



ForeScout

Hybrid Cloud Module: Amazon Web Services (AWS) Plugin

Configuration Guide

Version 2.2.1



Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

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

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

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

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-22 01:06

Table of Contents

Amazon Web Services Plugin Overview.....	6
About Certification Compliance Mode	7
Use Cases	7
Consolidated Visibility	7
Encryption	7
Dynamic Segmentation of Instances	7
Security Management of EC2 Instances	7
AWS Account	8
IAM Roles and Users	8
Network Awareness	8
Storage Access	8
How It Works.....	8
Polling.....	8
What to Do	9
Additional Amazon Web Services Documentation.....	9
Requirements.....	9
ForeScout Requirements	10
AWS Requirements.....	10
Networking Requirements	11
Define AWS Users	11
Specify Permissions Using Standard AWS Policies	12
Specify Permissions Using Generic Custom Policies	14
Specify Minimal Permissions Using Specific Custom Policies	14
EC2 Instance: Manual Poll	14
EC2 Instance: Take Action on a Resource	15
VPC: Manual Poll	15
VPC: Take Action on a Resource	16
IAM User: Manual Poll	16
IAM User: Take Action on a Resource.....	17
IAM Role: Manual Poll	17
S3 Buckets: Manual Poll	17
S3 Buckets: Take Action on a Resource	18
Config: Manual Poll.....	18
Polling of All Relevant Resources	19
Actions on All Resources.....	20
Deploy Lambda Artifacts on AWS.....	20
Complete Recommended Minimal JSON Permissions for AWS Plugin	21
Assume Role Option	23
Access AWS Credentials	26
Enable AWS Config on AWS Account	26
Install the Module	27
Configure the Module	28

Add an AWS Connection	28
About Delta Polling	37
AWS Pane with Failover Clustering	37
Ensure That the AWS Plugin Is Running	38
Test the AWS Connection	39
Manually Deploy Delta Polling Artifacts	40
Manually Poll AWS Entities.....	40
Edit the AWS Connection.....	41
Remove the AWS Connection	42
Configure AWS Policy Templates	43
Create a Policy from a Template.....	43
Scope for AWS Asset Classification Template	49
AWS Policy Templates.....	49
EC2 Instances Policy Templates	50
IAM Users and Roles Policy Templates.....	50
S3 Buckets Policy Templates.....	51
VPCs Policy Templates	51
OTHER Policy Templates.....	51
Update the AMI Whitelist.....	51
Detect Cloud Endpoints – Host Properties	53
AWS Properties	53
AWS EC2 Properties.....	54
AWS IAM Role Properties.....	58
AWS IAM User Properties	59
AWS S3 Properties	61
AWS Service Properties.....	62
AWS VPC Properties	63
Manage AWS Cloud Endpoints	65
Access AWS IAM Role Inventory.....	65
Access AWS EC2 Inventory.....	66
Access AWS IAM User Inventory	67
Access AWS S3 Inventory.....	68
Access AWS VPC Inventory.....	69
Run Policy Actions.....	70
Manually Run AWS Actions on EC2 Instance	70
Apply EC2 Security Groups Action	71
Disable EC2 Termination Protection Action.....	74
Enable EC2 Termination Protection Action.....	75
Start EC2 Instance Action.....	77
Stop EC2 Instance Action	79
Manually Run AWS IAM Actions	81
Activate User Access Key Action	82

Deactivate User Access Key Action	83
Delete User Access Key Action	85
Enforce Password Policy Action.....	87
Manually Run AWS S3 Actions.....	90
Block Public Access Action	91
Manually Run AWS VPC Actions.....	92
Detach Internet Gateway(s) Action.....	93
Set Action Thresholds	94
Best Practices for Working with the AWS Plugin	95
Hybrid Cloud Module Information	96
Additional Forescout Documentation.....	96
Documentation Downloads	96
Documentation Portal	97
Forescout Help Tools.....	97


Amazon Web Services Plugin Overview

The Amazon Web Services Plugin is a component of the Forescout Hybrid Cloud Module. See [Hybrid Cloud Module Information](#) for details about the module.

The AWS Plugin connects to the Amazon® Web Services (AWS) public cloud environment to retrieve information on Elastic Compute Cloud (EC2) instances and other AWS entities such as Identity and Access Management (IAM) users, Virtual Private Clouds (VPCs), and Amazon Simple Storage Service (S3). The EC2 instances, IAM users, and VPCs follow rules similar to those for other endpoints discovered by the Forescout platform where policies and actions can be defined on those entities. The Forescout platform's integration with AWS brings the detailed visibility, control, and compliance capabilities of the Forescout platform to EC2 instances and the associated AWS cloud configurations.

The AWS Plugin lets you:

- View endpoints, IAM users, and VPCs in Amazon's public cloud
- Create and apply Forescout policies across the AWS entities
- Maintain the security and compliance of cloud instances, IAM users, S3s, and VPCs
- Apply security groups to instances, enforce password policies, and perform a range of other policy actions

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

This plugin assists IT with a number of important challenges when it comes to cloud operations. By integrating the Forescout platform with AWS, you can:

- Have full visibility of your AWS instances and their properties. Since disparate teams may be starting and stopping instances in a public cloud environment, it is important for IT to have a good understanding of what resources are being used in the cloud. Regular checks provide valuable information on how and when AWS cloud resources are used.
- Use the Forescout Asset Inventory to review the distribution of endpoints in the cloud and mitigate them as required. For example, endpoints with out-of-date Amazon Machine Images (AMIs) are quickly identified for remediation.
- Enable/disable Termination Protection for AWS EC2 instances to prevent accidental termination (deletion) of an EC2 instance by establishing a policy in which all compliant and critical EC2 assets have termination protection enabled. See [Disable EC2 Termination Protection Action](#) and [Enable EC2 Termination Protection Action](#) for details.
- Collect information about the AWS environment across multiple AWS regions and multiple AWS accounts, all from a common deployment. This includes fine-grained details such as the creation of new IAM users, lack of password changes, the presence of Internet Gateways in a VPC, public access for S3, and other AWS operational details.

- Discover cloud-based endpoints early, allowing identification and compliance checking of the workload itself. A non-compliant endpoint can be stopped, assigned to a quarantined security group, and/or the AWS account team can be notified. If remediation fails, the endpoint can be fully isolated and stopped to prevent further damage.

About Certification Compliance Mode

Forescout Hybrid Cloud Module: Amazon Web Services (AWS) Plugin supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Use Cases

This section describes sample use cases supported by this plugin. To understand how this plugin helps you achieve these goals, see [How It Works](#).

Consolidated Visibility

Integrating with AWS extends the capability of the Forescout platform to see and control instances running in AWS. This allows visibility for campus, data center, and cloud endpoints from the same CounterACT® device (depending on the scale of the environment).

Encryption

Policy templates are provided to verify that EC2 Elastic Block Storage (EBS) or S3 resources are encrypted. EBS volumes associated with an EC2 instance are collected. An optional action to stop non-compliant EC2 instances is also provided.

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, and production. 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 default or non-complaint security groups. You can then take action to remediate that by applying stricter security policies using well-defined security groups, and making those security groups compliant.

AWS Account

Policy templates are provided to verify that Multi-Factor Authentication (MFA) is enabled for the root user, to continuously monitor if the password has not been changed, and to verify that AWS Config is enabled for an AWS account.

IAM Roles and Users

IAM users, group, and roles and associated properties can be collected. You can use policy templates to continuously monitor for new or modified IAM roles and IAM users, to verify that a password policy is enabled for every user, and to implement an action to enable a password policy for users who do not have a password policy set.

Network Awareness

VPCs configured for an AWS account and the associated properties, such as subnets, Internet gateways, and VPC peers, can be collected. You can use policy templates to verify that no EC2 instance has a public IP address that is an Internet-facing address, to monitor external ELB associated with a VPC, to monitor VPC peering connections, and to allow peering connections between central VPCs and sub-VPCs. An action to allow for termination of an Internet gateway is also provided.

Storage Access

S3 resources associated with an AWS account and the associated properties, such as name, owner, and tags can be collected. You can use policy templates to verify that an S3 bucket does not have public access. For those S3 buckets that have been misconfigured for public access, an action to block public access is provided.

How It Works

This plugin uses well-defined APIs from AWS to provide visibility of AWS EC2 instances, IAM users, S3s, and VPCs.

Once the configuration is completed using an AWS account with the appropriate IAM credentials and permissions, the Forescout platform starts communicating with one or more AWS accounts and retrieves information on EC2 instances running in AWS under that account, as well as the IAM users, S3s, and VPCs. Instance-related properties are collected as Forescout host properties, while other cloud entities (such as IAM users, S3s, and VPCs) are also displayed as *logical* endpoints in the Forescout platform. The query and collection of AWS entities and associated properties are invoked at configured time intervals.

Polling

To support continual updates of AWS properties, AWS 2.0 combines full polling with an optional delta polling mechanism. This ensures that AWS state changes are recognized in near real-time by the Forescout platform. The full poll gathers all aspects of the AWS environment from AWS APIs. The AWS APIs expose multiple attributes of the entities associated with an AWS account.

Because this data can be quite extensive, the full poll takes place at longer intervals (by default, every 30 minutes). The optional delta polling was added in AWS 2.0 so that EC2 instance state changes are recognized by the Forescout platform in near real-time. The delta poll leverages the functionality exposed by AWS Config, Lambda functions, and CloudWatch logs to quickly capture EC2 state changes as well as modifications to other AWS entities. Since this only looks for delta changes, it takes place over shorter intervals, with a default of one minute.

The Forescout platform requires a range of permissions to enable polling services, including the ability to deploy delta polling into the AWS environment.

See [Specify Permissions Using Standard AWS Policies](#) for details about AWS permissions, and [Best Practices for Working with the AWS Plugin](#).

What to Do

To set up your system for integration with AWS environments, perform the following steps:

1. Verify that you have met system requirements. See [Requirements](#).
2. [Define AWS Users](#).
3. [Configure the Module](#).
4. Use the in-depth information reported by the plugin to manage virtual devices:
 - [Configure AWS Policy Templates](#)
 - [Detect Cloud Endpoints – Host Properties](#)
 - [Manage AWS Cloud Endpoints](#)
 - [Run Policy Actions](#)

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 Forescout policies and other basic features work. For more information on installation, configuration, and general guides, refer to the following:

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

Requirements

This section describes system requirements, including:

- [Forescout Requirements](#)
- [AWS Requirements](#)

- [Networking Requirements](#)

Forescout Requirements

The plugin requires the following Forescout release and other components:

- Forescout version 8.2.
- Hybrid Cloud Module version 2.1, with the AWS component running.
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

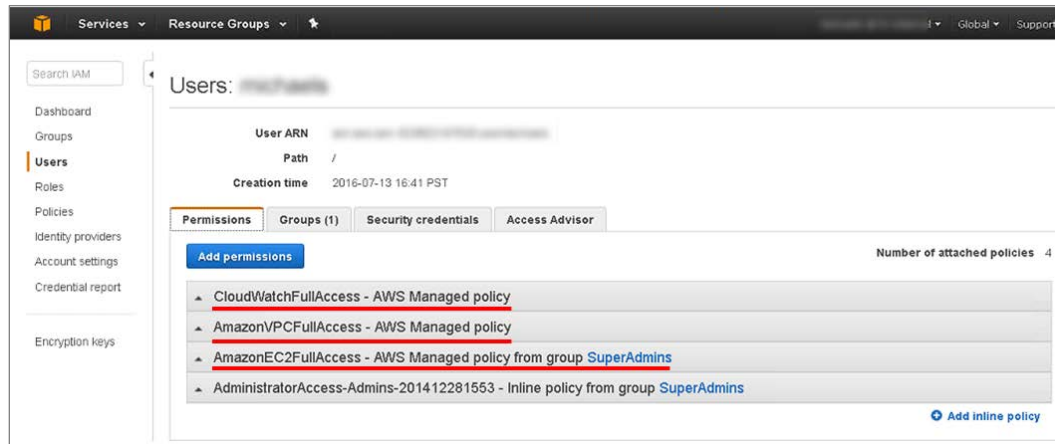
AWS Requirements

This plugin requires the following AWS components:

- An Amazon Web Services online account.
- 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 need that proxy's credentials.
- The plugin requires the following AWS services:
 - **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.
 - **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.

There are two user permissions options that can be used on the Forescout platform:

- Read-only permissions (the Forescout platform will support visibility only)
- Full permissions (the Forescout platform will support both visibility and control)



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 the Forescout platform 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

Define AWS Users

To let the Forescout platform query AWS, define a user with the Identity and Access Management (IAM) service. Specify the credentials of this user when you define the Forescout platform's connections to AWS.

Because the plugin detects and manages a range of AWS entities, the AWS user used on the Forescout platform should have full access across a range of permissions. If there is no need to manage AWS entities through Forescout actions, the AWS user used on the Forescout platform only needs read-only permissions.

The permissions are described in the following sections:

- [Specify Permissions Using Standard AWS Policies](#)
- [Specify Permissions Using Generic Custom Policies](#)
- [Specify Minimal Permissions Using Specific Custom Policies](#)

For all JSON examples in the permissions sections, copy them from the permissions sections and paste them unchanged into the AWS Console for the AWS Account.

In addition, see:

- [Assume Role Option](#)
- [Access AWS Credentials](#)

- [Enable AWS Config on AWS Account](#)

Specify Permissions Using Standard AWS Policies

The range of AWS permissions needed by the Forescout platform are listed in this section.

Review [Polling](#) for additional details on the differences.

Item	Resources	Permission Needed	Comments
Discover resource (FULL POLL)	EC2 Instances, VPC, Peering Connections	AmazonEC2ReadOnlyAccess	
Discover resource (FULL POLL)	IAM Users, IAM Roles	IAMReadOnlyAccess	
Discover resource (FULL POLL)	AWS Config	AWSConfigUserAccess	
Discover resource (FULL POLL)	S3 Buckets	AmazonS3ReadOnlyAccess	
Discover modification to a resource (DELTA POLL)	EC2 Instances	CloudWatchLogsReadOnlyAccess	This is determined by reading CloudWatch logs that are populated by CloudWatch Events. Prerequisite: CloudWatch Event Rules/Lambda functions and CloudWatch Log groups need to be deployed on that account/region.

Discover modification to a resource (DELTA POLL)	VPC, Peering Connections, IAM Users, IAM Roles	CloudWatchLogsReadOnlyAccess	This is determined by reading CloudWatch logs that are populated by AWS Config. Prerequisite: AWS Config needs to be enabled on that account/region, and CloudWatch Event Rules/Lambda functions and CloudWatch Log groups need to be deployed on that account/region.
Perform action on a resource	EC2 Instances, VPC	AmazonEC2FullAccess	
Perform action on a resource	IAM User	IAMFullAccess	
Perform user access key rotation	IAM User	IAMFullAccess	
Perform action on a resource	S3 Buckets	AmazonS3FullAccess	
Deploy AWS to the Forescout platform's delta polling update functionality	Per Account/ Per Region	AWSLambdaFullAccess	This enables the Forescout AWS Plugin to create a Lambda function in AWS so that the Forescout platform's delta polling has updated information related to EC2 instances.

 The permission policies in this table are standard policies present in AWS.

Use the following policies for the Forescout platform to perform the functions listed above:

- AWSConfigUserAccess
- CloudWatchLogsReadOnlyAccess
- AmazonEC2FullAccess
- IAMFullAccess
- AWSLambdaFullAccess
- AmazonS3FullAccess

Specify Permissions Using Generic Custom Policies

Alternatively, you can create a custom policy. The following JSON example allows read access on ELBs and read/write access on all resources on the other seven services listed.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:*",
        "config:*",
        "ec2:*",
        "elasticloadbalancing:Describe*",
        "events:*",
        "iam:*",
        "lambda:*",
        "logs:*"
      ],
      "Resource": "*"
    }
  ]
}
```

Specify Minimal Permissions Using Specific Custom Policies

This section contains the permissions for various operations, using the principle of the least or minimal privilege.

The following JSON examples are for the current set of operations that the plugin performs. A later version of the plugin, using newer APIs, will necessitate an update of these permissions.

These various individual permissions can be in common JSON. For additional details, refer to AWS postings on topics such as the following:

- <https://aws.amazon.com/blogs/security/back-to-school-understanding-the-iam-policy-grammar/>
- https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

EC2 Instance: Manual Poll

```
{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeImages",
            "ec2:DescribeAddresses",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeFlowLogs",
            "ec2:DescribeVolumes",
            "ec2:DescribeSubnets",
            "ec2:DescribeSecurityGroups"
        ],
        "Resource": "*"
    }
}

```

EC2 Instance: Take Action on a Resource

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifyInstanceAttribute",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        }
    ]
}

```

VPC: Manual Poll

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInternetGateways",

```

```

        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeEgressOnlyInternetGateways",
        "elasticloadbalancing:DescribeLoadBalancers"
    ],
    "Resource": "*"
}
]
}

```

VPC: Take Action on a Resource

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DetachInternetGateway"
      ],
      "Resource": "*"
    }
  ]
}

```

IAM User: Manual Poll

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:ListGroupsForUser",
        "iam:ListAccountAliases",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListMFADevices",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:ListVirtualMFADevices",
        "iam:GenerateCredentialReport",

```



```

        "iam:GetCredentialReport"
      ],
      "Resource": "*"
    }
  ]
}

```

IAM User: Take Action on a Resource

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:DeleteAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys",
        "iam:CreateAccessKey"
      ],
      "Resource": "*"
    }
  ]
}

```

IAM Role: Manual Poll

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "*"
    }
  ]
}

```

S3 Buckets: Manual Poll

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketTagging",
            "s3:GetEncryptionConfiguration",
            "s3:GetBucketObjectLockConfiguration"
        ],
        "Resource": "*"
    }
}
```

S3 Buckets: Take Action on a Resource

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketAccessBlock"
            ],
            "Resource": "*"
        }
    ]
}
```

Config: Manual Poll

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "config:DescribeDeliveryChannels",
            "Resource": "*"
        }
    ]
}
```

Polling of All Relevant Resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeEgressOnlyInternetGateways",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:ListGroupsForUser",
        "iam:ListAccountAliases",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListMFADevices",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateCredentialReport",
        "iam:GetCredentialReport",
        "iam:ListVirtualMFADevices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketObjectLockConfiguration",
        "config:DescribeDeliveryChannels",
        "logs:FilterLogEvents",
        "logs:DescribeLogStreams",
```

```

        "logs:GetLogEvents"
      ],
      "Resource": "*"
    }
  ]
}

```

Actions on All Resources

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "iam:DeleteAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys",
        "iam:CreateAccessKey",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DetachInternetGateway",
        "s3:PutBucketAccessBlock"
      ],
      "Resource": "*"
    }
  ]
}

```

Deploy Lambda Artifacts on AWS

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "iam:GetRole",

```

```

        "iam:CreateRole",
        "iam:PassRole",
        "events:PutRule",
        "events:PutTargets",
        "events:DescribeRule",
        "logs:DescribeLogGroups",
        "logs:PutMetricFilter",
        "logs:CreateLogGroup"
    ],
    "Resource": "*"
}
]
}

```

Complete Recommended Minimal JSON Permissions for AWS Plugin

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "config:DescribeDeliveryChannels",
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:StartInstances",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2>DeleteEgressOnlyInternetGateway",
        "ec2:DetachInternetGateway",

```


```

        "elasticloadbalancing:DescribeLoadBalancers",
        "events:PutRule",
        "events:PutTargets",
        "events:DescribeRule",
        "iam:ListGroupsForUser",
        "iam:ListAccountAliases",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListMFADevices",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateCredentialReport",
        "iam:GetCredentialReport",
        "iam:ListVirtualMFADevices",
        "iam:ListRoles",
        "iam:DeleteAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAccessKey",
        "iam:ListAccessKeys",
        "iam:CreateAccessKey",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PassRole",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "logs:FilterLogEvents",
        "logs:DescribeLogGroups",
        "logs:PutMetricFilter",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "s3:PutBucketAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketObjectLockConfiguration"
    ],
    "Resource": "*"
}
]
}

```

Assume Role Option

The Assume Role option is supported when integrating the Forescout platform with AWS. The Assume Role option is an alternative approach to defining the permissions at the individual account level as described above. With Assume Role, all the necessary permissions are added under AWS Role including the ability to reach into other AWS accounts, if desired.

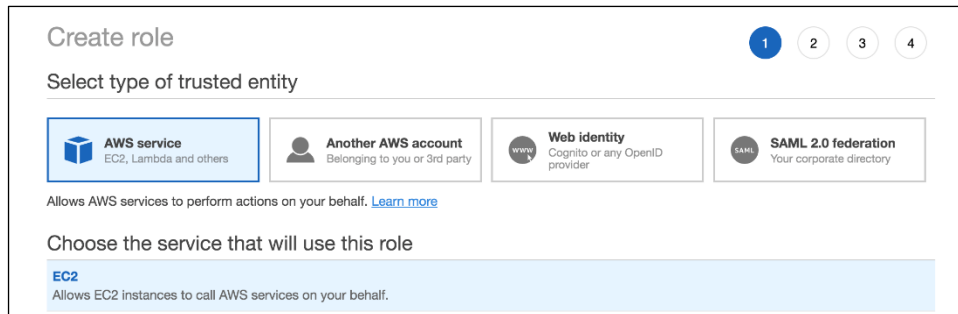
 *The Assume Role token defaults to one hour and has no ramifications on poll cycles.*

For more information on Assume Role, refer to:

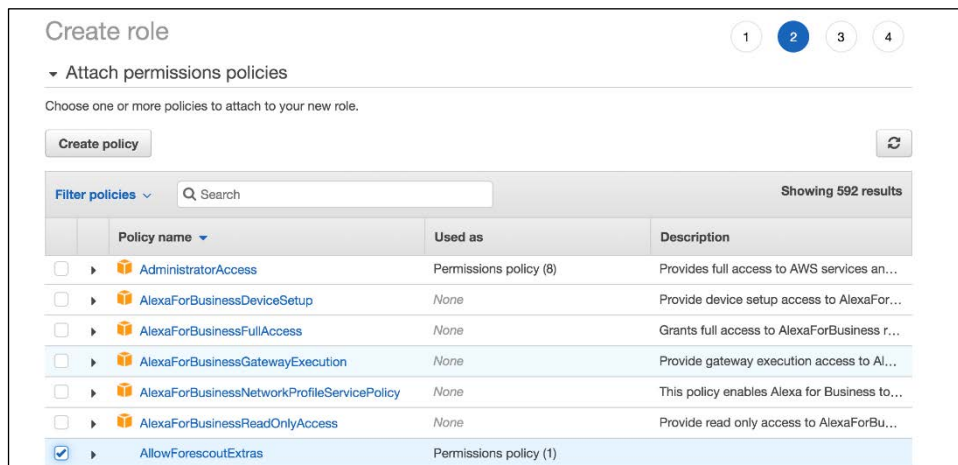
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html

To create an assume role and user:

1. Go to **IAM > Role**, select **Create role**, and then select the service type for the role, such as EC2.



2. Select **Next**, then select the desired policies, such as AllowForescoutExtras.



	Policy name	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Permissions policy (8)	Provides full access to AWS services an...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	None	Provide device setup access to AlexaFor...
<input type="checkbox"/>	AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusiness r...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	None	Provide gateway execution access to AI...
<input type="checkbox"/>	AlexaForBusinessNetworkProfileServicePolicy	None	This policy enables Alexa for Business to...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaForBu...
<input checked="" type="checkbox"/>	AllowForescoutExtras	Permissions policy (1)	

3. Select **Next** to optionally add tags.

Create role 1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
User	ForeScout	✕
Add new key		

You can add 49 more tags.

