ForeScout

ForeScout CounterACT®

Hybrid Cloud Module: Amazon® Web Services (AWS) Plugin

Configuration Guide

Version 1.3

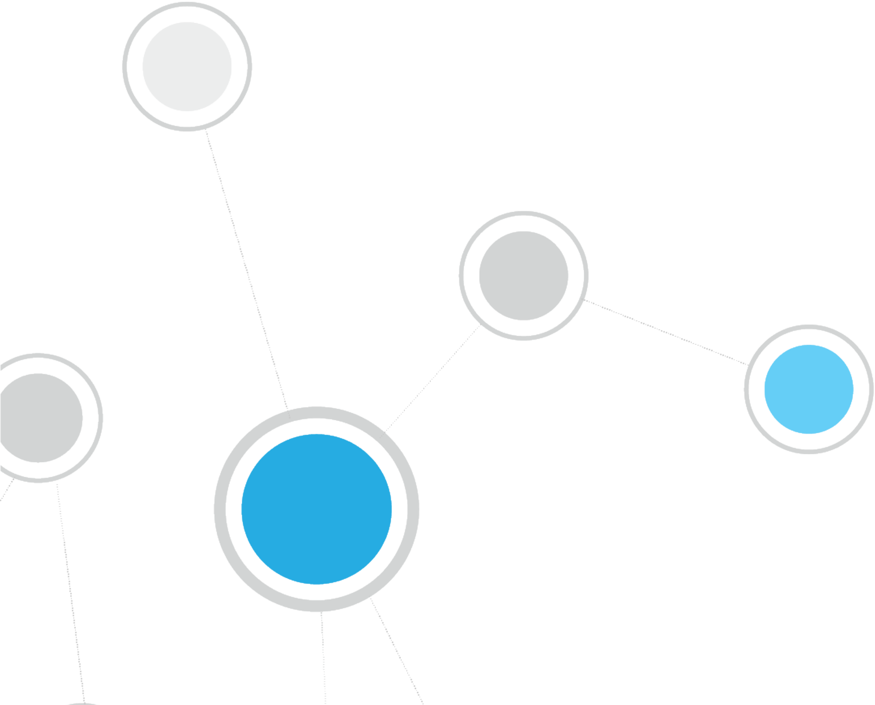


Table of Contents

Amazon Web Services Plugin Overview 4

Use Cases 5

Providing Consolidated Visibility 5

Dynamic Segmentation of Instances 5

Security Management of EC2 Instances 5

Detect and Prevent Unauthorized Access to and from EC2 Instances 5

How It Works 6

What to Do 6

Additional Amazon Web Services Documentation 6

Requirements 6

CounterACT Software Requirements 7

AWS Requirements 7

Networking Requirements 8

About Support for Dual Stack Environments 8

Define AWS Users 8

Configure the Plugin 9

Add an AWS Connection 9

Verify That the Plugin Is Running 13

Test the AWS Connection 13

Configure AWS Policy Templates 13

AWS EC2 AMI Classification Template 14

Updating the AMI Whitelist 16

AWS EC2 External Instance Classification Template 18

Detecting Cloud Endpoints – Host Properties 20

AWS CloudWatch Flow Logs 20

AWS EC2 23

Managing AWS Cloud Endpoints 25

AWS Admission Events 26

Manually Run AWS Actions on any EC2 Instance 26

EC2 Security Group Action 27

Disable EC2 Termination Protection Action 28

Enable EC2 Termination Protection Action 30

Start an EC2 Instance 31

Stop an EC2 Instance 32

Best Practices for Working with the AWS Plugin 33

Hybrid Cloud Module Information 34

Additional CounterACT Documentation 34

Documentation Downloads 34
Documentation Portal 35
CounterACT Help Tools...35

Amazon Web Services Plugin Overview

The Amazon Web Services Plugin is a component of the ForeScout CounterACT® Hybrid Cloud Module. See Hybrid Cloud Module Information for details about the module.

The AWS Plugin connects to Amazon's public cloud environment to retrieve information on Elastic Compute Cloud (EC2) instances. The instances follow the same rules as any other endpoint discovered by CounterACT where one can define policies and actions on those endpoints. CounterACT integrates with Amazon® Web Services (AWS), bringing the detailed visibility, control and compliance capabilities of CounterACT to instances in the public cloud.

The AWS Plugin enables:

- Visibility of endpoints in Amazon's public cloud
- Creating and applying CounterACT policies
- Maintaining security of cloud endpoints
- Enforcing compliance on endpoints

🗎 *In this guide, the terms "endpoint" and "instances" are used interchangeably.*

This plugin lets you integrate CounterACT with AWS so that you can:

- Have full visibility of your AWS instances and their properties. Since it is often much easier to start and stop instances in a public cloud environment, it's important to have a good understanding of what resources are being used in the cloud. Regular checks provide valuable information on how AWS cloud resources are being utilized. See Manually Run AWS Actions on any EC2 Instance for details.
- Review of data collected from AWS Flow Logs to gain insightful information on communications between instances. This information can be used to detect and prevent unauthorized access to an instance and determine if action needs to be taken. Flow Logs can also be used to discover short-lived instances that may have existed between the polling of AWS. See AWS CloudWatch Flow Logs for details.
- Discover cloud-based endpoints early, thus allowing identification and compliance checking prior to being given full network access. A non-compliant endpoint may be stopped, assigned to a quarantined security group, and the EC2 user may be notified. If automated remediation fails, the endpoint is isolated and stopped to prevent further damage. See EC2 Security Group Action for details.
- Use the CounterACT Asset Inventory to review the distribution of endpoints in the cloud and mitigate as required. For example, endpoints with out-of-date Amazon Machine Images (AMI) are quickly identified for remediation. See Manually Run AWS Actions on any EC2 Instance for details.

- Enable/disable Termination Protection for AWS EC2 instances to prevent accidental termination (deletion) of an EC2 instance. The CounterACT operator implements this by establishing a policy where all compliant and critical EC2 assets have termination protection enabled. See Disable EC2 Termination Protection Action and Enable EC2 Termination Protection Action for details.

Use Cases

This section describes use cases supported by this plugin. To understand how this plugin helps you achieve these goals, see How It Works.

Providing Consolidated Visibility

Integrating with AWS extends CounterACT's capability to see and control instances running in AWS. This allows visibility for both campus endpoints *and* AWS EC2 instances potentially on the same CounterACT Device.

Dynamic Segmentation of Instances

Instances can be segmented or isolated based on their classification and compliance posture. For example, tags can be used to classify and group instances that belong to a particular group such as testing, development, production, etc. Additionally, instances can be classified based on their function such as web, application, or database tier.

Security Management of EC2 Instances

The AWS plugin makes it easy for you to detect EC2 instances configured with either default or non-complaint security groups. You can then take action to remediate that by applying stricter security policies by using your own well-defined security groups, thus making that security group compliant.

Detect and Prevent Unauthorized Access to and from EC2 Instances

This plugin integrates with AWS CloudWatch Flow Logs service to provide deeper visibility of traffic flows for an EC2 instance. It captures incoming and outgoing flows for an instance and records information such as source IP, destination IP, port number, etc., and reports if the flow was accepted or denied.

This information can be used to detect and even prevent any unauthorized access to an EC2 instance. For example, if you find an EC2 instance sending requests or data to an unauthorized machine, that instance can easily be quarantined by replacing its current security groups with a more restrictive security groups.

The AWS CloudWatch Flow Logs can also identify misconfigurations of an EC2 instance. For example, if a database instance is communicating on port 80 (typically used for web traffic), it can be flagged as non-compliant and can be quarantined by applying a security group action isolating the endpoint and preventing further usage of that port.

How It Works

This plugin uses well-defined APIs from AWS to provide visibility of AWS EC2 instances. Once the configuration is complete using AWS Identity and Access Management (IAM) credentials, CounterACT starts communicating with one or more AWS accounts and retrieves information on EC2 instances running in AWS under that account. Many instance-related properties are collected as CounterACT host properties and cloud instances are displayed as endpoints in CounterACT. The queries are invoked based on configured time intervals.

The AWS plugin also pulls CloudWatch Flow Logs information if it is enabled for that AWS account. This information is shown when using the CounterACT session-as-a-server and session-as-a-client properties in policies.

See Best Practices for Working with the AWS Plugin for more information.

What to Do

This section describes steps you should take to set up your system when integrating with AWS environments:

1. Verify that you have met system requirements. See Requirements.
2. Define AWS Users.
3. Configure the Plugin.
4. Use the in-depth information reported by the plugin to manage virtual devices:
   - Configure AWS Policy Templates
   - Managing AWS Cloud Endpoints
   - Manually Run AWS Actions on any EC2 Instance

Additional Amazon Web Services Documentation

To use the AWS plugin, you should have a good understanding of Amazon Web Services and EC2 concepts, functionality and terminology, and understand how CounterACT policies and other basic features work. Installation, configuration and general guides relating to AWS can be found at:

https://aws.amazon.com/documentation/

Requirements

This section describes system requirements, including:

- CounterACT Software Requirements
- AWS Requirements

- Networking Requirements

CounterACT Software Requirements

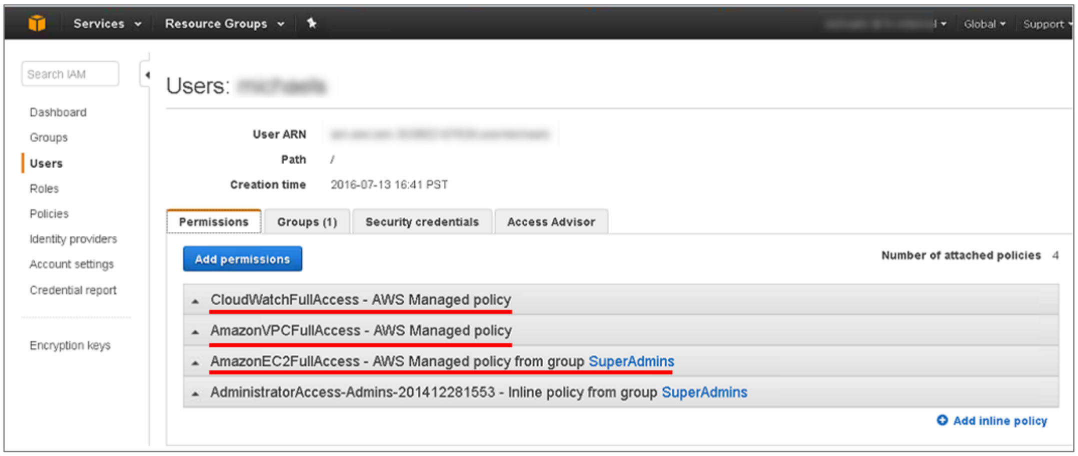
The plugin requires the following CounterACT release and other CounterACT components:

- CounterACT version 8.0.
- Hybrid Cloud Module version 1.0 or above with the AWS component running

AWS Requirements

This plugin requires the following AWS components:

- An Amazon Web Services online account is required.
- You will need one AWS Access Key ID and Secret Key to configure the AWS plugin. These are associated with a User profile on AWS. The access key ID is a unique identifier associated with a secret key. These two keys are used by the AWS plugin to communicate with AWS on behalf of that user.
- If you are using a proxy server with Basic Authentication, you will need that proxy's credentials.
- The plugin requires the following AWS services and the user must have the related permissions:
  - **Amazon EC2** – Amazon Elastic Compute Cloud (Amazon EC2) is a web service that enables you to launch and manage Linux / UNIX and Windows server instances in Amazon's public cloud. There are two user permissions options that can be used on CounterACT:
    - Read-only permissions (CounterACT will support visibility only)
    - Full permissions (CounterACT will support both visibility and control)



Users: [redacted]

User ARN [redacted]

Path /

Creation time 2016-07-13 16:41 PST

Number of attached policies 4

- CloudWatchFullAccess - AWS Managed policy
- AmazonVPCFullAccess - AWS Managed policy
- AmazonEC2FullAccess - AWS Managed policy from group SuperAdmins
- AdministratorAccess-Admins-201412281553 - Inline policy from group SuperAdmins

- **Amazon VPC** – Amazon Virtual Private Cloud (VPC) is a web service for provisioning a logically isolated section of AWS Cloud where you can launch AWS resources in a virtual network you define. You control your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
- **CloudWatch** - CloudWatch is a web service that enables you to monitor and manage various metrics. It also allows the configuration of alarm actions based on the metrics' data. The AWS plugin uses this service to gather flow log data.

