Introduction to Centrify Privilege Service

Centrify Privilege Service is a cloud-based password and access management system for servers and network infrastructure deployed on-premises and in the cloud. Centrify Privilege Service is delivered as a Software-as-a-Service (SaaS) solution. It is built on the Centrify identity platform, which is the underlying Identity-as-a-Service (IDaaS) platform that powers all of Centrify's cloud-based products and services.

Centrify Privilege Service and Centrify Server Suite are the foundation products of Centrify's privileged identity management solution for privileged users and IT resources. Centrify Privilege Service enables you to manage account passwords and access rules for the shared accounts that can log on and correct issues on target resources, such remote servers and network devices, inside or outside of a firewall. Logging on to the service, opens the Privilege Manager portal in your browser, enabling you to manage and access the resources and accounts you add to the service.

All Centrify cloud-based products and services rely on the cloud connectors you install and configure for your organization. The cloud connector acts as a gateway between your internal network and the Centrify cloud-based services you use. At least one cloud connector is required if you are connecting Active Directory domains on your internal network to Centrify services hosted on the Internet. In addition, Centrify Privilege Service requires one or more cloud connectors to enable the network connections to IT resources. Multiple cloud connectors can be installed to support fail-over and load balancing.

This chapter introduces the basic deployment architecture and provides examples of common use-cases for Centrify Privilege Service. For information about installing and configuring cloud connectors, see Getting started with Centrify privilege service or Installing Centrify cloud connectors and administrator consoles in the Cloud Manager help.

The following topics are covered:

What Privilege Manager provides

Through Centrify Privilege Manager, you can securely store, share, and manage administrative passwords from any computer or tablet with a browser and an account that is registered for access to the Centrify identity platform and cloud-based services.

By using Centrify Privilege Manager to manage administrative and shared account passwords, you can securely store encrypted passwords and control how frequently they are reset. By adding accounts with managed passwords and only granting specific privileges, you can share common accounts without members of different work groups knowing administrative account passwords.

Using the stored account information, administrators with the proper permissions can log on transparently without providing a password and open remote sessions on target servers and network devices to perform everyday tasks, diagnose problems, or fix issues. In addition, by requiring users to check out and check in stored passwords when they are not logging on transparently, you can prevent the reuse of shared account passwords for administrative activity.

Privilege Manager keeps a record of password checkout, checkin, and session activity, so you always know who had access to which resource when. If you also have Centrify Server Suite Enterprise Edition and have set up an audit installation, you can capture a complete audit trail of what administrators did after starting a remote session on a targeted resource. For information about how to create an audit installation to capture and replay session activity, see the *Auditing with Centrify Server Suite Administrator's Guide*. For information about configuring a cloud connector to enable auditing for the Centrify privilege service, see "Enabling auditing for sessions on target resources" on page 48.

Why managing privileged accounts is important

There are several key reasons your organization can benefit from using the Centrify cloud service to manage privileged accounts and access to remote servers and network devices. By using the Centrify cloud service to manage privileged accounts and access to servers, you can:

- Improve your overall operational security by limiting access to accounts with administrative privileges.
- Provide access to administrative operations without sharing privileged account passwords
- Log all password checkout, check-in, and reset activity.
- Change the password stored automatically after a viewed or copied password is checked in to prevent reuse.
- Enforce password complexity by generating passwords that cannot be guessed and that only the service knows.
- Provide remote access to servers and network devices through a secure channel.

Connecting to servers and network devices

With Centrify Privilege Manager, you can securely store user name and password combinations (accounts). You can then use those accounts to connect interactively to servers, switches, and routers (resources). You can also choose who is authorized to use the accounts on which resources and who is authorized to view or copy the account password.

The resources you manage might include servers and network devices inside of your organization's firewall, outside of the firewall, or a combination of the two. For example, you might have some users who can log on to specific resources inside of the firewall and others who can access specific resources located outside of the firewall.

In the most common scenario, you would add shared local accounts—such as `root`, `patrol`, or `oracle`—for the resources you add to the Centrify privilege service. You would also specify which users are allowed to use those accounts and what different users are allowed to do. For example, you can specify which users can connect using a given account without having to specify the password for the account.

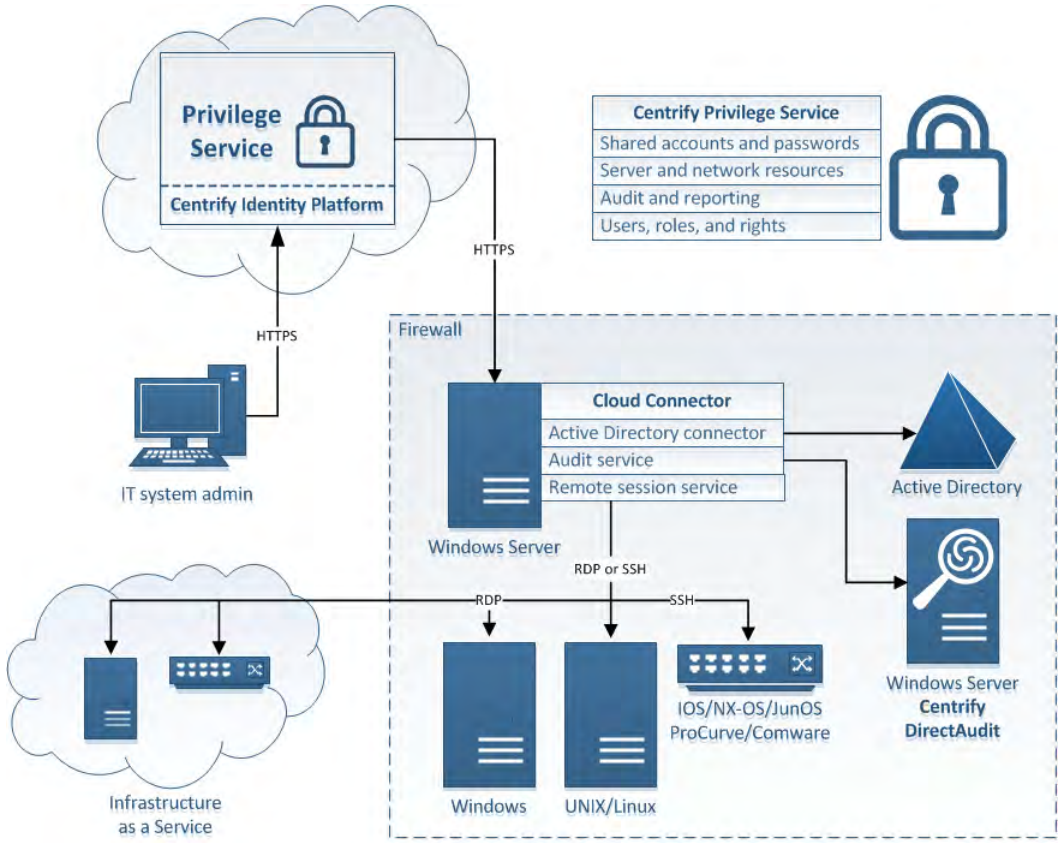
Using managed or unmanaged accounts

If you use secure shell or remote desktop connections for a resource, the session is connected from the administrator's workstation—either inside or outside of the firewall—to the Centrify privilege service through the cloud connector to the target resource. The account used to connect to the resource can be either a **managed account**, that is, an account with the password automatically changed by the Centrify privilege service, or an **unmanaged account** with a password that is stored by the Centrify privilege service but not changed. In either case, the Centrify privilege service can retrieve the password programmatically without revealing it, so that administrators can use the account without knowing the password being used.

Auditing sessions on target resources

All of the administrative activity that takes place through the Centrify privilege service is audited and stored in the cloud. In addition, if you have installed Centrify Server Suite Enterprise Edition and have an audit installation established, the administrator's activity on the target resource during a secure shell or remote desktop session can also be collected and stored in an audit database for further review and analysis.

The following diagram illustrates the deployment of the password management features provided by the Centrify privilege service and Privilege Manager.



The diagram illustrates the basic deployment model with only one cloud connector. In practice, however, most organizations would deploy at least two cloud connectors inside of the firewall for fault tolerance.

Checking out managed account passwords

If you are authorized to check out passwords, you can retrieve the password for an account to enable you to log on to a target resource. After you retrieve the password, it can remain checked out for a configurable period of time. What happens at the end of the allowed checkout period depends on whether the account password is managed by the Centrify privilege service or unmanaged.

If the password is a managed account password, the password you retrieved expires at the end of the checkout period and the Centrify privilege service automatically generates a new password for the account. If you check in the password before the end of the checkout period, the checkin also automatically generates a new password for the account. You can use policies to configure the maximum number of minutes a password can be checked out and whether multiple administrators can have a password checked out at the same time. You

can also extend the password checkout time for a currently checked out password if you need more time to complete your work. With a managed account password, however, the only valid password is the one known and updated by the Centrify privilege service.

Getting started

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**.

Registering for service

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.

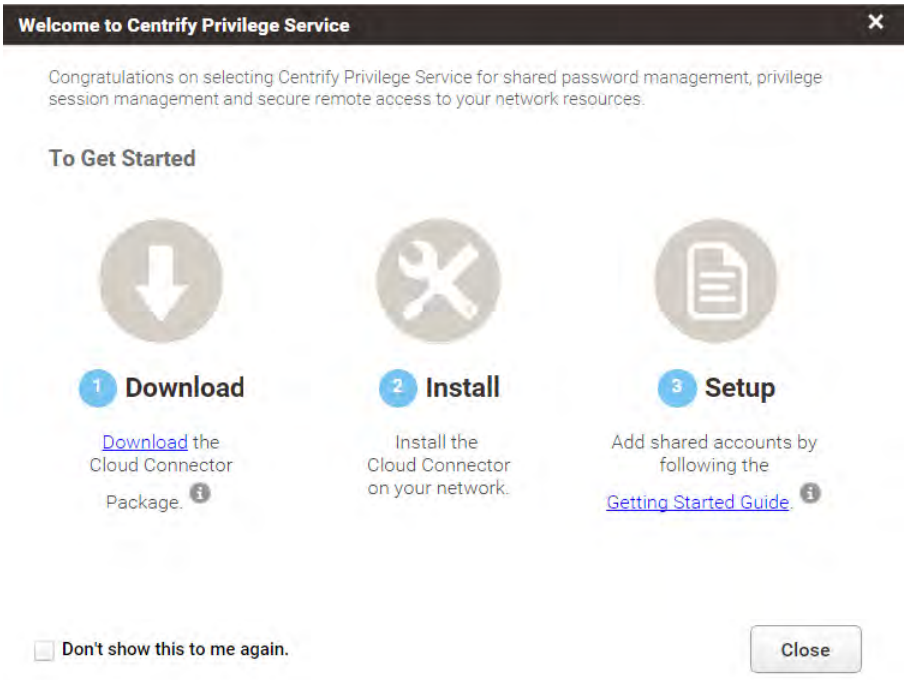
Your account details include the user name for an administrative account that is a member of the `sysadmin` role and a unique customer identifier. For example, your email might have account details similar to the following:

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.

Adding 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.