4. Select **Next**, enter a name for the role, then select **Create role**.

Create role 1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and '+', '@', '-' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '+', '@', '-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies [AllowForeScoutExtras](#)

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
User	ForeScout

* Required Cancel Previous **Create role**

The role is now in the list.

5. Configure users through the trust relationship under the Role configuration panel.

Roles > AssumeRoleForeScout

Summary

[Delete role](#)

Role ARN arn:aws:iam::840920012568:role/AssumeRoleForeScout [Copy](#)

Role description Allows EC2 instances to call AWS services on your behalf. [Edit](#)

Instance Profile ARNs arn:aws:iam::840920012568:instance-profile/AssumeRoleForeScout [Copy](#)

Path /

Creation time 2019-09-22 08:24 PDT

Maximum CLI/API session duration 1 hour [Edit](#)

Permissions **Trust relationships** **Tags (1)** **Access Advisor** **Revoke sessions**

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

[Edit trust relationship](#)

Trusted entities

The following trusted entities can assume this role.

Trusted entities

The identity provider(s) ec2.amazonaws.com

Conditions

The following conditions define how and when trusted entities can assume the role.

There are no conditions associated with this role.

- To add a user, edit the trust relationship.

Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": "ec2.amazonaws.com",
8         "AWS": [
9           "arn:aws:iam::840920012568:user/roleAssumer"
10        ]
11      },
12       "Action": "sts:AssumeRole"
13     }
14   ]
15 }

```

- Go to **IAM > User > the user to be configured > Permissions > Add permissions** to configure the following policy for a specific IAM user to be trusted by the role. (Sometimes, this may be the only policy for that user.)

Grant permissions

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

[Create policy](#) [Refresh](#)

Filter policies Showing 1 result

Policy name	Type	Used as	Description
AssumeRole	Managed		Allows an entity to assume the role

[Policy summary](#) [JSON](#) [Edit policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "sts:AssumeRole",
8       "Resource": "arn:aws:iam::*:role/*"
9     }
10   ]
11 }

```

Selecting Assume Role and Key Rotation together is currently not supported.

Access AWS Credentials

To access your AWS credentials:

1. Go to <https://console.aws.amazon.com> and log in using your username and password.
2. Select **Services**.
3. Select **IAM** from the Security section. 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. The sign-in credentials are displayed.
7. In the Access Keys section, the AWS Access key ID is displayed. Access Keys let you control the credentials you will need to configure in the Forescout AWS Plugin. Copy the **Access key ID** and locate the corresponding Secret Access Key.

Enable AWS Config on AWS Account

AWS Config needs to be manually enabled on your AWS account, per region. For global entities, such as IAM, the AWS Config recording only occurs on a selected "home" region.

The settings in the following example record all resources in the region and monitor global resources. You also need to configure an Amazon S3 bucket and an AWS Config role, however the AWS Plugin only uses CloudWatch logs and does not rely on the S3 buckets for information.

Recording is on

[Turn off](#)

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all resources in the region.

All resources ☒ Record all resources supported in this region ⓘ

☒ Include global resources (e.g., AWS IAM resources) ⓘ

Specific types

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.

☐ Create a bucket

☒ Choose a bucket from your account

☐ Choose a bucket from another account ⓘ

Bucket name* / Prefix (optional) / AWSLogs/840920012568/Config/eu-west-2

Amazon SNS topic

☐ Stream configuration changes and notifications to an Amazon SNS topic.

Amazon CloudWatch Events rule

AWS Config sends detailed information about the configuration changes and notifications to Amazon CloudWatch Events. To create rules, visit the [AWS Config console](#).

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon CloudWatch Events.

☐ Create a role

☒ Choose a role from your account

AWS Config can assume the following IAM roles. AWS Config will attach the required policies for recording resources and accessing your S3 bucket.

Role name* ☐ Use the role as is. AWS Config won't attach any policies.

Alternatively, you can select resources as needed. The AWS Plugin uses information from the following resources.

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all resources in the region.

All resources ☐ Record all resources supported in this region ⓘ

☐ Include global resources (e.g., AWS IAM resources) ⓘ

Specific types


Install the Module


To install the module:

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

To identify your licensing mode, select **Help > About ForeScout** from the Console.

2. Download the module **.fpi** file.
3. Save the file to the machine where the Console is installed.
4. Log into the Console and select **Options** from the **Tools** menu.
5. Select **Modules**. The Modules pane opens.
6. Select **Install**. The Open dialog box opens.
7. Browse to and select the saved module **.fpi** file.
8. Select **Install**. The Installation screen opens.
9. Select **I agree to the License Agreement** to confirm that you have read and agree to the terms of the License Agreement and select **Install**. The installation cannot proceed unless you agree to the license agreement.

 *The installation begins immediately after selecting Install and cannot be interrupted or canceled.*

 *In modules that contain more than one component, the installation proceeds automatically one component at a time.*


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

 *Some components are not automatically started following installation.*

Configure the Module

Configure the module to ensure that the Forescout platform can communicate with AWS API access points. For details, see:

- [Add an AWS Connection](#)
- [AWS Pane with Failover Clustering](#)

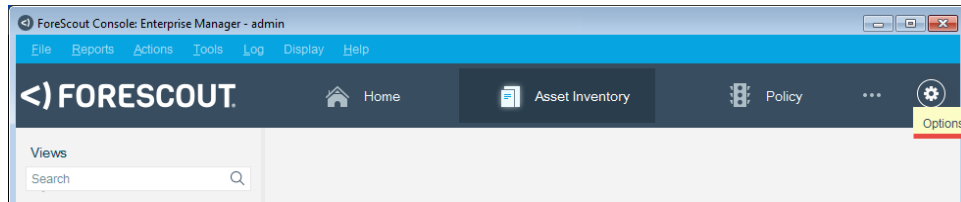
 *Before you configure the AWS Plugin, verify that the corresponding [Requirements](#) are met. Removing a configured connection stops endpoint discovery and property learning of virtual machines unique to the connection, but any actions remain enabled.*

Add an AWS Connection

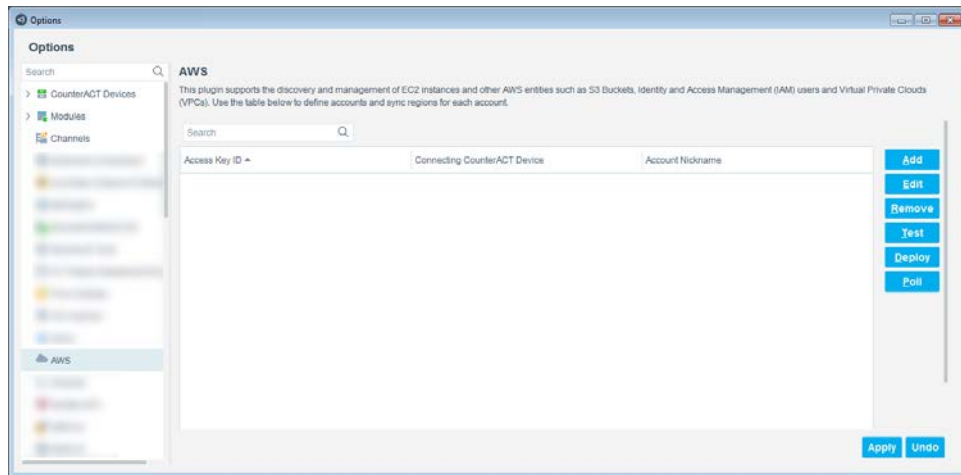
You can add an AWS connection from the Forescout platform. Verify that you have access to your AWS credentials before adding a connection. The Access Key ID corresponds to your AWS EC2 account on the AWS online portal.

To add an AWS connection:

1. In the Console, select **Options** from the **Tools** menu.



2. In the Options pane, select **AWS**.



3. Select **Add**. If you have not set up your AWS credentials, see [Access AWS Credentials](#).

4. Enter values for the following parameters, which are used to specify login credentials for AWS.

Access Key ID	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 provided when you created a user profile in your AWS account. The username of the IAM user is not required, but the credentials are used in the Access Key and Secret Access Key for authentication.
Secret Access Key	
Verify Secret Access Key	Re-enter the Secret Access Key to verify it.
Enable Assume Role	<p>Select this option to enable the Assume Role, which adds a security token to the Access Key ID and Secret Access Key for authentication. The Assume Role provides the IAM user temporary security credentials that enable access to certain AWS resources in your account. The account can be either controlled by you or by a third party. Through the AWS console, create a role that has access to the resources. See Assume Role Option.</p> <p>After selecting this option, enter the Assume Role ARN.</p> <p>Note that you cannot select both Enable Assume Role and Enable rotation of the access key.</p>

Assume Role ARN	Enter the Amazon Resource Name (ARN) of the Assume Role from the AWS console, for example, arn:aws:iam::123456789012:role/Test
Enable rotation of the access key	<p>Select this option to enable rotation of the access key when you do not want the Access Key ID and Secret Access Key to be hard-coded. Rotating access keys provides a higher level of security between the Forescout platform and AWS.</p> <p>Key rotation requires IAMFullAccess permission.</p> <p>For the same access key, you cannot enable key rotation on more than one configuration entry. For example, if you have two accounts configured with the same access key, an error message is displayed if you try to enable key rotation on both.</p> <p>Key rotation in AWS will fail if there is more than one key already present in the associated AWS account.</p> <p>After selecting this option, enter a Key rotation Interval (days). Note that you cannot select both Enable Assume Role and Enable rotation of the access key.</p>
Key rotation Interval (days)	Enter the number of days to specify the frequency of the key rotation. The values are from 30 to 365 days. The default is 90 days.
Environment	<p>From the drop-down menu, select AWS Standard Account, AWS US Gov Cloud Account, or AWS China Account.</p> <p>The access key credentials differ for these accounts.</p>
Connecting CounterACT Device	<p>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 AWS.</p> <p>In the drop-down list, select an IP Address listed in the Appliances folder. Only one IAM user is allowed for a connecting device.</p>
Account Nickname	(Optional) Add a label or nickname to distinguish this connection from other AWS connections.

5. Select **Next**.

Add AWS Connection - Step 2 of 4

Add AWS Connection

- General
- Proxy Server Definition**
- Regions
- 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 Host

Proxy Server Port

Proxy Server Username

Proxy Server Password

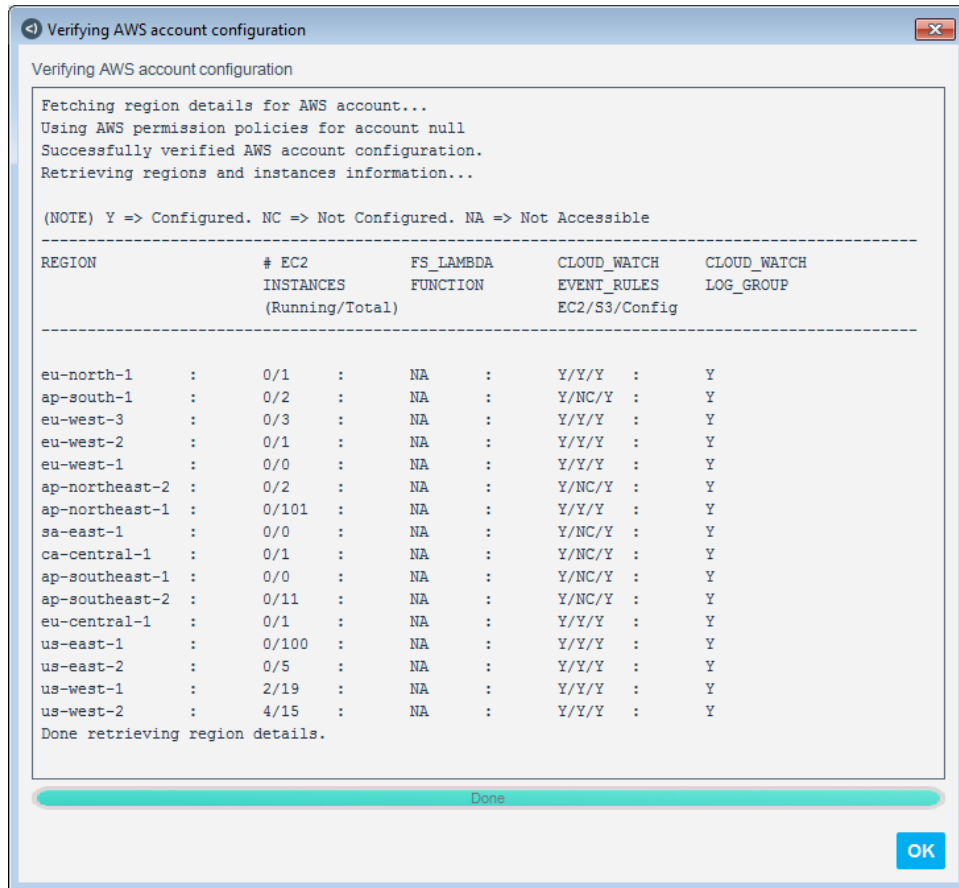
Verify Password

[Help](#) [Previous](#) [Next](#) [Finish](#) [Cancel](#)

(Optional) Enter the proxy server information. If a proxy server with Basic Authentication is used, the proxy credentials are required (see [AWS Requirements](#)).

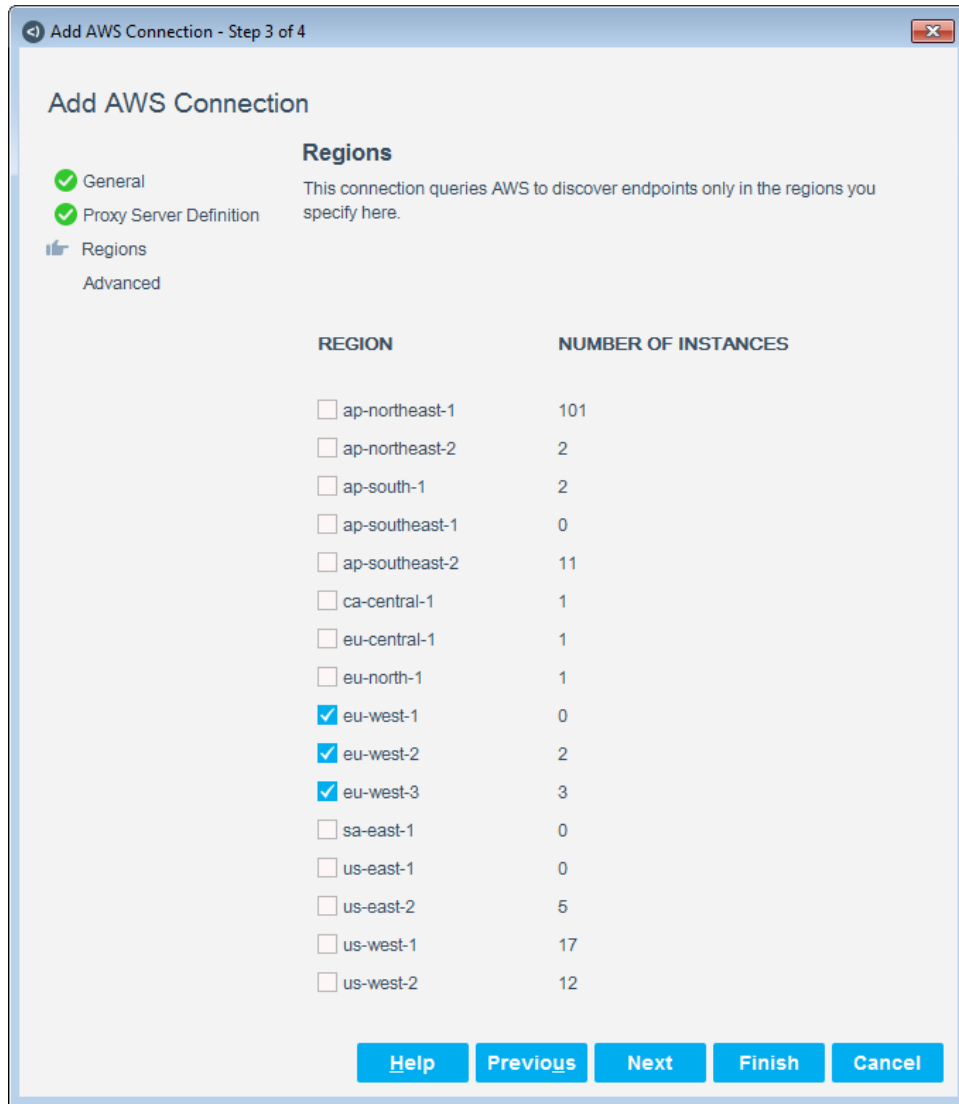
Use Proxy Server	If your environment routes internet communications through proxy servers, select this option.
Proxy Server Host	Enter the IPv4 address or the domain name of the proxy server.
Proxy Server Port	Select the port number of the proxy server.
Proxy Server Username	(Optional) If Basic Authentication is used, enter the proxy server's username.
Proxy Server Password	(Optional) If Basic Authentication is used, enter the proxy server's password.
Verify Password	Re-enter the proxy server's password.

6. Select **Next**. The list of available regions is retrieved for the connected account. The following successful results are for a user who has all Discovery-related permissions (AmazonEC2ReadOnlyAccess, IAMReadOnlyAccess, and AWSConfigUserAccess). Errors are displayed if the user does not have all the required permissions.



If key rotation is enabled, a line will be displayed near the top of the **Verifying AWS account configuration** dialog box stating the access key for which key rotation is enabled.

7. Select **OK**.



Add AWS Connection

General
Proxy Server Definition
Regions
Advanced

Regions
This connection queries AWS to discover endpoints only in the regions you specify here.

REGION	NUMBER OF INSTANCES
<input type="checkbox"/> ap-northeast-1	101
<input type="checkbox"/> ap-northeast-2	2
<input type="checkbox"/> ap-south-1	2
<input type="checkbox"/> ap-southeast-1	0
<input type="checkbox"/> ap-southeast-2	11
<input type="checkbox"/> ca-central-1	1
<input type="checkbox"/> eu-central-1	1
<input type="checkbox"/> eu-north-1	1
<input checked="" type="checkbox"/> eu-west-1	0
<input checked="" type="checkbox"/> eu-west-2	2
<input checked="" type="checkbox"/> eu-west-3	3
<input type="checkbox"/> sa-east-1	0
<input type="checkbox"/> us-east-1	0
<input type="checkbox"/> us-east-2	5
<input type="checkbox"/> us-west-1	17
<input type="checkbox"/> us-west-2	12

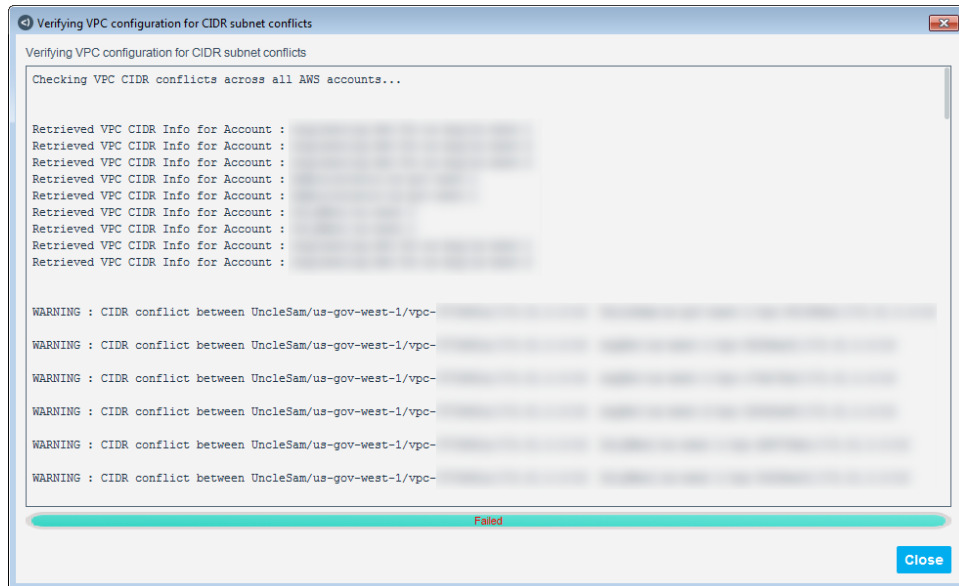
Help Previous Next Finish Cancel

8. Select one or more regions.

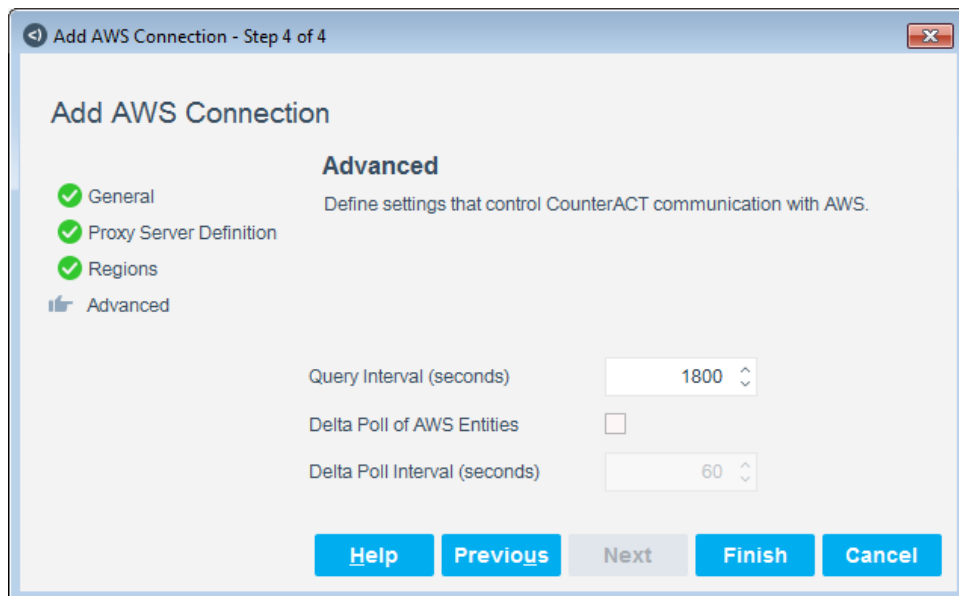
The Regions pane is automatically populated:

- If Amazon adds a new region, it will be displayed.
- If you add a connection using AWS US Gov Cloud Account credentials, us-gov regions, such as us-gov-west-1, will be displayed.
- If you add a connection using AWS China Account credentials, cn regions, such as cn-north-1, will be displayed.

