FORESCOUT

Forescout

eyeExtend for CyberArk

Configuration Guide

Version 1.4

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.Forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2020-11-12 09:59

Table of Contents

About the CyberArk Integration

Forescout eyeExtend for CyberArk® integrates with the CyberArk Privileged Account Security Solution.

Forescout integration with the CyberArk Privileged Account Security Solution eliminates the need for the Forescout platform to store privileged account credentials and allows highly sensitive credentials to be stored, logged, and managed by the CyberArk Enterprise Password Vault®.

This integration lets Forescout customers, who use CyberArk products, benefit from enhanced privileged account management and greater security.

These advantages include the enforcement of granular privileged access controls, automated workflows, and password rotation at regular intervals that do not require manual IT efforts, as well as enhanced security, auditing, and accountability.

The unique ability of the Forescout platform to discover privileged accounts and report them to CyberArk enhances the CyberArk solution for privileged account management by extending the visibility and coverage of managed accounts. The account discovery and reporting are available for Windows, Linux, and Mac OS endpoints.

CyberArk integration with Forescout provides Privileged Threat Analytics™ (PTA) Alerts that can be used by the Forescout platform to take policy-based mitigating actions on accounts or endpoints that display anomalous privileged activity, for example, isolating an endpoint reported by the CyberArk PTA Alert, so that no other machine can communicate with that endpoint.

Additional Benefits of the CyberArk Integration

Integration with the CyberArk Privileged Account Security Solution provides support for managing the credentials of Forescout users according to a defined CyberArk policy, enhancing the security of Forescout user accounts.

The Forescout platform is compatible with the CyberArk Privileged Session Manager (PSM) solution that keeps audit logs and video recordings of privileged account sessions, allowing accountability and auditing history for Forescout sessions in the CyberArk Vault.

Supported Forescout Platform Version

The following table lists the Forescout platform version that works with each version covered by this guide.

Version	Forescout Platform Version
1.4.0	Minimum version: 8.1.4

About Certification Compliance Mode

Forescout eyeExtend for CyberArk supports Certification Compliance mode. For information about this mode, refer to "Certification Compliance" in the *Forescout Installation Guide.*

Use Cases

This section describes important use cases supported by Forescout eyeExtend for CyberArk. To understand how this module helps you achieve these goals, see About the eyeExtend for CyberArk Module. Be sure to review the Best Practices for Working with CyberArk.

Credential Retrieval from CyberArk Enterprise Password Vault

The Forescout platform supports privileged access management through the CyberArk Application Identity Manager™ (AIM). By integrating the CyberArk Application Credential Provider, highly sensitive credentials can be retrieved from the CyberArk Vault by a credential retrieval service. Privileged account credentials are requested on a per-use basis without storing them in the Forescout system. This integration enhances the security of the sensitive credentials, as they are only stored in the CyberArk Vault. Examples that use the credential retrieval service are the HPS Inspection Engine and the Switch Plugin.

Discover and Report Local Privileged Accounts

The Forescout platform detection capabilities enable the discovery of new devices and accounts, and in particular local privileged accounts. All managed Windows, Linux, and Mac OS endpoints are scanned, and the discovered privileged accounts are reported to CyberArk via an API and stored in the CyberArk Vault Pending Account list. This enhances CyberArk's ability to be aware of and manage privileged accounts.

Discover and Report Assets

The Forescout platform detection capabilities enable the discovery of new assets. Assets whose admin accounts cannot be resolved (for example: IoT, OT, network gear) are reported to CyberArk via an API and stored in the CyberArk Vault Pending Account list. This enhances CyberArk's ability to be aware of and manage privileged accounts on such assets.

Receive Privileged Threat Analytics Alerts

The Forescout platform can respond to alerts from CyberArk Privileged Threat Analytics (PTA) that notify of suspicious behavior or malicious activity in privileged accounts on the network. The Forescout platform can act upon each incidence according to criteria and actions set in policies.

About the eyeExtend for CyberArk Module

Forescout eyeExtend for CyberArk lets you:

- Gain access to endpoints without saving or managing the login credentials locally. The credentials are managed and provided on demand by the CyberArk Enterprise Password Vault. See Configure the Module for Credential Retrieval for details.
- React in real-time to threats reported by the CyberArk PTA with actions defined by Forescout platform policies. See Create a CyberArk PTA Alert Policy for details.

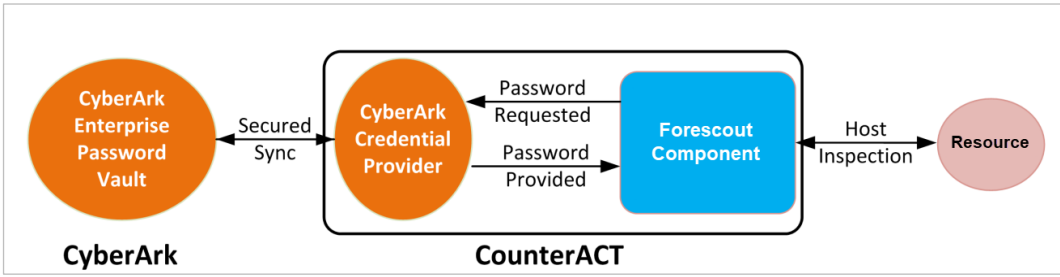
- Enhance CyberArk visibility and monitoring of privileged accounts on Windows, Linux, and Mac OS endpoints. See Create a Report Accounts to CyberArk Vault Windows Policy, Create a Report Accounts to CyberArk Vault Linux Policy, and Create a Report Accounts to CyberArk Vault MacOS Policy.
- Report assets to the CyberArk Vault. See Create a Report Assets to CyberArk Vault Policy.

To use the different features of this module, you should have a solid understanding of the CyberArk Privileged Account Security Solution and the functionality and terminology of the CyberArk Enterprise Password Vault.

Architecture

The basic architecture of the Forescout integration with CyberArk consists of:

- The CyberArk Enterprise Password Vault, where privileged account credentials are stored and managed.
- A Forescout component, that wants to perform an action that requires privileged access, for example, to remote inspect a Windows endpoint.
- The CyberArk Credential Provider, which communicates with the credential retrieval service and with the CyberArk Enterprise Password Vault to provide privileged account credentials on a per-use basis.



- CyberArk Pending Account Security Web Service and complementary SDK/API, which allows an external privilege account scanner (such as the Forescout platform) that identifies an unmanaged privileged account, to add it to the CyberArk Vault.
- CyberArk Privileged Threat Analytics (PTA), which sends detected security events to the Forescout platform as syslog messages. The PTA messages are received by the Forescout Core Extensions Module: Syslog Plugin and can be acted upon according to specifically defined Forescout platform policies.

How It Works

The integration of CyberArk with Forescout enables communication and collaboration between the two systems and enables the processes described below.

Retrieve Credentials

Whenever a Forescout component requires credentials to access a resource, the component will query the CyberArk Enterprise Password Vault. The Vault provides the needed domain credentials through the Credential Provider, which is integrated into each CounterACT® Appliance. The credentials are used to authorize access

without saving them locally or at any point along the way between the Vault and the resource.

Discover and Report Local Privileged Accounts

Forescout endpoint detection and inspection can discover privileged accounts on endpoints where CyberArk has no visibility. The Forescout platform sends lists of the newly discovered privileged accounts, and CyberArk adds them to a list of pending privileged accounts that are to be reviewed and approved by a CyberArk operator.

Discover and Report Assets

Forescout discovers and classifies all assets on the network. Assets whose admin accounts cannot be resolved (for example: IoT, OT, network gear) are reported to CyberArk via an API and stored in the CyberArk Vault Pending Account list (with a predefined user). A CyberArk operator can create onboarding workflows for the newly reported assets.

Receive Privileged Threat Analytics Alerts

CyberArk Privileged Threat Analytics (PTA) monitors the activities of privileged accounts on the network, and reports any anomalous behavior that may be a security threat by sending PTA Alerts. The PTA Alerts are received by the Forescout platform and the related endpoints are assigned to a Forescout group. The threat information related to an endpoint is processed and Forescout actions can be defined in the policy to handle the endpoint. For example, to block, isolate, or remediate the endpoint, or notify the security authority.

How to Work with eyeExtend for CyberArk

This topic describes how to work with the module and module requirements.

What to Do

Perform the following steps to set up the integration:

1. Verify that all requirements are met. See Module Requirements.
2. Review the Best Practices for Working with CyberArk.
3. Install the eyeExtend for CyberArk Module.
4. Configure the eyeExtend for CyberArk Module.
5. Create CyberArk Policies.

Module Requirements

Verify that the following requirements are met:

- Forescout Requirements
- Supported Vendor Requirements
- Networking Requirements
- Endpoint Requirements

Forescout Requirements

This module requires the following Forescout components:

- A module license for Forescout eyeExtend for CyberArk. See Forescout eyeExtend (Extended Module) Licensing Requirements.
- Endpoint Module with the HPS Inspection Engine running or Network Module with the Switch Plugin running.
- Core Extension Module with the Syslog Plugin running.
- (Optional) Endpoint Module with the Linux Plugin and/or the OS X Plugin running with the following hotfix versions required for Forescout 8.1.4:
  - Linux version 1.4.3.1073
  - OS X version 2.2.3.1091

About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this eyeExtend module.*** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this eyeExtend module.

Supported Vendor Requirements

The module uses and works with the following CyberArk Privileged Account Security Solution components:

- CyberArk Enterprise Password Vault®
- CyberArk Password Vault Web Access®
- CyberArk AIM®
- CyberArk PTA™
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

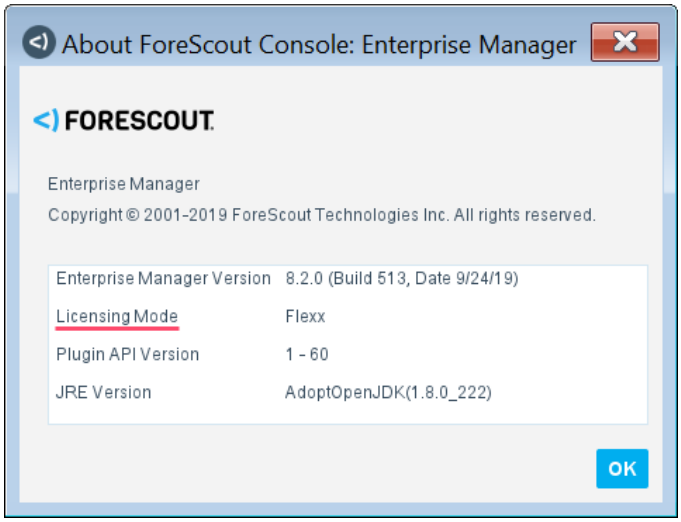
Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.



Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

Demo license extension requests and permanent license requests are made from the Console.

> *This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.*

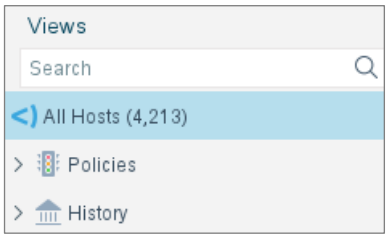
Requesting a License

When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the **Devices** pane of the Module License Request wizard, in the Console Modules pane.

To view the number of currently detected devices:

1. Select the **Home** tab.
2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.



Flexx Licensing Mode

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend modules. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend modules. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

- *No demo license is automatically installed during system installation.*

License entitlements are managed in the Forescout Customer Portal. After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.

- *Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend modules, packaging individual licensed modules are supported.* The eyeExtend Connect Module is an *eyeExtend* module even though it packages more than one module.

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing**. Refer to the *Forescout Administration Guide*.
- **Flexx Licensing**. Refer to the *Flexx Licensing How-to Guide*.

You can also contact your Forescout sales representative for more information.

Networking Requirements

The following ports must be open on enterprise firewalls to support communication between the Forescout platform and the CyberArk server:

- TCP 443 – The default port for communicating with the Pending Account Security Web Service.
- UDP 514 – The default listening port for the Syslog Plugin, this should also be configured on the CyberArk server as the sending port.
- TCP 1858 – The default port used by the CyberArk Credential Provider to communicate with the CyberArk Vault.

Endpoint Requirements

For credential retrieval, the endpoints to be handled must be manageable by a Forescout component such as the HPS Inspection Engine or the Switch Plugin.

Install the eyeExtend for CyberArk Module

This topic describes how to install the module.

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - ***Per-Appliance Licensing Mode***
   - Customer Portal, Downloads Page - ***Flexx Licensing Mode***

   To identify your licensing mode, select **Help > About ForeScout** from the Console.
2. Download the module `.fpi` file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module `.fpi` file.
8. Select **Install**. The Installation screen opens.

9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

   - *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*
   - *In modules that contain more than one component, the installation proceeds automatically one component at a time.*

10. When the installation completes, select **Close** to close the window. The installed module is displayed in the Modules pane.

    - *Some components are not automatically started following installation.*

Configure the eyeExtend for CyberArk Module

After Forescout eyeExtend for CyberArk is installed, configure the module as follows:

- Configure the Module for Credential Retrieval
- Configure the Module to Report Discovered Privileged Accounts
- Configure the Module to Receive PTA Alerts
- Configure User Groups for eyeExtend for CyberArk

Configuration Steps

There are four configuration steps:

1. Define CounterACT Application ID. See CounterACT Application ID.
2. Configure CounterACT Appliances.
3. Add CounterACT Appliance users' membership to safe(s).
4. Add Vault user to credential provider.

Configure the Module for Credential Retrieval

Configure the module to enable the Forescout platform to accomplish the following:

- Communicate with the CyberArk Enterprise Password Vault using the CyberArk Credential Provider installed in a CounterACT device.
- Query the Vault to receive credentials from a credential retrieval service.

To configure the module for credential retrieval, perform the following tasks in the order specified:

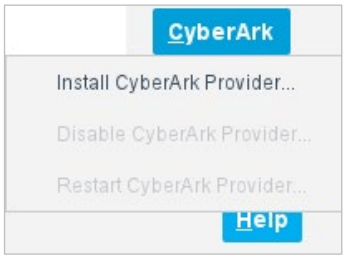
- Install the CyberArk Credential Provider on CounterACT Devices
- Define the CyberArk Enterprise Password Vault Query
- Configure Users in the CyberArk Vault

Install the CyberArk Credential Provider on CounterACT Devices

Each CounterACT Appliance retrieving passwords from the CyberArk Vault must be installed with a CyberArk Credential Provider and use one of the license instances provisioned in your CyberArk service. It is recommended to verify that you have enough licenses in your CyberArk Enterprise Password Vault for the number of Appliances you want to configure.

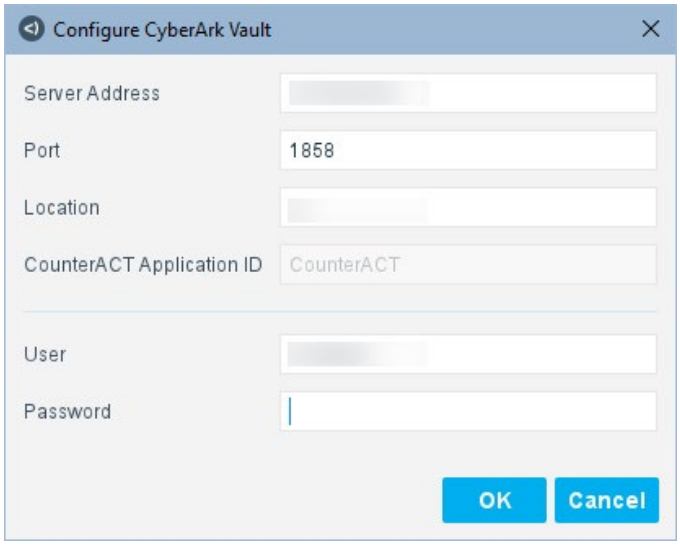
To install the CyberArk Credential Provider:

1. In the Console, select **Options** from the Tools menu, and then select **CounterACT Devices**.
2. Select the CounterACT devices to be configured, scroll to the right, and select **CyberArk** and then select **Install CyberArk Provider**.



3. When prompted for confirmation in the Enterprise Manager Console, select **Yes**.

You can select more than one device at a time. The installation process automatically installs a Provider instance for each CounterACT device.



4. Configure the following settings:

Server Address	Enter the address of the CyberArk Vault server. To access the CyberArk Vault in High Availability or Disaster Recovery scenarios, you can enter more than one IP address, using commas to separate the entries.
Port	Enter the default port (1858) for communication with the CyberArk Vault server.
Location	Enter the name of the Location in the Vault to which the CounterACT device is assigned. If the Location name is not defined, a new one is created. Make sure that the CounterACT device has not already been assigned to this Location.
CounterACT Application ID	The default name used for creating a new user in the CyberArk Vault.
User	Enter the user name for logging in to the Vault. See Set Minimal Permissions for Vault User.
Password	Enter the password for logging in to the Vault.