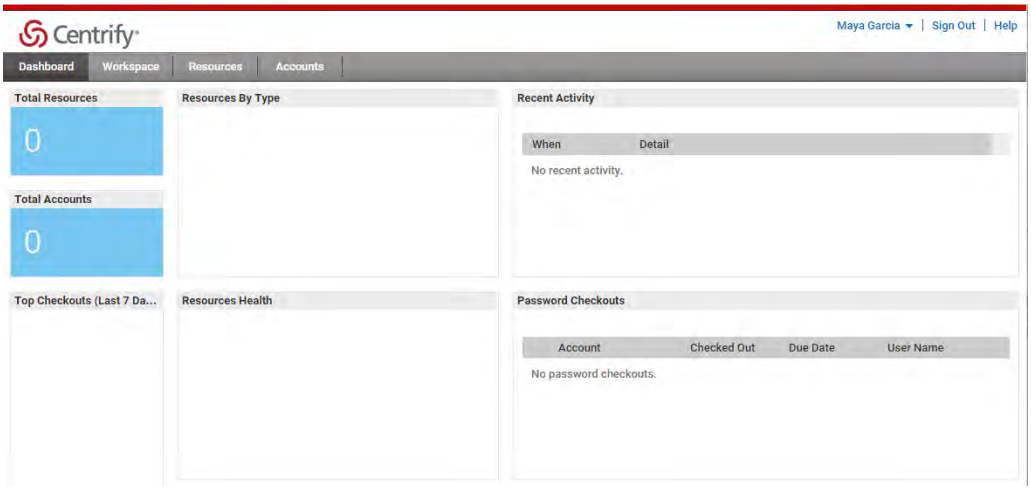
5 Click Finish to complete the configuration and open the cloud connector configuration panel, which displays the status of the connection and your customer ID.

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

7 Click Close.

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. The next time you log on and see 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:

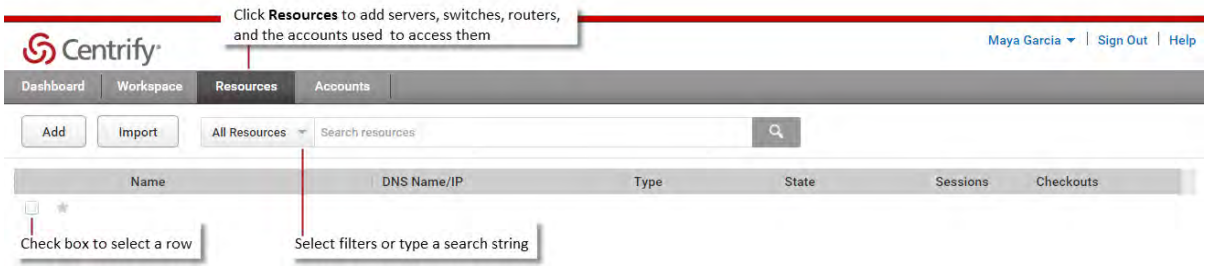
Quick tour

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.

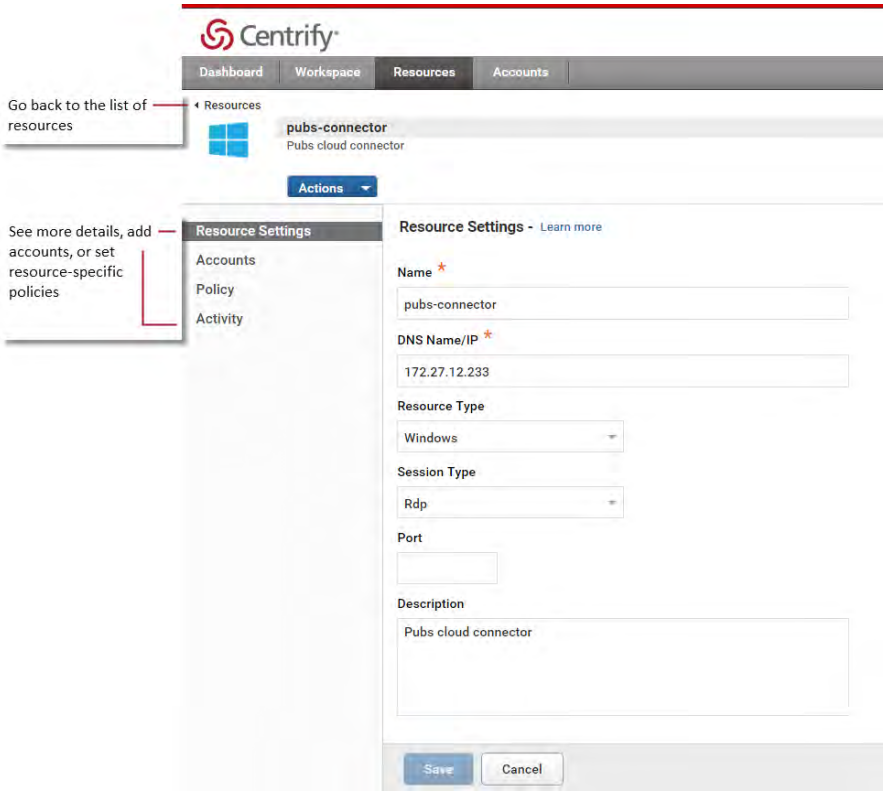


As you can see, the Resources tab is where you can click Add or Import to begin adding servers, switches, and routers. You can click Help for details about how to do that, but before you do, there are a few common motifs to notice here that you will also see on other tabs:

- 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.

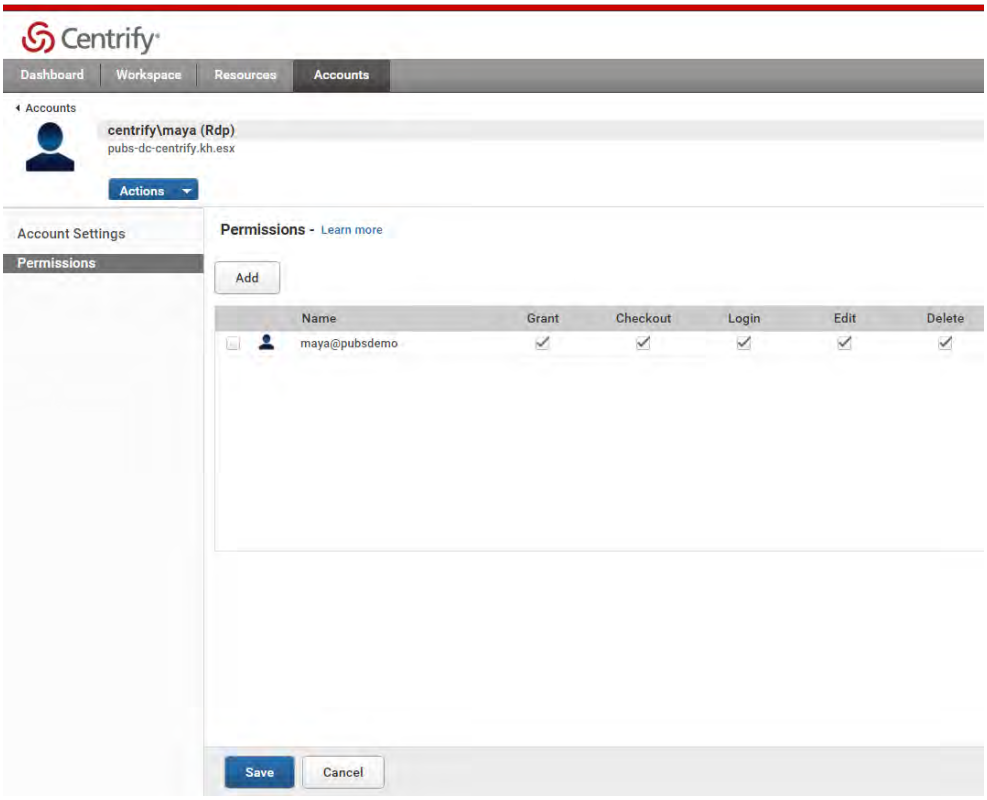
Viewing resource and account details

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



The Actions menu you see in the resource or account details is the same menu you can display by selecting a row using the check box. When you are viewing the details for a target resource or account, you can also set or change resource-specific or account-specific information.

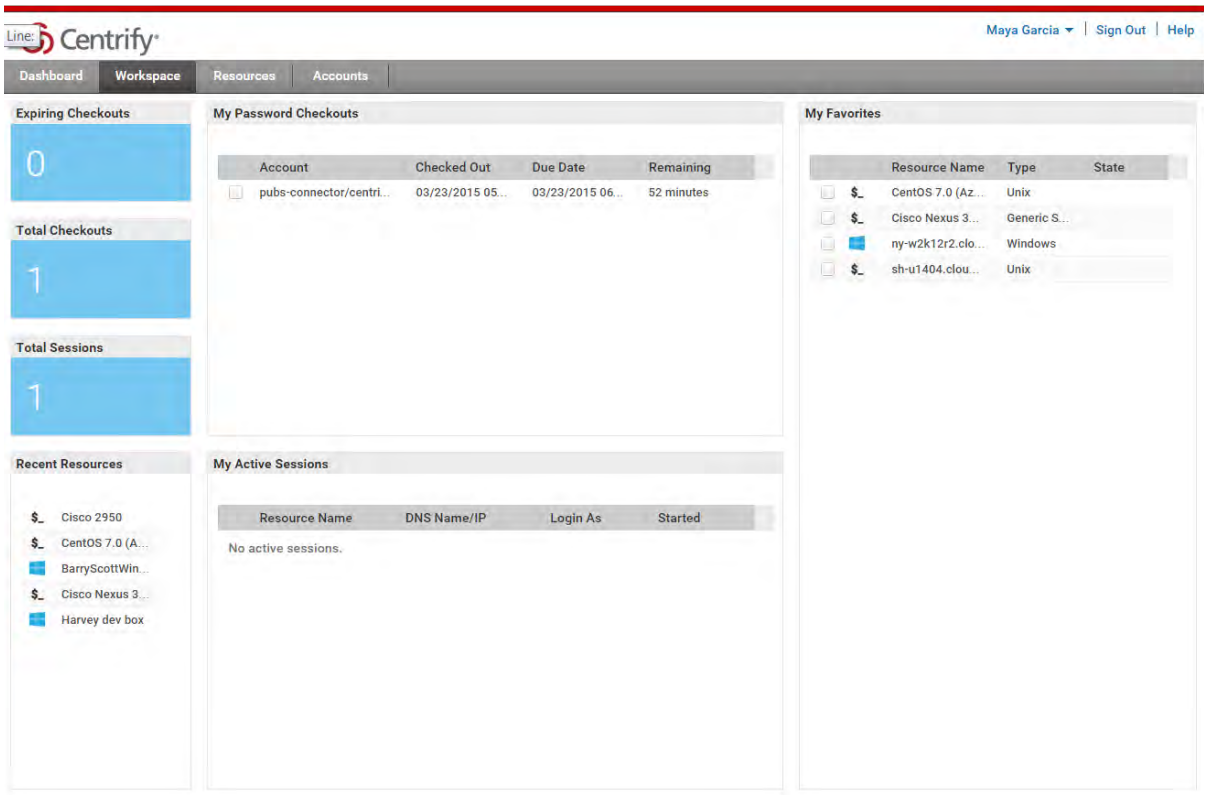
For example, as with Resources, you can click an account to see its details and edit the information or set permissions.