For further information about AWS EC2, refer to the AWS EC2 User Guide.

Networking Requirements

The following must be configured on enterprise firewalls to support communication between CounterACT and AWS regional access points.

- Outgoing communication on port 443/TCP must be allowed
- The **`*.amazonaws.com`** domain must be reachable with HTTPS
- (Optional) Proxy communication, for example, port 8080 is open

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.

Define AWS Users

To allow CounterACT to query AWS, define a user with the IAM (Identity and Access Management) service. Specify the credentials of this user when you define CounterACT connections to AWS.

Because the plugin detects and manages EC2 instances, the AWS user used by CounterACT should have either full EC2 access (AmazonEC2FullAccess). The following example shows an AWS policy that explicitly grants full access to all AWS functions related to EC2 instances.

```
{
"Statement": [{
     "Action": "ec2:*",
     "Effect": "Allow",
     "Resource": "*"
     }]
}
```

Configure the Plugin

Configure the plugin to ensure that CounterACT can communicate with AWS API access points.

🗎 *To begin configuration of the AWS plugin, you must meet the corresponding Requirements first. Removing a configured connection will stop endpoint discovery and property learning of virtual machines unique to the connection, but any actions will remain enabled.*

Add an AWS Connection

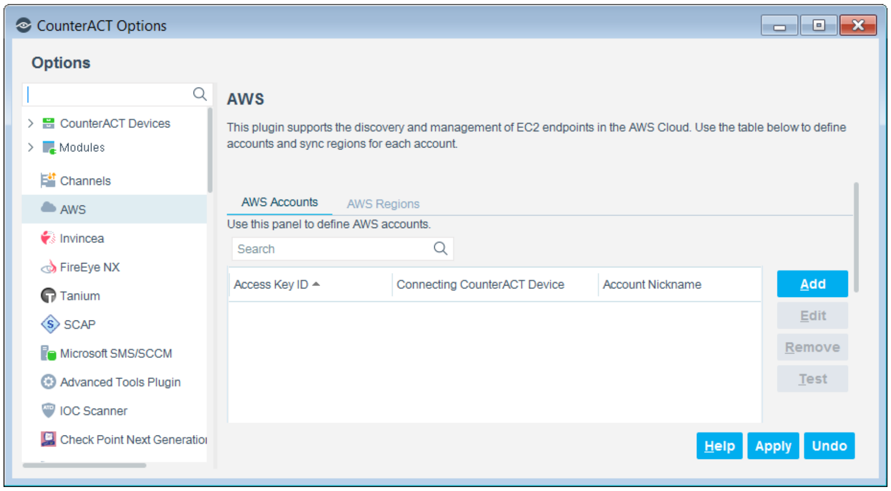
This section describes how to add an AWS Connection from CounterACT. Verify that you have access to your AWS credentials before adding a connection. The Access Key ID corresponds to your AWS EC2 account on the AWS online portal.

To access your AWS credentials:

1. Go to https://console.aws.amazon.com and Login using your username and password.
2. Select **Services**.
3. Select **IAM** from the Security section drop-down menu. The Welcome to Identity and Access Management page opens.
4. In the IAM Resources section, select the **Users** link. The Users page opens.
5. Each user has a unique Access Key ID. Select a user. The Users: [Name of User] page opens.
6. Select the **Security credentials** tab and the sign-in credentials display.
7. In the Access Keys section, the AWS Access key ID displays. Copy the **Access key ID**.
8. Proceed to the next section to create an AWS connection.

To add an AWS connection:

1. In the CounterACT Console, select **Options** from the **Tools** menu.
2. Select **AWS** from the Options pane. The right pane opens to display two tabs: AWS Accounts and AWS Regions.



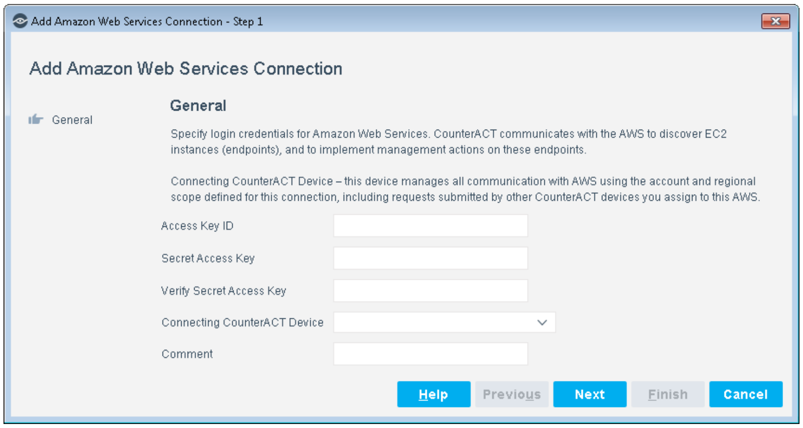
AWS

This plugin supports the discovery and management of EC2 endpoints in the AWS Cloud. Use the table below to define accounts and sync regions for each account.

Use this panel to define AWS accounts.

Access Key ID ▲	Connecting CounterACT Device	Account Nickname

3. In the AWS Accounts tab, select **Add**. The Policy Wizard opens. If you have not set up your AWS credentials, see Add an AWS Connection.



Add Amazon Web Services Connection

General

Specify login credentials for Amazon Web Services. CounterACT communicates with the AWS to discover EC2 instances (endpoints), and to implement management actions on these endpoints.

Connecting CounterACT Device – this device manages all communication with AWS using the account and regional scope defined for this connection, including requests submitted by other CounterACT devices you assign to this AWS.

Access Key ID

Secret Access Key

Verify Secret Access Key

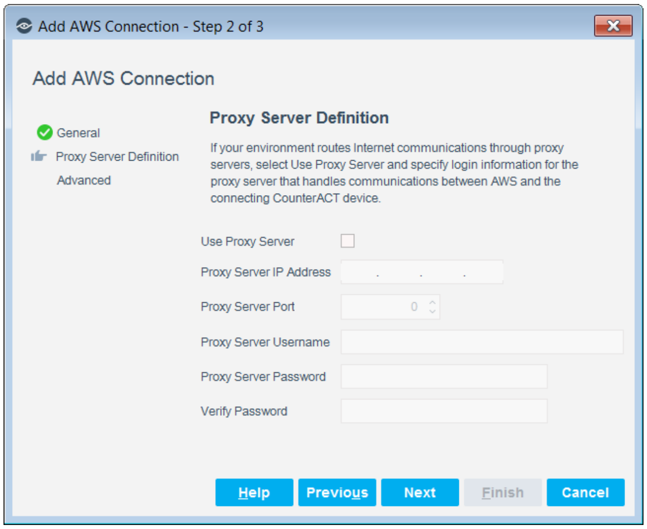
Connecting CounterACT Device

Comment

4. Enter values for the following parameters, which are used to connect to AWS and retrieve information about endpoints in the cloud.

Access Key ID **Secret Access Key**	Enter the credentials of the IAM user you want this connection to use when it connects to AWS. The Access Key ID and the Secret Access Key were given to you when you created a User profile in your AWS account. The username of the IAM user is not required.
Verify Secret Access Key	Confirm the accuracy of the Secret Access Key by re-entering it.
Connecting CounterACT Device	Indicates the CounterACT device that connects to AWS using these connection settings. The device specified in this field is the only CounterACT device that communicates with the AWS. In the drop-down, select an IP Address listed under the Appliances folder. Only one IAM user is allowed per connecting device.
Account Nickname	Add an optional label or nickname to distinguish this connection from other AWS connections.

5. Select **Next.** The Proxy Server Definitions pane opens.



Add AWS Connection - Step 2 of 3

Add AWS Connection

- ✓ General
- Proxy Server Definition
- Advanced

Proxy Server Definition

If your environment routes Internet communications through proxy servers, select Use Proxy Server and specify login information for the proxy server that handles communications between AWS and the connecting CounterACT device.

Use Proxy Server □

Proxy Server IP Address . . .

Proxy Server Port 0

Proxy Server Username

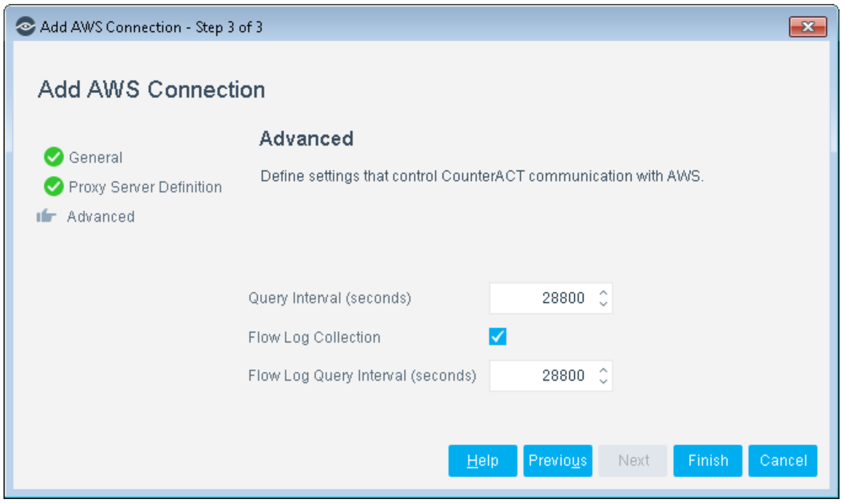
Proxy Server Password

Verify Password

- It is optional to enter proxy server information. If using a proxy server with Basic Authentication, you will need that proxy's credentials (see AWS Requirements).

Use Proxy Server	If your environment routes internet communications through proxy servers, select this box.
Proxy Server IP Address	Enter the IP address of the proxy server.
Proxy Server Port	Select the port number of the proxy server.
Proxy Server Username	(Optional) For proxies using Basic Authentication, enter the proxy server’s username.
Proxy Server Password	(Optional) For proxies using Basic Authentication, enter the proxy server’s password.
Verify Password	Verify the proxy server’s password.

6. Select **Next**. The Advanced pane opens.



Add AWS Connection - Step 3 of 3

Add AWS Connection

- ✓ General
- ✓ Proxy Server Definition
- Advanced

Advanced

Define settings that control CounterACT communication with AWS.