9. Select **Next.**



10. Select **Close**.

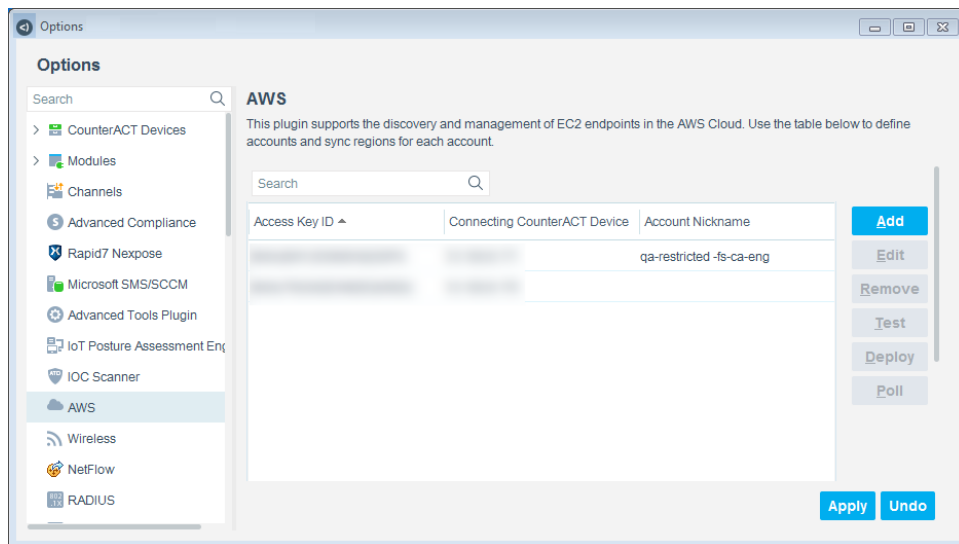


11. Set the communication controls between the Forescout platform and AWS.

Query Interval (seconds)	Specify how frequently the plugin should query AWS for a full poll. The default is 1800 seconds (30 minutes). The range is from 60 seconds (one minute) to 86400 seconds (24 hours).
---------------------------------	---

Delta Poll of AWS Entities	<p>Select this option to enable delta polling of AWS entities (EC2 instances, IAM users and roles, S3 buckets, VPCs, and more). This option enables AWS Lambda functions and the CloudWatch monitoring service. See About Delta Polling for details.</p> <p>After selecting this option, enter the Delta Poll Interval (seconds).</p>
Delta Poll interval (seconds)	<p>Specify the delta polling interval for which the AWS Plugin reaches out to CloudWatch log streams to get the most recent logs.</p> <p>The default is 60 seconds (one minute). The range is from 60 seconds (one minute) to 86400 seconds (24 hours).</p>

12. Select **Finish**. The new account is displayed in the AWS pane.



13. If delta polling is enabled, you are prompted for confirmation. Select **OK** to continue.

When delta polling is enabled, AWS Lambda functions, and CloudWatch Event Rules are created for each of the selected AWS regions. See [About Delta Polling](#).

14. (Recommended) Select **Test** to test the connection.

Information is displayed in the **Testing AWS Connection** dialog box, but a full poll is not yet successfully completed. See [Test the AWS Connection](#).

You cannot trigger a manual poll until after you select Apply and save the configuration.

15. In the AWS pane, select **Apply** and confirm the changes.

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

About Delta Polling

The delta polling mechanism recognizes state changes to the EC2 instance, such as a change from the Running to the Stopped state. Many attributes (other than EC2 instance state) can also change.

Amazon exposes these attributes through AWS Config, which is a recording of any configuration changes on the AWS account. The AWS Plugin leverages the functionality exposed by AWS Config to identify changes to EC2 properties, IAM users, IAM groups and IAM roles, VPC properties, and S3 properties.

Delta polling works as follows:

1. AWS Config records changes to EC2/IAM/VPC/S3 and sends them to CloudWatch and CloudTrail.
2. CloudWatch and CloudTrail receive the changes and forward them to the Lambda function.
3. The Lambda function logs the changes to CloudWatch and CloudTrail.
4. The delta polling mechanism reads the CloudWatch and CloudTrail logs at every delta polling interval.

Note the following:


- Changes to EC2 state information are reflected in the Forescout platform in approximately a minute. This delay is due to delta polling.
- Changes to EC2/IAM/VPC/S3 configuration propagated through AWS Config are reflected in the Forescout platform in approximately 10 to 15 minutes. This delay is due to AWS Config.

 *The polling response time for CloudWatch has a default of 10 minutes. CloudTrail has a default of 15 minutes.*

AWS Pane with Failover Clustering

When a connecting CounterACT Appliance is part of a failover cluster and the Appliance fails, it automatically falls back to another available Appliance in the cluster.

Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for details on installing and configuring Failover Clustering. See [Additional Forescout Documentation](#) for information on how to access this guide.

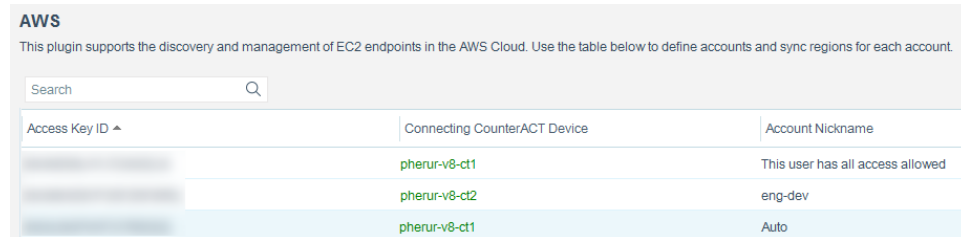
 *Failover Clustering supports continuous management of EC2 instances, but does not currently support non-IP/MAC AWS entities, such as IAM users or VPCs.*

To work with Failover Clustering, ensure that you have the relevant product license that supports the feature. The type of license required depends on which licensing mode your deployment is using. Refer to the *Forescout Resiliency and Recovery Solutions User Guide* for more information.

To view Failover Clustering in the AWS pane:

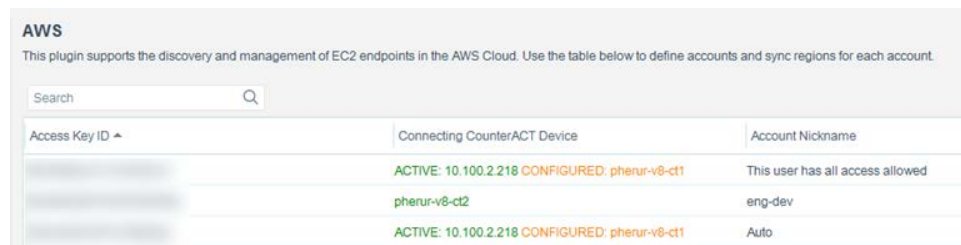
1. In the Console, select **Options** from the **Tools** menu.
2. In the Options pane, select **AWS**.

The status of Failover Clustering is displayed in green when a configured CounterACT Appliance is up and running.




Access Key ID	Connecting CounterACT Device	Account Nickname
[Redacted]	pherur-v8-ct1	This user has all access allowed
[Redacted]	pherur-v8-ct2	eng-dev
[Redacted]	pherur-v8-ct1	Auto

The status of Failover Clustering is displayed in green and orange when a configured CounterACT Appliance fails and another CounterACT Appliance becomes active.



Access Key ID	Connecting CounterACT Device	Account Nickname
[Redacted]	ACTIVE: 10.100.2.218 CONFIGURED: pherur-v8-ct1	This user has all access allowed
[Redacted]	pherur-v8-ct2	eng-dev
[Redacted]	ACTIVE: 10.100.2.218 CONFIGURED: pherur-v8-ct1	Auto

 When the original configured CounterACT Appliance returns, it becomes active.




Ensure That the AWS Plugin Is Running

After installing the AWS Plugin (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools** > **Options** > **Modules**.
2. In the *Modules* pane, hover over the AWS Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.

The name is preceded by one of the following icons:

-  - The AWS Plugin is stopped on all Forescout devices.
-  - The AWS Plugin is stopped on some Forescout devices.
-  - The AWS Plugin is running on all Forescout devices.

3. If the AWS Plugin is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

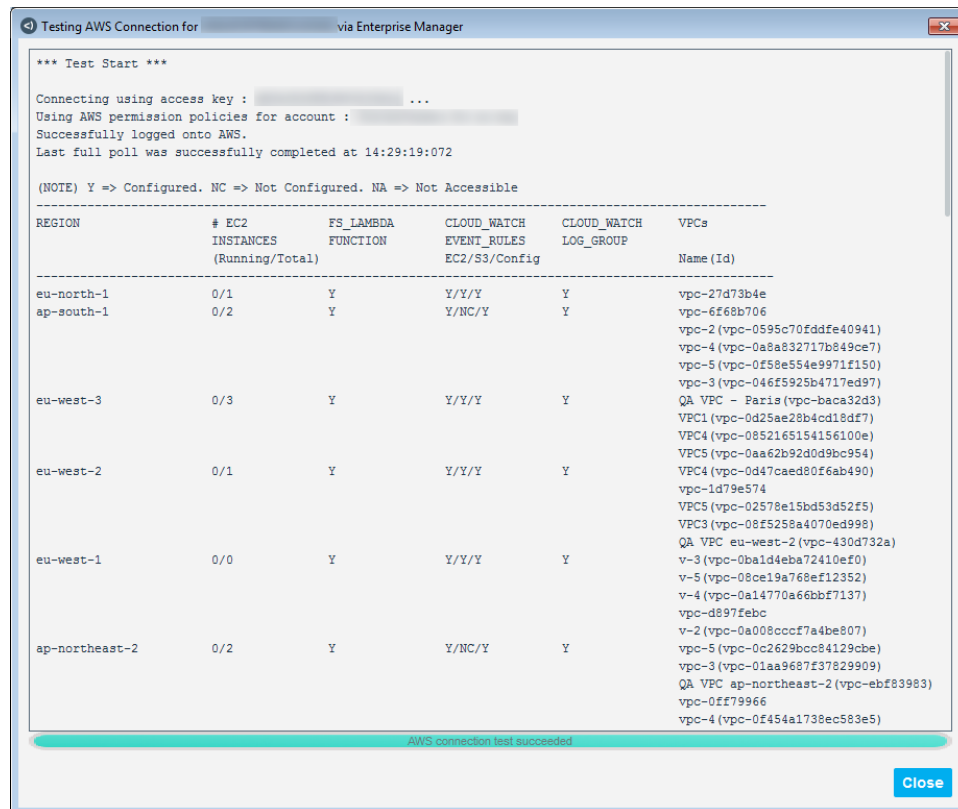
Test the AWS Connection

Using the configured settings, the Forescout platform attempts to connect to AWS and retrieve sample data associated with the IAM user in the AWS regions specified in the connection. The test functionality also indicates whether CloudWatch Event Rules have been configured to receive EC2 state change notifications and receive AWS Config notifications.

To test the AWS connection:

1. In the AWS pane, select an AWS connection and select **Test**.

The following successful results are for a user who has all Discovery-related permissions (AmazonEC2ReadOnlyAccess, IAMReadOnlyAccess, and AWSConfigUserAccess). Errors are displayed if the user does not have all the necessary permissions.



If key rotation is enabled, a line will be displayed near the top of the **Testing AWS configuration** dialog box warning that the user must have the appropriate permissions.

2. View the results, and then select **Close**.

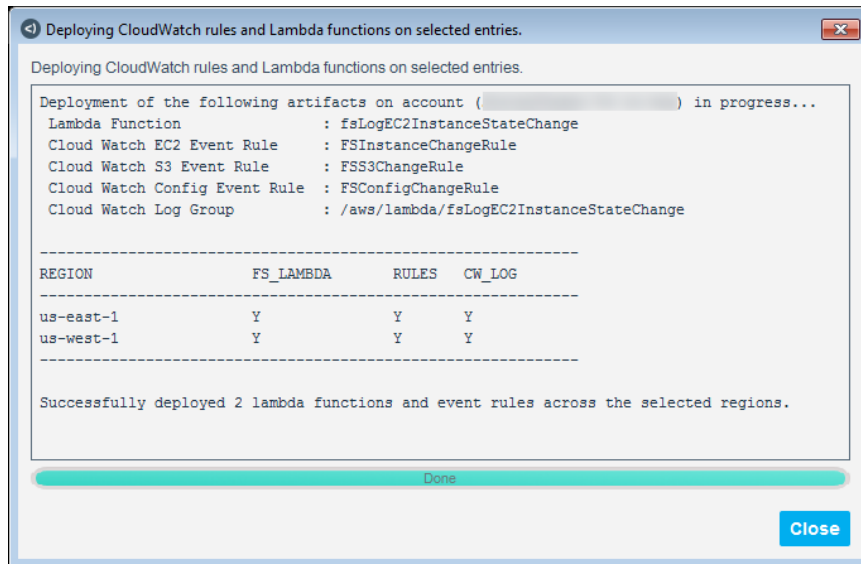
It is recommended you test the AWS connection after the AWS Plugin has been running for 1-2 minutes.

Manually Deploy Delta Polling Artifacts

You can deploy delta polling artifacts to see if any specific region does not have Lambda functions, CloudWatch Event Rules, or CloudWatch Logs configured. The deploy mechanism deploys the CloudWatch Event Rule that is needed to consume events from AWS Config. Errors are displayed if the user does not have all the required permissions.

To manually deploy delta polling artifacts on an AWS account:

1. In the AWS pane, select an AWS connection and select **Deploy**. The following successful results are for a user who has all the required permissions.



2. View the results, and then select **Close**.

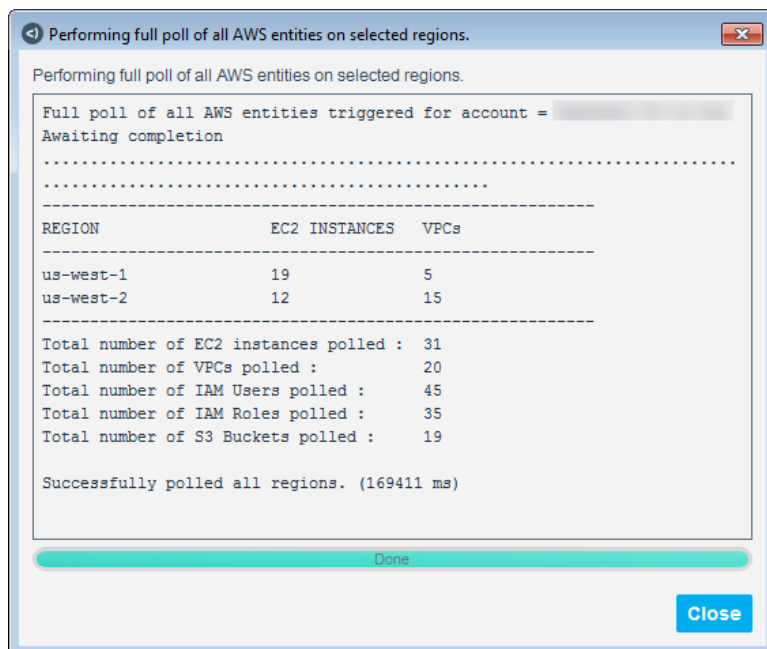
Manually Poll AWS Entities

You can manually poll AWS entities (EC2 instances, IAM users and roles, S3 buckets, VPCs, and more), when you do not want to wait for the scheduled poll. The full poll collects information from AWS, such as EC2 instance-related data. The poll results depend on the access permissions of the user. If the user does not have read permissions to EC2 or IAM, an error is displayed.

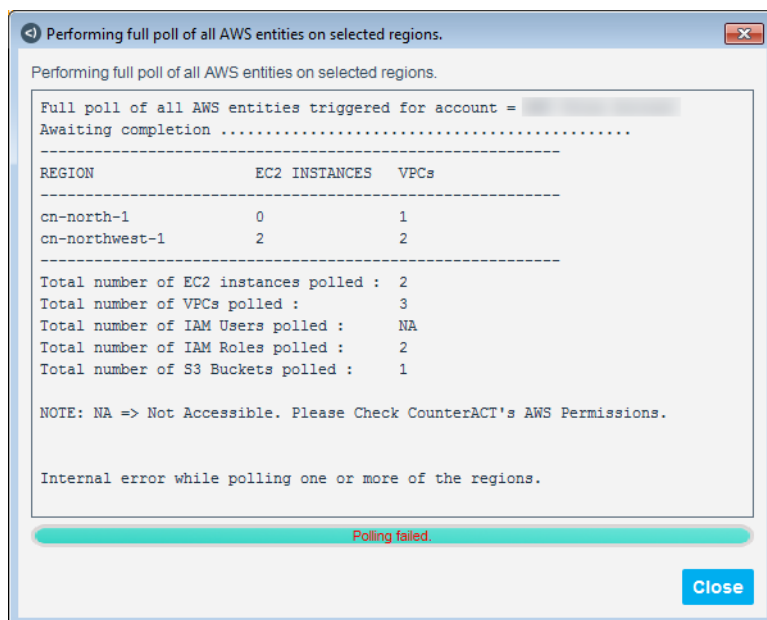
To manually poll AWS entities for an account:

1. In the AWS pane, select an AWS connection and select **Poll**.
2. View the results, and then select **Close**.

The following successful results are for a user who has both AmazonEC2ReadOnlyAccess and IAMReadOnlyAccess permissions. There are no errors even though this user does not have AWSConfigUserAccess permissions. However, in this case, no AWS Config-related information is displayed.



The following failed poll is for a user who does not have all the permissions.



3. Select **Close**.

Edit the AWS Connection

You can edit an AWS connection.

To edit an AWS connection:

1. In the AWS pane, select an AWS connection and select **Edit**.

The screenshot shows the 'Edit AWS Connection' dialog box with the 'General' tab selected. The dialog has a title bar with a back arrow, the text 'Edit AWS Connection', and a close button. Below the title bar are four tabs: 'General', 'Proxy Server Definition', 'Regions', and 'Advanced'. The 'General' tab is active and contains the following fields and options:

- General**
Specify login credentials for AWS. CounterACT communicates with the AWS to discover and implement management actions on the EC2 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 connection.
- Access Key ID: [text input field]
- Secret Access Key: [password input field with 8 asterisks]
- Verify Secret Access Key: [password input field with 8 asterisks]
- Enable Assume Role: ☐
- Assume Role ARN: [text input field]
- Enable rotation of the access key: ☐
- Key rotation Interval (days): [spin box set to 90]
- Environment: [dropdown menu showing 'AWS Standard Account']
- Connecting CounterACT Device: [dropdown menu showing 'Enterprise Manager']
- Account Nickname: [text input field]

At the bottom right of the dialog are three buttons: 'Help', 'OK', and 'Cancel'.

2. Edit the connection parameters in the General, Proxy Server Definition, Regions, and Advanced tabs, and select **OK**.

Remove the AWS Connection

You can remove a connection. Any actions already launched remain active and are not undone.

To remove an AWS connection:

1. In the AWS pane, select an AWS connection and select **Remove**.
2. When prompted for confirmation, select **OK**.

Configure AWS Policy Templates

The AWS Plugin provides additional endpoint properties and actions that are useful for the 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.

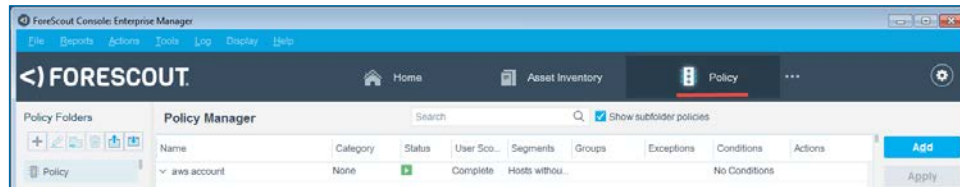
Before applying the templates, it is recommended that you have a basic understanding of Forescout policies. For more information about creating custom policies, refer to the Policy Management and Policy Templates chapters in the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

Create a Policy from a Template

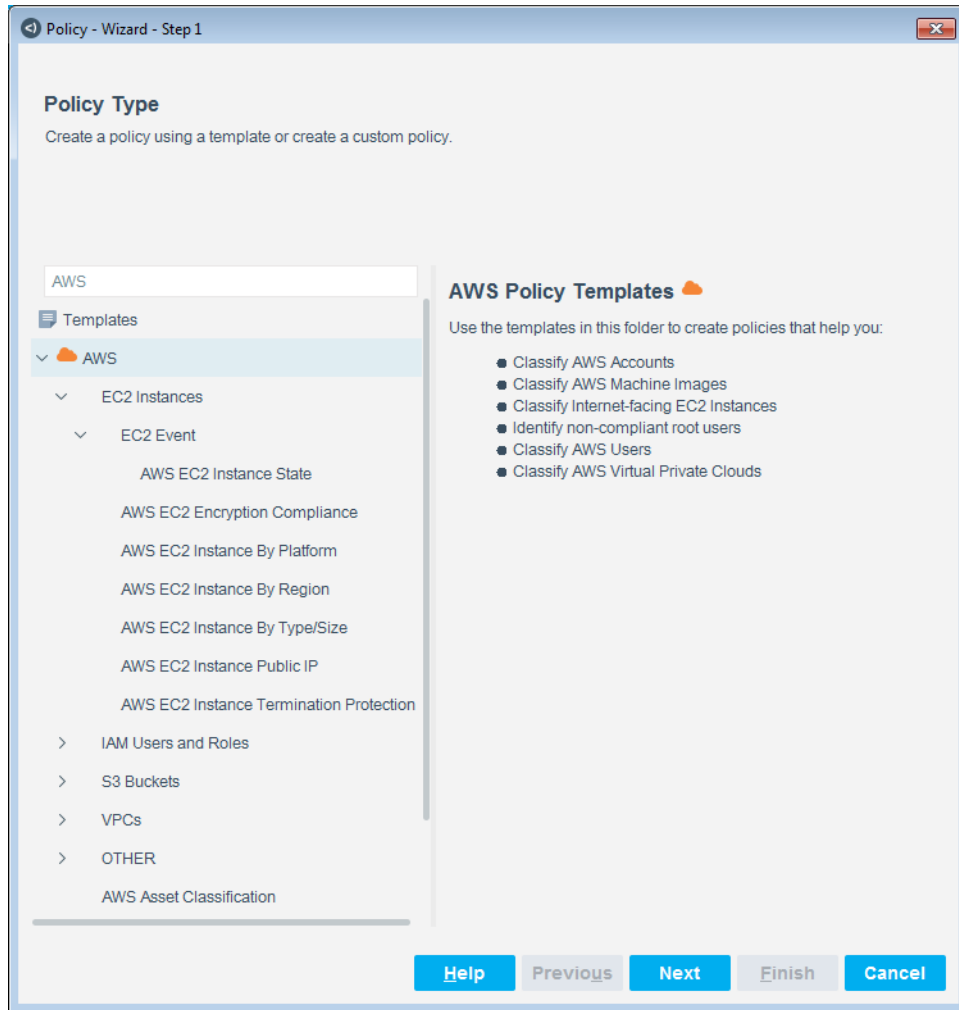
You can use a policy template to create an AWS policy.

