



ForeScout[®] Extended Module for CyberArk[®]

Configuration Guide

Version 1.1

Table of Contents

| | |
|---|-----------|
| About the CyberArk Integration | 3 |
| Use Cases | 4 |
| Credential Retrieval from CyberArk Enterprise Password Vault | 4 |
| Discovering and Reporting Local Privileged Accounts..... | 4 |
| Receiving Privileged Threat Analytics Alerts | 4 |
| About this Module | 4 |
| Architecture..... | 5 |
| How It Works..... | 5 |
| Retrieving Credentials..... | 5 |
| Discovering and Reporting Local Privileged Accounts..... | 6 |
| Receiving Privileged Threat Analytics Alerts | 6 |
| What to Do | 6 |
| Requirements..... | 6 |
| CounterACT Software Requirements | 6 |
| Supported Vendor Requirements | 7 |
| About Support for Dual Stack Environments | 7 |
| ForeScout Extended Module License Requirements | 7 |
| Per-Appliance Licensing Mode | 8 |
| Centralized Licensing Mode..... | 9 |
| More License Information | 10 |
| Networking Requirements | 10 |
| Endpoint Requirements | 10 |
| Install the Module | 10 |
| Configure the Module | 12 |
| Configure the Module for Credential Retrieval | 12 |
| Install the CyberArk Credential Provider on CounterACT Devices | 12 |
| Configure Users in the CyberArk Vault | 14 |
| Define the HPS Inspection Engine Vault Query | 14 |
| Configure the Module for Reporting Discovered Privileged Accounts | 17 |
| Configure the Module to Receive PTA Alerts | 18 |
| Run CyberArk Policy Templates..... | 19 |
| Report Accounts to CyberArk Vault Policy Template | 20 |
| CyberArk PTA Alert Policy Template | 23 |
| Using Information from PTA Alerts..... | 26 |
| Using CyberArk | 27 |
| Best Practices | 27 |
| Windows Endpoint Credential Management | 27 |

| | |
|--|-----------|
| Detection of CyberArk Unmanaged Local Accounts..... | 27 |
| CyberArk PTA Notification to CounterACT of Unusual Account Use | 27 |
| CyberArk Management of Accounts..... | 28 |
| Direct CyberArk Login to CounterACT Console..... | 28 |
| CounterACT to CyberArk Mapping..... | 28 |
| CounterACT Disassociation from CyberArk..... | 29 |
| Access the Asset Inventory..... | 29 |
| Endpoint Module Information..... | 30 |
| Additional CounterACT Documentation | 31 |
| Documentation Downloads | 31 |
| Documentation Portal | 31 |
| CounterACT Help Tools..... | 32 |

About the CyberArk Integration

ForeScout CounterACT® Extended Module for CyberArk allows integration with the CyberArk Privileged Account Security Solution.

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

This integration allows ForeScout customers who use CyberArk products to 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 CounterACT 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.

CyberArk integration with CounterACT provides Privileged Threat Analytics™ (PTA) Alerts that can be used by CounterACT to take policy-based mitigating actions on accounts or endpoints that display anomalous privileged activity. For example, by 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 CounterACT users according to a defined CyberArk policy, enhancing the security of CounterACT user accounts.

CounterACT 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 CounterACT sessions in the CyberArk Vault.

Use Cases

This section describes important use cases supported by this Module. To understand how this Module helps you achieve these goals, see [About this Module](#). Be sure to review the [Best Practices](#).

Credential Retrieval from CyberArk Enterprise Password Vault

CounterACT supports privileged access management through the CyberArk Application Identity Manager™ (AIM). By integrating the CyberArk Application Credential Provider, the CounterACT HPS Inspection Engine can retrieve highly sensitive credentials from the CyberArk Vault. During HPS Remote Inspection of Windows endpoints, privileged account credentials are requested on a per-use basis without storing them in the CounterACT system. This integration enhances the security of the sensitive credentials, as they are only stored in the CyberArk Vault.

Discovering and Reporting Local Privileged Accounts

CounterACT detection capabilities enable the discovery of new devices and accounts, and in particular local privileged accounts. Every managed Windows endpoint is 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.

Receiving Privileged Threat Analytics Alerts

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

About this Module

This module lets you:

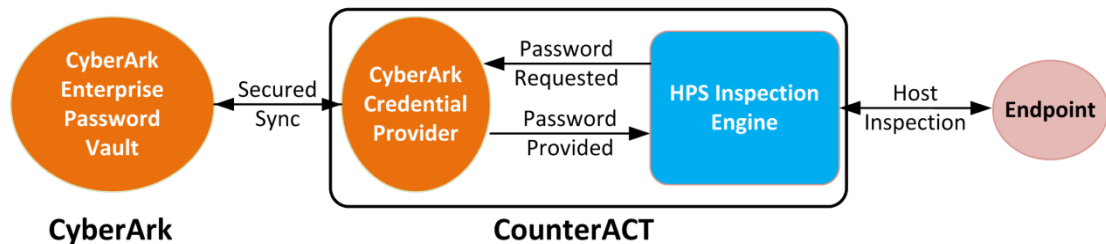
- Gain access to endpoints for Remote Inspection by the HPS Inspection Engine, without saving or managing the login credentials locally. The credentials are managed and provided on demand by the CyberArk Enterprise Password Vault®. See [Configure the Module for Credential Retrieval](#) for details.
- Enhance CyberArk visibility and monitoring of privileged accounts on endpoints managed by the HPS Inspection Engine. See [Report Accounts to CyberArk Vault Policy Template](#) for details.
- React in real-time to threats reported by the CyberArk PTA with actions defined by CounterACT Policies. See [CyberArk PTA Alert Policy Template](#) for details.

