ForeScout® Extended Module for CyberArk

Configuration Guide

Version 1.0.0 and Above

Table of Contents

About the CyberArk Integration

ForeScout® 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.

- Credential Retrieval from CyberArk Enterprise Password Vault
- Discovering and Reporting Local Privileged Accounts
- Receiving Privileged Threat Analytics Alerts

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 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.

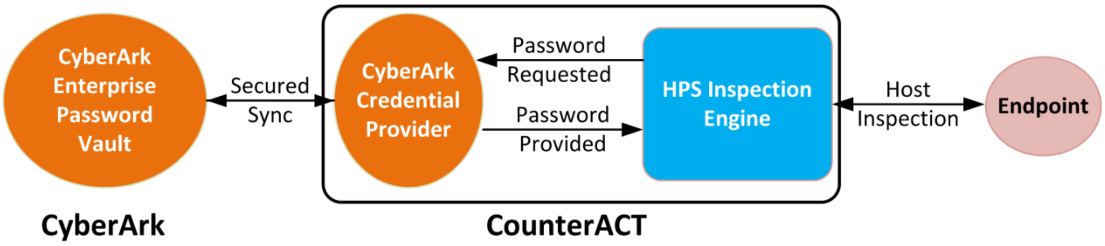
To use the different features of this module, you should have a solid understanding of the CyberArk Privileged Account Security Solution and the functionality and terminology of the CyberArk Enterprise Password Vault.

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. Install the Module.
3. Configure the Module.
4. Run CyberArk Policy Templates.

Requirements

This section presents the following requirements:

- CounterACT Software Requirements
- Supported Vendor Requirements
- Networking Requirements
- Endpoint Requirements

CounterACT Software Requirements

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

- CounterACT version 7.0.0
- HPS Inspection Engine , version 10.7.0 or above
- Service Pack 3.0.0 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.
- Syslog Plugin, version 3.2.0 or above

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

ForeScout Module License Requirements

This ForeScout Module requires a module license. The installation package for the module is in the form of a CounterACT plugin. When installing the plugin 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.

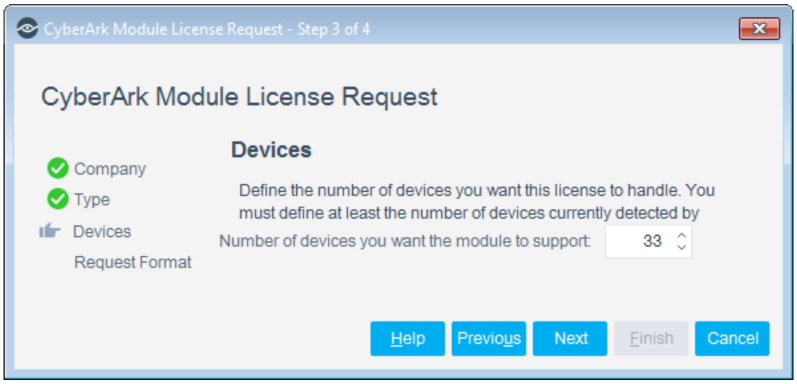
When the demo period expires, you will be required to purchase a permanent module license. *In order to continue working with the module, you must purchase the license*.

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

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.



CyberArk Module License Request - Step 3 of 4

CyberArk Module License Request

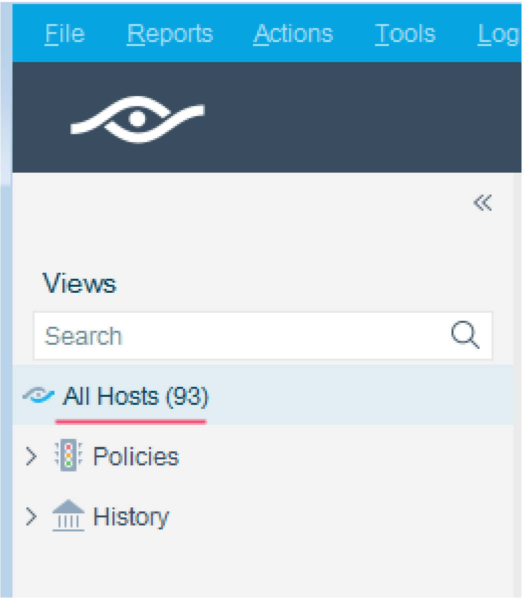
Devices

Define the number of devices you want this license to handle. You must define at least the number of devices currently detected by

Number of devices you want the module to support: 33

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.



More License Information

See the CounterACT Console User Manual for information on requesting a permanent license or a demo license extension. 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.

The installation package for the module is in the form of a CounterACT plugin.

