centrify.com` URL.

2 Type the user name from your account details and the password you set when you activated the service.

3 On the welcome page, select Don't show this to me again, then click Close.

After you close the welcome page, you are in the **Privilege Manager** portal, where an empty dashboard is displayed.



If you happen to log on **before** you install and register a cloud connector, a reminder banner prompts you to download and install the cloud connector before continuing. For example:

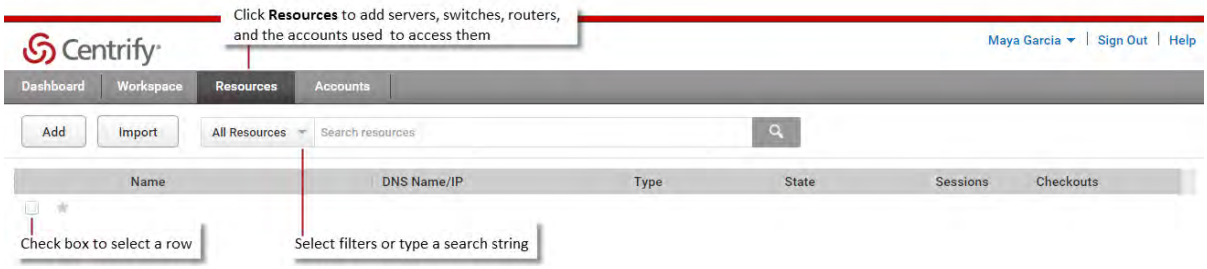
Quick tour

Across the top are the tabs you use to see and work with different kinds of information. For example, here you see the following tabs:

- Dashboard
- Workspace
- Resources
- Accounts

The dashboard tab is empty because you have yet to add any resources or accounts, so the first place you need to go after logging on is the Resources tab. The Resources tab is where

you add the resources—such as servers, workstations, switches, and routers—you want to manage and the local accounts you use to access those resources. The next step is to add resources, so click the Resources tab.



As you can see, the Resources tab is where you can click Add or Import to begin adding servers, switches, and routers. You can click Help for details about how to do that, but before you do, there are a few common motifs to notice here that you will also see on other tabs:

- Items are typically displayed as rows in a table.
- You can sort the items displayed by clicking the column headers.
- You can select filters or type a search string to change the information included in the table.
- You can click any row to drill down into details about an item.
- You can click the check box for a row and view an item's details to activate an Actions menu with a list of selection-appropriate actions you can take.

Adding a resource and account

Now that you are familiar with the basic navigation between tabs and working with the items listed in tables, the next step is to add a resource and account you want to manage. To illustrate the process, click Add and follow the steps in the wizard to add a single resource and account.

Here is a summary of what you'll do. If you need more information about any step, click Help, then open Managing resources and Adding a single resource.

To add a resource

1. Click Add to open the Add Resource Wizard.
2. Type a unique name, the DNS host name or IP address, and select the resource type—UNIX, Windows, or Generic SSH—for the resource you want to add, then click Next to continue.

3 Type a user name and password for an account to be used with the resource, then click Next to continue.

The accounts you add for different resources might include shared accounts for which you want to manage passwords and any other local accounts you want to make available through the privilege service. For example, you might want to include accounts for which you don't want the password changed but do want to make available for password lookups or login requests from outside of the firewall.

If you used a fully-qualified domain name for the resource, you should use the *domain**username* format for the account. If you used an IP address for the resource, you should use the *IPaddress**username* format for the account.

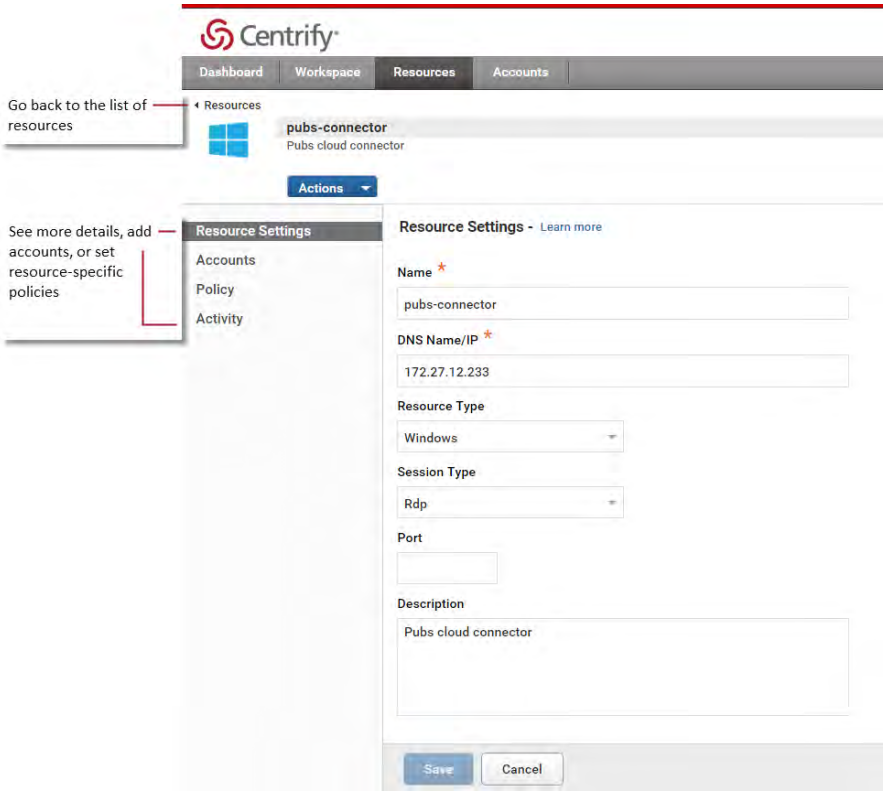
4 If you selected UNIX as the resource type and added `root` as the account to use with the server, you are prompted to specify whether the `root` user account is allowed to log on using secure shell (`ssh`) connections.