To create an AWS policy:

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



2. Select **Add**. The Policy Wizard opens.
3. Select **Templates** and expand the **AWS** folder.



4. The AWS policy templates are organized in folders. Expand the AWS folders to view the policy templates for EC2 Instances, IAM Users and Roles, S3s, VPCs, and OTHER, as well as the policy template for AWS Asset Classification.
5. For details on the folder structure and the available templates, see [AWS Policy Templates](#).
6. Select an AWS policy template and then select **Next**.

Policy - Wizard - Step 2 of 4

Name
Enter a name and description for the policy.

Policy Type
Name
Scope
Sub-Rules

Name: Policy Name
Description:

Help Previous Next Finish Cancel

7. Enter the name of the new policy. Optionally, add a description. Select **Next**.

Policy - Wizard - Step 3 of 4

Scope

NOTE:
AWS Policy Templates for non-EC2 instances do not need an IP segment to be explicitly selected. Hence, "**Hosts without a known IP address**" has been preselected for you.

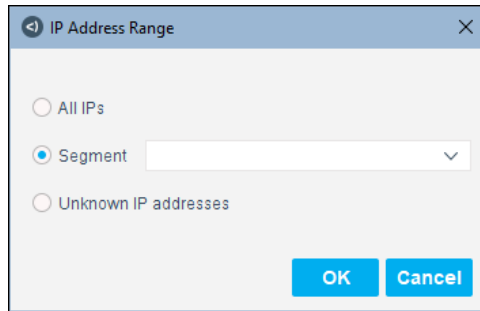
Hosts inspected by the policy

Segment	Ranges
No Name Assigned	Hosts without a known IP address

Add
Remove
Segments

Help Previous Next Finish Cancel

8. AWS policy templates for non-EC2 instances do not need an IP segment to be explicitly selected. Hence, **Hosts without a known IP address** has been preselected in the Scope pane. For EC2 instances, select **Add**. Otherwise, go to Step [12](#).
9. Use the IP Address Range dialog box to define which endpoints are inspected.



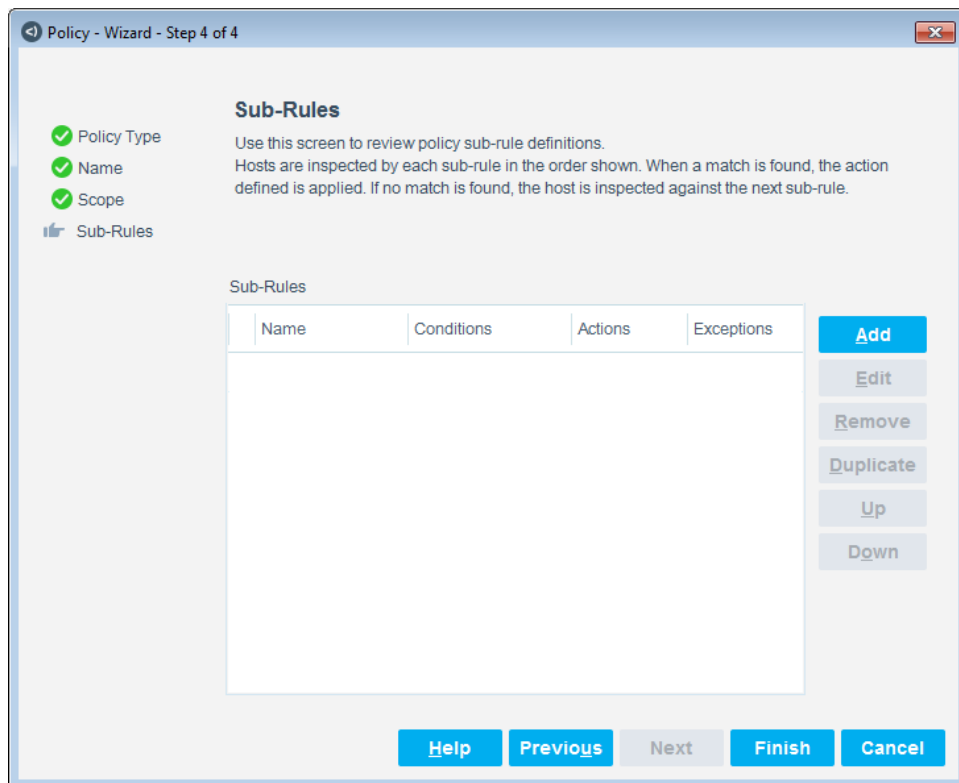
The following options are available:

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

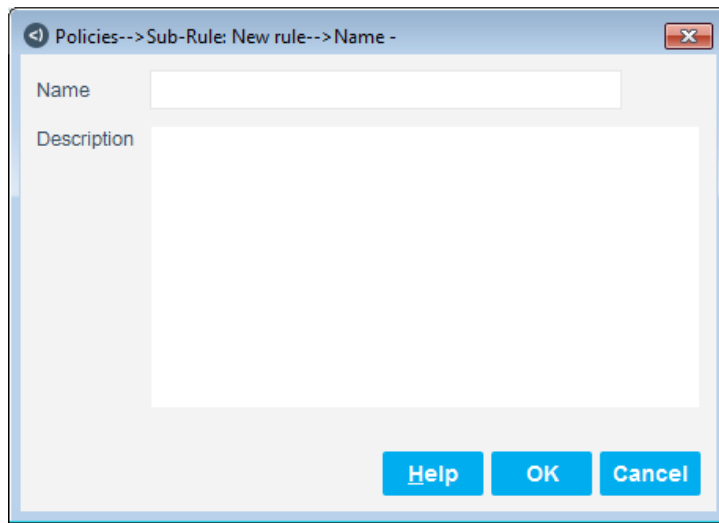
10. In the IP Address Range dialog box, select **OK**.

11. To add other IP address ranges, select **Add** in the Scope pane. For a special case, see [Scope for AWS Asset Classification Template](#).

12. In the Scope pane, select **Next**.



- 13.** Select **Add**. Both the Policies --> Sub-Rule: New rule dialog box and the Policies --> Sub-Rule dialog box open.



- 14.** Enter the name of the new rule. Optionally, add a description.
- 15.** Select **OK**.

Policies-->Sub-Rule: New rule -

Name
 Name: new sub-rule
 Description: None.
 Edit

Condition
 A host matches this rule if it meets the following condition:
 All criteria are True
 Criteria
 No items to display
 Add
 Edit
 Remove

Actions
 Actions are applied to hosts matching the above condition.
 Enable Action Details
 No items to display
 Add
 Edit
 Remove

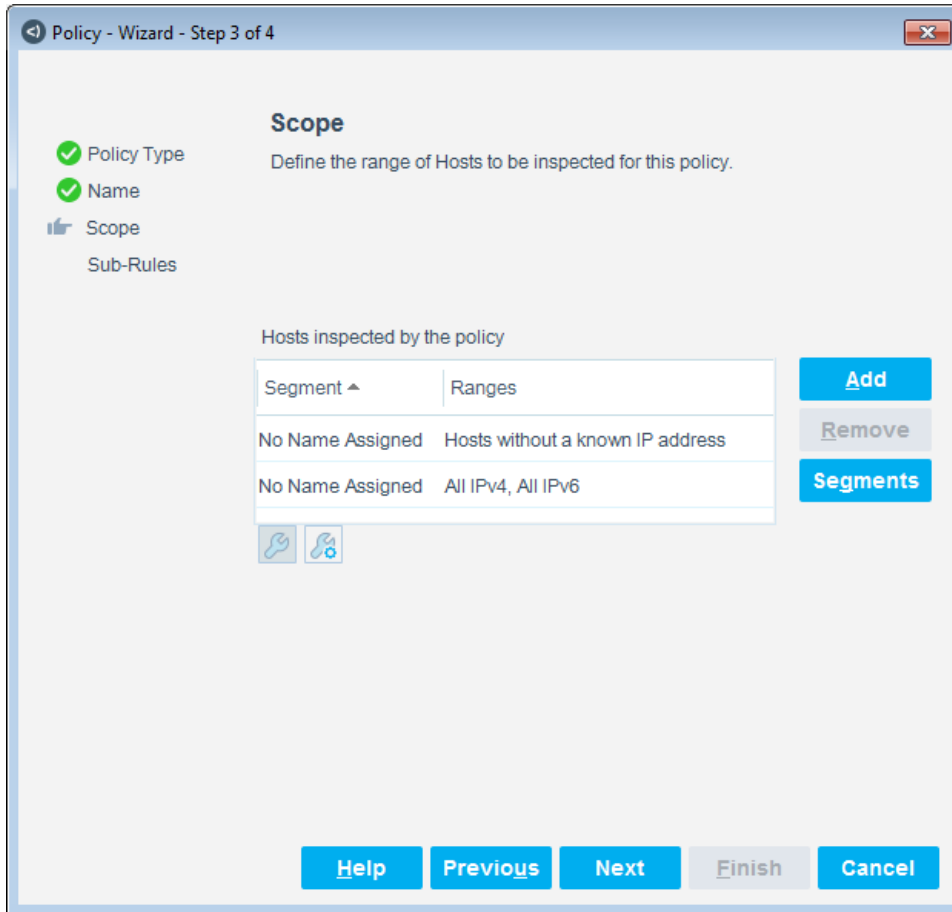
Advanced
 Recheck match: Every 8 hours, All admissions
 Exceptions: None.
 Edit

Help OK Cancel

16. To edit the policy name or condition, select **Edit** in the Name section.
17. To add a condition, select **Add** in the Condition section. See [Detect Cloud Endpoints – Host Properties](#).
18. To add an action, select **Add** in the Actions section. See [Run Policy Actions](#).
19. Select **OK**.
20. In the Sub-Rules pane of the Policy Wizard, select **Finish**.
21. In the Policy Manager, select **Apply**.

Scope for AWS Asset Classification Template

Some AWS entities do not have IP addresses. In order to classify all AWS entities with the AWS Asset Classification policy template, you must select both **Unknown IP addresses** and **All IPs** in the IP Address Range dialog box. To select both, you need to select **Add** in the Scope pane. This configuration is shown in the following figure.



AWS Policy Templates

The AWS policy templates are organized in the following folders:

EC2 Instances	Use the templates in this folder to create policies on EC2 instances. There is a sub-folder called EC2 Event. Use the templates in this folder to create policies on EC2 instance events.
IAM Users and Roles	Use the templates in this folder to create policies on IAM users and roles. There is a sub-folder called IAM Event. Use the templates in this folder to create policies on IAM User and role events.
S3 Buckets	Use the templates in this folder to create policies on S3 buckets.

VPCs	Use the templates in this folder to create policies on VPCs. There is a sub-folder called VPC Event. Use the templates in this folder to create policies on VPC events.
OTHER	Use the templates in this folder to create policies on other AWS resources.
AWS Asset Classification	Use this template to classify all AWS resources.

EC2 Instances Policy Templates

The following EC2 Instances policy templates are available:

EC2 Event > AWS EC2 Instance State	Identify EC2 instances with a specific state.
AWS EC2 Encryption Compliance	Identify whether EC2 instances are encryption-compliant.
AWS EC2 Instance by Platform	Classify EC2 instances by platform. The only platforms are Windows or Non-Windows.
AWS EC2 Instance by Region	Classify EC2 instances by region.
AWS EC2 Instance by Type/Size	Classify EC2 instances by type/size.
AWS EC2 Instance Public IP	Identify EC2 instances with a public IP address.
AWS EC2 Instance Termination Protection	Identify EC2 instances that have Termination Protection enabled.

IAM Users and Roles Policy Templates

The following IAM Users and Roles policy templates are available:

IAM Event > AWS IAM Role Created	Identify when an IAM role is created.
IAM Event > AWS IAM User Created	Identify when an IAM user is created.
AWS IAM Root Password	Identify whether the root account is compliant with the password policy.
AWS IAM User Console Access	Identify whether the IAM user has console access enabled.
AWS IAM User Console Password	Identify whether the IAM user's console access is compliant.
AWS IAM User MFA	Identify whether the IAM user is MFA-compliant.

S3 Buckets Policy Templates

The following S3 buckets policy templates are available:

AWS S3 Access Type	Identify S3 buckets with public access allowed.
AWS S3 Encrypted	Identify S3 buckets that are encrypted.

VPCs Policy Templates

The following VPCs policy templates are available:

VPC Event > AWS VPC State	Identify when a VPC is created or deleted.
AWS VPC ELB	Identify VPCs with ELB configured.
AWS VPC Flowlog	Identify VPCs with Flowlogs configured.
AWS VPC Internet Gateway Compliance	Identify whether VPCs are compliant with respect to Internet Gateways.
AWS VPC Peering Status	Identify VPCs with peering connections.

OTHER Policy Templates

The following OTHER policy template is available:

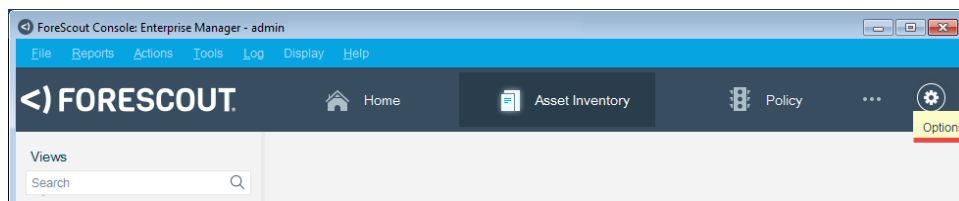
AWS Config Compliance	Identify whether your account/region is AWS Config-compliant.
------------------------------	---

Update the AMI Whitelist

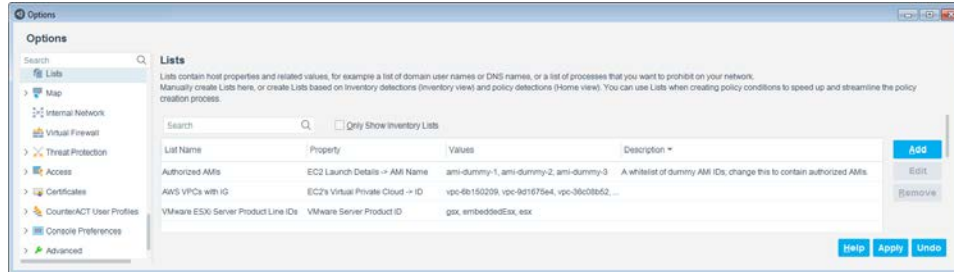
The AMI Whitelist lists the “good” Amazon Machine Images (AMIs).

To update the AMI whitelist:

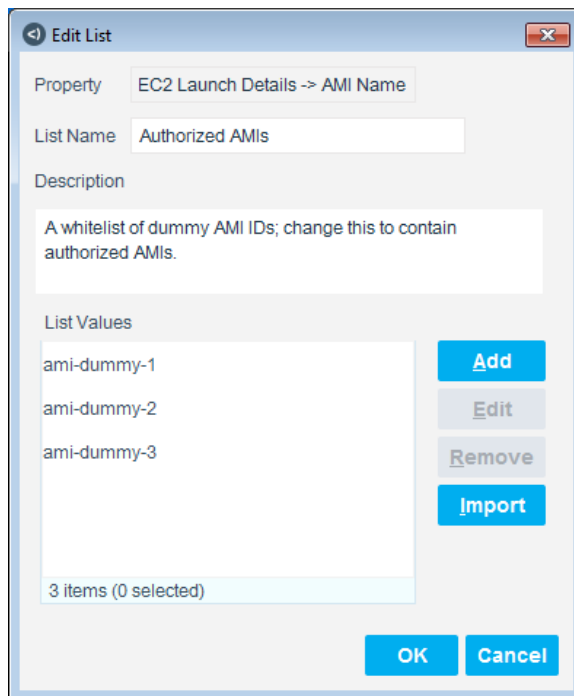
1. Log in to the Console and select **Options** from the **Tools** menu.



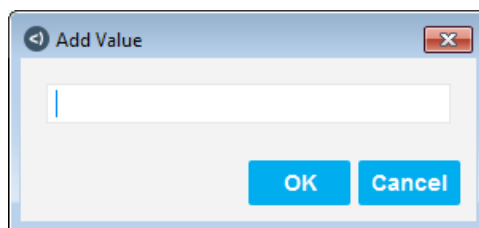
2. In the left pane, select **Lists**. The AMIs are listed in the Lists pane.



3. Select an item and select **Edit**.



4. To add values to the list, select **Add**.



5. Paste the AMI Name from the AWS online portal into the field, for example, ami-b70554c8, and select **OK**.
6. Copy and paste additional AMIs from the AWS online portal into the Edit List dialog box (if applicable).
7. Select **OK** in the Edit List dialog box.
8. Select **Apply** in the Lists pane.

Detect Cloud Endpoints – Host Properties

There are many AWS-specific host properties available. These properties are displayed in the Condition dialog box, which is accessed through the policy templates. In the Console, some properties are also visible in the profile section within the Home tab.

Host properties are organized into the following groups:

- [AWS Properties](#)
- [AWS EC2 Properties](#)
- [AWS IAM Role Properties](#)
- [AWS IAM User Properties](#)
- [AWS S3 Properties](#)
- [AWS Service Properties](#)
- [AWS VPC Properties](#)

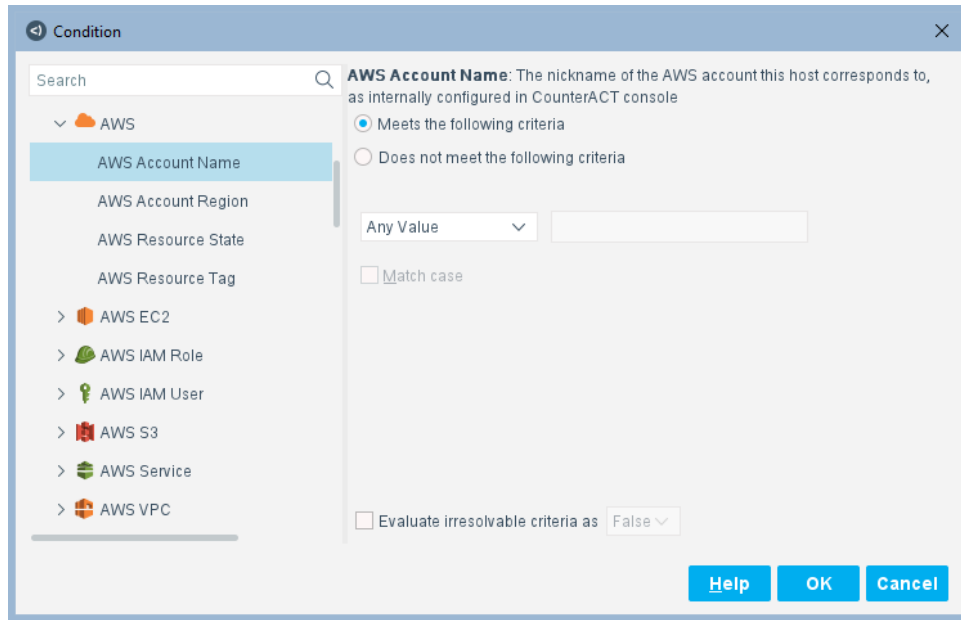
For more information about setting conditions, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

AWS Properties

The AWS properties are common properties, such as Account Name, that are added to EC2, IAM, or VPC hosts.

To access the AWS properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS folder.



The following properties are available:

AWS Account Name	Indicates the nickname of the AWS account to which this host corresponds, as internally configured in the Console.
AWS Account Region	Indicates the region of the AWS account.
AWS Resource State	Indicates the most recently reported state of the AWS Resource, such as Active or Deleted.
AWS Resource Tag	Indicates an internal tag to differentiate between EC2/IAM and VPC hosts.

AWS EC2 Properties

This section describes the AWS EC2 properties for EC2 instances over and above an instance's MAC and IP addresses.

If an EC2 instance has been configured with an IPv6 address, it can be displayed in the All Hosts pane.

To access the AWS EC2 properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS EC2 folder.

The screenshot shows the 'Condition' dialog in the AWS CloudFormation console. The left sidebar lists various AWS EC2 properties, with 'EC2 Attached Block Devices' selected. The main panel displays the configuration for this property, which is described as 'Elastic Block Storage volumes attached to this EC2 instance.' The configuration includes several criteria that can be checked or unchecked, each with a 'Meets the following criteria' or 'Does not meet the following criteria' radio button. The criteria are: 'Is root device', 'Device ID', 'Encrypted', 'KMS Key ID', and 'Size (GB)'. Each criterion has a text input field for specifying values. At the bottom, there are checkboxes for 'Evaluate irresolvable criteria as' and 'Evaluate empty list value as', both set to 'False'. The dialog has 'Help', 'OK', and 'Cancel' buttons at the bottom right.