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 CounterACT integration with CyberArk consists of:

- The CyberArk Enterprise Password Vault, where privileged account credentials are stored and managed.
- The HPS Inspection Engine which detects and monitors endpoints through Remote Inspection.
- The CyberArk Credential Provider, which communicates with the HPS Inspection Engine and with the CyberArk Enterprise Password Vault in order 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 CounterACT) that identifies an unmanaged privileged account, to add it to the CyberArk Vault.
- CyberArk Privileged Threat Analytics (PTA) sends detected security events to CounterACT as syslog messages. The PTA messages are received by the CounterACT Syslog Plugin, and can be acted upon according to specifically defined CounterACT policies.

How It Works

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

Retrieving Credentials

Whenever CounterACT requires credentials to access an endpoint, the HPS Inspection Engine queries 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 endpoint.

Discovering and Reporting Local Privileged Accounts

CounterACT endpoint detection and inspection can discover privileged accounts on endpoints where CyberArk has no visibility. CounterACT 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.

Receiving 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 CounterACT and the related endpoints are assigned to a CounterACT group. The threat information related to an endpoint is processed and CounterACT 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.

What to Do

This section lists the steps you should take to set up your system when integrating with CyberArk

1. Verify that you have met system requirements. See [Requirements](#).
2. Review [Best Practices](#).
3. [Install the Module](#).
4. [Configure the Module](#).
5. [Run CyberArk Policy Templates](#).

Requirements

This section presents the following requirements:

- [CounterACT Software Requirements](#)
- [Supported Vendor Requirements](#)
- [Networking Requirements](#)
- [Endpoint Module Information](#)

CounterACT Software Requirements

This module requires the following CounterACT releases and other CounterACT components:

- CounterACT version 8.0
- A module license for the CyberArk Module

- An active Maintenance Contract for the licensed module is required
- Endpoint Module version 1.0 or above with the HPS Inspection Engine running
- Core Extension Module version 1.0 or above with the Syslog Plugin running

Supported Vendor Requirements

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

- CyberArk Enterprise Password Vault® - version 9.8
- CyberArk Password Vault Web Access® - version 9.8
- CyberArk AIM® - Credential Provider version 9.7
- CyberArk PTA™ - version 3.4

About Support for Dual Stack Environments

CounterACT version 8.0 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, **IPv6 addresses are not yet supported by this component**. 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 component.

ForeScout Extended Module License Requirements

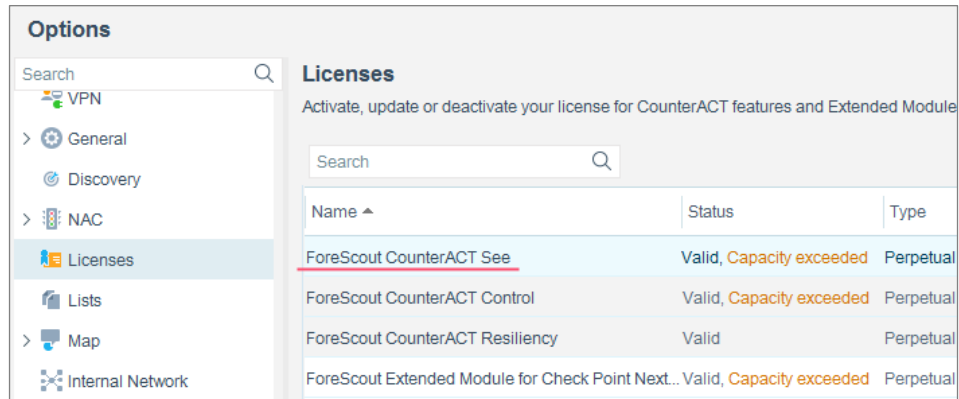
This ForeScout Extended Module requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- [Per-Appliance Licensing Mode](#)
- [Centralized Licensing Mode](#)

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Per-Appliance Licensing Mode

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

When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license.*

Demo license extension requests and permanent license requests are made from the CounterACT 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 CounterACT Administration Guide for more information.

Requesting a License

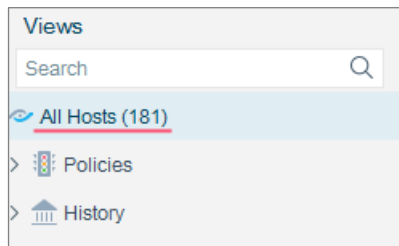
When requesting a demo license extension or permanent license, you are asked to provide the device *capacity* requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by CounterACT. You can request a license that 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 CounterACT, 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.



Centralized Licensing Mode

When you set up your CounterACT deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including Extended Modules. After the initial license file has been activated, you can update the file to add additional Extended Module licenses or change endpoint capacity for existing Extended Modules. For more information on obtaining Extended Module licenses, contact your ForeScout 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 Extended Module license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each Extended Module license varies by module, but does not exceed the capacity of the See license.

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

More License Information

Refer to the *CounterACT Administration Guide* for information on Extended Module licenses. You can also contact your ForeScout representative or license@forescout.com for more information.

Networking Requirements

The following ports must be open on enterprise firewalls to support communication between CounterACT 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, endpoints to be handled must be manageable by the HPS Inspection Engine.

Install the Module

This section 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](#) - **Centralized Licensing Mode**

To find out which licensing mode your deployment is working with, see [Identifying Your Licensing Mode in the Console](#).

