Monitoring Microsoft Azure

Microsoft: Azure PowerPack version 104

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Microsoft Azure resources that are managed with Azure Resource Manager (ARM) in the ScienceLogic platform using the *Microsoft: Azure* PowerPack.

NOTE: For information about monitoring Azure resources that are managed with the Azure Classic portal, see the ***Monitoring Microsoft Azure Classic*** manual.

The following sections provide an overview of Microsoft Azure and the *Microsoft: Azure* PowerPack:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Azure?

Azure is a Microsoft service that provides both infrastructure and platform capabilities for cloud computing. Azure enables users to build, deploy, and manage applications and services using Microsoft data centers, and offers users numerous capabilities such as website hosting, virtual machine creation, data management, business analytics, and media services.

Microsoft offers two methods for managing Azure resources: Azure Resource Manager (ARM) portal and the Azure Classic portal.

What Does the Microsoft: Azure PowerPack Monitor?

To monitor Microsoft ARM resources using the ScienceLogic platform, you must install the *Microsoft: Azure* PowerPack. This PowerPack enables you to discover, model, and collect data about ARM resources.

The *Microsoft: Azure* PowerPack includes:

- Example credentials you can use as templates to create SOAP/XML credentials to connect to ARM
- Dynamic Applications to discover, model, and monitor performance metrics and/or collect configuration data for the following ARM resources:
    - Active Directory tenants
    - Application gateways
    - Load balancers
    - Network security groups
    - Recovery Services vaults
    - Resource groups
    - SQL databases
    - SQL servers
    - Storage accounts
    - Traffic Manager profiles
    - Virtual machines
    - Virtual network subnets
    - Virtual networks
    - VPN gateways
- Device Classes for each Azure data center location and all of the ARM resources the ScienceLogic platform monitors
- Event Policies and corresponding alerts that are triggered when ARM resources meet certain status criteria

NOTE: The *Microsoft: Azure* PowerPack does not currently monitor Azure Government cloud resources or resources that use IPv6.

What are Azure Locations?

An Azure location is an individual data center located in a specific geographic locale. The Dynamic Applications in the *Microsoft: Azure* PowerPack create a "location" component device for each discovered data center location.

The PowerPack supports the following Azure data center locations:

- Australia East (New South Wales)
- Australia Southeast (Victoria)
- Brazil South (Sao Paulo)
- Canada Central (Toronto)
- Canada East (Quebec)
- Central India (Pune)
- Central US (Iowa)
- East Asia (Hong Kong)
- East US (Virginia)
- East US 2 (Virginia)
- Germany Central (Frankfurt)
- Germany Northeast (Magdeburg)
- Japan East (Saitama)
- Japan West (Osaka)
- Korea Central (Seoul)
- Korea South (Busan)
- North Central US (Illinois)
- North Europe (Ireland)
- South Central US (Texas)
- South India (Chennai)
- Southeast Asia (Singapore)
- UK South (London)
- UK West (Cardiff)
- West Central US
- West Europe (Netherlands)
- West India (Mumbai)

- West US (California)
- West US 2

Installing the Microsoft: Azure PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Microsoft: Azure* PowerPack.

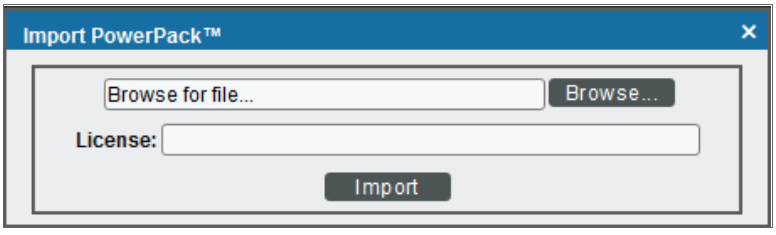
NOTE: If you are already using the ScienceLogic platform to monitor Azure Classic and/or ARM resources, you must upgrade to the latest version of the *Microsoft: Azure Classic* PowerPack before using the *Microsoft: Azure* PowerPack to monitor ARM resources.

NOTE: The following instructions describe how to install the *Microsoft: Azure* PowerPack for the first time. If you are upgrading to the latest version from a previous version, see the ***Microsoft: Azure* PowerPack** Release Notes for specific upgrade instructions.

To download and install a PowerPack:

TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuring Azure for Monitoring

Overview

The following sections describe how to configure Microsoft Azure resources for monitoring by the ScienceLogic platform using the *Microsoft: Azure* PowerPack:

Configuring an Azure Active Directory Application

To create a SOAP/XML credential that allows the ScienceLogic platform to access Microsoft Azure, you must know the following information about an Active Directory application in your Azure account:

- Application ID
- Subscription ID (if monitoring a single subscription)
- OAuth 2.0 token endpoint URL
- Tenant ID
- Secret key

To capture the above information, you must first create (or already have) an Azure Active Directory registered application with Reader or Contributor access. You can then enter the required information about the application when configuring the SOAP/XML credential in the platform.

Creating an Active Directory Application in the Azure Portal

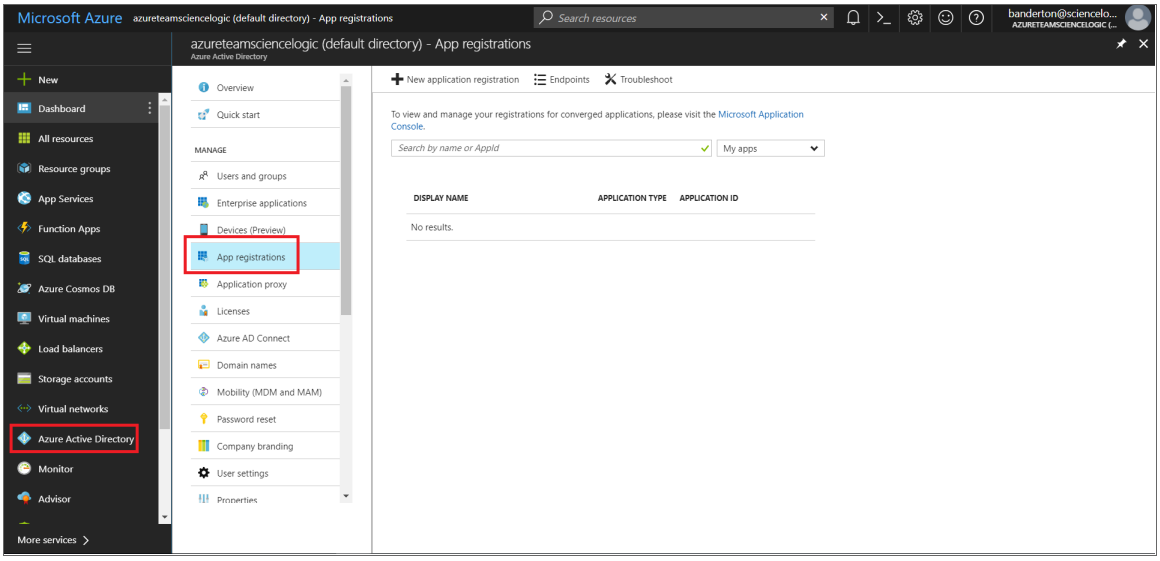
When configuring a SOAP/XML credential in the ScienceLogic platform, you must provide the application ID, subscription ID, OAuth 2.0 token endpoint URL, tenant ID, and secret key of the Azure Active Directory application you will use to authenticate your Azure account.

NOTE: You must have Service Administrator rights to create an Azure Active Directory application.