The following properties are available:

EC2 Attached Block Devices	<p>Indicates the Elastic Block Storage (EBS) volumes attached to this EC2 instance.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Is root device: Is the Attached Block Device a root device? Device ID: The Device ID of the Attached Block Device. Encrypted: Is the Attached Block Device encrypted? KMS Key ID: The Key Management Server (KMS) key ID used to perform encryption. Size (GB): The size of the Attached Block Device. Device Type: The device type of the Attached Block Device.
EC2 AMI Launch Index	<p>Indicates the order in which the EC2 instance was launched. The first or only instance has an index value of 0.</p>
EC2 Dedicated Tenancy	<p>Indicates that the instance runs on single-tenant, dedicated hardware.</p>

EC2 Elastic Network Interfaces	<p>Indicates the Elastic Network Interfaces (ENIs) of the EC2 instance.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Local Interface Name: The local interface name, such as eth0 or eth1. Private IP Address: The private IP address of the ENI. Private DNS: The private DNS of the ENI. MAC Address: The MAC address of the ENI. Elastic IP Address: The elastic IP address of the ENI. Source/destination check: The source/destination check of the ENI. Description: The description of the ENI. Security Group: The security group of the ENI.
EC2 IAM Role	Indicates the Identity and Access Management (IAM) role associated with this EC2 instance.
EC2 Instance ID	Indicates the EC2 instance ID of the endpoint.
EC2 Internet Gateway Information	<p>Provides information about the Internet gateways on this EC2 instance's VPC.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Internet Gateway ID: The stable and unique string identifying the Internet Gateway. Internet Gate Name: The friendly name identifying the Internet Gateway. Egress Gateway: The Internet Gateway as either egress or ingress.
EC2 Kernel ID	Indicates the operating system kernel associated with the AMI.
EC2 Key Pair Name	Indicates the key pair required for logging in to the instance securely.
EC2 Launch Details	<p>Indicates the launch details of the EC2 instance.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> AMI ID: The full Amazon Image ID used to create the EC2 instance. AMI Name: The Amazon Image name used to create the EC2 instance. Launch Time: The time when this EC2 instance was launched.
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 when the bid price is higher than the Spot Price. If the Spot Price goes over the bid price, it may be terminated.
EC2 Location	<p>Provides location information of the AWS EC2 endpoint.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> Location: The region in which the AWS endpoint is located, such as us-west-1. Availability Zone: The availability zone of the endpoint, such as us-west-1b.

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 Instance Name	Indicates the EC2 instance name of the endpoint.
EC2 AMI Owner	Indicates the AWS account number belonging to the owner of the Amazon Machine Image (AMI) used for this EC2 instance.
EC2 Placement Group	Indicates the cluster group to which this instance belongs, if it is a cluster instance.
EC2 Platform	Indicates the platform of the EC2 instance, such as Windows or Non-Windows.
EC2 Public DNS	Indicates the public hostname of the EC2 instance, which resolves to the public IP address or Elastic IP address of the instance.
EC2 Public IP	Indicates the public IP address of the EC2 instance.
EC2 RAM disk ID	Indicates the RAM disk associated with the image, if a specific one was selected.
EC2 Secondary Private IP	Indicates the secondary private IP addresses assigned to a network interface attached to this EC2 instance.
EC2 Security Group	Indicates the security groups to which the EC2 instance belongs. The following sub-properties are available: <ul style="list-style-type: none"> ▪ Given Name: The user-defined name of the security group. ▪ Group Name: The AWS-supplied security group name. ▪ ID: The AWS-supplied security group ID. ▪ Description: The user-defined description of the security group. ▪ Associated VPC ID: The Virtual Private Cloud to which this security group belongs.
EC2 State	Indicates the most recent power state of the EC2 instance, such as Pending, Running, Stopped, Stopping, or Terminated. This value may be influenced by the Query Interval configured for the Forescout platform's connection to AWS.
EC2 Subnet	Indicates the AWS subnet into which the EC2 instance was launched. The following sub-properties are available: <ul style="list-style-type: none"> ▪ EC2 Subnet ID: The AWS ID of the subnet into which the EC2 instance was launched. ▪ EC2 Subnet Name: The name of the subnet into which the EC2 instance was launched. ▪ EC2 Subnet CIDR: The CIDR block of the subnet into which the EC2 instance was launched. ▪ EC2 Subnet IPv6 CIDR: The IPv6 CIDR block of the subnet into which the EC2 instance was launched.

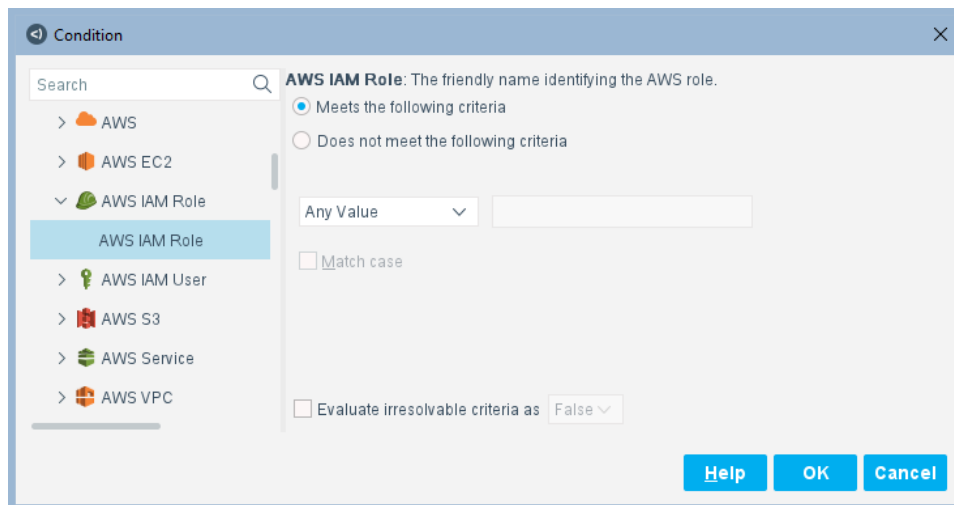
EC2 Tags	Indicates the tags given to the EC2 instance. The following sub-properties are available: <ul style="list-style-type: none"> Tag Name: The name of the tag. Note: Do not use the value "Name" as the Tag Name. Tag Value: The value of the tag.
EC2 Termination Protection	Indicates whether termination protection is enabled. When protection is enabled, this EC2 instance cannot be terminated using the console, API, or CLI.
EC2 Instance Type	Indicates the type of EC2 instance by CPU capacity, memory, and storage. For example, m1.small, c1.xlarge.
EC2's Virtual Private Cloud	Indicates the Virtual Private Cloud (VPC) into which the EC2 instance was launched. The following sub-properties are available: <ul style="list-style-type: none"> VPC Name: The VPC name. ID: The VPC ID.
EC2 CloudWatch Monitoring	Indicates the level of CloudWatch monitoring that is enabled for this instance, such as Basic or Detailed.

AWS IAM Role Properties

This section describes the AWS IAM Role properties.

To access the AWS IAM Role properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS IAM Role folder.



The following property is available:

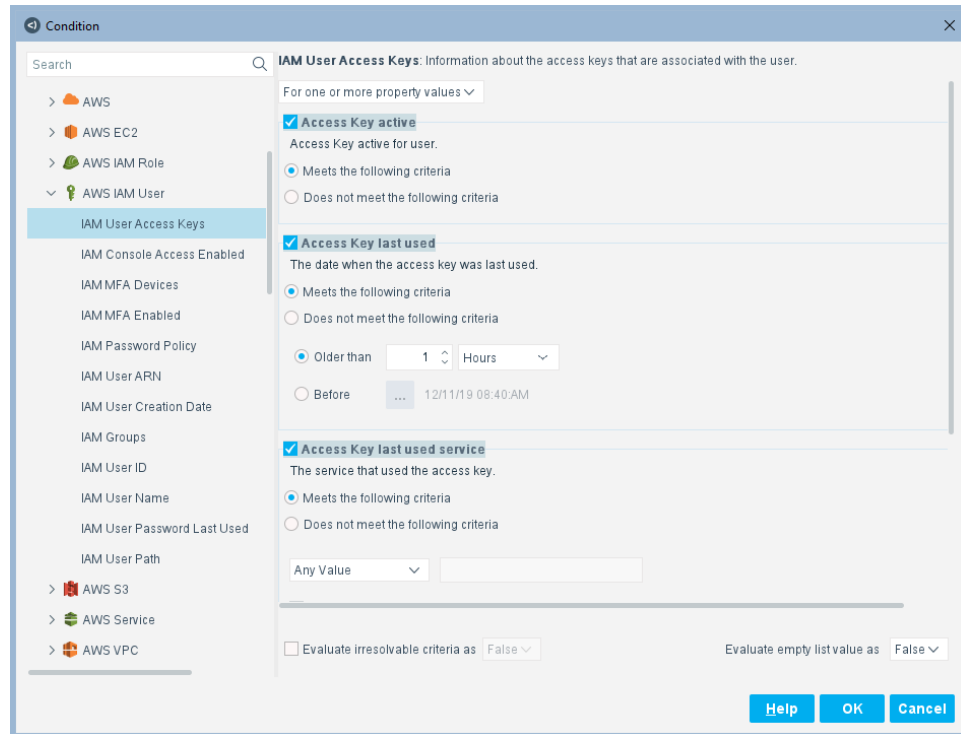
AWS IAM Role	Indicates the friendly name that identifies the AWS role.
---------------------	---

AWS IAM User Properties

This section describes the AWS IAM User properties.

To access the AWS IAM User properties:

1. When configuring policies, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS IAM User folder.



The following properties are available:

IAM User Access Keys	<p>Provides information about the access keys that are associated with the user.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Access Key active: The active access key for the user. ▪ Access Key last used: The date the access key was last used. ▪ Access Key last used service: The service that last used the access key. ▪ Access Key last used region: The region in which the access key was last used.
IAM Console Access Enabled	Indicates whether Console access is enabled for the user.

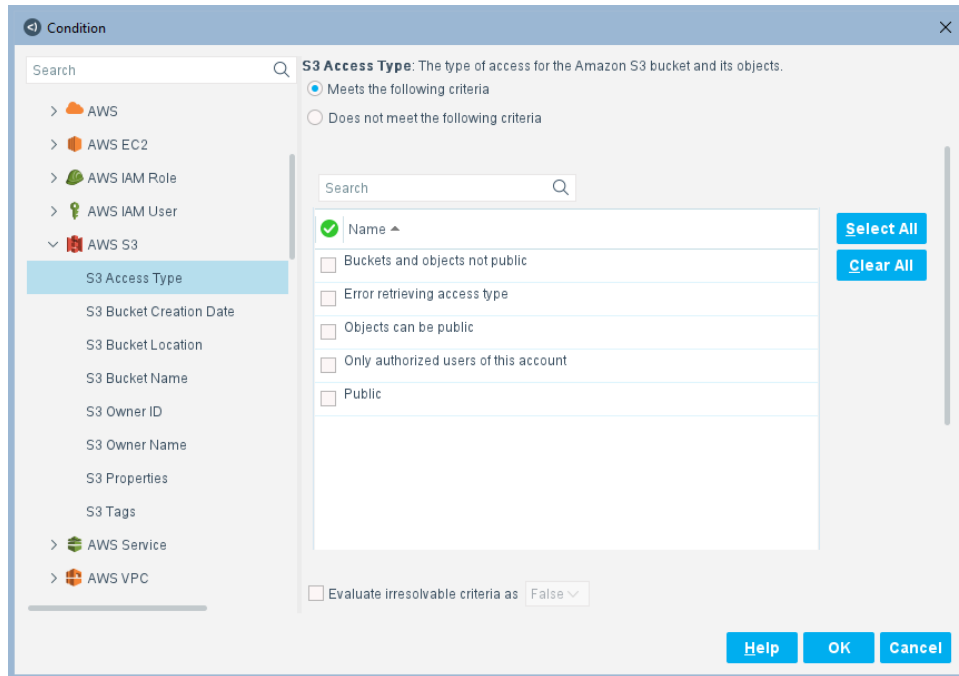
IAM MFA Devices	<p>Provides information about the MFA devices.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ MFA Serial Number: The serial numbers that uniquely identify the MFA devices. ▪ MFA Enable Date: The date in which the MFA device was enabled for the user.
IAM MFA Enabled	<p>Indicates whether Multi-Factor Authentication (MFA) is enabled for the user.</p>
IAM Password Policy	<p>Provides information about the account password policy.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Allow Users to Change Password: Whether IAM users are allowed to change their own password. ▪ Expire Passwords: Whether passwords in the account expire. ▪ Hard Expiry: Whether IAM users are prevented from setting a new password after their password has expired. ▪ Max Password Age: The number of days for which an IAM user password is valid. ▪ Minimum Password Length: The minimum length required for IAM user passwords. ▪ Password Reuse Prevention: The number of previous passwords that IAM users are prevented from re-using. ▪ Require Lowercase Characters: Whether to require lowercase characters for IAM user passwords. ▪ Require Numbers: Whether to require numbers for IAM user passwords. ▪ Require Symbols: Whether to require symbols for IAM user passwords. ▪ Require Uppercase Characters: Whether to require uppercase characters for IAM user passwords.
IAM User ARN	<p>Indicates the Amazon Resource Name (ARN) that identifies the user.</p>
IAM User Creation Date	<p>Indicates the date and time the user was created.</p>
IAM Groups	<p>Provides information about the groups to which the user belongs.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Group Name: The name of the group. ▪ Group ID: The ID of the group. ▪ Group Path: The path of the group. ▪ Group ARN: The ARN of the group. ▪ Group Creation Date: The date when the group was created.
IAM User ID	<p>Indicates the stable and unique string that identifies the user.</p>
IAM User Name	<p>Indicates the friendly name that identifies the user.</p>
IAM User Password Last Used	<p>Indicates the date and time the password was last used to sign in to an AWS website.</p>
IAM User Path	<p>Indicates the path to the user.</p>

AWS S3 Properties

This section describes the AWS S3 properties.

To access the AWS S3 properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS S3 folder.



The following properties are available:

S3 Access Type	<p>Indicates the type of access for the Amazon S3 bucket and its objects:</p> <ul style="list-style-type: none"> ▪ Buckets and objects not public: Both bucket- and object-level access are not public (specific users can be granted access to read and write to both buckets and the objects within them) ▪ Error retrieving access type: Received an error retrieving the access type ▪ Objects can be public: Objects within this bucket are public (specific users can be given access to the objects within buckets) ▪ Only authorized users of this account: Only authorized users of this account have access ▪ Public: Both buckets and the objects within them are public to everyone
S3 Bucket Creation Date	Indicates the date and time when the S3 bucket was created.
S3 Bucket Location	Indicates the location of the specified Amazon S3 bucket.

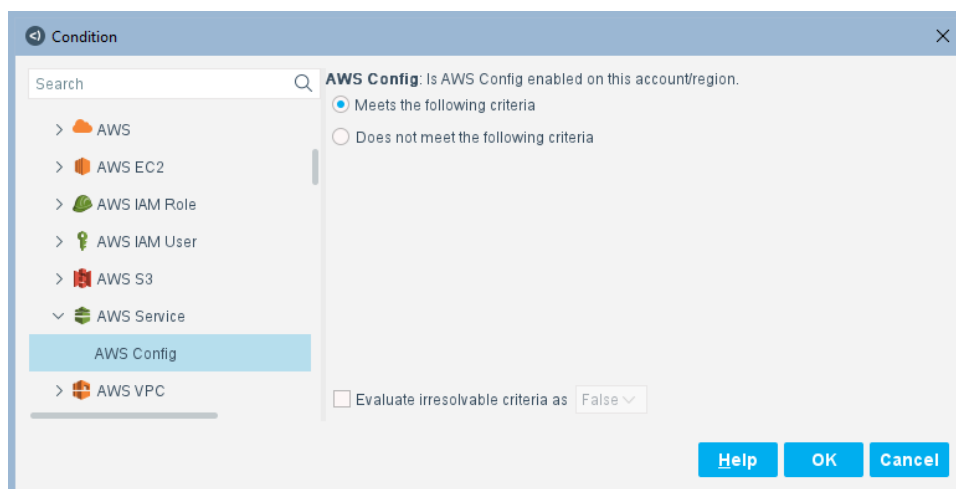
S3 Bucket Name	Indicates the DNS-compliant bucket name.
S3 Owner ID	Indicates the ID that identifies the S3 bucket owner.
S3 Owner Name	Indicates the name of the S3 bucket owner.
S3 Properties	<p>Indicates the S3 bucket properties.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Encrypted: Is S3 bucket encrypted? ▪ KMS Master Key ID: The ID of the KMS managed key used to encrypt S3 bucket objects. ▪ SSE Algorithm Used: The Server-Side Encryption (SSE) algorithm used for default encryption. The types of encryption are AWS:AES-256 and AWS:KMS. ▪ Object Locking Status: The status of the lock on objects within this S3 bucket.
S3 Tags	<p>Indicates the tags given to the S3 bucket.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Tag Name: The name of the tag. Note: Do not use the value "Name" as the Tag Name. ▪ Tag Value: The value of the tag.

AWS Service Properties

This section describes the AWS Service properties.

To access the AWS Service properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS Service folder.



The following property is available:

AWS Config	Indicates whether AWS Config is enabled on this account/region.
-------------------	---

AWS VPC Properties

This section describes the AWS VPC properties.

To access the AWS VPC properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the AWS VPC folder.

The screenshot shows a 'Condition' dialog box with a search bar and a list of AWS services on the left. The 'AWS VPC' folder is expanded, showing various VPC properties. The 'Peering Connection' property is selected. The right pane shows the configuration for 'Peering Connection ID' and 'Peering Connection Name'. Both are set to 'Meets the following criteria' with a value of 'Any Value'. The 'Match case' checkbox is unchecked. At the bottom, there are buttons for 'Help', 'OK', and 'Cancel'.

Condition

Search

- > AWS
- > AWS EC2
- > AWS IAM Role
- > AWS IAM User
- > AWS S3
- > AWS Service
- ▼ AWS VPC
 - Peering Connection
 - VPC ID
 - VPC Internet Gateway Information
 - VPC Load Balancer Information
 - VPC Name
 - VPC Network ACL
 - VPC Route Tables
 - VPC Subnet Information

Peering Connection: Information about the VPC peering connection

For one or more property values

☒ **Peering Connection ID**
The id of the peering connection

☒ Meets the following criteria
☐ Does not meet the following criteria

Any Value

☐ Match case

☒ **Peering Connection Name**
The name of the peering connection

☒ Meets the following criteria
☐ Does not meet the following criteria

Any Value

☐ Evaluate irresolvable criteria as False Evaluate empty list value as False

Help OK Cancel

The following properties are available:

Peering Connection	<p>Provides information about the VPC peering connection.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Peering Connection ID: The ID of the peering connection. ▪ Peering Connection Name: The name of the peering connection. ▪ Peering Connection Status: The status of the peering connection. ▪ Peering Connection Requester Region: The region of the peering connection requester. ▪ Peering Connection Requester VPC ID: The VPC ID of the peering connection requester. ▪ Peering Connection Requester VPC Name: The VPC Name of the peering connection requester. ▪ Peering Connection Acceptor Region: The region of the peering connection acceptor. ▪ Peering Connection Acceptor VPC ID: The VPC ID of the peering connection acceptor. ▪ Peering Connection Acceptor VPC Name: The VPC Name of the peering connection acceptor.
VPC Flowlog Enabled	Indicates whether VPC flowlog is enabled.
VPC ID	Indicates the stable and unique string that identifies the VPC.
VPC Internet Gateway Information	<p>Provides information about Internet gateways on this VPC.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Internet Gateway ID: The stable and unique string identifying the Internet Gateway. ▪ Internet Gate Name: The friendly name identifying the Internet Gateway. ▪ Internet Gate State: The Internet Gateway state. ▪ Egress Gateway: The Internet Gateway as either egress or ingress.
VPC Load Balancer Information	<p>Provides information about load balancers on this VPC.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Load Balancer Scheme: The scheme of the load balancer. ▪ Load Balancer Type: The type of the load balancer. ▪ Load Balancer Name: The name of the load balancer.
VPC Name	Indicates the friendly name that identifies the VPC.
VPC Network ACL	Indicates the VPC network ACL.
VPC Route Tables	Provides information about route tables on this VPC.
VPC Subnet Information	<p>Provides information about subnets on this VPC.</p> <p>The following sub-properties are available:</p> <ul style="list-style-type: none"> ▪ Subnet Name: The friendly name identifying the VPC subnet. ▪ Subnet IPv4 CIDR: The IPv4 CIDR of the VPC subnet. ▪ Subnet IPv6 CIDR: The IPv6 CIDR of the VPC subnet.

Manage 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 Console. This provides activity information, accurate at the time of the poll, on cloud endpoints based on certain instance 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

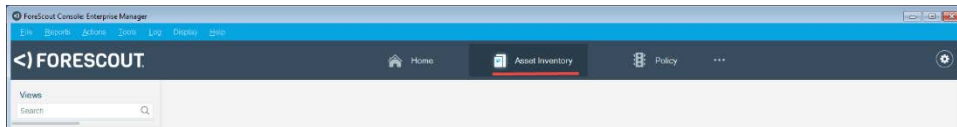
Refer to *Working with Asset Inventory Detections* in the *Forescout Administration Guide* or the Online Help for information about how to work with the Asset Inventory. See [Additional Forescout Documentation](#) for information on how to access this guide.

Access AWS IAM Role Inventory

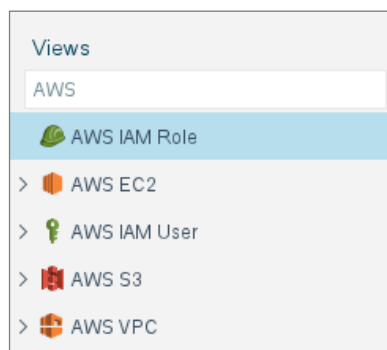
Use the AWS IAM Role inventory to view IAM role-related summary and detailed information.

