PAM Essentials for Administrators

PAM Essentials allows you to use OneLogin's existing IdP tools and integrations to set up simple, easy-to-use platform access that users and admins can make the most of without requiring extensive technical know-how. Our proprietary technology simplifies the complex process of privileged access management (PAM) into role-based access policies, eliminating the need to configure VPNs and define subnets, and reducing the risks and vulnerabilities that can come from human error.

Instead, your PAM configuration with OneLogin can be up and running in under an hour with the process described in this guide. Using our secure network access connection, as well as powerful auditing features like full session recordings, your organization can dramatically improve security while still ensuring that your privileged users have easy access to the servers and systems they need.

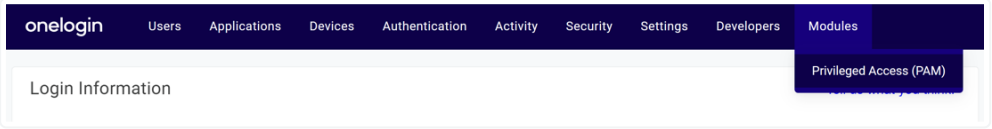
Related Documentation

- PAM Essentials for Auditors
- PAM Essentials for Users

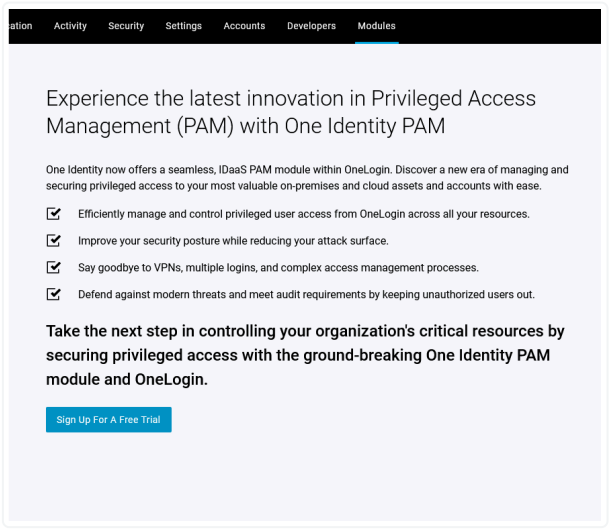
Table of Contents

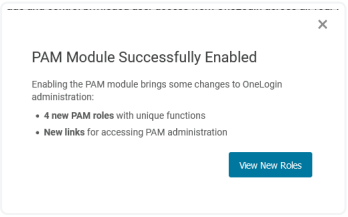
Connecting to PAM Essentials

1. In your OneLogin admin portal, go to **Modules > Privileged Access (PAM)**.



2. When prompted, **Sign Up For A Free Trial** to connect with PAM Essentials. A dialogue confirms that the module has been enabled and provides a brief overview of the PAM portal.

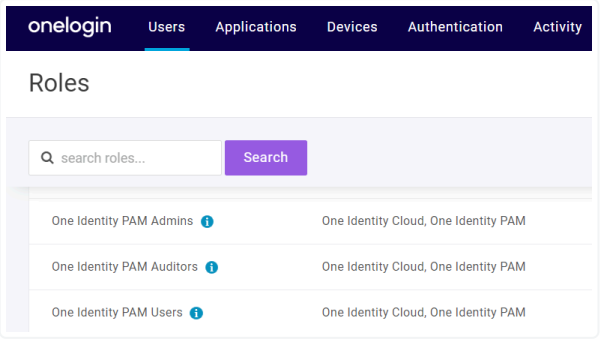




To return to the PAM Essentials portal at any time, go to **Managed Infrastructure** from your OneLogin user portal and select **PAM Administration**, or return to **Modules > Privileged Access (PAM)** in your OneLogin admin portal.

Granting OneLogin Users Access to PAM Essentials

On subscribing to PAM essentials, several new user roles are automatically created in your OneLogin tenant and can be assigned to your users. Only OneLogin users assigned one of these roles are able to view the managed infrastructure portal or any privileged access tools; the OneLogin environment will remain completely unchanged for all other users.

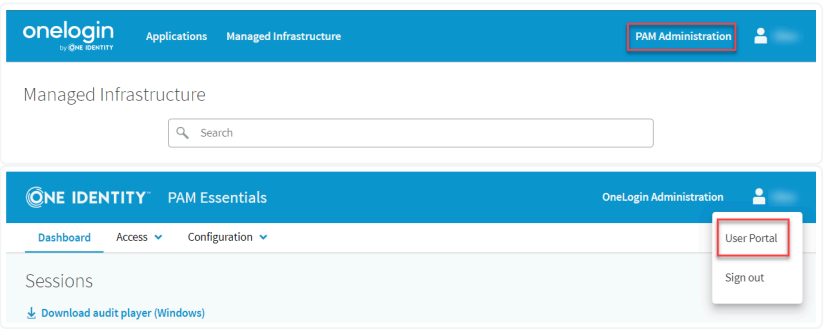


Important: Do **not** delete or rename these roles for any reason, as doing so will prevent module use.

Note: PAM Essentials admins and auditors are not automatically granted access to the PAM user portal for separation of duties. If a user requires access to both the PAM admin portal and the PAM user portal, they must be assigned both roles in OneLogin.

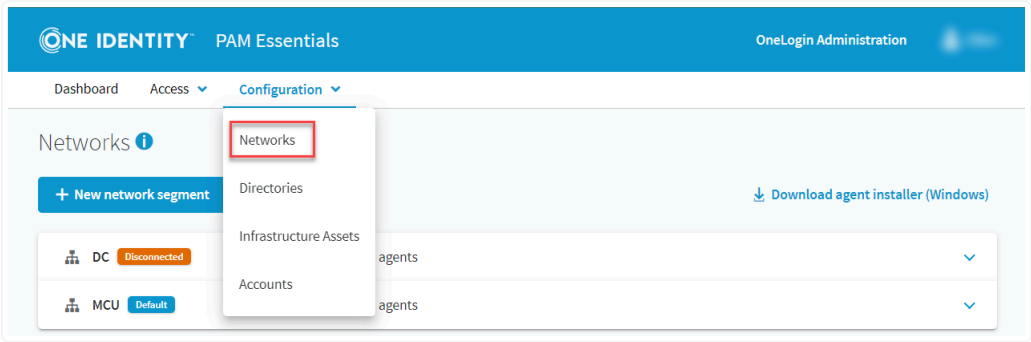
One Identity PAM Admins	Assign a user this role to grant them full configuration and audit access in the PAM administration interface. **Note:** The user must also have Super user privileges in order to access the Modules menu in the OneLogin administration portal.
One Identity PAM Auditors	Assign a user this role to grant them auditing access to PAM sessions and read-only access to the PAM administration interface. **Note:** The user must also have Super user privileges in order to access the Modules menu in the OneLogin administration portal.
One Identity PAM Users	Assign a user this role to grant them access to the PAM user portal for launching privileged access sessions.

Users assigned to both the PAM Users role and a PAM Admins or PAM Auditors role can navigate between the two portals in the upper-right corner of PAM Essentials.