The CyberArk Vault password used to install the CyberArk Credential Provider is used only during the installation stage. It is not saved by the Forescout platform.

5. Select **OK** to save the configuration.
6. Select **Close**.

Create an Application on the PVWA

To ensure that the CyberArk and PrivateArk integration is successful, create an application on the Password Vault Web Access (PVWA).

To create an application on the Password Vault Web Access:

1. Create an Application on Password Vault Web Access by providing Application name (counteract) and Location (if needed).
2. Add Enterprise Manager and Appliance IP Addresses to the Allowed Machines.

   The application is added to the Vault in the PrivateArk.

Set Minimal Permissions for Vault User

Instead of providing Vault Administrator credentials to configure a connection, you can use a less privileged Vault user.

In the CyberArk Vault, set the following User Rights under **Users and Groups on Server Vault**:

- Add Safes
- Audit Users
- Add/Update Users

Define the CyberArk Enterprise Password Vault Query

To configure the Forescout component to query the CyberArk Vault whenever it needs credentials to access, refer to the component's corresponding Configuration Guide.

Configure Users in the CyberArk Vault

When the CyberArk Credential Provider is installed, a new CyberArk Vault *User* is created for each Appliance that is configured with the Provider. Before the Provider can retrieve passwords from the Vault, each new User must be assigned ownership to a safe or safes, and to have *Authorizations* defined for that ownership (for example, *Monitor Safe*, *Retrieve files from Safe*, or *Store files in Safe*).

The following is a general procedure. Refer to the CyberArk documentation for details.

To define safe ownership in the Vault:

1. Log in to the PVWA as administrator.
2. On the left-hand side, select **Policies > Access Control (Safes)**.
3. Select a safe in which to add a member.
4. On the right-hand side, select **Members**.
5. Below the Members tab, select **Add Member**.
6. Search the Vault for *Counteract_<ip_address>* user and *counteract* user.
7. Select only **Retrieve accounts** and **List accounts** for the member (and deselect other checkboxes).
8. Select **Add**. Repeat steps 6 and 7 for another user.
9. Select **Close**.

Configure the Module to Report Discovered Privileged Accounts

This topic describes how to configure the module to report changes in privileged accounts or newly discovered privileged accounts to CyberArk.

The CyberArk Vault provides an API to a Pending Account Security Web Service. The web service enables an external privileged account scanner to report privileged accounts that are not managed by the CyberArk Vault, and to add them to the Vault through the CyberArk privileged account workflow as follows:

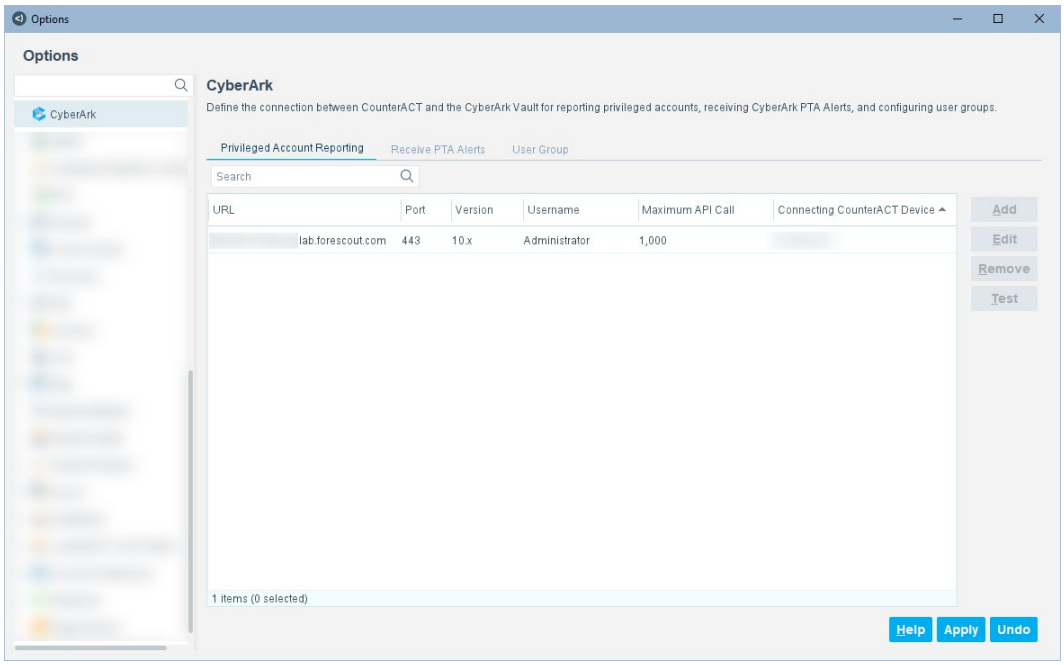
- An unmanaged privileged account is reported to the web service, and labeled as *Pending*
- The Pending account is *On Boarded* to the Vault by a Vault Admin
- The privileged account is now *managed* by the Vault.

For more information, refer to the CyberArk documentation for the *Pending Account Security Web Service*.

Forescout eyeExtend for CyberArk only communicates over HTTPS. Make sure that the web binding in the CyberArk installation is configured to use HTTPS for all services involved in logging into the server and receiving reports of privileged accounts.

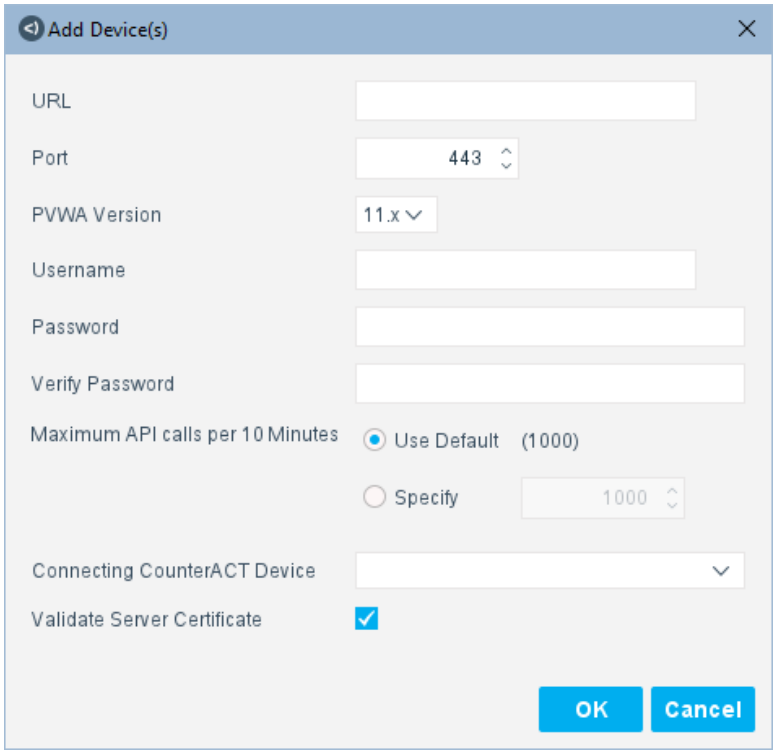
To configure the module to report privileged accounts:

1. In the Console, select **Options** from the **Tools** menu, and then select **Modules**.
2. In the Modules pane, select **CyberArk** and then select **Configure**.



By default, the Privileged Account Reporting tab is selected.

3. Select **Add**.



4. Configure the device settings as follows:

URL	Enter the domain portion of the URL of the server's address (FQDN), for example, console.cyberark.local. The rest of the URL is hard-coded and provided by default by Password Vault Web Access (PVWA).
Port	Enter the default port (443) for communicating with the Pending Account Security Web Service.
PVWA Version	Select the version of the Password Vault Web Access, either 10.x or 11.x.
Username	Enter the user name needed to log in to the Pending Account Security Web Service.
Password	Enter the password needed to log in to the Pending Account Security Web Service.
Verify Password	Re-enter the password to verify it.
Maximum API calls per 10 minutes	Select **Use Default (1000)** or select **Specify** to set a different maximum value.
Connecting CounterACT Device	Select a connecting CounterACT device from the list. This is the device that reports the newly discovered or changed accounts.

Validate Server Certificate	Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend module communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed: ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*.

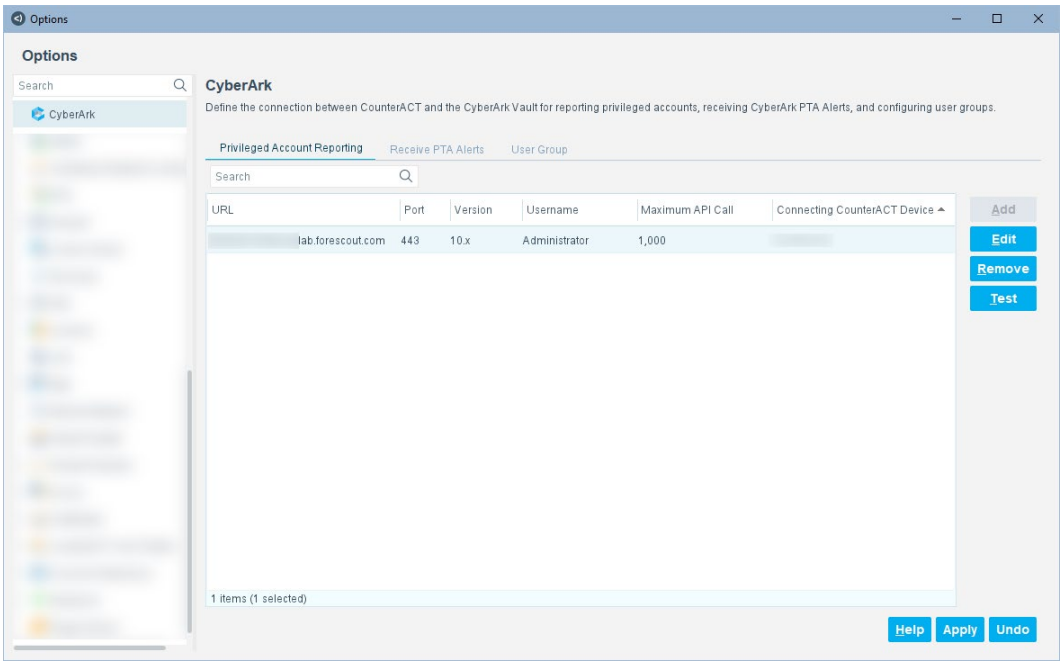
5. Select **OK** to save the configuration.
6. Select **Apply** to save the configuration.

Test a Connection

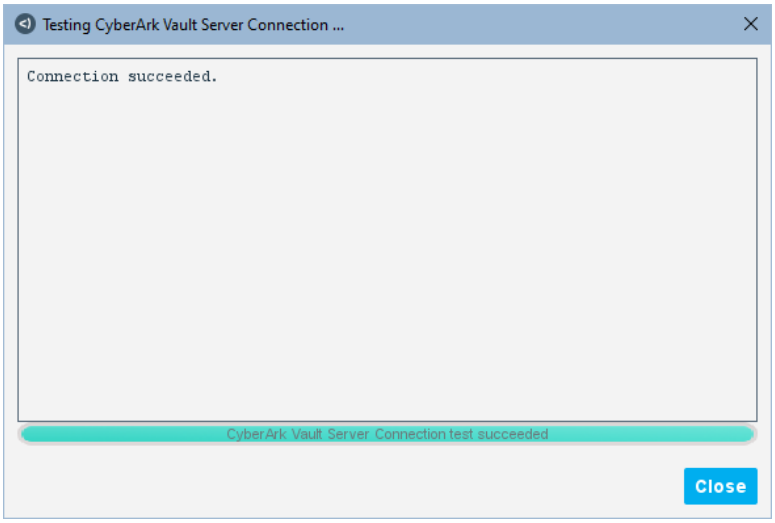
The best practice is to perform a test after setting up a connection.

To test a connection:

1. In the Privileged Account Reporting tab, select the configured connection to enable **Test**.



2. Select **Test**.



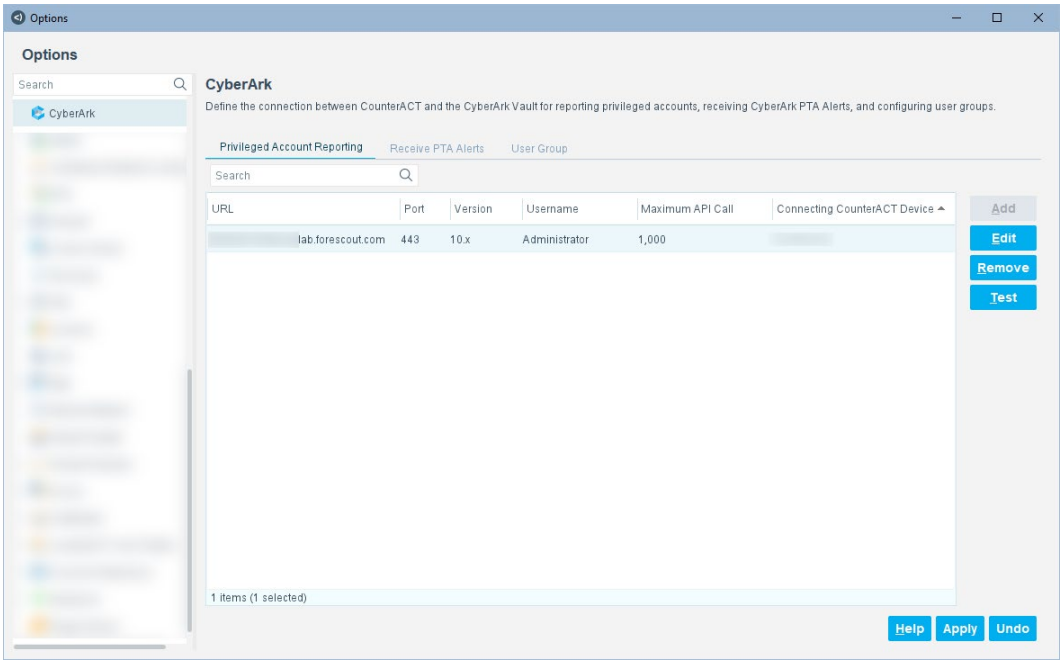
3. Select **Close**.

Edit a Connection

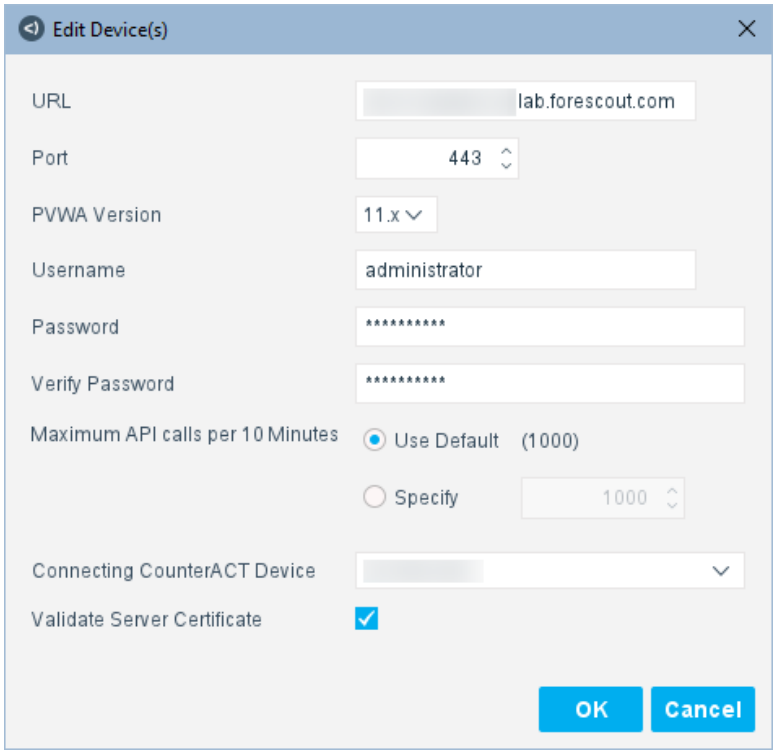
You can edit a configured connection.