Query Interval (seconds) 28800

Flow Log Collection ☑

Flow Log Query Interval (seconds) 28800

7. Set the communication controls between CounterACT and AWS.

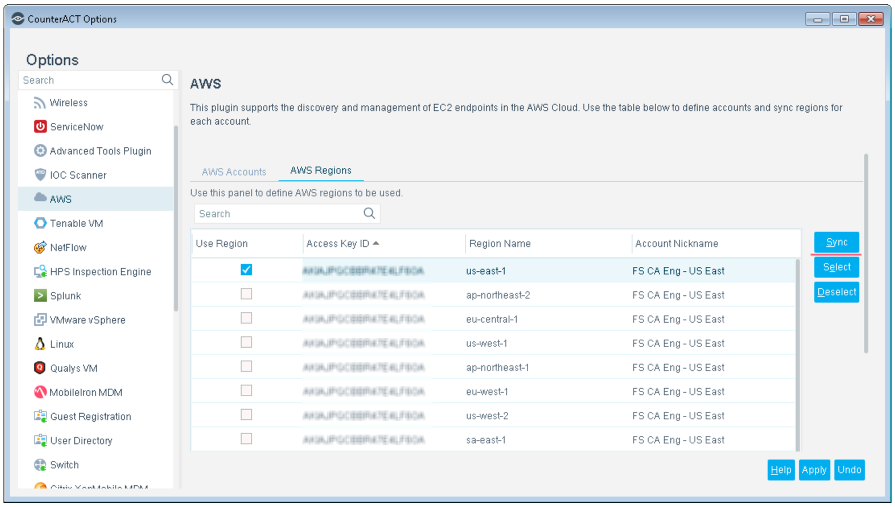
Query Interval (seconds)	Specify how frequently the plugin should query AWS.
Flow Log Collection	Check the box if you choose to enable flow log collection. This allows the collection of information about the IP traffic going to and from network interfaces in your VPC. For more information about flow logs, refer to Amazon VPC Flow Logs.
Flow Log Query Interval (seconds)	Indicate the interval of flow logs collection. It is recommended that you set it for 8 hours / 28800 seconds (default). 🗎 *Flow Log collection may require considerable amount of time and hardware/network resources.*

8. Select **Finish**. The new account displays in the AWS Accounts pane.

9. In the CounterACT Enterprise Manager, select **Apply** and confirm the changes.

🗎 *Allow 1-2 minutes for the changes to take effect.*

10. After the account has been added, navigate to the AWS Regions tab and select **Sync** to retrieve the available AWS regions.



AWS

This plugin supports the discovery and management of EC2 endpoints in the AWS Cloud. Use the table below to define accounts and sync regions for each account.

Use this panel to define AWS regions to be used.

Use Region	Access Key ID ▲	Region Name	Account Nickname
☑	[redacted]	us-east-1	FS CA Eng - US East
☐	[redacted]	ap-northeast-2	FS CA Eng - US East
☐	[redacted]	eu-central-1	FS CA Eng - US East
☐	[redacted]	us-west-1	FS CA Eng - US East
☐	[redacted]	ap-northeast-1	FS CA Eng - US East
☐	[redacted]	eu-west-1	FS CA Eng - US East
☐	[redacted]	us-west-2	FS CA Eng - US East
☐	[redacted]	sa-east-1	FS CA Eng - US East

11. The Synchronizing AWS Regions dialog box displays the results. When finished, select **Close**.

12. In the AWS Regions pane, all the regions are now selected by default. Determine which regions that you would like the AWS account to discover EC2 instances. Make your selections based on the User Region, Access Key ID, Region Name, or Account Nickname. If you do not know which regions, use the default setting.

13. Select **Apply** and confirm the changes.

🗎 *Allow 1-2 minutes for the changes to take effect.*

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

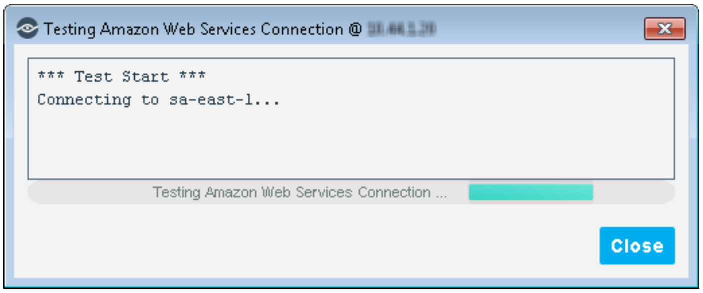
1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Test the AWS Connection

Using the configured settings, CounterACT attempts to connect to AWS and retrieve a list of all endpoints associated with the IAM user in the AWS regions specified in the connection.

To test the AWS connection:

1. Select the AWS Accounts tab and then select **Test**. CounterACT tests the AWS Connection to the Connected Device.


Testing Amazon Web Services Connection @ [redacted]
Testing Amazon Web Services Connection ...
Close

```
*** Test Start ***
Connecting to sa-east-1...
```

2. After viewing the test results, select **Close**.

🗎 *It is recommended you test the AWS connection after the AWS plugin has been running for 1-2 minutes.*

Configure AWS Policy Templates

The AWS plugin provides additional endpoint properties and actions that are useful for management of AWS virtual devices. Use these properties and actions to construct customized policies for detecting, managing and remediating endpoints based on the AWS integration.

Before applying the templates, it is recommended that you have a basic understanding of CounterACT policies. For more information about creating custom policies, see the CounterACT Templates and Policy Management chapters in the *CounterACT Administration Guide*.

- AWS EC2 AMI Classification Template
- AWS EC2 External Instance Classification Template

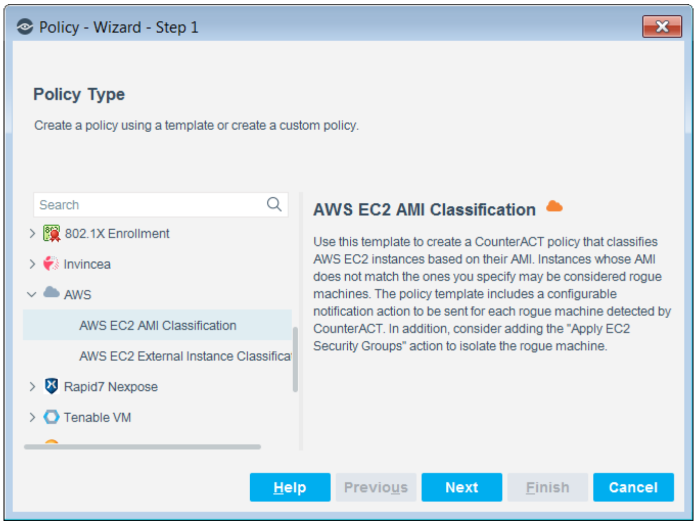
AWS EC2 AMI Classification Template

Use the AWS EC2 AMI Classification template to create a CounterACT policy that classifies AWS EC2 instances based on their Amazon Machine Image (AMI). Instances where AMI does not match the ones you specify may be considered unauthorized machines. The policy template includes a configurable notification action to be sent for each rogue machine detected by CounterACT.

🗎 *Consider adding the "Apply EC2 Security Groups" action to isolate the unauthorized machine.*

To create an AWS EC2 AMI Classification policy:

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add**. The Policy Wizard opens.
3. Select Templates and expand the **AWS** folder.
4. Select **AWS EC2 AMI Classification**.


Policy - Wizard - Step 1

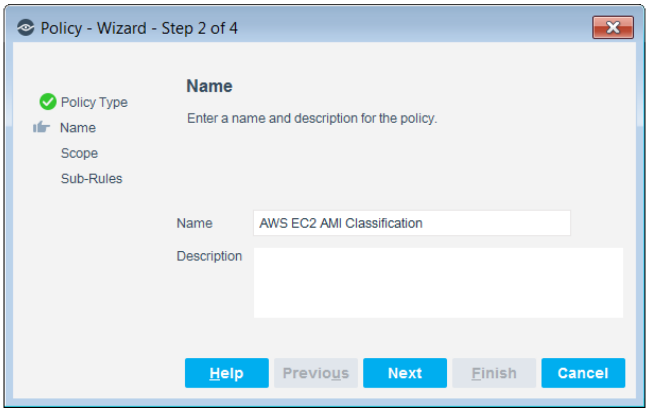
Policy Type

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

AWS EC2 AMI Classification

Use this template to create a CounterACT policy that classifies AWS EC2 instances based on their AMI. Instances whose AMI does not match the ones you specify may be considered rogue machines. The policy template includes a configurable notification action to be sent for each rogue machine detected by CounterACT. In addition, consider adding the "Apply EC2 Security Groups" action to isolate the rogue machine.

5. Select **Next**. The Policy Name dialog box opens. Enter the name of the new policy and (optional) description.


Policy - Wizard - Step 2 of 4

Name

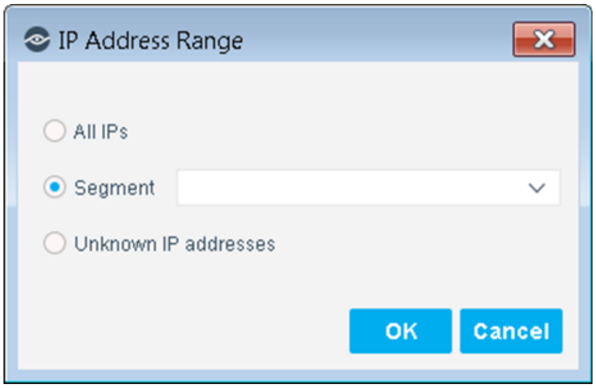
Enter a name and description for the policy.

Name: AWS EC2 AMI Classification

Description:

6. Select **Next**. The Scope pane opens.

7. Use The IP Address Range dialog box to define which endpoints are inspected.



IP Address Range

○ All IPs

● Segment

○ Unknown IP addresses

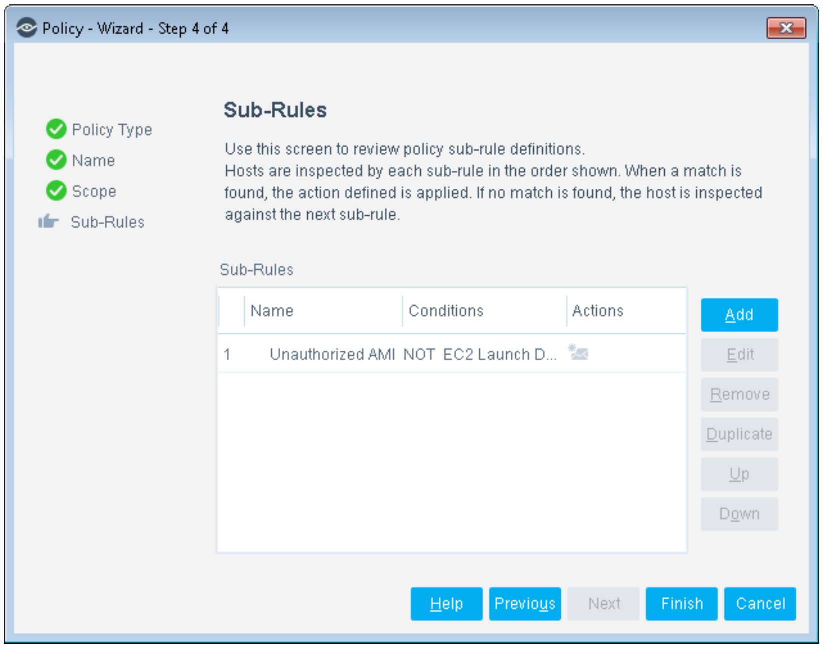
The following options are available:

– **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 page.