To install the plugin:

1. Acquire the plugin **`.fpi`** file from your ForeScout representative or contact beta@forescout.com.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.
7. Select **Install**.
8. If you have not yet purchased a permanent module license, a message appears indicating that the plugin will be installed with a demo module license. Select **Yes** and then select **Install**.
9. An installation or upgrade information dialog box and an End User License Agreement will open. Accept the agreement to proceed with the installation.
10. When the installation completes, select **Close**. The plugin is displayed in the Plugins pane. The **Module Status** column indicates the status of your license. See ForeScout Module License Requirements or the *CounterACT Console User Manual* for details on requesting a permanent license or a demo license extension.
11. Select the plugin and select **Start**. The Select Appliances dialog box opens.
12. Select the CounterACT devices on which to start the plugin.
13. Select **OK**. The plugin runs on the selected devices.

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:

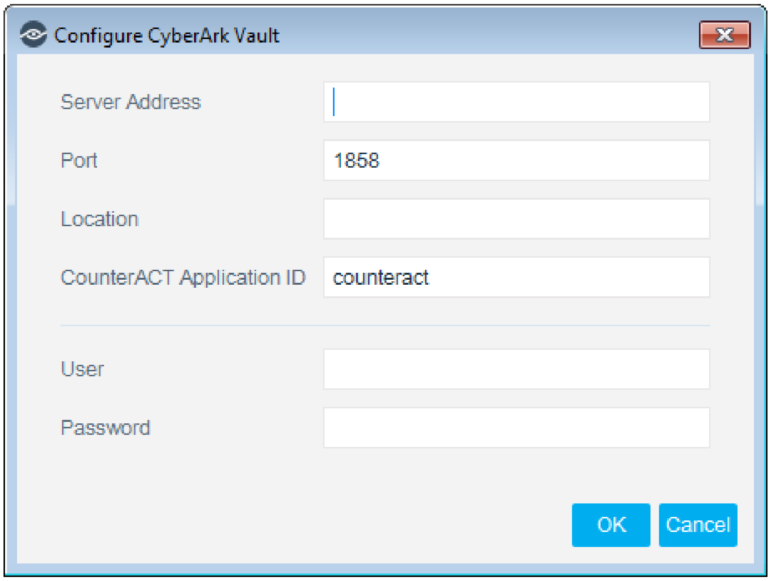
- Communicate with the CyberArk Enterprise Password Vault using the CyberArk Credential Provider installed in a CounterACT device.
- Query the Vault to receive credentials required by the HPS Inspection Engine to access and preform Remote Inspection on endpoints.

🗎 *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.*



Server Address

Port 1858

Location

CounterACT Application ID counteract

User

Password

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 plugin configuration.

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:

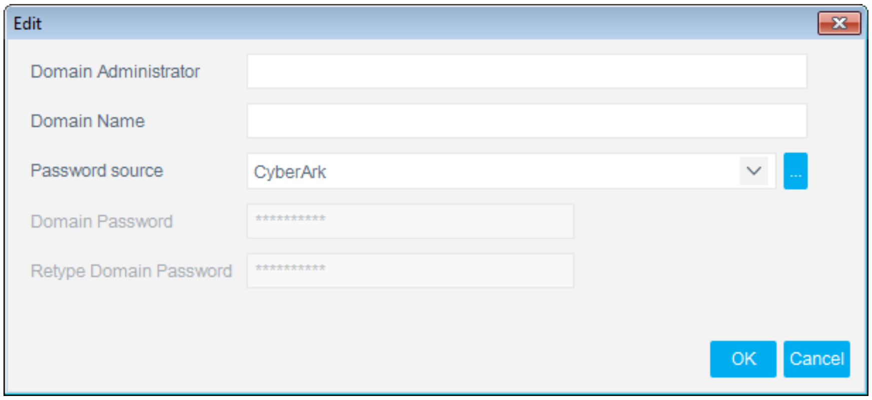
1. Log in to the CyberArk PrivateArk server, and log in to the Vault.
2. Select **Tools > Administrative Tools > Users and Groups**, the Users and Groups dialog box opens.
3. Select the new User (*Counteract_<name or IP address>*) that was created by the Provider installation.
4. Select **Safe Ownership**. 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** plugin.
3. In the HPS Inspection Engine pane, select the Remote Inspection tab.