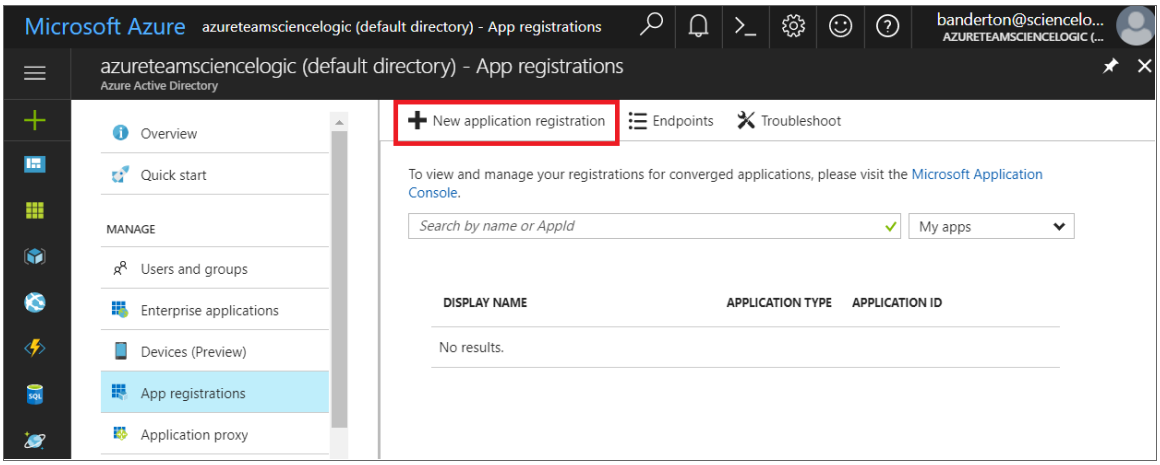
To create an Active Directory application in the Azure Portal:

1. Log in to the Azure portal at https://portal.azure.com.

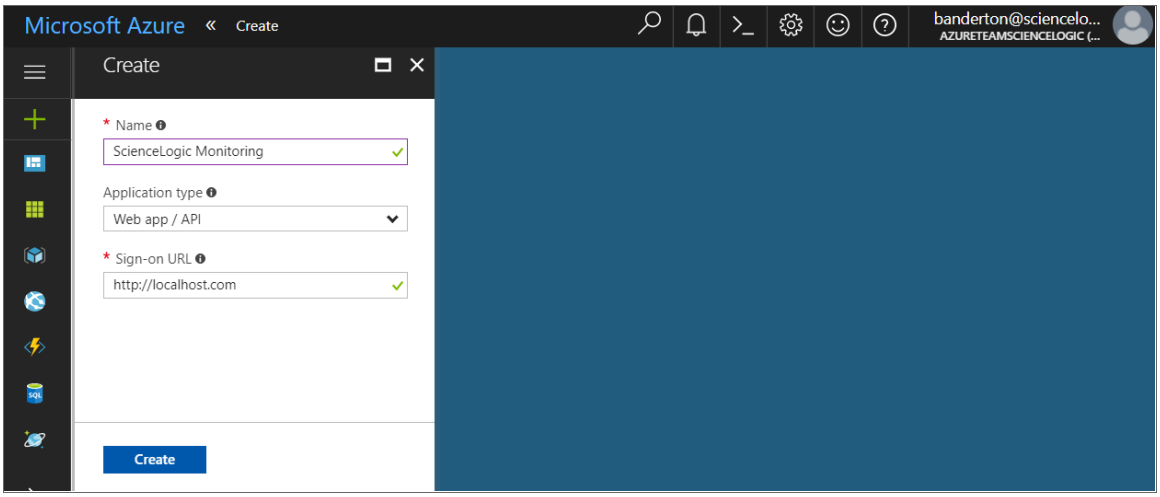
2. From the left panel, click **[Azure Active Directory]**, then click **App registrations**. The **App registrations** page appears:



3. Click the **[New application registration]** button.



4. Enter a ***Name*** for the application and select *Web app / API* in the ***Application Type*** field. In the ***Sign-On URL*** field, enter any valid URL, then click the **[Create]** button.



5. A message appears confirming that your application was added.

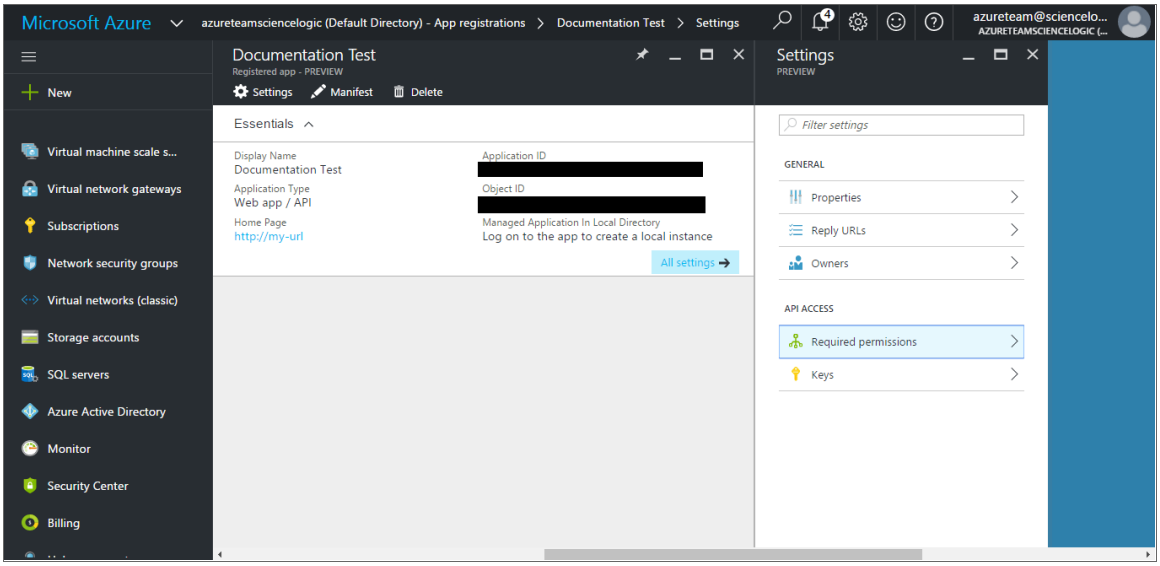
Adding the Microsoft Graph and Windows Azure Active Directory APIs

You must add the Microsoft Graph and Windows Azure Active Directory application programmable interfaces (APIs) to the Azure Active Directory application you will use to authenticate your Azure account. At a minimum, the Microsoft Graph and Windows Azure Active Directory APIs must have permission to read directory data.

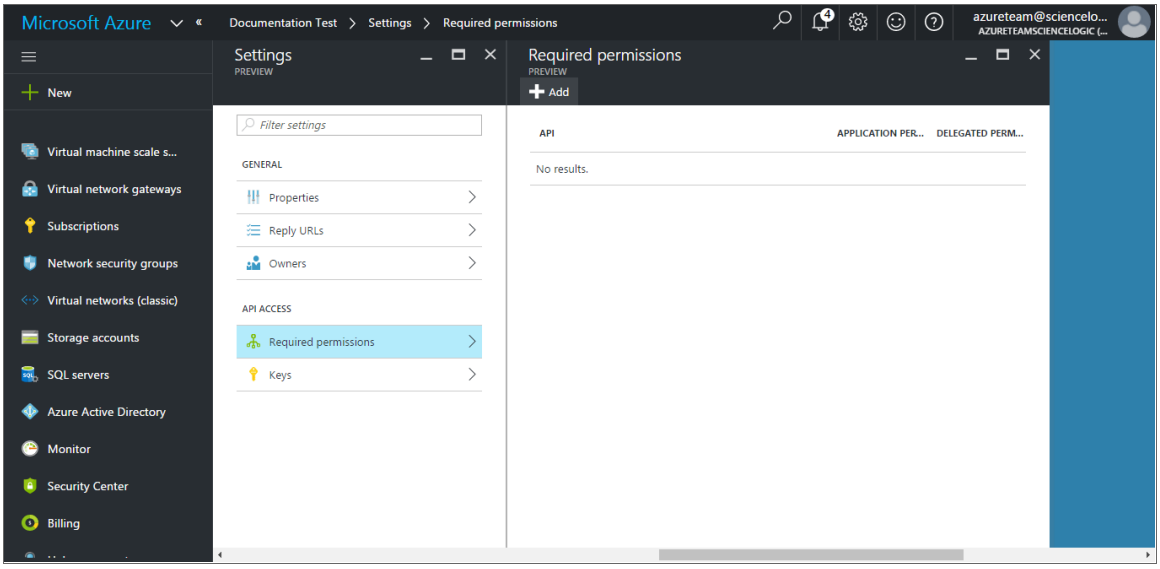
To add the Microsoft Graph and Windows Azure Active Directory APIs:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Azure Active Directory]**.
2. Click **[App registrations]**, then click on the name of the Azure Active Directory application you will use to authenticate your Azure account.

