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

Legal Notice

© 2019 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.

2019-04-05 09:41
Table of Contents

Azure Plugin Overview ........................................................................................................... 5
   About Certification Compliance Mode .................................................................................. 6
   Use Cases ............................................................................................................................. 6
   Consolidated Visibility ......................................................................................................... 6
   Dynamic Policies ................................................................................................................ 6
   Network ................................................................................................................................ 6
   How It Works ......................................................................................................................... 6
   Polling ..................................................................................................................................... 7

What to Do .................................................................................................................................. 7
   Additional Azure Documentation ............................................................................................ 7

Requirements ............................................................................................................................ 7
   Forescout Requirements ....................................................................................................... 8
   Azure Requirements .............................................................................................................. 8
   Networking Requirements ...................................................................................................... 9

Define Azure Users ................................................................................................................... 9
   Required Permissions Using Azure Built-in Roles ............................................................... 10
   Specify Minimal Permissions Using Specific Custom Roles .............................................. 10
      Azure Resource Polling and Actions (Visibility and Control) ........................................... 11
      Azure Resource: Manual Poll (Visibility Only) ............................................................... 11
      Azure Instance: Start/Stop/Restart VM Actions ............................................................... 12
      Azure Instance: Enable/Disable Delete Protection Actions ............................................ 13
   Access Azure Account .......................................................................................................... 13
      Check Azure AD Permissions ............................................................................................ 14
      Check Azure Subscription Permissions ........................................................................... 16
      Create an Azure AD Application ....................................................................................... 17
      Obtain the Application ID and Authentication Key ......................................................... 19
      Obtain Tenant ID ............................................................................................................... 21
      Assign Application to Role ............................................................................................... 23

Install the Module ..................................................................................................................... 25

Configure the Module ............................................................................................................... 26
   Add Azure Connection ......................................................................................................... 26
   Verify That the Plugin Is Running ......................................................................................... 31
   Test an Azure Connection .................................................................................................... 31
   Poll an Azure Connection .................................................................................................... 33
   Edit an Azure Connection .................................................................................................... 33
   Remove an Azure Connection .............................................................................................. 34

Create an Azure Policy ............................................................................................................. 35
   Create a Policy from a Template ......................................................................................... 35
      Scope for Azure Entities without IP Addresses ................................................................. 41
      Scope for Azure Asset Classification Template ............................................................... 41
<table>
<thead>
<tr>
<th>Hybrid Cloud Module Information</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Forescout Documentation</td>
<td>68</td>
</tr>
<tr>
<td>Documentation Downloads</td>
<td>68</td>
</tr>
<tr>
<td>Documentation Portal</td>
<td>69</td>
</tr>
<tr>
<td>Forescout Help Tools</td>
<td>69</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Azure Policy Templates</th>
<th>42</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Instances Templates</td>
<td>43</td>
</tr>
<tr>
<td>Azure VNets Templates</td>
<td>43</td>
</tr>
<tr>
<td>Azure Subscriptions Templates</td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detect Cloud Endpoints – Host Properties</th>
<th>43</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Properties</td>
<td>44</td>
</tr>
<tr>
<td>Azure Local Network Gateway Properties</td>
<td>45</td>
</tr>
<tr>
<td>Azure Subscription Properties</td>
<td>45</td>
</tr>
<tr>
<td>Azure VM Properties</td>
<td>46</td>
</tr>
<tr>
<td>Azure VNet Properties</td>
<td>49</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>View Asset Inventory</th>
<th>51</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Azure Inventory</td>
<td>51</td>
</tr>
<tr>
<td>Access Azure Subscription Inventory</td>
<td>53</td>
</tr>
<tr>
<td>Access Azure VM Inventory</td>
<td>54</td>
</tr>
<tr>
<td>Access Azure VNet Inventory</td>
<td>55</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Run Azure Policy Actions</th>
<th>56</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Azure Instance Delete Protection Action</td>
<td>57</td>
</tr>
<tr>
<td>Disable Azure Instance Delete Protection Action</td>
<td>59</td>
</tr>
<tr>
<td>Start Azure Instance Action</td>
<td>61</td>
</tr>
<tr>
<td>Stop Azure Instance Action</td>
<td>63</td>
</tr>
<tr>
<td>Restart Azure Instance Action</td>
<td>65</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hybrid Cloud Module Information</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Forescout Documentation</td>
<td>68</td>
</tr>
<tr>
<td>Documentation Downloads</td>
<td>68</td>
</tr>
<tr>
<td>Documentation Portal</td>
<td>69</td>
</tr>
<tr>
<td>Forescout Help Tools</td>
<td>69</td>
</tr>
</tbody>
</table>
Azure Plugin Overview

The Microsoft Azure® Plugin is a component of the Forescout® Hybrid Cloud Module. See Hybrid Cloud Module Information for details about the module.

The Azure Plugin connects to the Microsoft® Azure public cloud environment to retrieve information on Virtual Machine (VM) instances and other Azure entities, such as Virtual Networks (V Nets). The VM instances and V Nets follow rules similar to those of other endpoints discovered by the Forescout platform, where policies and actions can be defined on those entities. The integration of the Forescout platform with Azure brings the detailed visibility, control, and compliance capabilities of the Forescout platform to Azure VM instances and the associated Azure cloud configurations.

The Azure Plugin lets you:

- See VM instances and V Nets in Microsoft Azure’s public cloud
- Create and apply Forescout policies across Azure entities
- Maintain the security and compliance of Azure VM instances and V Nets
- Start and stop a VM instance, enable delete protection on a VM instance, and 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. With the integration of the Forescout platform with Azure, you can:

- Have full visibility of your Azure VM instances and their properties. Since disparate teams may be starting and stopping VMs in a public cloud environment, it is important for all of IT to have a good understanding of the resources that are being used in the cloud. Regular checks provide valuable information on how and when Azure 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 public IP addresses are quickly identified for remediation.
- Enable delete protection for Azure VM instances to prevent accidental deletion of a VM, by establishing a policy in which all compliant and critical VM assets have delete protection enabled. See Enable Azure Instance Delete Protection Action and Disable Azure Instance Delete Protection Action.
- Collect information about the Azure environment across multiple Azure accounts and subscriptions, all from a common deployment. This includes fine grain details, such as the Azure Tags applied to a virtual machine, Azure VNet settings and routes, as well as the creation of new Subscriptions, and many other Azure operational details.
- Discover cloud-based endpoints early, allowing identification and compliance checking of the workload itself. A non-compliant endpoint can be stopped and/or the Azure account team can be notified. If remediation fails, the endpoint can be stopped to prevent further damage.
About Certification Compliance Mode

Forescout Hybrid Cloud Module: Microsoft Azure Plugin supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation 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 Azure extends Forescout’s eyeSight and eyeControl to instances running in Azure. This allows visibility for campus, data center, and cloud endpoints from the same CounterACT® device (depending on the scale of the environment).