– **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 Sub-Rules pane opens.



Policy - Wizard - Step 4 of 4

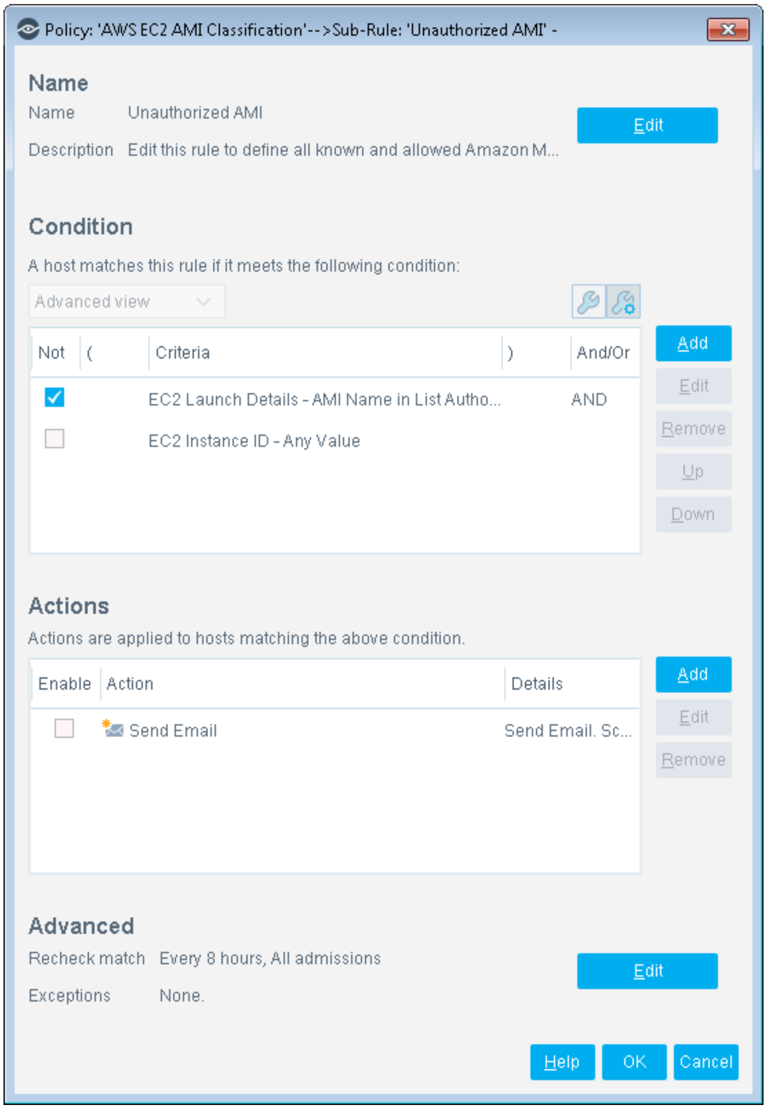
Sub-Rules

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.

Sub-Rules

	Name	Conditions	Actions
1	Unauthorized AMI	NOT EC2 Launch D...	

9. Double-click the Unauthorized AMI sub-rule to open it. The [Name of AWS EC2 AMI Classification policy] Unauthorized AMI dialog box opens.



Policy: 'AWS EC2 AMI Classification'-->Sub-Rule: 'Unauthorized AMI' -

Name

Name Unauthorized AMI

Description Edit this rule to define all known and allowed Amazon M...

Condition

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

Advanced view

Not	(	Criteria	)	And/Or
☑		EC2 Launch Details - AMI Name in List Autho...		AND
☐		EC2 Instance ID - Any Value		

Actions

Actions are applied to hosts matching the above condition.

Enable	Action	Details
☐	Send Email	Send Email. Sc...

Advanced

Recheck match Every 8 hours, All admissions

Exceptions None.

10. In this page, you can add conditions and actions. A list of these properties can be found in Detecting Cloud Endpoints – Host Properties.

11. Select **OK**. In the [Name of AWS EC2 AMI Classification policy] Unauthorized AMI dialog box, select **OK**.

12. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

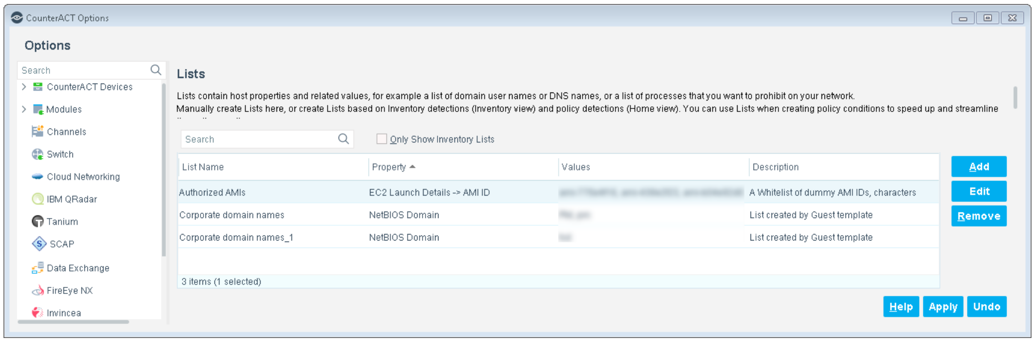
Updating the AMI Whitelist

The AMI Whitelist lists the “good” AMIs. The default AWS EC2 AMI Classification policy template checks this list to find out if an instance’s AMI is listed in the whitelist or not.

Once the AWS EC2 AMI Classification template has been set up, the AMI classification itself needs to be configured into the EC2 instance. You will need to access the AWS online portal and obtain the AMI ID of all sanctioned AMIs. Once the AMI IDs are available, you can then update the AMI whitelist.

To update the AMI whitelist:

1. Log in to the CounterACT Console and select **Options** from the Tools menu. The Options page opens.
2. In the left pane, select **Lists**. In the right pane, all the AMIs are listed.



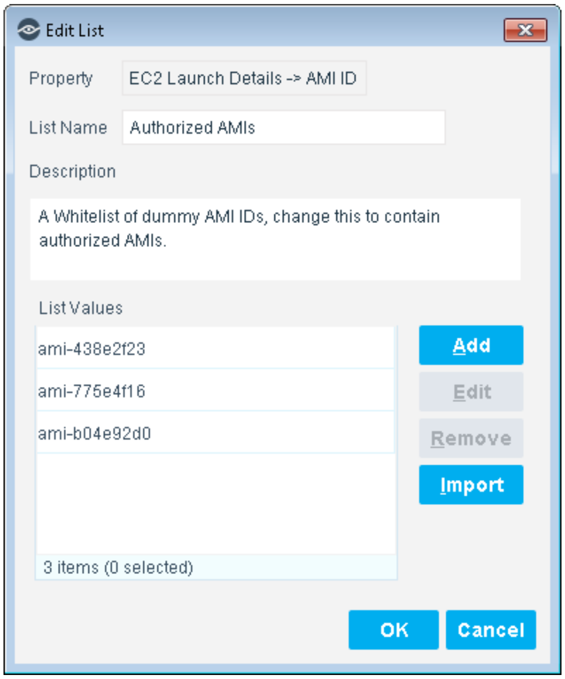
Lists

Lists contain host properties and related values, for example a list of domain user names or DNS names, or a list of processes that you want to prohibit on your network.
Manually create Lists here, or create Lists based on Inventory detections (Inventory view) and policy detections (Home view). You can use Lists when creating policy conditions to speed up and streamline

List Name	Property ▲	Values	Description
Authorized AMIs	EC2 Launch Details -> AMI ID	[redacted]	A Whitelist of dummy AMI IDs, characters
Corporate domain names	NetBIOS Domain	[redacted]	List created by Guest template
Corporate domain names_1	NetBIOS Domain	[redacted]	List created by Guest template

3 items (1 selected)

3. Select an item and then select **Edit**. Alternately, double-click the item. The Edit List dialog box opens.



Property: EC2 Launch Details -> AMI ID

List Name: Authorized AMIs

Description

A Whitelist of dummy AMI IDs, change this to contain authorized AMIs.

List Values

ami-438e2f23
ami-775e4f16
ami-b04e92d0

3 items (0 selected)

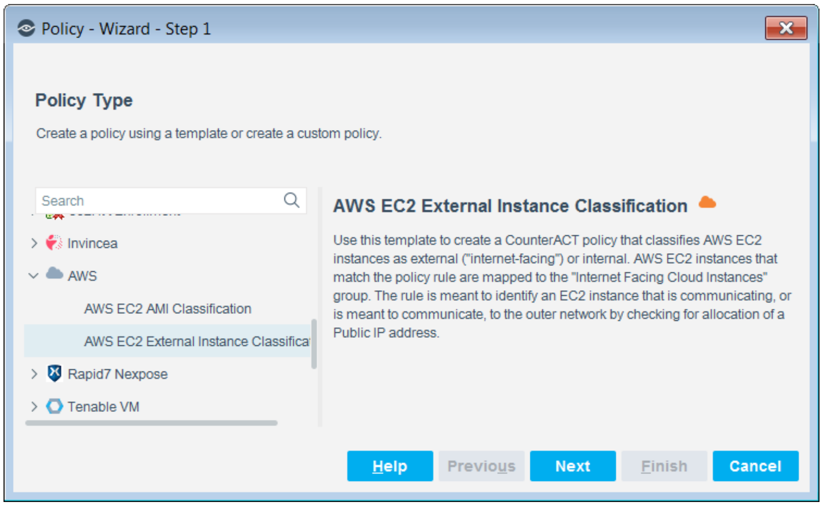
4. To add additional values to the list, select **Add**. The Add Value dialog box opens.
5. Paste the AMI ID from the AWS online portal into the field and then select **OK**.
6. Copy/paste additional AMIs from the AWS online portal into the Edit List dialog box (if applicable).
7. When finished, select **OK**.
8. Select **Apply** in the Lists pane.

AWS EC2 External Instance Classification Template

Use the AWS EC2 External Instance Classification template to create a CounterACT policy that classifies AWS EC2 instances as external ("internet-facing") or internal. AWS EC2 instances that match the policy rule are mapped to the "Internet Facing AWS EC2 Instances" group. The rule is meant to identify an EC2 instance that is communicating, or is meant to communicate, to the outer network by checking for allocation of a Public IP address. These instances are grouped into the “External Instances” group by default.

To create an AWS EC2 External Instance Classification policy:

1. Login to the CounterACT Console and select the **Policy** tab.
2. Select **Add**. The Policy Wizard opens.
3. Select Templates and expand the **AWS** folder.
4. Select **AWS EC2 External Instance Classification**.