3. In the **Settings** pane, under **API Access**, click **[Required permissions]**.

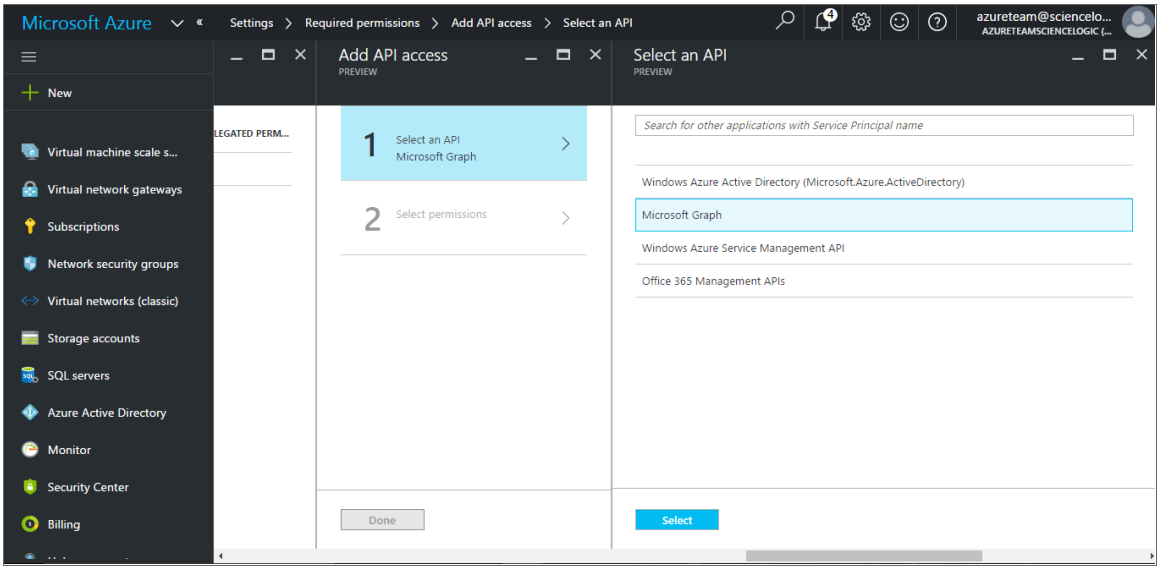


4. In the **Required permissions** pane, click **[Add]**.

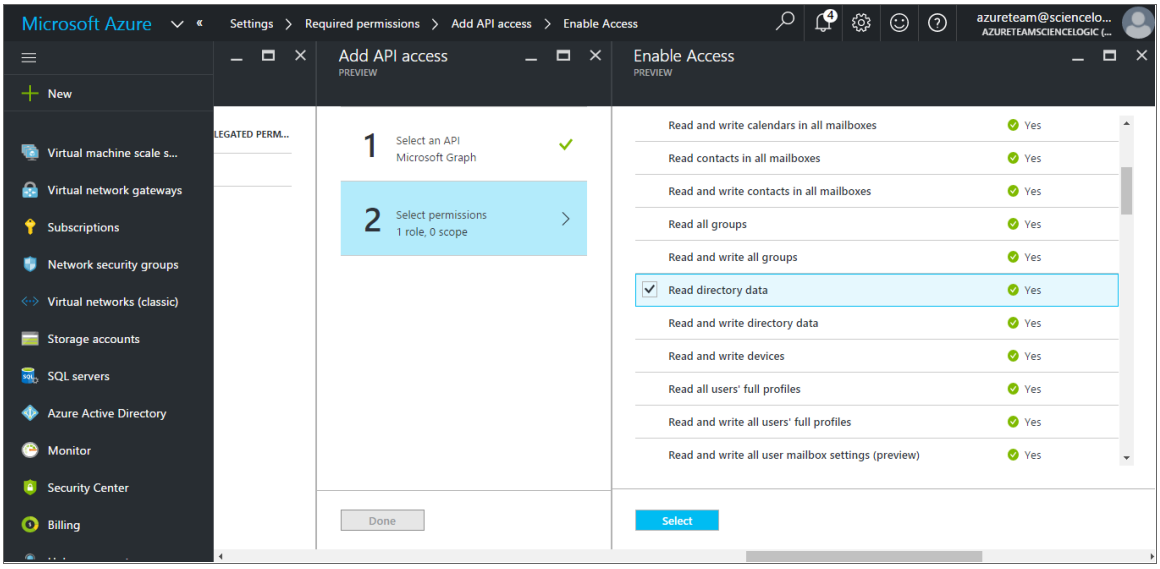


5. In the **Add API access** pane, click **[Select API]**.

6. In the **Select an API** pane, choose *Microsoft Graph*. Click **[Select]**.



7. In the **Enable access** pane, under **Application Permissions**, select *Read directory data*. Click **[Select]**.



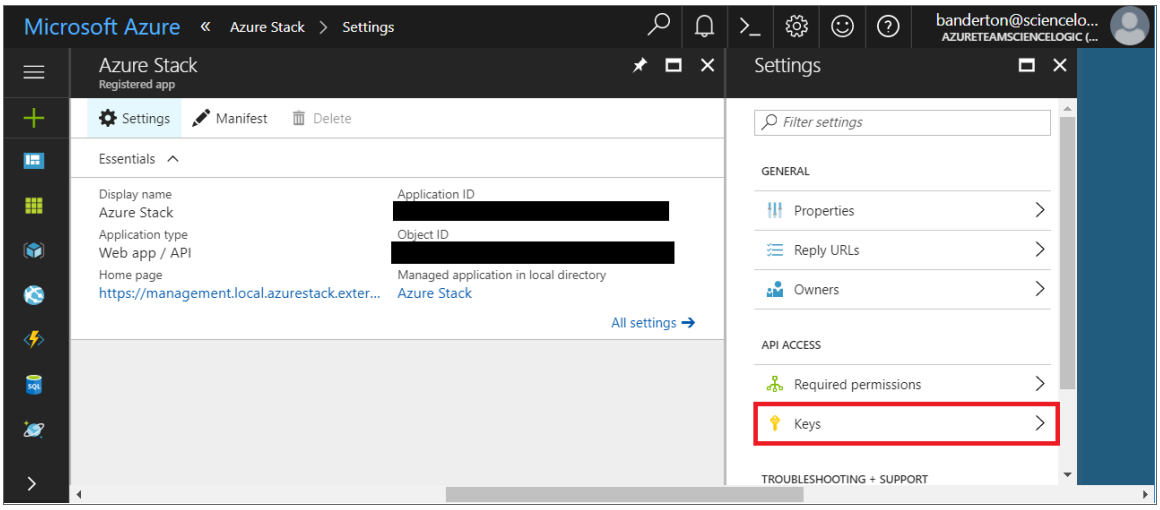
8. Click **[Done]** to save.
9. Repeat these steps for the Windows Azure Active Directory API. To do so, choose *Windows Azure Active Directory* (rather than *Microsoft Graph*) in step 6.
10. After you add the Microsoft Graph and Windows Azure Active Directory APIs, return to the **Required permissions** pane and click **[Grant Permissions]**.