To access the AWS IAM Role inventory:

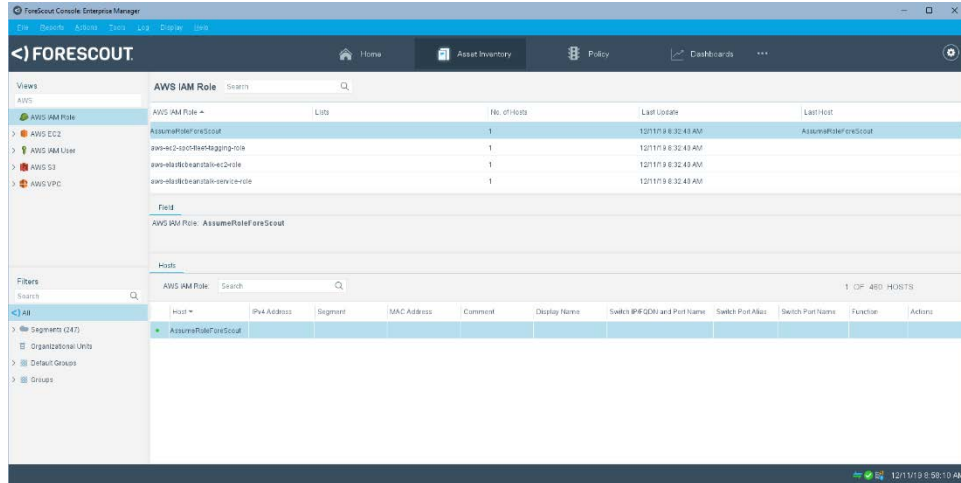
1. Log in to the Console and select **Asset Inventory**.



2. In the Views pane, select **AWS IAM Role**.



The AWS IAM Role information is displayed.



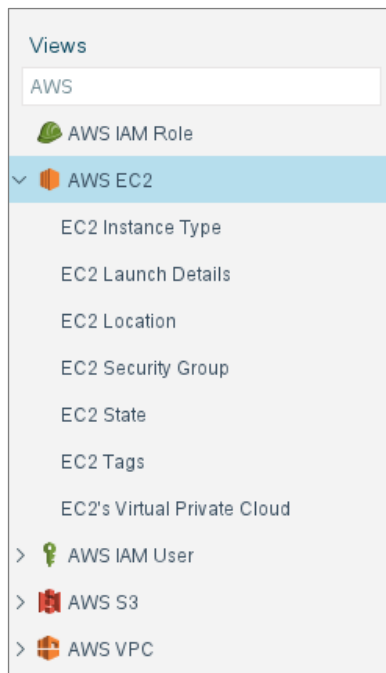
3. To view details, select a specific AWS IAM Role.

Access AWS EC2 Inventory

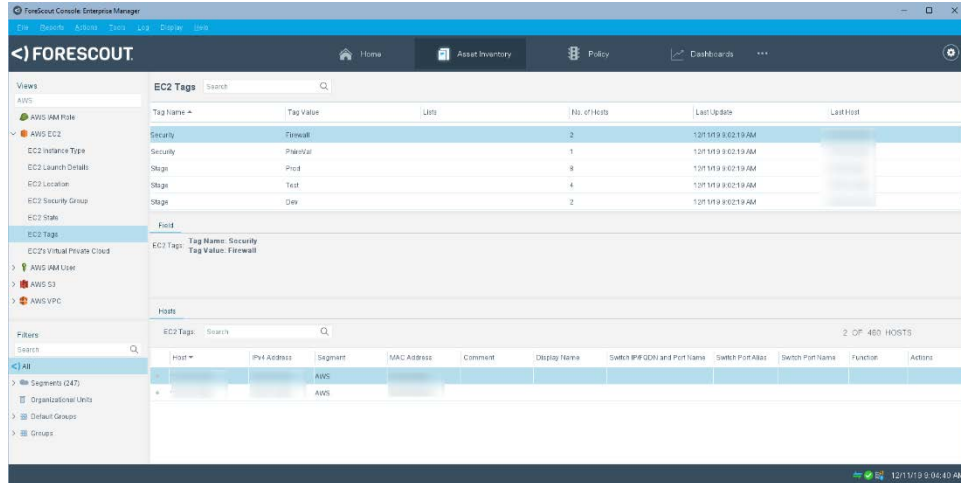
Use the AWS EC2 inventory to view EC2-related summary and detailed information.

To access the AWS EC2 inventory:

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



3. Select an AWS EC2 item, for example, EC2 Tags, to view the real-time inventory information. For details, select a specific AWS EC2.



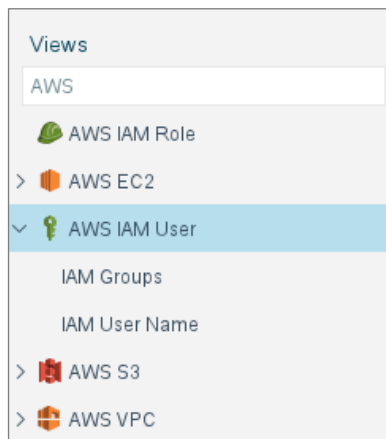
4. To view more inventory information, select another AWS EC2 item, for example, EC2 Instance Type, EC2 Launch Details, EC2 Location, EC2 Security Group, EC2 State, or EC2's Virtual Private Cloud.

Access AWS IAM User Inventory

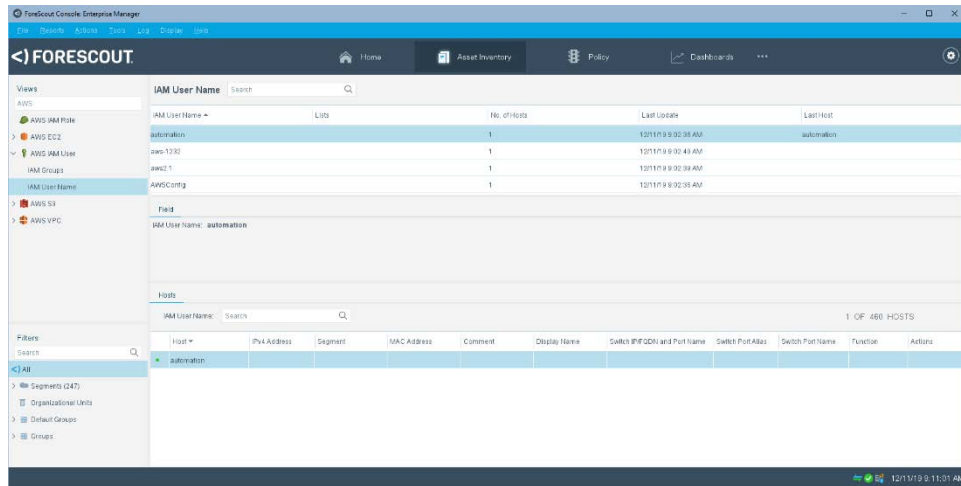
Use the AWS IAM User inventory to view IAM user-related summary and detailed information.

To access the AWS IAM User inventory:

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



3. Select an AWS IAM User item, for example, IAM User Name, to view the real-time inventory information. For details, select a specific IAM User Name.



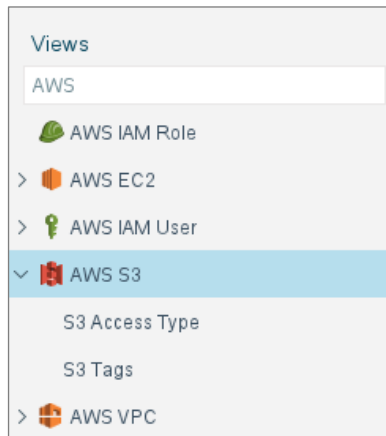
4. To view more inventory information, select another AWS IAM item, for example, IAM Groups.

Access AWS S3 Inventory

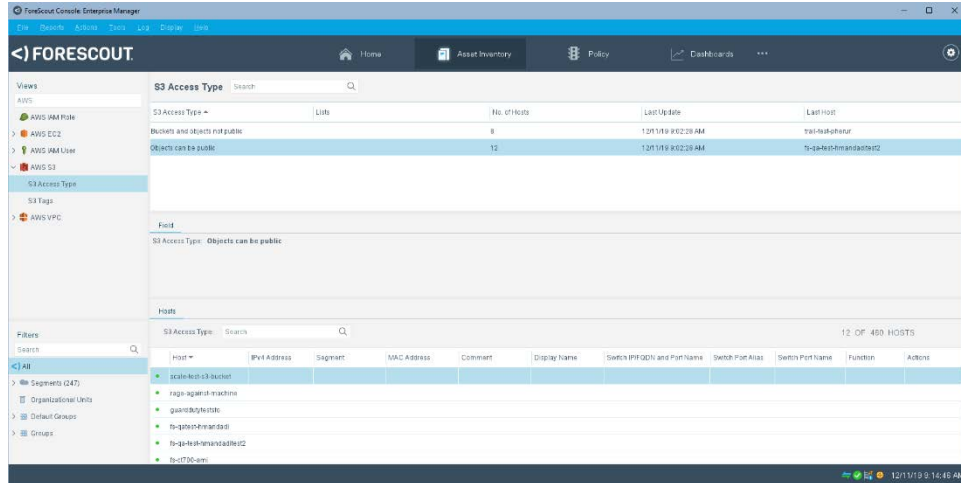
Use the AWS S3 inventory to view S3-related information.

To access the AWS S3 inventory:

1. Log in to the Console and select **Asset Inventory**.
2. In the Views pane, expand the **AWS S3** folder.



3. Select an AWS S3 item, for example, S3 Access Type, to view the real-time inventory information. For details, select a specific S3 Access Type.



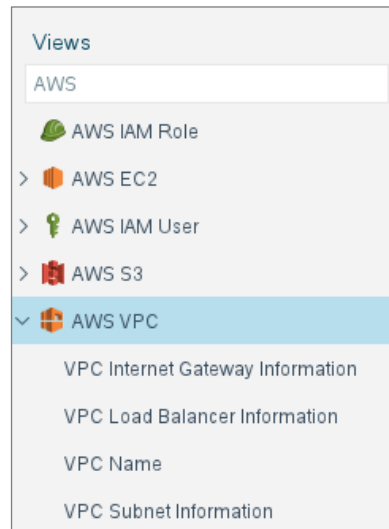
4. To view more inventory information, select another AWS S3 item, for example, S3 Tags.

Access AWS VPC Inventory

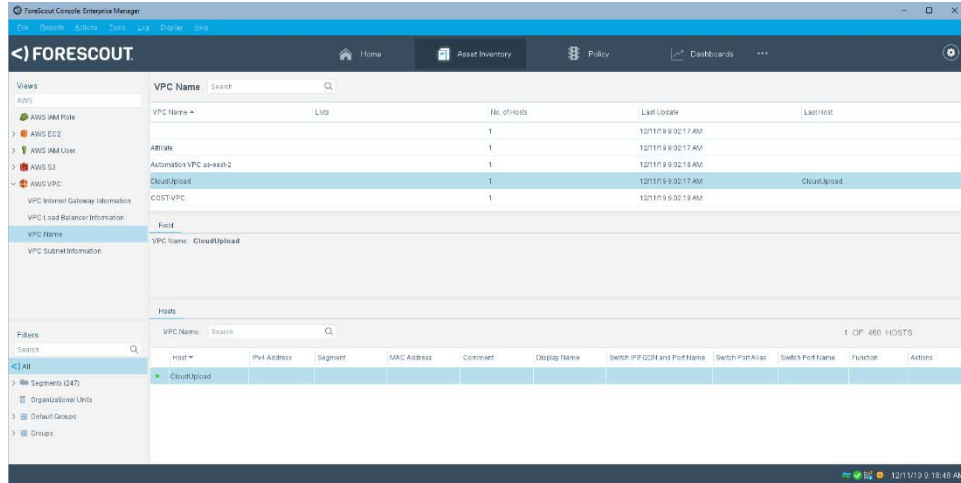
Use the AWS VPC inventory to view VPC-related summary and detailed information.

To access the AWS VPC inventory:

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



3. Select an AWS VPC item, for example, VPC Name, to view the real-time inventory information. For details, select a specific VPC Name.



4. To view more inventory information, select another AWS VPC item, for example, VPC Internet Gateway Information, VPC Load Balancer Information, or VPC Subnet Information.

Run Policy Actions

Policy actions are organized into the following groups:

- [Manually Run AWS Actions on EC2 Instance](#)
- [Manually Run AWS IAM Actions](#)
- [Manually Run AWS S3 Actions](#)
- [Manually Run AWS VPC Actions](#)

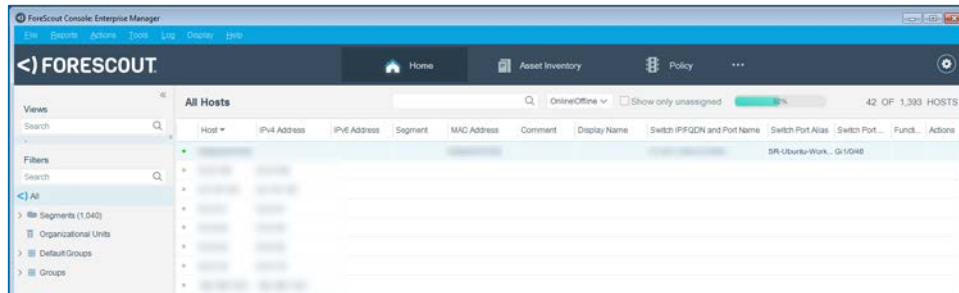
If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl license to use these actions. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing licenses.

Manually Run AWS Actions on EC2 Instance

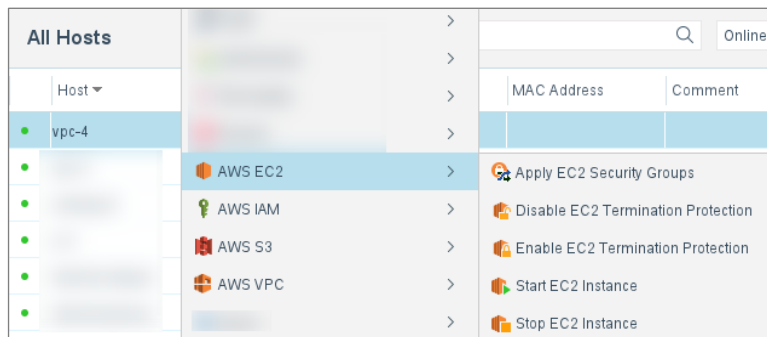
Use the actions described in this section for visibility and control of AWS. While AWS EC2 actions can be launched as part of a policy, you can also manually run an action.

To manually run an AWS EC2 action:

1. Log in to the Console, select **Home**, and select **All Hosts**.



2. In the All Hosts pane, select a host entry.
3. Right-click an endpoint, select **AWS EC2**, and select an action.



4. For details on the AWS EC2 actions, see:
 - [Apply EC2 Security Groups Action](#)
 - [Disable EC2 Termination Protection Action](#)
 - [Enable EC2 Termination Protection Action](#)
 - [Start EC2 Instance Action](#)
 - [Stop EC2 Instance Action](#)

Apply EC2 Security Groups Action

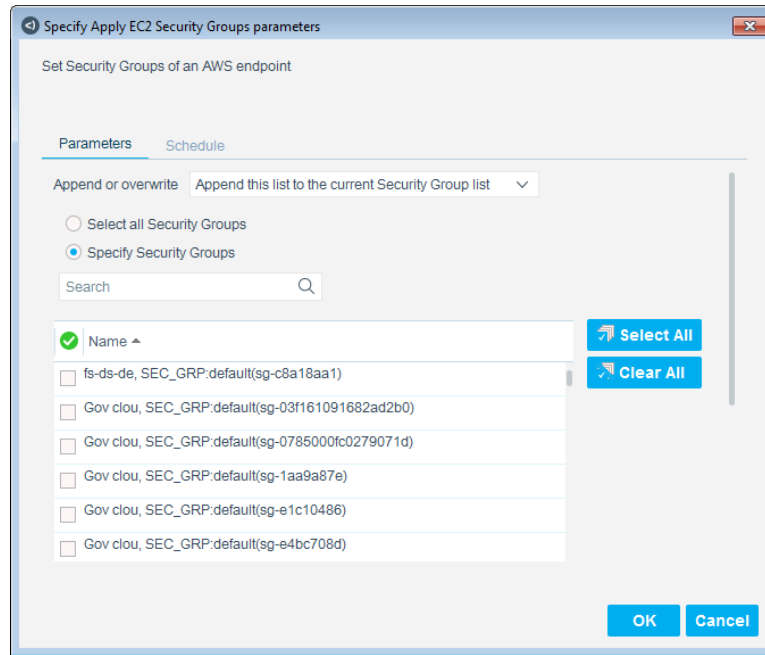
Use this action to set security groups for an AWS endpoint.

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, which specify the kind of connections, such as the IP addresses, ports, or protocols that are allowed. These rules are defined in the AWS console.

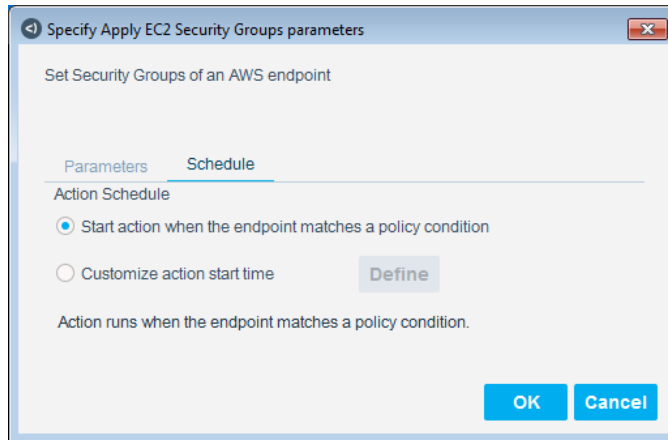
When a security group action is applied to a cloud instance, that instance is allowed to send/receive traffic based on the security group's rules.

To run the Apply EC2 Security Groups action:

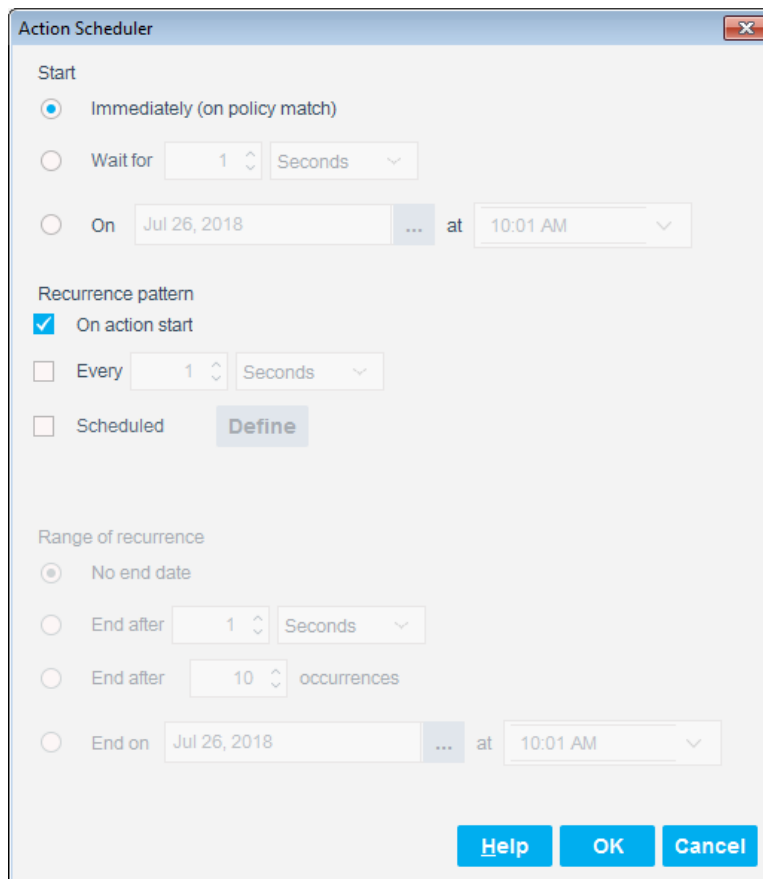
1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Apply EC2 Security Groups**.



3. In the Append or overwrite field, select one of the following:
 - **Append this list to the current Security Group list**, which adds the selected security groups to the current Security Group list.
 - **Overwrite the current Security Group list with this list**, which replaces the current Security Group list with the list you selected. This option is useful for isolating a non-compliant endpoint by applying it only with restrictive security groups.
4. To select all security groups, select **Select all Security Groups** or select **Specify Security Groups** and select one or more security groups in the table.
 - To select all security groups, select **Select All**.
 - To clear all security groups, select **Clear All**.
 - To filter the security groups, enter text in the **Search** field to match security group names.
5. Select **OK** or select the Schedule tab to schedule the action.



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



7. Set the schedule parameters and select **OK**.
8. In the Specify Apply EC2 Security Groups parameters dialog box, select **OK**.

Disable EC2 Termination Protection Action

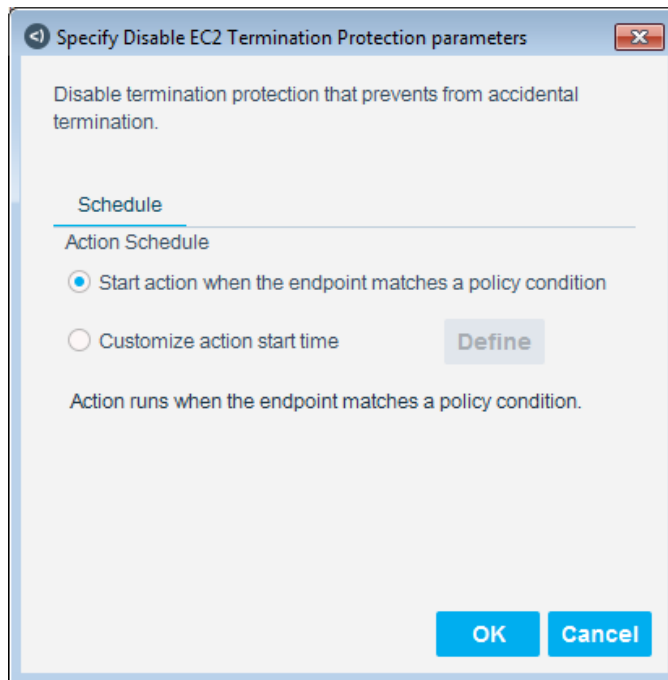
Use this action to remove (disable) termination protection from an EC2 instance.

If termination protection is disabled, EC2 instances can be terminated through the AWS Console, API, or CLI.