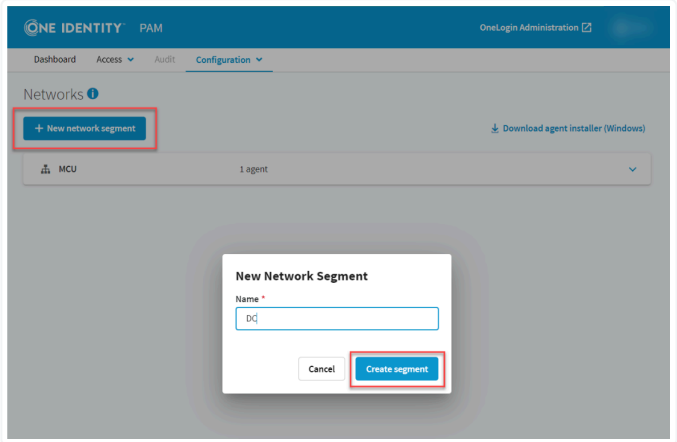
Connecting Isolated Networks

In your PAM Essentials administration portal, go to **Configuration** > **Networks** to establish secure connections between PAM Essentials and your private networks. These connections can be organized into individual network segments to optimize for location and performance.



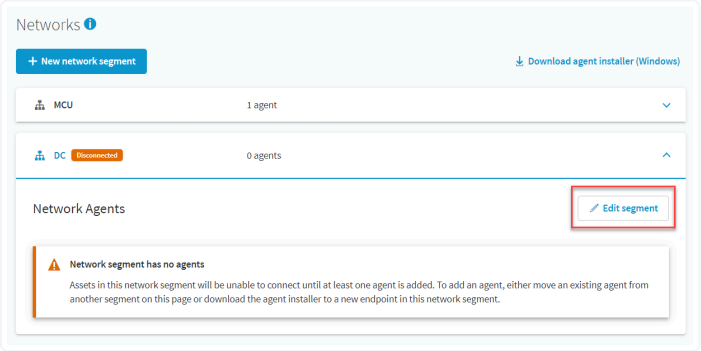
Network Segments

To create a network segment, click **+ New network segment** and give the segment a unique and descriptive name, then click **Create segment**.



> **Best Practice!** We recommend configuring agents for at least two computers in each of your networks, in order to provide redundancy and ensure uninterrupted connectivity in the event of server failure.

Select any segment and click **Edit segment** to rename or remove it.

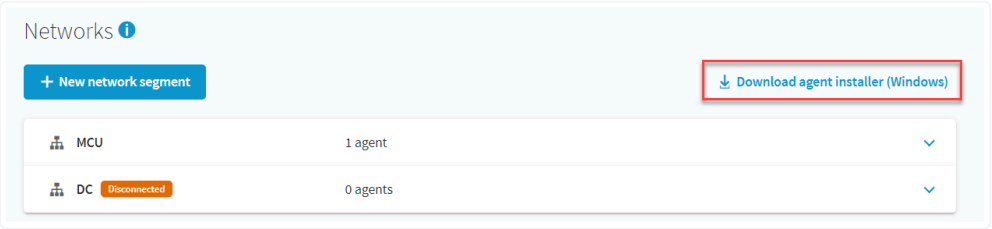


Note: At least one network segment is required. If a network agent is installed before creating your first network segment, a segment will automatically be created for you. If you have only one segment, it cannot be deleted until another segment has been created.

Network Agents

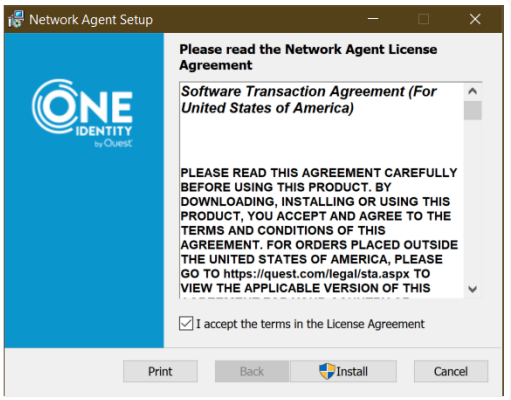
The One Identity Network Agent is what facilitates the connection between PAM Essentials and your network. The agent must be installed on at least one computer in each of your network segments.

1. Click **Download agent installer** to download an installation file containing the One Identity Network Agent utility.

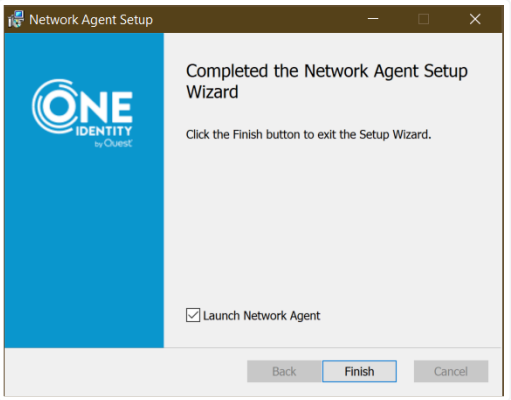


2. Run the installation file on at least one machine in each of your network segments. The installer can be downloaded or copied to any number of computers necessary.

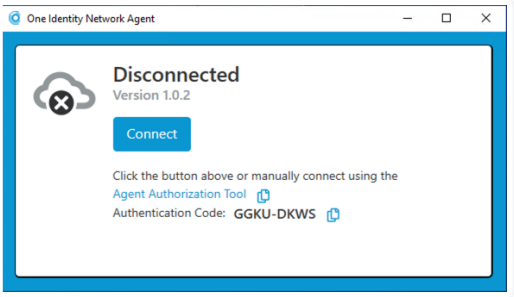
3. Accept the license agreement in the installation wizard and click **Install**. If prompted by the operating system, allow the installer to make changes to your device.



4. Once the installation is complete, check **Launch Network Agent** and **Finish** the installation.



5. The Network Agent launches in the lower-right corner of the screen and can be accessed again from the system tray at any time. Click **Connect** to automatically connect the network agent to PAM Essentials.



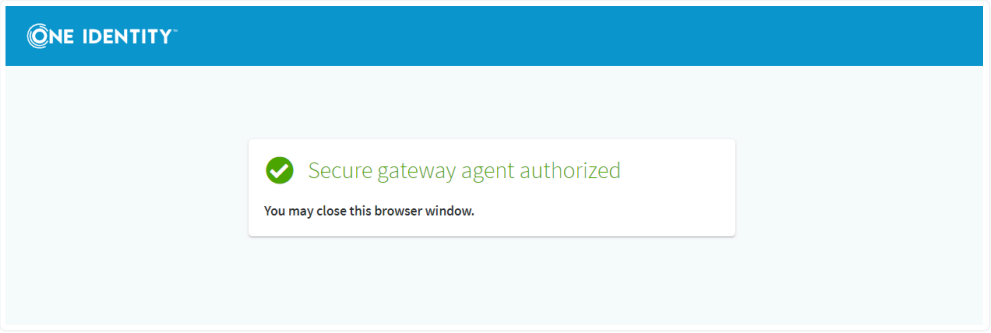
Troubleshooting

If automatic connection fails, you may instead visit the Agent Authorization Tool linked in the network agent and manually paste in the Authentication Code when prompted.