Using the dashboard and workspace

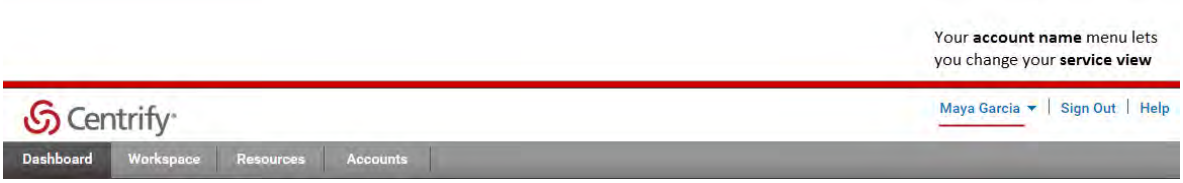
The dashboard provides an overview of all of the activity taking place in the Centrify privilege service for your organization. It provides a summary of what everyone is doing. The workspace provides a focused view with a summary of your current and recent activity.

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.



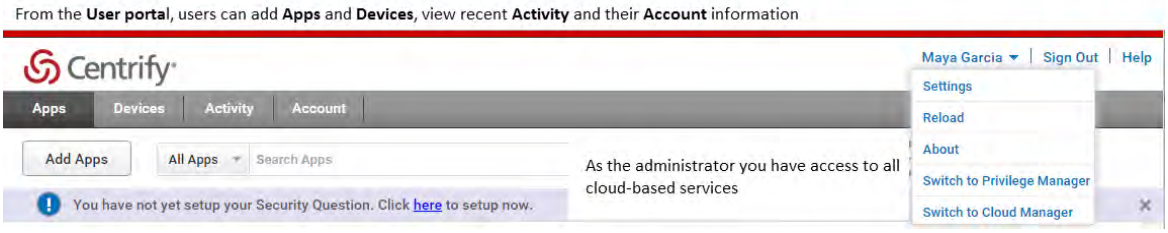
Switching between services and portals

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



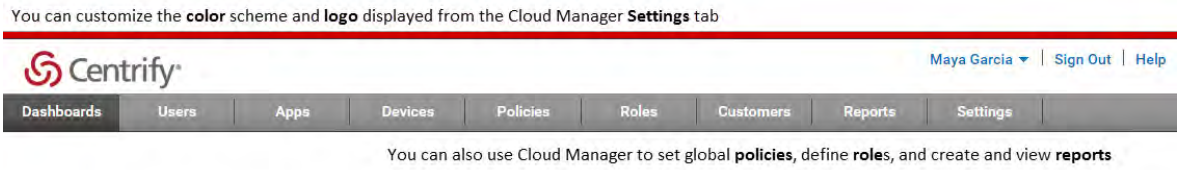
From the account name menu, you can switch between services. For example, if you are currently using the Privilege Manager portal, you can use the account name menu to switch to the User Portal or Cloud Manager administrative portal:

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:



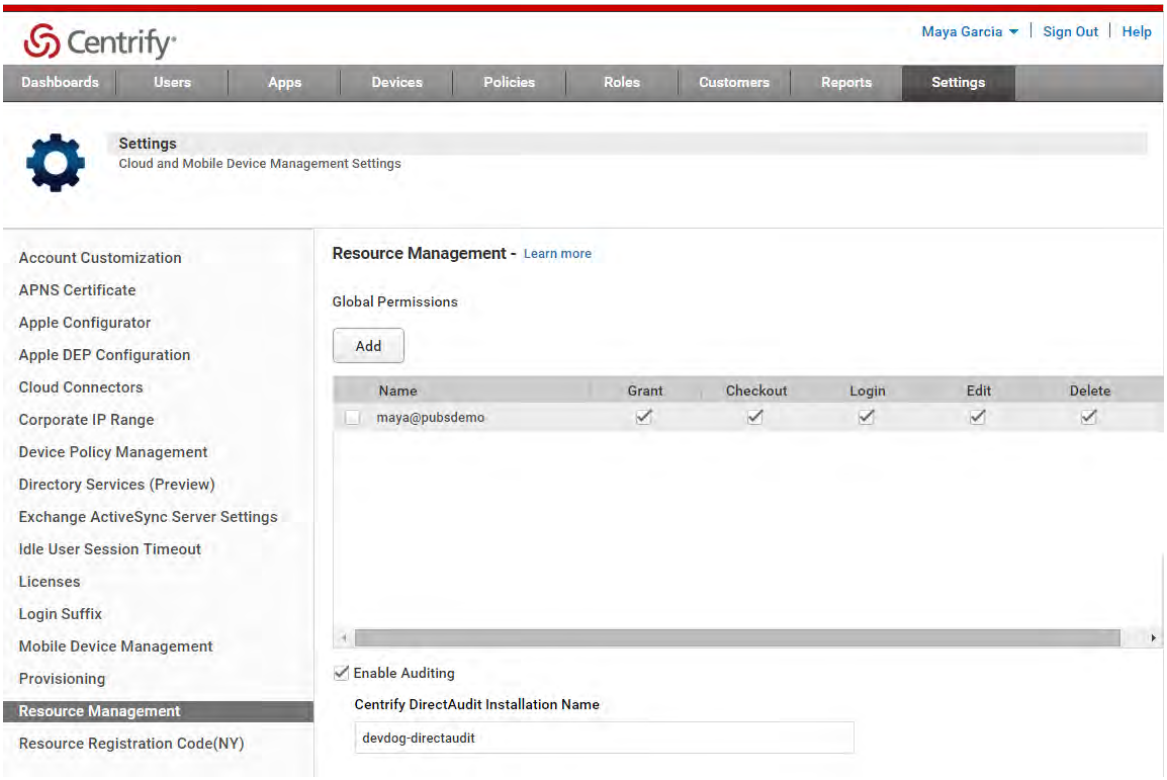
Cloud Manager is the primary administrative interface for all Centrify cloud-based services, and initially it is only available to members of the `sysadmin` role. You use Cloud Manager when you want to define global settings, such as the color scheme and logo displayed in the browser.

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:



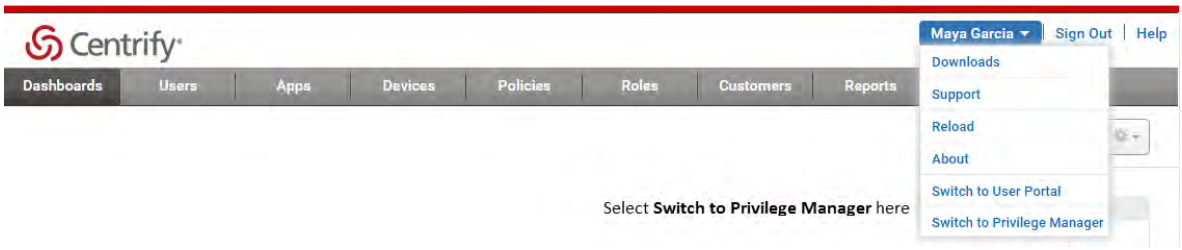
You can follow the steps listed in the Getting Started dashboard to begin adding users and creating roles. For Centrify privilege service, you are going to use the following Cloud Manager tabs:

- 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.

Managing resources

The Resources tab lists all of the resources—such as servers, workstations, switches and routers—available for you to manage. If you are a member of a role with the appropriate privilege management rights, you can add or delete resources from this list.

For more information, see the following topics:

- Planning to add resources
- Adding a single resource
- Importing multiple resources and accounts
- Viewing the resources you've added
- Filtering the resources displayed
- Identifying favorites
- Selecting a resource
- Selecting account actions for a resource
- Viewing and modifying resource-specific details
- Checking out an account password
- Extending the password checkout time
- Checking in a password
- Logging on without a password
- Specifying a user name and password
- Using the remote connection to work on a target resource
- Removing account information for a resource
- Deleting a resource

Planning to add resources

Before adding any resources to the Centrify privilege service, you might want to consider which accounts you need to manage and whether there are any restrictions on those accounts that you should be aware of.

For more information, see the following topics:

- Identifying the accounts to manage
- Using a proxy account for root

Identifying the accounts to manage

Some of the common accounts that are likely candidates for being managed through the Centrify privilege service include:

- `root`
- `oracle` for Oracle database administration
- *`sid`*`adm` for SAP administration
- `db2inst` for IBM DB2 instance administration
- `patrol` for BMC Patrol administration

You might have many other administrative tools or in-house accounts that require special privileges or have access to sensitive information. You can use the Centrify privilege service to manage the password for any of these accounts or add any other accounts of your choice to securely store the account information without having the password managed by the Centrify privilege service.

Using a proxy account for root

The most common scenario for most resources is to have the Centrify privilege service manage the password for the local `root` user. However, it is also very common to configure secure shell environments to prevent the `root` user from opening secure shell connections, which would prevent the account from being used to log on to target resources.

To address these two common scenarios, the Centrify privilege service allows you to specify a "proxy" account to use in place of the `root` account. The "proxy" account is used to open the secure shell session on the target resource. The account used as the "proxy" for the root account does not require any special privileges. The only requirement for the "proxy" account is that it must be allowed to open secure shell sessions on the target resource. After the "proxy" account opens the secure shell connection, the Centrify privilege service gets `root` privileges programmatically, enabling the account to perform administrative tasks on the target resource.

If you have configured `ssh` to prevent the `root` user account from logging on by opening a secure shell (`ssh`) connection, you also have the option to have the password for the "proxy" account managed by the Centrify privilege service. If you select **Manage this password** for a "proxy" account, only the Centrify privilege service will know the password for the account. The managed proxy account password will not be available to any other applications or users.

Adding a single resource

If you want to manage accounts for a server, workstation, or network device through the Centrify privilege service, you must first add the computer or network device to the Resources list. Initially, you might add resources and shared accounts one-by-one using the

Add Resource Wizard, which guides you through the information required. Alternatively, you can create an import file to add multiple resource and shared accounts at once.

To add a new computer or network device to the resources list

1 From the list of Resources, click Add to open the Add Resource Wizard.

2 Type a unique name to identify the resource, the DNS host name or IP address, and select the type of server or network device you want to add.

Optionally, you can type a longer description of the server or device. For example, you might want to make note of the manufacturer and model number or the physical location of the server or device, then click Next to continue.

3 Optionally, add a user name and password for an account to be used with the server or network device, then click Next to continue.

If you specified the resource by using a fully-qualified domain name, you should use the *`domain`*`\`*`username`* format for the account. If you specified the resource by using an IP address, you should use the *`IPaddress`*`\`*`username`* format for the account.

You can specify any valid user account and password. In most cases, however, you would specify `root` or Administrator or an account with similar privileges for which you want to manage the password. For any account you add, you can also choose to whether or not you want the Centrify privilege service to manage the account password. If you select Manage this password, the Centrify privilege service automatically resets the password immediately after the account and resource are added and each time the account is checked in. Only the Centrify privilege service knows the password stored. You should deselect this option if you don't want the Centrify privilege service to manage the password for the account.

Optionally, you can also type a longer description of the account. For example, you might want to describe the tasks the account is used to perform, then click Next to continue.

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 is allowed to 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 necessary, you can open the `/etc/ssh/sshd_config` file on the server to verify whether the `PermitRootLogin` parameter is set to `no`.

  If you have configured `ssh` to prevent the `root` user account from logging on by opening a secure shell (`ssh`) connection, you must add a user name and password for an account that can open a secure shell connection on the target resource. The account

name and password you specify become a "proxy" account used in place of the `root` account. The account used as the "proxy" for the root account must be able to open secure shell sessions on the target resource, but no other special privileges are required. After the "proxy" account opens the secure shell connection, it gets its `root` privileges programmatically to perform administrative tasks on the target resource.