Generating the Secret Key

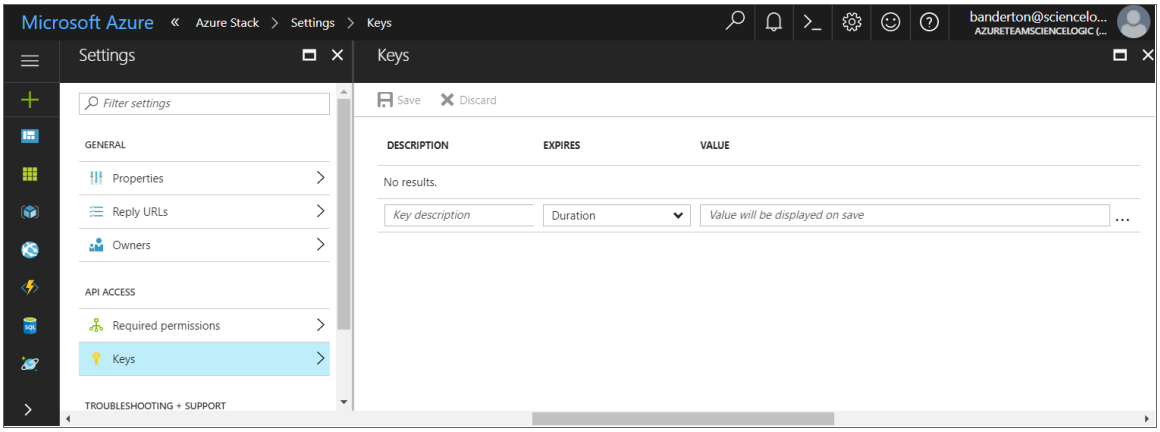
When configuring a SOAP/XML credential for Azure in the ScienceLogic platform, you need to provide a secret key for the Azure Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. In the left pane of the Azure portal (https://portal.azure.com), click **Active Directory**, then click **App registrations**.
2. Click the application name.
3. In the **Settings** pane, click **[Keys]**.



4. In the **Keys** pane, enter a name in the ***Key Description*** field and select a duration in the ***Expires*** field.
5. Click **[Save]** to generate the secret key.



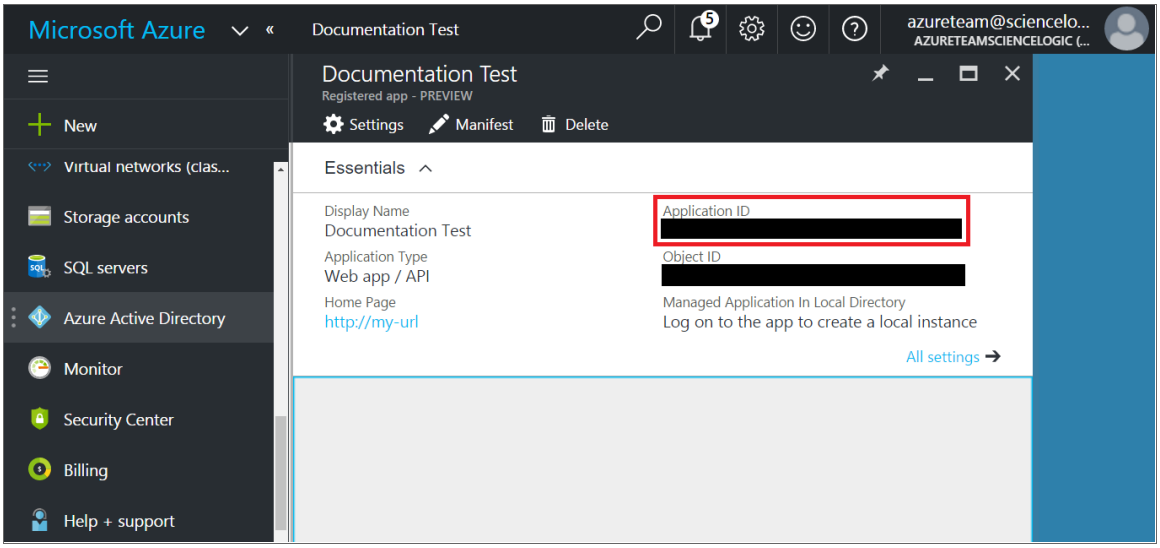
6. Copy and save the key value.

Locating the Application ID

When configuring a SOAP/XML credential for Azure in the ScienceLogic platform, you need to provide the Application ID of the Azure Active Directory application you will use to authenticate your Azure account.

To locate the Application ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Azure Active Directory]**.
2. Click **[App registrations]**, then click on the name of the Active Directory application you will use to authenticate your Azure account. The Application ID appears in the **Essentials** section.



3. Copy and save the ***Application ID***.

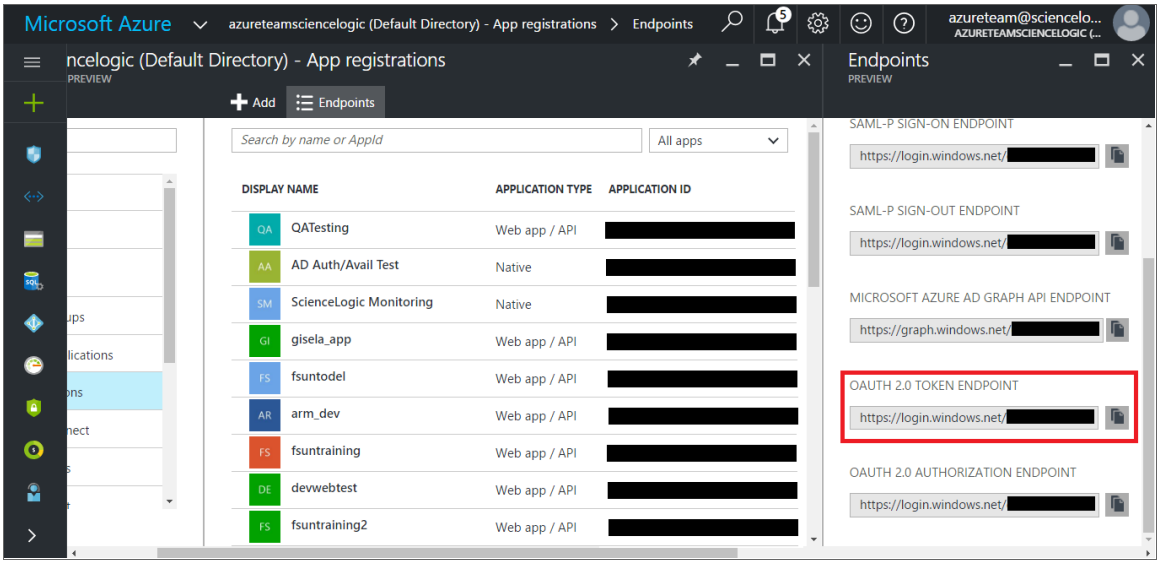
Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID

When configuring a SOAP/XML credential for Azure in the ScienceLogic platform, you need to provide the OAuth 2.0 token endpoint URL and the tenant ID of the Azure Active Directory application you will use to authenticate your Azure account.

To locate the OAuth 2.0 token endpoint URL and the tenant ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Azure Active Directory]**.

2. Click **[App registrations]**, then click **[Endpoints]**. The ***OAUTH 2.0 TOKEN ENDPOINT*** URL appears in the Endpoints pane.



3. Copy and save the ***OAUTH 2.0 TOKEN ENDPOINT*** URL.
4. The OAuth 2.0 token endpoint URL contains a GUID, a string of characters in the middle of the URL.

   For example, in the following OAuth 2.0 token endpoint URL, the GUID is in bold:
   https://login.windows.net/**eg58975d-1953-5509-4654-b5d4bbga22ceg**/oauth2/token

   Azure uses this GUID as the tenant ID. Copy and save the GUID.