Dynamic Policies

As instances come online, they can be automatically checked for range properties. For example, the Forescout platform can check for the presence of Azure Tags and dynamically add these tags to groups, such as testing, development, and production. These groups, in turn, can be assessed by additional fine-grained policies. Instances can also be classified based on their function, such as web, application, or database tier.

Network

VNets configured for an Azure environment and their associated properties can be collected. Policy templates are provided to highlight context, such as IP Address Space, Subnets and Route Tables, as well as the presence of a new VNet to ensure proper connectivity policies.

How It Works

This plugin uses well-defined APIs from Azure to provide visibility into Azure VMs and VNets.

Once the configuration is completed using an Azure account with the appropriate credentials and permissions, the Forescout platform communicates with one or more Azure accounts. The Azure Plugin polls both running and non-running VMs on the Azure cloud and retrieves information on the VMs as well as the VNets under that account.

Instance-related properties are collected as Forescout host properties, while other cloud entities, such as VNets, are also displayed as logical endpoints in the Forescout platform. The query and collection of Azure entities and associated properties are invoked at configured time intervals.
Azure classic resources (VM and VNet) are not supported. For details, refer to https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model

Polling

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

Because this data can be quite extensive and there are certain API throttle limits in Azure, the full poll takes place at longer intervals (by default, every 120 minutes). The optional delta polling means that VM instance state changes are recognized immediately by the Forescout platform. The delta poll only looks for changes to VM instances, so it takes place at shorter intervals (by default, one minute intervals).

What to Do

To set up your system for integration with Azure environments:

1. Verify that you have met system requirements. See Requirements.
2. Define Azure Users.
3. Configure the Module.
4. Use the in-depth information reported by the plugin to manage virtual devices:
   - Create an Azure Policy
   - Detect Cloud Endpoints – Host Properties
   - View Asset Inventory
   - Run Azure Policy Actions

Additional Azure Documentation

To use the Azure Plugin, you should have a good understanding of Microsoft Azure services and VM concepts, functionality, and terminology. You should also understand how Forescout policies and other basic features work. For more information on installation, configuration, and general guides, refer to:

https://docs.microsoft.com/en-us/azure/

Requirements

This section describes system requirements, including:

- Forescout Requirements
Forescout Requirements

The Azure Plugin requires the following Forescout release and other components:

- Forescout version 8.1
- Hybrid Cloud Module version 2.0.0 or above with the Azure component running
- (Flexx licensing) A valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the plugin/component. If you do not have this license, these actions will be disabled in the Console. Refer to the Forescout Flexx Licensing How-to Guide for more information about managing Flexx licenses and how to request/purchase this license.

Azure Requirements

This plugin requires the following Azure components:

- An Azure online account.
- One Azure account tenant ID, one Azure account client/application ID, and one access key to configure the Azure Plugin. These are associated with a User account on Azure.

  The following Azure services:

  - **Azure Virtual Machine** – A web service that enables you to launch and manage Linux and Windows server instances in Azure’s public cloud.
  - **Azure VNet** (VNet) – A web service for provisioning a logically isolated section of the Azure Cloud where you can launch Azure resources in a virtual network you define. You control your virtual networking environment, including the selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
  - **Azure Subscriptions** – A web service that grants you access to Azure services. It includes the Azure account for usage and billing as well as governing the use of Azure subscription services.

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

- Read-only permissions (the Forescout platform supports visibility only)
- Full permissions (the Forescout platform supports both visibility and control)
Networking Requirements

The following must be configured on enterprise firewalls to support communication between the Forescout platform and Azure regional access points.

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

Define Azure Users

Before the Forescout platform can query Azure, you need to define an Azure service principal and generate an access key for it. The Forescout Azure Plugin authenticates against an Azure account via this service principal (the application). The Forescout platform uses the Account Client/App ID in the actual Azure account set up. Both Account Client and App ID terms are used in Azure documentation and portal but they both link back to the service principal. You should name the service principal something that helps create a logical linkage to the Forescout platform's integration such fs-az-plugin-app. For additional details on creating a service principal, refer to: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal.

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

Permissions can be set using built-in roles or custom roles. See Required Permissions Using Azure Built-in Roles and Specify Minimal Permissions Using Specific Custom Roles.
Required Permissions Using Azure Built-in Roles

The following table summarizes the Azure permissions needed by the Azure plugin to access the Azure environment (for example, the `fs-az-plugin-app` application for the above.

Note that permissions within Azure can be defined as granular as per subscription, or they can be defined at the Management Groups level. Management Groups provide a level of scope above subscriptions, letting you organize subscriptions into a hierarchy. Permissions can then be applied to all subscriptions in a Management Group. For more information on Azure Management Groups, refer to: [https://docs.microsoft.com/en-us/azure/governance/management-groups/](https://docs.microsoft.com/en-us/azure/governance/management-groups/).

<table>
<thead>
<tr>
<th>Item</th>
<th>Resources</th>
<th>Minimum Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover resources (full poll)</td>
<td>Resource groups belonging to the target subscription and the objects under the resource group, such as VMs and VNets</td>
<td>Reader role, assigned at the Subscription scope or Management Group scope</td>
</tr>
<tr>
<td>Administrative actions on VM instance</td>
<td>Perform actions, such as Start Azure Instance, Stop Azure Instance, and Restart Azure Instance</td>
<td>Reader and Virtual Machine Contributor roles, assigned at the Subscription scope or Management Group scope</td>
</tr>
<tr>
<td>Resource lock</td>
<td>Add, Remove, CanNotDelete lock on resources, such as Enable/Disable Azure Instance Delete Protection</td>
<td>Either Owner role or Reader and User Access Administrator roles, assigned at the Subscription scope or Management Group scope</td>
</tr>
</tbody>
</table>

Specify Minimal Permissions Using Specific Custom Roles

The Forescout platform’s access to an Azure environment can be tightly controlled through permissions using custom roles. This section contains permissions for various operations using the principle of the least or minimal privilege.