If you are adding a "proxy" account to open secure shell sessions, you have the option to have the password for this account managed by the Centrify privilege service. If you select **Manage this password**, only the Centrify privilege service will know the password for the account from this point on. The managed proxy account password will not be available to any other applications or users.

After you specify whether `root` is allowed to open secure shell sessions on the target resource and, if necessary, the 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 server or network device using the account information provided, then click Finish.

If the resource and account settings are successfully verified, click Close.

If there's an error, verify the resource name or IP address is accessible over the network and that the user name and password you provided are valid for the server or network device you are attempting to add. If verification fails, close the error message, deselect the Verify Resource Settings option, then click Finish to add the resource without an account and close the Add Resource Wizard.

Note You can only deselect the Verify Resource Settings option if the password for the account is unmanaged. If the password for an account is managed, the resource settings must be verified to ensure the correct password is stored by the privilege management service.

Importing multiple resources and accounts

If you are familiar with the information required to add resources and shared accounts, you can create an import file to add multiple resources and shared accounts at once. The import file provides a comma-separated set of required and optional fields that describe the resources and accounts you want to add.

To import multiple resources and accounts

1 From the list of Resources, click Import.

2 Click Bulk Resource Import Template to download the template for importing resources and shared accounts.

The import template is a file with comma-separated values for the fields used to import resources and accounts. This file illustrates the format to use in creating your own

comma-separated values (CSV) file with the resources and accounts you want to import. The template also provides an example of how you might add two accounts for the resource named host2.

3 Open the Bulk Resource Import Template in a text editor or spreadsheet program.

4 Click File > Save As to save the file using a new name in a location you can browse to from Privilege Manager.

5 Edit your custom file so that each line provides the following information for a specific resource:

For this template field	You need to do this
`Name`	Type the display name of the resource you want to add. This field is required. As illustrated by the example in the template, you can have multiple lines with the same resource name. For example, if you are adding more than one shared account for the same resource, list each account as a separate line with the same resource name.
`FQDN`	Type the fully-qualified domain name or IP address of the resource you want to add. This field is required.
`ComputerClass`	Specify the type of resource you are adding. This field is required. You can specify one of the following for the `ComputerClass` field: • Windows • UNIX • GenericSsh
`Description`	Type any descriptive information you want to add for the resource. This field is optional.
`ProxyUserPassword`	Provide the password for the "proxy" user that is allowed to change the password of the `root` account. This field is optional. This field is only applicable if your secure shell environment is configured to not allow the `root` user to access computers remotely using SSH.
`ProxyUser`	Type the name of the "proxy" user that is allowed to change the password of the `root` account. This field is optional. This field is only applicable if your secure shell environment is configured to not allow the `root` user to access computers remotely using SSH.
`ProxyUserIsManaged`	Specify whether you want to manage the password for the "proxy" user. This field is optional. You can specify `TRUE` if you want to manage the password for the "proxy" account, or `FALSE` if you want to leave the password unmanaged. This field is only applicable if your secure shell environment is configured to not allow the `root` user to access resources remotely using SSH.
`User`	Type the user name for an account to be used with the resource. This field is optional.
`Password`	Type the password for the account to be used with the resource. This field is optional.

For this template field	You need to do this
`Managed`	Specify whether you want to manage the password for the user account you are adding for the resource. This field is optional. You can specify `TRUE` if you want to manage the password for the account, or `FALSE` if you want to leave the password unmanaged.
`UseProxy`	Specify whether you want to add a "proxy" account for the resource. This field is optional. You can specify `TRUE` if you want to use a "proxy" account, or `FALSE` if you don't want to add a "proxy" account for the resource. This field is only applicable if your secure shell environment is configured to not allow the `root` user to access resources remotely using SSH.
`UserDescription`	Type any descriptive information you want to add for the user account. This field is optional.

As illustrated by the examples in the template file, you can leave optional fields blank. When you are finished adding the resources and accounts you want to import, remove the template fields and examples—if you haven't done so already—and save your changes to the file.

6 From the list of Resources, click Import, then click Browse.

7 Select your customer CSV file and click Open.

8 Verify the email address is the email address where you want to be notified of the import result, then click **Import**.

The import process runs in the background. Depending on the number of resources and accounts you are importing, the process might take some time to complete. You will receive email notification of the results when the import process is complete.

Viewing the resources you've added

After you have added at least one resource, you can click the Resources to view the following information for all resources:

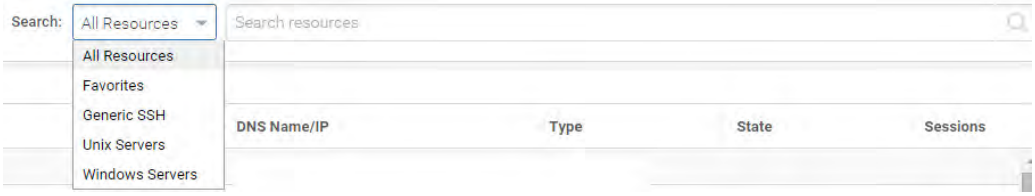
- Name is the unique name you use to identify the resource.
- DNS Name/IP address is the fully-qualified domain name or IP address defined for the resource in DNS.
- Type specifies the type of resource as a UNIX, Windows, or Generic SSH resource.
- State displays nothing if the last health check for the resource was successful. If the resource health check failed for any reason—for example, because the port used to check resource health is blocked or a network connection to the resource is not available—the column displays Unreachable.
- Sessions specifies the number of currently active sessions for the resource.

- Checkouts specifies the number of password checkouts for the resource.

Filtering the resources displayed

By default, the Resources tab displays all of the servers and network devices you have added to the cloud service. You can filter the list by selecting a filter, such as Windows or Favorites, from the menu of filtering options.

For example, click the arrow next to All Resources to view the list of filtering options:



You can then use the drop down menu to select resources of a specific type. You can also filter the list of resources displayed by typing a search string, or by combining a filter and a search string. If you type a search string, resources and network devices with either a display name or a DNS name matching the string are included.

Within the resource list, you can click column headers to change how the listed resources are sorted.

Identifying favorites

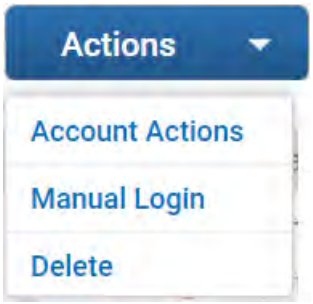
As you add servers, workstations, and network devices to the resource list, you might find it convenient to identify the ones you work with most frequently as favorites. You can identify the resources as your favorites by clicking the star icon next to the resource name.

You can then filter the resource list to only display the servers, workstations, and network devices that you work with most often. Identifying a resource as a favorite also adds that resource to the workspace you see when you click the Workspace tab, enabling you to see activity and take action at a glance without navigating the full list of resources that have been added to the privilege service.

Selecting a resource

You can select a resource to work with by clicking anywhere in the row that contains the resource name to display the resource details or by clicking the check box for a row. Selecting a resource displays the Actions menu to select the action you want to perform.

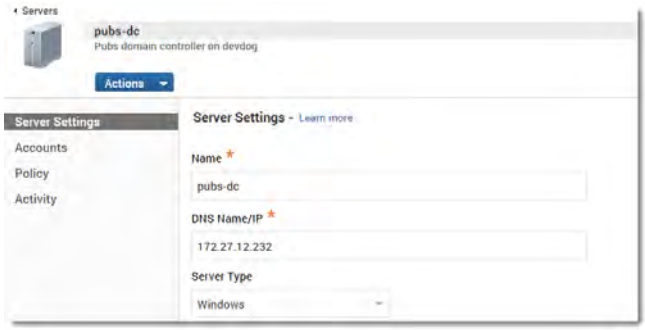
For example, select a resource using the check box, then click Actions to display the list of potential actions.



From here, you can click:

- Account Actions to select an account and an action specific to that account.
- Manual Login to log on by specifying a user name and password.
- Delete to remove a resource from the list.

You can also select an action from the Actions menu when viewing the details for an individual resource. For example:



When displaying the details for a selected resource, you can also change resource settings, add accounts, set resource-specific policies, and view recent activity for the resource, including who has logged on, and who has checked out or checked in a password for accessing the resource.

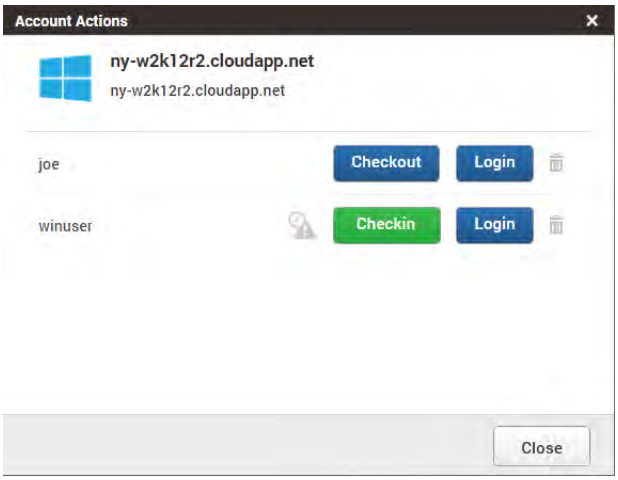
Selecting account actions for a resource

When you select a resource and click the Actions menu, you can select Account Actions to see the complete list of shared accounts that have been added for the resource. From the list of shared accounts, you can perform the different types of tasks, depending on the current state of the account. For example, you might see any of the following actions available for an account:

- Extend the checkout time if password is currently checked out.

- Checkout or Checkin depending on whether the shared account password if it is currently checked out or not.
- Login to log on to the resource using the shared account without knowing the password.
- Delete the shared account and password.

For example, if you select Account Actions, you can view the list of shared accounts and select the appropriate action to take:



Viewing and modifying resource-specific details

When you are viewing the details for an individual resource, you can also change resource settings, view and add account information, define resource-specific policies, and review recent logon and password activity. For more information about viewing and modifying resource-specific information, see the following topics:

- Changing resource settings
- Viewing and adding accounts for a resource
- Setting resource management policies
- Viewing activity for a resource

Changing resource settings

You can click Resource Settings to change the display name, DNS name or IP address for a previously added resource. You can also use the resource settings to correct the resource type or add an optional description for the selected resource.

If you set the resource-specific or global policy to allow remote access to a resource, you can use the Resource Settings to specify the session type and the port number to use for remote access. If the resource is a Windows server, you can select **Rdp** to allow remote

desktop connections to the server. If the resource is a UNIX server or workstation or a network device that supports secure shell (`ssh`) connections, you can select **Ssh** as the session type. The default port used for secure shell connections is 22, but you can specify a different port number, if appropriate.

If the resource is a UNIX server and you have configured `ssh` to prevent the `root` user account from logging on using secure shell connections, you can select the **Enable proxy account** option and specify a user name and password of a user with sufficient privileges to change the password for the root account.

If you make changes to any of these settings for a server or network device, click **Save**.

Viewing and adding accounts for a resource

You can click Accounts to add, modify, or delete the accounts used to access a previously added resource.

In most cases, you add one account to use for accessing a resource when you initially add the resource to the Centrify privilege service. If you skipped the step for adding an account, provided invalid account information when you added the resource, or want to update the resource information to include additional accounts, you can do so after adding a resource by clicking Account when viewing the details for the resource.

To add a new account for a resource

1. Click Add.
2. Type the user name and password for an account you want to use to access the currently selected resource.
3. Select the **Manage this password** option if you want the Centrify privilege service to manage the password for the specified account.