- Select **Yes** if the `root` user account can log on using secure shell (`ssh`) connections, then click Next to continue.
- Select **No** if you have configured `ssh` to prevent the `root` user account from logging on using secure shell connections. If you select No, you must add a user name and password for a "proxy" account that can open a secure shell connection on the target resource. After you specify an account to be used as the "proxy" for the `root` account, click Next to continue.

5 Select Verify Resource Settings to test access to the resource using the account information provided, then click Finish.

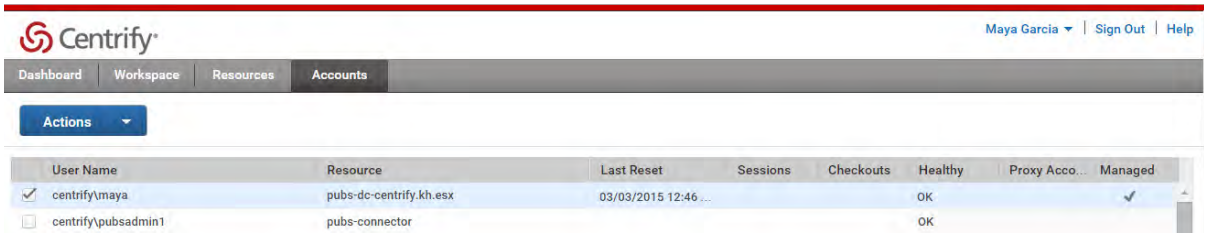
Viewing resource and account details

After you have added at least one resource, you can click in the row for the resource to display its details. For example:



Selecting actions for a resource

The Actions menu you see in the resource details is the same menu you can display by selecting the row using the check box. For example:



From the Actions menu, you can click:

- Account Actions to select an account and an action—such as Checkout to see the password or Login to log on to the target resource using the stored account password—that is specific to that account.

- Manual Login to log on to the target resource using a user name and password of your choice.
- Delete to remove a target resource from the list.

Viewing and modifying resource-specific details

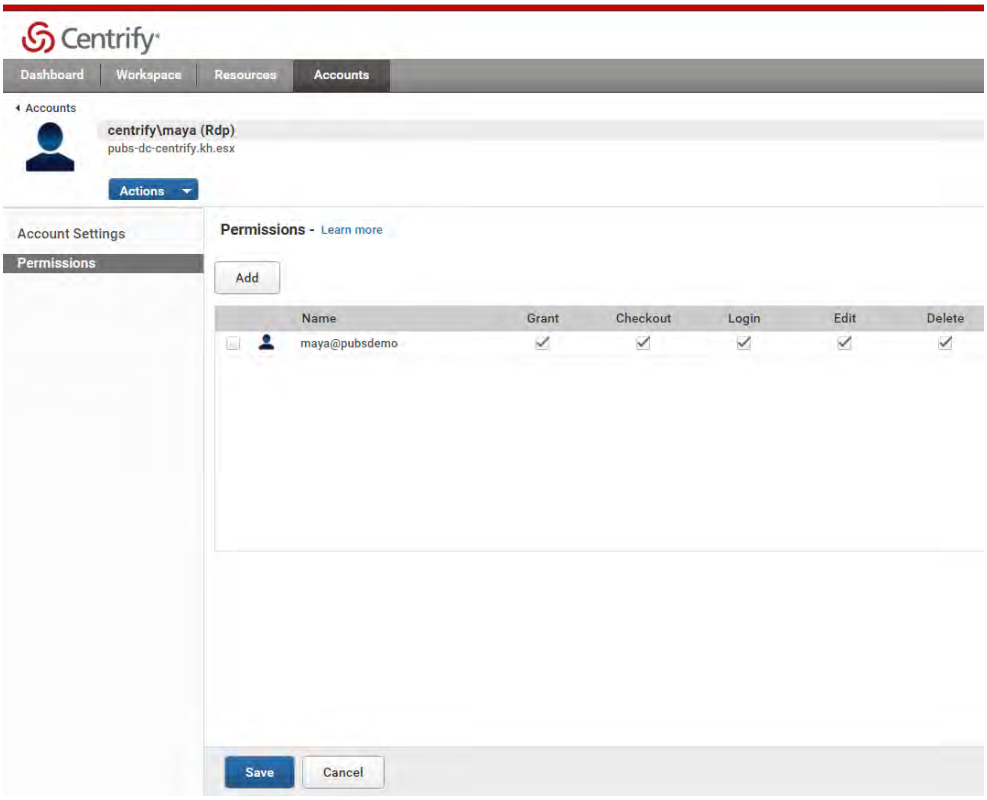
When you are viewing the details for a target resource, you can set or change resource-specific information. From the resource details, you can click:

- Resource Settings to change basic information—such as the type of resource or the port to use for remote sessions—about the resource.
- Accounts to add or view accounts to use for the resource.
- Policy to set resource-specific policies—such password checkout lifetime or remote access policy—for the resource.
- Activity to see recent activity—such as password checkout or login activity—for the resource.