Note that any customization may negatively impact the Azure Plugin’s ability to function properly. For example, if the Forescout platform is not granted permission for start/stop/restart actions, trying such an action will fail.

For additional assistance with Azure custom roles, refer to: [https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles).

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 Azure postings on topics such as the following:

Azure Resource Polling and Actions (Visibility and Control)

The least privilege needed for resource polling and actions includes all the permissions for the Azure Plugin functionality.

```json
{
  "Name": "FS Visibility and Control Operator",
  "IsCustom": true,
  "Description": "Can monitor Azure resources and perform power and deletion protection operations on virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Authorization/*/read",
    "Microsoft.ResourceHealth/availabilityStatuses/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [
  ],
  "AssignableScopes": [
    "/subscriptions/{subscriptionId1}"
  ]
}
```

Azure Resource: Manual Poll (Visibility Only)

The least privilege needed for manual poll is more restrictive than the built-in Reader role.

```json
{
  "Name": "FS Visibility Operator",
  "IsCustom": true,
  "Description": "Can monitor virtual network and virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read"
  ]
}
```
Azure Instance: Start/Stop/Rerstart VM Actions

The least privilege needed for start/stop/restart actions is more restrictive than the built-in Virtual Machine Contributor role.

```json
{
    "Name": "FS VM Power Operator",
    "IsCustom": true,
    "Description": "Can monitor and start/stop/restart virtual machines.",
    "Actions": [
        "Microsoft.Storage/*/read",
        "Microsoft.Network/*/read",
        "Microsoft.Compute/*/read",
        "Microsoft.Compute/virtualMachines/start/action",
        "Microsoft.Compute/virtualMachines/restart/action",
        "Microsoft.Compute/virtualMachines/powerOff/action",
        "Microsoft.Authorization/*/read",
        "Microsoft.ResourceHealth/availabilityStatuses/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Insights/alertRules/*",
        "Microsoft.Support/*"
    ],
    "NotActions": [
    ],
    "AssignableScopes": [
        "/subscriptions/{subscriptionId1}",
        "/subscriptions/{subscriptionId2}
    ]
}
```
Azure Instance: Enable/Disable Delete Protection Actions

The least privilege needed for enable/disable delete protection actions is more restrictive than the built-in Owner or User Access Administrator roles.

```json
{
    "Name": "FS VM Delete Protection Operator",
    "IsCustom": true,
    "Description": "Can enable or disable delete protection on virtual machines.",
    "Actions": [
        "Microsoft.Storage/*/read",
        "Microsoft.Network/*/read",
        "Microsoft.Compute/*/read",
        "Microsoft.Authorization/locks/*",
        "Microsoft.Authorization/*/read",
        "Microsoft.ResourceHealth/availabilityStatuses/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Insights/alertRules/*",
        "Microsoft.Support/*"
    ],
    "NotActions": [
    ],
    "AssignableScopes": [
        "/subscriptions/{subscriptionId1}",
        "/subscriptions/{subscriptionId2}
    ]
}
```

Access Azure Account

Before the Forescout Azure Plugin can authenticate against an Azure account via the service principal (the application), you need to perform the following procedures to register an application and service principal on the Azure Active Directory (AD) as well as ensure that you have defined the appropriate permissions.

- Check Azure AD Permissions
- Check Azure Subscription Permissions
- Create an Azure AD Application
- Obtain the Application ID and Authentication Key
- Obtain Tenant ID
- Assign Application to Role
Check Azure AD Permissions

To register an app, you must have global Admin permissions or the **App registrations** option must be configured to allow all users to register apps.

**To check Azure AD permissions:**


2. Select **Azure Active Directory**.
3. Select **User settings**.

4. Check the setting of **App registrations**.
5. If **App registrations** is set to **Yes**, any user in the Azure AD tenant, including a non-admin user, can register an app. See [Check Azure Subscription Permissions](#).

6. If **App registrations** is set to **No**, only global administrators can register AD apps. Check if your account is an admin for the Azure AD tenant. Select **Overview** and view your user information. If your account is assigned to the User role, but the setting of **App registrations** is limited to admin users, ask your administrator to assign you to the global administrator role or to enable users to register apps.

---

**Check Azure Subscription Permissions**

In your Azure subscription, your account must have `Microsoft.Authorization/*/Write` access to assign an AD app to a role. This action is granted through the User Access Administrator role. If your account is assigned to the Virtual Machine Contributor role, you do not have adequate permission and an error message is displayed if you attempt to assign the service principal to a role.

**To check Azure subscription permissions:**

1. Select your account in the upper right corner and select **My permissions**, which may be listed under ....

The My permissions dialog box opens.
2. From the **Subscription** drop-down menu, select the subscription.

3. Select **Click here to view complete access details for this subscription**.

4. View your assigned roles. If you do not have adequate permissions to assign an AD app to a role, ask your subscription administrator to add you to the User Access Administrator role.

The following example shows a user who is assigned the Owner role and therefore has adequate permissions.

---

**Create an Azure AD Application**

**To create an Azure AD application:**

2. Select **Azure Active Directory**.

3. Select **App registrations**.
4. Select **New application registration**.

5. Enter the **Name** and **URL** for the application.

   *The application name must be unique across an Azure region.*

6. Select **Web app / API** for the Application type.

7. Review the application details.

**Obtain the Application ID and Authentication Key**

To log in, you need to obtain the ID for your application and an authentication key.

**To obtain the application ID and authentication key:**

1. Select **Azure Active Directory > App registrations**.
2. Select your application.

3. Copy the **Application ID** and store it in your application code. The application ID is also referred to as the client ID.

4. To generate an authentication key, select **Settings**.

5. Select **Keys**.
6. Enter a description of the key and a duration (expiry) for the key (In 1 year, In 2 years, or Never expires).

7. Select Save. The value of the key is displayed.

8. Copy the key value. You cannot retrieve the key later. You need to provide the key value with the application ID to log in to the application. Store the key value where your application can retrieve it.