To edit a connection:

1. In the Privileged Account Reporting tab, select the configured connection to enable **Edit**.



2. Select **Edit**.



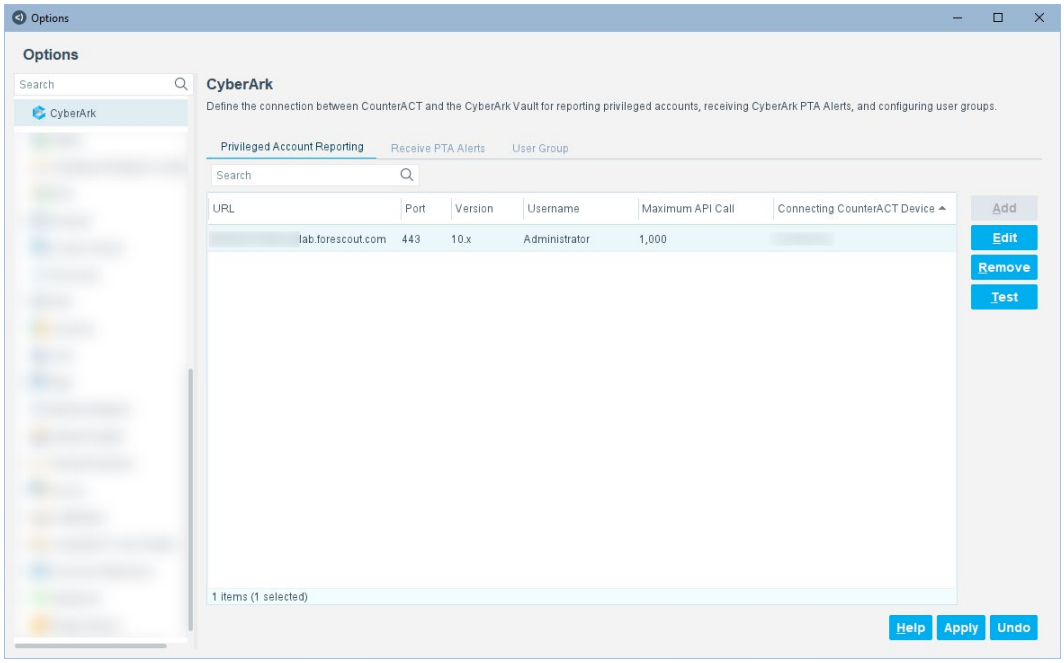
3. Make your changes and select **OK**.
4. Select **Apply** to save the configuration.

Remove a Connection

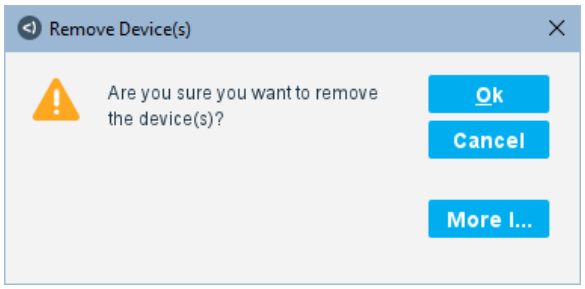
You can remove a connection after setting it up.

To remove a connection:

1. In the Privileged Account Reporting tab, select the configured connection to enable **Remove**.



2. Select **Remove**. You can select **More Info** to get more information.



3. Select **OK**.
4. Select **Apply** to save the configuration.

Configure the Module to Receive PTA Alerts

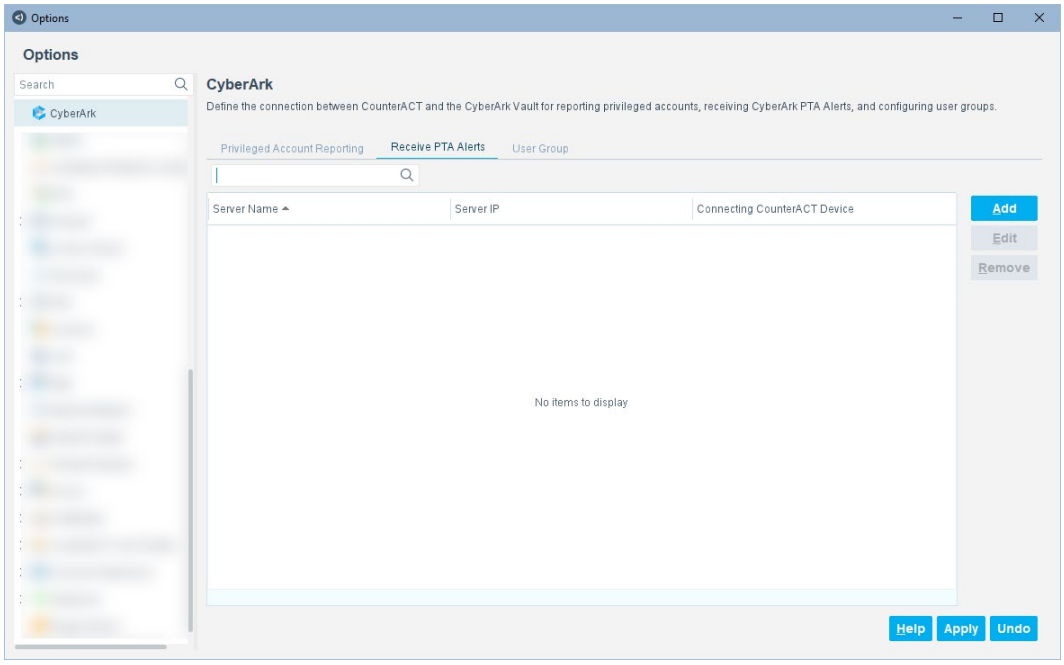
This topic describes how to configure the module to receive event alerts from the CyberArk PTA. You can create Forescout platform policies that apply actions based on the information in a PTA Alert. See Create a CyberArk PTA Alert Policy.

To configure PTA alerts:

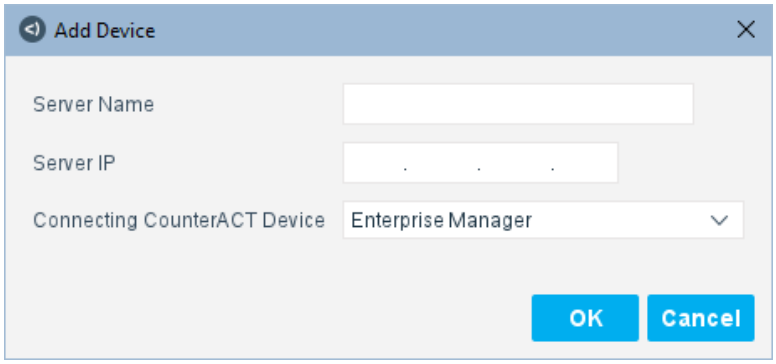
1. Before configuring Forescout eyeExtend for CyberArk, you must configure the CyberArk PTA server to send Syslog messages from a UDP port, the default port is UDP 514.

If you need to use a different port from the default, configure it in the Options > Modules > Syslog > Configure *pane.*

2. In the Console, select **Options** from the **Tools** menu, and then select **Modules**.
3. In the **Modules** pane, select **CyberArk** and then select **Configure**.
4. Select the Receive PTA Alerts tab.



5. Select **Add**.



6. Configure the settings as follows:

Server Name	Enter a name to identify this server.
Server IP	Enter the IP address of the PTA Alert source.
Connecting CounterACT device	Select the CounterACT device that receives the PTA Alert.

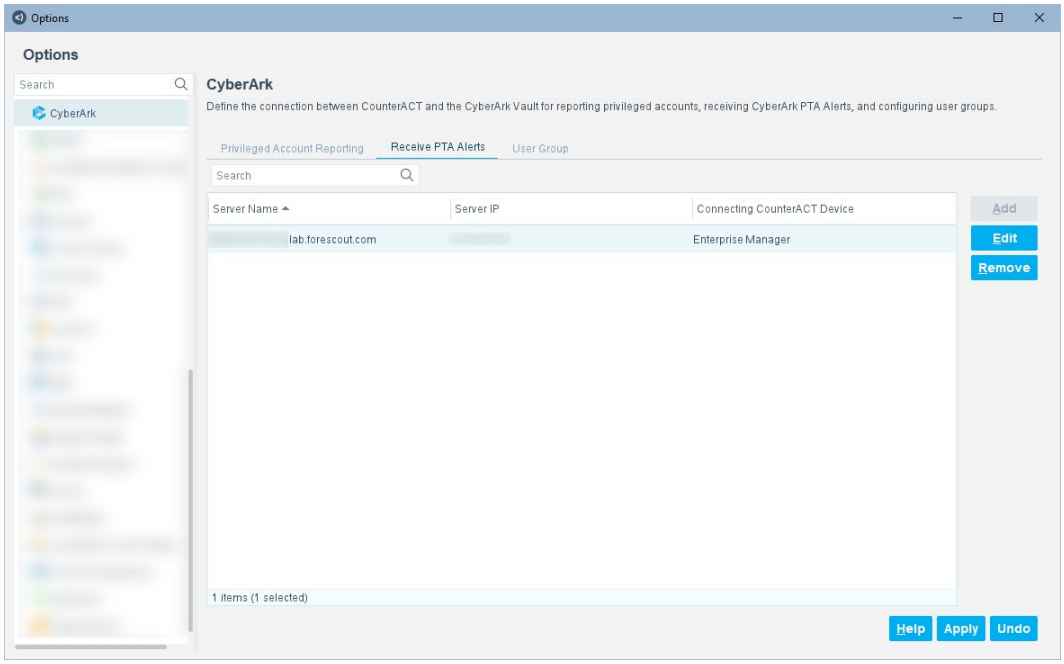
7. Select **OK**.
8. Select **Apply** to save the configuration.

Edit the Receive PTA Alerts

You can edit the configured Receive PTA Alerts.

To edit the Receive PTA Alerts:

1. In the Receive PTA Alerts tab, select the configuration to enable **Edit**.



2. Select **Edit**.

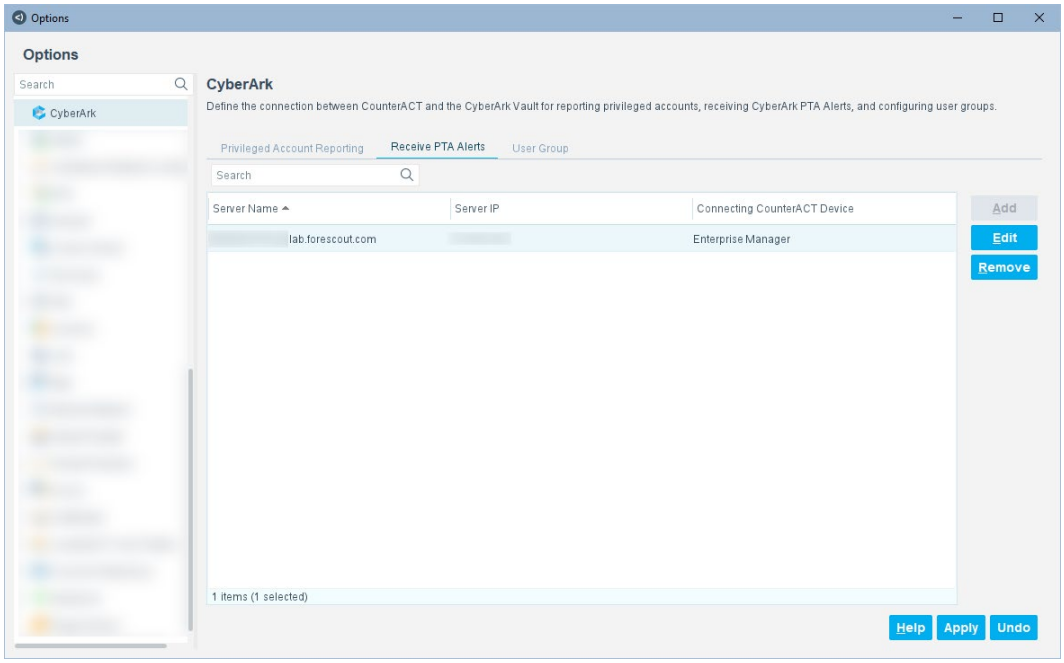
3. Make your changes and select **OK**.
4. Select **Apply** to save the configuration.

Remove the Receive PTA Alerts

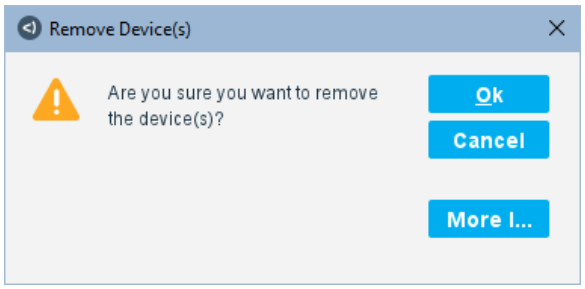
You can remove the configured Receive PTA Alerts.

To remove the Receive PTA Alerts:

1. In the Receive PTA Alerts tab, select the configuration to enable **Remove**.



2. Select **Remove**. You can select **More Info** to get more information.



3. Select **OK**.
4. Select **Apply** to save the configuration.

Configure User Groups for eyeExtend for CyberArk

You can configure user groups for Windows, Linux, or Mac OS. You can use configured groups to discover accounts. Several default groups are provided.

You add user groups based on the OS type, which is used to discover the privileged users of that group for each endpoint.

Default groups for Windows are:

- Administrators
- Power Users
- Backup Operators

- Cryptographic Operators
- Distributed COM Users

Default groups for Linux are:

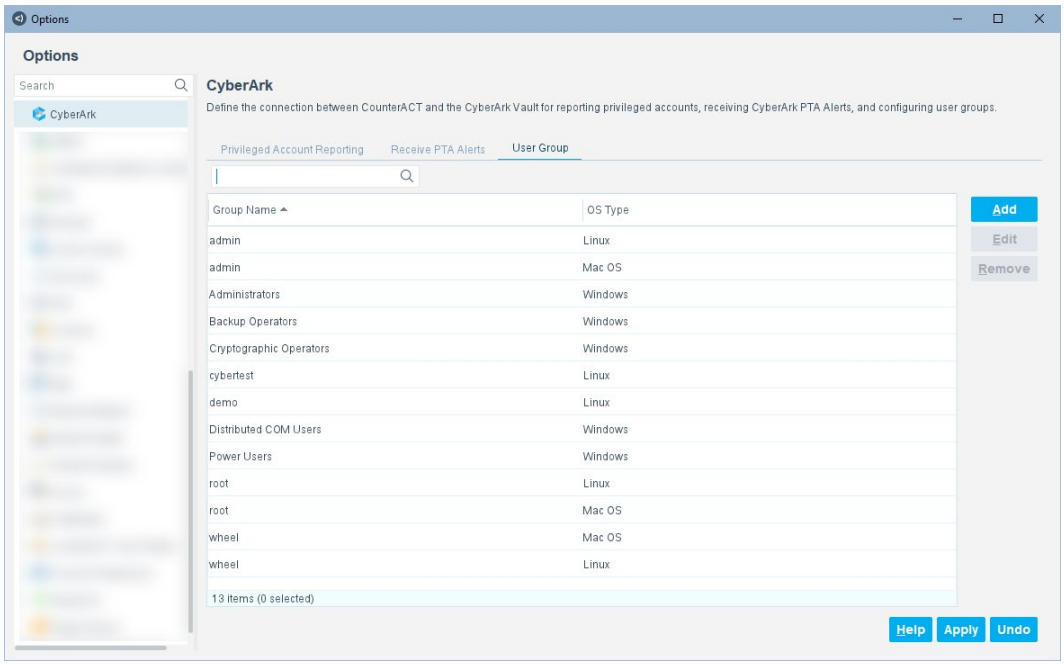
- root
- admin
- wheel

Default groups for Mac OS are:

- root
- admin
- wheel

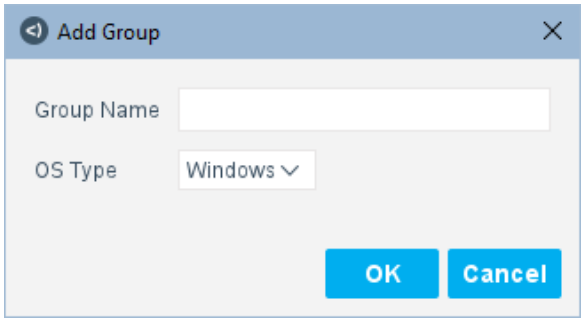
To configure user groups:

1. In the Console, select **Options** from the **Tools** menu, and then select **Modules**.
2. In the **Modules** pane, select **CyberArk** and then select **Configure**.
3. Select the User Group tab.



In the User Group tab, default groups as well as configured groups are displayed.

4. Select **Add**.



5. Configure the settings as follows:

Group Name	Enter a name to identify the group. For Windows, the name can have a maximum of 256 ASCII characters and numbers. The following special characters can also be used in the name: ▪ !, #, $, %, ^, &, (,), _, -, {, }, and . For Linux, the name can have a maximum of 32 ASCII characters and numbers. The following special characters can also be used in the name: ▪ -, _, $, and . For Mac OS, the name can have a maximum of 32 ASCII characters and numbers. The following special characters can also be used in the name: ▪ -, _, and .
OS Type	Select the operating system to which the group belongs: Windows, Linux, or Mac OS.