Locating the Subscription ID

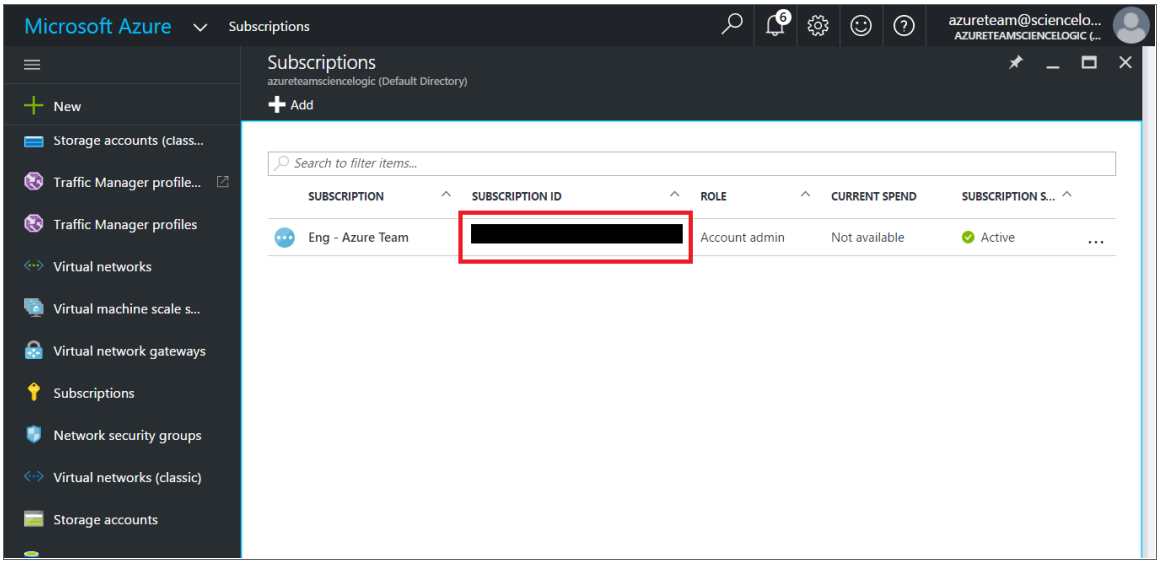
If you are monitoring only a single Azure subscription, you must provide the Subscription ID of the Azure Active Directory application you will use to authenticate your account when you configure your SOAP/XML credential for Azure in the ScienceLogic platform.

NOTE: If you are monitoring an account with multiple child subscriptions, you can skip this section.

To locate the Subscription ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click **[Subscriptions]**.

2. Copy and save the ***Subscription ID*** of the subscription where you created the Azure Active Directory application you will use to authenticate your account.



Adding Reader or Contributor Access to the Active Directory Application

To allow ScienceLogic to access your Azure account, you must specify the type of access the user whose information you will use in your SOAP/XML credential has to the Active Directory application used to authenticate your account.

You can select one of the following access roles:

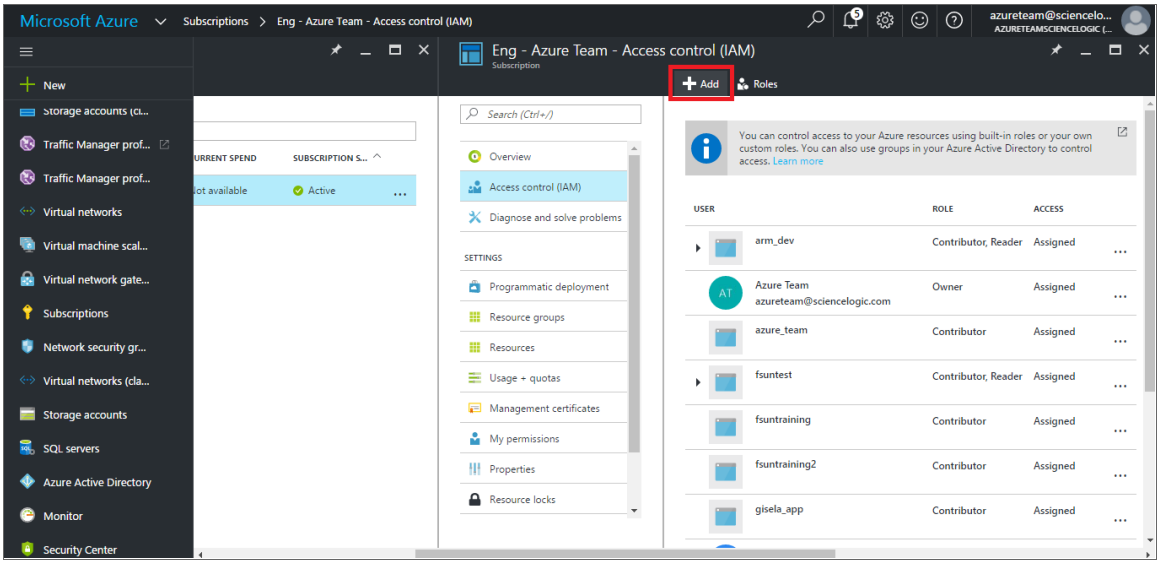
- ***Reader***. This read-only user can view everything but cannot make changes.
- ***Contributor***. This user can read and manage everything in Azure except access rights.

NOTE: You must have Contributor access to collect performance data for Azure storage queues, tables, and blobs.

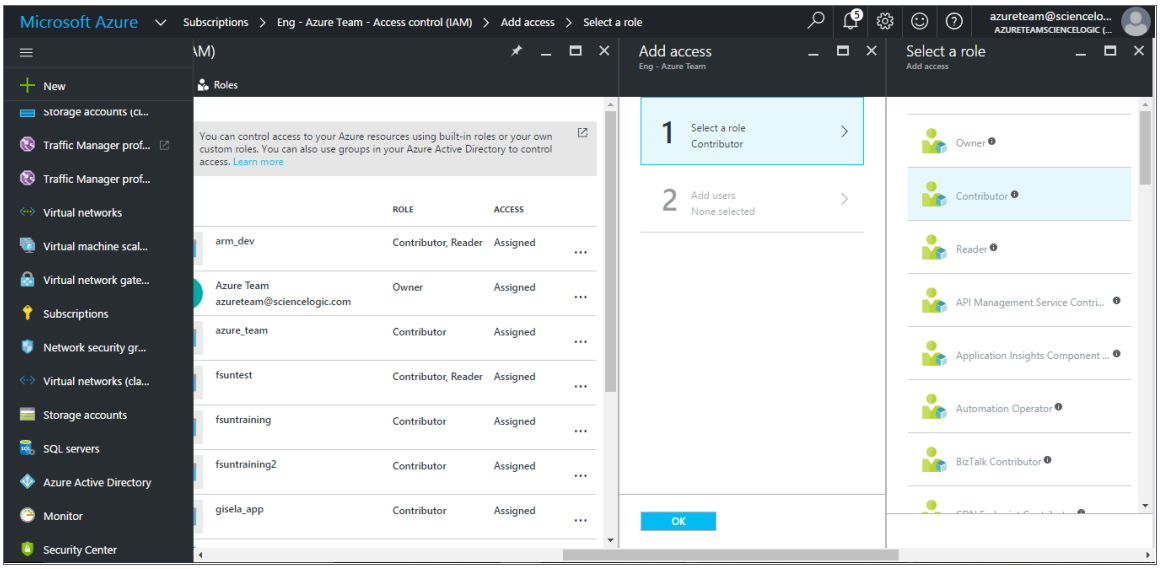
To specify access roles to the Azure Active Directory application:

1. In the left pane of the Azure Portal (https://portal.azure.com), click **[Subscriptions]**.
2. Click the name of your subscription, and then click **[Access control (IAM)]**.

3. In the **Access Control (IAM)** pane, click **[Add]**.

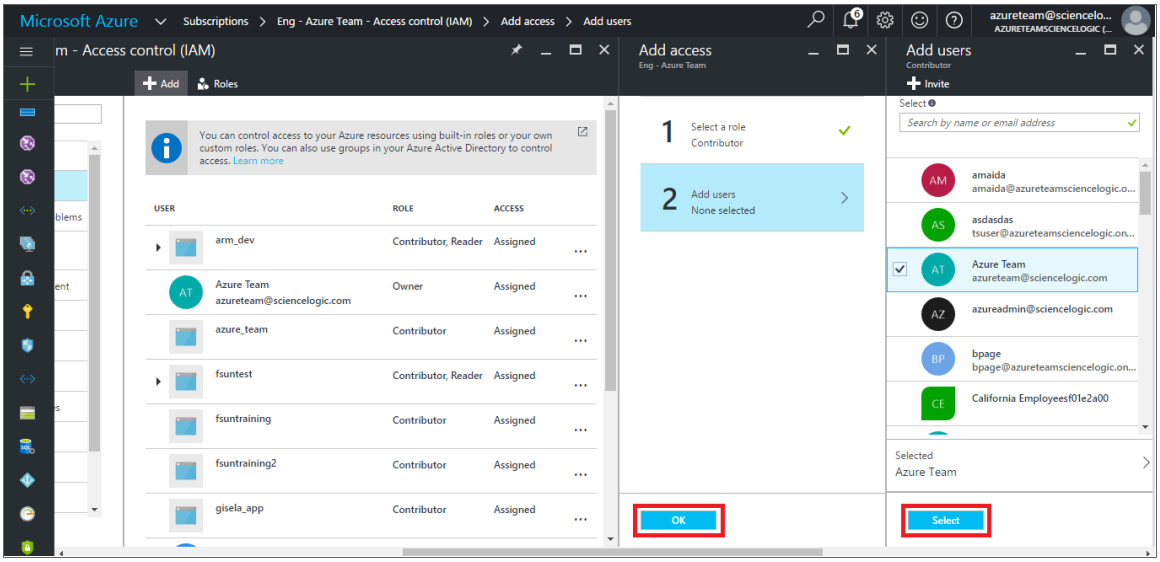


4. In the **Select a role** pane, select *Reader* or *Contributor*.



5. In the **Add users** pane, click the name of the Azure Active Directory application you will use to authenticate your account, and then click **[Select]**.