4. Select **Add**. The Add dialog box opens.


Edit

Domain Administrator

Domain Name

Password source: CyberArk

Domain Password: **********

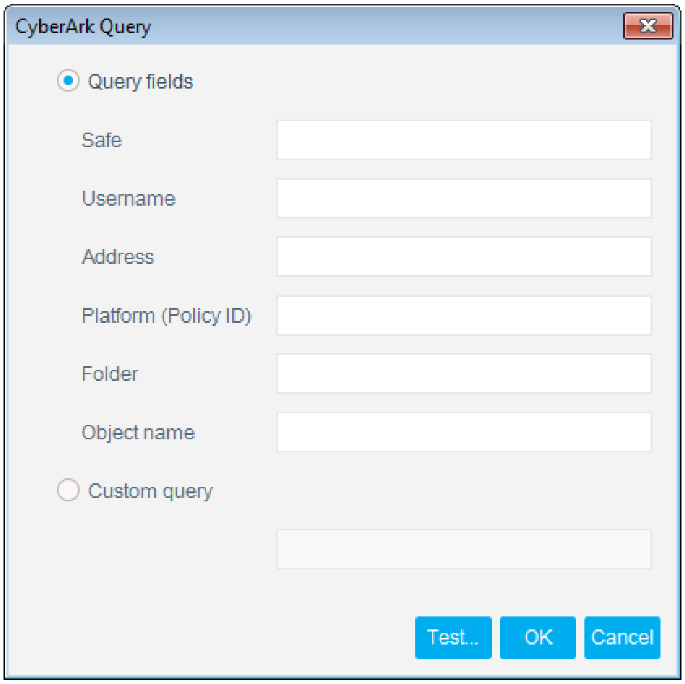
Retype Domain Password: **********

5. Enter the following information:

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

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

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


CyberArk Query

● Query fields

Safe

Username

Address

Platform (Policy ID)

Folder

Object name

○ Custom query

7. 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.

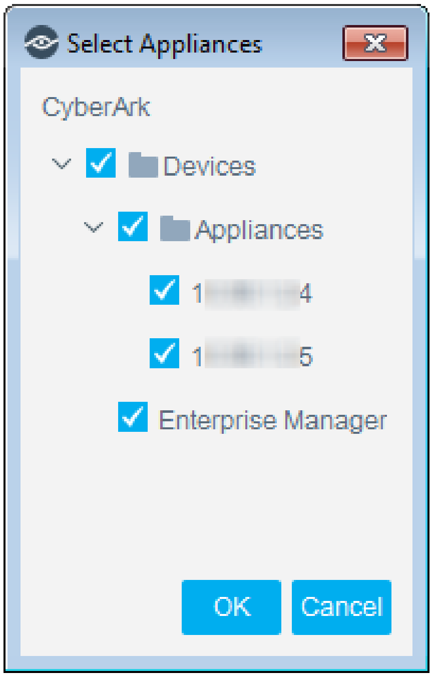
Safe	The name of the safe being queried in the vault
Username	A custom property defined for an object in the safe
Address	A custom property defined for an object identifying the location of the object in the safe
Platform (Policy ID)	A custom property identifying an object in a safe
Folder	The name of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

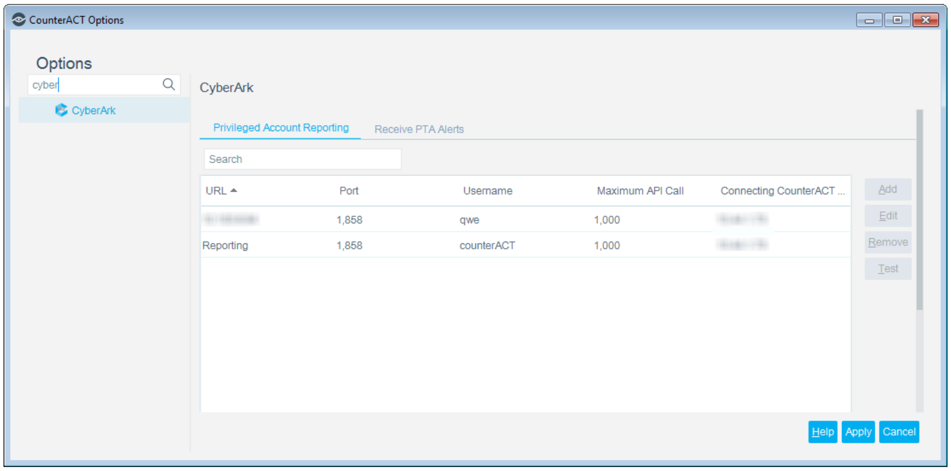
- An unmanaged privileged account is reported to the web service, and labeled as *Pending*
- The Pending account is *On Boarded* to the Vault by a Vault Admin
- The privileged account is now *managed* by the Vault.