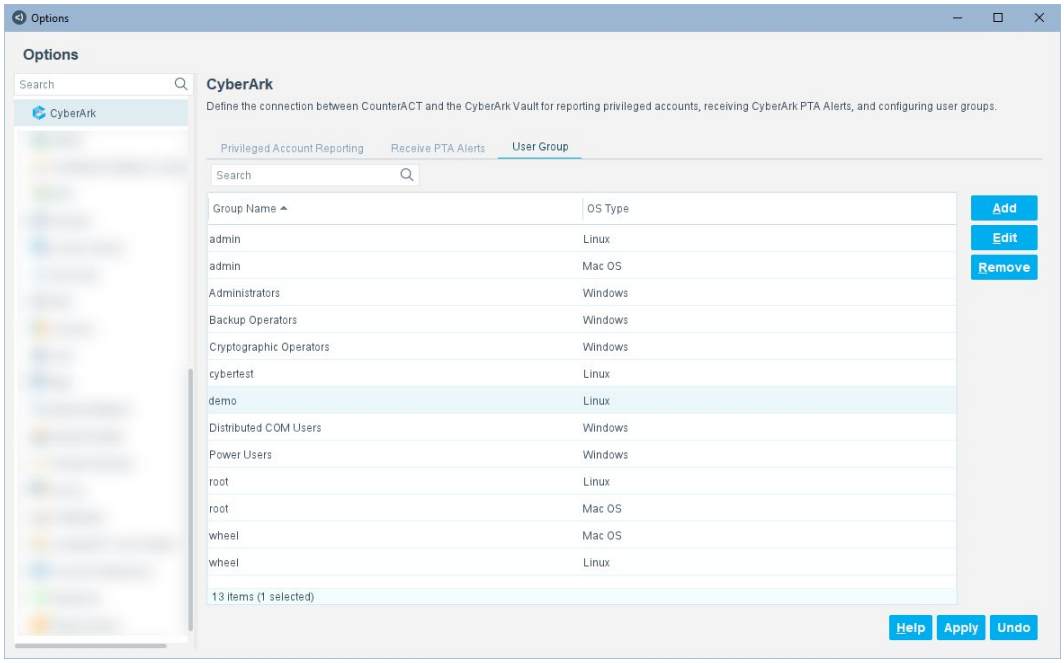
6. Select **OK**.
7. Select **Apply** to save the configuration.

Edit User Groups

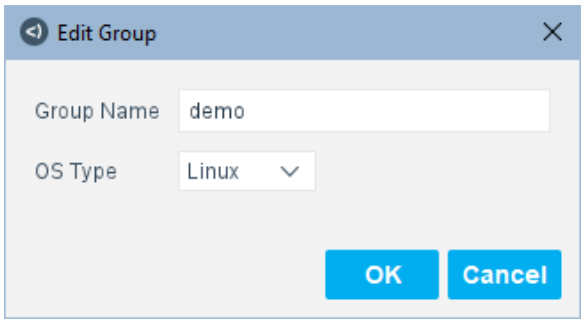
You can only edit configured user groups. Default user groups cannot be edited.

To edit user groups:

1. In the User Group tab, select a configured user group to enable **Edit**.



2. Select **Edit**.



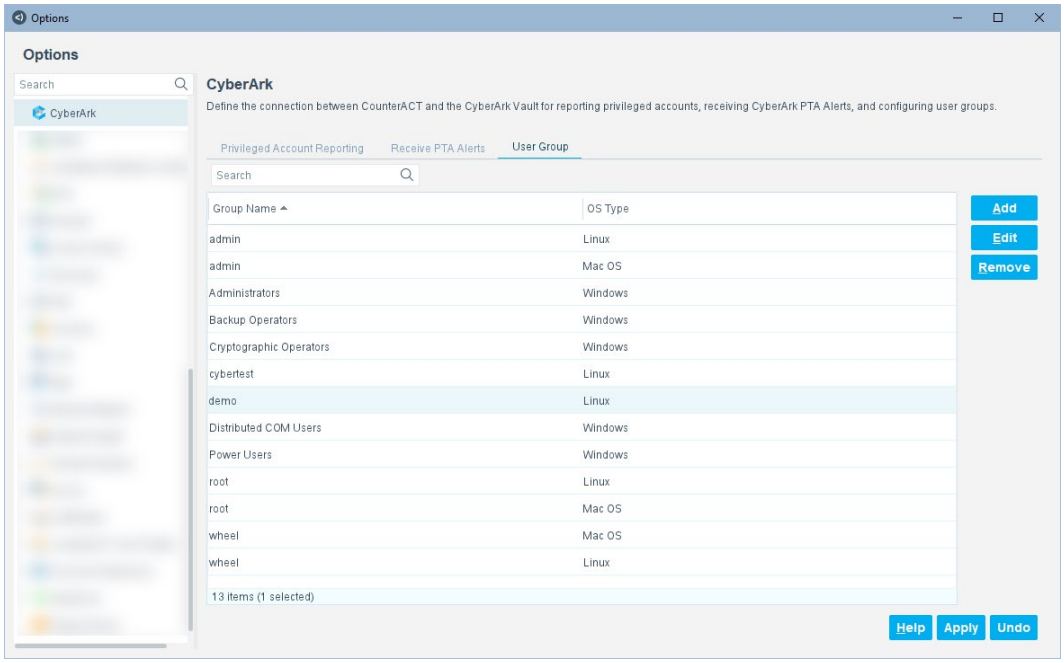
3. Edit the group and select **OK**.
4. Select **Apply** to save the configuration.

Remove User Groups

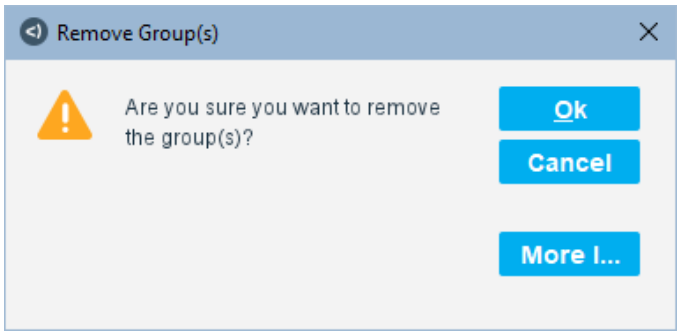
You can only remove configured user groups. Default user groups cannot be removed.

To remove user groups:

1. In the User Group tab, select a configured user group to enable **Remove**.



2. Select **Remove**. You can select **More Info** to get more information.



3. Select **OK**.
4. Select **Apply** to save the configuration.

Create CyberArk Policies

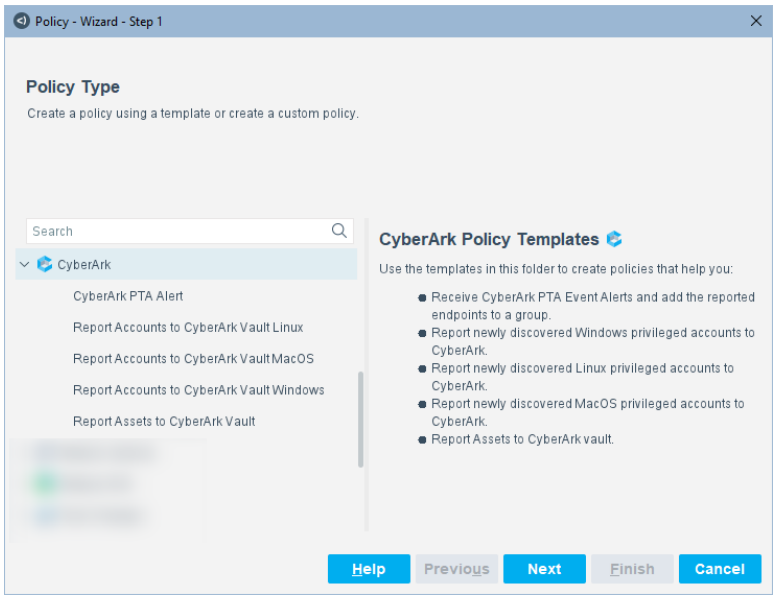
Forescout templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

Predefined actions – instructions regarding how to handle endpoints – are generally disabled by default when working with templates. You should only enable actions after testing and fine-tuning the policy.

The CyberArk policy templates generate the following Forescout platform policies:

- Create a CyberArk PTA Alert Policy
- Create a Report Accounts to CyberArk Vault Windows Policy

- Create a Report Accounts to CyberArk Vault Linux Policy
- Create a Report Accounts to CyberArk Vault MacOS Policy
- Create a Report Assets to CyberArk Vault Policy



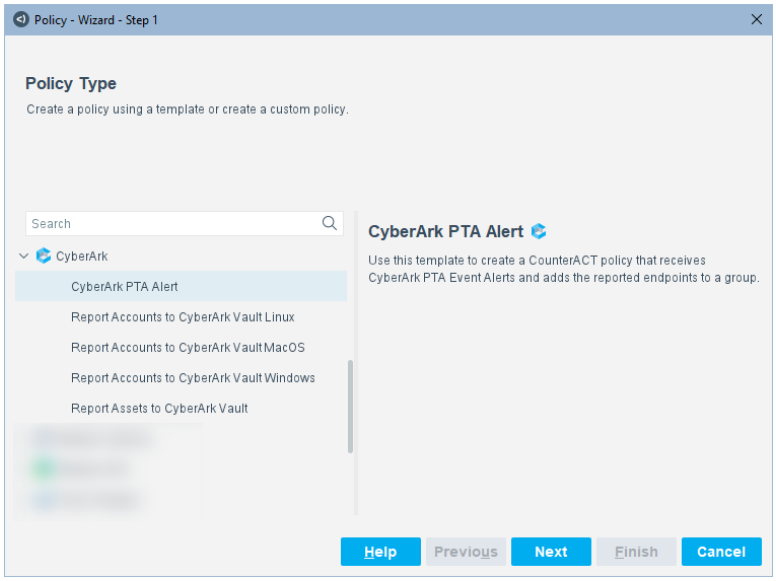
It is recommended that you have a basic understanding of Forescout platform policies before working with the templates. Refer to "Policy Templates" and "Working with the Policy Manager" in the Forescout Administration Guide.

Create a CyberArk PTA Alert Policy

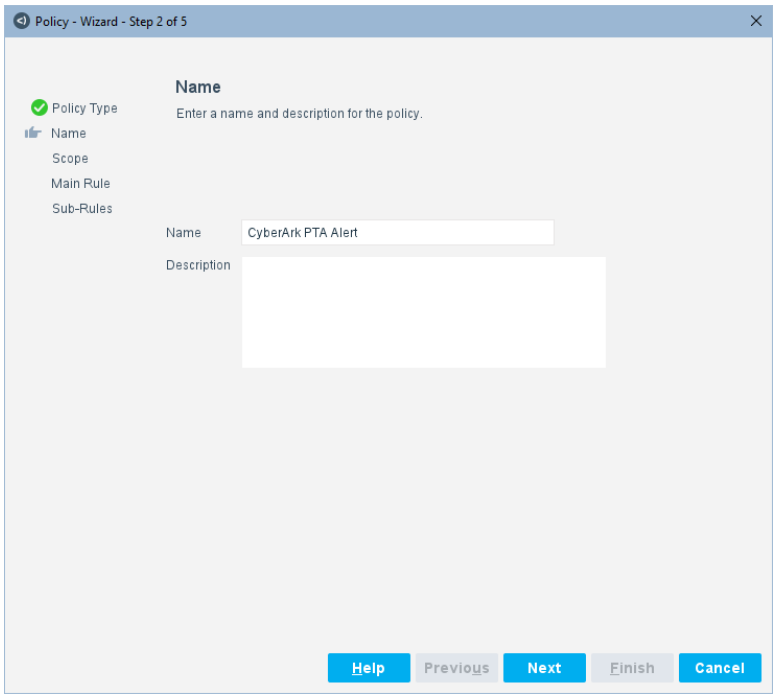
Use this template to create a policy for handling Privileged Threat Analytics Alerts that arrive from the CyberArk Vault, placing all reported endpoints in a pre-defined group.

To create a policy:

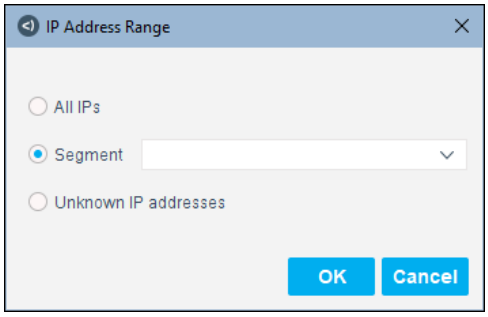
1. Log in to the Console and select **Policy**.
2. Select **Add** in the Policy Manager.
3. Expand the **CyberArk** folder and select **CyberArk PTA Alert**.



4. Select **Next**.



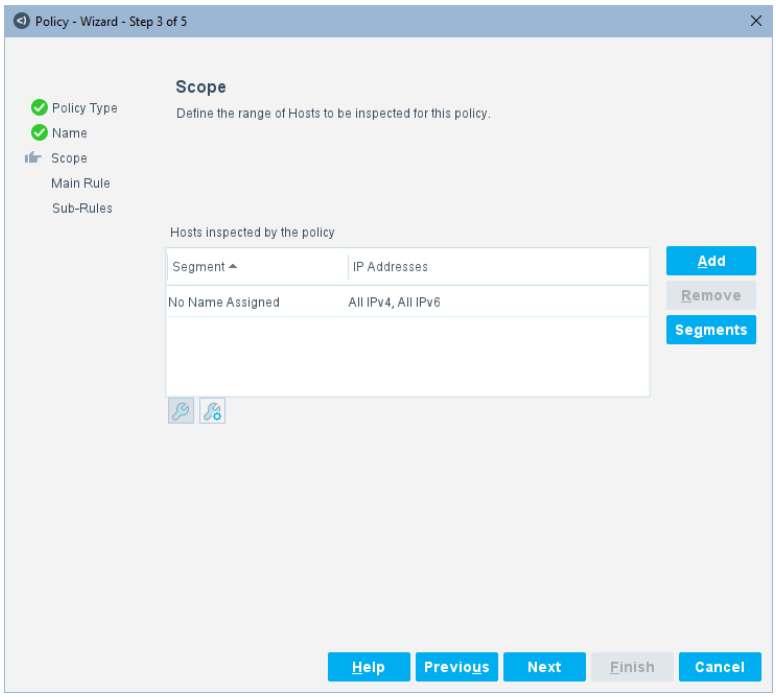
5. Enter a name and optionally add a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



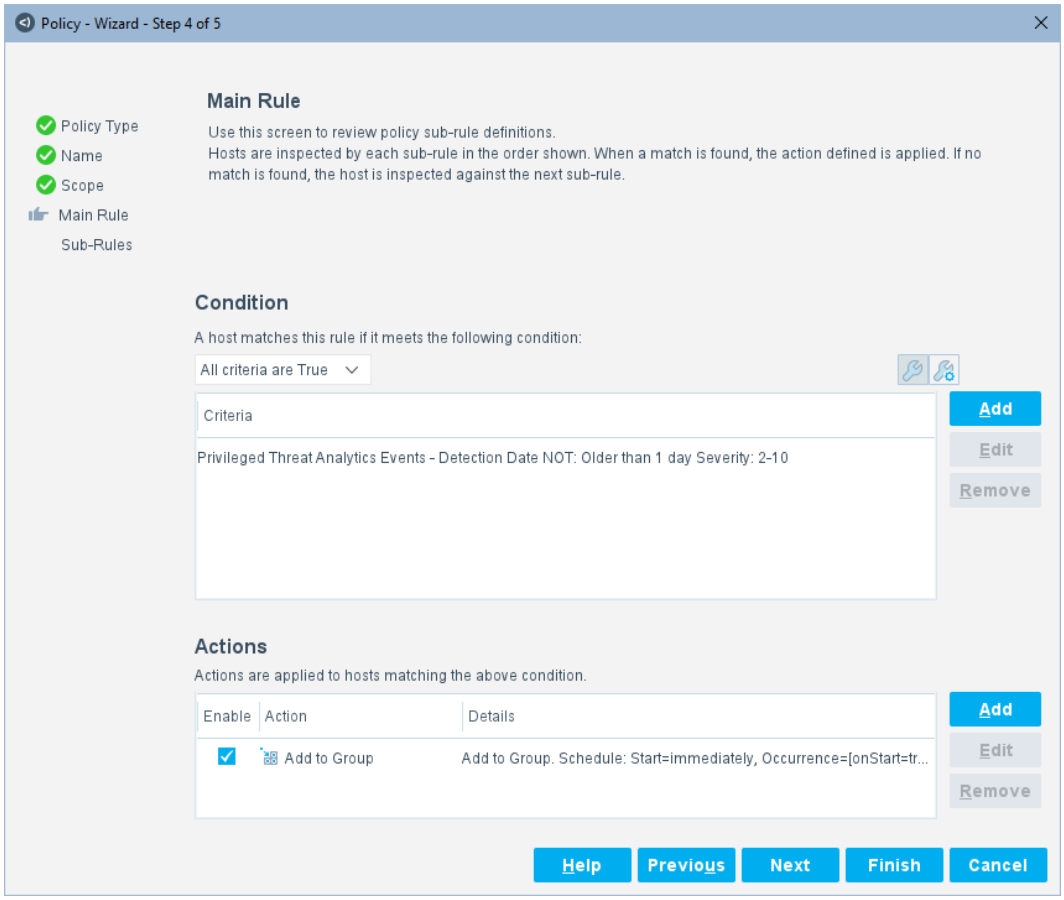
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.