Viewing account details and permissions

After you add resources and accounts from the Resources tab, you can click the Accounts tab to see account information for all resources listed in a table. Selecting a row using the check box displays the Actions menu for accounts.

As with Resources, you can click an account to see its details and edit the information or set permissions. For example:



Checking out and checking in passwords

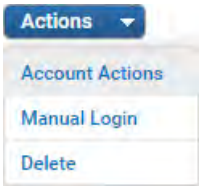
There are several different ways to get to common account and resource tasks depending on where you are. For example, you might click Account Actions on the Actions menu to select a task if you are viewing resource details or a select a task directly from the Actions menu if you are viewing an account. The most common tasks—Checkout, Checkin, Login, and Delete—are essentially the same whether you are working with resources or accounts, but how you get to them can vary.

Here's a summary of what you'll do to check out and check in passwords if you are starting from the Resources tab. If you need more information about any step, click Help, then open Managing resources and the task of interest.

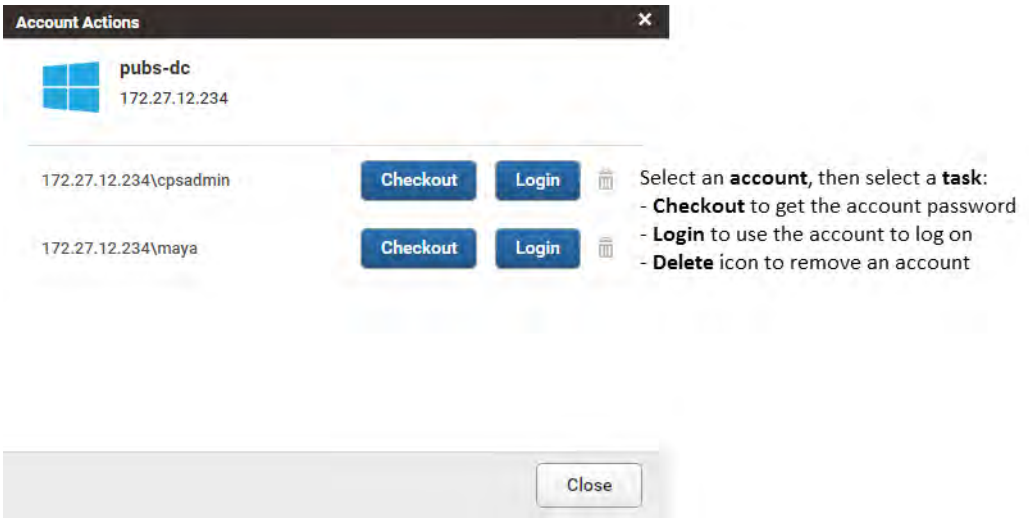
To check out and check in the password for a resource

1 Select a target resource.

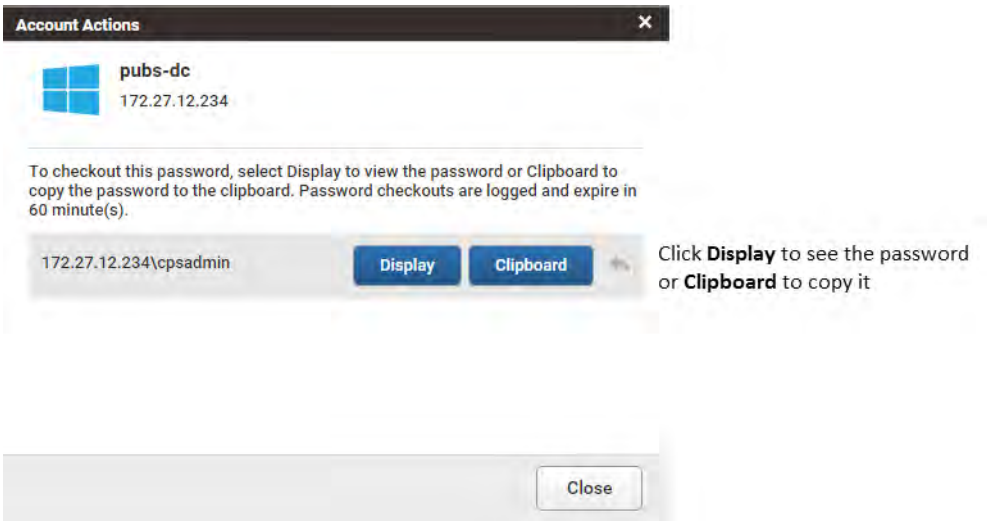
2 Click the Actions menu, then select **Account Actions**.