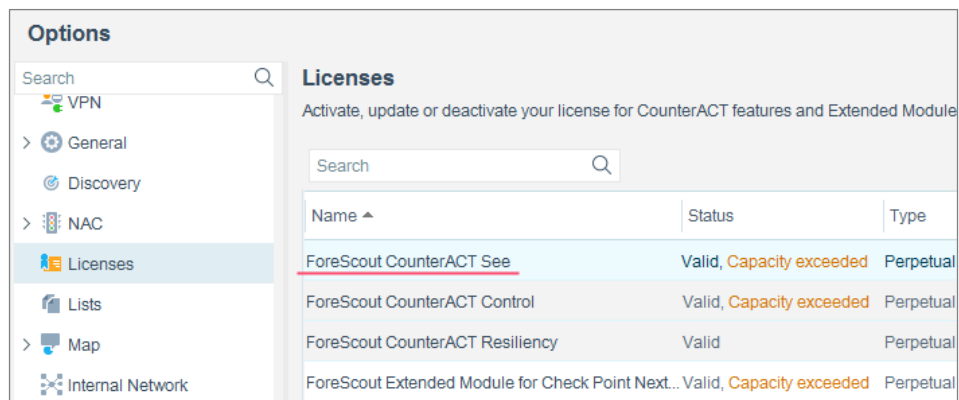
2. Download the module `.fpi` file.
3. Save the file to the machine where the CounterACT Console is installed.
4. Log into the CounterACT Console and select **Options** from the **Tools** menu.

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 will not proceed if you do not agree to the license agreement.
 - 📄 *The installation will begin 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.*

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



The screenshot shows the 'Options' menu with 'Licenses' selected. The 'Licenses' section displays a table with the following data:

| Name | Status | Type |
|---|--------------------------|-----------|
| ForeScout CounterACT See | Valid, Capacity exceeded | Perpetual |
| ForeScout CounterACT Control | Valid, Capacity exceeded | Perpetual |
| ForeScout CounterACT Resiliency | Valid | Perpetual |
| ForeScout Extended Module for Check Point Next... | Valid, Capacity exceeded | Perpetual |

Contact your ForeScout representative if you have any questions about identifying your licensing mode.


Configure the Module

- [Configure the Module for Credential Retrieval](#)
- [Install the CyberArk Credential Provider on CounterACT Devices](#)
- [Configure Users in the CyberArk Vault](#)
- [Define the HPS Inspection Engine Vault Query](#)
- [Configure the Module for Reporting Discovered Privileged Accounts](#)
- [Configure the Module to Receive PTA Alerts](#)

Configure the Module for Credential Retrieval


Configure the Module to enable CounterACT 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 required by the HPS Inspection Engine to access and perform Remote Inspection on endpoints.

 *Each CounterACT Appliance retrieving passwords from the CyberArk Vault must be installed with a CyberArk Credential Provider, and uses 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.*


Install the CyberArk Credential Provider on CounterACT Devices

1. In the CounterACT Console Tools menu, select **Options** and navigate to **CounterACT Devices**.
2. Select the CounterACT devices to be configured, and select **CyberArk** and Install CyberArk Provider from the list.
3. Select **Yes** in the CounterACT Enterprise Manager Console confirmation message to continue.
4. The Configure CyberArk Vault dialog box opens.

 *You can select more than one device at a time, and the installation process will automatically install a Provider instance for each CounterACT device.*

5. Enter the following information:

| | |
|----------------------------------|---|
| Server Address | The IP address or the Fully Qualified Domain Name 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 | The default port (1858) for communication with the CyberArk Vault server |
| Location | The name of the Location in the Vault to which CounterACT Device is assigned. If the Location name is not defined, a new one is created. Make sure that the CounterACT Device has not been assigned yet to this Location. |
| CounterACT Application ID | The default name used for creating a new user in the CyberArk Vault |
| User | User name for logging in to the Vault. This must be an Administrator level user. |
| Password | 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, and is not saved by CounterACT.*

6. Select **OK** to save the module configuration.

To ensure that the CyberArk and PrivateArk integration is successful the user needs to 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 need).
2. Add Enterprise Manager and Appliance IP Addresses to the Allowed Machines. Application is added to the Vault in the PrivateArk.

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*).

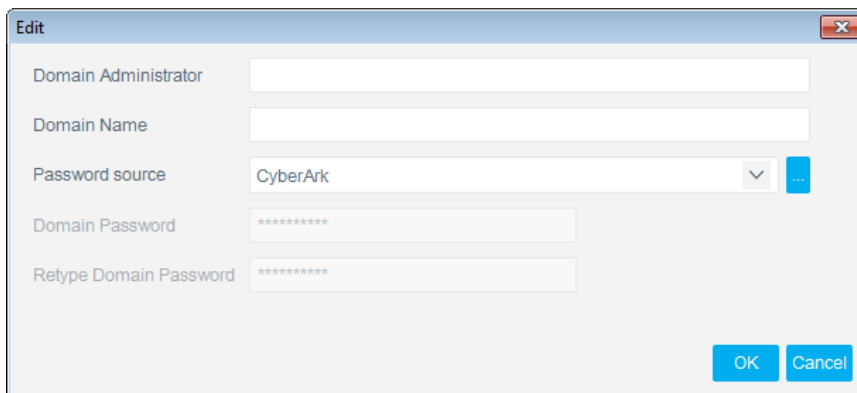
To define safe ownership in the Vault:

1. Log in to the CyberArk PrivateArk server, and log in to the Vault.
2. Select **Tools > Administrative Tools > Users and Groups**, the Users and Groups dialog box opens.
3. Select the new User (*Counteract_<name or IP address>*) that was created by the Provider installation.
4. Select **Safe Ownership**. The Safe Ownership dialog box opens.
5. Select a safe that you want to grant ownership to, select permissions that are given to that User, and (optionally) set an expiration date for the safe ownership. Use the arrows to move the selected safe from the **Available Safes** list to the **Owner of** list.
6. Select **OK** to save the safe ownership settings, and select **Close** to close the Users and Groups dialog box.

Define the HPS Inspection Engine Vault Query

This section describes how to configure the HPS Inspection Engine to query the CyberArk Vault whenever it needs credentials to access and perform Remote Inspection on an endpoint.

1. In the CounterACT Console select Tools and select **Options**
2. Navigate to the **HPS Inspection Engine**.
3. In the HPS Inspection Engine pane, select the Remote Inspection tab.
4. Select **Add**. The Add dialog box opens.