**Obtain Tenant ID**

To log in, you need to include the tenant ID with your authentication request.

To obtain tenant ID:

1. Select Azure Active Directory > Properties.
The Microsoft – Properties window opens.
2. Copy the Directory ID. This is the tenant ID.

**Assign Application to Role**

To access resources in your subscription, you must assign the application to a role. Decide which role represents the appropriate permissions for the application.

You can set the scope at the level of the subscription, resource group, or resource. Permissions are inherited to lower levels of the scope. For example, adding an application to the Reader role for a resource group means it can read the resource group and any resources it contains.

The recommendation is to assign the role at the subscription scope.

**To assign application to role:**

1. Go to the level of scope to which you want to assign the application. For example, to assign a role at the subscription scope, select **Subscriptions**.

The Subscriptions pane opens.

2. Select the subscription to which to assign the application, for example, Acme-Test-Sub.
3. Select **Access control (IAM)**.

4. Select **Add**.

5. Select the **Role** to which you want to assign the application. See [Required Permissions Using Azure Built-in Roles](#) for details.

6. From the **Assign access to** drop-down menu, select the group to be assigned access. By default, Azure AD applications are not displayed in the available options. To find your application, type its name in the **Select** field.

7. Select **Save**. The application is displayed in the list of users assigned to a role for that level of scope.
Accounts can have multiple subscriptions. Repeat this procedure to assign a role for another subscription or apply roles at the Management Groups level to have subscriptions inherit the appropriate roles.

**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 will not proceed if you do not agree to the license agreement.

   - The installation will begin immediately after selecting Install, and cannot be interrupted or canceled.

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

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

   - Some components are not automatically started following installation.
Configure the Module

Configure the module to ensure that the Forescout platform can communicate with Azure API access points.

Before you begin the plugin configuration, verify all Requirements have been met. Removing a configured connection stops endpoint discovery and property learning of virtual machines unique to the connection, but any actions remain enabled.

Add Azure Connection

The Forescout platform communicates with Azure to discover and implement management actions on endpoints. This section describes how to add a connection to Azure from the Forescout platform. Verify that you have access to your Azure credentials before adding a connection. One side of the connection is on the Azure platform, the other is on the Forescout platform. Multiple Azure connections can be configured.

To add an Azure connection:

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

2. From the Options pane, select Azure.

3. Select Add.
4. Enter the login credentials for Azure.

<table>
<thead>
<tr>
<th><strong>Azure Account Tenant ID</strong></th>
<th>Enter the Azure account tenant ID. This is the Azure Active Directory ID for this Azure account.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Account Client/App ID</strong></td>
<td>Enter the Azure account client/application ID. The Azure application ID is also known as the service principal ID.</td>
</tr>
<tr>
<td><strong>Access Key</strong></td>
<td>Enter the generated access key. See Obtain the Application ID and Authentication Key.</td>
</tr>
<tr>
<td><strong>Verify Access Key</strong></td>
<td>Re-enter the access key to verify it.</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td>From the drop-down menu, select Azure Standard Account or Azure US Gov Cloud Account. The access key credentials differ for these accounts.</td>
</tr>
<tr>
<td><strong>Connecting CounterACT Device</strong></td>
<td>Select the CounterACT device used to connect to Azure. This device manages all communication with Azure using the tenant ID and the client/application ID defined for this connection, including requests submitted by other CounterACT devices you assign to this connection. From the drop-down menu, select Enterprise Manager or the IP address of an Appliance.</td>
</tr>
<tr>
<td><strong>Account Nickname</strong></td>
<td>(Optional) Enter a nickname for this account to distinguish it from other Azure accounts.</td>
</tr>
</tbody>
</table>

5. Select **Next**.
6. (Optional) Enter proxy server information. If your environment routes Internet communications through proxy servers, select **Use Proxy Server** and specify information for the proxy server that handles communications between Azure and the connecting CounterACT device. Only anonymous proxy is supported.

<table>
<thead>
<tr>
<th><strong>Use Proxy Server</strong></th>
<th>Select this option if your environment routes Internet communications through proxy servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Server Host</strong></td>
<td>Enter the host IP address of the proxy server.</td>
</tr>
<tr>
<td><strong>Proxy Server Port</strong></td>
<td>Set the port number of the proxy server.</td>
</tr>
</tbody>
</table>

7. Select **Next**. Subscription information for the Azure account is fetched from the Azure cloud, such as the ID and name of each subscription. Multiple subscriptions can be created under an Azure account. Use subscriptions to break down an Azure account to manageable sizes.

*Azure permissions dictate which subscriptions can be accessed by the Forescout platform*. If specific Azure subscriptions are not listed, double-check the permissions assigned to the Forescout platform in the Azure portal.
8. Select **Close**.

9. Select one or more subscription. This connection queries Azure to discover endpoints only in the subscriptions you select here.

10. Select **Next**. Virtual Network (VNet) information from all connecting Appliances is checked for IP Address Space conflicts. A VNet IP Address Space conflict is detected when there is a conflict with the IP address range of the subnet.

11. Select **Close**.
12. Define the settings that control communication of the Forescout platform with Azure.

<table>
<thead>
<tr>
<th><strong>Query Interval (seconds)</strong></th>
<th>Specify how frequently the plugin queries Azure for a full poll. The range is from 60 to 86400 seconds (1 minute to 24 hours). The default is 7200 seconds (2 hours). All VMs are polled with the full poll.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delta Poll of Azure Instances</strong></td>
<td>Enable delta polling of Azure instances (default). The VMs with a status change during the last delta poll interval, for example, the last 60 seconds, are polled.</td>
</tr>
<tr>
<td><strong>Delta Poll Interval (seconds)</strong></td>
<td>Specify the delta polling interval. The range is from 60 to 86400 seconds (1 minute to 24 hours). The default is 60 seconds (1 minute).</td>
</tr>
</tbody>
</table>

13. Select **Finish**. The new connection is displayed in the Azure pane.

14. Before selecting **Apply** in the Azure pane, which saves the plugin configuration, you can select **Test** to test the connection. Some information is displayed in the Testing Azure account configuration dialog box, but a full poll will not yet have been successfully completed. See [Test an Azure Connection](#) for details.
You cannot trigger a manual poll before you select **Apply** and save the configuration.