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:

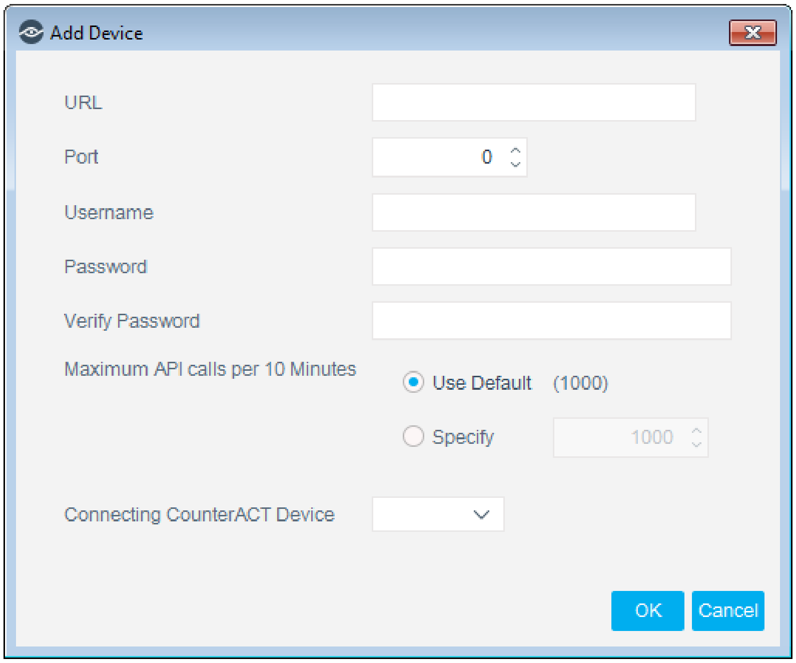
1. In the CounterACT Console Tools menu, select **Options** and navigate to **Plugins**.
2. In the **Plugins** pane, select CyberArk and then select **Configure**. The CyberArk pane opens.



CyberArk

URL ▲	Port	Username	Maximum API Call	Connecting CounterACT ...
[redacted]	1,858	qwe	1,000	[redacted]
Reporting	1,858	counterACT	1,000	[redacted]

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



URL

Port 0

Username

Password

Verify Password

Maximum API calls per 10 Minutes ● Use Default (1000) ○ Specify 1000

Connecting CounterACT Device

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 plugin configuration.

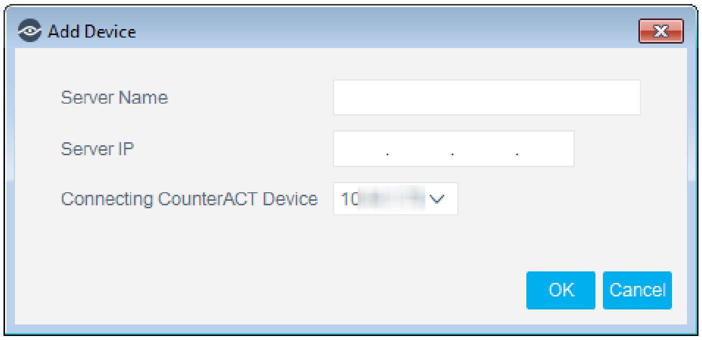
Configure the Module to Receive PTA Alerts

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 > Plugins > Syslog > Configure*** *pane.*

2. In the CounterACT Console Tools menu, select **Options** and navigate to **Plugins**.
3. In the **Plugins** 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.



Add Device

Server Name

Server IP . . .

Connecting CounterACT Device 10[redacted]

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

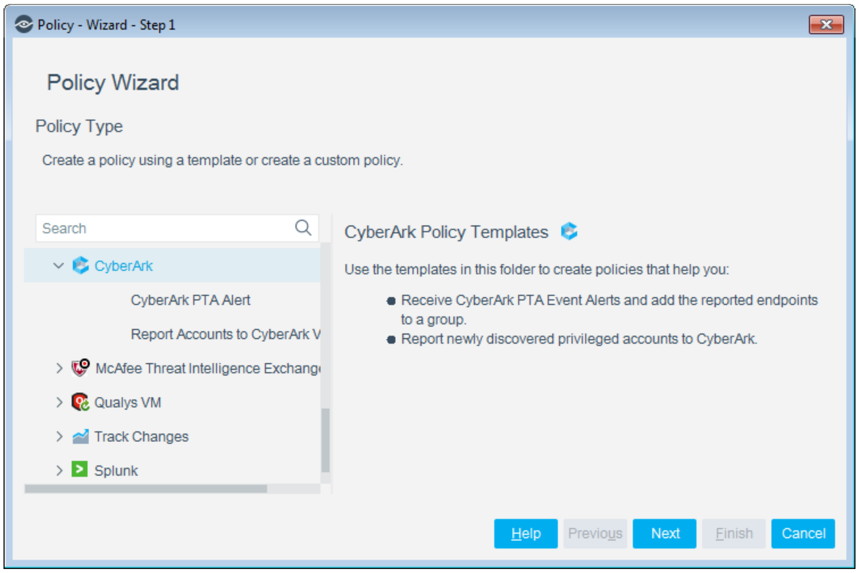
CounterACT templates help you quickly create important, widely used policies that easily control endpoints and can guide users to compliance.