The screenshot shows a dialog box titled "Edit" with a close button (X) in the top right corner. It contains the following fields and controls:

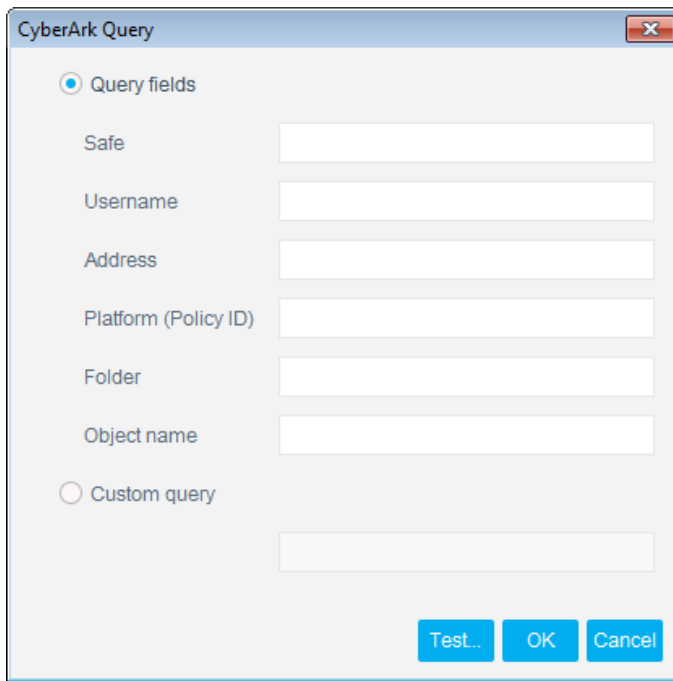
- Domain Administrator: Text input field.
- Domain Name: Text input field.
- Password source: Dropdown menu with "CyberArk" selected and a blue button with three dots to its right.
- Domain Password: Password input field with masked characters (*****).
- Retype Domain Password: Password input field with masked characters (*****).
- OK and Cancel buttons: Located at the bottom right of the dialog box.

5. Enter the following information:


| | |
|-----------------------------|---|
| Domain Administrator | The domain administrator for the endpoints that are to be handled by the module |
| Domain Name | The domain name for the endpoints that are to be handled by the module |

 *The Domain Password in this dialog box is not needed when working with CyberArk as a password source.*

- In the Password Source field, select **CyberArk**. The CyberArk Query dialog box opens.



- Enter the following information.

 *Not all fields in a CyberArk query to the Vault are mandatory. The fields needed for each query depend on the definitions and structure in the safe and for each set of objects in that safe. A query must be formulated so that it only returns a single object. If you specify the safe and object, but not the folder, the root folder will be used by default.*

| | |
|-----------------------------|---|
| Safe | The name of the safe being queried in the vault. |
| Username | A custom property defined for an object in the safe. |
| Address | A custom property defined for an object identifying the location of the object in the safe. |
| Platform (Policy ID) | A custom property identifying an object in a safe. |
| Folder | The name of the folder being queried in the safe. |

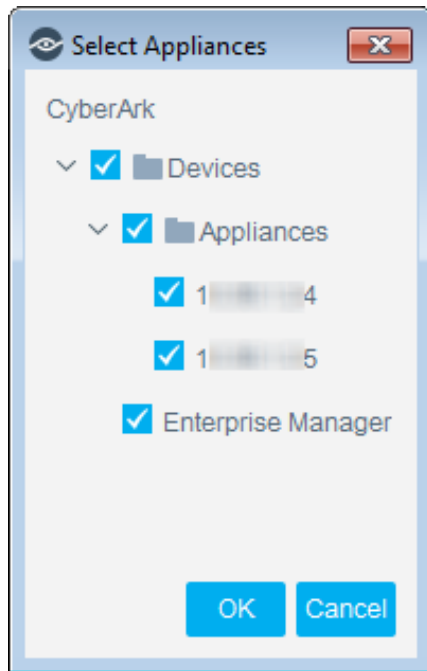
| | |
|--------------------|---|
| Object Name | The name of the object inside the queried folder. |
|--------------------|---|

Optionally, you can enter a *Custom Query* according to the following format:

- For a simple Custom Query for a single account:
`Safe=<safe name>;Folder=<folder name>;Object=<object name>`
- For a Custom Query to a dual account:
`Safe=<safe name>;Folder=<folder name>;VirtualUserName=<virtual user name>`

For more information see the *CyberArk Credential Provider and Application Server Credential Provider Implementation Guide*

8. Select **Test** to test the connection.



Select an Appliance connection to test. If there are a number of devices configured, select one device at a time to be tested.

The test attempts to draw an object containing credentials from the Vault, if the query is not formulated correctly, or returns more than a single object, the test fails.

9. If the test is successful, select OK.
10. Select **Apply** to save the settings.


Configure the Module for Reporting Discovered Privileged Accounts

This section 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:

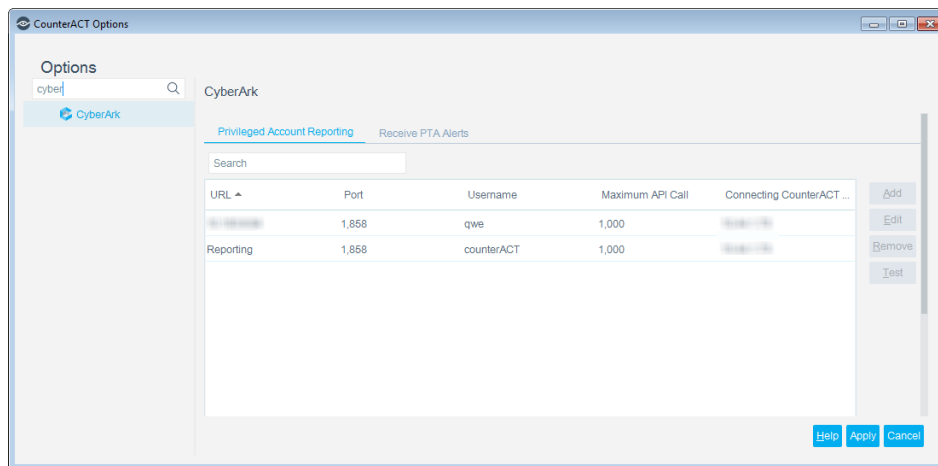
- An unmanaged privileged account is reported to the web service, and labeled as *Pending*
- The Pending account is *On Boarded* to the Vault by a Vault Admin
- The privileged account is now *managed* by the Vault.