Policy - Wizard - Step 1

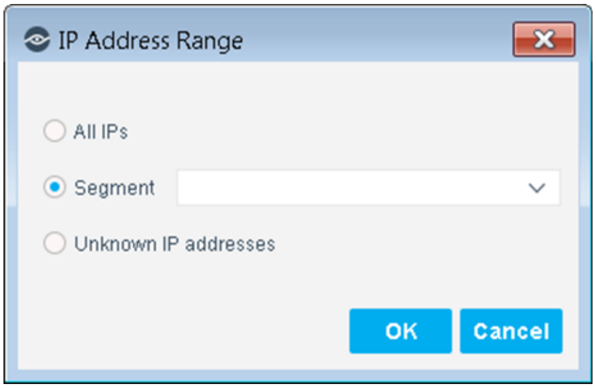
Policy Type

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

AWS EC2 External Instance Classification

Use this template to create a CounterACT policy that classifies AWS EC2 instances as external ("internet-facing") or internal. AWS EC2 instances that match the policy rule are mapped to the "Internet Facing Cloud Instances" group. The rule is meant to identify an EC2 instance that is communicating, or is meant to communicate, to the outer network by checking for allocation of a Public IP address.

5. Select **Next**. The Name pane opens. Enter the name of the new policy.
6. Select **Next**. The Scope pane opens.
7. Use The IP Address Range dialog box to define which endpoints are inspected.



IP Address Range

○ All IPs

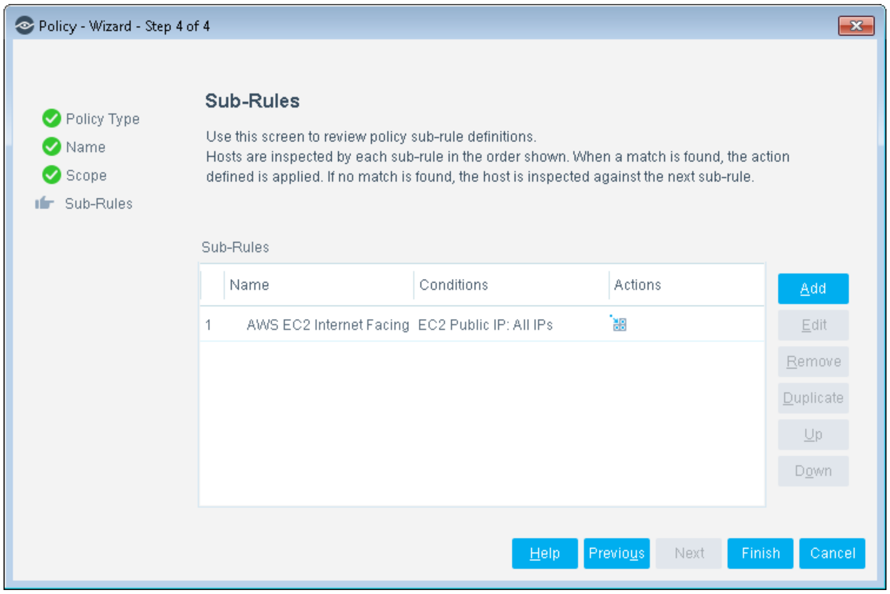
● Segment

○ Unknown IP addresses

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 page.
- **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 Sub-Rules pane opens.



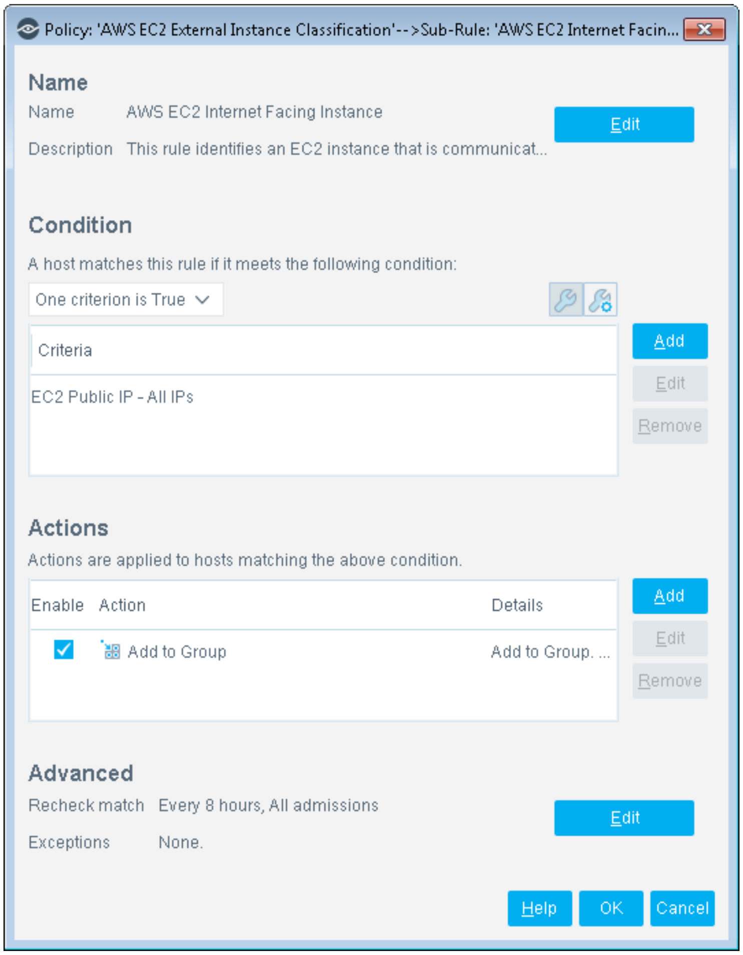
Sub-Rules

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.

Sub-Rules

	Name	Conditions	Actions
1	AWS EC2 Internet Facing	EC2 Public IP: All IPs	⊞

9. Double-click the Unauthorized AMI sub-rule to open it. The [Name of AWS EC2 External Instance Classification policy] EC2 Internet Facing Instance dialog box opens.



Policy: 'AWS EC2 External Instance Classification'-->Sub-Rule: 'AWS EC2 Internet Facin...

Name

Name AWS EC2 Internet Facing Instance

Description This rule identifies an EC2 instance that is communicat...

Condition

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

One criterion is True

Criteria
EC2 Public IP - All IPs

Actions

Actions are applied to hosts matching the above condition.

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

Advanced

Recheck match Every 8 hours, All admissions

Exceptions None.

10. In this page, you can add conditions and actions. A list of these properties can be found in Detecting Cloud Endpoints – Host Properties.

11. Select **OK**. In the [Name of AWS EC2 External Instance Classification policy] EC2 Internet Facing Instance dialog box, select **OK**.

12. In the Sub-Rules pane of the Policy Wizard, select **Finish**.

Detecting Cloud Endpoints – Host Properties

There are many AWS-specific host properties that are available. These properties are displayed in the Condition pane accessible through the policy templates. In the CounterACT Console, some properties are also visible in the profile section within the Home tab.

AWS CloudWatch Flow Logs

This plugin integrates with AWS CloudWatch Flow Logs service to provide deeper visibility of traffic flow between instances. It captures incoming and outgoing flows for an instance and records information such as source IP, destination IP, port number, etc., and reports if the flow was accepted or denied.

CounterACT parses these Flow Logs and identifies specific information about the to-and-from communications for an EC2 instance. This information helps identify unusual communication. For example, if you find EC2 instances are sending requests from an unauthorized machine, those instances can easily be quarantined by applying a restrictive security group.

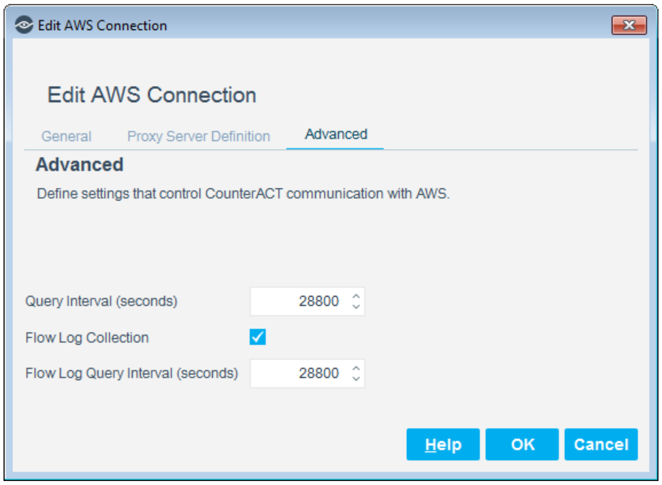
The AWS CloudWatch Flow Logs can also identify misconfigurations of an EC2 instance. For example, if a database instance is communicating on port 80, it can be flagged as non-compliant and can be quarantined by applying a security group action isolating the endpoint and preventing further usage of that port.

In order to utilize this feature, you must have the Flow Log Collection enabled (checked) in AWS the accounts configuration.

🗎 *All instances detected via Flow Logs, will be initially displayed as online, even though their current status may be listed as* ***stopped*** *or* ***terminated****.*

To enable flow log collection:

1. In the CounterACT Console, select **Options** from the **Tools** menu and select **Modules**.
2. Select **Hybrid Cloud > AWS** from the Modules pane and select **Configure**. The right pane opens to display two tabs: AWS Accounts and AWS Regions.
3. In the AWS Accounts tab, select an item and select **Edit**.
4. The Edit AWS Connection dialog box opens. Select the **Advanced** tab.



Edit AWS Connection

Advanced

Define settings that control CounterACT communication with AWS.

Query Interval (seconds) 28800

Flow Log Collection ☑

Flow Log Query Interval (seconds) 28800

5. Select the **Flow Log Collection** checkbox and set the **Flow Log Query Interval**. It is recommended to set the interval to 28800 seconds. This is equivalent to an 8-hour interval.
6. Select **OK**.
7. In the AWS pane, select **Apply**.

🗎 *Allow 1-2 minutes for the changes to take effect.*

Flow Log Traffic

When creating or editing a policy, you can set the traffic details of EC2 instances through the Conditions dialog box.

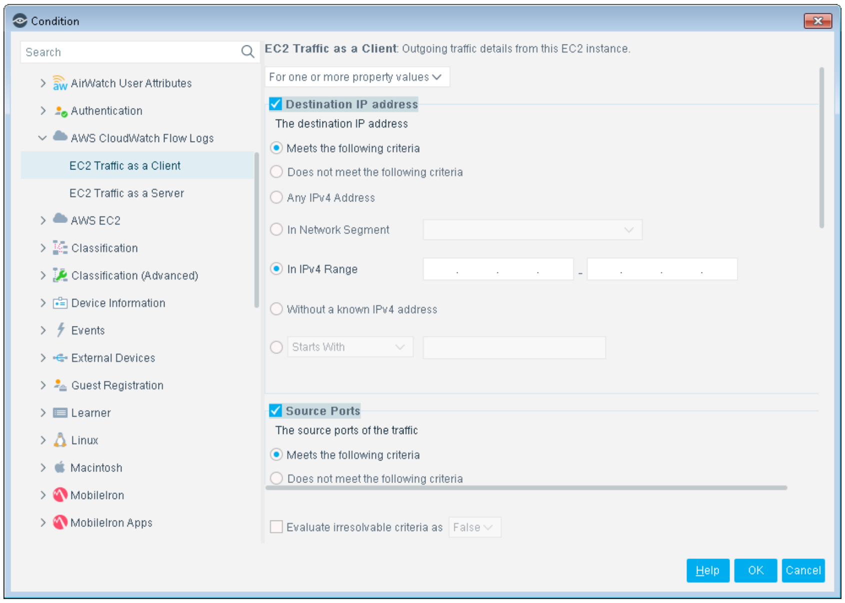
To access the AWS CloudWatch Flow Logs properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the AC2 CloudWatch Flow Logs folder in the Properties tree.