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 Console User Manual or select CounterACT Templates and Policy Management from the Help menu in the CounterACT Console.*



Create a policy using a template or create a custom policy.

Use the templates in this folder to create policies that help you:

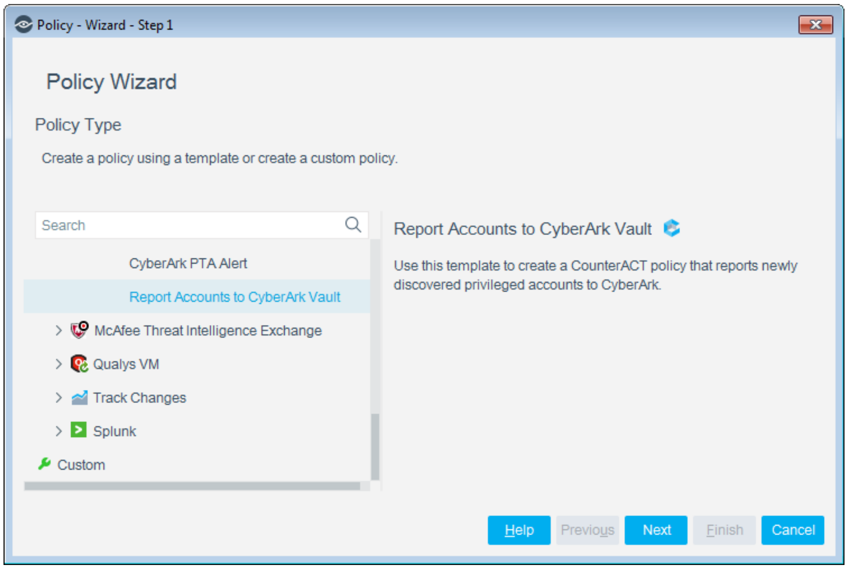
- Receive CyberArk PTA Event Alerts and add the reported endpoints to a group.
- Report newly discovered privileged accounts to CyberArk.

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.



Policy - Wizard - Step 1

Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

Report Accounts to CyberArk Vault

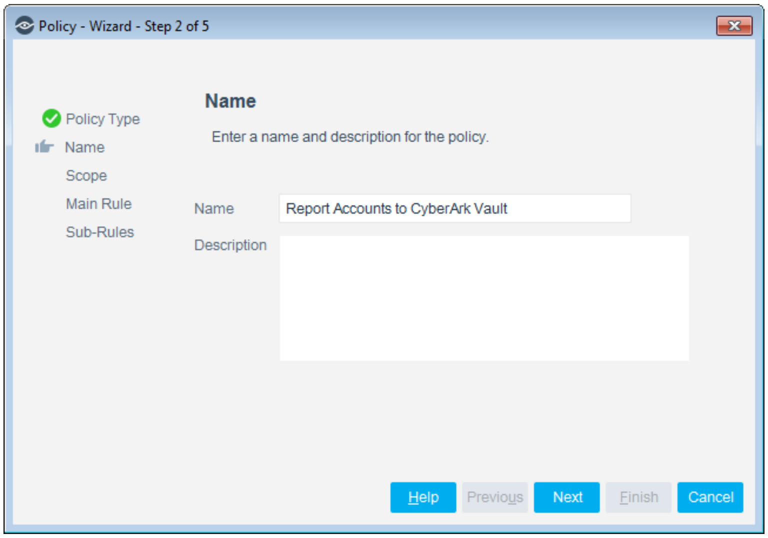
Use this template to create a CounterACT policy that reports newly discovered privileged accounts to CyberArk.

4. Select **Next.** The **Name** page 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.

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



Policy - Wizard - Step 2 of 5

Name

Enter a name and description for the policy.

Name: Report Accounts to CyberArk Vault

Description:

Naming Tips

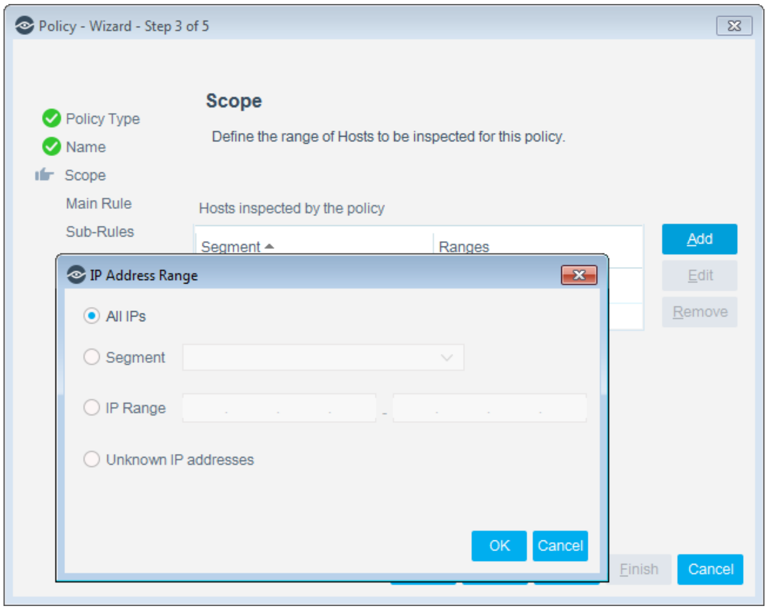
- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be taken.

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

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

Define which Hosts will be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.



Define the range of Hosts to be inspected for this policy.

1. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

All IPs	Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
Segment	Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope page.
IP Range	Define a range of IP addresses. These addresses must be within the Internal Network.
Unknown IP addresses	Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

🗎 *Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.*

2. Select **OK**. The added range appears in the Scope pane.
3. Select **Next**. The Sub-Rules pane opens. There are no default Sub-Rules in this policy template.
4. Select **Finish**. The policy is created.

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

Main Rule

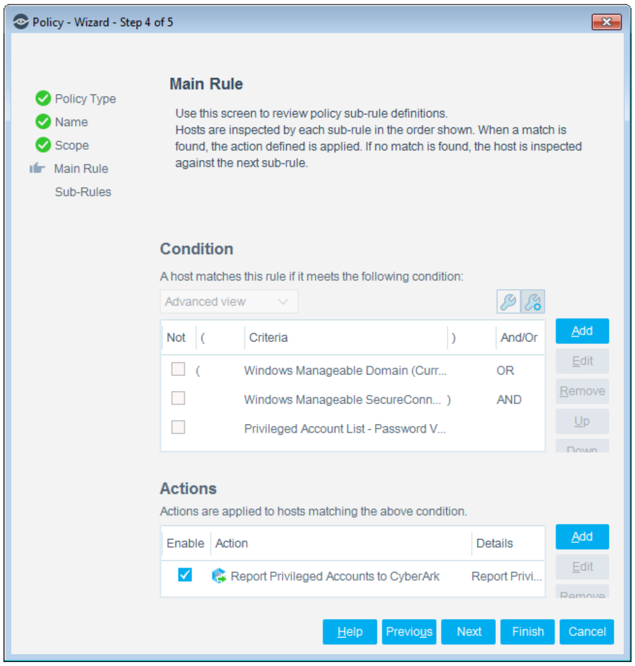
When the Main Rule is applied, CounterACT detects privileged account that have been added or removed from managed endpoints since the last recheck, and reports them to CyberArk. The default scan interval for rechecking privileged accounts is 8 hours.

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 a Secure Connector.
- The privileged account has not been reported, or exists in the pending account list.

To edit the Main Rule:

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



Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

Not	(	Criteria	)	And/Or
□	(	Windows Manageable Domain (Curr...		OR
□		Windows Manageable SecureConn...	)	AND
□		Privileged Account List - Password V...		

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
☑	Report Privileged Accounts to CyberArk	Report Privi...

2. 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.*

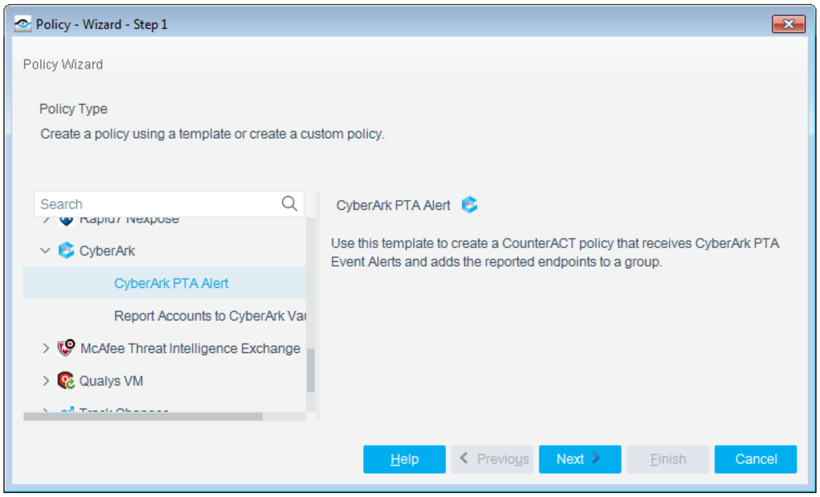
    OR
  - Updated from *exists in pending account list* to *managed.*
- Once the *CyberArk Pending Account List* is updated, the CyberArk operator needs to go to the CyberArk management console, review the newly added accounts in the *Pending Account List,* and onboard them to make them managed by CyberArk.