For more information see the CyberArk documentation for the *Pending Account Security Web Service*.

 *The Extended Module 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 for reporting privileged accounts:

1. In the CounterACT Console Tools menu, select **Options** and navigate to **Modules**.
2. In the **Modules** pane, select **CyberArk** and then select **Configure**. The CyberArk pane opens.



3. Select the **Privileged Account Reporting** tab.
4. Select **Add**. The Add Device dialog box opens.

5. Enter the following information:


| | |
|---|--|
| URL | The URL of the CyberArk Pending Account Security Web Service that receives retrieved privileged account information. |
| Port | The default port (443) for communicating with the Pending Account Security Web Service. |
| Username | The user name needed to log in to the Pending Account Security Web Service. |
| Password | The password needed to log in to the Pending Account Security Web Service. |
| Verify Password | Re-enter the password for verification. |
| Maximum API calls per 10 minutes | Select Use Default (1000) or select Specify to set a different maximum value. |
| Connecting CounterACT Device | Select a CounterACT connecting device from the list. This is the device that reports the newly discovered or changed accounts. |

6. Select **OK** to save the module configuration.

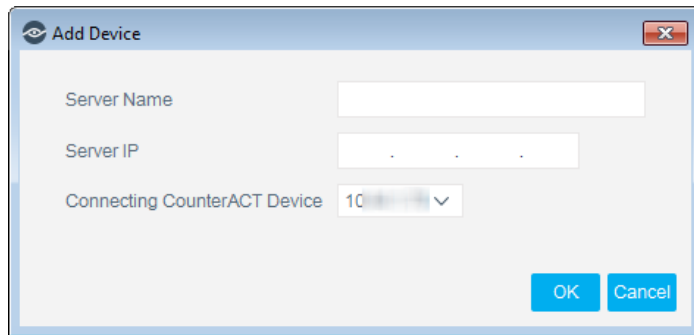
Configure the Module to Receive PTA Alerts

This section describes how to configure the module to receive event alerts from the CyberArk PTA. You can create CounterACT policies that apply actions based on the information in a PTA Alert. See [CyberArk PTA Alert Policy Template](#).

1. Before configuring the Extended Module 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 CounterACT Console Tools menu, select **Options** and navigate to **Modules**.
3. In the **Modules** pane, select *CyberArk* and then select **Configure**. The CyberArk pane opens.
4. Select the **Receive PTA Alerts** tab.
5. Select **Add**. The Add Device dialog box opens.



6. Enter the following information:

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

7. Select OK and select Apply to save the configuration.


Run CyberArk Policy Templates

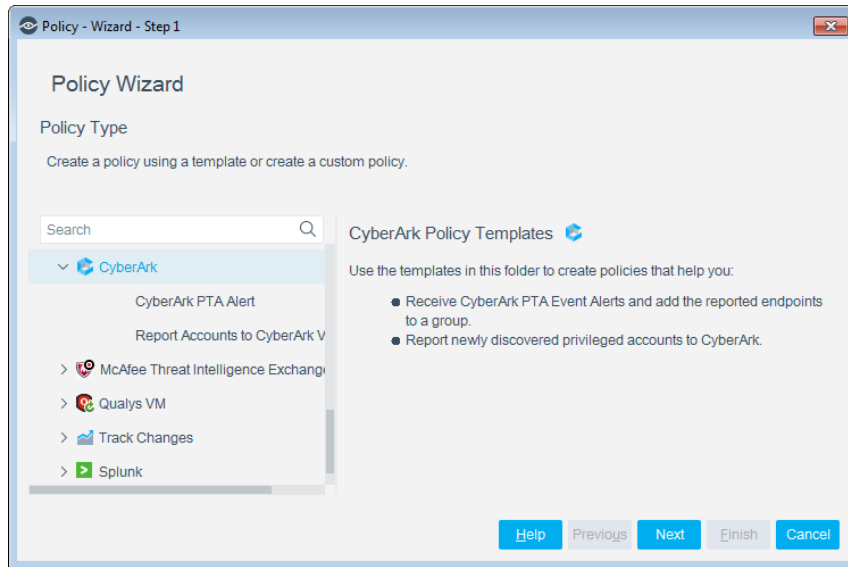
CounterACT templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

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 CounterACT policies:

- [Report Accounts to CyberArk Vault Policy Template](#)
- [CyberArk PTA Alert Policy Template](#)

 *It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters in the CounterACT Administration Guide or select CounterACT Templates and Policy Management from the Help menu in the CounterACT Console.*