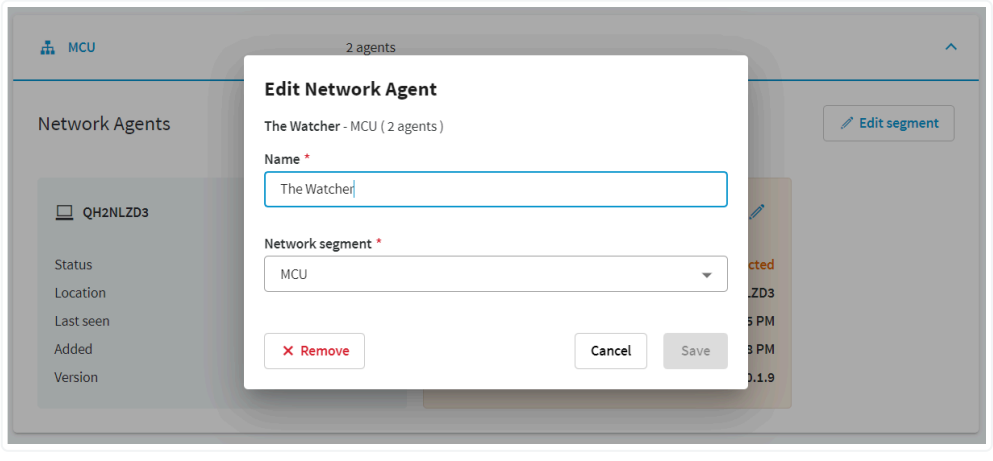
6. Sign in with your OneLogin credentials if prompted.

   Note: Do not sign in using Starling or Azure Active Directory.

   When the **Secure gateway agent authorized** confirmation appears, close this window and return to the Networks configuration in your PAM Essentials admin portal. You may need to refresh the configuration page before the new Network Agent appears.



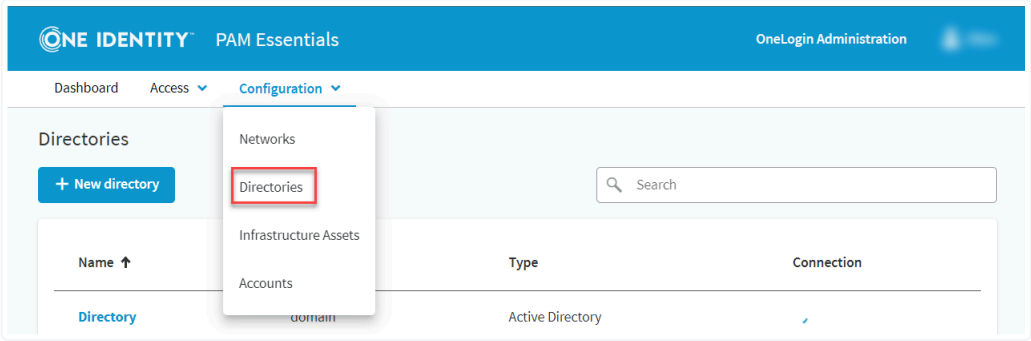
7. Click the pencil icon in the upper right corner of any Network Agent to rename it, remove it, or to reassign it to a different network segment.



Note: Removing a network agent from the network segment in PAM Essentials will disconnect it, but the network agent application will remain installed on the remote computer until manually uninstalled. If the agent is uninstalled without being removed from PAM Essentials, it will display disconnected in the PAM portal.

Managing Directories

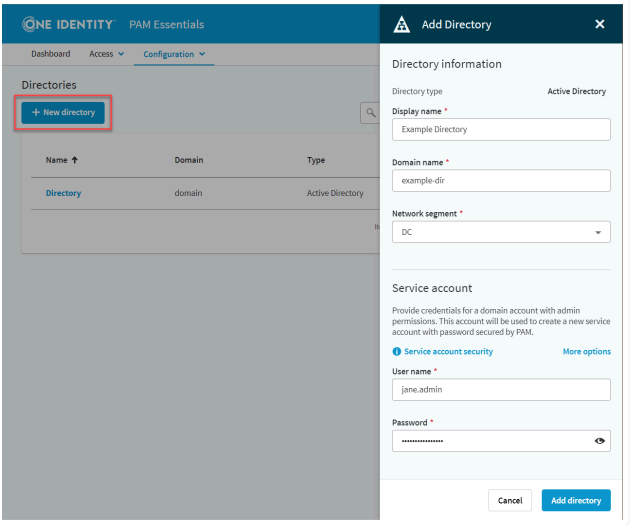
Go to **Configuration** > **Directories** to add and manage the directories associated with the network segments connected to PAM Essentials.



Note: Currently, only Active Directory is supported by PAM's directory management.

Adding a Directory

To add a directory, click **+ New Directory** and configure the following details:



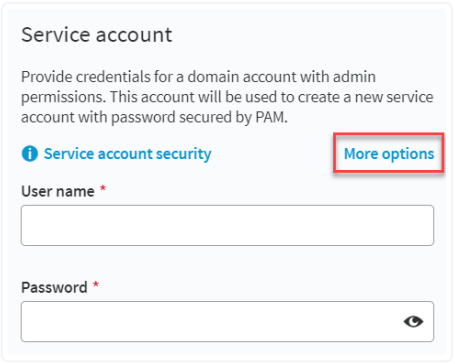
Display name	Enter a unique and descriptive name for the directory.
Domain name	Enter the directory's domain name.
Network segment	Select the network segment containing at least one of the directory's domain controllers.
Service account	Enter the **User name** and **Password** for a domain account with administrative privileges in this directory. This account will be used to create a new service account secured by PAM.

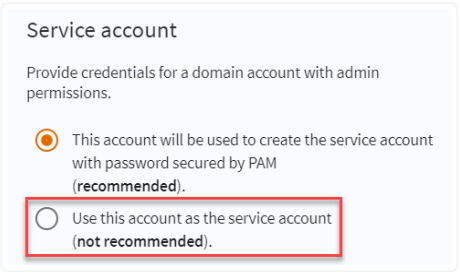
After clicking **Add directory**, the asset appears in your **Directories** list, where you can monitor its connection status or select it to manage its details.

Using an Existing Service Account

> **Important:** For security reasons, this is **not recommended**.

If necessary, you may connect PAM with an existing service account rather than granting it access to create and manage a new service account. To connect the account, click **More options** and select **Use this account as the service account**.