   This option is not displayed if the resource type is Generic SSH for a network device.
4. Optionally, type a description for the account, then click Add.

From the list of Accounts, you can also view the following additional information:

- Last reset specifies the date and time the account password was last reset.
- Sessions specifies the number of currently active sessions for the account.
- Checkouts specifies the number of password checkouts for the account.
- Healthy displays OK if the password check for an account is successful. If the password stored by the Centrify privilege service is not longer valid, the column displays Failed. If the state of the password cannot be determined—for example, because the port used to check account health is blocked or the account is in an untrusted forest—the column displays Unknown.

- Proxy Account displays a check mark if the account uses the proxy account defined for `root` at the resource level.
- Managed displays a check mark if the password for the account is managed through the Centrify privilege service.

You can also select an account in the list, then Actions menu to check out the password for the account, log on to the target resource using the stored password for the account, or delete the account.

Setting resource management policies

You can set resource management policies for individual resources or set global resource management policies to apply to all resources. If you use a combination of global and resource-specific policies, the resource-specific policies take precedence over the global policies you set. You can use Privilege Manager to set resource-specific policies and Cloud Manager to set global resource management policies.

You can set the following policies to only apply on a specific resource or to apply globally to all resources you add to the Centrify privilege service except where you have explicitly defined a resource-specific policy:

- Allow multiple password checkouts for this resource

  Select No if only one administrator is allowed check out the password for a selected resource at any given time. If you select No, the administrator must check the password in and have a new password generated before another administrator can access the resource with the updated password.

  Select Yes if you want to allow multiple users to have the account password checked out at the same time for a selected resource. If you select Yes, multiple administrators can access the resource without waiting for the password to be checked in.

- Allow remote access to this resource

  Select Yes if you want to allow connections from outside of the firewall to access the selected resource. If you select No, administrators will be denied access if they attempt to log on to the selected resource from a connection outside of the firewall.

- Checkout lifetime (minutes)

  Type the maximum number of minutes administrators are allowed to have a password checked out. After the number of minutes specified, the Centrify privilege service automatically checks the password back in. The minimum checkout lifetime is 15 minutes. If the policy is not defined, the default checkout lifetime is 60 minutes.

Setting resource-specific policies

If you are not using global policies, only want to set policies on individual resource, or want to override global policies on specific resources, you can set policies using Privilege Manager.

To set resource-specific policies

1 Select the resource to display the resource details.

2 Click Policy.

3 Select settings for any or all of the following policies:

- Allow multiple password checkouts for this resource
- Allow remote access to this resource
- Checkout lifetime (minutes)

4 Click **Save**.

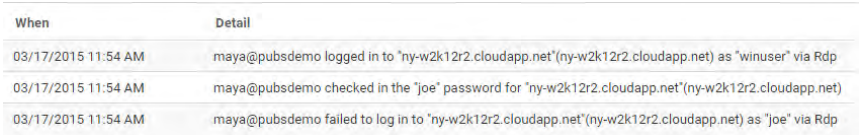
Setting global policies for all resources

If you have the appropriate rights, you can also create policy sets that include resource management policies that apply globally to all of the resources you add to the Centrify privilege service. The policies and default settings are the same as described in "Setting resource-specific policies" on page 28. You create policy sets with resource management settings in the same way you create other policy sets using Cloud Manager. The global policies are then used for all resources except for where you have explicitly set a resource-specific policy.

If you want to set global resource management policies or add resource management policies to an existing policy set, you must switch from Privilege Manager to Cloud Manager. In Cloud Manager, click the Policies tab. You can then click Add Policy Set or select an existing policy to display the Policy Settings. Expand Resource Management and select Resource Management Settings to set global resource management policies. For more information about setting global resource management policies, see "Creating global policies for resource management" on page 45.

Viewing activity for a resource

You can click Activity to review recent activity, such as password check out and check in activity, for the selected resource. For example, if a user has successfully logged on to the selected resource using a shared account, you might see information similar to the following:



When	Detail
03/17/2015 11:54 AM	maya@pubsdemo logged in to "ny-w2k12r2.cloudapp.net"(ny-w2k12r2.cloudapp.net) as "winuser" via Rdp
03/17/2015 11:54 AM	maya@pubsdemo checked in the "joe" password for "ny-w2k12r2.cloudapp.net"(ny-w2k12r2.cloudapp.net)
03/17/2015 11:54 AM	maya@pubsdemo failed to log in to "ny-w2k12r2.cloudapp.net"(ny-w2k12r2.cloudapp.net) as "joe" via Rdp

Checking out an account password

When you add accounts for resources to the Centrify privilege service, you store the passwords for those accounts securely in the Centrify cloud. If you have the appropriate global or resource-specific permissions, you can check out the password for a stored account to access a resource. When you check out a password, you choose whether to display or copy it to the clipboard for use. The password remains checked out until either you check it back in or the Centrify privilege service checks it automatically.

The maximum length of time you are allowed to keep a password checked out is configured using a resource management policy. However, you can extend the checkout time for a password that is currently checked out, if needed. For more information about configuring the Checkout lifetime policy, see "Setting resource management policies" on page 27. For more information about extending the checkout time, see "Extending the password checkout time" on page 29.

To check out a password

1. Select the Resources tab.
2. Select a resource from the resource list.
3. Click the Actions menu, then select **Account Actions**.
4. Find the appropriate account from the list of shared accounts, then click **Checkout**.
5. 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.

   The checkout is recorded as recent activity in the dashboard and in the list of resource activity.
6. Click **Close**.
7. Log on to the remote computer using the selected account name and password.

After taking the appropriate action on the target resource, close the session to log off and check in the password. For more information about checking in a password, see "Checking in a password" on page 30.

Extending the password checkout time

If you have the appropriate administrative rights and you have checked out the password for a saved account name, you can extend the checkout time to allow you to continue maintenance or perform administrative operations. The default maximum length of time you are allowed to keep a password checked out is configured using a resource management policy. If the maximum checkout lifetime is 60 minutes and you extend the checkout time before time runs out, the password expiration is reset to 60 minutes.

You can extend the checkout time for a password indefinitely at any point in its lifetime as long as you extend the checkout time before the checkout period expires. For example, if you have extended the checkout time for 60 minutes, but need more time to resolve an issue, you can extend the checkout time for another 60 minutes as long as you do so before the first 60 minutes expires. For more information about configuring the Checkout lifetime policy, see "Setting resource management policies" on page 27.

To extend the check out time for a password

1. Select the Resources tab.
2. Select a resource from the resource list.
3. Click the Actions menu, then select **Account Actions**.
4. Find the appropriate account from the list of shared accounts, then click the **Extend Checkout Time** icon.

   After you extend the checkout time for a password, the activity is logged on the Privilege Manager dashboard.
5. Click **Close**.

After you are finished performing maintenance or administrative tasks on the target resource, log off, and check in the password. For more information about checking in a password, see "Checking in a password" on page 30.

Checking in a password

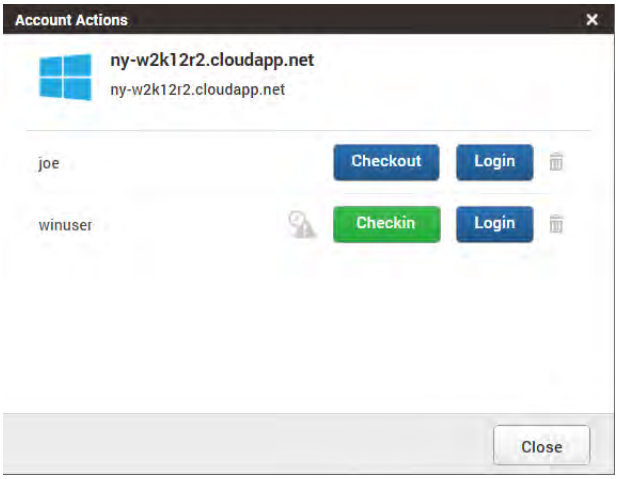
After you check out a password, you have a limited period of time in which the password you checked out is valid for activity on a remote resource. If the Centrify privilege service manages the password for the account, you should check in the password when you end the session on the remote resource, so that a new secure password can be generated for the account you used.

You can check in a password you have previously checked out from the Resources, Accounts, or Workspace tab. For example, if you are viewing the list of resources or the details for an individual resource, you can navigate to Account Actions to check in a password that you currently have checked out.

To check in a password you have previously checked out

1. Select the Resources tab.
2. Select a resource from the resource list.
3. Click the Actions menu, then select **Account Actions**.

4 Find the appropriate account from the list of accounts, click **Checkin**, then click **Close**.



You can also check in an account password when you are viewing your own activity on the Workspace tab. or when viewing accounts on the Account tab. For more information about reviewing the summary of your activity, see "Using the workspace" on page 42. For more information about working with accounts directly, see "Managing accounts and resource-specific permissions" on page 36.

Logging on without a password

After you add account information to the Centrify privilege service, other users with the appropriate global or resource-specific permission can log on using the account without knowing the password for the account.

When you select an account stored in the Centrify privilege service to log on to a target resource, the Centrify privilege service opens a secure shell connection if the target resource is a UNIX or Generic SSH resource or a remote desktop connection if the target resource is a Windows computer. If the target resource does not use the default port for secure shell or remote desktop connections, you can specify the port to use by clicking Resource Settings for a selected resource. For more information about changing settings for a target resource, see "Changing resource settings" on page 25.

To log on to a resource using saved account information

1 Select the Resources tab.

2 Select a resource from the resource list.

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

4 Find the appropriate account from the list of shared accounts, then click **Login**.

If the stored credentials are valid, logging on starts a new interactive secure shell or remote desktop session on the target resource. Within the secure shell or remote desktop session,

most operations—such as cut and paste or resizing of windows—work as you would expect them to. For more information about working in the remote session, see "Using the remote connection to work on a target resource" on page 32.

Specifying a user name and password

You can also log on to any target resource you add to the Centrify privilege service without using any account information that's stored in the Centrify privilege service. You can use any valid credentials to log on manually to a target resource.

To log on to a resource by specifying a user name and password

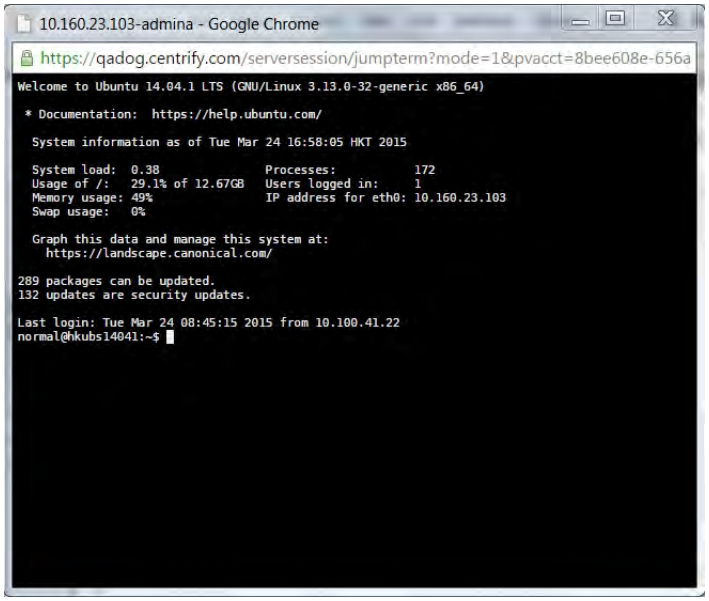
1. Select the Resources tab.
2. Select a resource from the resource list.
3. Click the Actions menu, then click **Manual Login**.
4. Type the user name and password and click **Login**.