   The following properties are available:

   – EC2 Traffic as a Client

   – EC2 Traffic as a Server



EC2 Traffic as a Client: Outgoing traffic details from this EC2 instance.

For one or more property values

☑ **Destination IP address**

The destination IP address

● Meets the following criteria

○ Does not meet the following criteria

○ Any IPv4 Address

○ In Network Segment

● In IPv4 Range . . . - . . .

○ Without a known IPv4 address

○ Starts With

☑ **Source Ports**

The source ports of the traffic

● Meets the following criteria

○ Does not meet the following criteria

□ Evaluate irresolvable criteria as False

EC2 Traffic as a Client	Information on the outgoing traffic from the selected EC2 instance (acting as a client) is presented as a list of items (one item per Destination IP address). This information is derived from the communication observed in Flow Logs. Each item has a distinct Destination IP address, a collection of Source and Destination Ports, as well as a collection of IANA Protocols and Associated actions used to communicate with that Destination. 🗎 *CounterACT displays communication details with up to 100 destinations.*

EC2 Traffic as a Server	Information on the incoming traffic to the selected EC2 instance (acting as a server), presented as a list of items (one item per each Source IP address). This information is derived from the communication observed in Flow Logs. Each item has a distinct Source IP address, a collection of Source and Destination Ports, as well as a collection of IANA Protocols and Associated actions used to communicate with that Source. 🗎 *CounterACT displays communication details with up to 100 sources.*

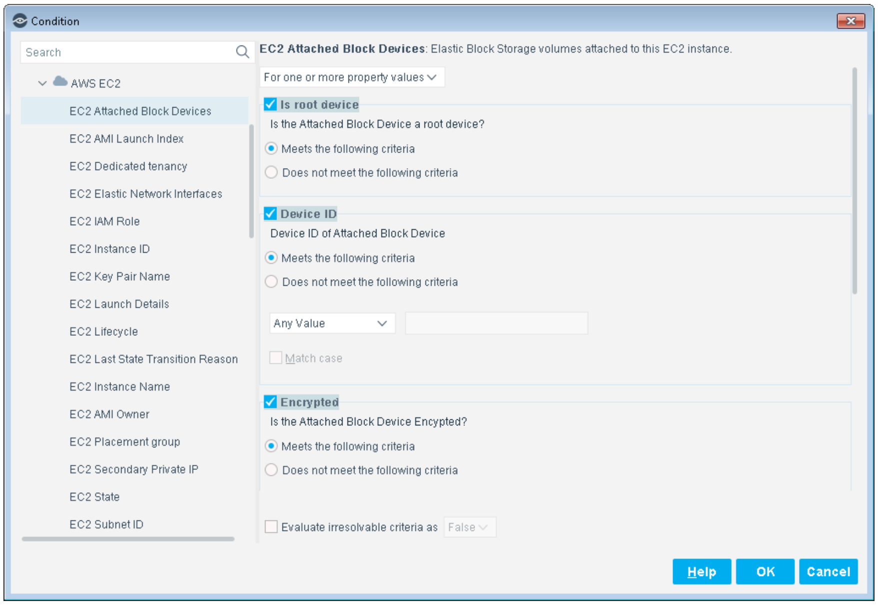
For more information about setting conditions, refer to the *CounterACT Administration Guide*.

AWS EC2

This section describes the properties that are available with this module.

To access the AWS EC2 properties:

1. Navigate to the Properties tree from the Policy Conditions dialog box.
2. Expand the AC2 EC2 folder in the Properties tree.



EC2 Attached Block Devices: Elastic Block Storage volumes attached to this EC2 instance.

For one or more property values

☑ **Is root device**

Is the Attached Block Device a root device?

● Meets the following criteria

○ Does not meet the following criteria

☑ **Device ID**

Device ID of Attached Block Device

● Meets the following criteria

○ Does not meet the following criteria

Any Value

□ Match case

☑ **Encrypted**

Is the Attached Block Device Encypted?

● Meets the following criteria

○ Does not meet the following criteria

□ Evaluate irresolvable criteria as False

AWS CloudWatch Monitoring	CloudWatch is a web service that enables you to monitor and manage various metrics. It also allows the configuration of alarm actions based on the metrics' data.
AWS Virtual Private Cloud	Indicates the Virtual Private Cloud into which the endpoint was launched.
EC2 AMI Launch Index	Indicates the order in which the EC2 instance was launched. The first or only instance has an index value of 0.

EC2 AMI Owner	Indicates the AWS account number of the owner of the Amazon Machine Image used for this EC2 instance.
EC2 Attached Block Devices	Indicates the Elastic Block Storage volumes attached to this EC2 instance.
EC2 Dedicated Tenancy	Indicates that the instance runs on single-tenant, dedicated hardware.
EC2 Elastic Network Interfaces	Indicates the Elastic Network Interfaces of the EC2 instance.
EC2 IAM Role	Indicates the Identity and Access Management role associated with this EC2 instance.
EC2 Instance ID	Indicates the instance ID of the EC2 endpoint.
EC2 Instance Name	Indicates the instance name of the EC2 endpoint.
EC2 Instance Type	Indicates the CPU capacity, memory, and storage of this AWS endpoint. For example, m1.small, c1.xlarge.
EC2 Kernel ID	The operating system kernel associated with the AMI.
EC2 Key Pair Name	Indicates the key pair used to log in to the instance securely.
EC2 Last State Transition Reason	Indicates the reason for the last change of EC2 instance state. For example, if the last instance state was 'Terminated', the reason might be 'User initiated shutdown'.
EC2 Launch Details	Indicates launch details of the EC2 instance.
EC2 Lifecycle	Indicates whether this is a Normal or Spot EC2 instance. A Normal instance is usually launched and terminated at a user's request. A Spot Instance is launched automatically when the bid price is higher than the Spot Price, and may be terminated if the Spot Price goes over the bid price.
EC2 Location	Indicates location information of the AWS endpoint.
EC2 Placement Group	Indicates the cluster group to which this instance belongs, if it is a cluster instance.
EC2 Platform	The operating system platform, such as Windows.
EC2 Public DNS	Indicates the public hostname of the AWS endpoint, which resolves to the public IP address or Elastic IP address of the endpoint.
EC2 Public IP	Indicates the public IP address of the AWS endpoint.
EC2 RAM disk ID	The RAM disk associated with the image, if a specific one was selected.
EC2 Secondary Private IP	Indicates secondary private IP addresses assigned to a network interface attached to this EC2 instance.
EC2 Security Group	Indicates the security groups to which this AWS endpoint belongs.
EC2 State	Indicates the most recent power state of the EC2 instance. This value may be influenced by the Query Interval configured for the CounterACT connection to AWS.
EC2 Subnet ID	Indicates the AWS ID of the subnet that the EC2 instance was launched into, if applicable. A subnet is a range of IP addresses in a Virtual Private Cloud.
EC2 Tags	Indicates the tags given to the AWS endpoint.

EC2 Termination Protection	Indicates whether termination protection is enabled. When protection is enabled, this EC2 instance cannot be terminated using the console, API, or CLI.

For more information about setting conditions, refer to the *CounterACT Administration Guide*.

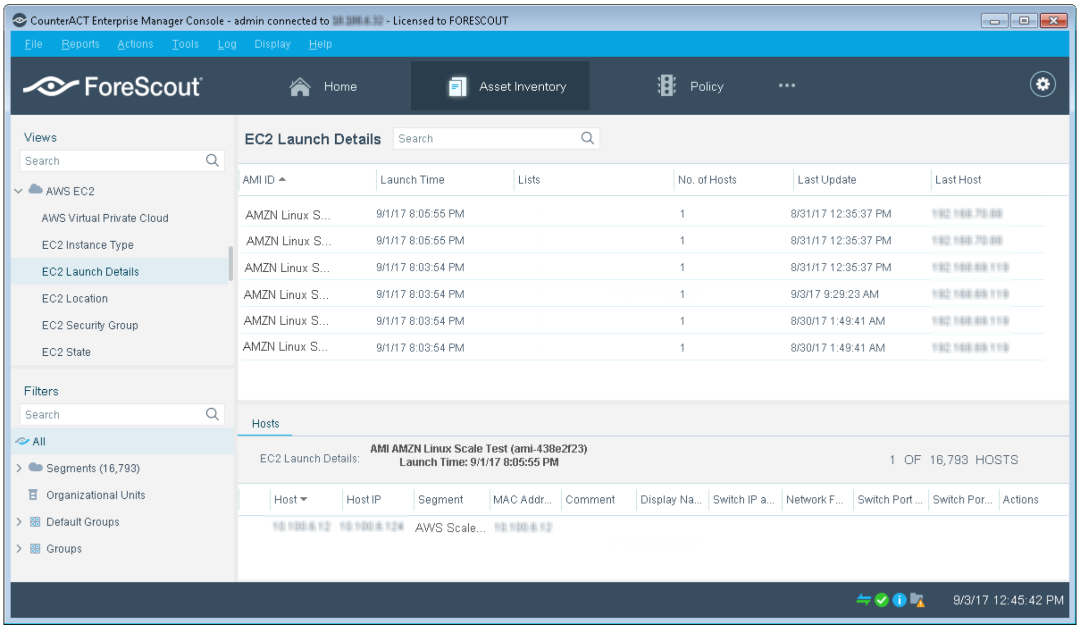
Managing AWS Cloud Endpoints

Once the AWS plugin has been configured, you can view and manage the virtual endpoints from the Asset Inventory view in the CounterACT Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instances' properties. The Asset Inventory lets you:

- Complement a device-specific view of the organizational network with an activity-specific view
- View virtual machine endpoints that were detected with specific attributes
- Incorporate inventory detections into policies

To access the inventory:

1. Log in to the CounterACT Console and select the **Asset Inventory** tab.
2. In the Views pane, expand the **AWS EC2** folder.



AMI ID	Launch Time	Lists	No. of Hosts	Last Update	Last Host
AMZN Linux S...	9/1/17 8:05:55 PM		1	8/31/17 12:35:37 PM	[redacted]
AMZN Linux S...	9/1/17 8:05:55 PM		1	8/31/17 12:35:37 PM	[redacted]
AMZN Linux S...	9/1/17 8:03:54 PM		1	8/31/17 12:35:37 PM	[redacted]
AMZN Linux S...	9/1/17 8:03:54 PM		1	9/3/17 9:29:23 AM	[redacted]
AMZN Linux S...	9/1/17 8:03:54 PM		1	8/30/17 1:49:41 AM	[redacted]
AMZN Linux S...	9/1/17 8:03:54 PM		1	8/30/17 1:49:41 AM	[redacted]

EC2 Launch Details: **AMI AMZN Linux Scale Test (ami-438e2f23)**
Launch Time: 9/1/17 8:05:55 PM

1 OF 16,793 HOSTS

Host	Host IP	Segment	MAC Addr...	Comment	Display Na...	Switch IP a...	Network F...	Switch Port ...	Switch Por...	Actions
[redacted]	[redacted]	AWS Scale...	[redacted]							

9/3/17 12:45:42 PM

3. Select an AWS EC2 item to view the real-time inventory information, for example, EC2 Launch Details.

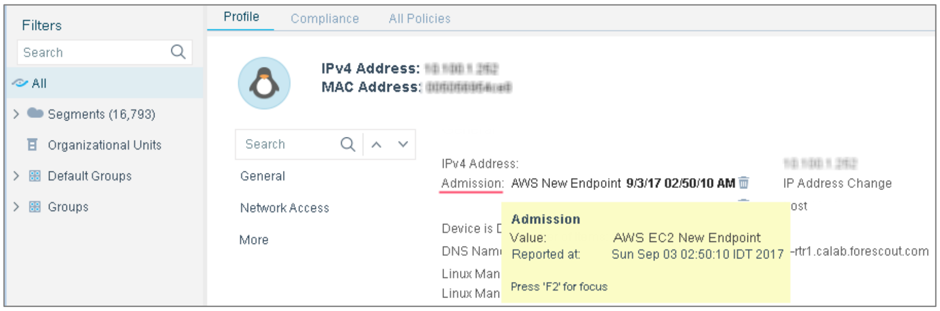
Refer to *Working with Inventory Detections* in the *CounterACT Administration Guide* or the CounterACT Help for information about how to work with the CounterACT Asset Inventory.