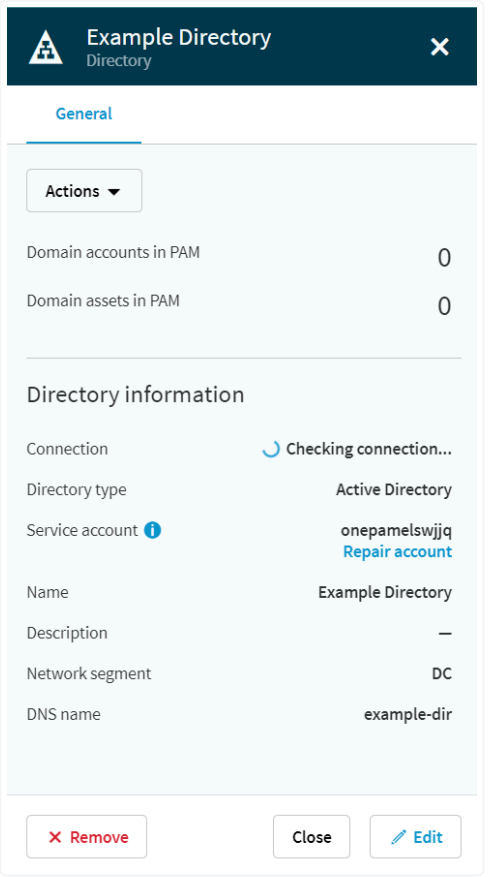
Once this is configured, PAM Essentials will immediately change the password for the admin account entered and rotate it regularly. Only PAM will have access to this account until the service account is replaced. **Do not use this option with any account that your administrators require access to.**

Directory Details

Click a directory's name to view and edit its details, check its connection status, or repair connection issues to the service account.

Open the **Actions** menu to perform the following actions:

Check connection	Verify connectivity between PAM and the directory
Add domain accounts	Create a new privileged account using this directory



Repair service account	Enter the credentials of another admin account in the domain to allow PAM to reconnect to the domain's service account **Note:** This will typically be the same account used when originally configuring the directory. **Do not** enter the credentials for the service account itself.

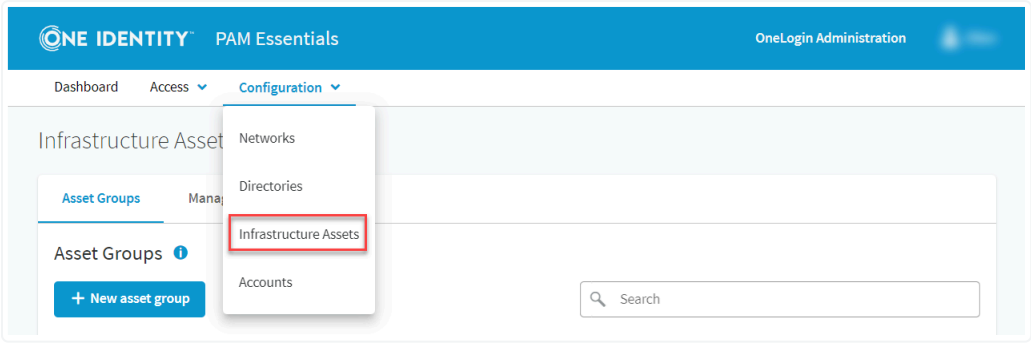
Under **General**, click the number of Accounts or Assets to view those related to this domain.

Click **Edit** to update the directory's name, domain, or network segment, and **Save** your changes.

Click **Remove** to revoke access to this asset or permanently delete it from PAM Essentials.

Managing Infrastructure Assets

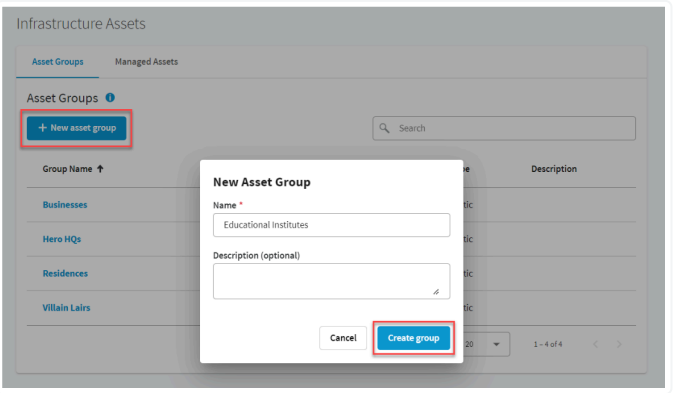
Go to **Configuration** > **Infrastructure Assets** to add and manage the assets that will be accessed by the privileged accounts you configure in the PAM portal.



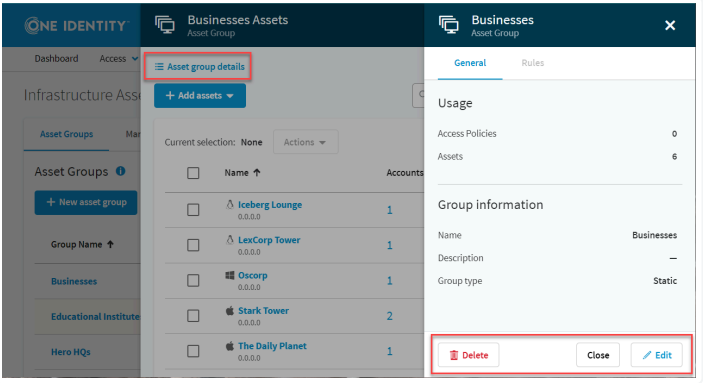
Asset Groups

All managed infrastructure assets configured in PAM Essentials are organized into groups. These groups are later assigned to your privileged accounts, giving them access to a collection of their necessary resources all at once with one simple policy.

To create a group, go to **Asset Groups** and click **+ New asset group**. Give the group a unique name, as well as a description if desired, then click **Create group**.



Select any group to view and manage its assets. Click **Asset group details** to edit or delete the group.



Warning: Deleting an asset group will not remove its assets from PAM Essentials, but will prevent them from being accessed with any policies relying on the group. Be sure to update any policies using the deleted asset group to ensure uninterrupted access to its assets.

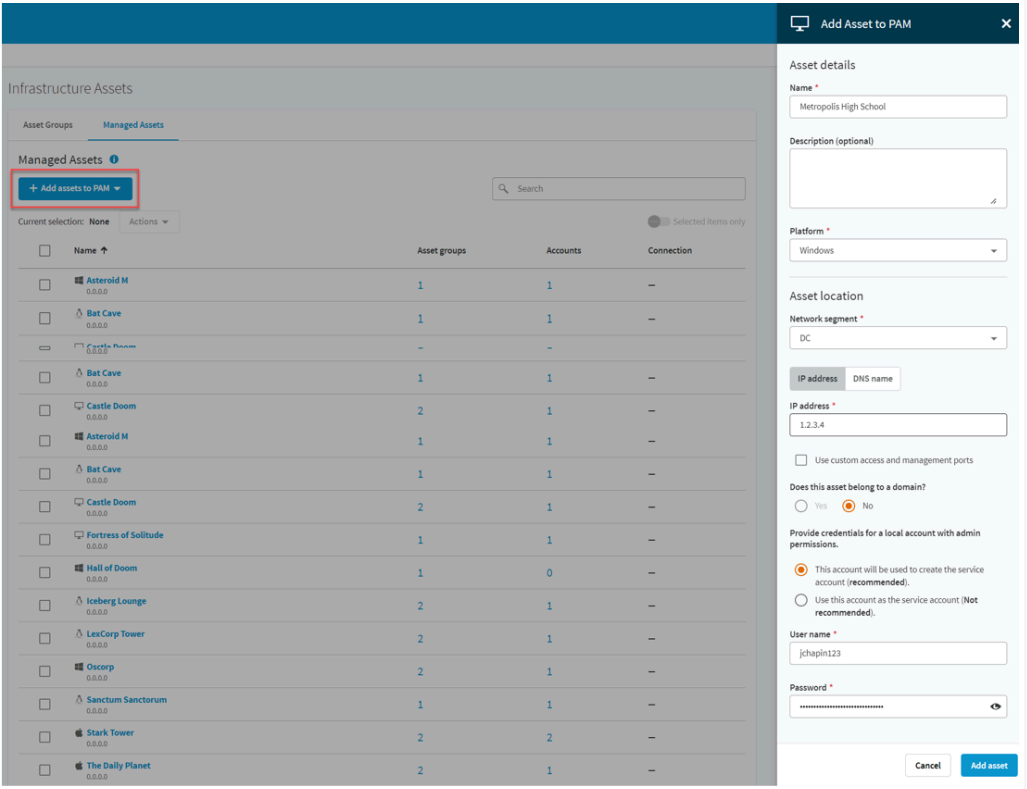
Managed Assets

Adding an Asset

To add a new asset, go to **Managed Assets** and click **+ Add assets to PAM**, then configure the following details:

Name	Enter a unique and descriptive name for the asset.
Description	If desired, provide a more detailed description of the asset's purpose or use.
Platform	Select the operating system used by the asset.
Network segment	Select the network segment where this asset is located.
IP address / DNS name	Select and enter either the DNS name or the IP address for the asset. **Note:** The DNS is resolved from the network agent and therefore not required to be publicly resolvable, provided that it's resolvable inside your network.
Use custom access and management ports	Enable this setting if you wish to manually assign the asset's RDP session and WinRM management ports. By default, the asset uses ports `3389` and `5985`, respectively.

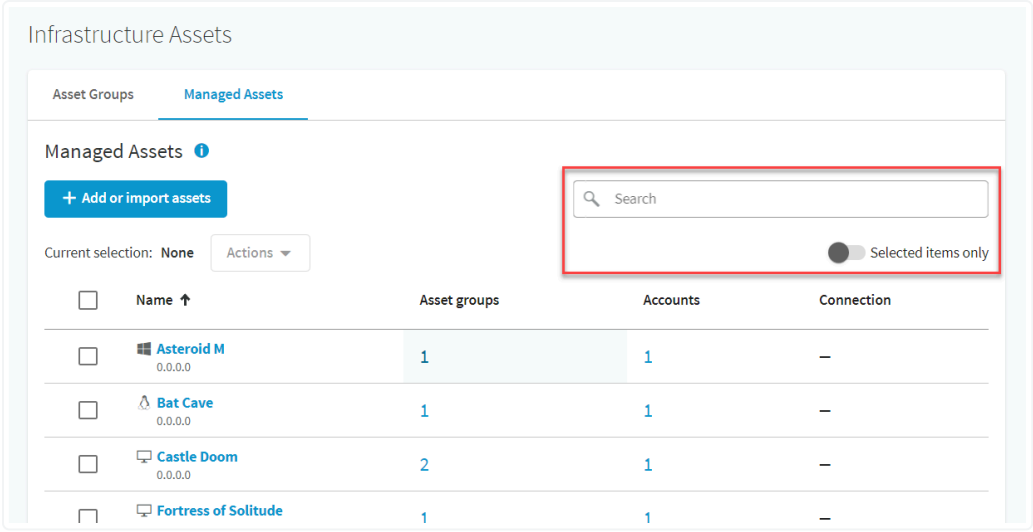
Does this asset belong to a domain?	If the asset belongs to a domain, select **Yes** and choose the appropriate directory. Otherwise, leave **No** selected to configure this as a local asset. **Note:** Domain assets can be used with both local and domain accounts, but local assets may **only** be used with local accounts. **Note:** Once the asset is configured, this setting cannot be modified. If you later wish to change your selection, the asset must be fully removed and re-added.
Provide credentials for a local account with admin permissions.	If configuring a local asset, enter the administrator credentials for an existing account on the asset device. This account will be used to create a service account managed by PAM Essentials for managing the credentials of local privileged accounts. **Note:** If necessary, you may instead select **Use this account as the service account** to use your existing admin account for PAM services, rather than create a new service account. This is **not recommended**, particularly if the existing account is in use for any other administrative functions. Once converted to a service account, the account's password will be automatically changed, rotated regularly, and only accessible to PAM until a new service account is configured.



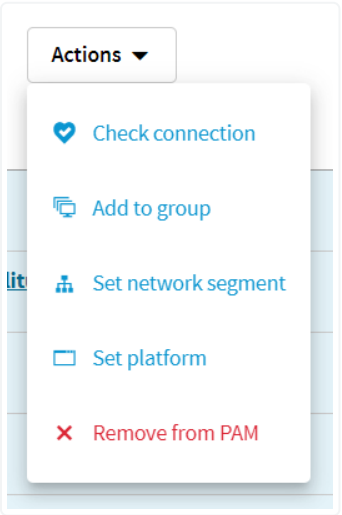
After clicking **Add asset**, the asset appears in your **Managed Assets** list, where you can add it to one or more asset groups. **An asset must belong to at least one group in order to assign it to an access policy.**

Asset List

If you have a large number of assets to navigate, you can use the **Search** tool to filter them by name, DNS, or IP address, or the **Selected items only** toggle to view only those assets you've manually selected.



Select any number of assets, then click **Actions** to perform the following actions:



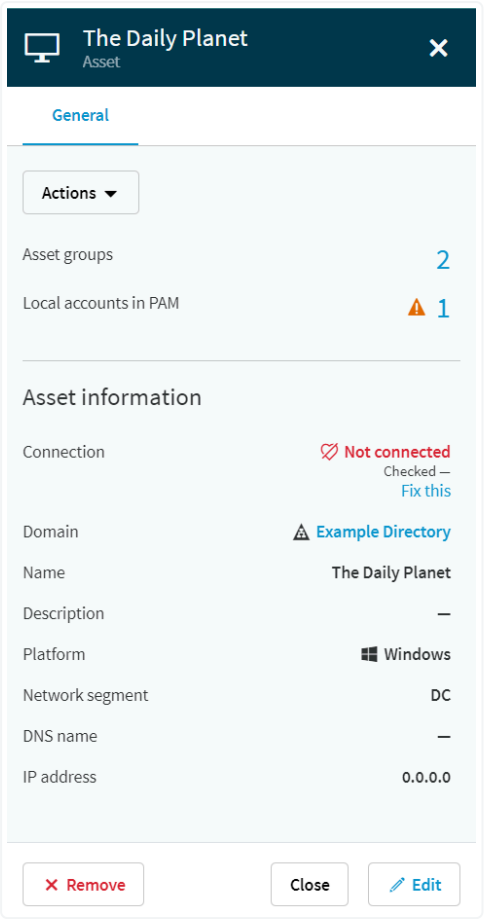
Check connection	Verify the selected asset(s)' connection status
Add to group	Add the selected asset(s) to a given asset group
Set network segment	Change the network segment for the selected asset(s)
Set platform	Change the platform of the selected asset(s)
Remove from PAM	Permanently remove the selected asset(s) and any local accounts of this asset from PAM Essentials. The service account used by PAM will remain on the asset but will no longer be managed by PAM.

Asset Details

Click an asset's name to view and edit its details, or to revoke or remove the asset.