9. Select **Next**.



The PTA Alert Main Rule contains the following default conditions for receiving Alerts:

- Detection date is no more than one day old.
- The Severity is between 2 and 10 (CyberArk defines event severity from 1-lowest to 10-highest).

The Action taken by this policy is to add reported endpoints that match the conditions to the Forescout group *CyberArk PTA Alert Endpoints*.

10. Predefined conditions and actions for the policy are displayed in the Main Rule pane. Select a condition or action and then select **Edit** to modify its settings.
11. To add another condition, select **Add** in Condition section.
12. To add another action, select **Add** in the Actions section.
13. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
14. Select **Finish**. The policy is created.
15. Select **Apply** to save the policy.

Use Information from PTA Alerts

PTA Alert information received by the Forescout platform can be utilized to trigger actions on endpoints that are flagged with potential threat indicators. In addition, PTA Alert information can be combined with existing endpoint properties detected by the Forescout platform, and used to add confidence in policy rules that act on an endpoint

The following security event classifications are provided by the CyberArk PTA Alerts:

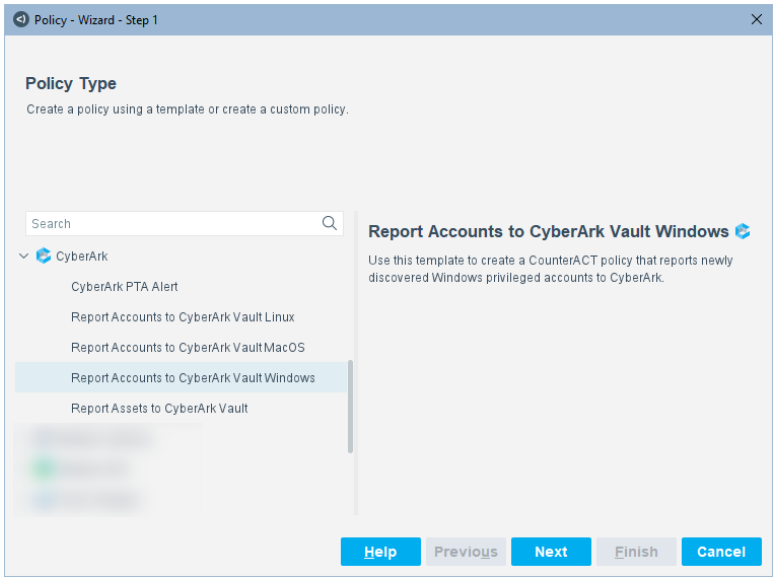
- **Suspected credential theft** – A group of suspicious activities that imply an attempt to steal credentials. For instance, a user who connects to a remote machine with a privileged account that is managed in the Vault, without retrieving the credentials beforehand.
- **Unmanaged privileged account** – A group of activities that imply that privileged accounts are not properly managed.
- **Suspicious behavior of Vault user** – A group of suspicious activities performed by a Vault user. For example, retrieving passwords from the Vault excessively.
- **Suspicious behavior of a machine** – A group of suspicious activities associated with an individual machine in the network. For instance, a machine that is accessed by an irregular source.
- **Suspicious behavior of user** – A group of suspicious activities associated with an individual user in the network. For instance, a user who accesses an unusual target machine for this user.

Create a Report Accounts to CyberArk Vault Windows Policy

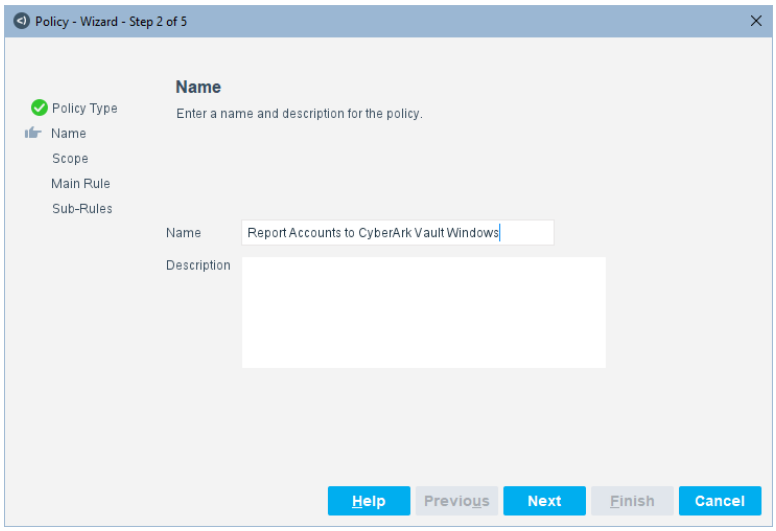
Use this template to create a policy to report privileged accounts on Windows endpoints that are not managed or listed by CyberArk.

To create a policy:

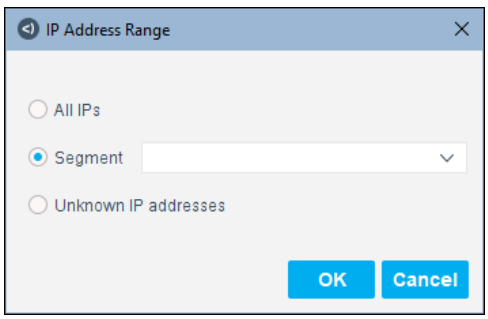
1. Log in to the Console and select **Policy**.
2. Select **Add** in the Policy Manager.
3. Expand the **CyberArk** folder and select **Report Accounts to CyberArk Vault Windows**.



4. Select **Next**.



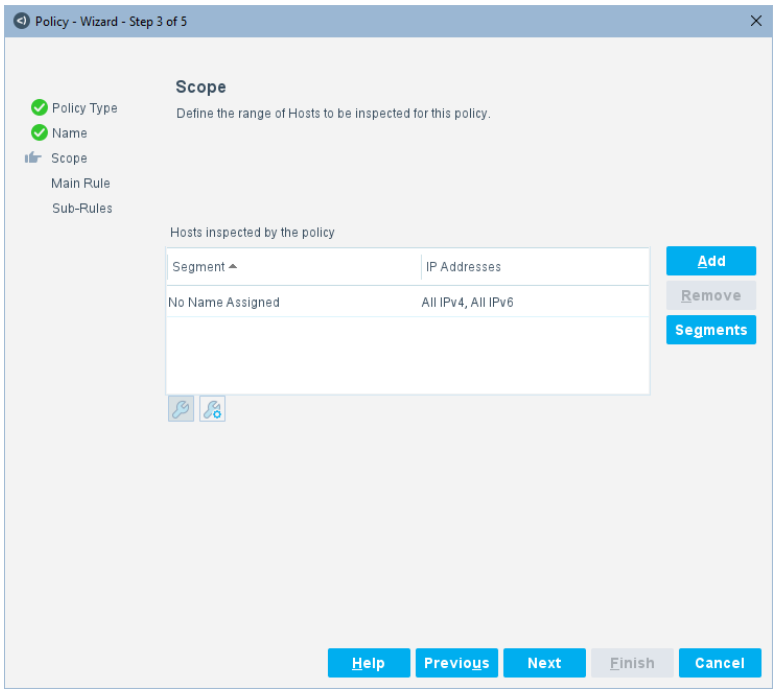
5. Enter a name and optionally add a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



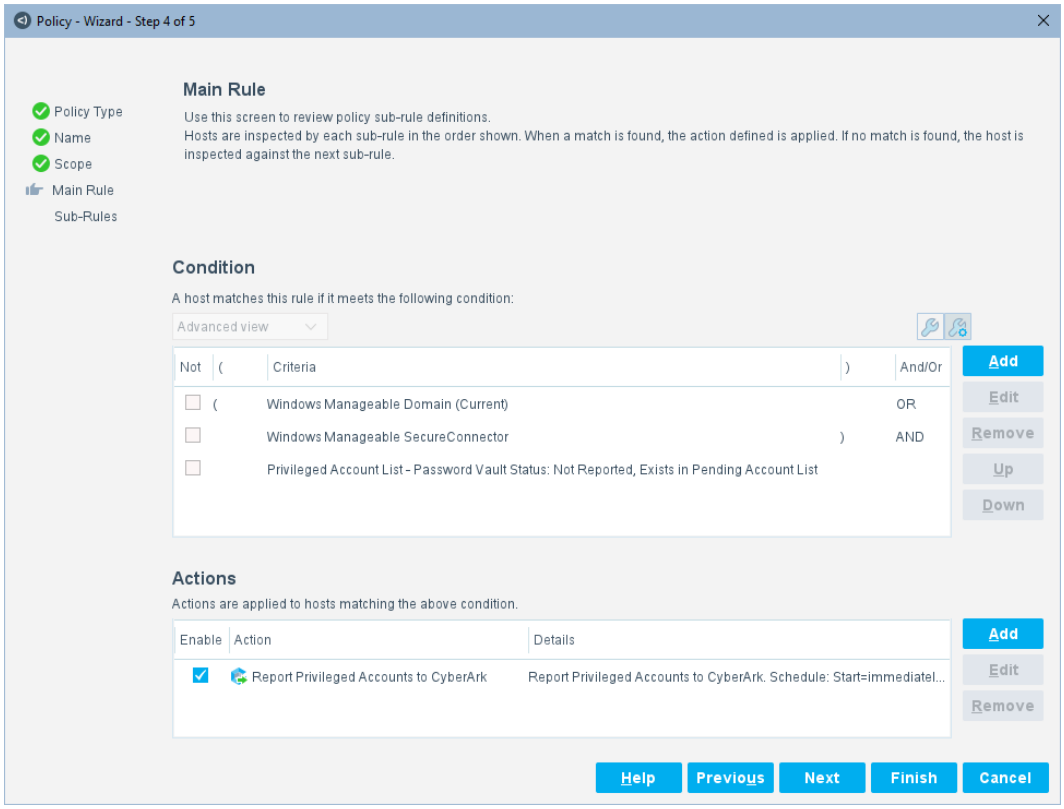
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.



9. Select **Next**.



When the main rule is applied, the Forescout platform detects privileged accounts that have been added or removed from managed endpoints since the last recheck and reports them to CyberArk. The default scan interval for rechecking privileged accounts is 8 hours.

The main rule of the Report Accounts to CyberArk Vault policy includes the following criteria for newly discovered privileged accounts that are reported to CyberArk:

- The discovered privileged account must belong to a Windows Managed Domain or must be managed by SecureConnector.
- The privileged account has not been reported or exists in the pending account list.

The default main rule does the following:

- The policy scans the Windows endpoint and retrieves a list of detected local privileged accounts and their properties.
- Based on the rule definition, accounts that match the conditions are reported to CyberArk, and CyberArk Vault returns a status for each account (*not reported, exists in pending account list*, or *managed*).
- The reported accounts are updated according to their status in the *CyberArk Pending Account List* as follows:
  - Updated from *not reported* to *exists in pending account list.*

    OR
  - Updated from *exists in pending account list* to *managed.*

- Once the *CyberArk Pending Account List* is updated, the CyberArk operator needs to go to the CyberArk management console, review the newly added accounts in the *Pending Account List,* and onboard them to make them managed by CyberArk.

10. Predefined conditions and actions for the policy are displayed in the Main Rule pane. Select a condition or action and then select **Edit** to modify its settings.
11. To add another condition, select **Add** in Condition section.
12. To add another action, select **Add** in the Actions section.
13. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
14. Select **Finish**. The policy is created.
15. Select **Apply** to save the policy.

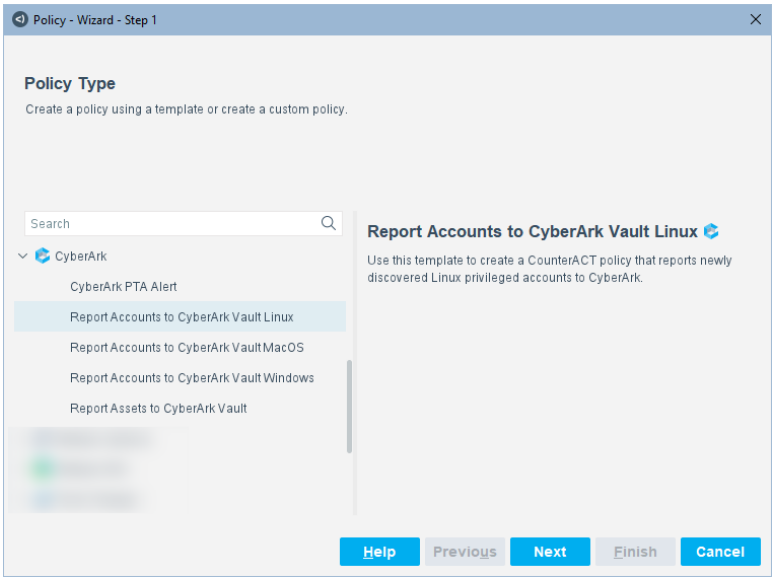
Create a Report Accounts to CyberArk Vault Linux Policy

Use this template to create a policy to report privileged accounts on Linux endpoints that are not managed or listed by CyberArk.

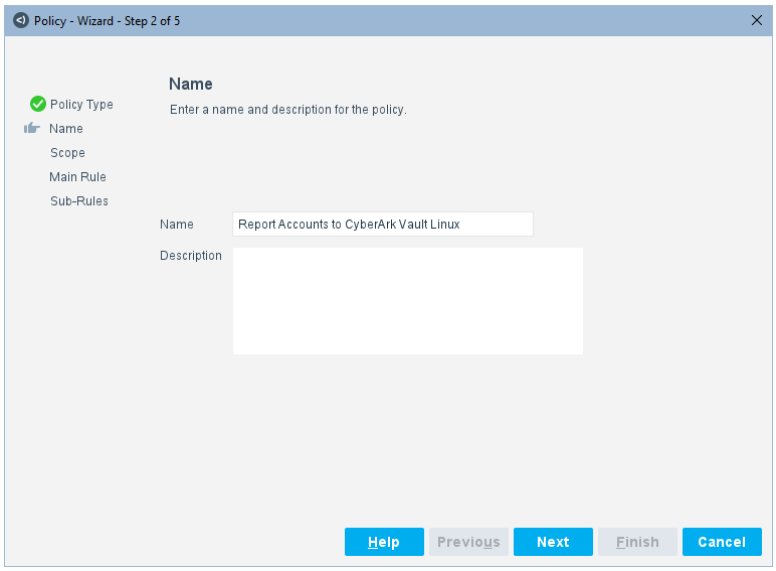
Install the latest Linux Plugin or upgrade to the latest. See Forescout Requirements.

To create a policy:

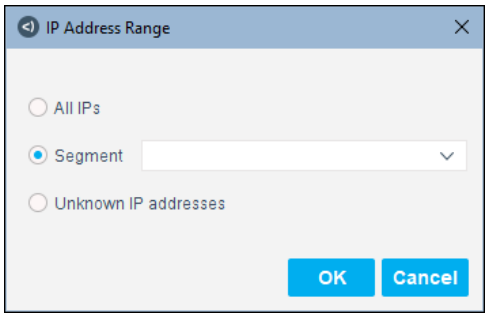
1. Log in to the Console and select **Policy**.
2. Select **Add** in the Policy Manager.
3. Expand the **CyberArk** folder and select **Report Accounts to CyberArk Vault Linux**.