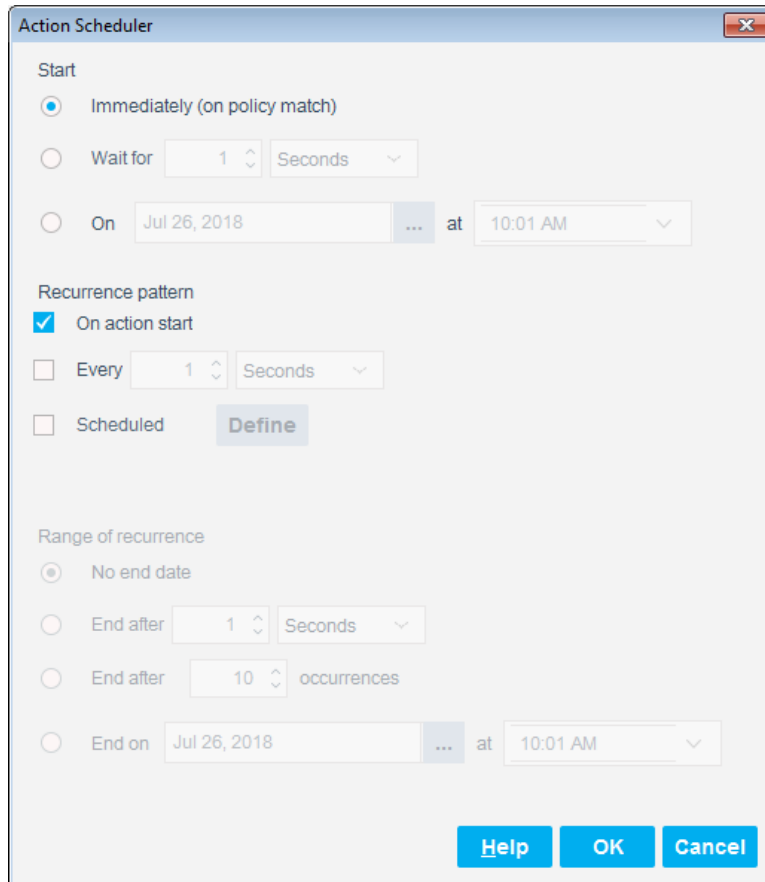
Enabling termination protection prevents accidental termination of EC2 instances.

To run the Disable EC2 Termination Protection action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Disable EC2 Termination Protection**.



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

The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). There is also an 'End on' option with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

4. Set the schedule parameters and select **OK**.
5. In the Specify Disable EC2 Termination Protection parameters dialog box, select **OK**.

Enable EC2 Termination Protection Action

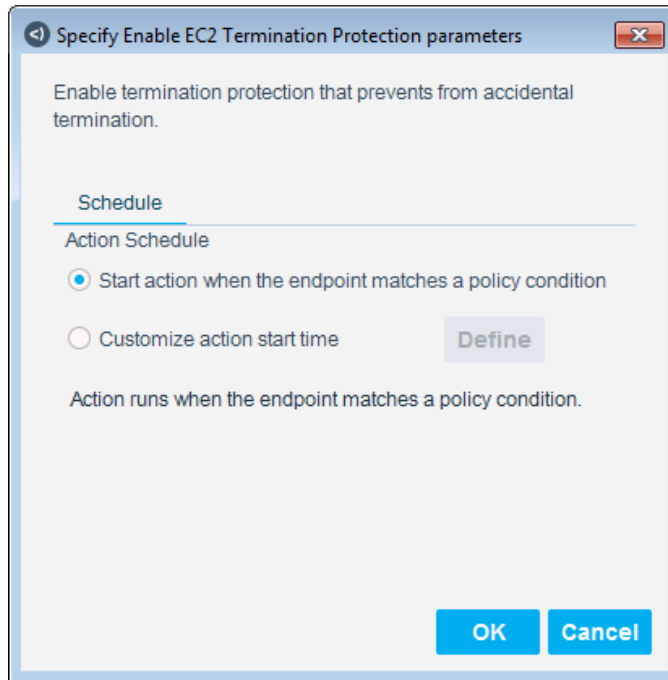
Use this action to apply (enable) termination protection for an EC2 instance. Enabling termination protection prevents accidental termination of EC2 instances.

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

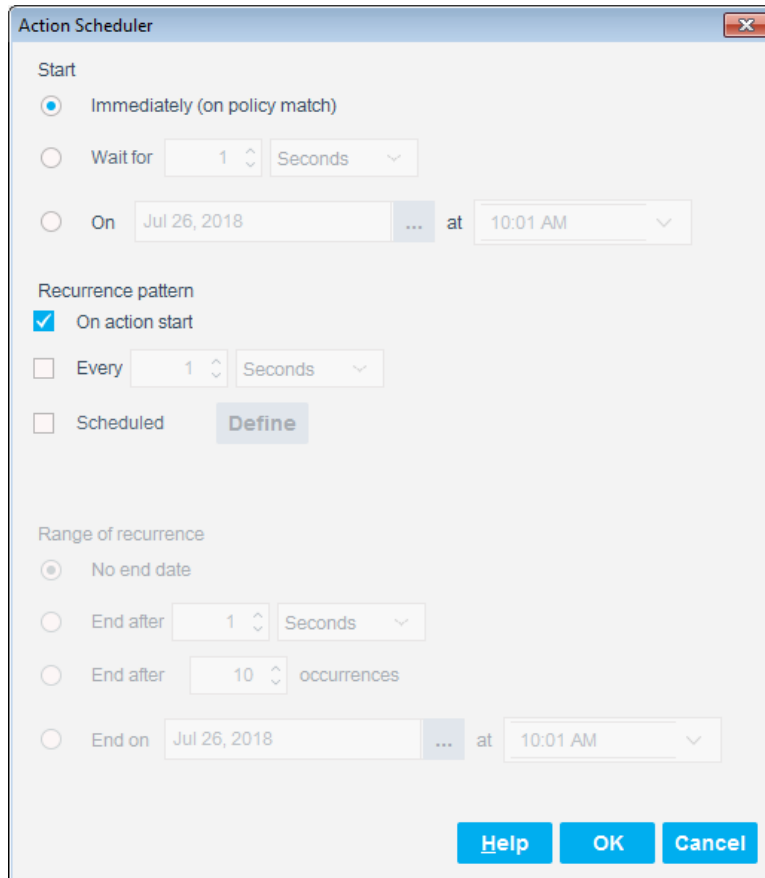
If termination protection is enabled, stopping EC2 instances does not terminate them.

To run the Enable EC2 Termination Protection action:

1. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Enable EC2 Termination Protection**.



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

The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). There is also an 'End on' option with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

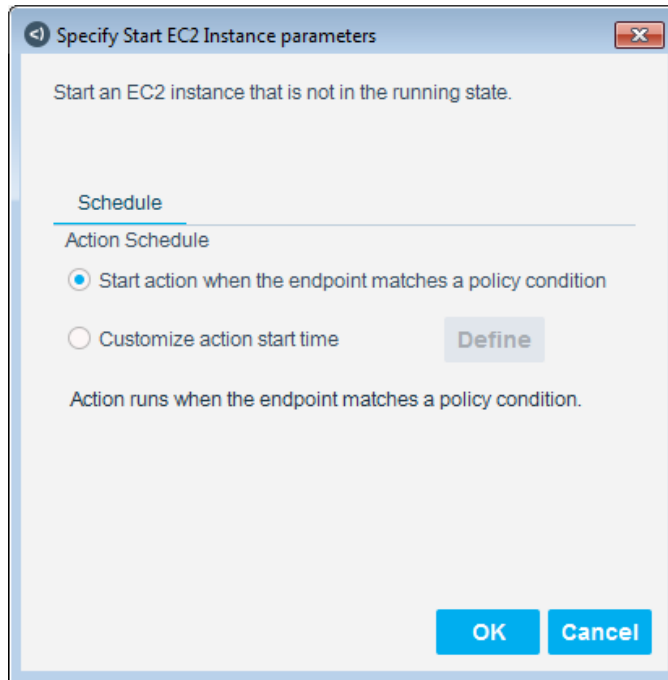
3. Set the schedule parameters and select **OK**.
4. In the Specify Enable EC2 Termination Protection parameters dialog box, select **OK**.

Start EC2 Instance Action

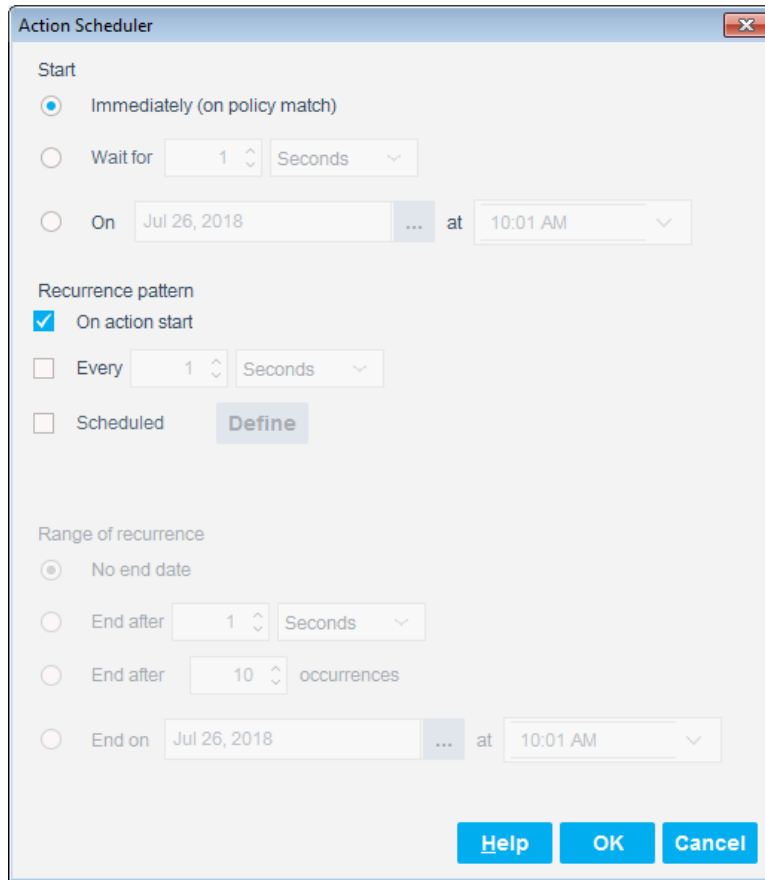
Use this action to start an EC2 instance that is not in the running state.

To run the Start EC2 Instance action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Start EC2 Instance**.



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



The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). The 'End on' option is also present with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

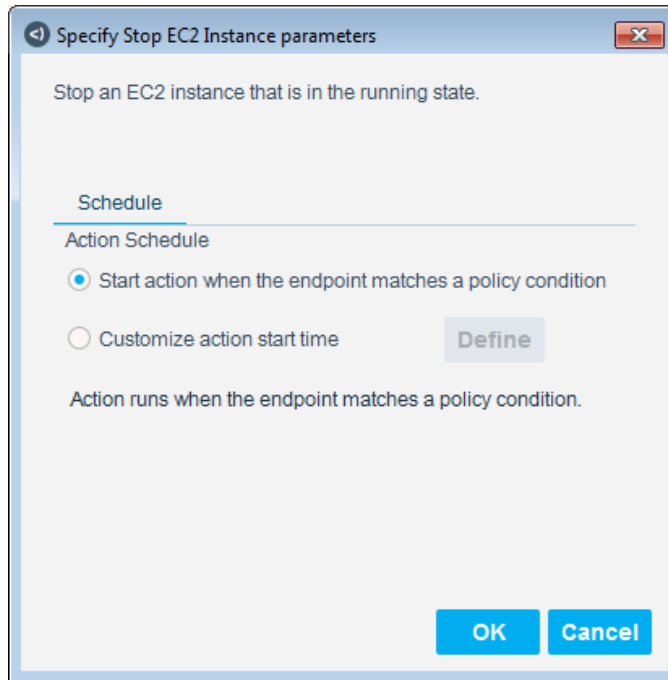
4. Set the schedule parameters and select **OK**.
5. In the Specify Start EC2 Instance parameters dialog box, select **OK**.

Stop EC2 Instance Action

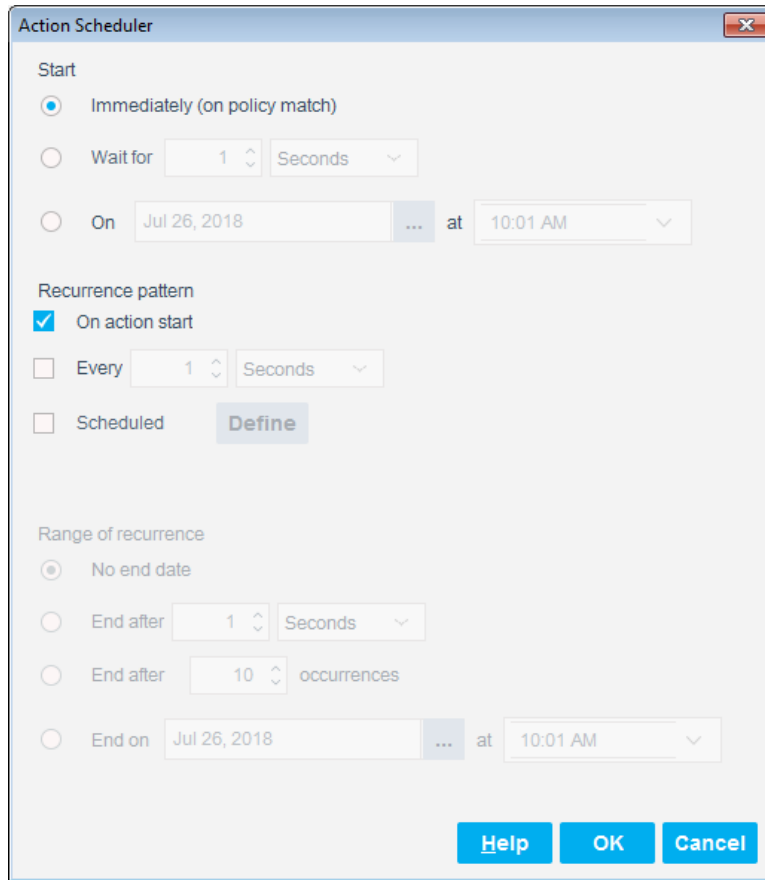
Use this action to stop an EC2 instance that is in the running state.

To run the Stop EC2 Instance action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **AWS EC2**, and select **Stop EC2 Instance**.



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

The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). There is also an 'End on' option with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

4. Set the schedule parameters and select **OK**.
5. In the Specify Stop EC2 Instance parameters dialog box, select **OK**.

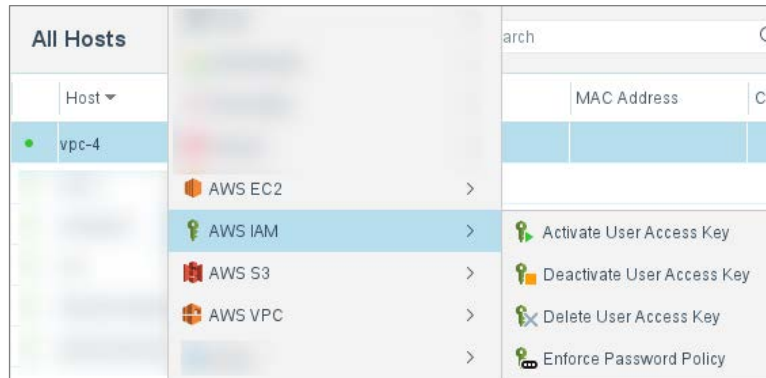
Manually Run AWS IAM Actions

Use the actions in this section for visibility and control of AWS IAM users. Control actions such as Activate/Deactivate User Access Key allow remediation upon non-compliance, allowing automated policies.

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

To manually run an AWS IAM action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, select a host entry.
3. Right-click an AWS endpoint, select **AWS IAM**, and select an action.



4. Select the following links for information on AWS IAM actions:

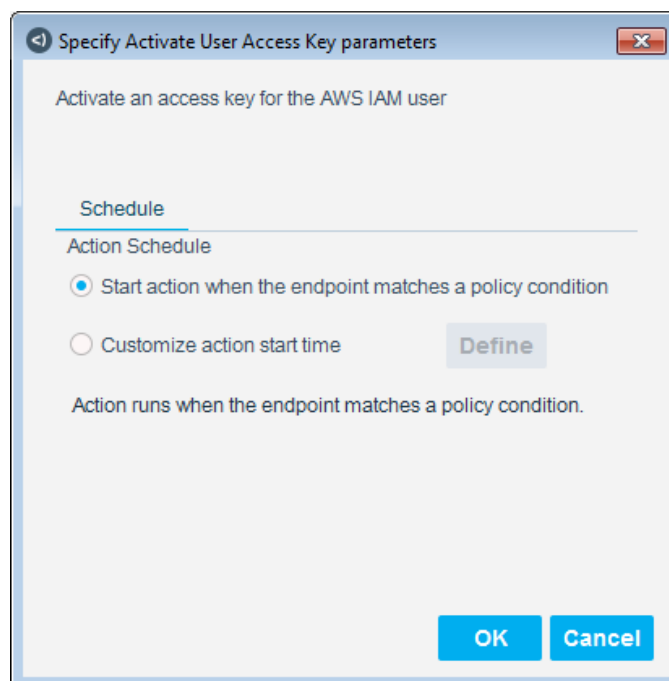
- [Activate User Access Key Action](#)
- [Deactivate User Access Key Action](#)
- [Delete User Access Key Action](#)
- [Enforce Password Policy Action](#)

Activate User Access Key Action

Use this action to activate an access key for the AWS IAM user.

To run the Activate User Access Key action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Activate User Access Key**.



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

Action Scheduler

Start

- ☒ Immediately (on policy match)
- ☐ Wait for
- ☐ On ... at

Recurrence pattern

- ☒ On action start
- ☐ Every
- ☐ Scheduled

Range of recurrence

- ☒ No end date
- ☐ End after
- ☐ End after occurrences
- ☐ End on ... at

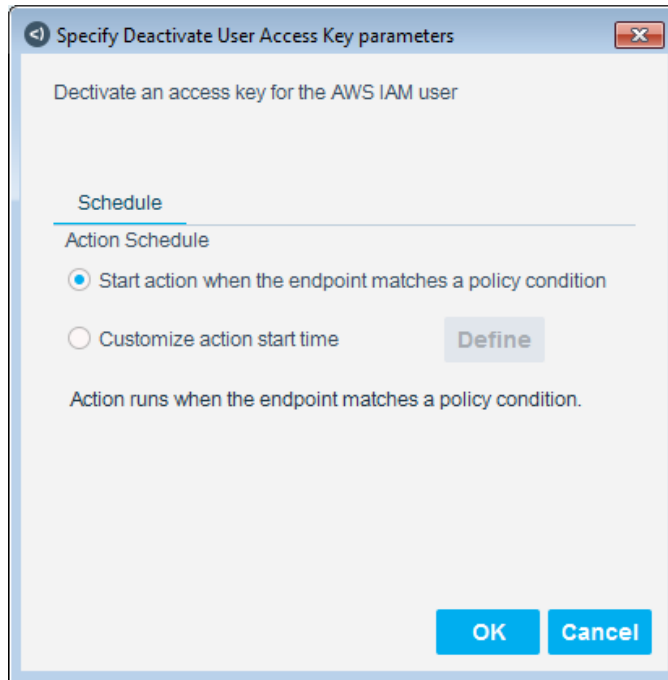
4. Set the schedule parameters and select **OK**.
5. In the Specify Activate User Access Key parameters dialog box, select **OK**.

Deactivate User Access Key Action

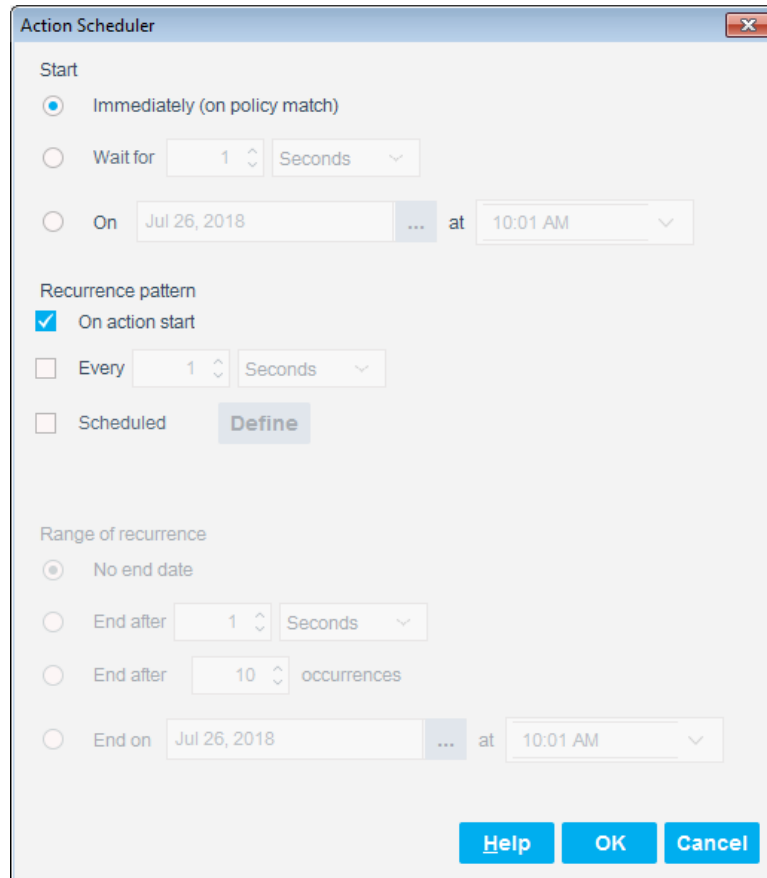
Use this action to deactivate an access key for the AWS IAM user.

To run the Deactivate User Access Key action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Deactivate User Access Key**.