If the credentials you specified are valid for the target resource, logging on starts a new interactive secure shell or remote desktop session on the target resource. Within the secure shell or remote desktop session, most operations—such as cut and paste or resizing of windows—work as you would expect them to. For more information about working in the remote session, see "Using the remote connection to work on a target resource" on page 32.

Using the remote connection to work on a target resource

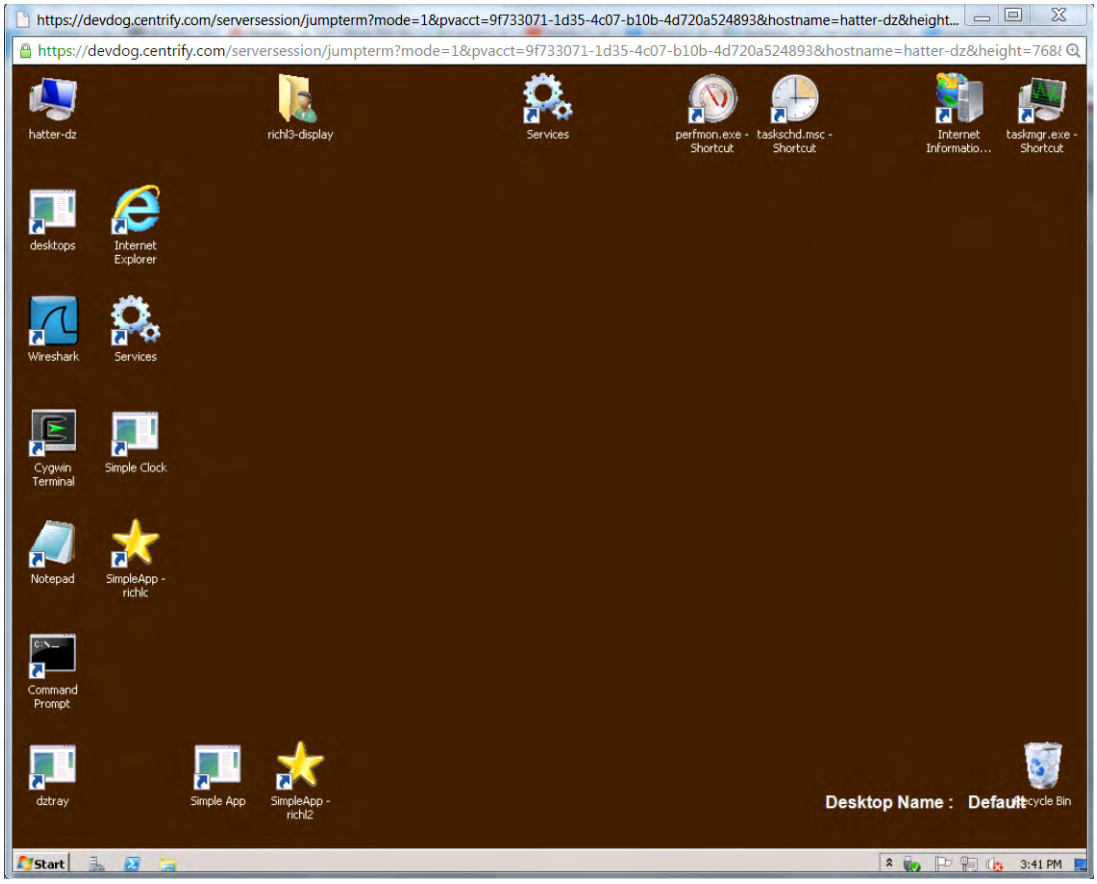
When you log on using stored account information for a resource or by manually specifying a user name and password, you open a web-based SSH client or RDP connection on the target resource. For example, if the target resource is a UNIX server or a network device

that supports SSH, the connection opens a new browser window with the secure shell session:



The secure shell terminal works as you would expect. For example, you can resize the window by dragging the window borders. You can also maximize or minimize the window to change your working area while the session is open or close the window to end the session. You must use a mouse to copy and paste in the secure shell, however, because Ctrl-C is used to terminate an operation in UNIX-based environments.

Similarly, if the target resource is a Windows computer, logging on opens a new browser window with a remote desktop connection:



The remote desktop works as you would expect. For example, you can resize the window by dragging the window borders. You can also maximize or minimize the window to change your working area while the session is open or close the browser window to end the session. Menus and keyboard shortcuts operate in the same way as when you log on locally to a Windows computer.

Removing account information for a resource

You can remove an account for a resource from the Centrify privilege service at any time. Removing a stored account from the Centrify privilege service does not affect account information stored locally on the target resource. However, you must display or copy the password to the clipboard before the account can be deleted to help ensure you can continue to use the account with its correct password after removing it from the Centrify privilege service.

To remove an account from a resource

1. Select the Resources tab.
2. Select a resource from the resource list.
3. Click the Actions menu, then select **Account Actions**.
4. Find the appropriate account from the list of shared accounts, then click the **Delete** icon.
5. 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.

   After displaying or copying the password, the account is deleted immediately. You can click the **Back to Accounts** icon if you want to cancel the operation or select a different account to remove.
6. Record the password for future reference, then click **Close**.

Deleting a resource

You can remove a resource from the Resources list and the Centrify privilege service only if you have removed all account information from the server.

To remove a resource from the service

1. Select the Resources tab.
2. Select a resource from the resource list to display its details.
3. Select Accounts to verify that there are no accounts associated with the resource.
4. Click the Actions menu, then click **Delete**.
5. Click **Yes** to confirm that you want to proceed with deleting the resource.

Managing accounts and resource-specific permissions

The Accounts tab lists all of the shared accounts you have added for managing resources, such as servers, workstations, and network devices.

The list of accounts presents all of the same information as listed under Accounts for each resource when you view the resource details. The information is presented on its own tab to make it easier to search, filter, and sort the accounts in which you are interested. For example, you can filter the accounts listed to only include managed accounts or only unmanaged accounts or type part of an account name to search for matching accounts or resource names.

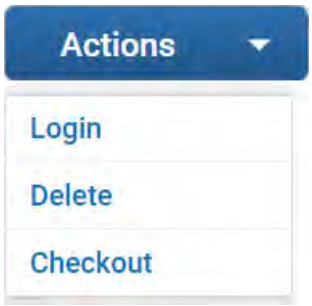
For more information about performing these tasks, click the following links:

- Selecting an account
- Changing account settings
- Adding users and setting permissions for an account
- Changing users or roles for an account
- Checking out account passwords
- Logging on without a password
- Deleting accounts

Selecting an account

You can select an account to work with by clicking anywhere in the row that contains the account name to display the account details or by clicking the check box for a row. Selecting an account displays the Actions menu to select the action you want to perform.

For example, select an account using the check box, then click Actions to display the list of potential actions.



From here, you can click:

- Login to log on the target resource using the selected account and stored password.
- Delete to remove the selected account from the Centrify privilege service.
- Checkout to check out the password for the selected account.

Changing account settings

If you are viewing the account details for an individual account and resource combination, the information you can change depends on the type of resource. If you are viewing an account for a Windows or UNIX server, you can select **Manage this password** to convert an unmanaged account into a managed account, deselect **Manage this password** to convert a managed account into an unmanaged account, or modify the account description. You cannot change the account name.

If you are viewing an account for a UNIX server, you can select or deselect **Use proxy account** depending on whether you want to use the proxy account defined for the resource for password management and to log on. In most cases, you would select this option for an account if the account cannot open secure shell sessions on the target resource.

If you are viewing an account for a generic SSH device, you can edit the account description. You cannot manage account passwords or change the account name.

If you make any changes to the account, click **Save**.

Adding users and setting permissions for an account

If you are viewing the account details for an individual account and resource combination, you can click Permissions to specify the individual users or roles that are allowed to use the account on the selected resource and what each user or role has permission to do when using the account.

For example, if you have added the account `root-1` for a resource, you might want to specify what members of the `onsite-IT@pubs.org` and `offshore-IT@pubs.org` can do with the `root-1` account on the target resource. For each of these roles, you can control what members are allowed to do using the following permissions:

- Select **Grant** to allow a selected user to grant permissions to other users for an account.

  As an administrator in the `sysadmin` role, your user account has this permission by default. You can assign this right to other users to allow them to update the permissions for the selected account.

- Select **Checkout** to allow a selected user to check out—that is, display or copy—the password for the selected account.

If the account is a managed account, checking the password in after checking it out generates a new password. If the account is not a managed account, the password remains unchanged until you manually reset it outside of the Centrify privilege service. For an unmanaged account, the same password might be used more than once. In most cases, you should not grant this permission for unmanaged accounts.

You should not select this option if the account is used to access a network device because the password cannot be changed for generic secure shell connections. Because the password doesn't change after being viewed or copied, this permission would make the device vulnerable to attack. This vulnerability also applies to any unmanaged account. However, in some rare cases, granting the Checkout permission might be useful if you want the ability to view or copy the password for an account that is stored but not managed by the Centrify privilege service.

- Select **Login** to allow a selected user to use the selected account to log on to the target resource using a secure shell (ssh) session or a remote desktop (rdp) connection.

  If you select the Login permission, the selected user or role who has access to the account can log on without knowing the account password. This is the most common permission to grant because it secures access to both managed and unmanaged accounts. Because the password is not visible to the user or role who is using the account, you should select this option if the account is used to access a network device.

- Select **Edit** to allow a selected user to edit information for the selected account.

  If the account and resource combination is an account for a UNIX or Windows server or workstation, you can specify whether the account password is managed or not and the edit the account description. You cannot change the account name. If the account is associated with a network device, you can only edit the account description.

- Select **Delete** to allow a selected user to delete the selected account.

  If you want to remove a resource from the Centrify privilege service, you must first delete all of the accounts that have been stored for that resource.

To add a user or role to an account with access to a target resource

1. From the list of Accounts, select the account to which you want to grant access.
2. From the account details, click Permissions, then click Add.
3. Type all or part of the user or role you want to find.
4. Select the appropriate users and roles from the search results, then click **Add**.
5. Select the appropriate permissions for each user and role you have added, then click **Save**.
   - Select **Grant** to allow a user to grant other users rights to use the account.
   - Select **Checkout** to allow a user to display or copy the password for the account.

- Select **Login** to allow a user to log on to the server or network device without knowing the password for the account.
- Select **Edit** to allow a user to edit information for the account.
- Select **Delete** to allow a user to delete the account.

You must select at least one permission for the user or role before you can save your changes to the account.

Managing global permissions for users

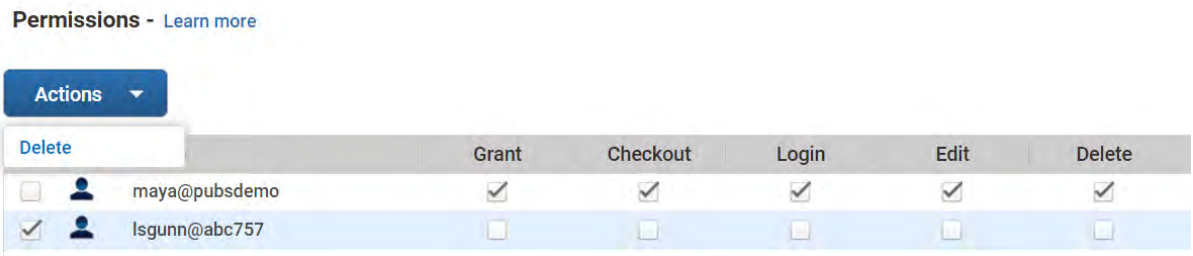
When you are managing permissions for the users who are allowed to use an account for a specific target resource, the permissions you set only apply to that account and resource combination. To set global permissions for a user or role, you must use settings defined in Cloud Manager. For more information about global settings for users, see "Defining global user permissions for resource management" on page 47.