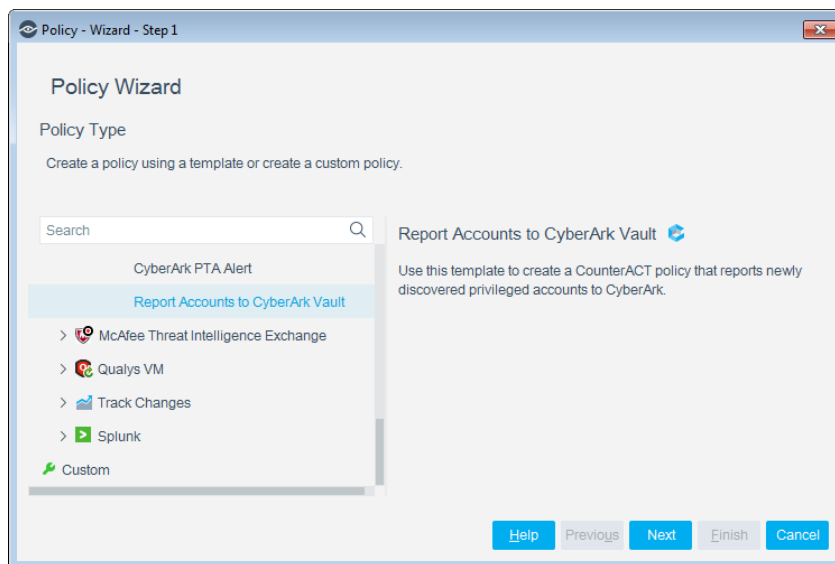


Report Accounts to CyberArk Vault Policy Template

This template creates a policy used for reporting privileged account on endpoints that are not managed or listed by CyberArk.

To run the template:

1. Log in to the CounterACT Console, and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **CyberArk** folder and select Report Accounts to CyberArk Vault. The Report Accounts to CyberArk Vault pane opens.

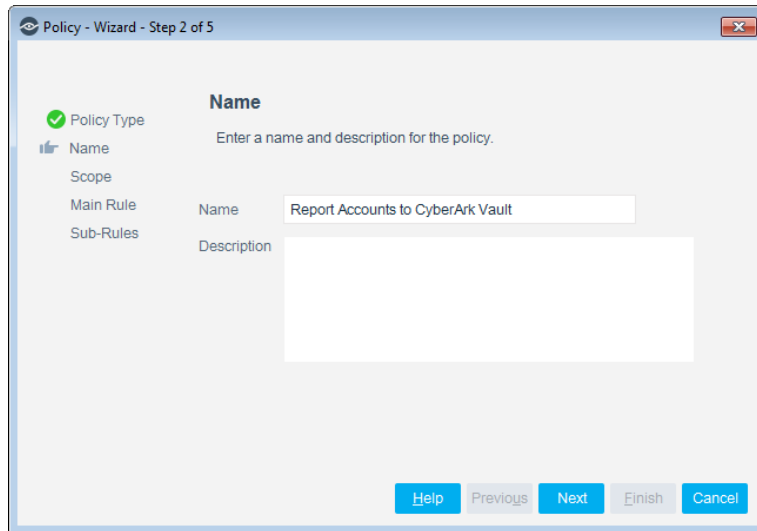


4. Select **Next**. The **Name** pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.



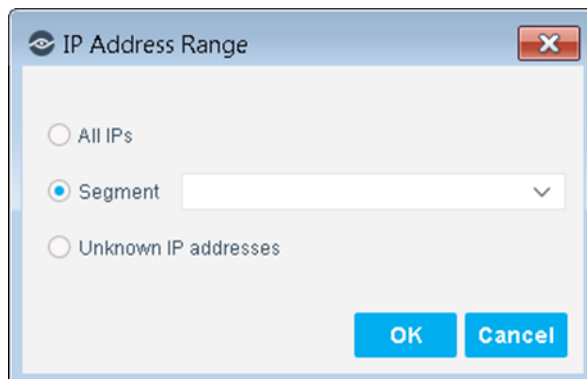
Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

6. Select **Next**. The Scope pane and IP Address Range dialog box opens.

Define which Hosts will be Inspected - Policy Scope

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 appears in the Scope pane.
 9. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
 10. Select **Finish**. The policy is created.
 11. Select **Apply** to save the policy.

Main Rule

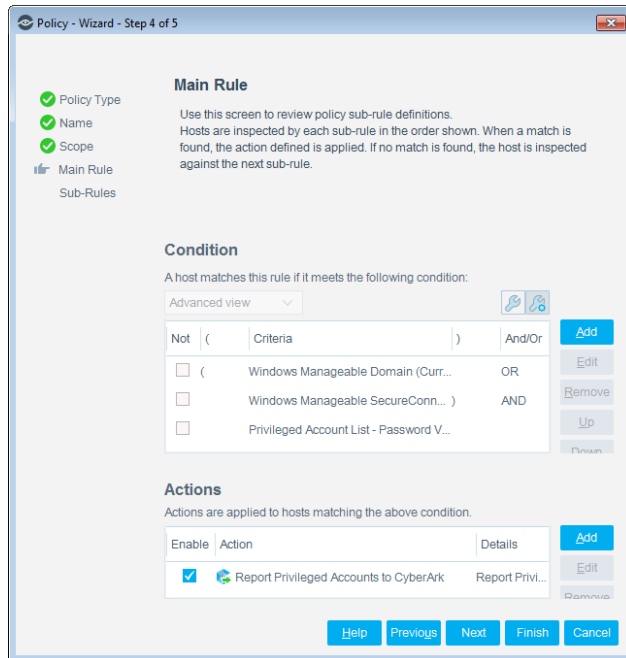
When the Main Rule is applied, CounterACT detects privileged account that have been added or removed from managed endpoints since the last recheck, and reports them to CyberArk. The default scan interval for rechecking privileged accounts is 8 hours.

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.

To edit the Main Rule:

12. Select the Report Accounts to CyberArk Vault policy and select Edit. The policy pane opens.



13. Select a Main Rule and select Edit. The Main Rule pane opens, and you can Add or Edit the conditions and actions for this rule.

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.