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



The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a spinner set to 1 and a dropdown set to Seconds), and 'On' (with a date field set to Jul 26, 2018 and a time field set to 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a spinner set to 1 and a dropdown set to Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a spinner set to 1 and a dropdown set to Seconds), and 'End after' (with a spinner set to 10 and a dropdown set to occurrences). There is also an 'End on' option with a date field set to Jul 26, 2018 and a time field set to 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

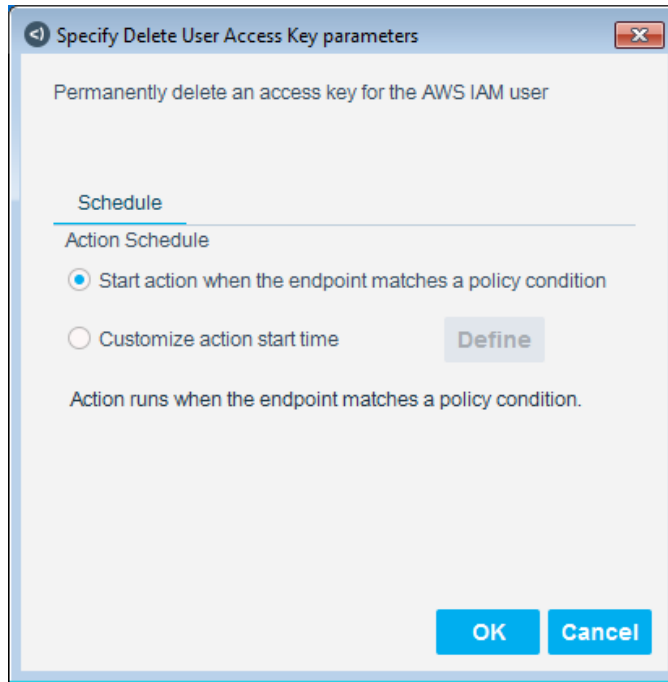
4. Set the schedule parameters and select **OK**.
5. In the Specify Deactivate User Access Key parameters dialog box, select **OK**.

Delete User Access Key Action

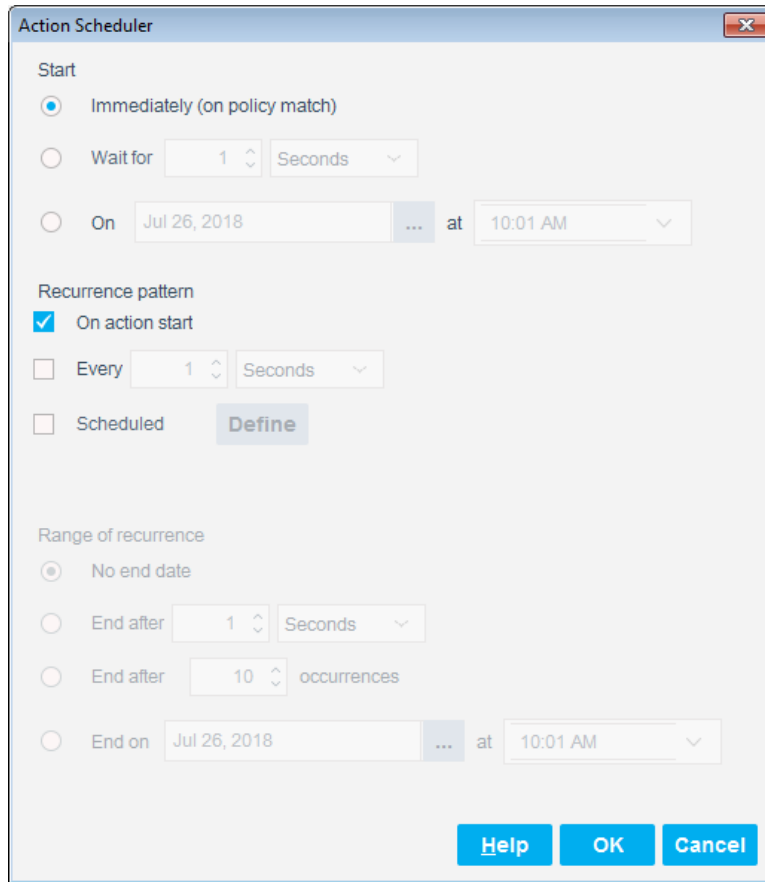
Use this action to permanently delete an access key for the AWS IAM user.

To run the Delete User Access Key action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Delete User Access Key**.



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

The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). There is also an 'End on' option with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

4. Set the schedule parameters and select **OK**.
5. In the Specify Delete User Access Key parameters dialog box, select **OK**.

Enforce Password Policy Action

Use this action to enforce the password policy for AWS IAM users with no password policy set.

To run the Enforce Password Policy action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS IAM**, and select **Enforce Password Policy**.

Specify Enforce Password Policy parameters

Enforce password policy

Parameters Schedule

☒ Allow Users To Change Password

☒ Expire Passwords

☒ Hard Expiry

Max Password Age 30

Minimum Password Length 6

Password Reuse Prevention 3

☒ Require Lowercase Characters

☒ Require Numbers

☒ Require Symbols

☒ Require Uppercase Characters

OK Cancel

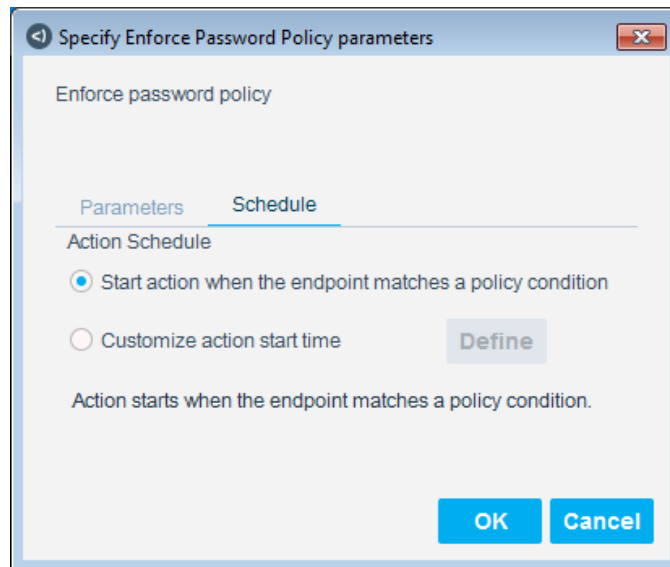
3. Set the password policy parameters.

Allow Users to Change Password	Specify whether users can change their own password.
Expire Passwords	Specify whether passwords expire.
Hard Expiry	Specify whether passwords have a hard expiry.
Max Password Age	Specify the value for maximum password age. The password expiration period must be a whole number between 1 and 1095 days, inclusive.
Minimum Password Length	Specify the value for minimum password length. The minimum password length must be a whole number greater than or equal to 6.
Password Reuse Prevention	Specify the value for password reuse prevention. The number of passwords to remember must be between 1 and 24, inclusive.
Require Lowercase Characters	Specify whether the password must contain lowercase characters.
Require Numbers	Specify whether the password must contain numbers.
Require Symbols	Specify whether the password must contain symbols.

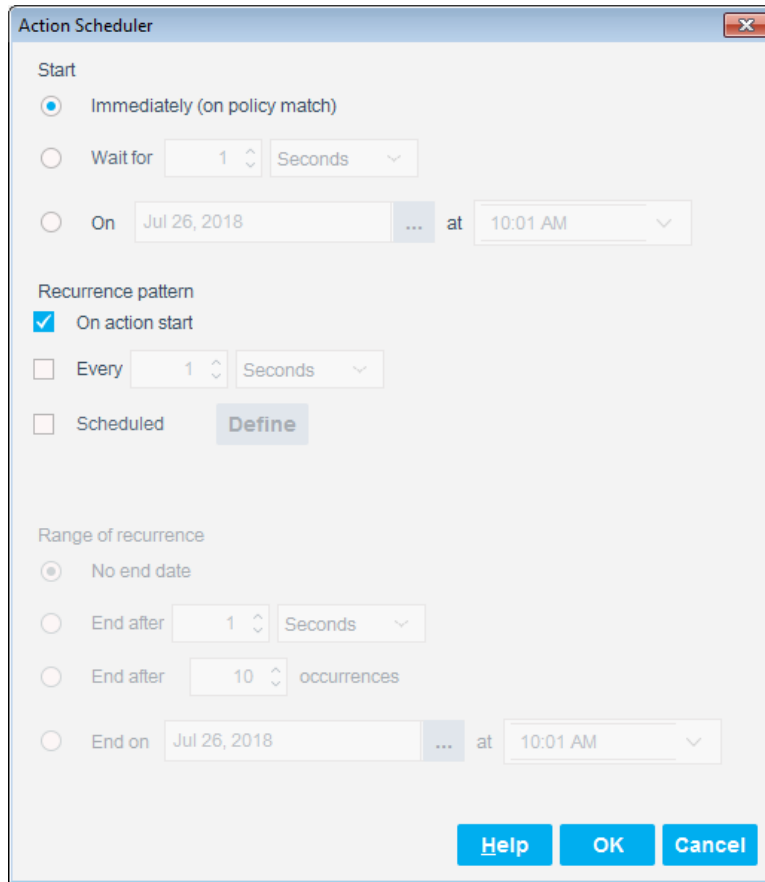
Require Uppercase Characters

Specify whether the password must contain uppercase characters.

4. Select the Schedule tab.



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

The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). There is also an 'End on' option with a date of Jul 26, 2018 and a time of 10:01 AM. At the bottom are 'Help', 'OK', and 'Cancel' buttons.

6. Set the schedule parameters and select **OK**.
7. In the Specify Enforce Password Policy parameters dialog box, select **OK**.

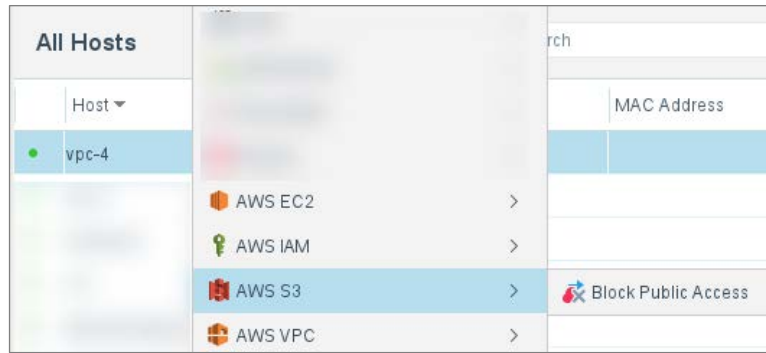
Manually Run AWS S3 Actions

Use the actions in this section for visibility and control of AWS S3s.

While AWS S3 actions can be launched as part of a policy, you can also manually run an action.

To manually run an AWS S3 action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, select a host entry.
3. Right-click an AWS endpoint, select **AWS S3**, and select an action.



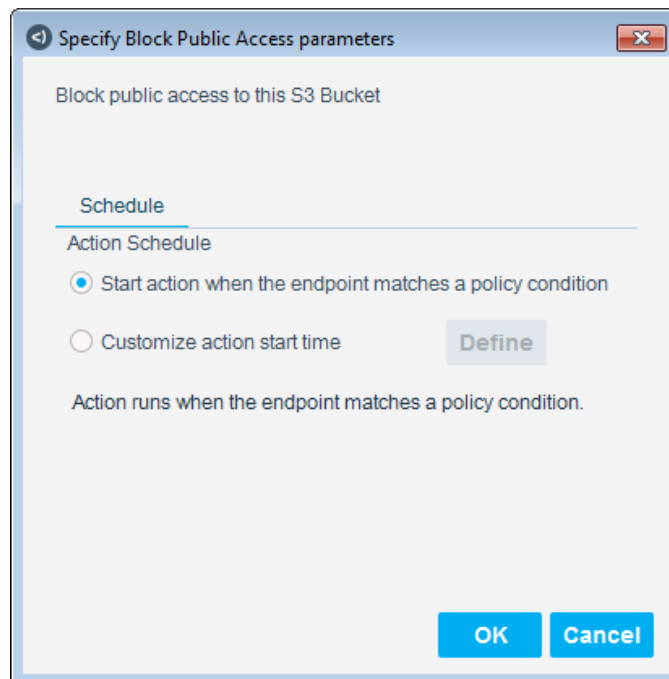
4. Select the following link for information on AWS S3 actions:
 - [Block Public Access Action](#)

Block Public Access Action

Use this action to block public access to a specific S3 bucket.

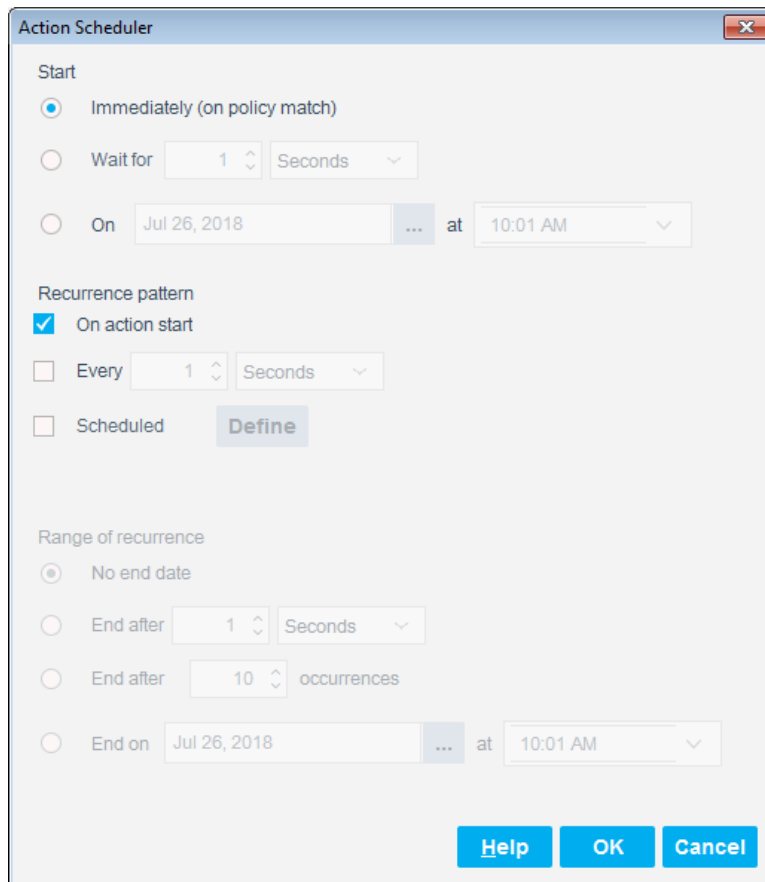
To run the Block Public Access action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS S3**, and select **Block Public Access**.



3. Select one of the following Action Schedule options:
 - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.

- **Customize action start time**, which opens the Action Scheduler dialog box.



The screenshot shows the 'Action Scheduler' dialog box. It has a title bar with a close button. The 'Start' section has three radio buttons: 'Immediately (on policy match)' (selected), 'Wait for' (with a value of 1 and unit of Seconds), and 'On' (with a date of Jul 26, 2018 and a time of 10:01 AM). The 'Recurrence pattern' section has three checkboxes: 'On action start' (checked), 'Every' (with a value of 1 and unit of Seconds), and 'Scheduled' (with a 'Define' button). The 'Range of recurrence' section has three radio buttons: 'No end date' (selected), 'End after' (with a value of 1 and unit of Seconds), and 'End after' (with a value of 10 and unit of occurrences). At the bottom, there are three buttons: 'Help', 'OK', and 'Cancel'.

4. Set the schedule parameters and select **OK**.
5. In the Specify Block Public Access parameters dialog box, select **OK**.

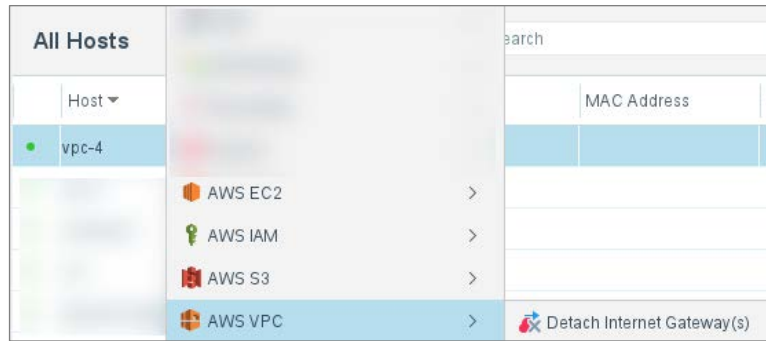
Manually Run AWS VPC Actions

Use the actions in this section for visibility and control of AWS VPCs.

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

To manually run an AWS VPC action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, select a host entry.
3. Right-click an AWS endpoint, select **AWS VPC**, and select an action.



4. Select the following link for information on AWS VPC actions:

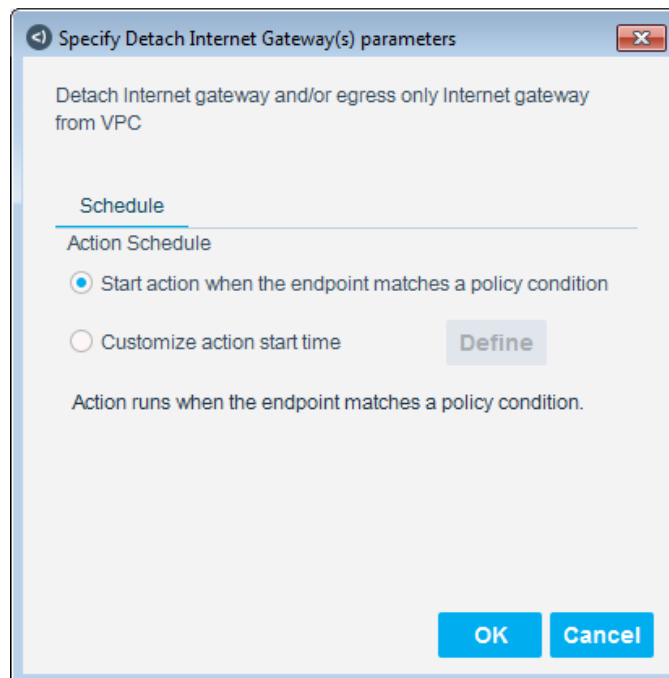
- [Detach Internet Gateway\(s\) Action](#)

Detach Internet Gateway(s) Action

Use this action to detach (terminate) the Internet gateway or egress-only Internet gateway from the AWS VPC.

To run the Detach Internet Gateway(s) action:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an AWS endpoint, select **AWS VPC**, and select **Detach Internet Gateway(s)**.



3. Select one of the following Action Schedule options:
 - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy condition(s) is met by the endpoint.

- **Customize action start time**, which opens the Action Scheduler dialog box.

Action Scheduler

Start

☒ Immediately (on policy match)

☐ Wait for Seconds

☐ On ... at

Recurrence pattern

☒ On action start

☐ Every Seconds

☐ Scheduled

Range of recurrence

☒ No end date

☐ End after Seconds

☐ End after occurrences

☐ End on ... at

4. Set the schedule parameters and select **OK**.
5. In the Specify Detach Internet Gateway(s) parameters dialog box, select **OK**.

Set Action Thresholds

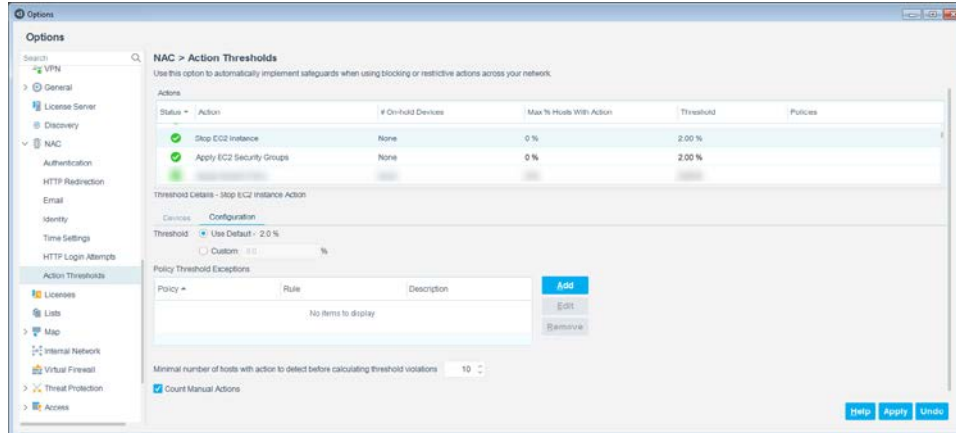
To restrict the number of actions, use action thresholds, which are designed to automatically implement safeguards. An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single device.

The Stop EC2 Instance and Apply EC2 Security Groups actions have a default 2% action threshold, which can be scaled up to 100%.

For more information about action thresholds, refer to the *Forescout Administration Guide*. See [Additional Forescout Documentation](#) for information on how to access this guide.

To change an action threshold:

1. In the Options pane, select **NAC > Actions Thresholds**.



2. In the Actions table, select **Stop EC2 Instance** or **Apply EC2 Security Groups**.
3. In the Threshold Details section, select the Configuration tab, select **Custom**, and type a value in the field.
4. Select **Apply**.

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 creates an access key ID and secret access key that is required when configuring the AWS Plugin. The recommended number of AWS accounts for a single Appliance is five.
2. **Level of Access** – The AWS user used by the Forescout platform should have full access across a range of permissions. See [Specify Permissions Using Standard AWS Policies](#).
3. **AWS Regions** – If you want complete visibility across all regions, select all of the available regions while performing sync during configuration. For a restrictive view, select specific regions only.
4. **Set Communications with AWS (Polling)** – When configuring the AWS Plugin, it is recommended to use the default setting for *Query Interval*. Depending on the amount of data, the polling of AWS entities can take 30 minutes for 20,000 instances.
5. **Active Discovery** – If you do not want the Forescout platform to perform Active Discovery, such as NMAP, HPS Inspection, or WMI on EC2 instances, make sure your EC2 instances are not reachable from the Forescout platform or their IP address segment is not included in any base classification policy.

Hybrid Cloud Module Information

The Amazon Web Services Plugin is installed with the Forescout Hybrid Cloud Module.

The Forescout Hybrid Cloud Module provides visibility and control functions across physical and virtual devices that are on-premises and off-premises through the following plugin integrations:

- AWS Plugin
- Azure Plugin
- VMware NSX Plugin
- VMware vSphere Plugin

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

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

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

Additional Forescout Documentation

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

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

Documentation Downloads

Documentation downloads can be accessed from the [Technical Documentation Page](#), and from one of two Forescout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** – [Product Updates Portal](#)
- **Flexx Licensing Mode** – [Customer Support Portal](#)

 *Software downloads are also available from these portals.*

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based [Documentation Portal](#), as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to <https://www.Forescout.com/company/technical-documentation/>

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. The portal also provides additional documentation.

To access the Product Updates Portal:

- Go to <https://updates.forescout.com/support/index.php?url=counteract> and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend Modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:

- Go to <https://Forescout.force.com/support/> and select **Downloads**.

Documentation Portal

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

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the [Documentation Portal](#), directly from the Forescout Console.

Console Help Buttons

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

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools > Options > Modules**, select the plugin, and then select **Help**.

Content Module, eyeSegment Module, and eyeExtend Module Help Files

- After the component is installed, select **Tools > Options > Modules**, select the component, and then select **Help**.

Documentation Portal

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