Changing users or roles for an account

You can change the users and roles, and the permissions for the users and roles associated with an account on a target resource at any time. For example, if members of the `audit` role should no longer have access to a target resource using a specific account, you can simply delete the role from the list of users and roles allowed to use that account.

To delete a user or role from an account

1. From the list of Accounts, select the account from which you want to remove one or more users or roles.
2. From the account details, click Permissions.
3. Select the user or role you want to remove to display the Actions menu.



4. Select Delete, then click **Save**.

Checking out account passwords

If you have the Checkout permission, you can check out the password for an account and resource combination while viewing resources or accounts. The maximum length of time a password you are allowed to keep a password checked out is configured using a resource management policy. The users who are allowed to check out account passwords are defined using account permissions.

For more information about configuring the Checkout lifetime policy, see "Setting resource management policies" on page 27. For information about controlling which users or roles are allowed to check out account passwords, see "Adding users and setting permissions for an account" on page 37.

To check out an account password

1. Select the Accounts tab.
2. Select an account and resource combination to display the account details.
3. Click Permissions to verify you have the Checkout permission.
4. Click the Actions menu, then click **Checkout**.
5. 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.

   The checkout is recorded as recent activity in the dashboard and in the list of resource activity.
6. Click **Close**.
7. Log on to the target resource using the selected account name and password.

After taking the appropriate action on the remote computer, log off, and check in the password. For more information about checking in a password, see "Logging on without a password" on page 40.

Logging on without a password

If you have the Login permission, you can log on using stored account information without knowing the password while viewing resources or accounts. You use account permissions to specify the users and roles who are allowed to log on using the stored account password. For information about controlling which users or roles are allowed to log on without knowing the account password, see "Adding users and setting permissions for an account" on page 37.

To log on to a resource using saved account information

1. Select the Accounts tab.

2 Select an account and resource combination to display the account details.

3 Click Permissions to verify you have the Login permission.

4 Click the Actions menu, then click **Login** to open a secure shell session or remote desktop connection on the target resource.

Deleting accounts

If you have the Delete permission, you can remove an account that has been stored for a resource from the Centrify privilege service while viewing resources or accounts. The users and roles allowed to delete accounts are defined using account permissions. For information about controlling which users or roles are allowed to delete accounts, see "Adding users and setting permissions for an account" on page 37.

Removing an account from the Centrify privilege service does not affect account information stored locally on the target resource. However, you must display or copy the password to the clipboard before the account can be deleted to help ensure you can continue to use the account with its correct password after removing it from the Centrify privilege service.

If you want to delete a resource, you must first delete all of the accounts that have been stored for that resource.

To remove an account from a resource

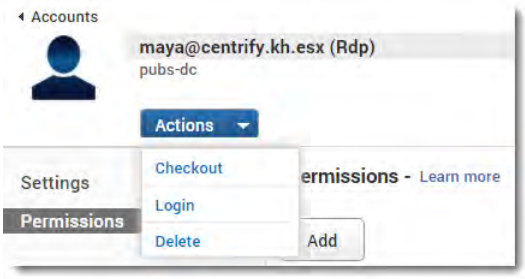
1 Select the Accounts tab.

2 Select an account and resource combination to display the account details.

3 Click Permissions to verify you have the Delete permission.

4 Click the Actions menu, then click **Delete**.

For example:



5 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.

After displaying or copying the password, the account is deleted immediately.

6 Record the password for future reference, then click **Close**.

Using the workspace

The Workspace provides an overview of your own password checkout and resource activity, including a list of the accounts for which you have a password checked out, your current sessions, and the servers and devices you have identified as favorites.

- **Expiring Checkouts** provides a quick reference for the number of passwords you have checked out that are due to be checked in within the next 15 minutes or have expired because they have not been checked in by their due date.
- **My Checkouts** lists the accounts for which you have a password currently checked out, when the password is due to be checked in, and the number of minutes remaining before the password expires. The number of minutes a password is allowed to be checked out can be configured on a server or device basis using the **Checkout lifetime** policy.
- **My Active Sessions** lists your currently active sessions, including the server DNS name or IP address where the sessions is running, the cloud service or Active Directory user account under which the session is running, and the date and time the session started.
- **Favorites** lists the servers and network devices you have identified as favorites in the resource list on the Resources tab.

Checking in a password from the Workspace

After you check out a password, you have a limited period of time in which the password you checked out is valid for activity on a target resource. When you end the session on the remote server, you should check in the password so that a new secure password can be generated for the account you used. From the Workspace tab, you can see a summary of your currently checked out account passwords at a glance.

To check in a password from the Workspace

1. Select the Workspace tab.
2. Select the server and account combination from the My Checkouts list.
3. Click the Actions menu, then select **Checkin**.

Working with favorites from the Workspace

If you have identified any servers or network devices as favorites in the server list, you can use the Workspace to manage accounts, log in remotely, or delete the server or network device.

To work with a server or network device from the Workspace

1. Select the Workspace tab.
2. Select a server or network device from the list of Favorites.
3. Click the Actions menu, then select the appropriate action.
   - Click **Account Actions** to work with shared accounts for the selected server or network device.
   - Click **Manual Login** to log on remotely to the selected server or network device using a user name and password of your choice.
   - Click **Delete** to delete the selected server or network device if all accounts for the server or network device have been deleted.

Viewing the privilege service dashboard

The dashboard provides an overview of information about all of the resources and accounts that have been added to the Centrify privilege service. The dashboard includes the total number of resources and accounts you are managing, the resources that have had the most password checkout activity, and a list of the account passwords that are currently checked out with the date and time when passwords where checked out and when the passwords are due to be checked back in. The dashboard also provides a summary of recent user activity, a list of currently active user sessions on managed resources, and a map that indicates where resource logins are taking place.

- **Total Resources** is the total number of servers and network devices you have added to the privilege service.
- **Total Accounts** is the total number of accounts you have added to the privilege service.
- **Top Checkouts** lists the resources that have had the password checkout activity for the last seven days.
- **Resources By Type** provides a pie chart overview of how many of the resources are Windows, UNIX, or Generic SSH (for Cisco, Juniper, and other network devices) resources.
- **Resource Health** indicates the number of resources that are reachable using the accounts stored in the privilege service and the number of resources that are not reachable.
- **Resource Logins** is a map that illustrates where the resources that have had login activity are located.
- **Recent Activity** lists the date and time for recent password check out, password check-in, and login activity.
- **Password Checkouts** lists all of the accounts that have a password checked out, when the password is due to be checked back in, and the user who checked out the password. You can check in passwords from the list in the dashboard if it is a password that you have checked out.
- **Active Sessions** lists the resources where there are sessions initiated from Privilege Manager using stored account information or manually-entered credentials.

Configuring global roles and settings for the privilege service

You do most of the work for the Centrify privilege service within the Privilege Manager portal. However, there are some settings and tasks that are done outside of Privilege Manager using the Cloud Manager administrative portal. For example, you use Cloud Manager to access reports for all Centrify cloud-based services, to add users and roles to the identity service, and to configure global settings for resource management. These global settings include resource management policies, the privilege management rights you can add to roles, and the specific permissions granted to different users when they use the accounts stored in the Centrify privilege service.

The global permissions you set using Cloud Manager apply to all resources you add to the privilege service except when you explicitly set permissions differently for a specific account and resource combination. You also use a global setting in Cloud Manager if you want to enable auditing using Centrify Server Suite, Enterprise Edition.

The following topics are covered:

- Creating global policies for resource management
- Creating roles with privilege management rights
- Defining global user permissions for resource management
- Enabling auditing for sessions on target resources

Creating global policies for resource management

As a user with the `sysadmin` role, you can create policy sets that include resource management policies that apply globally to the resources you add to the Centrify privilege service. The policies and default settings are the same as described in "Setting resource management policies" on page 27. You create policy sets with resource management settings in the same way you create other policy sets using Cloud Manager. The global policies are used for all resources unless you have explicitly set a resource-specific policy.

To set global policies for resource management

1. Select **Switch to Cloud Manager** from the account name menu.
2. Click the Policies tab.
3. Click Add Policy Set or select an existing policy to display Policy Settings.
4. Expand Resource Management and select Resource Management Settings to set global resource management policies.

5 Select settings for any or all of the following policies:
   - Allow multiple password checkouts
   - Allow remote access
   - Checkout lifetime (minutes)

6 Click **Save**.

Creating roles with privilege management rights

As a user with the `sysadmin` role, you can create roles that grant other users the rights required for managing servers, workstations, network devices, and the accounts used to access those resources. You create roles with these rights in the same way you create other roles using Cloud Manager. However, there are two administrative rights that are specifically for managing the resources and accounts you add to the Centrify privilege service:

- Privilege Management

  If you create a role with the Privilege Management administrative right, the users you add as role members can view resources and accounts where they have been granted permissions, and can add new resources and accounts to the Centrify privilege service. Users with this right can also grant permissions to other users for the specific resources and accounts they add to the Centrify privilege service.

- Privilege Management (Limited)

  If you create a role with the Privilege Management (Limited) administrative right, the users you add as role members can view resources and accounts where they have been granted permissions, but they cannot add any resources or account information to the Centrify privilege service.

Only users with the `sysadmin` role or a role with one of these administrative rights can access the Privilege Manager portal. You can then use global or resource-specific permissions to further control what users in a role can do. For example, some users who have the Privilege Management (Limited) administrative right might be granted the global Login permission so that they can log on to any resource without knowing any account passwords. Other users might be granted the Login permission only for a specific account and resource combination, such as the `oracle` shared account on the `db-main.ajax.org` server.

For more information about setting global user permissions for accounts in the Centrify privilege service, see "Defining global user permissions for resource management" on page 47. For more information about setting user permissions for accounts on specific resources, see "Adding users and setting permissions for an account" on page 37.

To create a role that includes privilege management rights

1 Select **Switch to Cloud Manager** from the account name menu.

2 Click the Roles tab.

3 Click Add Role or select an existing role to display the role details.

If you are creating a new role, you must provide at least a unique name for the role.

4 Click Administrative Rights, then click Add.

5 Select Privilege Management or Privilege Management (Limited) and any other rights you want included in this role, then click Add.

6 Click Save to save the role.

Defining global user permissions for resource management

Most of the activity in Privilege Manager involves managing resources and the accounts that are specifically used to access those resources. For example, when you manage user permissions for an account on a particular server, those permissions only apply in the context of that particular account on that specific server. There are, however, a few global settings for managing resources and accounts that are defined using Cloud Manager. For example, when you define global user permissions for resource management, those permissions apply for all resource you add to the Centrify privilege service.

To access the global resource management settings for user permissions

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 Click Add to search for and select users and roles.

- Type a search string to search for the users or roles to which you want to grant global permissions.
- Select the appropriate users and roles from the search results.
- Click Add.