15. In the Azure pane, select **Apply**. The Saving Azure Plugin Configuration on Enterprise Manager dialog box opens.

16. Select **Close** and then select **OK**.

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

### Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

**To verify:**

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

The plugin is located under Hybrid Cloud > Azure.

### Test an Azure Connection

You can test connectivity to Azure with the configured account information and test the permissions on the account. Information on resource groups and VMs is also retrieved. Errors might also be displayed, for example, if permissions are not set correctly.

- **The test polls all available subscriptions, whether a subscription is selected or not.**

**To test an Azure connection:**

1. In the Azure pane, select an Azure connection and select **Test**.
2. The following information is displayed.

<table>
<thead>
<tr>
<th><strong>Connecting using Client ID</strong></th>
<th>The Azure client/application ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last full poll was successfully completed at</strong></td>
<td>The timestamp of the last successful full poll.</td>
</tr>
<tr>
<td><strong>Subscription ID</strong></td>
<td>The subscription ID.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The subscription display name.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state (such as enabled or disabled) of the available subscriptions.</td>
</tr>
<tr>
<td><strong>SUBSCRIPTION</strong></td>
<td>Each subscription.</td>
</tr>
<tr>
<td><strong>SELECTED</strong></td>
<td>Whether a subscription is selected to be polled by the Azure Plugin.</td>
</tr>
<tr>
<td><strong># AZURE VM (Running/Total)</strong></td>
<td>The number of running and the total number of Azure VMs for each resource group.</td>
</tr>
<tr>
<td><strong>VNET Counts</strong></td>
<td>The number of virtual networks for each resource group.</td>
</tr>
<tr>
<td><strong>Resource Group Name</strong></td>
<td>The name of each resource group associated with each Azure subscription.</td>
</tr>
<tr>
<td><strong>Total numbers of virtual machine instances detected on this device are (running/total)</strong></td>
<td>The running and total counts of the number of VM instances in all selected subscriptions.</td>
</tr>
</tbody>
</table>

3. After viewing the results, select **Close**.

> It is recommended you test an Azure connection after the Azure Plugin has been running for 1-2 minutes.
Poll an Azure Connection

Polling an Azure connection performs a full synchronization of Azure instances on selected Azure subscriptions. Information about all VMs is obtained.

To poll an Azure connection:

1. In the Azure pane, select an Azure connection and select Poll. The results of a subscription poll and full poll on an Azure account are displayed in the Manual Poll dialog box.

2. The following information is displayed.

<table>
<thead>
<tr>
<th>Subscription poll and full poll on account, client/app ID</th>
<th>The Azure account nickname and client/application ID of the Azure account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription</td>
<td>The subscription ID.</td>
</tr>
<tr>
<td>VM Instances</td>
<td>The number of VM instances for that subscription.</td>
</tr>
<tr>
<td>Total number of Azure virtual machine instances polled</td>
<td>The total number of Azure VM instances polled.</td>
</tr>
</tbody>
</table>

3. After viewing the results, select Close.

Edit an Azure Connection

You can edit a configured Azure connection.

To edit an Azure connection:

1. In the Azure pane, select an Azure connection and select Edit.
2. Edit the connection parameters in the General, Proxy Server Definition, Subscriptions, and Advanced tabs.

3. Select **OK**.

**Remove an Azure Connection**

If you remove an Azure connection, host discovery and property learning of Azure endpoints hosted by this connection are stopped, however any actions remain enabled. In addition, any actions already launched remain active and are not undone.

**To remove an Azure connection:**

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

The Azure Plugin provides additional endpoint properties and actions that are useful for management of Azure virtual devices. Use these properties and actions to construct customized policies for detecting, managing, and remediating endpoints based on the Azure 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 Forescout Templates and Policy Management chapters in the Forescout Administration Guide.

Create a Policy from a Template

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

In the templates, the scope defines the range of hosts to be inspected by the policy. The policy rules instruct the Forescout platform how to detect and handle devices defined in the policy scope.

Hosts that match the Main Rule are included in the policy inspection. Hosts that do not match this rule are not inspected for this policy. Sub-rules automatically follow up with hosts after initial detection and handling, streamlining separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.

To create an Azure policy using a template:

1. Log in to the Console and select Policy.


3. Select Templates and select the Azure folder.
4. The Azure policy templates are organized in folders. Expand the Azure folders to view the policy templates and then select an Azure policy. For details on the folders and the available templates, see Azure Policy Templates.

5. Select Next.
6. Enter the name of the new policy. Optionally, add a description.

7. Select Next. Both the Scope pane and the IP Address Range dialog box open.

8. 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.

For two special cases, see Scope for Azure Entities without IP Addresses and Scope for Azure Asset Classification Template.

9. Select OK. The added range is displayed in the Scope pane.
10. Select **Next**. The default sub-rules for the selected policy template are displayed.

12. Enter the name of the new rule. Optionally, add a description.

13. Select OK.
14. To edit the policy name, select **Edit** in the Name section.

15. To add a condition, select **Add** in the Condition section. See [Detect Cloud Endpoints – Host Properties](#).

16. To add an action, select **Add** in the Actions section. See [Run Azure Policy Actions](#).

17. Select **OK**.

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

19. In the Policy Manager, select **Apply**.
Scope for Azure Entities without IP Addresses

Some Azure entities do not have IP addresses. For the policy templates under Azure VNets and Azure Subscriptions, **Hosts without a known IP address** is preselected in the Scope pane. This is indicated by the note shown in the following figure.

Scope for Azure Asset Classification Template

Some Azure entities do not have IP addresses. These include VNets, local network gateways, and subscriptions. To classify all Azure entities with the Azure Asset Classification policy template, you must select both **Unknown IP addresses** and **All IPs** in the IP Address Range dialog box.