AWS Admission Events

After adding and testing the AWS Connection, it is helpful to review the host profile, including admission events.

To review the host profile:

1. Login in to the CounterACT Console and select All Hosts.
2. The Detections pane opens. Select a host to review the profile of the host.
3. In the Profile tab, right-click on the **Admission** field. Information about the new EC2 endpoint opens in a pop-up.



IPv4 Address: [redacted]
MAC Address: [redacted]

IPv4 Address: [redacted]
Admission: AWS New Endpoint **9/3/17 02/50/10 AM** IP Address Change
Device is D
DNS Nam -rtr1.calab.forescout.com
Linux Man
Linux Man

Admission
Value: AWS EC2 New Endpoint
Reported at: Sun Sep 03 02:50:10 IDT 2017
Press 'F2' for focus

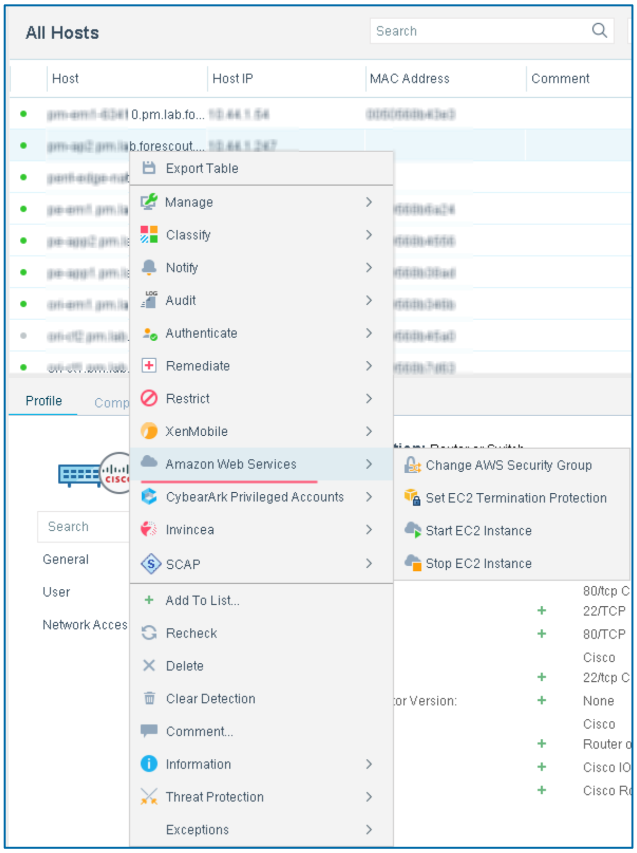
4. If you require further information, double-clicking the item in the table opens the Host Details dialog box.
5. Select the All policies tab and then select Show host log. The Host Log dialog box opens.
6. Enter the parameters for running the log on and then select **OK**.
7. The Host Log is displayed with all the information. You can export or print the results.

Manually Run AWS Actions on any EC2 Instance

While AWS actions can be launched as part of a policy, you can also manually run the policy.

To manually run an AWS Action:

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.
2. In the Detections pane, select a host entry.
3. Hover the mouse over the icon in the Action column. The status of the Action opens.
4. Right-click on an **AWS endpoint**, select **AWS** and then select the action you want done.



5. Click on the links to access further instructions on the AWS Actions.

   – EC2 Security Group Action
   – Disable EC2 Termination Protection Action
   – Enable EC2 Termination Protection Action
   – Start an EC2 Instance
   – Stop an EC2 Instance

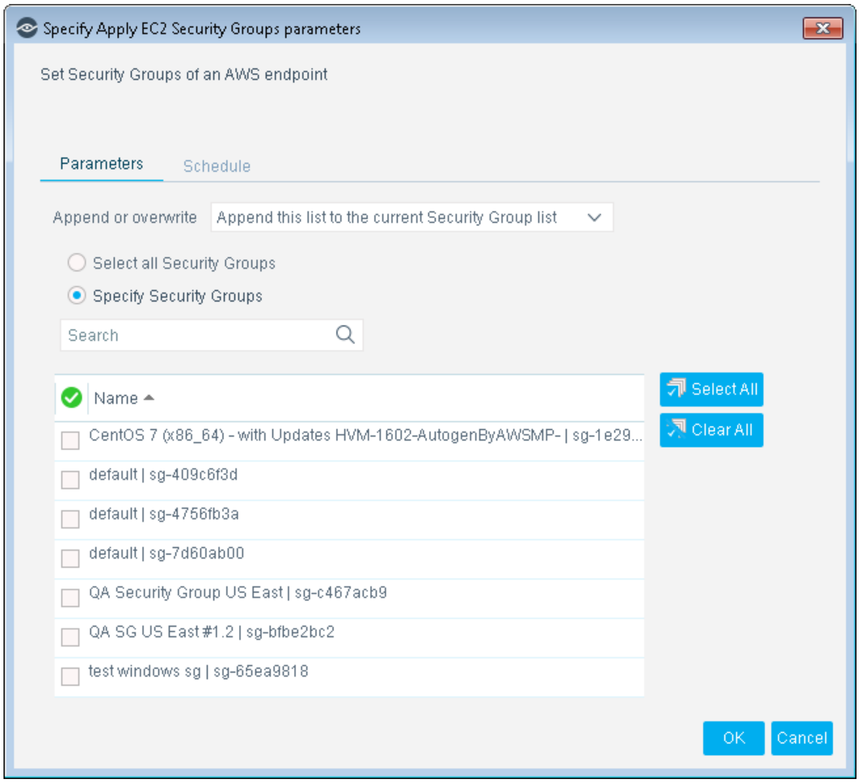
EC2 Security Group Action

A security group acts as a firewall that controls the traffic for one or more EC2 instances. Each security group has a set of rules that you define and these rules specify what kind of connections, such as IP addresses, ports, protocols, etc., are allowed. These rules are defined in the AWS console.

By applying a security group action to a cloud instance, that instance is allowed to send/receive traffic based on the security group's rules.

To start the Apply EC2 Security Groups action:

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.
2. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Apply EC2 Security Groups**. The Specify EC2 Security Groups parameters dialog box opens.



Specify Apply EC2 Security Groups parameters

Set Security Groups of an AWS endpoint

Append or overwrite: Append this list to the current Security Group list

○ Select all Security Groups

● Specify Security Groups

✓	Name ▲
□	CentOS 7 (x86_64) - with Updates HVM-1602-AutogenByAWSMP- | sg-1e29...
□	default | sg-409c6f3d
□	default | sg-4756fb3a
□	default | sg-7d60ab00
□	QA Security Group US East | sg-c467acb9
□	QA SG US East #1.2 | sg-bfbe2bc2
□	test windows sg | sg-65ea9818

3. Select a Security Group(s) or **Select All**.
4. In the Append or overwrite field, select **either:**
   - Append this list to the current Security Group list – Add the selected IP address to the current Security Group list.
   - Overwrite the current Security Group with this list – Selecting this option replaces the current Security Group with the selected one. This is useful for isolating a non-compliant endpoint by applying it only with restrictive security groups.
5. Select **OK**.

Disable EC2 Termination Protection Action

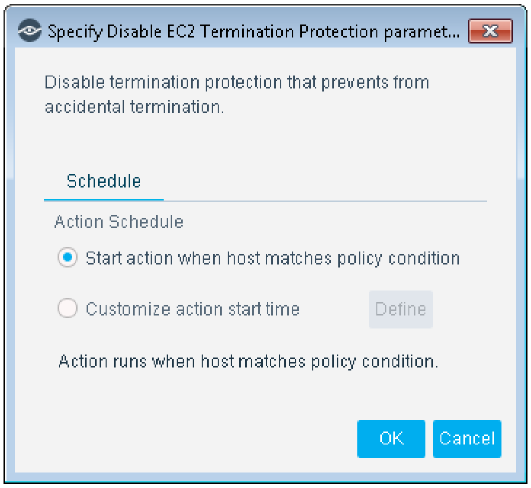
Use this action to remove (disable) termination protection from an EC2 instance.

If termination protection is disabled, it is possible to terminate EC2 instances via the AWS Console, API, or CLI.

Enabling termination protection prevents accidental termination of EC2 instances.

To run a Disable EC2 Termination Protection action:

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.
2. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Disable EC2 Termination Protection**. The Specify Disable EC2 Termination Protection parameters dialog box opens.



Disable termination protection that prevents from accidental termination.

Action Schedule

● Start action when host matches policy condition

○ Customize action start time

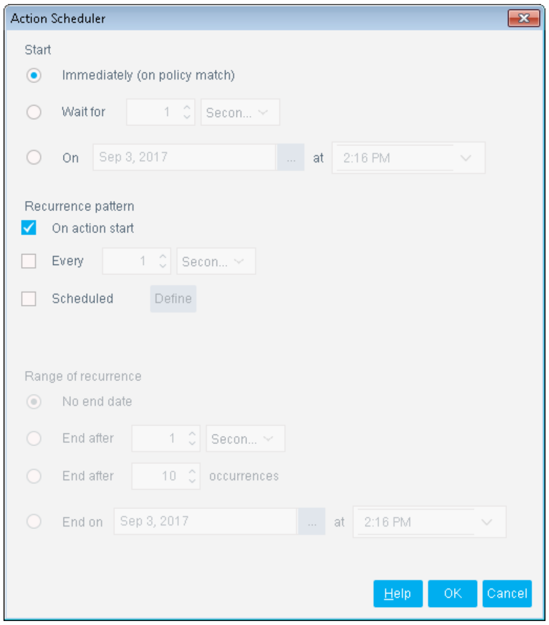
Action runs when host matches policy condition.

3. Set the parameters for the selected IP address' action schedule

   – Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.

   – Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

   a. The Action Scheduler dialog box opens.



Start

● Immediately (on policy match)

○ Wait for 1 Secon...

○ On Sep 3, 2017 ... at 2:16 PM

Recurrence pattern

☑ On action start

☐ Every 1 Secon...

☐ Scheduled

Range of recurrence

● No end date

○ End after 1 Secon...

○ End after 10 occurrences

○ End on Sep 3, 2017 ... at 2:16 PM

   b. Set parameters and then select **OK**.

4. In the specify Disable EC2 Termination Protection parameters dialog box, select **OK**.

Enable EC2 Termination Protection Action

Use this action to apply (enable) termination protection from an EC2 instance.