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.



Policy - Wizard - Step 1

Policy Wizard

Policy Type

Create a policy using a template or create a custom policy.

CyberArk PTA Alert

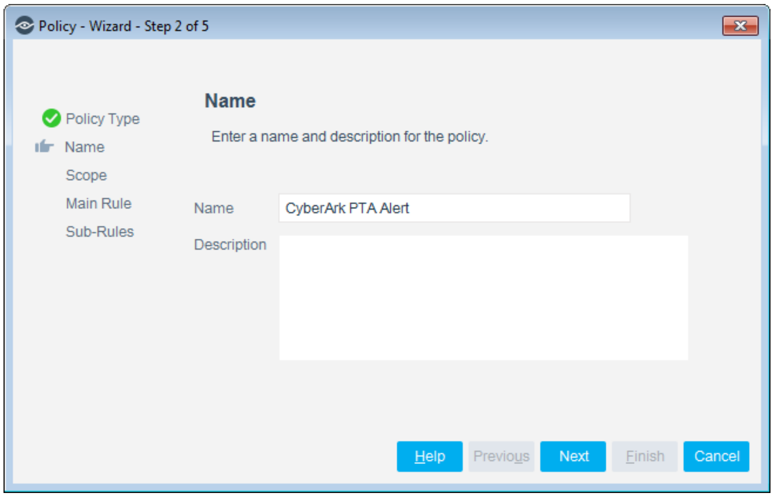
Use this template to create a CounterACT policy that receives CyberArk PTA Event Alerts and adds the reported endpoints to a group.

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.

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



Name

Enter a name and description for the policy.

Name: CyberArk PTA Alert

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.

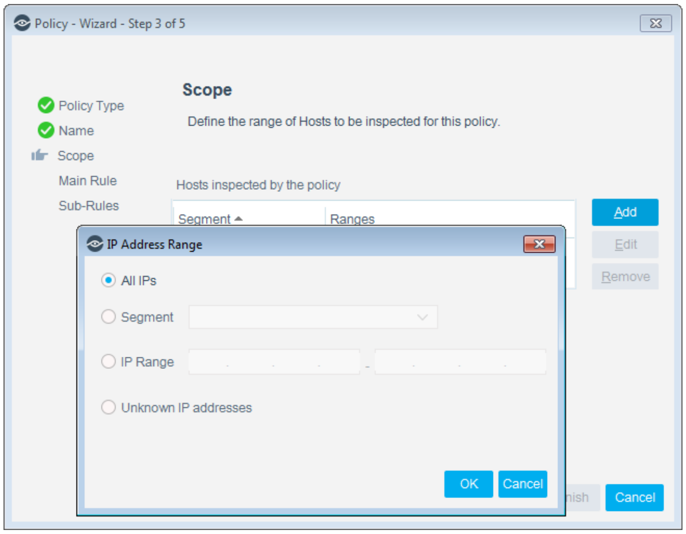
– Ensure that the name indicates whether the policy criteria must be met or not met.

– Avoid having another policy with a similar name.

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

Define which Hosts will be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.



Scope

Define the range of Hosts to be inspected for this policy.

Hosts inspected by the policy

Segment ▲	Ranges

IP Address Range

● All IPs

○ Segment

○ IP Range

○ Unknown IP addresses

3. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

All IPs	Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
Segment	Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope page.
IP Range	Define a range of IP addresses. These addresses must be within the Internal Network.
Unknown IP addresses	Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