To select both **Unknown IP addresses** and **All IPs**, you need to select the first IP address range in the IP Address Range dialog box and select **OK**, then select **Add** in the Scope pane to select the second IP address range. This configuration is shown in the following figure.
The Azure policy templates are organized in the following folders:

| Azure Instances       | Use the templates in this folder to create policies to classify Azure VM instances. 
<table>
<thead>
<tr>
<th></th>
<th>There is a sub-folder called Azure Instance Event. Use the templates in this folder to create policies on Azure instance events.</th>
</tr>
</thead>
</table>
| Azure VNets           | Use the templates in this folder to create policies to classify Azure VNets. 
<table>
<thead>
<tr>
<th></th>
<th>There is a sub-folder called Azure VNet Event. Use the templates in this folder to create policies on Azure VNet events.</th>
</tr>
</thead>
</table>
| Azure Subscriptions   | Use the templates in this folder to create policies to classify Azure account subscriptions. 
<table>
<thead>
<tr>
<th></th>
<th>There is a sub-folder called Azure Subscription Event. Use the templates in this folder to create policies on Azure subscription events.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Asset Classification</td>
<td>Use this template to create policies to classify Azure resources.</td>
</tr>
</tbody>
</table>
Azure Instances Templates
The Azure Instances policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Instance Event &gt; Azure Instance State</td>
<td>Identify Azure instances with a specific state.</td>
</tr>
<tr>
<td>Azure Instance by Region</td>
<td>Classify Azure instances by region.</td>
</tr>
<tr>
<td>Azure Instance Delete Protection</td>
<td>Identify Azure instances with Delete Protection enabled.</td>
</tr>
<tr>
<td>Azure Instance Public IP</td>
<td>Identify Azure instances with a public IP address.</td>
</tr>
</tbody>
</table>

Azure VNets Templates
The Azure VNets policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure VNet Event &gt; Azure VNet State</td>
<td>Identify Azure virtual networks with a specific state.</td>
</tr>
</tbody>
</table>

Azure Subscriptions Templates
The Azure Subscriptions policy templates are as follows:

<table>
<thead>
<tr>
<th>Policy Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Subscription Event &gt; Azure Subscription State</td>
<td>Identify Azure subscriptions with a specific state.</td>
</tr>
</tbody>
</table>

Detect Cloud Endpoints – Host Properties
There are many Azure-specific host properties available. Properties are displayed in the Condition dialog box, which can be accessed through the policy templates. In the Console, some properties are also visible in the profile section in the Home tab.

Use host properties to select appropriate conditions for the policy you are creating. Conditions can be optional, but are recommended to filter the policy scope.

Host properties are organized into the following groups:

- Azure Properties
- Azure Local Network Gateway Properties
- Azure Subscription Properties
- Azure VM Properties
- Azure VNet Properties
For more information about setting conditions, refer to the *Forescout Administration Guide*.

**Azure Properties**

**To access the Azure properties:**

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

![Azure Properties](image)

The following properties are available:

<table>
<thead>
<tr>
<th><strong>Azure Account Nickname</strong></th>
<th>Indicates the nickname of the Azure account to which this entity belongs, as internally configured in the Console.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Region</strong></td>
<td>Indicates the region to which the entity belongs. Servers are in different regions, such as eastus.</td>
</tr>
<tr>
<td><strong>Azure Resource Group</strong></td>
<td>Indicates the resource group to which the entity belongs. A resource group holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.</td>
</tr>
<tr>
<td><strong>Azure Resource State</strong></td>
<td>Indicates the most recently reported state of the Azure resource, such as Active or Deleted.</td>
</tr>
<tr>
<td><strong>Azure Resource Tag</strong></td>
<td>Indicates an internal tag to differentiate between Azure, VNet, and subscription hosts.</td>
</tr>
<tr>
<td><strong>Azure Subscription ID</strong></td>
<td>Indicates the subscription ID to which this entity belongs.</td>
</tr>
<tr>
<td><strong>Azure Subscription Name</strong></td>
<td>Indicates the subscription name to which this entity belongs.</td>
</tr>
</tbody>
</table>
Azure Local Network Gateway Properties

To access the Azure Local Network Gateway properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the Azure Local Network Gateway folder in Properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Local Gateway</td>
<td>Indicates the local network gateway address spaces.</td>
</tr>
<tr>
<td>Address Spaces</td>
<td></td>
</tr>
<tr>
<td>Azure Local Gateway</td>
<td>Indicates the Border Gateway Protocol (BGP) setting.</td>
</tr>
<tr>
<td>BGP Setting</td>
<td>The following sub-properties are available:</td>
</tr>
<tr>
<td></td>
<td>• ASN: The Autonomous System number (ASN).</td>
</tr>
<tr>
<td></td>
<td>• Peering IP Address: The peering IP address.</td>
</tr>
<tr>
<td></td>
<td>• Peer Weight: The peer weight.</td>
</tr>
<tr>
<td>Azure Local Gateway ID</td>
<td>Indicates the local network gateway ID.</td>
</tr>
<tr>
<td>Azure Local Gateway IP</td>
<td>Indicates the local network gateway IP address.</td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Azure Local Gateway Name</td>
<td>Indicates the local network gateway name.</td>
</tr>
</tbody>
</table>

Azure Subscription Properties

To access the Azure Subscription properties:

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the Azure Subscription folder in Properties.
The following properties are available:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Subscription Device</strong></td>
<td><strong>Client/App ID</strong></td>
</tr>
<tr>
<td><strong>Tenant ID</strong></td>
<td>Indicates the tenant ID with which this subscription is associated.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Indicates the subscription display name.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Indicates the locations that are accessible to this subscription.</td>
</tr>
<tr>
<td><strong>Sub-properties</strong></td>
<td></td>
</tr>
<tr>
<td>- Location Name</td>
<td>The location name.</td>
</tr>
<tr>
<td>- Location Region</td>
<td>The location region.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Indicates the subscription state, such as Enabled, Disabled, Deleted, PastDue, or Warned.</td>
</tr>
</tbody>
</table>

**Azure VM Properties**

To access the Azure VM properties:

1. When configuring a policy, select Add in the Condition section of the Sub-Rule dialog box.
2. Expand the Azure VM folder in Properties.
The following properties are available:

<table>
<thead>
<tr>
<th><strong>Azure VM Availability Set ID</strong></th>
<th>Indicates the ID of the availability set associated with this virtual machine. The VMs specified in the same availability set are allocated to different nodes to maximize availability.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure VM Delete Protection Enabled</strong></td>
<td>Indicates whether delete protection is enabled on this virtual machine or not. When delete protection is enabled, a lock is in place so an attempt to delete will fail.</td>
</tr>
<tr>
<td>Azure VM Managed Disk</td>
<td>Indicates the managed disk associated with this virtual machine. The following sub-properties are available:</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• ID: The disk ID.</td>
</tr>
<tr>
<td></td>
<td>• Name: The disk name.</td>
</tr>
<tr>
<td></td>
<td>• Type: The disk type.</td>
</tr>
<tr>
<td></td>
<td>• Size in GB: The disk size in GB.</td>
</tr>
<tr>
<td></td>
<td>• SKU: The disk SKU.</td>
</tr>
<tr>
<td></td>
<td>• OS Type: The disk OS type.</td>
</tr>
<tr>
<td></td>
<td>• Availability Zones: The disk availability zones.</td>
</tr>
<tr>
<td></td>
<td>• Creation Method: The disk creation method.</td>
</tr>
<tr>
<td></td>
<td>• Tags: The disk tags.</td>
</tr>
<tr>
<td></td>
<td>• Encryption Enabled: The disk encryption status.</td>
</tr>
<tr>
<td></td>
<td>• Encryption Secret URL: The disk encryption secret URL.</td>
</tr>
<tr>
<td></td>
<td>• Encryption Key Vault: The disk encryption key vault.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Azure VM FQDN</th>
<th>Indicates the Fully Qualified Domain Name (FQDN) associated with the virtual machine.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM ID</th>
<th>Indicates the identity of the Azure virtual machine.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM License Type</th>
<th>Indicates the license type of the virtual machine. The license type is for a Windows server.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Managed Disks Enabled</th>
<th>Indicates whether managed disks are enabled on this virtual machine or not.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Name</th>
<th>Indicates the name of the Azure virtual machine.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Network Security Group</th>
<th>Indicates the Network Security Group (NSG) applied to the virtual machine. An NSG is a list of security rules that allow or deny network traffic to resources connected to Azure VMs, similar to a firewall.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM OS Profile</th>
<th>Indicates the OS profile of the virtual machine, which specifies the operating system settings for the VM. The following sub-properties are available:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Admin User Name: The admin user name of the OS profile.</td>
</tr>
<tr>
<td></td>
<td>• Computer Name: The computer name of the OS profile.</td>
</tr>
<tr>
<td></td>
<td>• Custom Data: The custom data of the OS profile.</td>
</tr>
<tr>
<td></td>
<td>• Linux Configuration: The Linux configuration of the OS profile.</td>
</tr>
<tr>
<td></td>
<td>• Windows Configuration: The Windows configuration of the OS profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Azure VM Power State</th>
<th>Indicates the power state of the virtual machine. Power states include: VM deallocated, VM running, VM deallocated, VM starting, VM stopped, VM stopping, and VM unknown.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Private IP</th>
<th>Indicates the private IP address that identifies the virtual machine.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Provisioning State</th>
<th>Indicates the provisioning state of the virtual machine, such as if the VM has been successfully launched.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Azure VM Public IP</th>
<th>Indicates the public IP address of the virtual machine.</th>
</tr>
</thead>
</table>
### Azure VM Real Name
Indicates the Azure virtual machine real name of the endpoint. You can create a tag for a name that is different from the Azure VM Name.

### Azure VM State
Indicates the most recent state of the Azure virtual machine, such as Running, Starting, Stopping, Stopped, Deallocating, Deallocated, or Terminated. This state may be influenced by the query interval configured for the connection of the Forescout platform to Azure.

### Azure VM Tags
Indicates the tags given to the Azure virtual machine. The following sub-properties are available:
- Tag Name: The name of the tag.
- Tag Value: The value of the tag.

### Azure VM Size Type
Indicates the size and type of the virtual machine, for example, the CPU, memory, and storage disk.

### Azure VM VNet
Indicates the virtual network to which the virtual machine is attached. When a VM launches, it attaches to a VNet. Multiple VMs can attach to a VNet. Azure VNet enables many types of Azure resources, such as Azure VMs, to securely communicate with each other, the Internet, and on-premises networks. The following sub-properties are available:
- VNet ID: The VNet ID.
- Name: The VNet name.

---

## Azure VNet Properties

**To access the Azure VNet properties:**

1. When configuring a policy, select **Add** in the Condition section of the Sub-Rule dialog box.
2. Expand the Azure VNet folder in Properties.
The properties are as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VNet Address Spaces</strong></td>
<td>Indicates the address spaces associated with this virtual network. Multiple IP address ranges can be configured and can be checked for conflicts.</td>
</tr>
<tr>
<td><strong>VNet DDoS Protection Plan ID</strong></td>
<td>Indicates the ID of the Distributed Denial of Service (DDoS) protection plan if DDoS protection is enabled on this virtual network.</td>
</tr>
<tr>
<td><strong>VNet DDoS Protection Enabled</strong></td>
<td>Indicates whether DDoS protection is enabled on this virtual network or not.</td>
</tr>
<tr>
<td><strong>VNet DNS Server IPs</strong></td>
<td>Indicates the Domain Name Server (DNS) IP addresses configured on this virtual network.</td>
</tr>
<tr>
<td><strong>VNet Gateways</strong></td>
<td>Indicates the VNet gateway defined on the virtual network. The following sub-properties are available:</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway ID: The virtual network gateway ID.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway Name: The virtual network gateway name.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway VPN Type: The VPN type of the virtual network gateway.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway Type: The virtual network gateway type.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway SKU: The virtual network gateway SKU.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway Active-active Mode Enabled: Whether the active-active mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway BGP Enabled: Whether BGP is enabled.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway IP Configuration: The virtual network gateway IP address configuration.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway VPN Connections: The virtual network gateway VPN connections.</td>
</tr>
<tr>
<td></td>
<td>- VNet Gateway BGP Setting: The BGP setting.</td>
</tr>
</tbody>
</table>
VNet ID | Indicates the stable and unique string that identifies the virtual network.
---|---
VNet Name | Indicates the name that identifies the virtual network.
VNet Route Tables | Indicates the route tables defined on the virtual network. The following sub-properties are available:  
  - Route Table Name: The name of the route table.  
  - Routes: The routes of the route table.
VNet Subnets | Indicates the subnets defined under the virtual network. The following sub-properties are available:  
  - Address Space: The address space of the subnet.  
  - Subnet Name: The subnet name.  
  - IP Configuration Count: The network interface IP configuration count.  
  - Network Security Group ID: The network security group ID.  
  - Route Table Name: The route table name of this subnet.  
  - VNet Gateway Name: The VNet gateway name of this subnet.
VNet VM Protection Enabled | Indicates whether VM protection is enabled for all the subnets in this virtual network or not.