Open the **Actions** menu to perform the following actions:

Check connection	Verify the asset's connection status
Add to group	Add the asset to a given asset group
Add local accounts	Create a new local privileged account using this asset as its parent asset



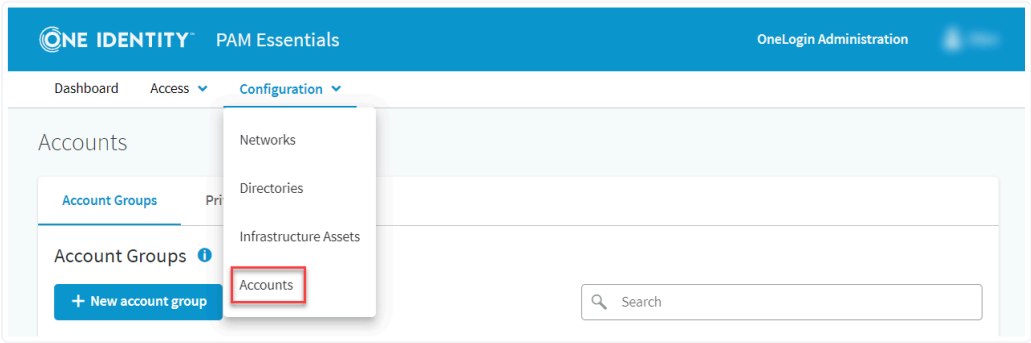
Under **General**, click the number of Groups or Accounts to view those related to this asset.

Click **Edit** to update the asset's name and description, platform, network segment, or DNS information, and **Save** your changes.

Click **Remove** to permanently remove the asset from PAM Essentials.

Managing Privileged Accounts

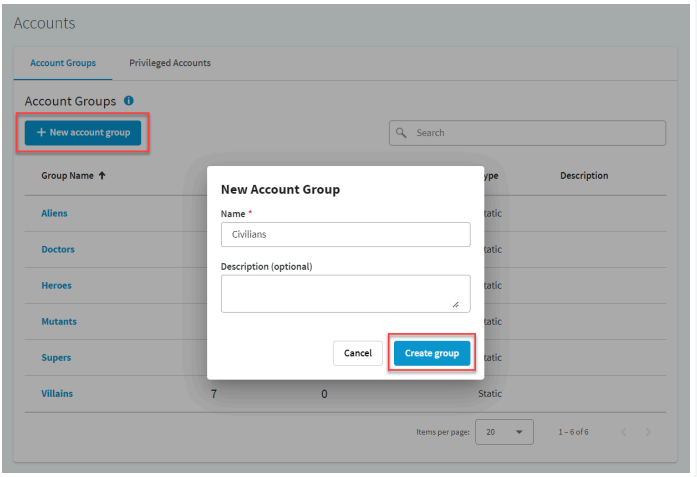
Go to **Configuration** > **Accounts** to add and manage the privileged accounts that will be granted access to the managed infrastructure assets you configure in the PAM portal.



Account Groups

Similarly to infrastructure assets, your organization's privileged accounts are collected into groups for ease of assigning access policies.

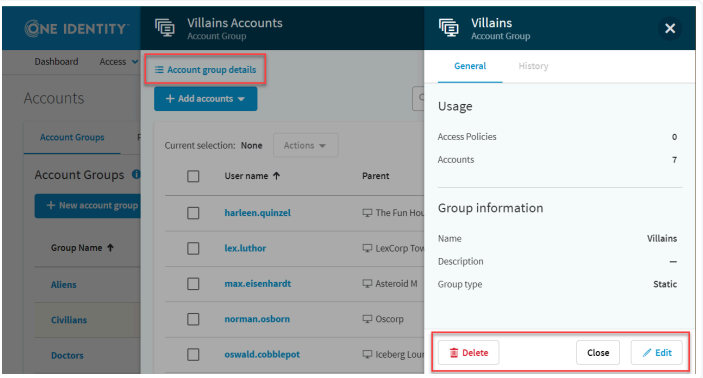
To create a group, go to **Account Groups** and click **+ New account group**. Give the group a unique name, as well as a longer description if desired, then click **Create group**.



> **Best Practice!** For your organization's security, assign as few accounts to each group as possible.

Access to your managed infrastructure is based on account groups, so only accounts with a confirmed need for a group's assets should be granted access.

Select any group to view and manage its accounts. Click **Account group details** to edit or delete the group.



Warning: Deleting an account group will not remove its accounts from PAM Essentials, but they must be assigned to an account group for access to be granted in an access policy. Be sure to update any

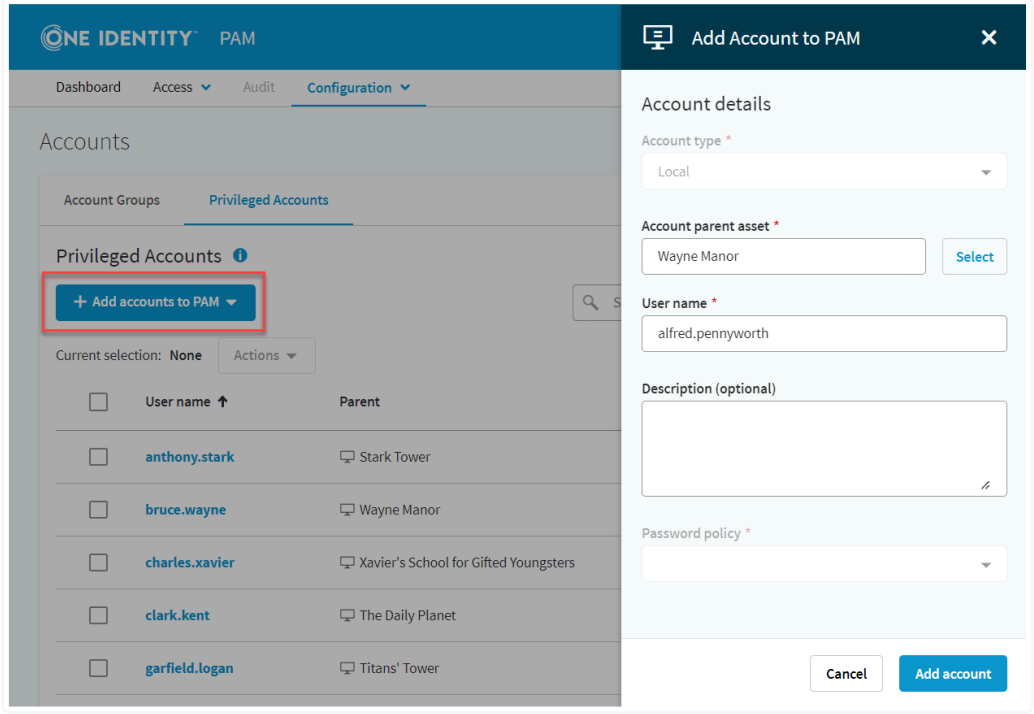
policies using the deleted account group to ensure uninterrupted access for its accounts.

Privileged Accounts

Adding an Account

To add a new account, go to **Privileged Accounts** and click **+ Add accounts to PAM**, then configure the following details:

Account type	Select either *Local* or *Domain*, then choose the account's parent asset or parent directory accordingly. Once the account parent is selected, additional options will appear.
User name	Enter the account's username.
Description	If desired, enter a description for the account.