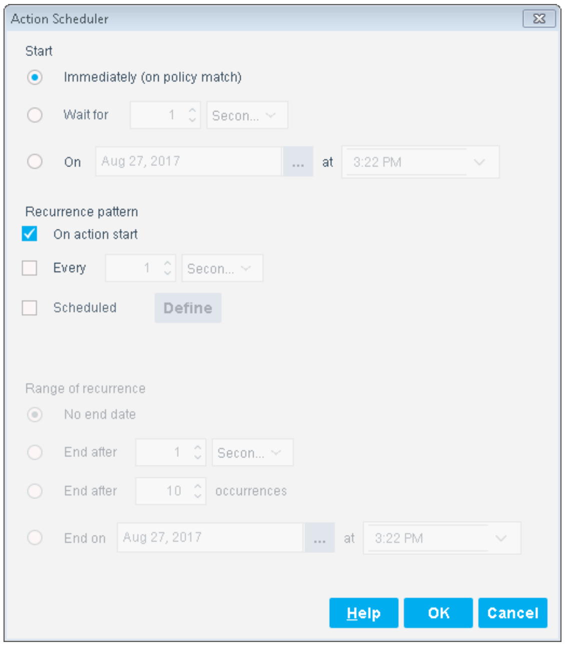
If termination protection is disabled, then stopping EC2 instances may also terminate them. You can start or stop the selected EC2 instance via the AWS Console, API, or CLI.

If termination protection is enabled, then stopping EC2 instances will not terminate them.

To run an Enable EC2 Termination Protection action:

1. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Enable EC2 Termination Protection**. The Specify Enable EC2 Termination Protection parameters dialog box opens.
2. Set the parameters for the selected IP address' action schedule
   - Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.
   - Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

   a. The Action Scheduler dialog box opens.



Action Scheduler

Start

● Immediately (on policy match)

○ Wait for 1 Secon...

○ On Aug 27, 2017 ... at 3:22 PM

Recurrence pattern

☑ On action start

□ Every 1 Secon...

□ Scheduled Define

Range of recurrence

● No end date

○ End after 1 Secon...

○ End after 10 occurrences

○ End on Aug 27, 2017 ... at 3:22 PM

   b. Set parameters and then select **OK**.

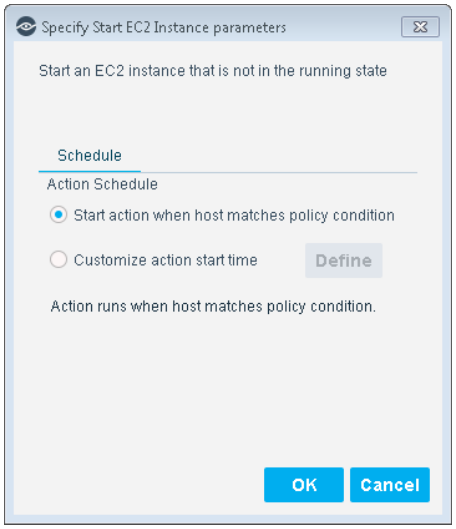
3. In the Specify Enable EC2 Termination Protection parameters dialog box, select **OK**.

Start an EC2 Instance

Use this action to start an EC2 instance.

To run a Start an EC2 Instance action:

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.
2. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Start EC2 Instance**. The Specify Start EC2 Instance parameters dialog box opens.



Specify Start EC2 Instance parameters

Start an EC2 instance that is not in the running state

Schedule

Action Schedule

● Start action when host matches policy condition

○ Customize action start time

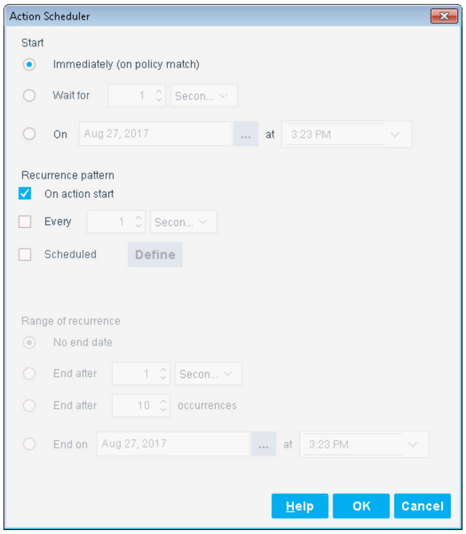
Action runs when host matches policy condition.

3. Set the parameters for the selected IP address' action schedule

   – Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.

   – Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

   a. The Action Scheduler dialog box opens.



Action Scheduler

Start

● Immediately (on policy match)

○ Wait for 1 Secon...

○ On Aug 27, 2017 ... at 3:23 PM

Recurrence pattern

☑ On action start

□ Every 1 Secon...

□ Scheduled

Range of recurrence

● No end date

○ End after 1 Secon...

○ End after 10 occurrences

○ End on Aug 27, 2017 ... at 3:23 PM

b. Set parameters and then select **OK**.

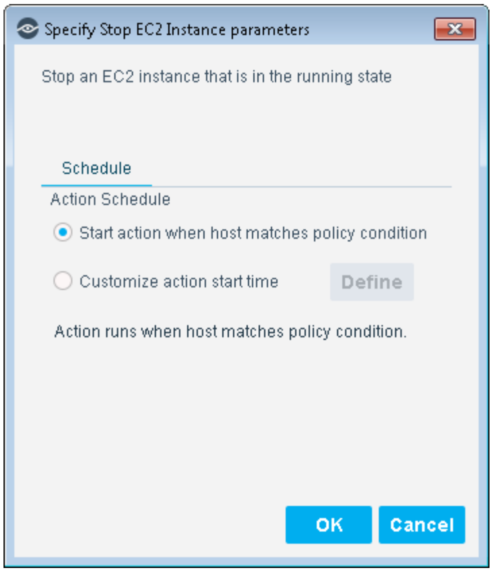
4. In the Specify Start EC2 Instance parameters dialog box, select **OK**.

Stop an EC2 Instance

This section covers how to stop a virtual computing environment (instance).

To run a Stop an EC2 Instance action:

1. Login to the CounterACT Console and select **All Hosts** in the Home tab.
2. In the Detections pane, right-click on an endpoint, select **AWS** and then select **Stop EC2 Instance**. The Specify Stop EC2 Instance parameters dialog box opens.



Specify Stop EC2 Instance parameters

Stop an EC2 instance that is in the running state

Schedule

Action Schedule

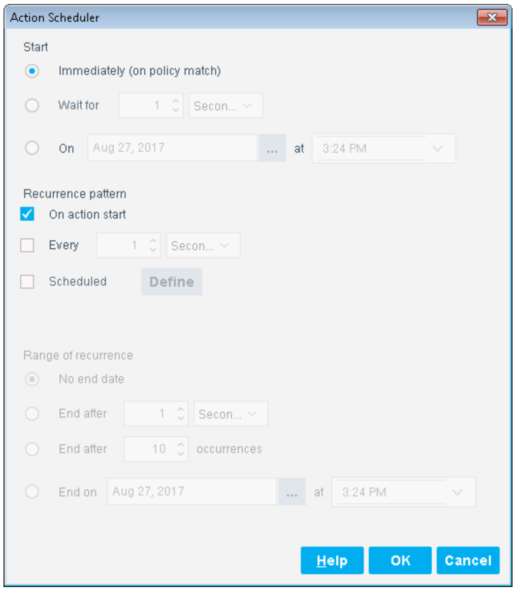
● Start action when host matches policy condition

○ Customize action start time

Action runs when host matches policy condition.

3. Set the parameters for the selected IP address' action schedule
   - Start action when host matches policy condition – implements the policy when the policy condition(s) is met by the host.
   - Customize action start time – selecting the radio button and then selecting the **Define** button opens the Action Scheduler dialog box.

a. The Action Scheduler dialog box opens.



Action Scheduler

Start

● Immediately (on policy match)

○ Wait for 1 Secon...

○ On Aug 27, 2017 ... at 3:24 PM

Recurrence pattern

☑ On action start

□ Every 1 Secon...

□ Scheduled Define

Range of recurrence

● No end date

○ End after 1 Secon...

○ End after 10 occurrences

○ End on Aug 27, 2017 ... at 3:24 PM

b. Set parameters and then select **OK**.

4. In the Specify Enable EC2 Termination Protection parameters dialog box, select **OK**.

Best Practices for Working with the AWS Plugin

The following are some helpful guidelines to follow when using the AWS plugin.

1. ***Create an AWS user account*** – Ask your AWS management personnel to create a new AWS user account with programmatic access for you. Programmatic access will create a access key ID and secret access key that is required when configuring the AWS plugin.
2. ***Level of Access*** – If you would like to be able to control EC2 instances from CounterACT using AWS actions, then you will need *AmazonEC2FullAccess* for the user account. For gaining visibility only, *AmazonEC2ReadOnlyAccess* is sufficient.
3. ***AWS Regions*** – If you want complete visibility across all regions then while performing sync during configuration choose all the regions available. For a restrictive view you can pick specific regions only.
4. ***Set Communications with AWS (Polling)*** – When configuring the AWS plugin, it is recommended to use the default settings for *Query Interval* and *Flow Log Query Interval*. Depending upon the amount of data, the polling of EC2 instances can take anywhere between 1-4 hours per 1,000 instances.
5. ***CounterACT Active Discovery*** – If you do not want CounterACT to perform Active Discovery such as nmap, HPS Inspection, WMI, etc., on EC2 instances, make sure your EC2 instances are not reachable from CounterACT or their IP segment is not included in any base classification policy.

Hybrid Cloud Module Information

The Amazon Web Services plugin is installed with the CounterACT Hybrid Cloud Module.

The ForeScout CounterACT® Hybrid Cloud Module provides See, Control and Orchestrate functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

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

Plugins listed above are installed and rolled back with the Hybrid Cloud Module.

Refer to the *ForeScout CounterACT Hybrid Cloud Module Overview Guide* for more module information, such as module requirements, upgrade and rollback instructions.

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**.

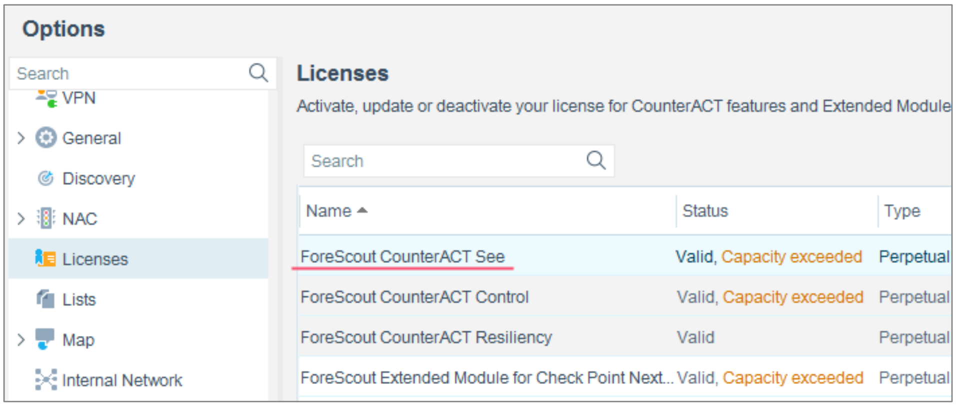
Documentation Portal

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.



Activate, update or deactivate your license for CounterACT features and Extended Module

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

2018-04-10 09:21