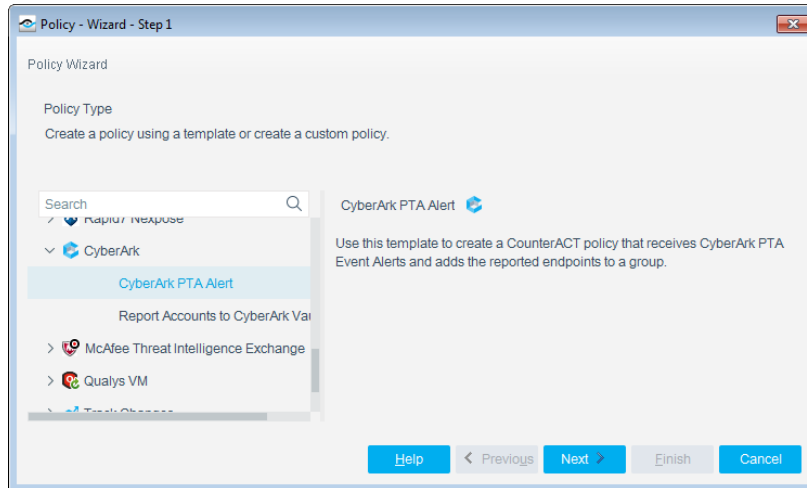
CyberArk PTA Alert Policy Template

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 use the PTA Alert policy template:

1. Log in to the CounterACT Console and select the **Policy** tab.

2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the CyberArk folder and select CyberArk PTA Alert. The CyberArk PTA Alert pane opens.

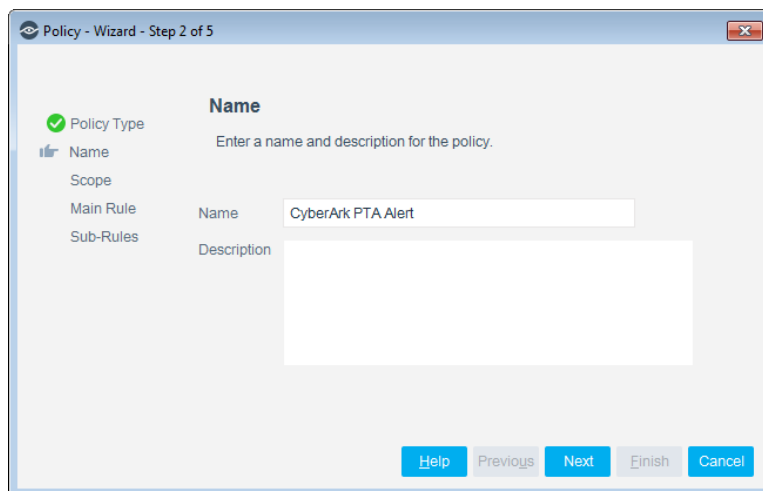


4. Select **Next**. The **Name** pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description



Naming Tips

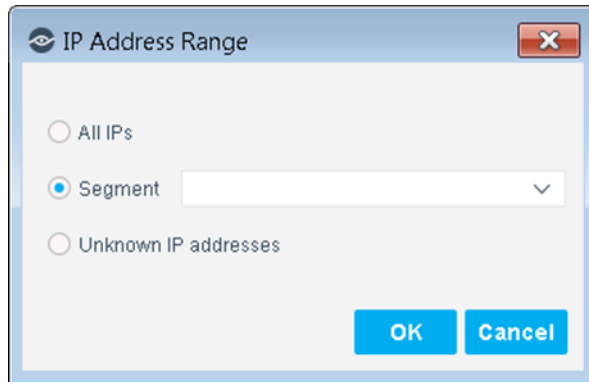
- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.

- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

6. Select **Next**. The **Scope** pane and IP Address Range box open.

Define which Hosts will be Inspected - Policy Scope

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 appears in the Scope pane.

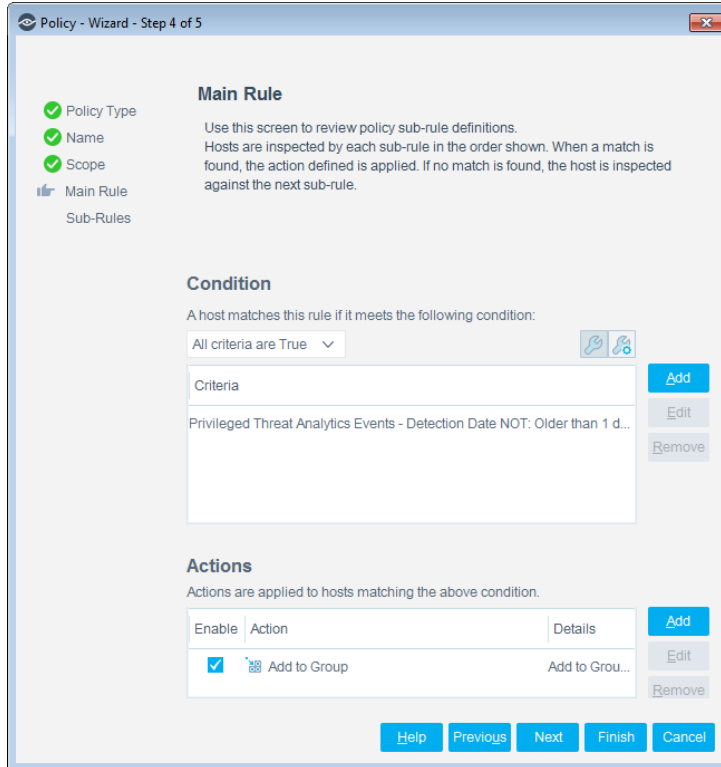
9. Select **Next**. The Main Rule pane opens.

Main Rule

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 CounterACT group *CyberArk PTA Alert Endpoints*.



Sub-Rules

The PTA Alert functionality does not require a policy sub-rule.

10. Select **Next**. The Sub-Rules pane opens.
11. Select **Finish**. The policy is created.
12. Select **Apply** to save the policy.

Using Information from PTA Alerts

PTA Alert information received by CounterACT 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 that have been detected by CounterACT, 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 at stealing 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 instance, 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 which 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.

Using CyberArk

This section covers how to best utilize the CyberArk Module.