4. Select **Next**.



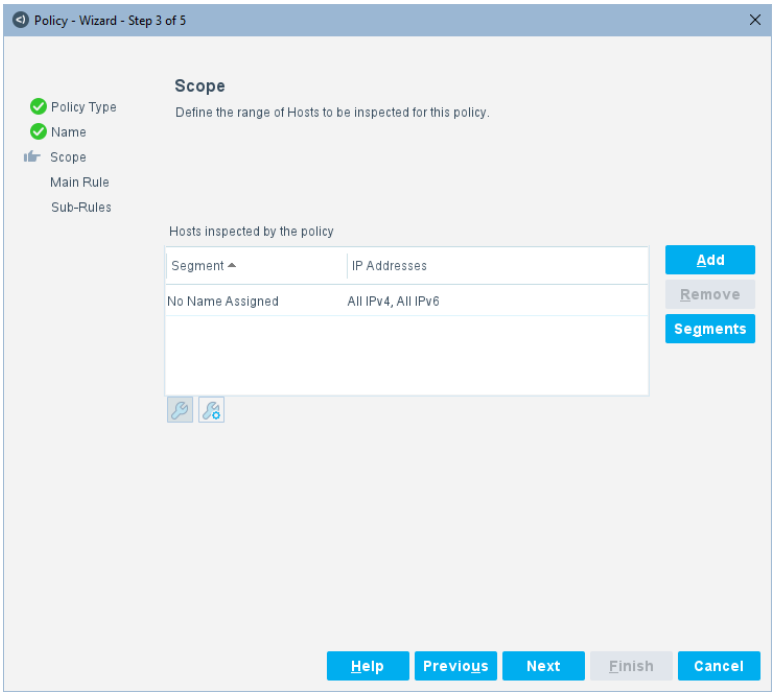
5. Enter a name and optionally add a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



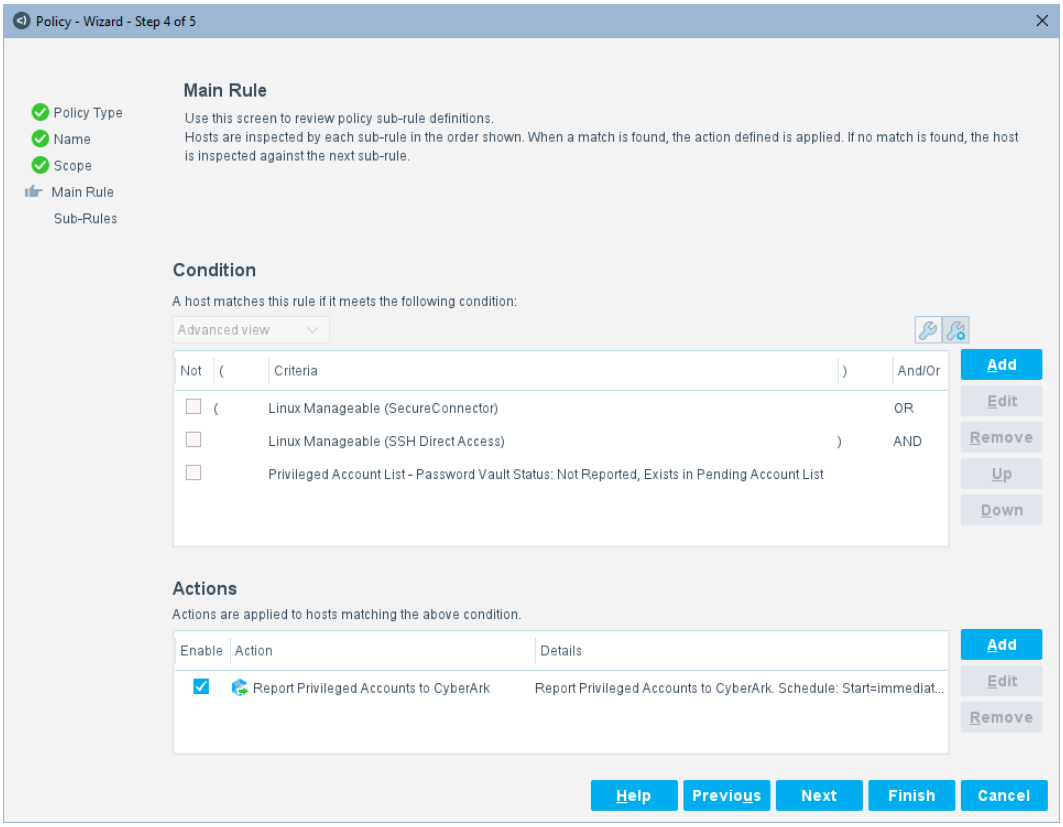
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.



9. Select **Next**.



The main rule of the Report Accounts to CyberArk Vault Linux policy includes the following criteria for newly discovered privileged accounts that are reported to CyberArk:

- The discovered privileged account must belong to a Linux Manageable endpoint managed by SecureConnector or SSH Direct Access.
- The privileged account has not been reported or exists in the pending account list.

The default main rule does the following:

- The policy scans the Linux endpoint and retrieves a list of detected local privileged accounts (from the defined user groups), and their properties.
- Based on the rule definition, accounts that match the conditions are reported to CyberArk, and CyberArk Vault returns a status for each account (*not reported, exists in pending account list*, or *managed*).
- The reported accounts are updated according to their status in the *CyberArk Pending Account List* as follows:
  - Updated from *not reported* to *exists in pending account list.*

    OR
  - Updated from *exists in pending account list* to *managed.*
- Once the *CyberArk Pending Account List* is updated, the CyberArk operator needs to go to the CyberArk management console, review the newly added accounts in the *Pending Account List,* and onboard them to make them managed by CyberArk.

10. Predefined conditions and actions for the policy are displayed in the Main Rule pane. Select a condition or action and then select **Edit** to modify its settings.
11. To add another condition, select **Add** in Condition section.
12. To add another action, select **Add** in the Actions section.
13. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
14. Select **Finish**. The policy is created.
15. Select **Apply** to save the policy.

Create a Report Accounts to CyberArk Vault MacOS Policy

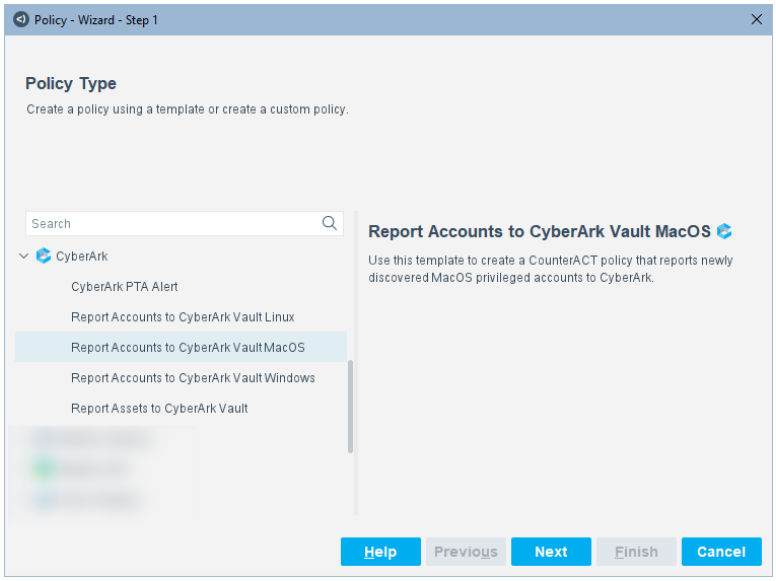
Use this template to create a policy to report privileged accounts on Mac OS endpoints that are not managed or listed by CyberArk.

Install the latest OS X Plugin or upgrade to the latest. See Forescout Requirements.

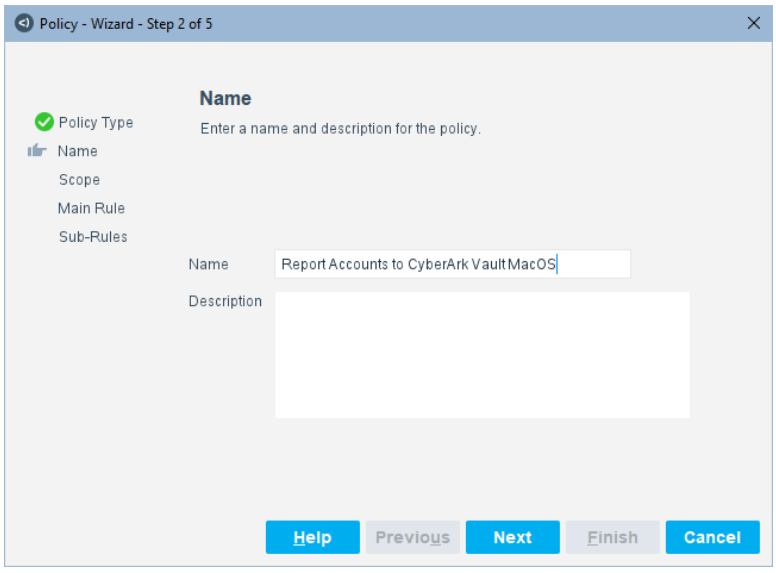
To create a policy:

1. Log in to the Console and select **Policy**.
2. Select **Add** in the Policy Manager.

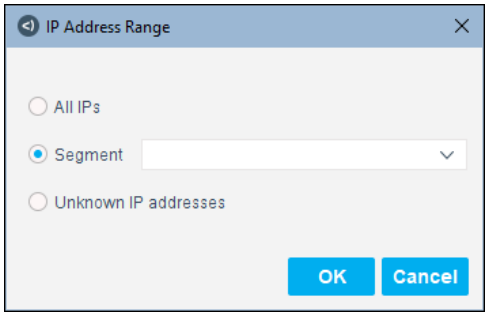
3. Expand the **CyberArk** folder and select **Report Accounts to CyberArk Vault MacOS**.



4. Select **Next**.



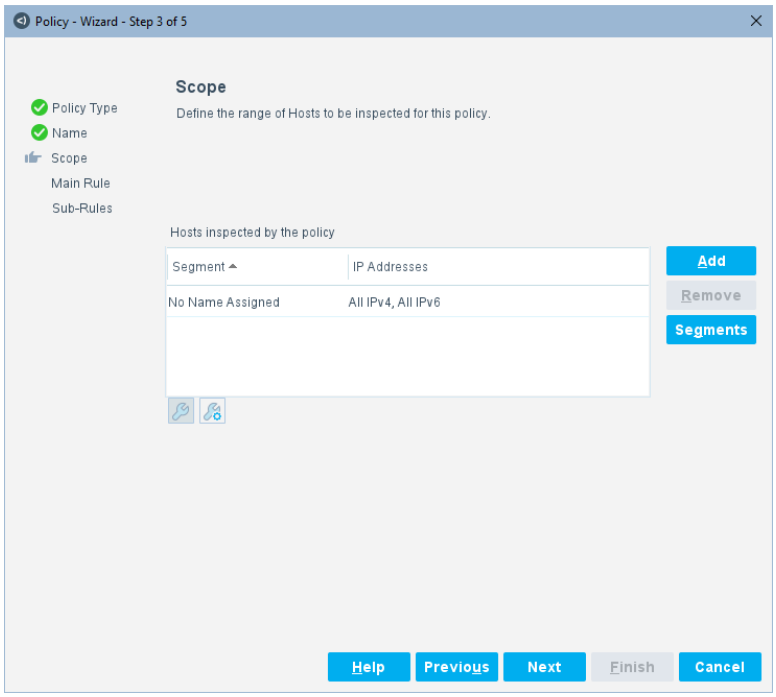
5. Enter a name and optionally add a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



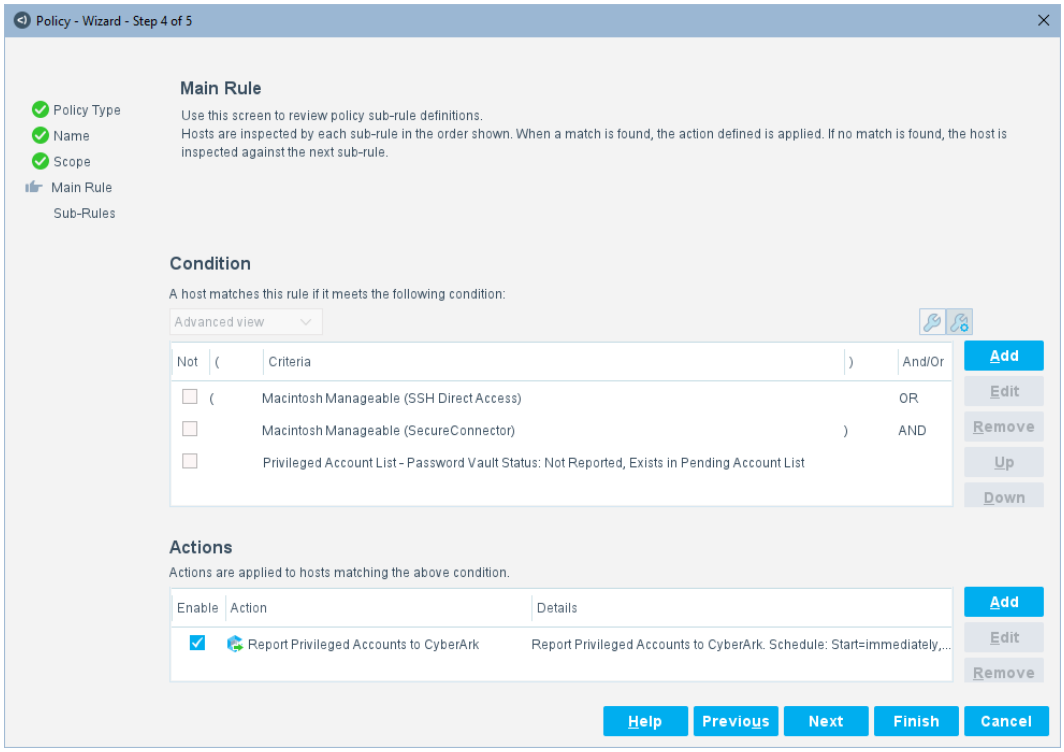
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.



9. Select **Next**.



The main rule of the Report Accounts to CyberArk Vault MacOS policy includes the following criteria for newly discovered privileged accounts that are reported to CyberArk:

- The discovered privileged account must belong to a Macintosh Manageable endpoint managed by SecureConnector or SSH Direct Access.
- The privileged account has not been reported or exists in the pending account list.

The default main rule does the following:

- The policy scans the Mac OS endpoint and retrieves a list of detected local privileged accounts (from the defined user groups), and their properties.
- Based on the rule definition, accounts that match the conditions are reported to CyberArk, and CyberArk Vault returns a status for each account (*not reported, exists in pending account list*, or *managed*).
- The reported accounts are updated according to their status in the *CyberArk Pending Account List* as follows:
  - Updated from *not reported* to *exists in pending account list.*

    OR
  - Updated from *exists in pending account list* to *managed.*
- Once the *CyberArk Pending Account List* is updated, the CyberArk operator needs to go to the CyberArk management console, review the newly added accounts in the *Pending Account List,* and onboard them to make them managed by CyberArk.

10. Predefined conditions and actions for the policy are displayed in the Main Rule pane. Select a condition or action and then select **Edit** to modify its settings.

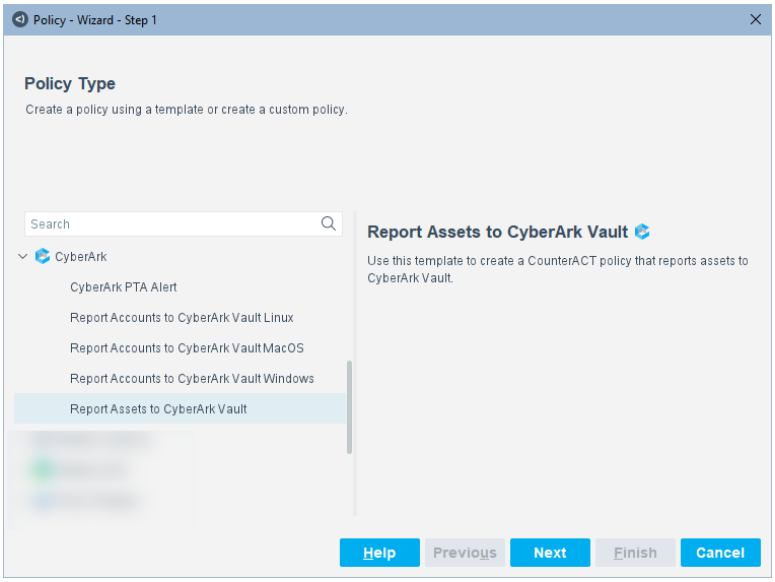
11. To add another condition, select **Add** in Condition section.
12. To add another action, select **Add** in the Actions section.
13. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
14. Select **Finish**. The policy is created.
15. Select **Apply** to save the policy.