**View Asset Inventory**

Once the Azure 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 Inventory Detections* in the *Forescout Administration Guide* or the Online Help for information about how to work with the Asset Inventory.

**Access Azure Inventory**

Use the Azure inventory to view information on Azure regions and resource groups.
To access the Azure inventory:

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

2. In the Views pane, select **Azure** and expand the folder.

3. Select an item from the folder, such as Azure Resource Group. The real-time inventory information is displayed. To view details, select a specific Azure instance.

4. To view more inventory information, select another Azure item, for example, Azure Resource Tag, Azure Subscription Name, Azure Region, or a specific region.
Access Azure Subscription Inventory

Use the Azure subscription inventory to view subscription-related information, such as Azure subscription states.

To access the Azure Subscription inventory:

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

2. In the Views pane, select Azure Subscription and expand the folder.

3. Select an item from the folder, such as Azure Subscription State. The real-time inventory information is displayed. To view details, select a specific Azure instance.

4. To view more inventory information, select another Azure Subscription item, for example, Azure Subscription Device Client/App ID.
Access Azure VM Inventory

Use the Azure VM inventory to view VM-related information, such as Azure VM states.

To access the Azure VM inventory:

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

2. In the Views pane, select Azure VM and expand the folder.

3. Select an item from the folder, such as Azure VM State. The real-time inventory information is displayed. To view details, select a specific Azure instance.
4. To view more inventory information, select another Azure VM item, for example, Azure VM Delete Protection Enabled, Azure VM Size Type, Azure VM Tags, or Azure VM VNet.

**Access Azure VNet Inventory**

Use the Azure VNet inventory to view VNet-related information.

**To access the Azure VNet inventory:**

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

2. In the Views pane, select **Azure VNet** and expand the folder.

3. Select an item from the folder, such as VNet VM Protection Enabled. The real-time inventory information is displayed. To view details, select a specific Azure instance.

4. To view more inventory information, select another Azure VNet item, for example, VNet DDoS Protection Enabled.
Run Azure Policy Actions

Use policy actions to perform actions for the policy you are creating. The actions provide visibility and control of Azure.

Actions are displayed in the Action pane, which is accessed through the policy templates. While Azure actions can be launched as part of a policy, you can also manually run an action.

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

**To manually run an Azure 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 **Azure**, and select an action.
4. For information on Azure actions, see:
   - Enable Azure Instance Delete Protection Action
   - Disable Azure Instance Delete Protection Action
   - Start Azure Instance Action
   - Stop Azure Instance Action
   - Restart Azure Instance Action

**Enable Azure Instance Delete Protection Action**

Use this action to enable delete protection on an Azure instance. The type of management lock is delete. Multiple management locks of the same type can be created on the same resource. Any delete lock prevents the resource from being deleted.

When enabling delete protection, this action checks if a delete lock already exists. If the lock exists, no further action is performed. If the lock does not exist, the lock is created.
To enable Azure instance delete protection:

1. Log in to the Console, select Home, and select All Hosts.
2. In the All Hosts pane, right-click an endpoint, select Azure, and select Enable Azure Instance Delete Protection.

3. In the Action Schedule section, select one of the following:
   - **Start action when the endpoint matches a policy condition**, which implements the policy when the policy conditions are met by the endpoint.
   - **Customize action start time**, which opens the Action Scheduler dialog box.
4. Set parameters and select **OK**.

5. In the Specify Enable Azure Instance Delete Protection parameters dialog box, select **OK**.

### Disable Azure Instance Delete Protection Action

Use this action to disable delete protection on an Azure instance. The type of management lock is delete. Multiple management locks of the same type can be created on the same resource. Any delete lock prevents the resource from being deleted.

When disabling delete protection, this action checks if one or more delete locks already exist on the resource. If a lock does not exist, no further action is performed. Any existing locks are deleted, including locks not created by the Azure Plugin.

**To disable Azure instance delete protection:**

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

2. In the All Hosts pane, right-click an endpoint, select **Azure**, and select **Disable Azure Instance Delete Protection**.
3. In the Action Schedule section, select one of the following:

- **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.
4. Set parameters and select **OK**.

5. In the Specify Disable Azure Instance Delete Protection parameters dialog box, select **OK**.

### Start Azure Instance Action

Use this action to start (power on) a stopped Azure VM instance. The instance is not in the running state and then it is started.

**To start an Azure instance:**

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **Azure**, and select **Start Azure Instance**.
3. In the Action Schedule section, select one of the following:

- **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.
4. Set parameters and select **OK**.

5. In the Specify Start Azure Instance parameters dialog box, select **OK**.

**Stop Azure Instance Action**

Use this action to stop (power off) a running Azure VM instance. The instance is in the running state and then it is stopped. The stopped state is not a de-allocated state.

**To stop an Azure instance:**

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

2. In the All Hosts pane, right-click an endpoint, select **Azure**, and select **Stop Azure Instance**.
3. In the Action Schedule section, select one of the following:

   - **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.
4. Set parameters and select **OK**.

5. In the Specify Stop Azure Instance parameters dialog box, select **OK**.

**Restart Azure Instance Action**

Use this action to restart an Azure VM instance. The instance is in the running state and then it is restarted.

- The restart action has no effect on Azure VM instances that are in the stopped state.

To restart an Azure instance:

1. Log in to the Console, select **Home**, and select **All Hosts**.
2. In the All Hosts pane, right-click an endpoint, select **Azure**, and select **Restart Azure Instance**.
3. In the Action Schedule section, select one of the following:

   - **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.
4. Set parameters and select OK.

5. In the Specify Restart Azure Instance parameters dialog box, select OK.

**Hybrid Cloud Module Information**

The Azure 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 Forescout Resources Page, or 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 Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:


Product Updates Portal

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

To access the Product Updates Portal:


Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.
To access documentation on the Forescout Customer 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.

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

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

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

Forescout Administration Guide

- Select Forescout Help from the Help menu.

Plugin Help Files

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

Online Documentation

- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).