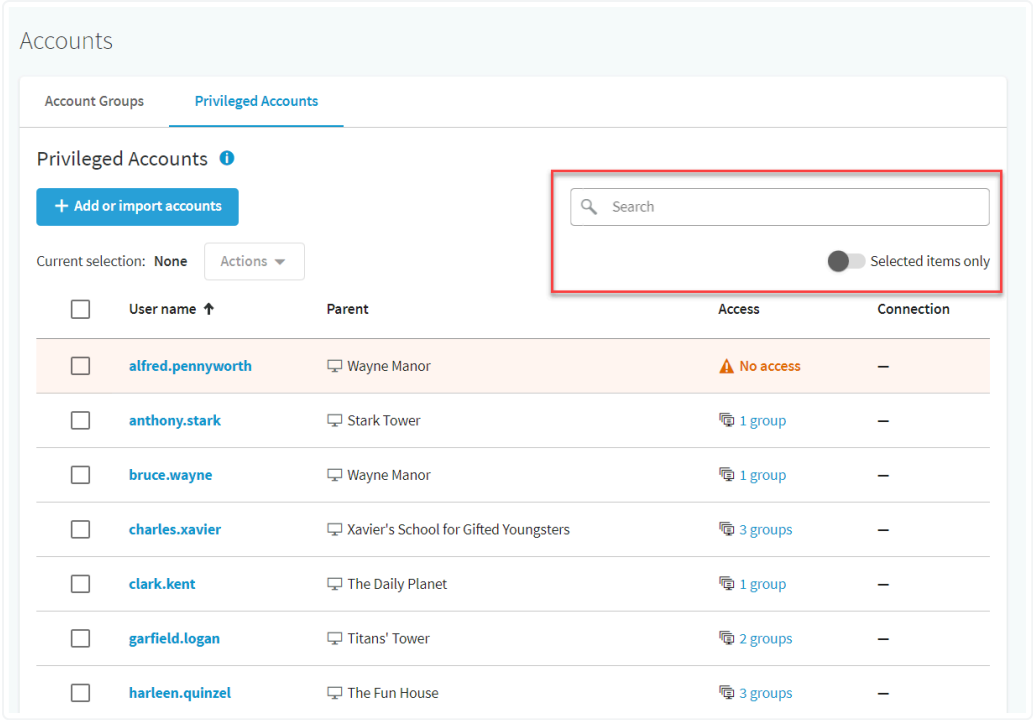


Click **Add account** to finish account creation. Unless previously disabled, a confirmation dialog verifies that you wish to **Give PAM control** of the account.

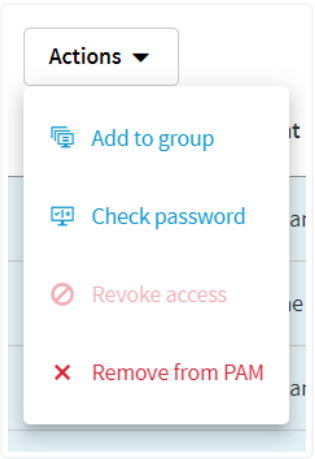
> **Note:** Accounts added directly through this interface are not assigned to any given account group and therefore cannot be immediately used. To enable access to the new account, you must also assign it to a group from the accounts list.

Navigating Privileged Accounts

If you have a large number of accounts to navigate, you can use the **Search** tool to filter them by name or parent asset, or the **Selected items only** toggle to view only those accounts you've manually selected.



Select any number of accounts, then click **Actions** to perform the following actions:



Add to group	Add the selected account(s) to a given account group
Check password	Verify/repair the selected account(s)' current password status
Revoke access	Remove the selected account(s) from all account groups. The account(s) will remain in PAM but cannot be used to access any assets.
Remove from PAM	Permanently remove the selected account(s) from PAM Essentials.

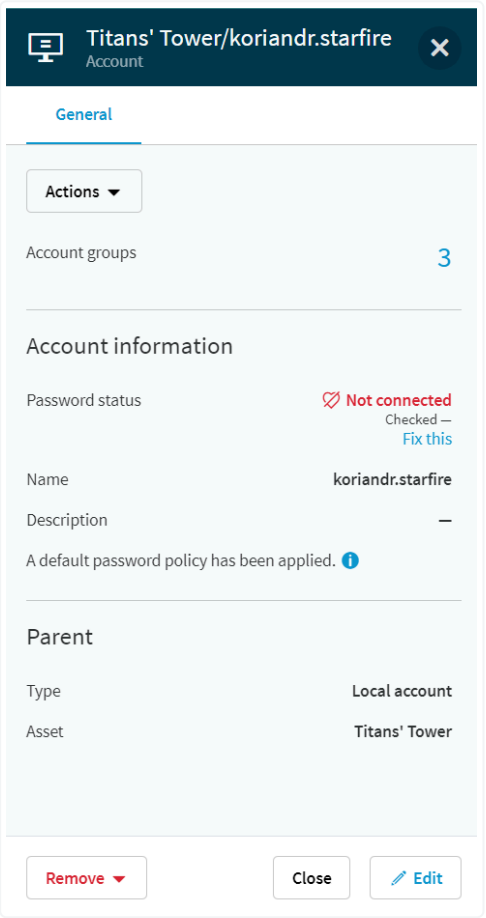
Note: An account removed from PAM will no longer have its credentials managed by PAM. Another administrator account must be used to reset the password for use outside of PAM.

Account Details

Click an account's name to view and edit its details, or to revoke or remove the account.

Open the **Actions** menu to perform the following actions:

Add to group	Add the account to a given account group
Check password	Verify/repair the account's current password status
Rotate password	Manually rotate the account's password. Passwords are automatically rotated on a weekly basis and immediately following a session during which the account was used.



Show password	Display the account's current password. **Warning:** This option should only be used in the event of an emergency. Showing the password will result in an audit event in the history and an automatic password rotation 30 minutes after the password is revealed.

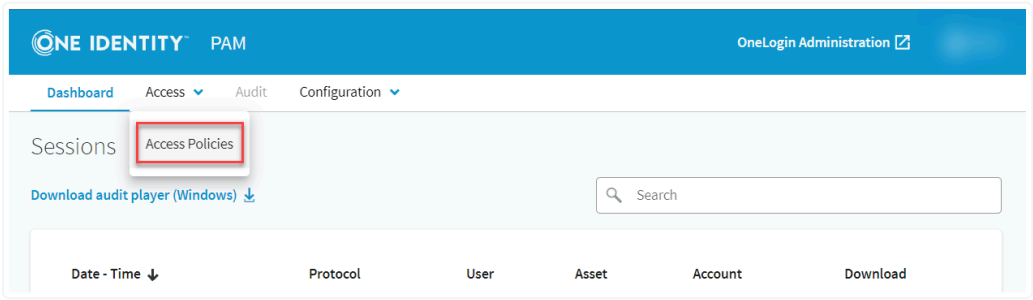
Under **General**, click the number of Groups to view those assigned to this account.

Click **Edit** to update the account's description and **Save** your changes.

Click **Remove** to revoke access for this account or permanently remove it from PAM Essentials.