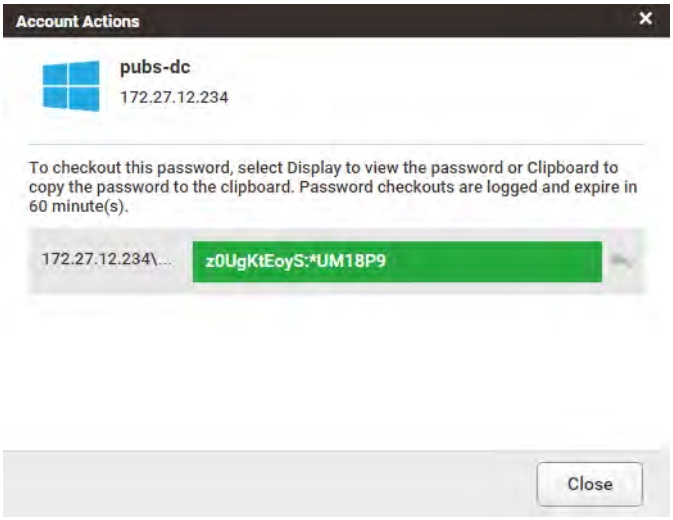
3 Find the appropriate account from the list of accounts for the select resource, then click **Checkout**.



4 Click **Display** if you want to view the password for the selected account as plain text or click **Clipboard** to copy the password without viewing it.



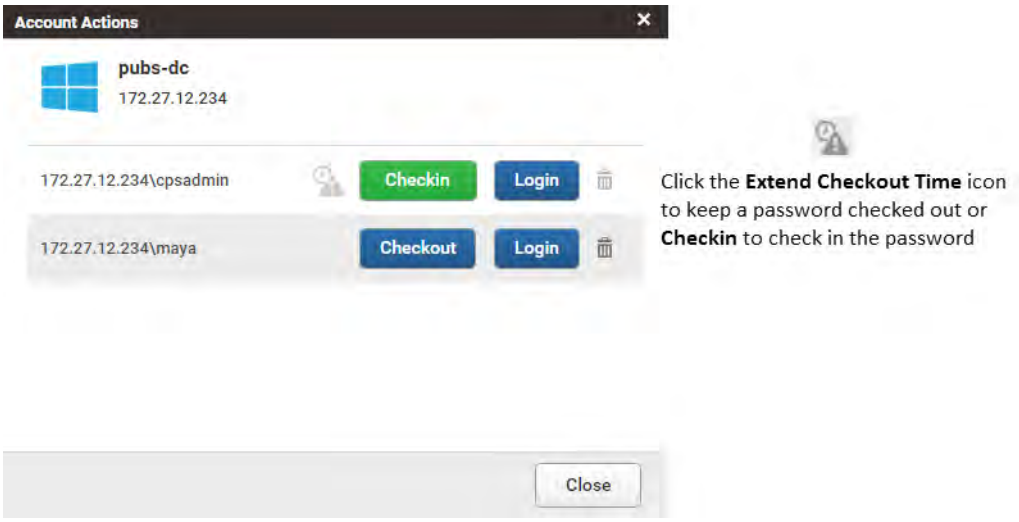
If you click Display and the password for the account is managed by the Centrify privilege service, you might see something like this:



The checkout is recorded as recent activity in the dashboard, in your workspace, and in the list of resource activity.

5 Click **Close**.

If you return to the Account Actions, you now have different actions available. For example:

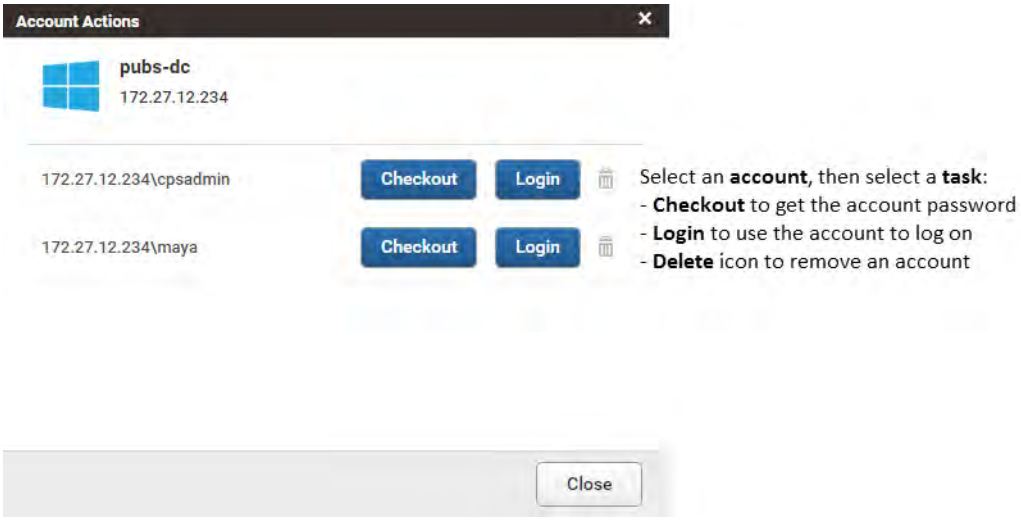


6 When you are finished using the account, you can select Account Actions, click Checkin, then click Close.

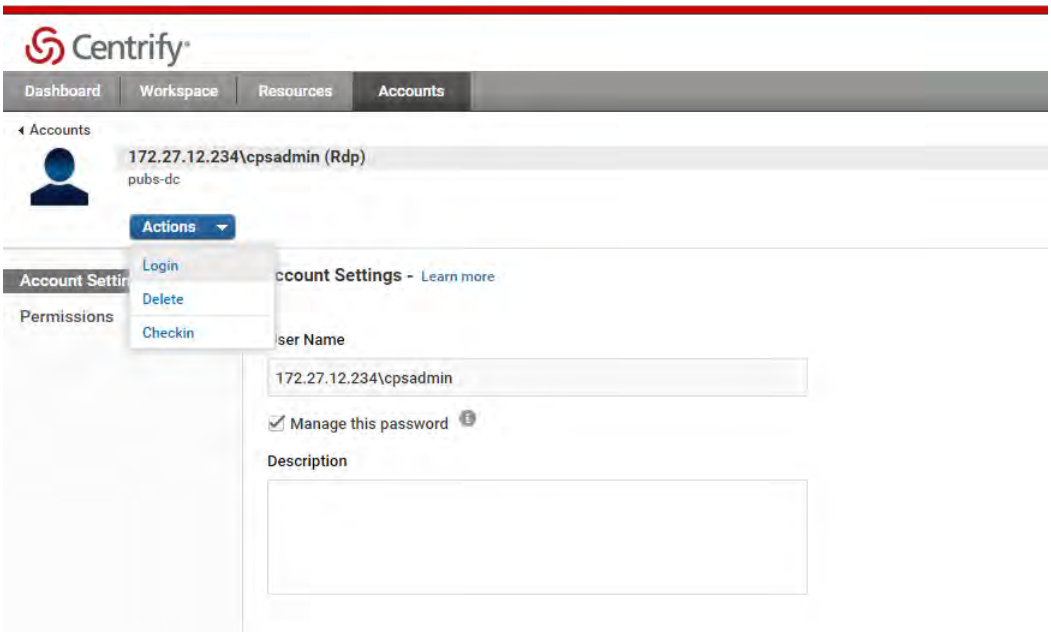
If you don't extend the checkout time or check the password in before it expires, at the end of the checkout lifetime, the password is automatically checked back in.

Logging on using a stored account name and password

Like the Checkout and Checkin tasks, there are several ways to get to the Login task to log on to a target resource using stored account information. For example, you might click Login in the Account Actions for a resource:



Alternatively, you might select Login directly from the Actions menu if you are viewing an account. For example:



Starting a session on a target resource

If you want to log on to a target resource you have added to the Centrify privilege service, you have a few different options. For example, you can:

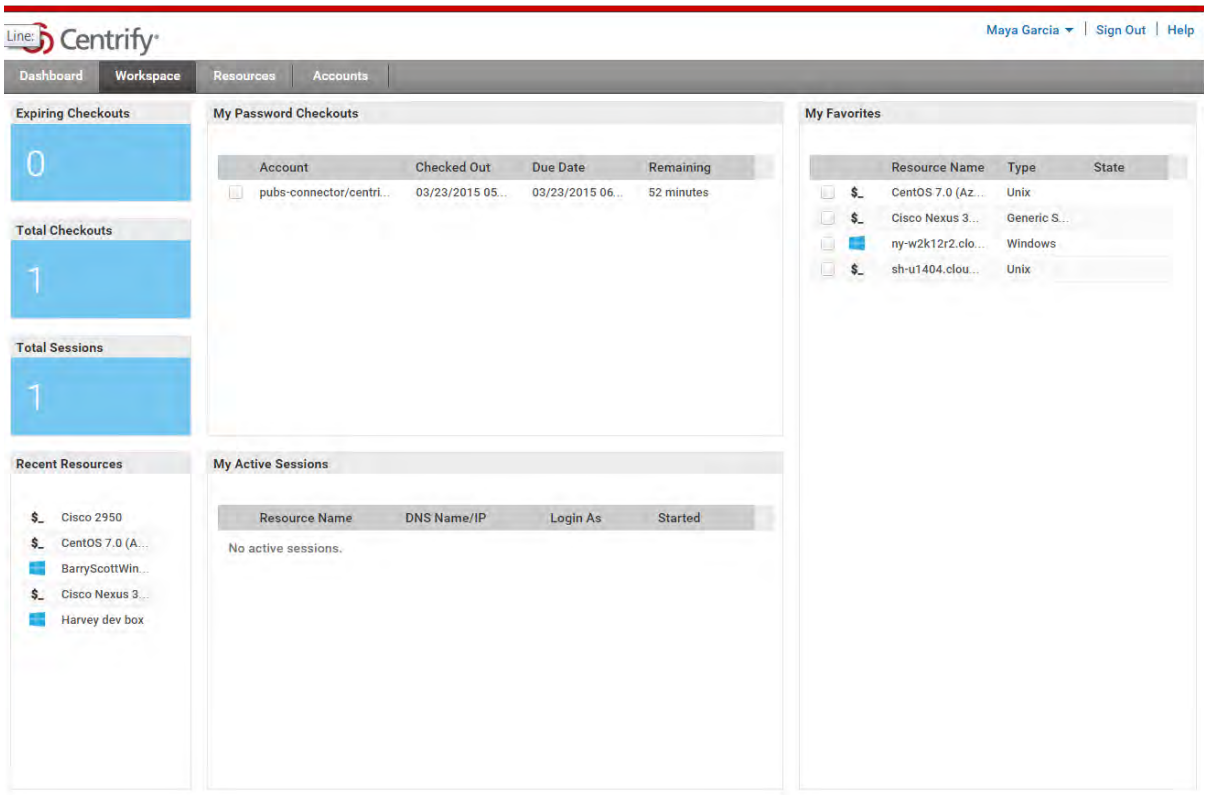
- Log on using stored the account information you have added for the resource without knowing the account password.
- Get the password for an account you have added for the resource so you can log on when you don't know the password or after the password has been changed.
- Log on manually using any valid user name and password without using information stored in the Centrify privilege service.