6. Click **[OK]**.



Setting Up a Proxy Server

Depending on your needs, you can optionally enable the ScienceLogic platform to connect to Azure through a third-party proxy server. With this configuration, the ScienceLogic platform connects to the proxy server, which then connects to Azure. Azure relays information to the proxy server and the platform then retrieves that information from the proxy.

NOTE: You can connect to Azure via a proxy server regardless of whether you are monitoring a single subscription or an account with multiple child subscriptions.

NOTE: The *Microsoft: Azure* PowerPack is certified to work with SQUID version 3.5.12 proxy servers.

If you choose to use this configuration, you will first need to set up the proxy server. To do so:

NOTE: For the following steps, you must have openssh-server.x86_64 and telnet installed.

1. Using SSH, connect to the proxy server.
2. Run the following commands in the command-line interface:

```
sudo apt-get install squid3
cd /etc/squid3
sudo cp squid.conf squid.conf.bak
sudo rm squid.conf
sudo touch squid.conf
sudo vim squid.conf
```

3. Do one of the following, depending on your needs:

    - If you want to connect to the proxy server using basic authentication, add the following lines to the new squid.conf file:

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/passwords
auth_param basic realm proxy
acl authenticated proxy_auth REQUIRED
http_access allow authenticated
http_port [port number]
visible_hostname [hostname]
sudo htpasswd -c /etc/squid3/passwords [username]
[password]
[password]
```

    - If you do not want to use basic authentication to connect to the proxy server, add the following lines to the new squid.conf file:

```
http_access allow all
http_port [port number]
visible_hostname [hostname]
```

4. Restart the SQUID service:

```
sudo service squid3 restart
```

5. Using SSH, connect to the ScienceLogic collector, then telnet to the opened port on the proxy server to verify that the proxy server is set up properly.

Creating a SOAP/XML Credential for Azure

After you know the application ID, subscription ID, OAuth 2.0 token endpoint URL, tenant ID, and secret key of the Active Directory application you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in the ScienceLogic platform. This credential allows the Dynamic Applications in the *Microsoft: Azure* PowerPack to communicate with your Azure subscriptions.

If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential.

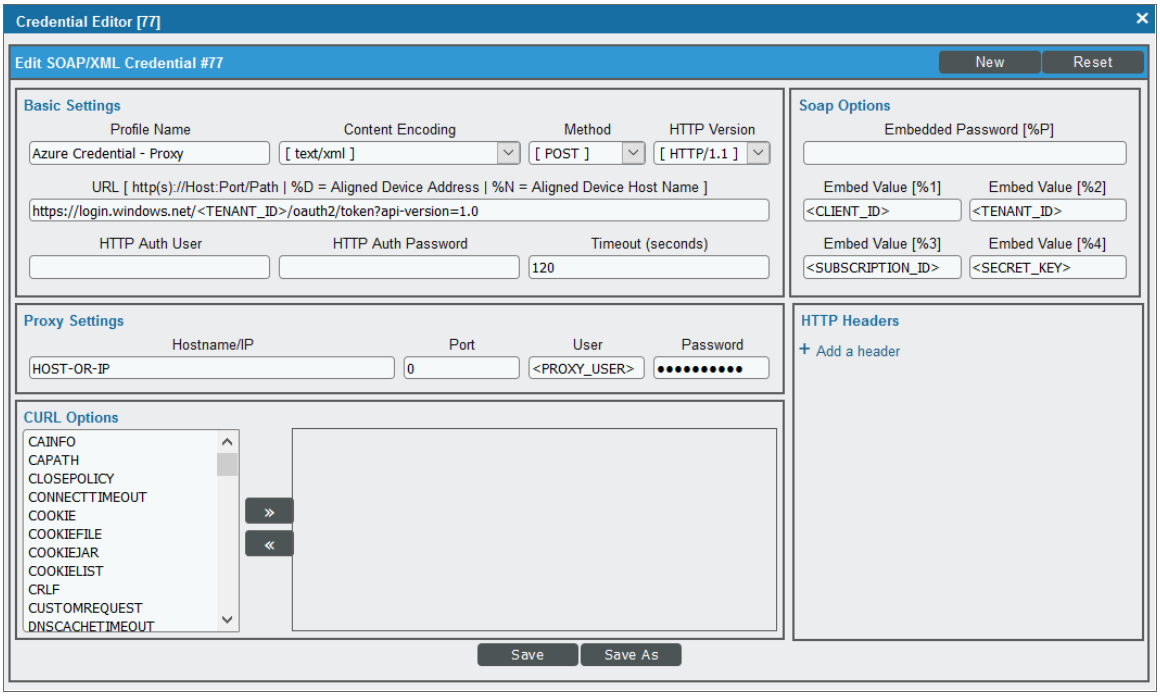
The *Microsoft: Azure* PowerPack includes two sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- **Azure Credential - Proxy**, for users who connect to Azure through a third-party proxy server
- **Azure Credential - SOAP/XML**, for users who do not use a proxy server

TIP: When monitoring an account with multiple child subscriptions, you can load-balance your Azure components by discovering groups of subscriptions and their components across multiple collectors. If you do so, each group of subscriptions must have its own unique virtual root device, credential, collector, collector group, and dynamic component map. You cannot have multiple collectors in a single collector group or discover the same device in multiple dynamic component maps.

To create a SOAP/XML credential for Azure:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Azure Credential - Proxy** or **Azure Credential - SOAP/XML** credential, and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears:



3. Enter values in the following fields:

Basic Settings

- ***Profile Name***. Type a new name for the Azure credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select *POST*.
- ***HTTP Version***. Select *HTTP/1.1*.
- ***URL***. Type the OAuth 2.0 token endpoint URL for the Azure Active Directory application.
- ***HTTP Auth User***. Leave this field blank.

- ***HTTP Auth Password***. Leave this field blank.
- ***Timeout (seconds)***. Type "120".

Proxy Settings

- ***Hostname/IP***. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Azure via a proxy server, type the port number you opened when *setting up the proxy server*. Otherwise, leave this field blank.
- ***User***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

- ***CURL Options***. Do not make any selections in this field.

SOAP Options

- ***Embedded Password [%P]***. Leave this field blank.
- ***Embed Value [%1]***. Type the Application ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Azure Active Directory application.
- ***Embed Value [%3]***. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- ***Embed Value [%4]***. Type the secret key for the Azure Active Directory application.

HTTP Headers

- ***HTTP Headers***. Do not make any selections in this field.

4. Click **[Save As]**.
5. In the confirmation message, click **[OK]**.

Testing the Azure Credential

The ScienceLogic platform includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that the platform can execute on demand to validate whether a credential works as expected.

The Azure Credential Test can be used to test a SOAP/XML credential for monitoring Azure using the Dynamic Applications in the *Microsoft: Azure* PowerPack. The Azure Credential Test performs the following steps:

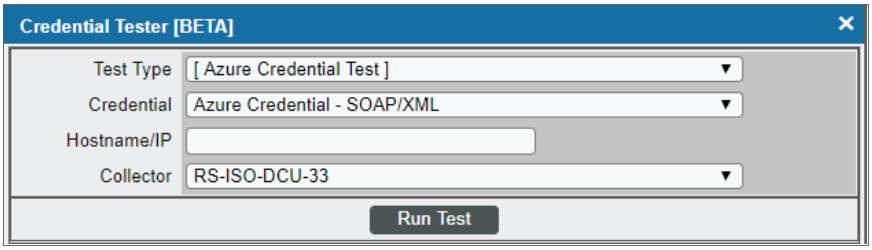
- ***Test Port Availability***. Performs an NMAP request to test the availability of the Azure endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Azure endpoint.

- ***Make connection to Azure account***. Attempts to connect to the Azure service using the account specified in the credential.
- ***Make Azure Active Directory Request***. Verifies that the Azure Active Directory service can be queried.

NOTE: The Azure Credential Test has not been certified for use with credentials that use a proxy server.

To test the Azure credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Locate the **Azure Credential Test** and click its lightning bolt icon ( ). The **Credential Tester** modal page appears:



3. Supply values in the following fields:
   - ***Test Type***. This field is pre-populated with the credential test you selected.
   - ***Credential***. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
   - ***Hostname/IP***. Leave this field blank.
   - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:
   - ***Step***. The name of the step.
   - ***Description***. A description of the action performed during the step.
   - ***Log Message***. The result of the step for this credential test.
   - ***Status***. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).
   - ***Step Tip***. Mouse over the question mark icon ( ) to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".

Chapter 3

Discovering Azure Resources

Overview

The following sections describe how to discover Microsoft Azure resources for monitoring by the ScienceLogic platform using the *Microsoft: Azure* PowerPack.

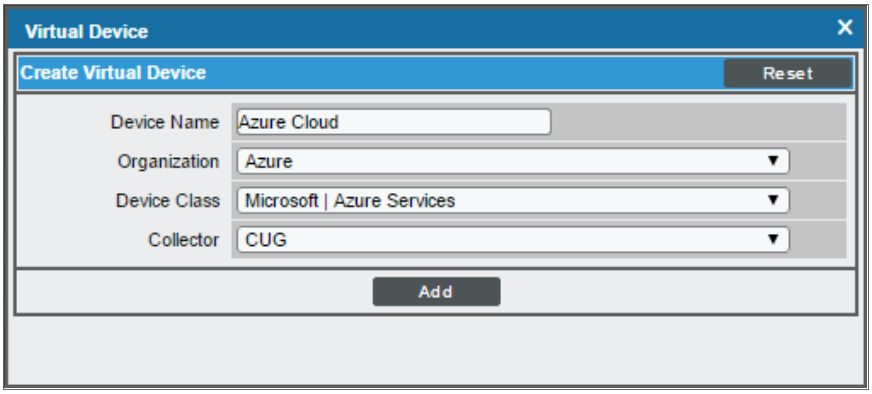
Creating an Azure Virtual Device

Because the Azure service does not have a static IP address, you cannot discover an Azure device using discovery. Instead, you must create a ***virtual device*** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered by the ScienceLogic platform. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Azure service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.

3. Enter values in the following fields:



- ***Device Name***. Enter a name for the device. For example, "Azure Cloud".
- ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- ***Device Class***. Select *Microsoft | Azure Services*.
- ***Collector***. Select the collector group that will monitor the device.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance your Azure components by discovering groups of subscriptions and their components across multiple collectors. If you do so, each group of subscriptions must have its own unique virtual root device, credential, collector, collector group, and dynamic component map. You cannot have multiple collectors in a single collector group or discover the same device in multiple dynamic component maps.