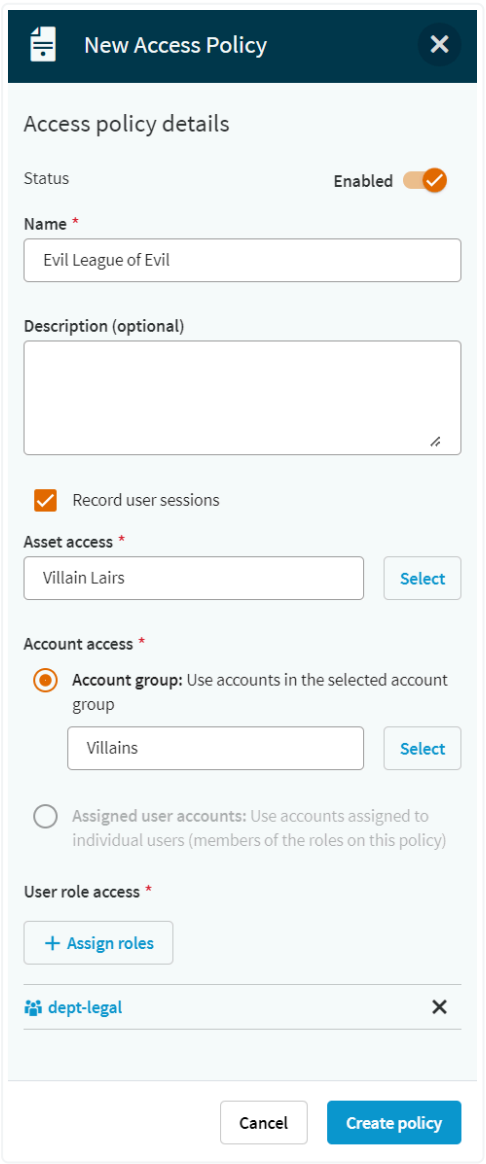
Assigning Access Policies

Go to **Access > Access Policies** to manage and assign the policies that allow your account groups to access the asset groups that you've configured.



To create a policy, click **+ New access policy** and configure the following details:

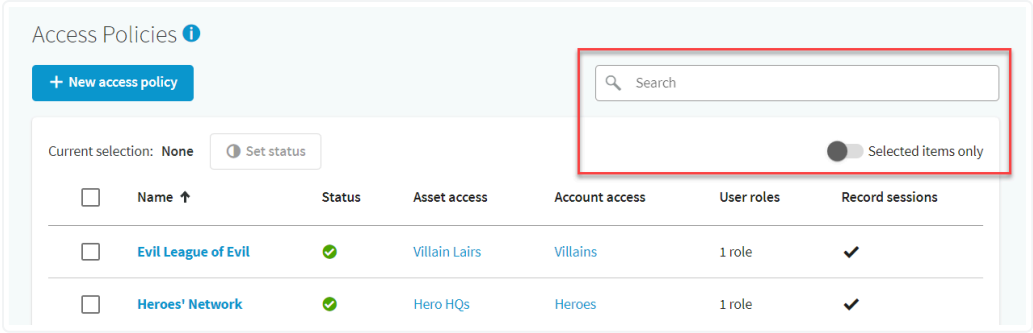
Status	Leave toggled on to enable the new policy immediately, or toggle off to leave the policy disabled at time of creation.
Name	Give the policy a unique and descriptive name.
Description	If desired, enter a detailed description for the policy.
Record user sessions	Leave enabled to save recordings of all user sessions enabled by this policy for future auditing.
Asset access	Select the asset groups that accounts assigned this policy may access.



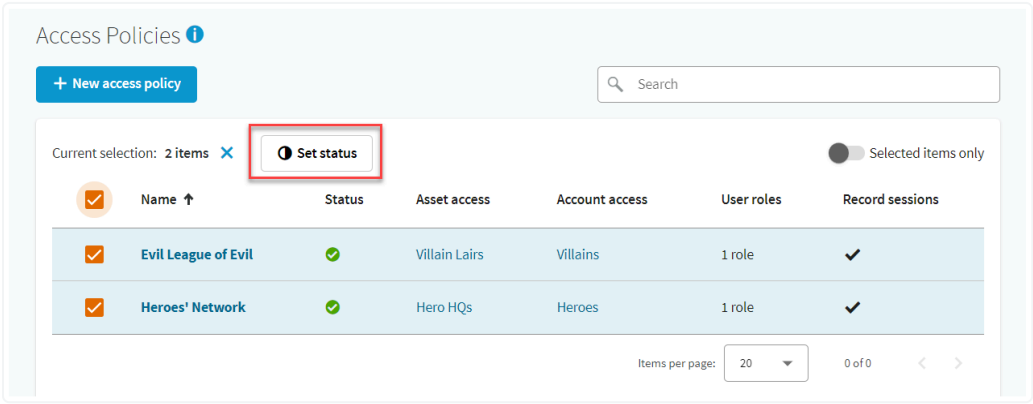
Account access	Select the account group containing the accounts who may access this policy's assets.
User role access	Select one or more OneLogin roles. Users who have been assigned at least one of these roles in OneLogin will see the assets and accounts assigned by this policy, provided that they have access to the PAM user portal and that the accounts assigned are compatible with the assets assigned.

Click **Create policy** to add the access policy to PAM Essentials.

If you have many policies to navigate, you can use the **Search** tool to filter them by name, or the **Selected items only** toggle to view only those policies you've manually selected.



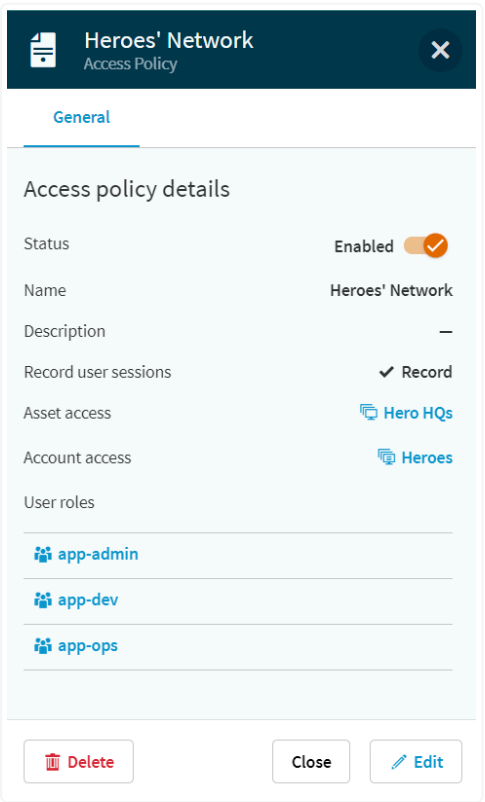
To quickly enable or disable multiple policies at once, select them and click **Set status**.



Click an access policy's name to enable or disable, edit, or remove it.

While the policy is enabled, users who have been assigned one or more of the selected OneLogin roles will have access to the selected assets and accounts via the PAM user portal.

If *Record user sessions* is enabled for the policy, assigned auditors and admins may view the session recordings in PAM Essentials.



> **Note:** Policies are automatically disabled if their asset group or account group is deleted, rendering the policy invalid. An administrator must update the policy with valid asset and account groups before re-enabling.