Create a Report Assets to CyberArk Vault Policy

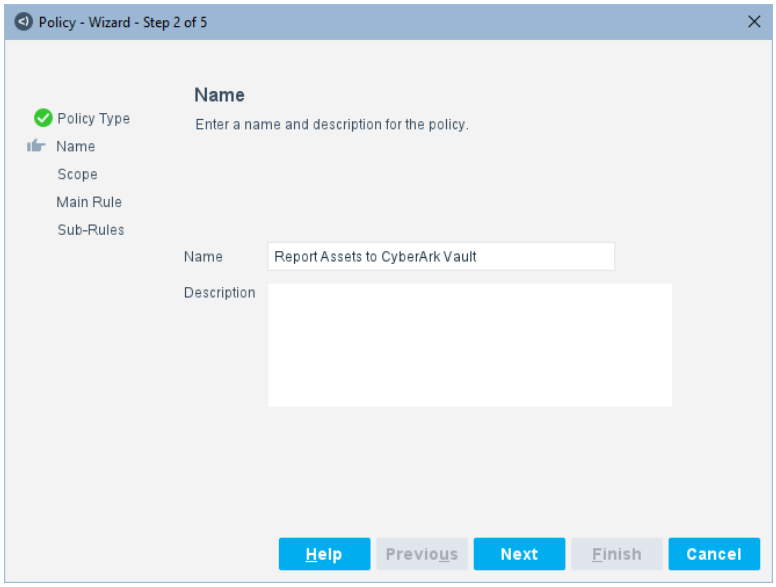
Use this template to create a policy to report assets to the CyberArk Vault. The policy template inserts endpoints based on their Network Function. It reports Internet of Things (IoT), Operational Technology (OT), or network devices to the accounts pending queue in CyberArk.

To create a policy:

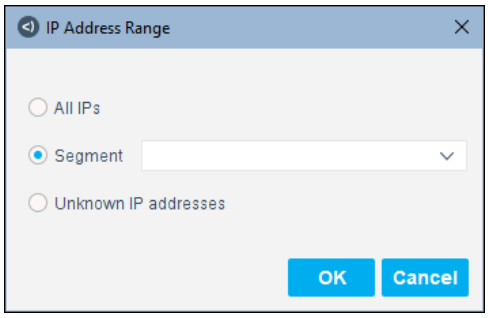
1. Log in to the Console and select **Policy**.
2. Select **Add** in the Policy Manager.
3. Expand the **CyberArk** folder and select **Report Assets to CyberArk Vault**.



4. Select **Next**.



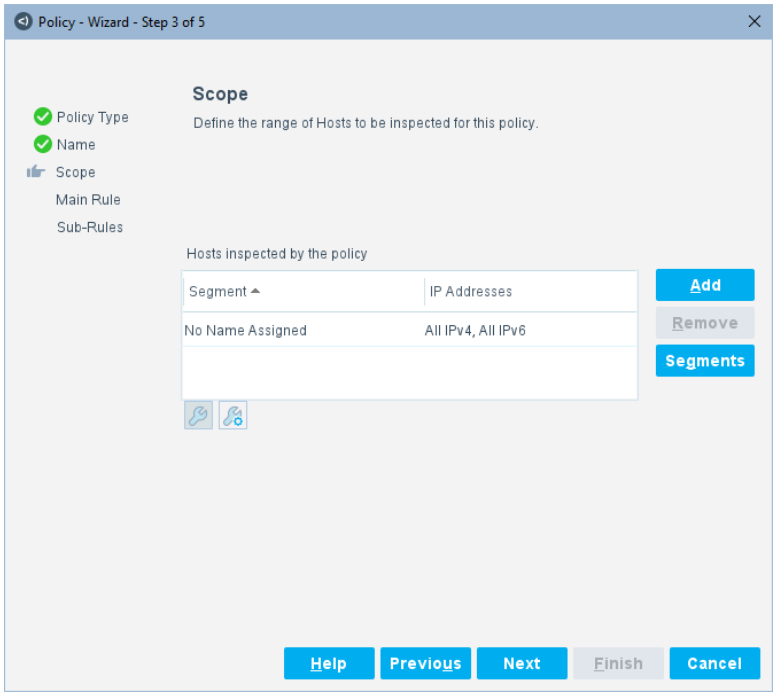
5. Enter a name and optionally add a description.
6. Select **Next**. Both the Scope pane and the IP Address Range dialog box open.
7. Use the IP Address Range dialog box to define which endpoints are inspected.



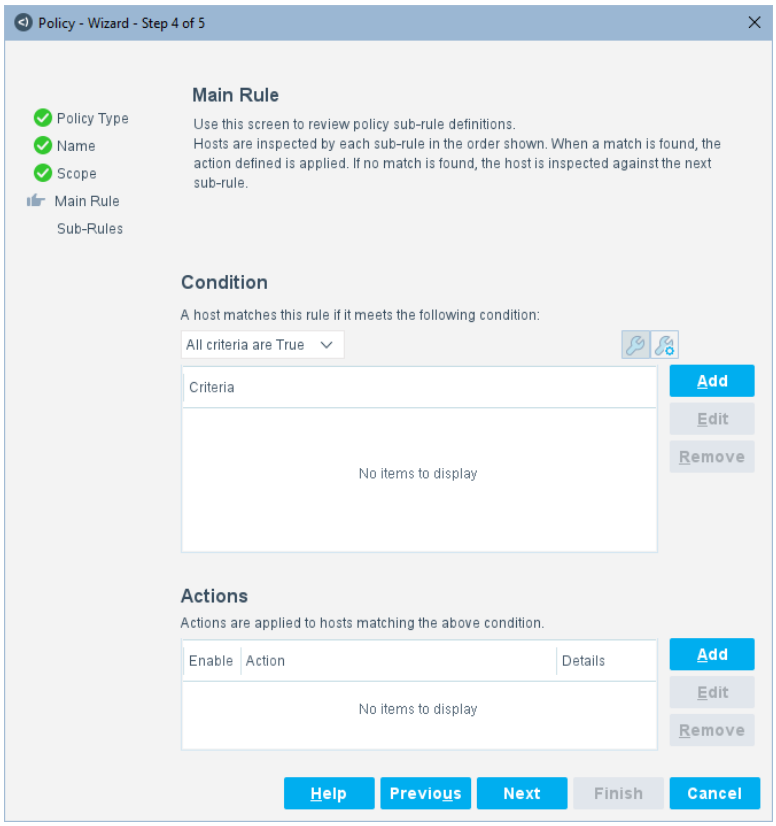
The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** or **Cancel** to close this dialog box, and select **Segments** from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

8. Select **OK**. The added range is displayed in the Scope pane.

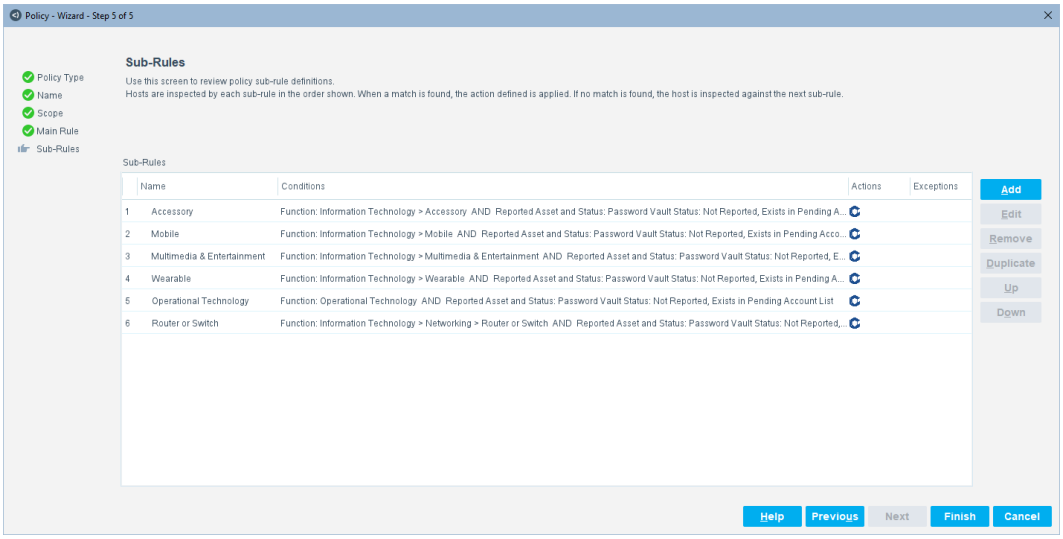


9. Select **Next**.



The Report Assets to CyberArk Vault policy has no main rule.

10. Select **Next**.



Each sub-rule filters a different Internet of Things (IoT), Operational Technology (OT), or network endpoint and reports it to the CyberArk Vault.

The Network Functions for IoT devices are:

- Accessory
- Mobile
- Multimedia & Entertainment
- Wearable

The Network Function for OT devices is:

- Operational Technology

The Network Function for network devices is:

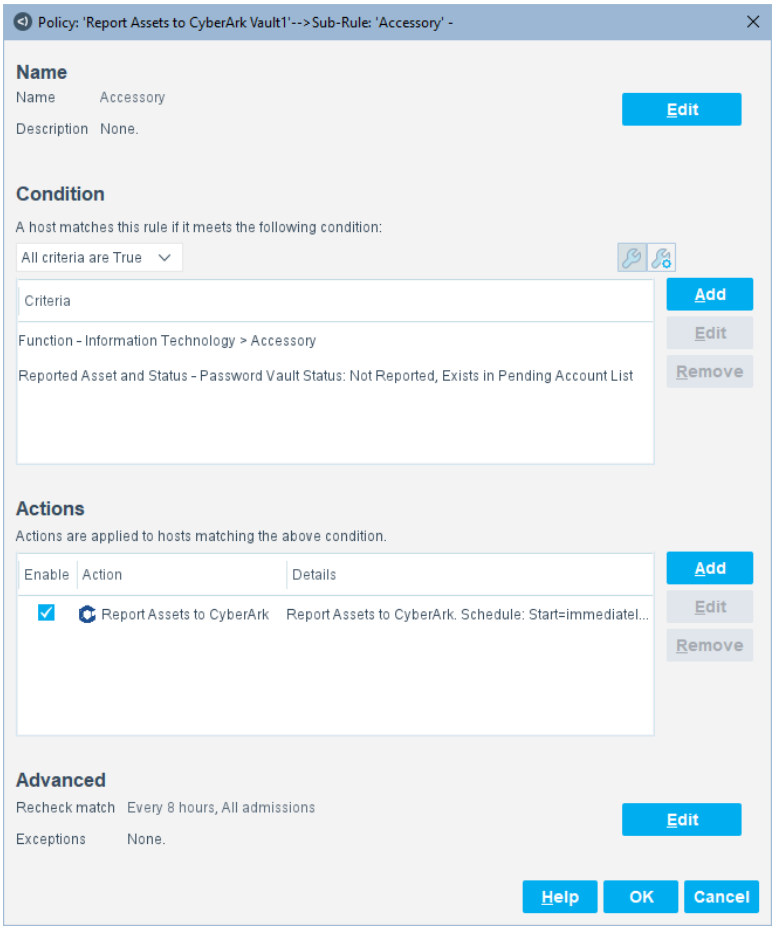
- Router or Switch

Each sub-rule condition also has a property:

- Reported Asset and Status: Password Vault Status: Not Reported, Exists in Pending Account List

These sub-rules allow different configuration of the reporting action, Report Assets to CyberArk. See eyeExtend for CyberArk Policy Actions.

11. (Optional) To edit a sub-rule, select a sub-rule and select **Edit** or double-click a sub-rule.



12.(Optional) To add a condition, select **Add** in Condition section.

13.(Optional) To add an action, select **Add** in the Actions section.

14. Select **OK**.

15. Select **Finish**. The policy is created.

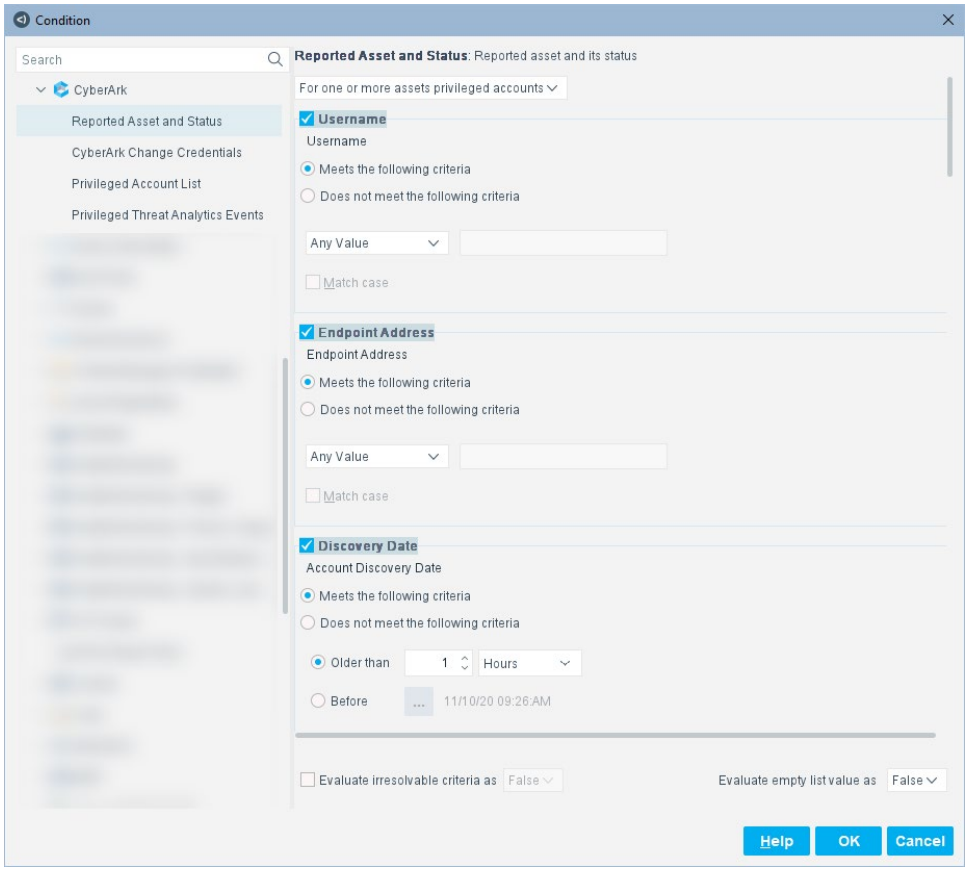
16. Select **Apply** to save the policy.

eyeExtend for CyberArk Policy Properties

You can customize policies with policy properties.

To access CyberArk properties:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the **CyberArk** folder in the Properties tree.


Condition
Search
CyberArk
Reported Asset and Status
CyberArk Change Credentials
Privileged Account List
Privileged Threat Analytics Events
Reported Asset and Status: Reported asset and its status
For one or more assets privileged accounts
Username
Username
Meets the following criteria
Does not meet the following criteria
Any Value
Match case
Endpoint Address
Endpoint Address
Meets the following criteria
Does not meet the following criteria
Any Value
Match case
Discovery Date
Account Discovery Date
Meets the following criteria
Does not meet the following criteria
Older than
1
Hours
Before
11/10/20 09:26:AM
Evaluate irresolvable criteria as
False
Evaluate empty list value as
False
Help
OK
Cancel

3. The following properties are available:

Reported Asset and Status	Indicates the asset reported to CyberArk and the status of the Report Assets to CyberArk action. The following sub-properties are available: ▪ Username: The username. ▪ Endpoint Address: The endpoint address. ▪ Discovery Date: The account discovery date. ▪ Account Source: The account sources are Local Privileged Account, Local Privileged Scheduled Tasks Accounts, or Local Privileged Service Account. ▪ OS type: The operating system type. ▪ Account Enabled: The Account state as defined in the source (from AD for domain account, from the machine for local) ▪ Account Type: The account type is Local Account. ▪ Account Domain: The domain to which the account belongs. ▪ Account Description: The account description. ▪ UID: The user ID. ▪ GID: The group ID. ▪ Account OS Group: The account operating system group. ▪ Discovery Platform Type: The discovery platform type. ▪ Password Vault Status: The Password Vault statuses are Exists in Pending Account List, Exists in Vault, or Not Reported.
CyberArk Change Credentials	Indicates the list of users and the results of the Change Credentials action. This property stores the change credentials action status of each user available for an endpoint. The following sub-properties are available: ▪ Change Credentials Action Status: The action status is Not Reported or Reported to CyberArk. ▪ Username: The username.