Best Practices

Windows Endpoint Credential Management

CounterACT may manage Windows endpoints via remote inspection using supplied Active Directory credentials in the HPS Inspection Engine plugin. CyberArk can manage these credentials.

Password Change Frequency

CounterACT 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, but may 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, CounterACT can identify local accounts present on Windows endpoints, and compare them to accounts that exist on CyberArk. When a local account exists that is not managed by CyberArk, CounterACT can report it to CyberArk. There is no direct best practice guidance for this feature other than to utilize it.

CyberArk PTA Notification to CounterACT 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 CounterACT via Syslog, creating an actionable property that CounterACT 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 CounterACT 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 CounterACT Console, it is best practice not to have any local accounts on CounterACT. Wherever possible, CyberArk should manage accounts that CounterACT uses.

CounterACT Accounts

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

Accounts Used by CounterACT

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

Non-Administrative Accounts

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

Direct CyberArk Login to CounterACT Console

Using CyberArk's Privileged Session Manager (PSM), users can log into CounterACT directly.

Requirements

The CounterACT 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 CounterACT Console.

Recommendation

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

CounterACT to CyberArk Mapping

Each CounterACT appliance can point to a single CyberArk Vault. If more than one CyberArk Vault exists in the enterprise, then 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, then the CounterACT appliance(s) should also be matched to that region, connecting to the regional CyberArk and managing endpoints in that same region.

CounterACT Disassociation from CyberArk

When CounterACT disassociates its connection to CyberArk, which can happen when the appliance physically fails or is otherwise manually and permanently disconnected, it will need to be reconnected to CyberArk again.

CyberArk Accounts

When a CounterACT appliance initially connects to CyberArk, a unique account is created. When a CounterACT appliance then disassociates with CyberArk, the account is left on CyberArk. This will inherently disallow the appliance to reconnect, and the account must first be removed from CyberArk.

CounterACT 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 will work because of the newly unique IP address, but the account created from the old IP address will still exist on CyberArk and should be updated.

CyberArk Application ID

The CounterACT application ID must be defined in CyberArk *before* CounterACT configuration. This ID is not unique among CounterACT appliances and will be 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.

Access the Asset Inventory

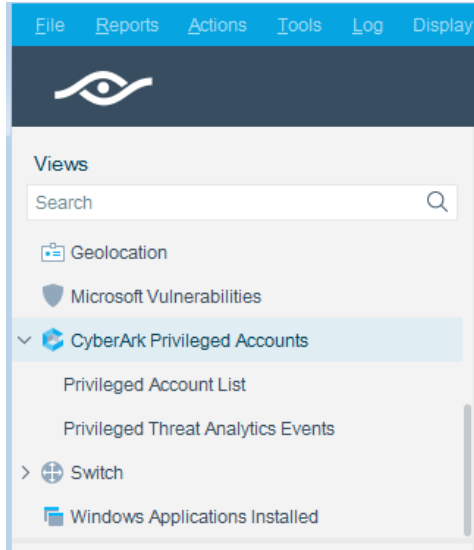
Use the CounterACT Asset Inventory to view a real-time display of the module network activity at multiple levels.

The Asset Inventory lets you:

- View Privileged Accounts that have been detected
- Incorporate inventory detections into policies

To access the inventory:

1. Select **Asset Inventory** from the Console toolbar.
2. Navigate to the CyberArk entries.



The following information is available:

- Privileged Accounts List: displays a table of privileged accounts.
- PTA Events: displays reported PTA events, and a list of hosts to which the events are attributed.

Refer to *Working at the Console> Working with Inventory Detections* in the *CounterACT Administration Guide* or the Console, Online Help for information about how to work with the CounterACT Inventory.

Endpoint Module Information

The ForeScout CounterACT® Endpoint Module provides connectivity, visibility and control to network endpoints through the following CounterACT components:

- HPS Inspection Engine
- Hardware Inventory Plugin
- Linux Plugin
- Microsoft SMS/SCCM Plugin
- OS X Plugin

The Endpoint Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are installed and rolled back with the Endpoint Module.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

Customer Portal


The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to <https://forescout.force.com/support/>.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

 If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

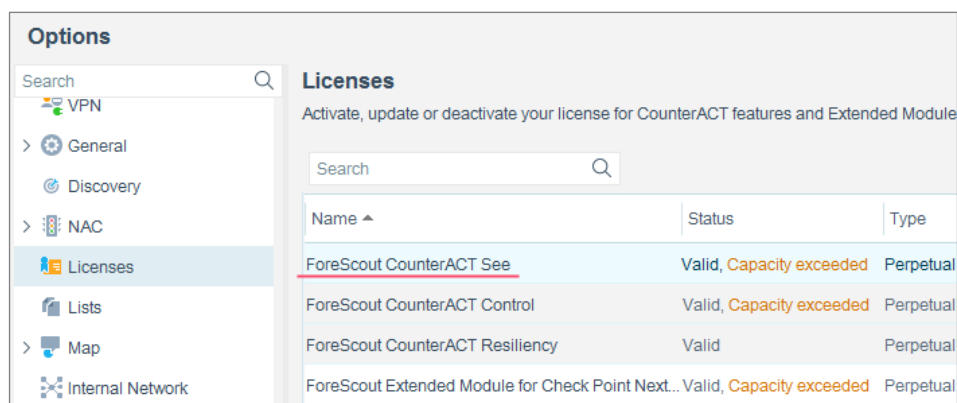
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



The screenshot shows the 'Options' menu with 'Licenses' selected. The 'Licenses' section displays a table with the following data:

| Name | Status | Type |
|---|--------------------------|-----------|
| ForeScout CounterACT See | Valid, Capacity exceeded | Perpetual |
| ForeScout CounterACT Control | Valid, Capacity exceeded | Perpetual |
| ForeScout CounterACT Resiliency | Valid | Perpetual |
| ForeScout Extended Module for Check Point Next... | Valid, Capacity exceeded | Perpetual |

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-27 20:31