5 Select the appropriate global permissions for each user.

- Select **Grant** to allow the selected user to grant permissions to other users.
- Select **Checkout** to allow the selected user to check out—that is, display or copy—passwords for accounts.
- Select **Login** to allow the selected user to use the shared account to log on to resources without knowing the account password.

- Select **Edit** to allow the selected user to edit information for accounts on all resources.
- Select **Delete** to allow the selected user to delete accounts stored in the Centrify privilege service.

  As an administrator in the `sysadmin` role, your user account has these permissions by default. You can assign specific global rights to other users to allow them to work with accounts on all managed resources.

6 Click Save to save the global user permissions settings.

Enabling auditing for sessions on target resources

The Centrify privilege service always logs audit trail events for the activity on resources and in the accounts you add to the service. If you also want to audit the session activity you initiate from Privilege Manager on target resources, you can enable auditing through Centrify Server Suite Enterprise Edition and the Centrify privilege service.

To prepare for auditing, you must have a working audit installation running in your environment. 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.

The audit installation must include the following core components:

- a management database to store installation information.
- the audit store and audit store database to define the scope and store session activity.
- at least two collectors to collect session activity and send it to the audit store database.
- the Audit Manager console to manage installation components, audit roles, and permissions.
- the Audit Analyzer console to view, query, and manage recorded activity.

For information about creating the audit installation and configuring the core components of the installation, see the *Auditing with Centrify Server Suite Administrator's Guide*.

If you are familiar with auditing using Centrify Server Suite, you might have an agent installed on some or all of your target resources. However, the agent is not required when you are using the Centrify privilege service to audit session activity. Instead, you can use the cloud connector to send session activity directly to the collector without installing an agent or the auditing service on the target resource. The only additional requirement to enable auditing using the cloud connector is that the computer you are using for the cloud connector must be within the scope of an audit store—that is, the computer must be included in the site, subnet, or IP address identified as the audit store. The session activity for all target resources will be sent to the audit store that includes the computer where the cloud connector is installed.

For more information about defining the scope for an audit store, see the *Auditing with Centrify Server Suite Administrator's Guide*.

For more information about auditing through the Centrify privilege service, see the following topics:

- Capturing and replaying sessions
- Differences in Windows sessions recorded by a cloud connector
- Differences in UNIX sessions recorded by a cloud connector
- Specifying the audit installation

Capturing and replaying sessions

If you have an audit installation available and enable auditing, the cloud connector captures all of the secure shell and remote desktop activity in the sessions you open from Privilege Manager. The cloud connector sends the recorded sessions to the collector service, which forwards the sessions to the audit store database. You can play back the recorded sessions using Audit Analyzer. You can also use Audit Analyzer to create queries and reports based on session activity and to review, update, or delete the sessions.

If you have multiple cloud connectors, the cloud connector used to record the session is selected randomly when you start the SSH or RDP session. If the cloud connector with an active session stops running, the session is disconnected. If the cloud connector is recording a remote desktop session when it stops, you can manually reconnect to the target resource using a different cloud connector to resume the session. However, the session segments are recorded in the audit store database as two separate audit sessions. The cloud connector will spool audited session activity if it can't connect to any collectors.

You must have Centrify Server Suite 2015, or later, Enterprise Edition, to audit the sessions you open from Privilege Manager. If you have an older version of Centrify Server Suite, you must upgrade before enabling auditing using the cloud connector.

For more information about managing the audit installation, querying and reviewing session activity, and other auditing-specific topics, see the *Auditing with Centrify Server Suite Administrator's Guide*.

Differences in Windows sessions recorded by a cloud connector

If you are already auditing session activity on Windows computers, you might notice a few differences between sessions recorded directly on a Windows computer that has an agent installed and the remote desktop sessions recorded by the cloud connector. For example, if a Windows session is recorded by the cloud connector, you might notice the following differences:

- Windows sessions recorded by the cloud connector do not include an indexed list of events.

- You cannot specify any agent configuration settings, such as the color depth to use or the offline data storage location.
- There is no role-based auditing or integration to skip auditing for some activity or to audit only privileged activity.
- Windows sessions recorded by the cloud connector do not include any information about the DirectAuthorize desktop being used or about desktop changes. However, you can use the desktop label to determine the desktop used for different operations when replaying Windows sessions.

Differences in UNIX sessions recorded by a cloud connector

If you are already auditing session activity on UNIX computers, you might notice a few differences between sessions recorded directly on a Linux or UNIX computer that has an agent installed and the remote desktop sessions recorded by the cloud connector. For example, if a UNIX session is recorded by the cloud connector, you might notice the following differences:

- UNIX sessions recorded by the cloud connector do not include standard input (`stdin`).
- You cannot specify any agent configuration settings that you control using the `centrifyda.conf` file, such as password masking.
- There is no role-based auditing or integration to skip auditing for some activity or to audit only privileged activity.
- You cannot configure "per command" auditing.
- You cannot obfuscate any sensitive information that might be captured in a session.

Specifying the audit installation

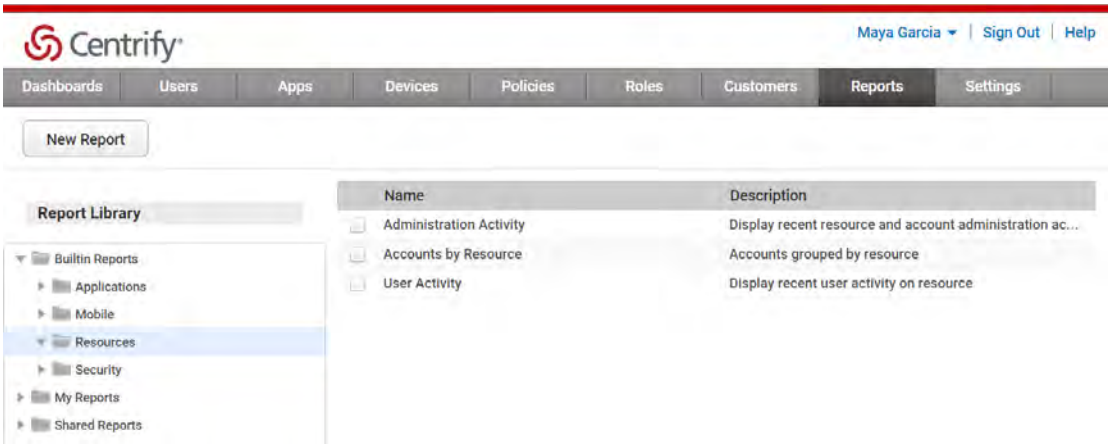
After you have created an audit installation and verified you have a working environment, you can use Cloud Manager to enable auditing and specify the installation name for the resources you manage.

To access the global resource management settings for 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 to save the global settings.

Creating and viewing reports

To create and review reports for managed resources, you must switch to Cloud Manager, then click the Reports tab. The Reports tab lists all of the built-in, private, and shared reports that are currently available for the Centrify identity platform and cloud-based services. Open the Builtin Reports, then select Resources to see the built-in reports for the Centrify privilege service. For example:



Select the report in which you are interested:

- Administration Activity provides details about recent administrative activity

  Administrative activity occurs when users or roles added to or deleted from accounts, when permissions are granted or changed, when resources or accounts are added or removed, when auditing is enabled, when resource information is updated.

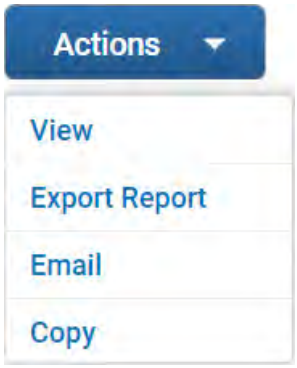
- Accounts by Resource lists the accounts for each resource grouped by resource name.

  The Accounts by resource report enables you to see all of the accounts added for each resource and the user names associated with each account in a single place.

- User Activity provides details about recent user activity on managed resources.

  User activity occurs when users attempt to log on using stored accounts whether the login attempt is successful or fails, when users check out or check in account passwords, and when the Centrify privilege service updates an account password.

After you select a report, click Actions to display the list of potential actions.



From here, you can click:

- View to generate the report in HTML format and view it in the browser.
- Export Report to creates the report as a file on your computer in either CSV or Microsoft Excel format.
- Email to send the report as either a Microsoft Excel file attachment or in an HTML table to the email address you specify.
- Copy to duplicate the report and save it in another report folder, such as a folder under My Reports or Shared Reports.

Troubleshooting

There are a few common errors you might see when using Centrify Privilege Service, particularly if you have set up a demonstration environment for evaluation and testing. This section describes the most common errors, how to check the cause of the error, and what you can do to prevent the error from occurring.

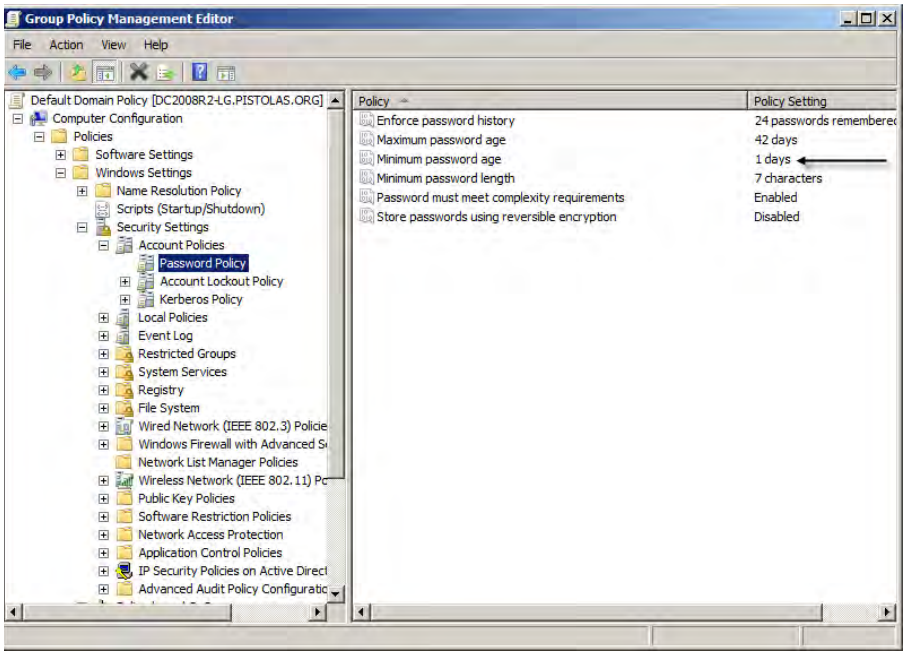
Unable to update account password

If you attempt to add a local account to the privilege service and see the "Unable to update account password" error, it is most likely caused by the Minimum password age policy you have configured. It is common for organizations to configure to the Minimum password age policy to be 1 day. If you create a new local account for testing, then attempt to add the account and have its password managed by the privilege service, the service cannot update the password if the password fails the Minimum password age requirement.

To check the Minimum password age policy

1. Open Administrative Tools and select Group Policy Management.
2. Select the Default Domain Policy, right-click, then select Edit.
3. Expand Computer Configuration > Windows Settings > Security Settings > Account Policies, then select Password Policy.

4 Check the Minimum password age setting.



If this policy is defined, you can either wait more than one day before adding the account with a password to be managed to the privilege service or you can disable the policy while testing with newly-created local accounts on computers joined to the domain. The issue doesn't exist on computers that are not joined to the domain where the policy is set or for local accounts with a password exceeding the Minimum password age.