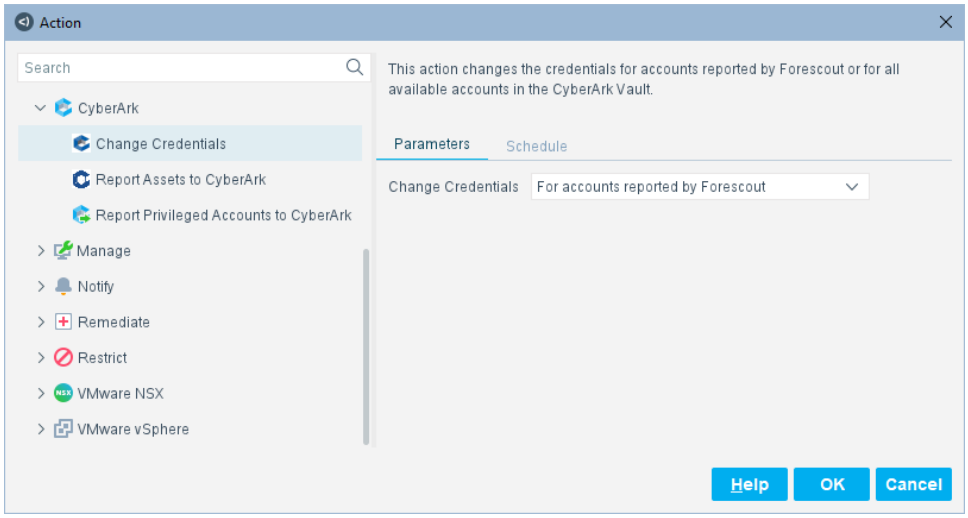
Privileged Account List	Indicates the list of privileged accounts on the endpoint. The following sub-properties are available: ▪ Username: The username. ▪ Endpoint Address: The endpoint address. ▪ Discovery Date: The account discovery date. ▪ Account Source: The account sources are Local Privileged Account, Local Privileged Scheduled Tasks Accounts, or Local Privileged Service Account. ▪ OS type: The operating system types are Linux, Mac, Unix, or Windows ▪ Account Enabled: The Account state as defined in the source (from AD for domain account, from the machine for local) ▪ Account Type: The account type is Local Account. ▪ Account Domain: The domain to which the account belongs. ▪ Account Description: The account description. ▪ UID: The user ID. ▪ GID: The group ID. ▪ Account OS Group: The account operating system group. ▪ Discovery Platform Type: The discovery platform type. ▪ Password Vault Status: The Password Vault statuses are Exists in Pending Account List, Exists in Vault, or Not Reported.
Privileged Threat Analytics Events	Indicates the list of PTA events. The following sub-properties are available: ▪ Event Name: The event names are Suspected Credentials Theft, Suspicious Behavior of Machine, Suspicious Behavior of User, Suspicious Behavior of Vault User, or Unmanaged Privileged Account. ▪ Severity: The severity. ▪ Source Machine: The source machine. ▪ Target Machine: The target machine. ▪ Destination Username: The destination username. ▪ Vault User: The Vault user. ▪ Extension Fields: The extension fields. ▪ Detection Date: The detection date.

eyeExtend for CyberArk Policy Actions

You can customize policies with policy actions.

To access CyberArk actions:

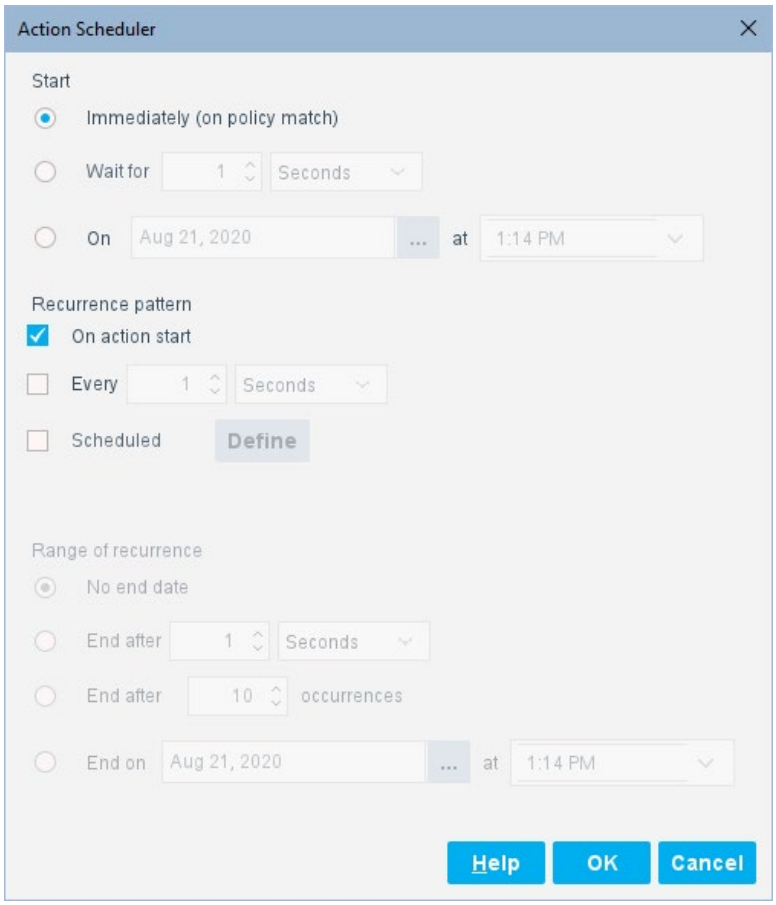
1. Go to the Actions tree from the Policy Conditions dialog box.
2. Expand the **CyberArk** folder in the Actions tree.



3. The following actions are available:

Change Credentials	This action changes the credentials on all privileged accounts of an endpoint. For example, use this action to mitigate risk by rotating passwords on endpoints that are identified as compromised. The action applies to Windows, Linux, and Mac OS endpoints. Select the accounts on which to change credentials: ▪ For accounts reported by Forescout ▪ For all available accounts in the CyberArk Vault The action is successful if all accounts for the selection are changed.
Report Assets to CyberArk	This action reports assets to CyberArk. It has two parameters (Username and Description) that are configurable for each condition in the Report Assets to CyberArk Vault policy. The following configured parameter values are sent to the CyberArk Vault: ▪ Username: Configure the username that will be reported ▪ Description: Configure a body message Select **Tags** to use Forescout properties in the Description.
Report Privileged Accounts to CyberArk	This action reports privileged accounts to CyberArk.

4. Select the Schedule tab and select one of the following Action Schedule options:
   - Start action when the endpoint matches a policy condition, which implements the policy when the policy condition(s) is met by the endpoint.
   - Customize action start time, which opens the Action Scheduler dialog box.



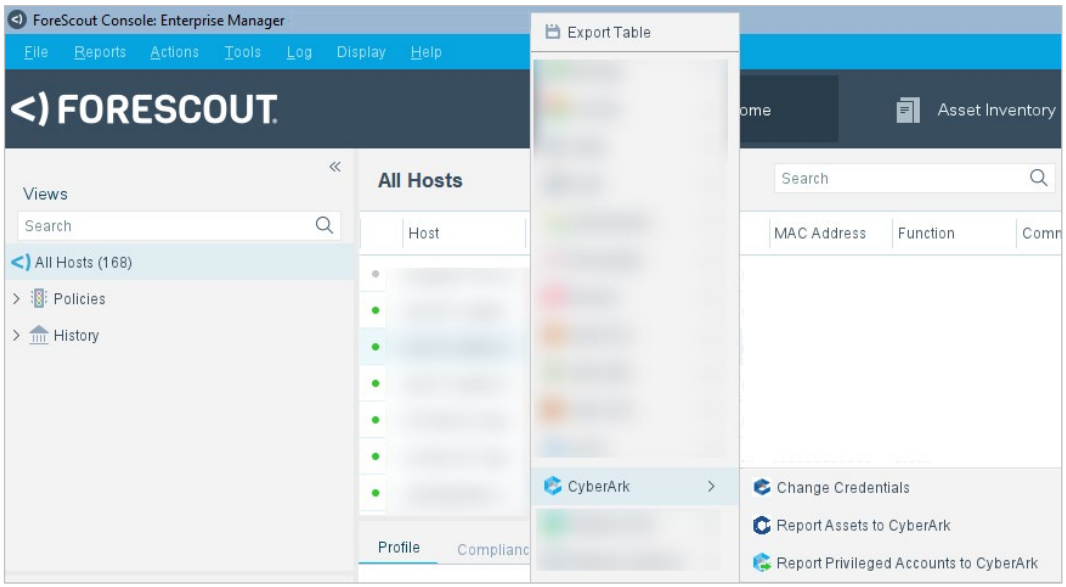
5. Set the schedule parameters and select **OK**.
6. Select **OK**.

Manually Run an Action

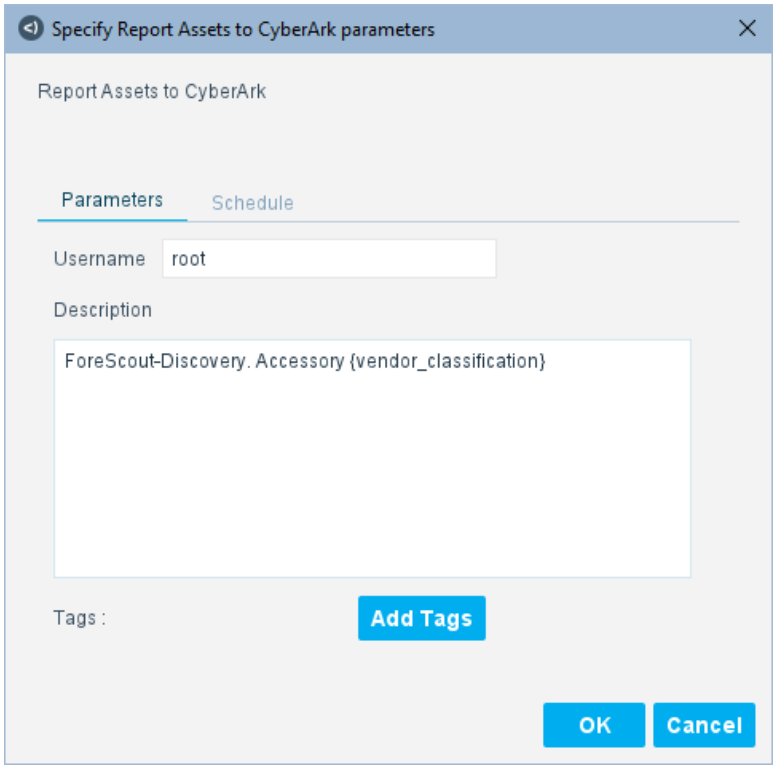
A CyberArk action can be launched as part of a policy or you can manually run an action.

To manually run an action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select CyberArk, and select an action.



3. Select Change Credentials, Report Assets to CyberArk, or Report Privileged Accounts to CyberArk. A Specify parameters dialog box opens based on your selection.



4. To configure the action, select the Parameters and/or Schedule tabs.
5. In the Specify parameters dialog box, select **OK**.

Working with eyeExtend for CyberArk

The following topics describe how best to use Forescout eyeExtend for CyberArk:

- Best Practices for Working with CyberArk
- Asset Inventory for CyberArk

Best Practices for Working with CyberArk

This topic describes best practices for working with Forescout eyeExtend for CyberArk.

Password Change Frequency

The Forescout platform uses Windows credentials to verify domain membership and manage endpoints constantly. While configurable, this is multiple times per day, per endpoint. As such, it is not recommended to change the credential on each use. Not only will this conflict with the constant use of the credential, it may also create a large resource load on CyberArk. Forescout does not recommend changing the password more than once per day, or less than once per month.

Detection of CyberArk Unmanaged Local Accounts

Using remote or agent-based inspection, the Forescout platform can identify local accounts present on Windows, Mac OS, and Linux endpoints and compare them to accounts that exist on CyberArk. When a local account exists that is not managed by CyberArk, the Forescout platform can report it to CyberArk. There is no direct best practice guidance for this feature other than to utilize it.

CyberArk PTA Notification to the Forescout Platform of Unusual Account Use

CyberArk's feature Privilege Threat Analysis detects anomalous account behavior based on several configurable options. When anomalous behavior is detected, it can notify the Forescout platform via Syslog, creating an actionable property that the Forescout platform can use to remove or restrict network access to that device. Refer to CyberArk documentation for configuring the rules that describe the anomalous behavior.

Syslog Receptors

When designing the overall solution, take into consideration that the Forescout platform is limited to three Syslog sources. These may all be CyberArk sources, or a single CyberArk source and two other sources.

CyberArk Management of Accounts

Other than the required root access to CLI and admin access to the Console, it is best practice not to have any local accounts on the Forescout platform. Wherever possible, CyberArk should manage the accounts that Forescout uses.

Forescout Accounts

CyberArk can and should be configured to manage all CounterACT Appliance root account access via CLI over SSH.

Accounts Used by the Forescout Platform

CyberArk can and should be configured to manage the Active Directory account that the Forescout platform uses to authenticate.

Non-Administrative Accounts

Normal user access to the Forescout platform over CLI or through the Console should be managed by an external directory service such as Active Directory or TACACS.

Direct CyberArk Login to Forescout Console

Users can use the CyberArk Privileged Session Manager (PSM) to log in to the Console directly.

Requirements

The Console software must be installed on a Windows Remote Desktop Services (RDS) server. CyberArk PSM is then configured to use the RDS, automatically supplying the required login credentials to the Console.

Recommendation

To simplify access management, this is best used when local accounts must exist on the Console, or when it is preferred that no password is visualized during a one-time admin login.

CounterACT Appliance to CyberArk Mapping

Each CounterACT Appliance can point to a single CyberArk Vault. If more than one CyberArk Vault exists in the enterprise, they must be matched correctly. Appliances matched to a specific CyberArk should not manage endpoints that rely on credentials from another CyberArk. If one CyberArk manages credentials for a specific enterprise region, the CounterACT Appliance(s) should also be matched to that region, connecting to the regional CyberArk and managing endpoints in that same region.

Disassociation from CyberArk

When a CounterACT Appliance disassociates its connection to CyberArk, which can happen when the Appliance physically fails or is otherwise manually and permanently disconnected, it needs to be reconnected to CyberArk.

CyberArk Accounts

When a CounterACT Appliance initially connects to CyberArk, a unique account is created. When a CounterACT Appliance then disassociates from CyberArk, the account is left on CyberArk. This inherently disallows the Appliance from reconnecting. The account must be removed from CyberArk.

CounterACT Appliance IP Address Changes

When a CounterACT Appliance's IP address changes, this constitutes a disassociation and it must be reconnected to the CyberArk Vault. The reconnection works because of the new unique IP address, but the account created from the old IP address continues to exist on CyberArk and should be updated.

CounterACT Application ID

The CounterACT application ID must be defined in CyberArk *before* configuration. This ID is not unique among CounterACT Appliances and is used by all of them. For best security, the Application ID should be specifically locked down from access by any IP address that is not a CounterACT Appliance.

CyberArk Safe Access

Each CyberArk Vault contains Safes that hold account passwords. Safes allow CyberArk to further separate credential access. Each Safe should be configured to only allow access to CounterACT devices that need to use account passwords within that Safe.

Asset Inventory for CyberArk

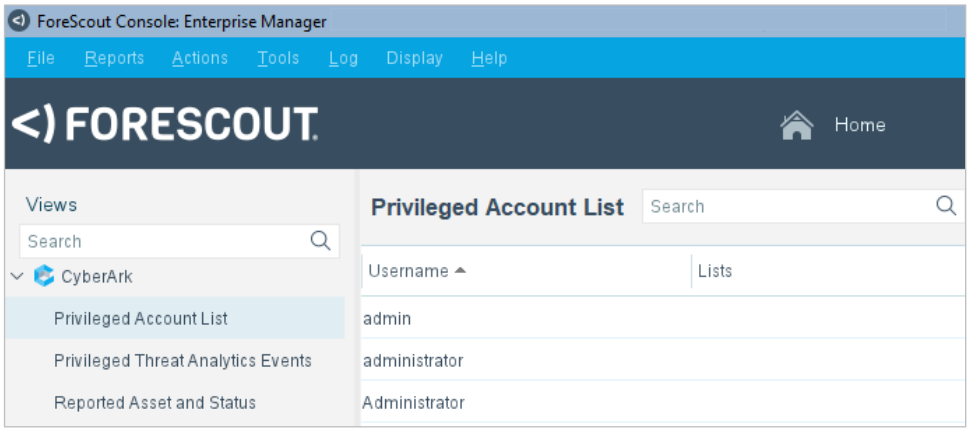
Use the Asset Inventory to view a real-time display of the network activity at multiple levels.

The Asset Inventory lets you:

- View detected Privileged Accounts
- Incorporate inventory detections into policies

To access the inventory:

1. In the Console toolbar, select **Asset Inventory**.
2. In the Views pane, go to the CyberArk entries.



The following information is available:

- **Privileged Account List**: Displays a table of privileged accounts.
- **Privileged Threat Analytics Events**: Displays reported PTA events, and a list of hosts to which the events are attributed.
- **Reported Asset and Status**: Displays information reported to CyberArk for an asset and the status of the action, Report Assets to CyberArk.

Refer to "Working with Asset Inventory Detections" in the *Forescout Administration Guide* for information about how to work with the Inventory.