4. Click **[Add]** to create the virtual device.

Aligning the Azure Dynamic Applications

The Dynamic Applications in the *Microsoft: Azure* PowerPack are divided into the following types:

- ***Discovery***. These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- ***Configuration***. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- ***Performance***. These Dynamic Applications poll Azure for performance metrics.

When configuring the ScienceLogic platform to monitor Azure services, you can manually align Dynamic Applications to discover Azure component devices.

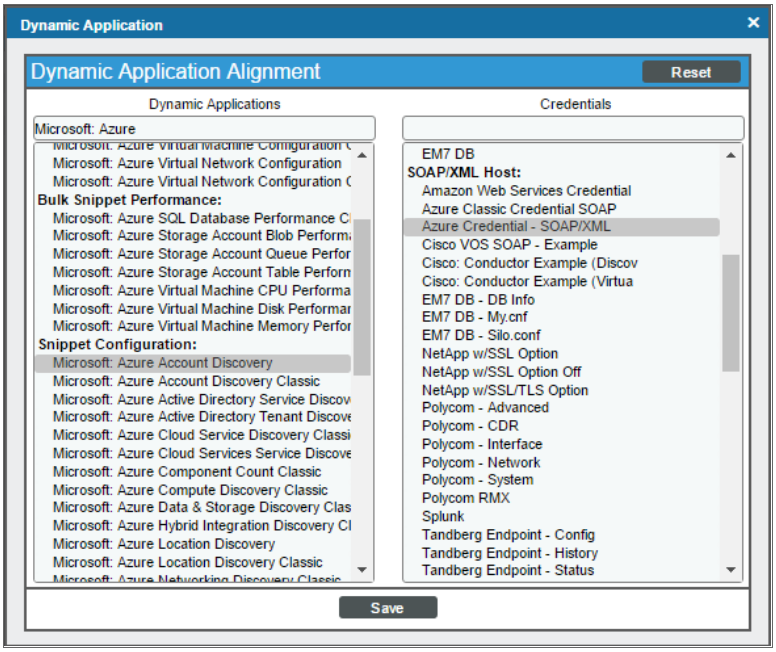
Discovering Azure Component Devices

To discover all the components of your Azure platform, you must manually align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device.

TIP: When monitoring an account with multiple child subscriptions, ScienceLogic recommends that you first review your device capacity and load limits to determine the best method for implementation prior to discovery.

To manually align the "Microsoft: Azure Account Discovery" Dynamic Application:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon ( ) for your Azure virtual device.
3. In the ***Device Administration*** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Actions]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:



   - In the ***Dynamic Applications*** field, select *Microsoft: Azure Account Discovery*.
   - In the ***Credentials*** field, select the credential you created for your Azure service.
6. Click **[Save]** to align the Dynamic Application with the Azure virtual device.

When you align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device, the ScienceLogic platform does one of the following, depending on your subscription model:

- If you are monitoring an account with multiple child subscriptions, the platform creates a root component device representing the Azure account and one or more child component devices representing all of your Azure subscriptions.
- If you are monitoring a single subscription, the platform creates a root component device representing your Azure subscription.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance your Azure components by discovering groups of subscriptions and their components across multiple collectors. If you do so, each group of subscriptions must have its own unique virtual root device, credential, collector, collector group, and dynamic component map. You cannot have multiple collectors in a single collector group or discover the same device in multiple dynamic component maps.

The ScienceLogic platform then automatically aligns several other Dynamic Applications to the subscription component devices. These additional Dynamic Applications discover and create component devices for Active Directory tenants, Traffic Manager profiles, and each location used by the Azure account.

Under each location, the ScienceLogic platform then discovers the following component devices:

- Application Gateway Services
    - Application Gateways
- Resource Groups Services
    - Resource Groups
- Storage Services
    - Storage Accounts
- Virtual Machines Services
    - Virtual Machines
- Virtual Network Services
    - VPN Gateways
    - Virtual Networks
        - Virtual Network Subnets
- SQL Server Services
    - SQL Servers
    - SQL Databases
- Recovery Service Vaults Services
    - Recovery Service Vaults
- Network Security Group Services
    - Network Security Groups

- Load Balancer Services
    - Load Balancers

NOTE: The ScienceLogic platform might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

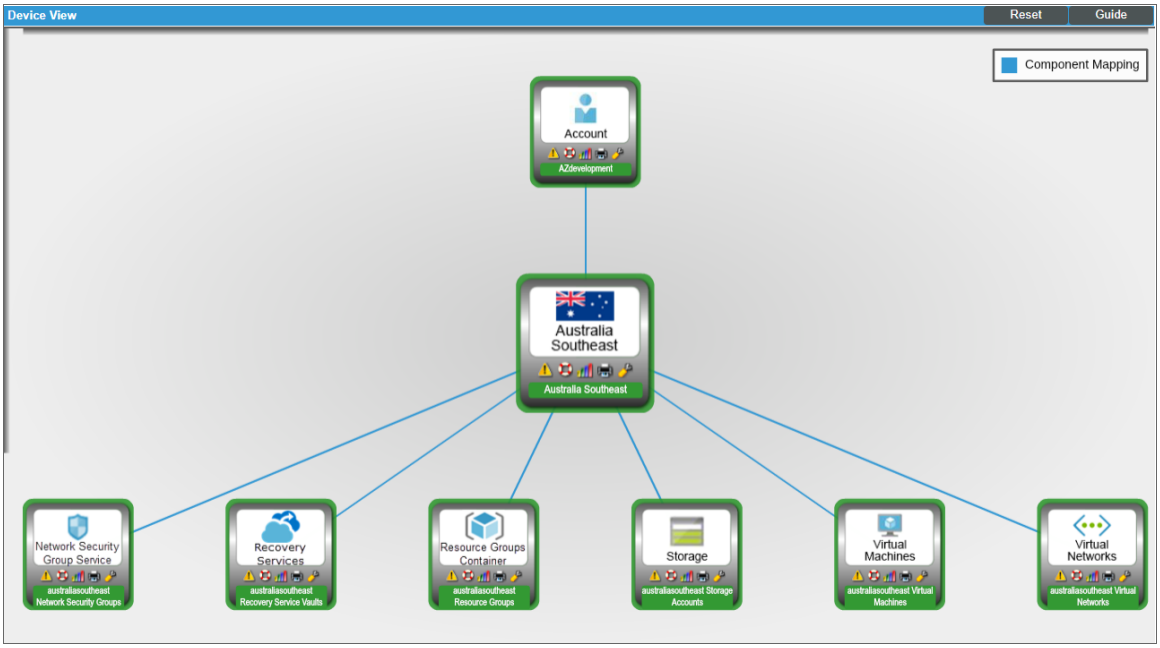
NOTE: When discovering a large number of component devices, such as when discovering an account with multiple child subscriptions, the discovery process can cause the appearance of numerous critical events with the message, "`Large backlog of asynchronous jobs detected`". This will occur only during the initial discovery session.

Viewing Azure Component Devices

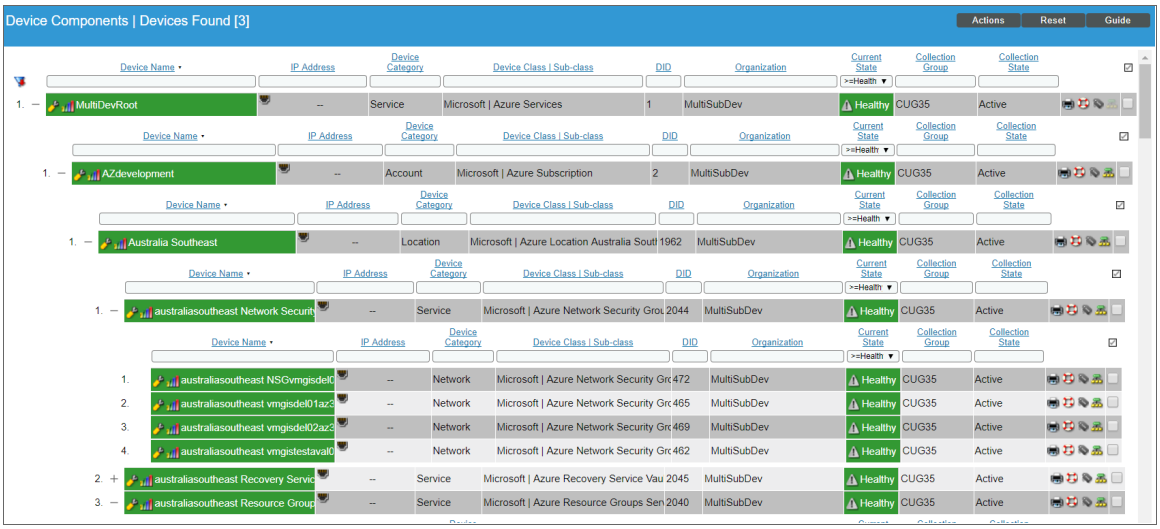
In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the Azure service and all associated component devices in the following places in the user interface:

NOTE: If you are using both the *Microsoft: Azure* and *Microsoft: Azure Classic* PowerPacks to monitor resources in the same Azure subscription, duplicate Active Directory and SQL database component devices will appear in the ARM and Classic component maps in the ScienceLogic platform.

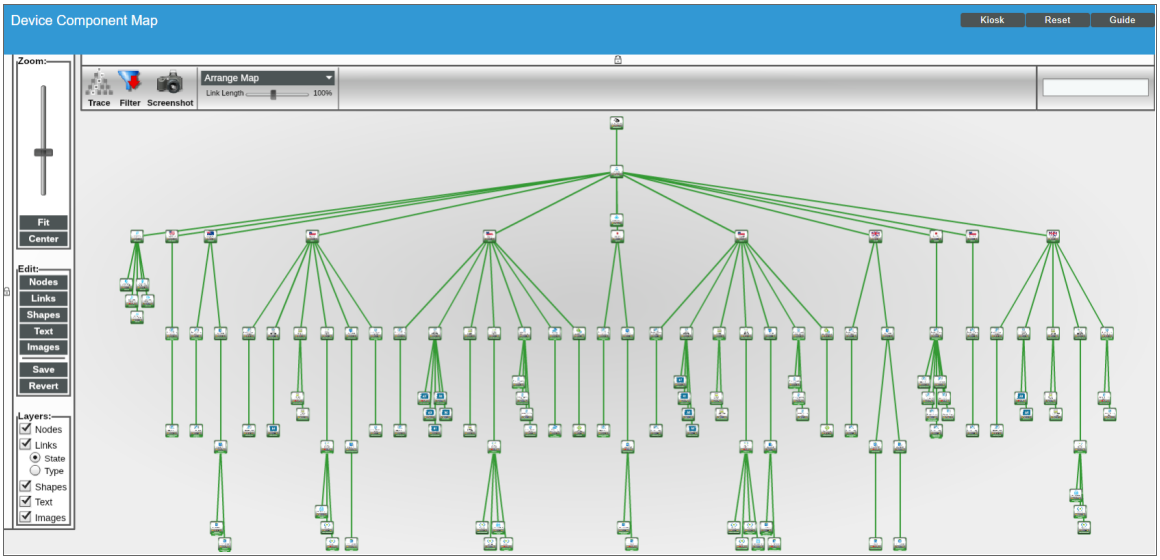
- The **Device View** modal page (click the bar-graph icon [] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an Azure service, find the Azure virtual device and click its plus icon (+):



- The **Component Map** page (Views > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. The ScienceLogic platform automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for an Azure service, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Relationships Between Component Devices

In addition to parent/child relationships between component devices, the ScienceLogic platform also creates relationships between the following component devices:

- Virtual Machines and Storage Accounts
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups
- Virtual Machines and Virtual Networks
- Virtual Machines and Subnets
- Application Gateways and Subnets
- Application Gateways and Resource Groups
- VPN Gateways and Subnets
- VPN Gateways and Resource Groups
- Storage Accounts and Resource Groups
- Virtual Networks and Resource Groups
- SQL Servers and Resource Groups
- SQL Databases and Resource Groups
- Traffic Manager Profiles and Resource Groups
- Azure Traffic Managers and Traffic Managers
- Network Security Groups and Resource Groups
- Network Security Groups and Virtual Network Subnets
- Recovery Service Vaults and Resource Groups

Additionally, the platform can automatically build relationships between Azure component devices and other associated devices:

- If you discover Cisco Cloud Center devices using the Dynamic Applications in the *Cisco: Cloud Center* PowerPack version 103 or later, the platform will automatically create relationships between Azure Virtual Machines and Cisco Cloud Center applications.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010