🗎 *Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.*

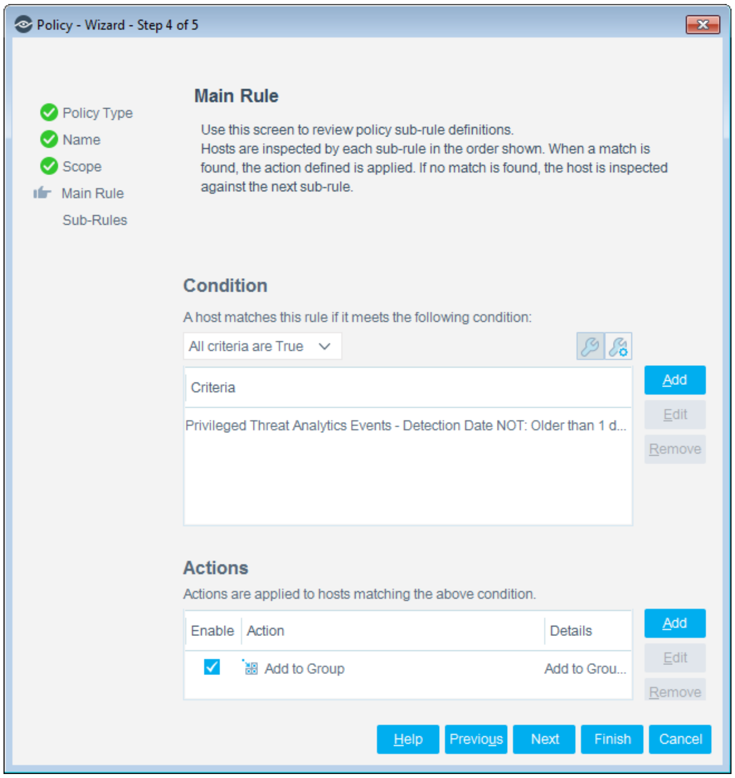
4. Select **OK**. The added range appears in the Scope pane.
5. Select **Next**. The Main Rule pane opens.

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*.


Policy - Wizard - Step 4 of 5

Main Rule

Use this screen to review policy sub-rule definitions.
Hosts are inspected by each sub-rule in the order shown. When a match is found, the action defined is applied. If no match is found, the host is inspected against the next sub-rule.

Condition

A host matches this rule if it meets the following condition:

All criteria are True

Criteria
Privileged Threat Analytics Events - Detection Date NOT: Older than 1 d...

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
☑	Add to Group	Add to Grou...

Sub-Rules

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

1. Select **Next**. The Sub-Rules pane opens.
2. Select **Finish**. The policy is created.
3. 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.

Displaying CyberArk Inventory Information

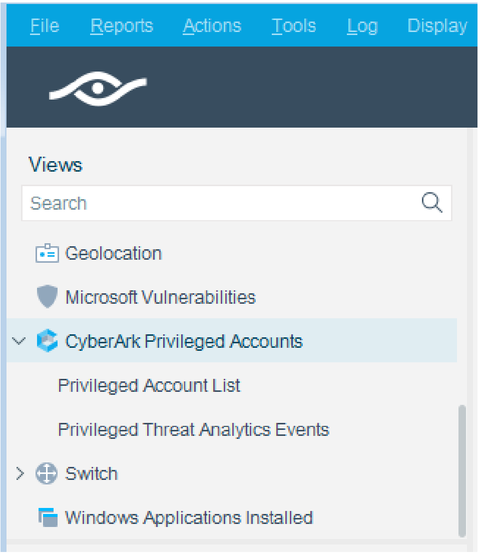
Use the CounterACT Inventory to view a real-time display of the module network activity at multiple levels.

The inventory lets you:

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

To access the inventory:

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


File
Reports
Actions
Tools
Log
Display
Views
Search
Geolocation
Microsoft Vulnerabilities
CyberArk Privileged Accounts
Privileged Account List
Privileged Threat Analytics Events
Switch
Windows Applications Installed

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 Console User's Manual* or the Console, Online Help for information about how to work with the CounterACT Inventory.

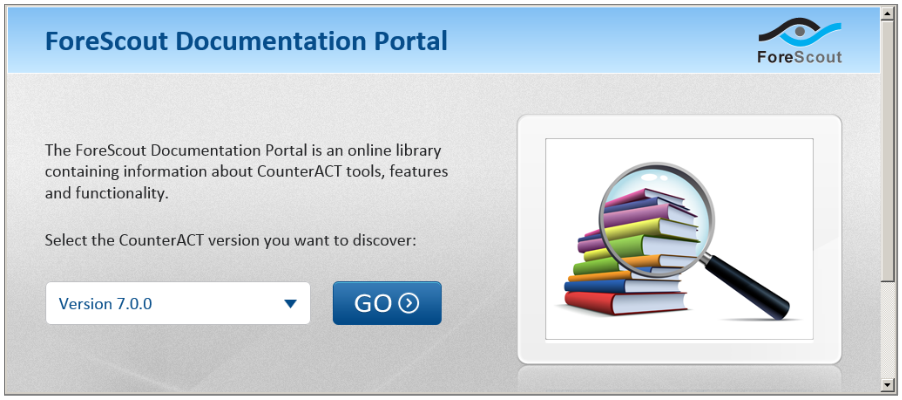
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

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



ForeScout Documentation Portal

The ForeScout Documentation Portal is an online library containing information about CounterACT tools, features and functionality.

Select the CounterACT version you want to discover:

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.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:

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

CounterACT Console Online 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.

Console User Manual

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 **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

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

Legal Notice

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service (“ActiveCare”), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
    - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
    - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
    - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-06-18 15:36