Logging on using stored account information or manually with a user name and password opens a secure shell or remote desktop session on the target resource. The password and login activity is recorded and can be viewed in the resource details, your workspace, and the dashboard.

Using the dashboard and workspace

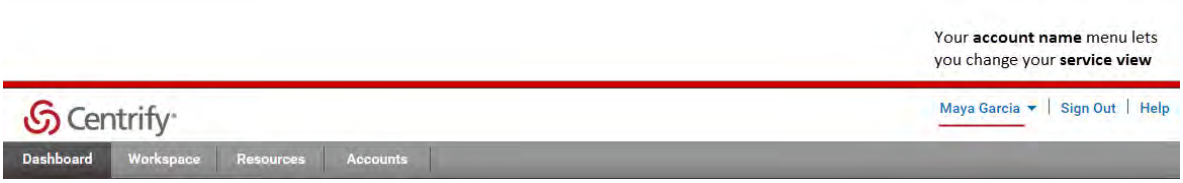
The dashboard provides an overview of all of the activity taking place in the Centrify privilege service for your organization. It provides a summary of what everyone is doing. The workspace provides a focused view with a summary of your current and recent activity.

After you have checked out passwords, logged on to resources, selected favorites, you can click the Workspace tab to view your current and recent activity and the status of the passwords you have checked out and any open sessions.



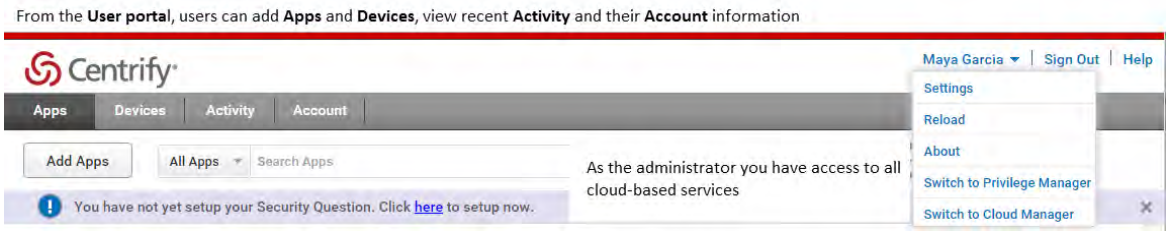
Switching between services and portals

The Centrify privilege service gives access to multiple services. You can switch from one service to another by clicking on your account name menu.



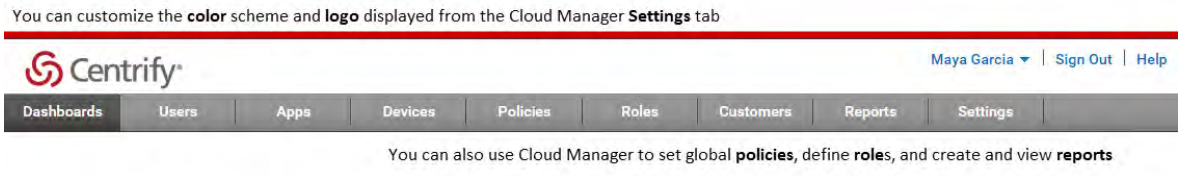
From the account name menu, you can switch between services. For example, if you are currently using the Privilege Manager portal, you can use the account name menu to switch to the User Portal or Cloud Manager administrative portal:

When you change from one service to another, the tabs displayed across the top banner change to reflect the types of tasks you can perform. If you use your account name menu to switch to User Portal or Cloud Manager, you see a different set of tabs displayed in the top banner. For example, if you switch to the User Portal, you see the Apps, Devices, Activity, and Account tabs:



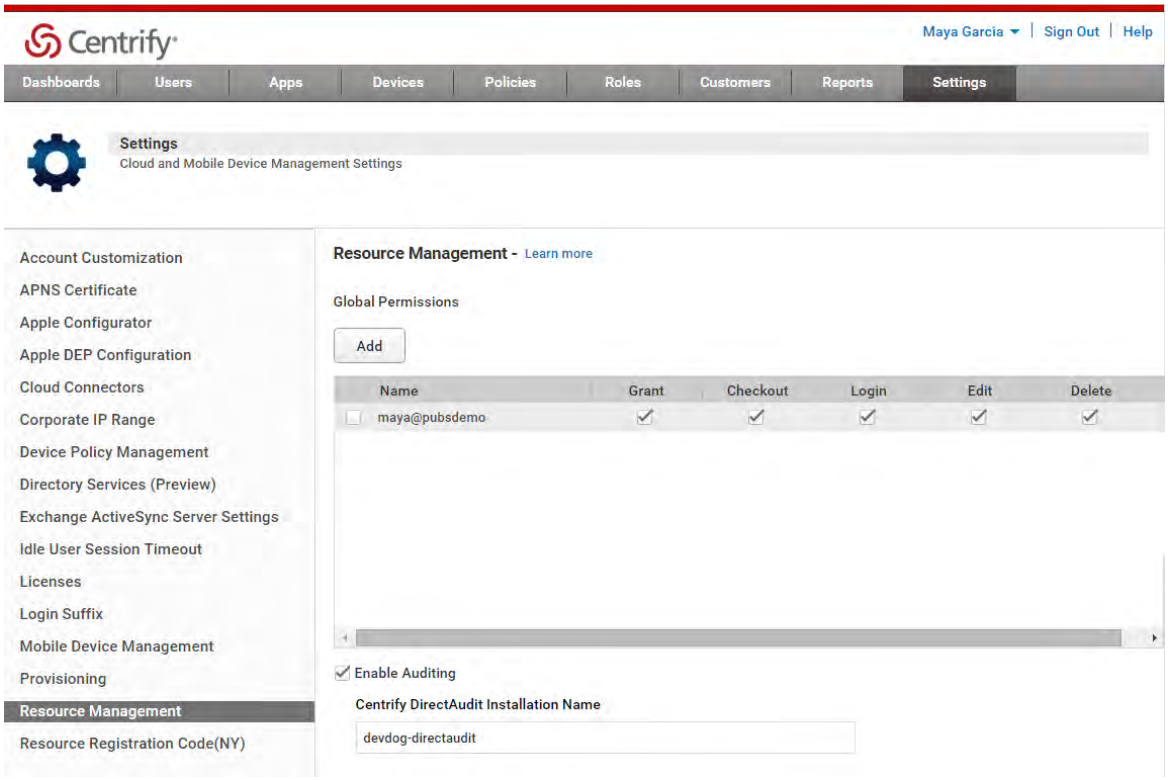
Cloud Manager is the primary administrative interface for all Centrify cloud-based services, and initially it is only available to members of the `sysadmin` role. You use Cloud Manager when you want to define global settings, such as the color scheme and logo displayed in the browser.

After you use the account name menu to switch to Cloud Manager, you see the Centrify identity service welcome page, where you have the option to Skip or Start the Wizard. If you want to proceed without configuring information for the Centrify identity service, select Don't show this to me again, then click Skip. After clicking Skip, the default Getting Started dashboard is displayed in Cloud Manager and you see a different set of tabs displayed in the top banner. For example:



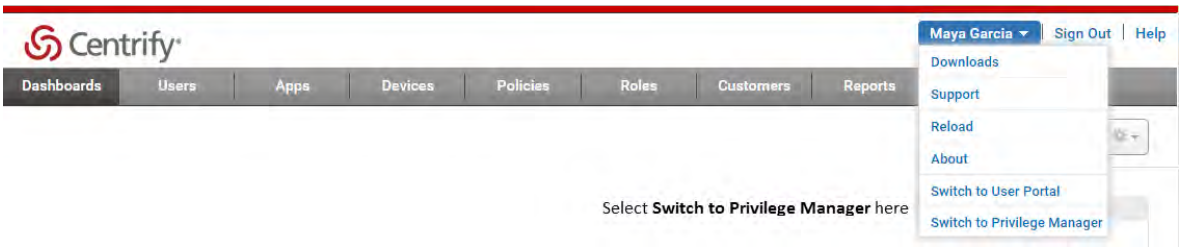
You can follow the steps listed in the Getting Started dashboard to begin adding users and creating roles. For Centrify privilege service, you are going to use the following Cloud Manager tabs:

- Policies to set global Resource Management policies that apply across all resources.
- Roles to set Privilege Management rights.
- Settings to add cloud connectors, to define global permissions for users that apply across all resources, and to enable auditing if you are using Centrify Server Suite, Enterprise Edition.



After you have added more resources and accounts, you also use Cloud Manager Reports tab to generate built-in or custom reports.

When you are done working in Cloud Manager, you can open the account name menu and select Switch to Privilege Manager. For example:



Now that you have an overview of where to find different types of information for resources and accounts and how to navigate between services and portals, you are ready to explore Privilege Manager in more detail. For more information about performing tasks in Privilege Manager, click Help or Learn More.

Auditing session activity

Centrify privilege service records audit trail events for all password check out and check in and login activity involving the resources and accounts you add. If you have Centrify Server Suite Enterprise Edition, you can also audit session activity on target resources. For example, you can capture all of the desktop activity on target Windows computers when you open a remote desktop connection or all command-line activity on target Linux and UNIX computers when you start a secure shell session.

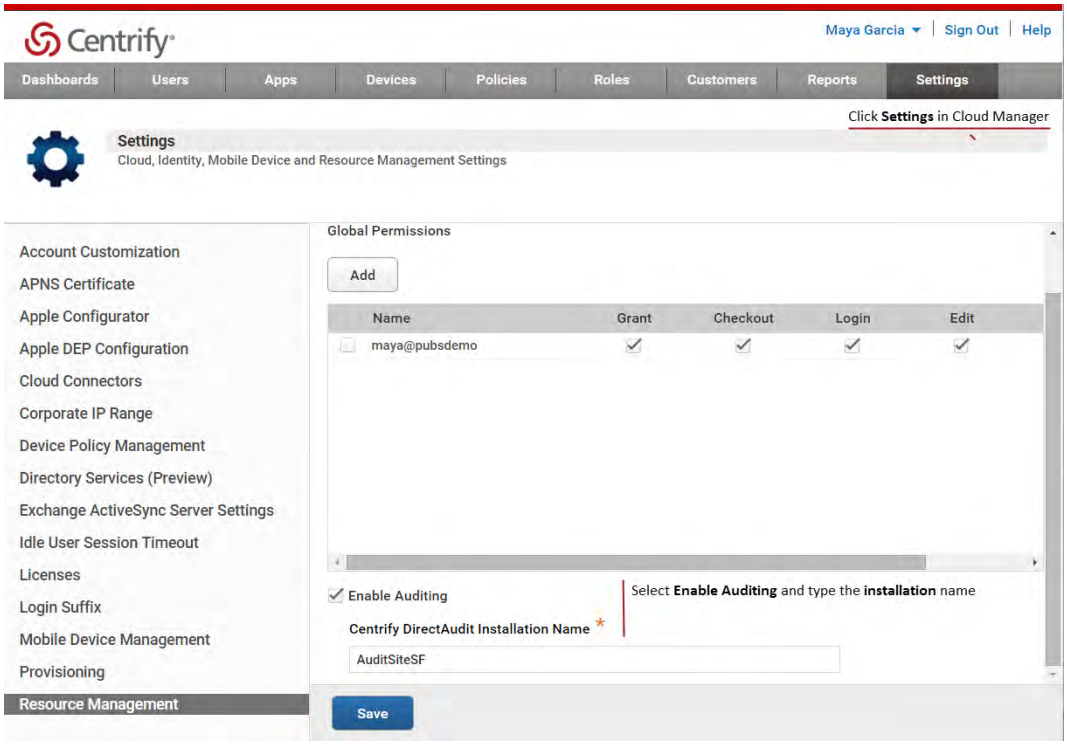
If you currently have an audit installation, you simply need to enable auditing and specify the name of the installation to have the cloud connector send session activity directly to a collector and have it stored in an audit store database. If you don't have an audit installation and want to create one, you can download Centrify Server Suite Enterprise Edition from the Customer Support Portal on the Centrify website, then follow the instructions in the *Auditing with Centrify Server Suite Administrator's Guide* to set up a working environment.

If you have created an audit installation and verified you have a working environment, you can use Cloud Manager to enable auditing and specify the installation name for the resources you manage.

To enable auditing

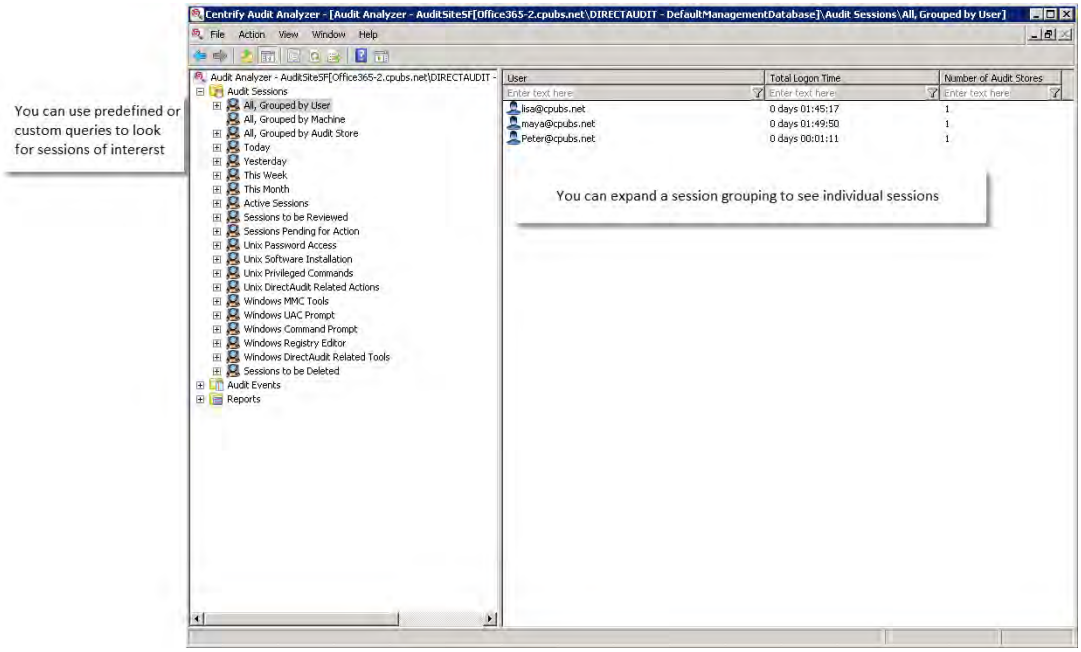
1. Select **Switch to Cloud Manager** from the account name menu.
2. Click the Settings tab.
3. Select Resource Management from the list of settings.
4. Select Enable Auditing and type the name of the audit installation if you want to audit user activity on the resources you manage.
5. Click Save.

For example:



Because the cloud connector captures the session activity, you don't need to install an agent on the target resources. You must have the other components required for a functioning audit installation, but the agent is optional. You might want to install an agent on some or all target resources if you want to capture activity in sessions started interactively on those resources rather than through a remote desktop or secure shell connection from the privilege service.

After you have captured some activity, you can query, replay, and review the sessions you have stored in an audit database using Audit Analyzer.



Depending on the type of session, replaying the session might display desktop activity or command-line activity, For example, if you captured a remote desktop session starting on a target resource, replaying the session might look like this: