Monitoring Microsoft Azure Classic

Microsoft: Azure Classic PowerPack version 3.5

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Microsoft Azure resources that are managed with the Azure Classic portal in the ScienceLogic platform using the *Microsoft: Azure Classic* PowerPack.

NOTE: For information about monitoring Azure resources that are managed with Azure Resource Manager (ARM), see the ***Monitoring Microsoft Azure*** manual.

The following sections provide an overview of Microsoft Azure Classic services and the *Microsoft: Azure Classic* 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 are Azure Locations?

Microsoft currently has data centers in the following locations to support the Azure Classic portal:

- East US (Virginia)
- East US 2 (Virginia)
- US Gov (Virginia)
- North Central US (Illinois)
- Central US (Iowa)
- US Gov (Iowa)
- South Central US (Texas)
- West US (California)
- Brazil South (Sao Paulo)
- North Europe (Ireland)
- West Europe (Netherlands)
- Japan East (Saitama)
- Japan West (Osaka)
- East Asia (Hong Kong)
- Southeast Asia (Singapore)
- Australia East (New South Wales)
- Australia Southeast (Victoria)
- West India (Mumbai)
- Central India (Pune)
- South India (Chennai)

What Does the Microsoft: Azure Classic PowerPack Monitor?

The Dynamic Applications in the *Microsoft: Azure Classic* PowerPack can monitor performance metrics and/or collect configuration data for the classic versions of the following Azure services and components:

- Blob storage
- Cloud services
- Queue storage
- Table storage
- Virtual machines
- Virtual networks
- Service Bus services
- Active Directory tenants
- Traffic Manager profiles
- SQL databases

Installing the Microsoft: Azure Classic PowerPack

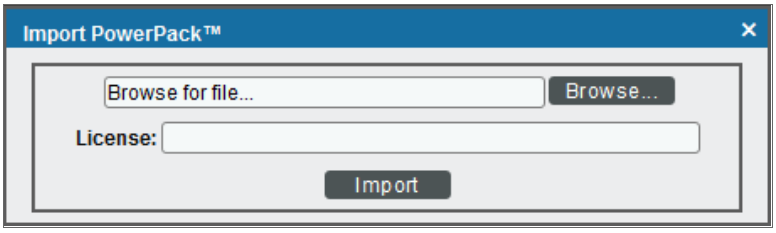
Before monitoring Azure Classic resources in the ScienceLogic platform, ensure that you have installed the latest version of the *Microsoft: Azure Classic* PowerPack.

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 Classic Credentials

Overview

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

Configuring an Azure Classic Active Directory Application

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

- OAuth 2.0 token endpoint URL
- Active Directory username and password
- Client ID
- Tenant ID (GUID)
- Subscription ID

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

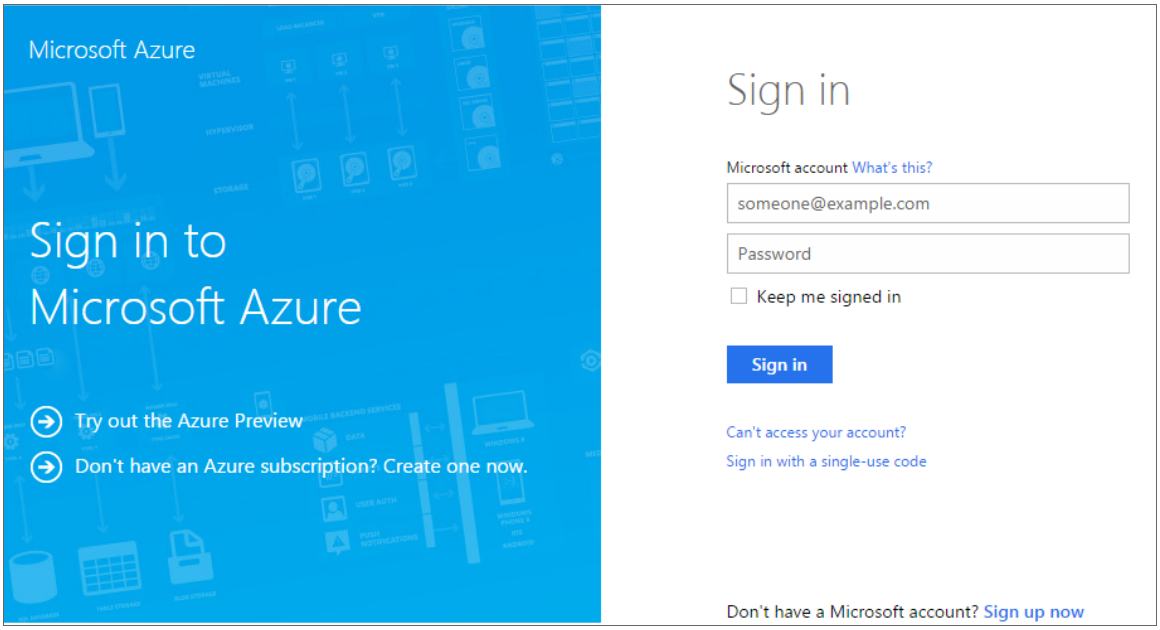
Creating a Client Active Directory Application in the Azure Classic Portal

When configuring a SOAP/XML credential in the ScienceLogic platform to access Microsoft Azure, you must know the OAuth 2.0 token endpoint URL, Client ID, and Tenant ID (GUID) of an Active Directory web application that can be used to authenticate your Azure account. This application must have permission to access the Microsoft Azure Service Management API as an organization user.

This section describes the process for creating a new Active Directory application in the Azure Classic portal, and for assigning permission to the application to access the Azure Service Management API as an organization user. This section also describes where you can find the information about the Active Directory application that you need to configure the credential.

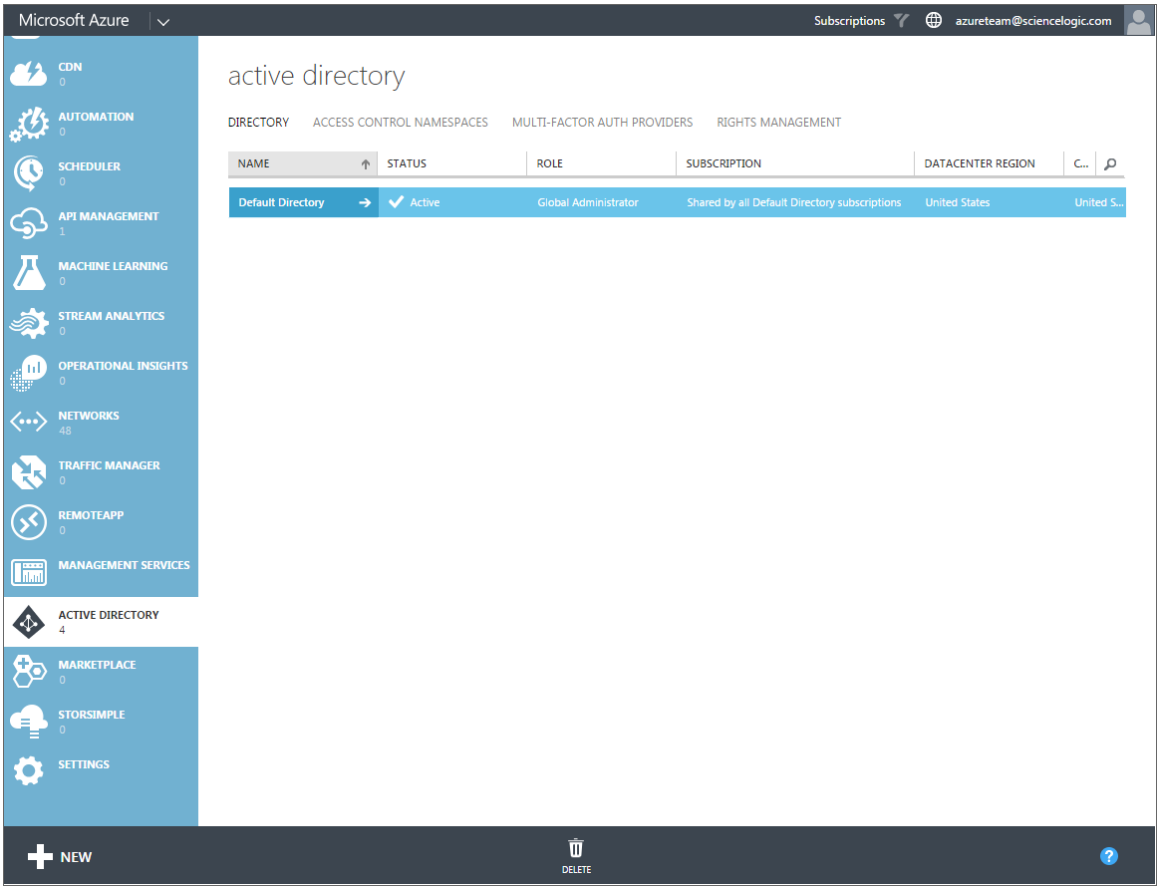
To create a client Active Directory application in the Azure Classic portal:

1. Open a browser session and go to https://manage.windowsazure.com.
2. If you are not currently logged in to the Azure Classic portal, a login prompt appears:

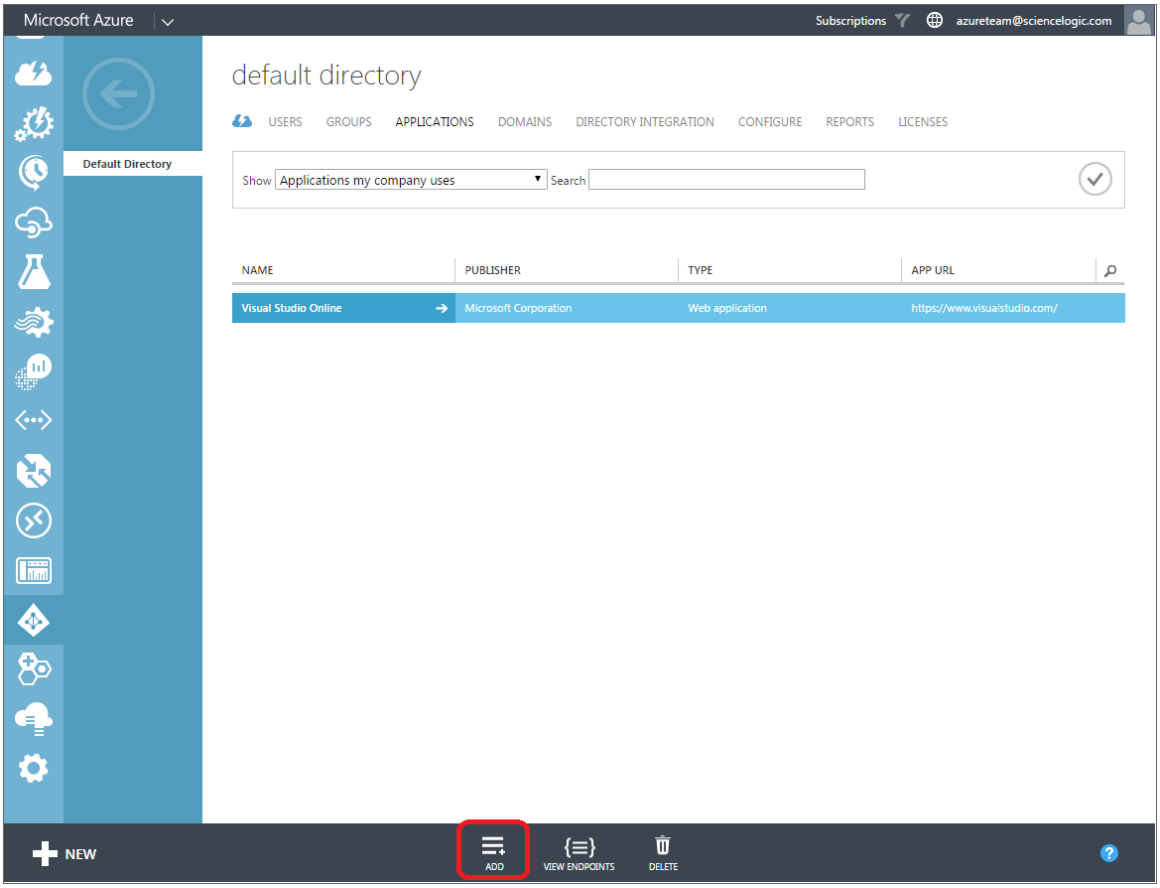


After logging in, the **All Items** page appears.

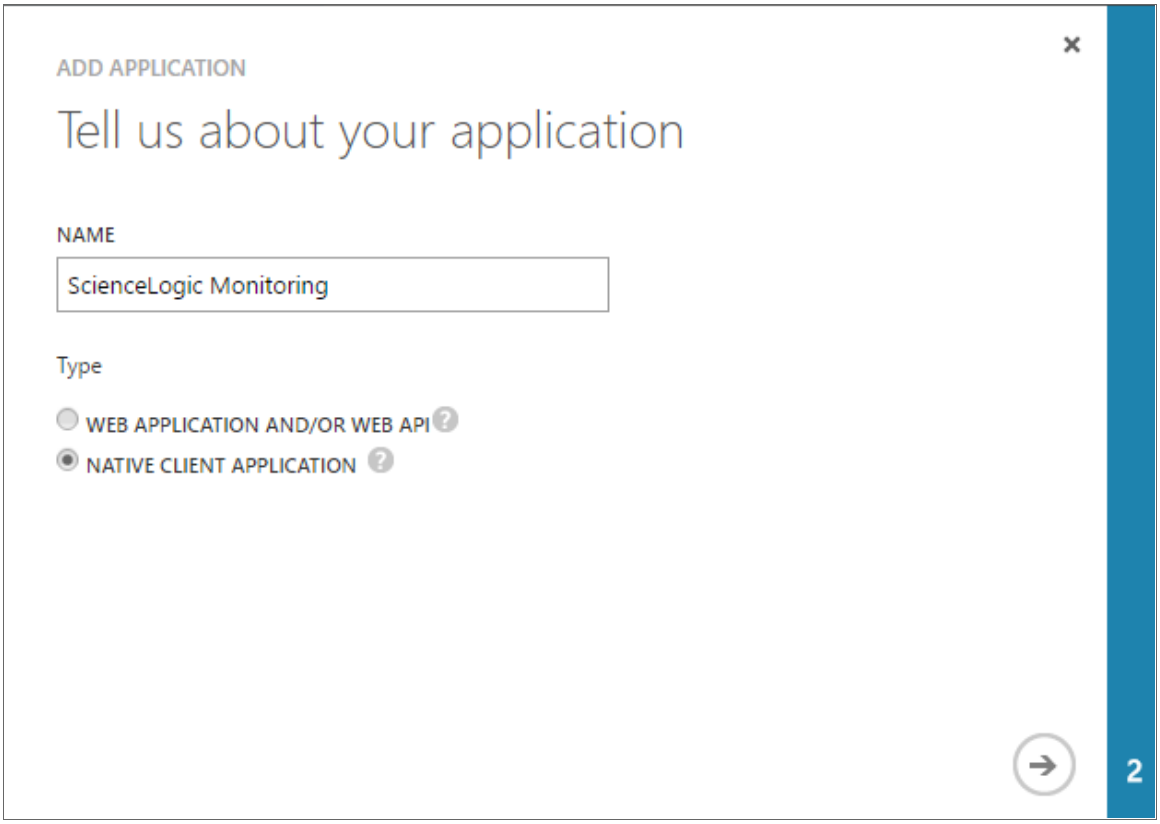
3. From the left panel, click **[Active Directory]**. The **Active Directory** page appears:



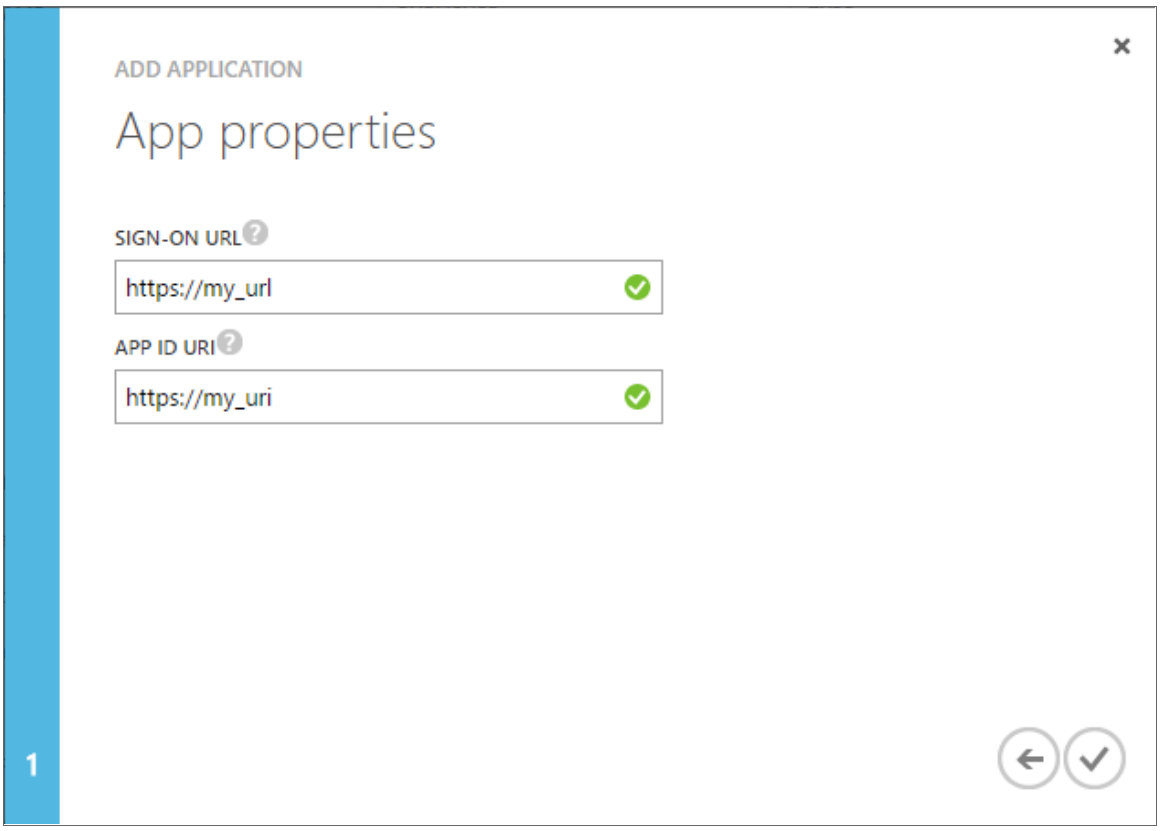
4. Click the ***Name*** of the Active Directory you want to use, then click the **[Applications]** tab. The **Applications** page appears.
5. Click the **[Add]** button.



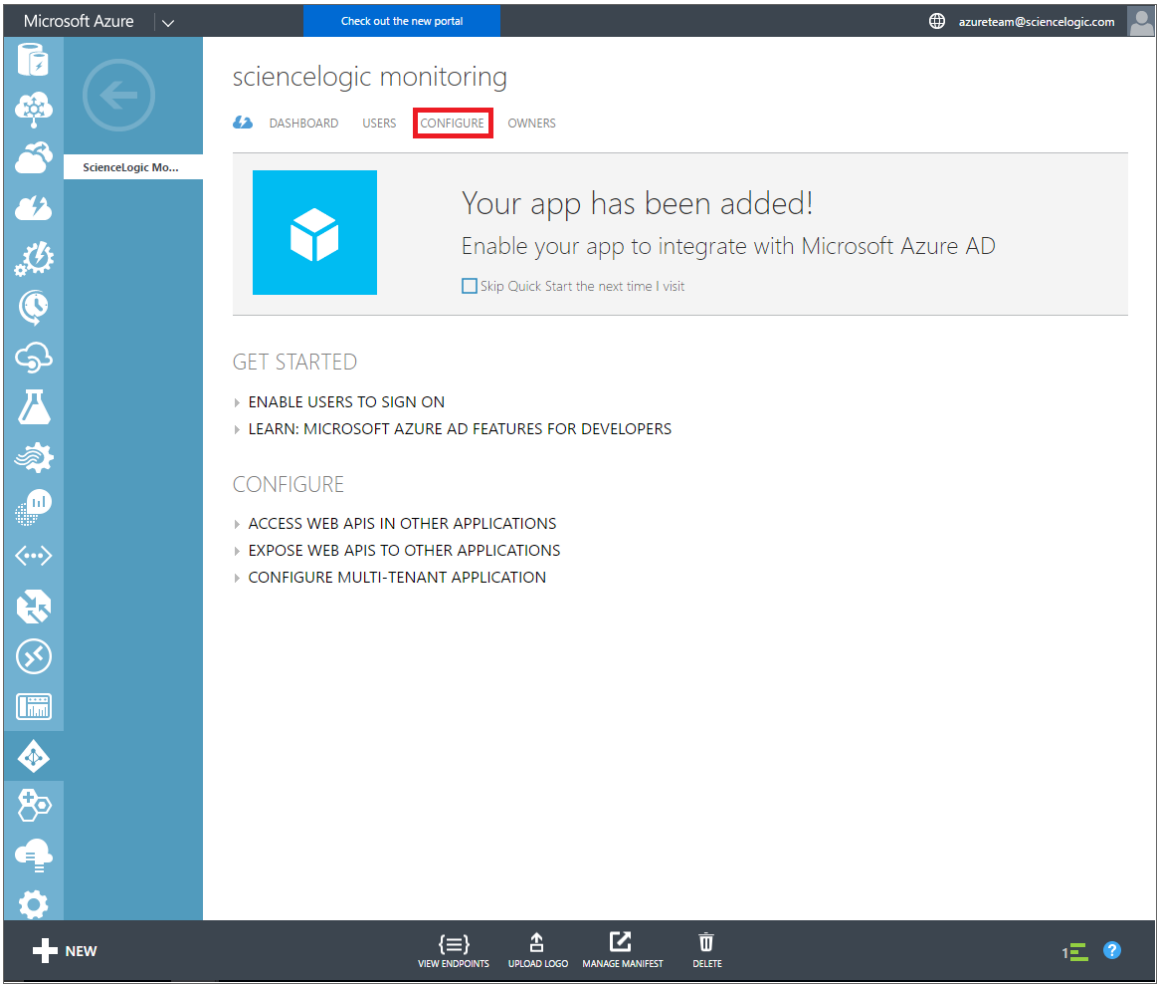
6. At the prompt, click **[Add an application my organization is developing]**. The **Add Application** modal page appears.
7. Enter a ***Name*** for the application, select the **[Native Client Application]** radio button, and then click the right-arrow button to continue.



8. In the ***Sign-On URL*** field, enter any valid URL.
9. In the ***App ID URI*** field, enter any valid URI. Click the checkmark button.



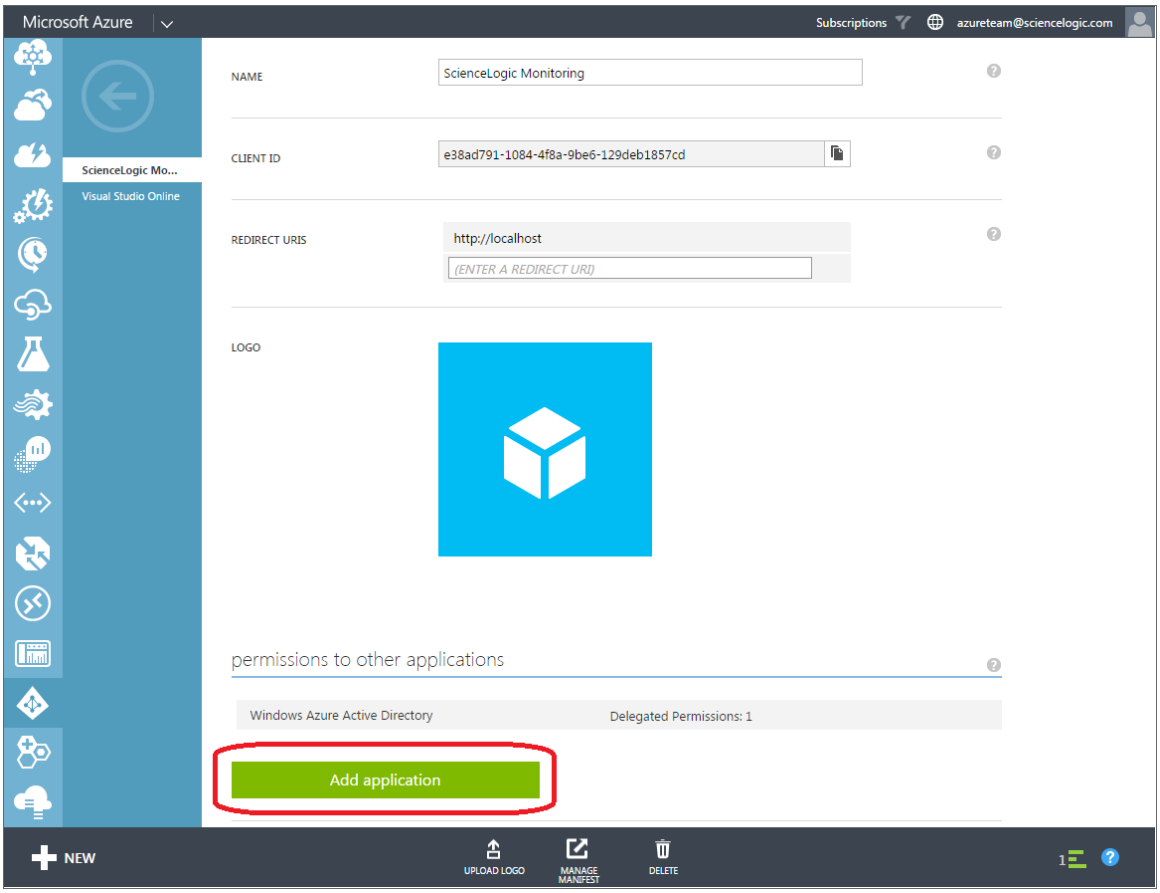
9. A message appears confirming that your application was added.
10. Click the **[Configure]** tab.



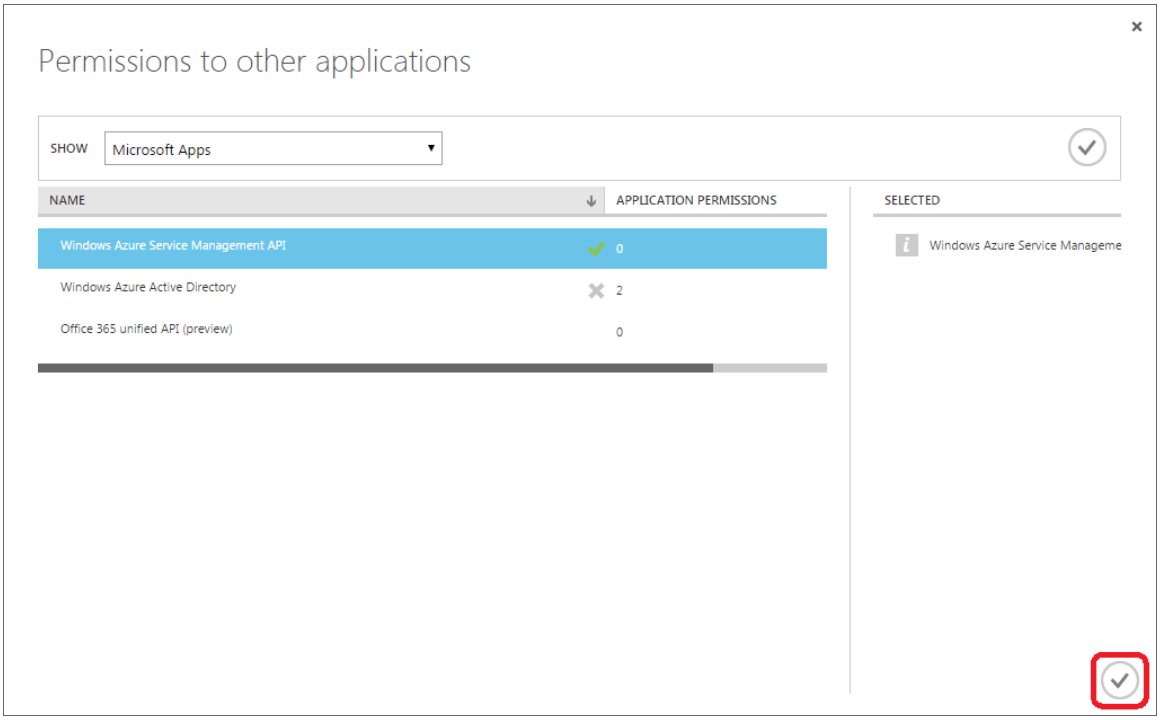
11. The **Properties** page appears. Write down or copy the ***Client ID***.

TIP: You can click the **Copy** icon next to the ***Client ID*** to copy the ID to your computer's clipboard.

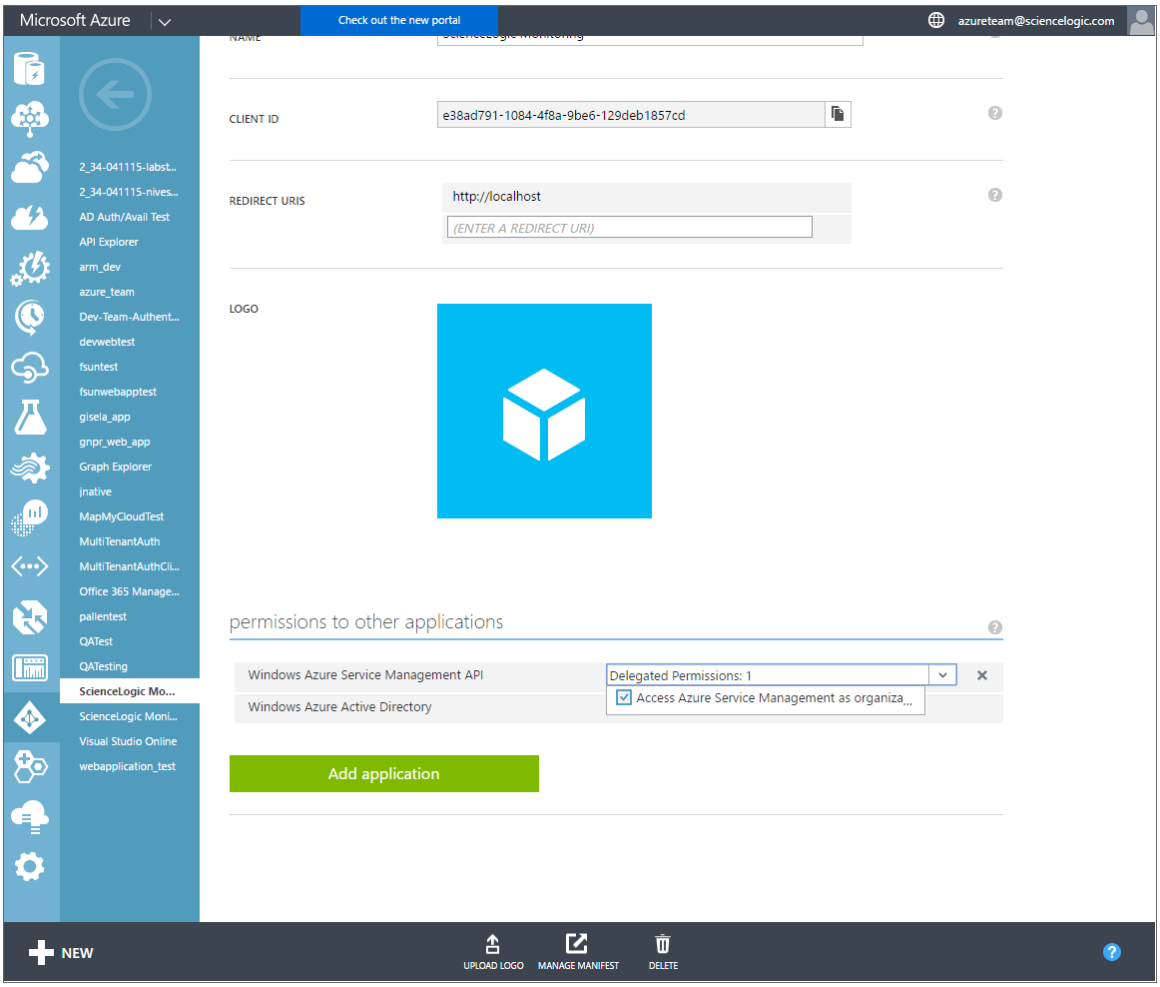
12. On the **Properties** page, click the **[Add application]** button.



13. The **Permissions to other applications** modal page appears. From the list of applications, select **Microsoft Azure Service Management API**, then click the checkmark button.

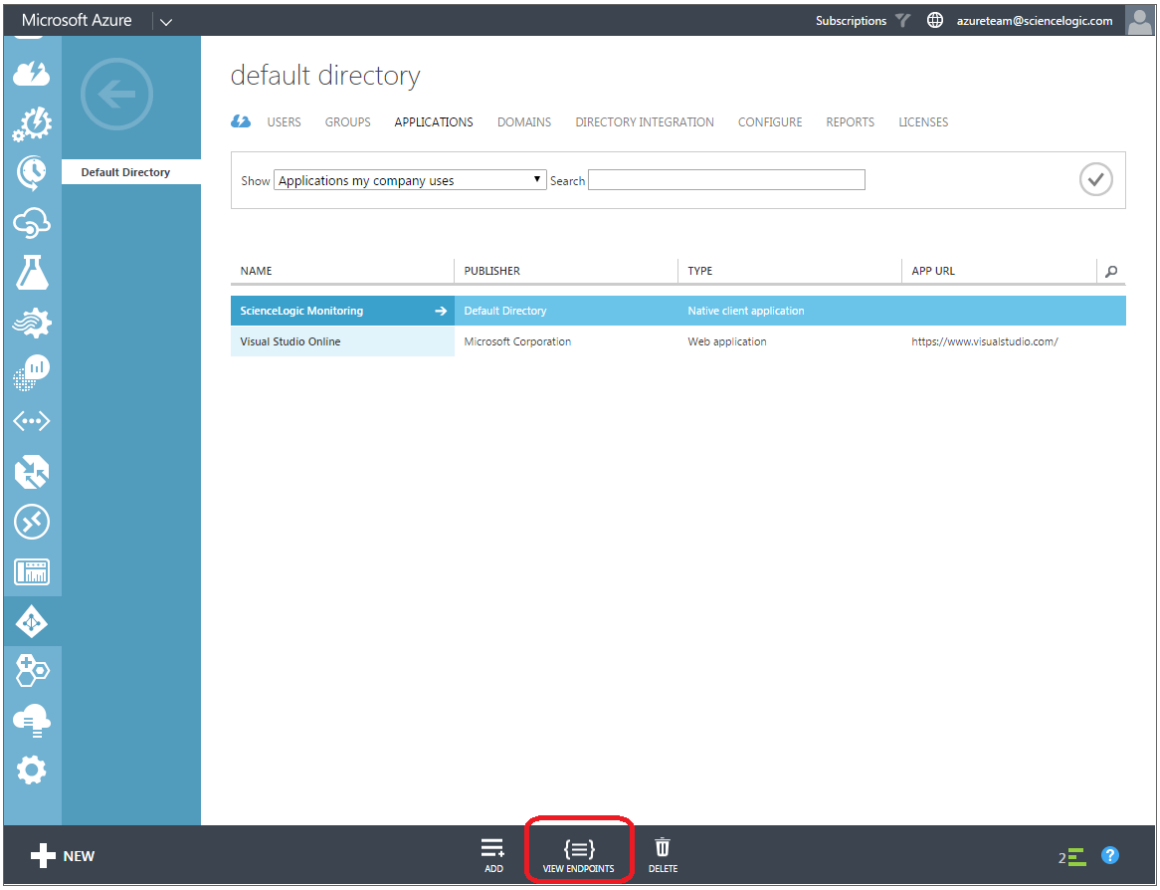


14. On the **Properties** page, hover over the Windows Azure Service Management API ***Delegated Permissions*** field to make a drop-down menu appear. From the drop-down menu, select **Access Azure Service Management as organization user (preview)**.

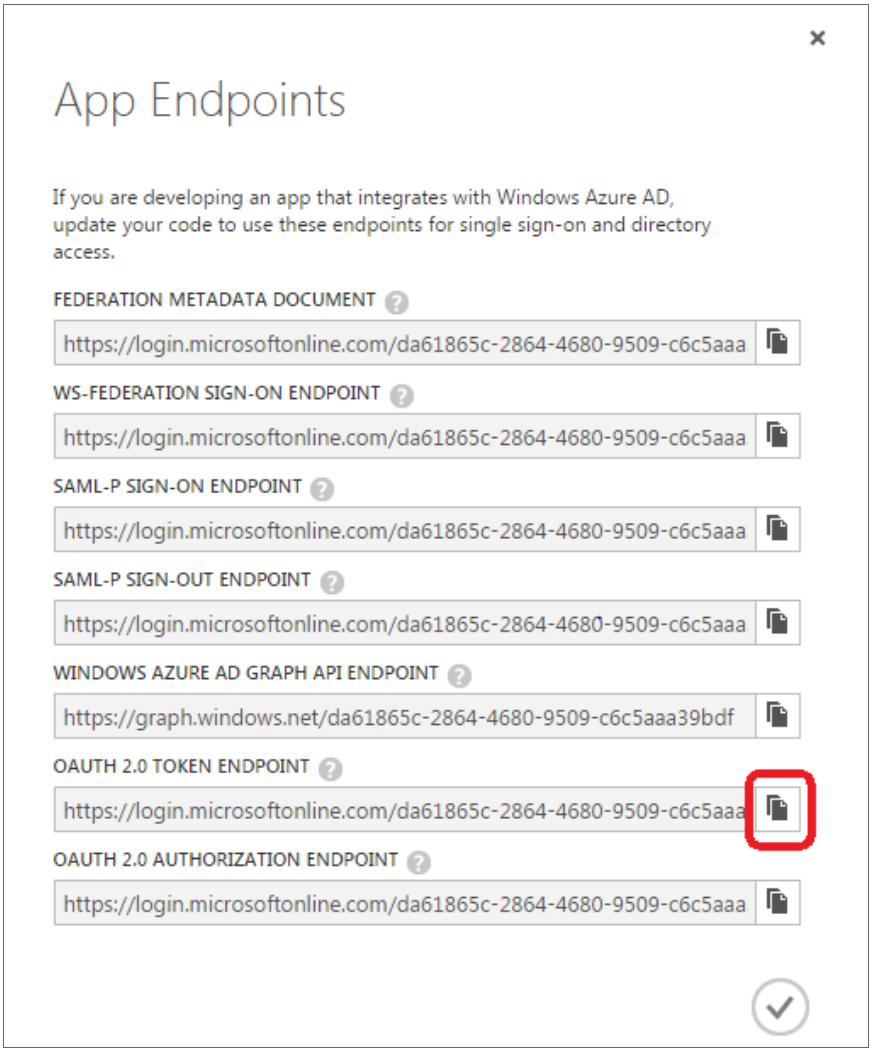


15. Click **[Save]**.
16. In the Active Directory menu in the left pane, click the left-arrow (**[Back]**) to return to the **Applications** page.

17. On the **Applications** page, select the application (specified in step #7) from the list and then click **[View Endpoints]**.

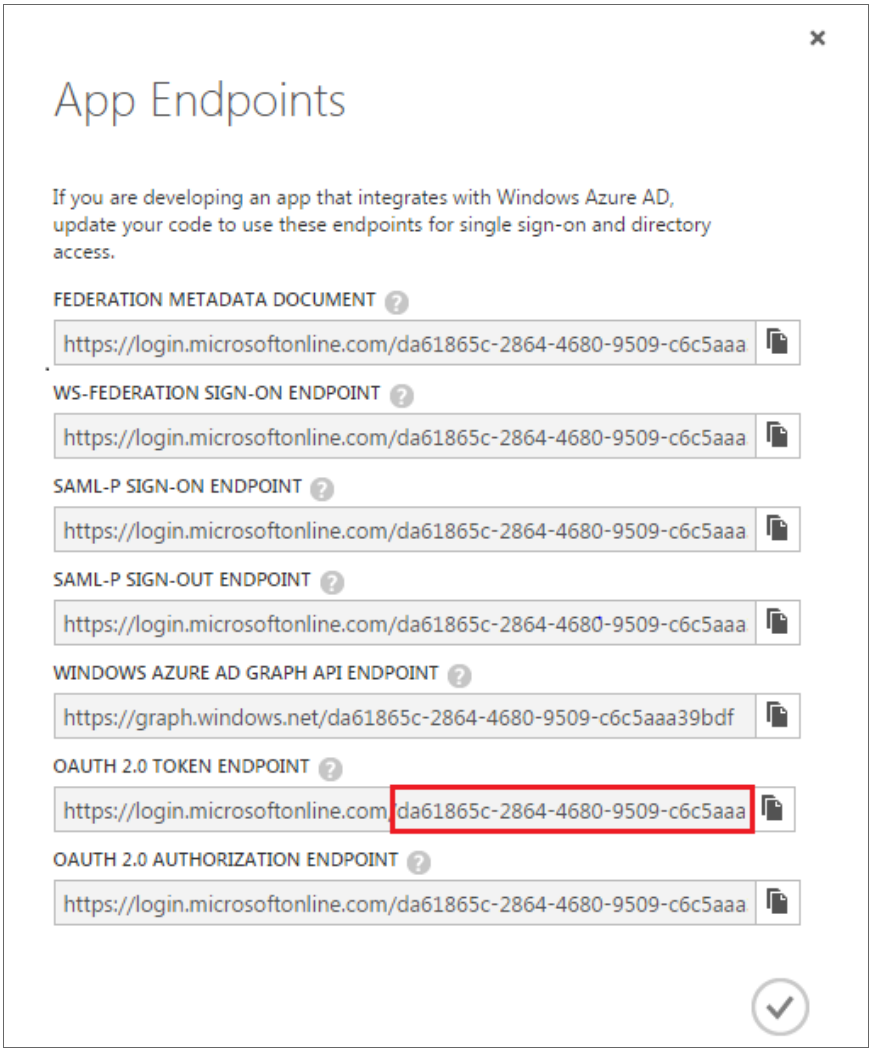


18. The **App Endpoints** modal page appears. Write down or copy the ***OAUTH 2.0 TOKEN ENDPOINT*** URL. You must supply the ***OAUTH 2.0 Token Endpoint URL*** when you create the SOAP/XML credential in the ScienceLogic platform.



TIP: You can click the **Copy** icon next to the URL to copy it to your computer's clipboard.

19. The OAuth 2.0 Token Endpoint URL contains a GUID. Copy or write down the GUID. Azure uses this GUID as the Tenant ID.



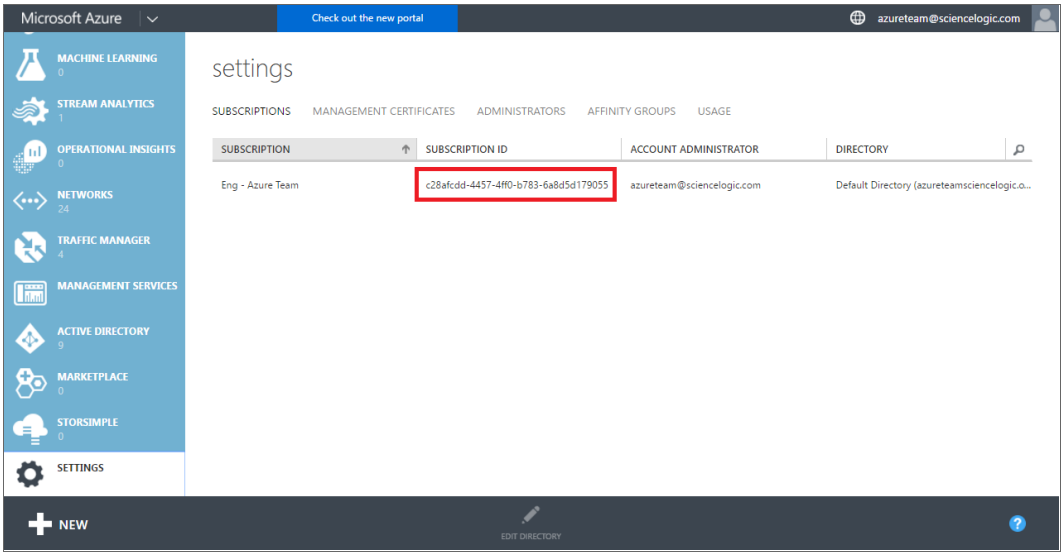
Adding Co-Administrator Access to a User Account in the Azure Classic Portal

When configuring a SOAP/XML credential in the ScienceLogic platform, you need to know your Azure subscription ID and the Active Directory username and password of a Co-Administrator user assigned to the subscription. This section describes the process for assigning Co-Administrator access to an existing user account in your Azure subscription using the Azure Classic portal.

NOTE: You must have Service Administrator access to your Azure subscription to assign Co-Administrator access to another user.

To add Co-Administrator access to a user account in the Azure Classic portal:

1. If you are not currently logged in to the Azure Classic portal, open a browser session and go to https://manage.windowsazure.com, then log in.
2. From the left panel, select **[Settings]**. The **Settings** page displays.

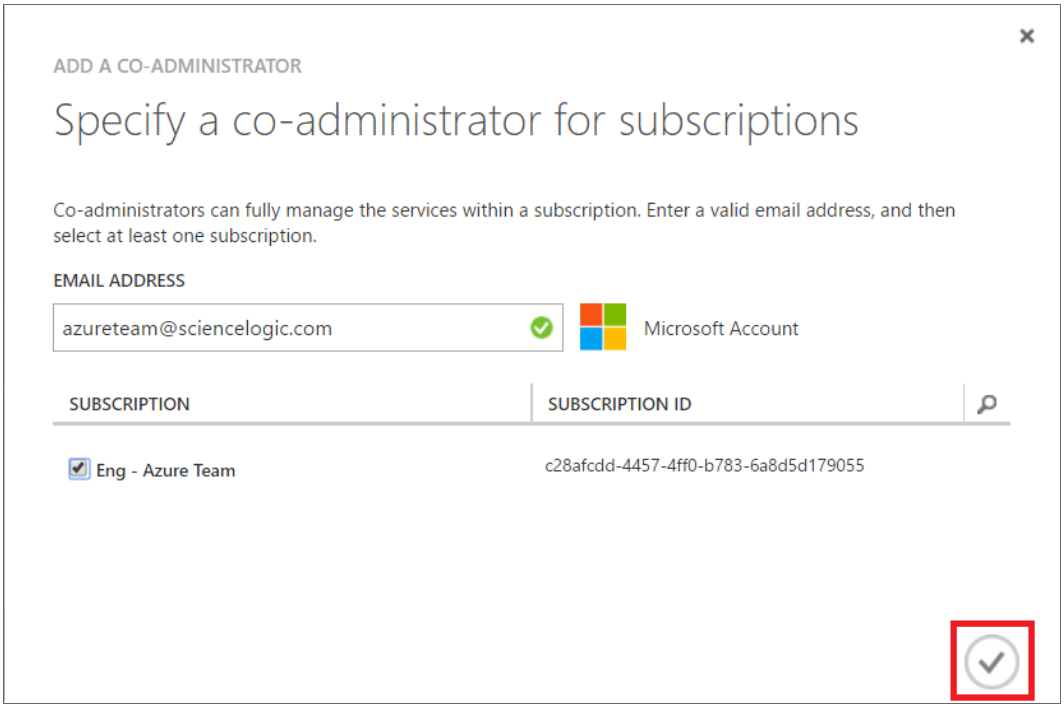


3. Write down or copy the ***Subscription ID***.
4. From the **Settings** page, click the **[Administrators]** tab, and then click **[Add]**.
5. In the **Add a Co-Administrator** modal page, type the email address of the Active Directory user you will use to authenticate your Azure account.

NOTE: The co-administrator must either have a Microsoft account or be a user in the Azure Default Directory.

6. Select the *Subscription* for the user, and then click the checkmark to save.

NOTE: To authenticate your account, the co-administrator must be in the same Azure subscription as the Active Directory application that you created.



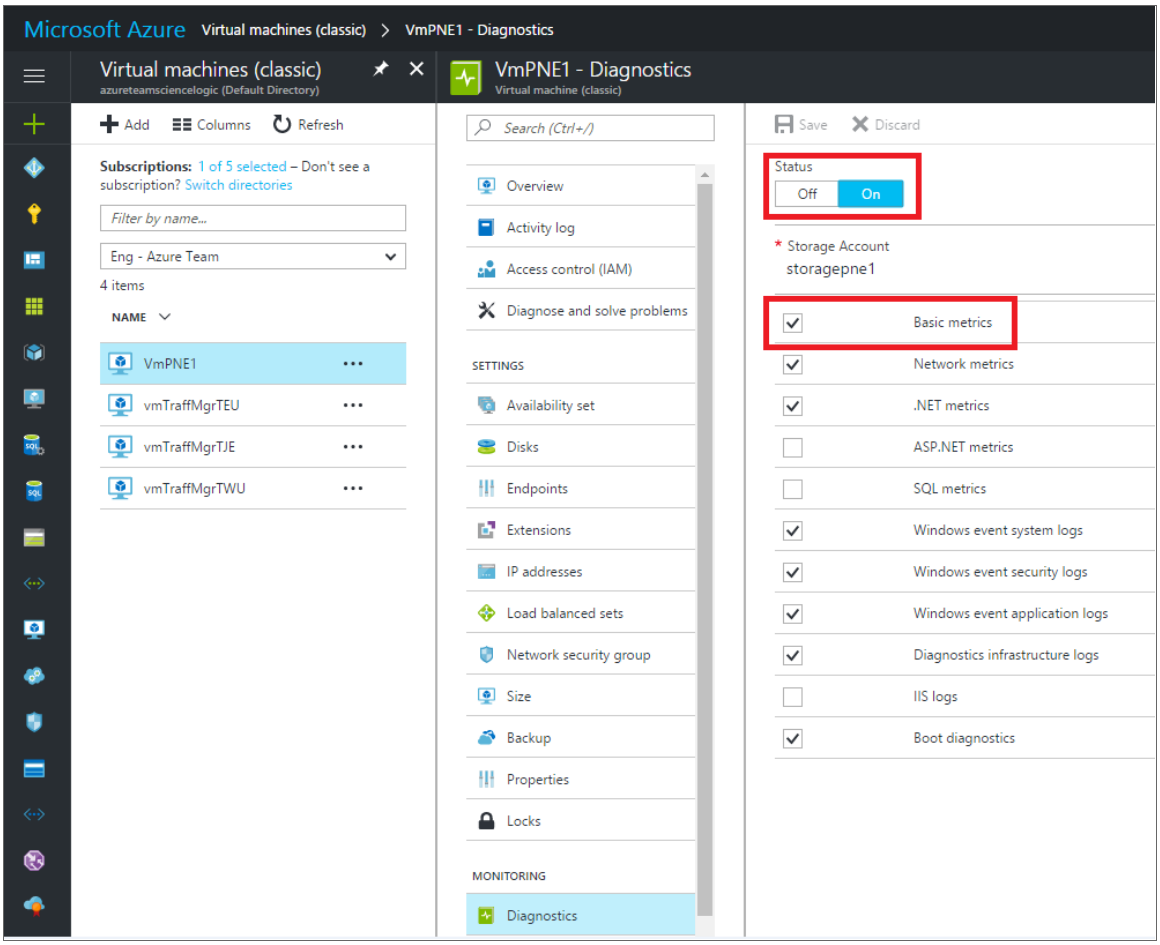
Configuring Virtual Machine Diagnostics Settings

Optionally, if you use the ScienceLogic platform to monitor a virtual machine managed with Microsoft Azure, you must configure the appropriate virtual machine diagnostics settings.

To configure virtual machine diagnostics settings in Azure:

1. Log in to the Azure portal at https://portal.azure.com.
2. In the left panel, select **Virtual Machines (classic)**. Click on the name of the virtual machine you will monitor with the ScienceLogic platform.

3. In the virtual machine pane, under ***Manage***, select **Diagnostics**, then make entries in the following fields:



- ***Status***. Select *On*.
- ***Basic Metrics***. Select this checkbox.

4. Click **[Save]**.

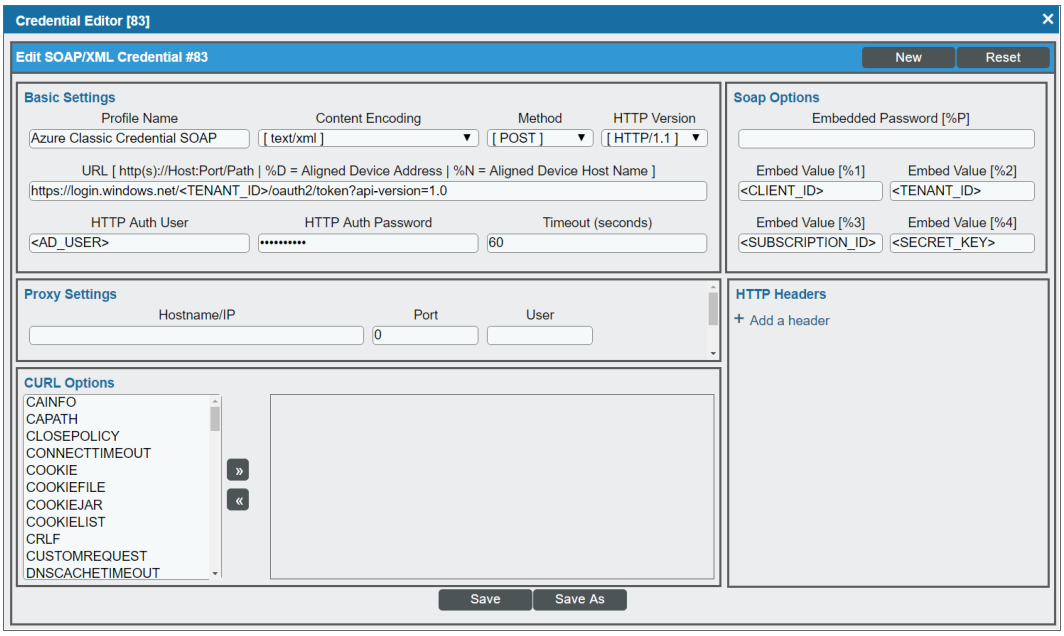
Creating a SOAP/XML Credential for Azure Classic

After you have the information you need from the Active Directory application and user, you can create a SOAP/XML credential in the ScienceLogic platform to monitor Azure Classic resources. This credential allows the Dynamic Applications in the *Microsoft: Azure Classic* PowerPack to communicate with your Azure account.

To configure a SOAP/XML credential to access Azure:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential included in the Microsoft: Azure Classic PowerPack, called **Azure Classic Credential SOAP**, then click its wrench icon ( ).

3. Enter values in the following fields:



- ***Profile Name***. Enter a new name for the Azure credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select POST.
- ***HTTP Version***. Select HTTP/1.1.
- ***URL***. Enter the OAuth 2.0 token endpoint URL for the Azure Active Directory application.
- ***HTTP Auth User***. Enter the Active Directory username of the Azure user assigned to the subscription.
- ***HTTP Auth Password***. Enter the Active Directory password of the Azure user assigned to the subscription.
- ***Timeout(seconds)***. Enter "60".
- ***Hostname/IP***. Leave this field blank.
- ***Port***. Enter "0".
- ***User***. Leave this field blank.
- ***CURL Options***. Do not make any selections in this field.
- ***Embedded Password***. Leave this field blank.
- ***Embed Value [%1]***. Enter the Client ID for the Azure Active Directory application.
- ***Embed Value [%2]***. Enter the Tenant ID (GUID) for the Azure Active Directory application.
- ***Embed Value [%3]***. Enter the Subscription ID for the Azure account.
- ***Embed Value [%4]***. Leave this field blank.
- ***HTTP Headers***. Do not make any selections in this field.

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

Chapter 3

Discovering Azure Classic Services and Devices

Overview

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

Creating an Azure Virtual Device

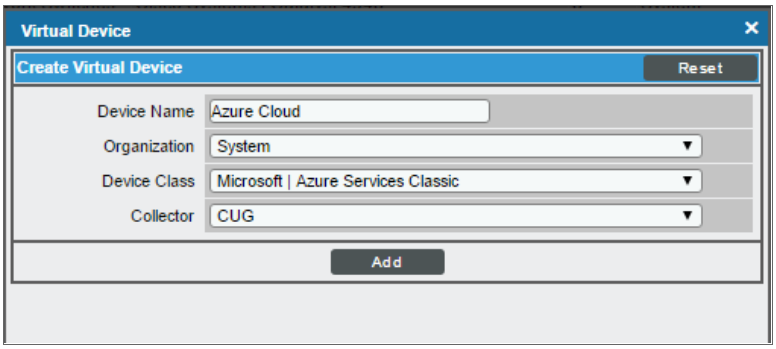
Because the Azure service does not have a static IP address, you cannot discover an Azure device using discovery. Instead, you must create a ***virtual device*** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered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

TIP: If you have multiple Azure subscriptions you want to monitor, you should create a separate credential and virtual root device for each.

To create a virtual device that represents your Azure service:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click **[Actions]** 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, you could enter "Azure Cloud" in this field.
- ***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 Classic*.
- ***Collector***. Select the collector group that will monitor the device.

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

Aligning the Azure Dynamic Applications

The Dynamic Applications in the Microsoft: Azure Classic PowerPack are divided into four types:

- ***Count***. This Dynamic Application polls Azure to determine the number of component devices monitored by the ScienceLogic platform.
- ***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.

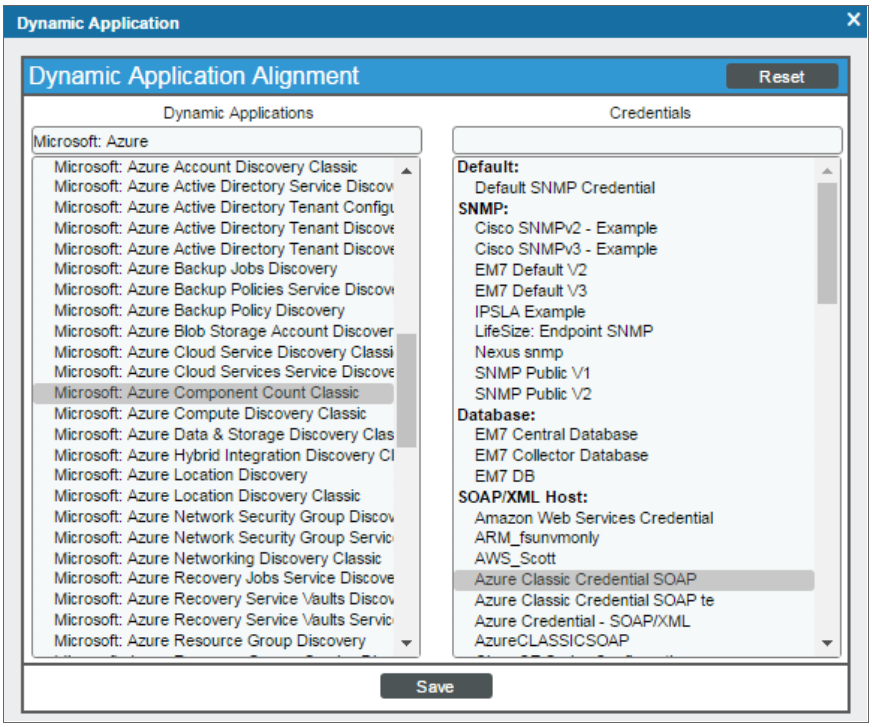
Counting Azure Component Devices

If you want to determine the number of Azure component devices that will be monitored prior to running discovery (e.g., to estimate future license usage), you can manually align the "Microsoft: Azure Component Count" Dynamic Application with the Azure virtual device.

To align the "Microsoft: Azure Component Count" Dynamic Application to your Azure virtual device, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

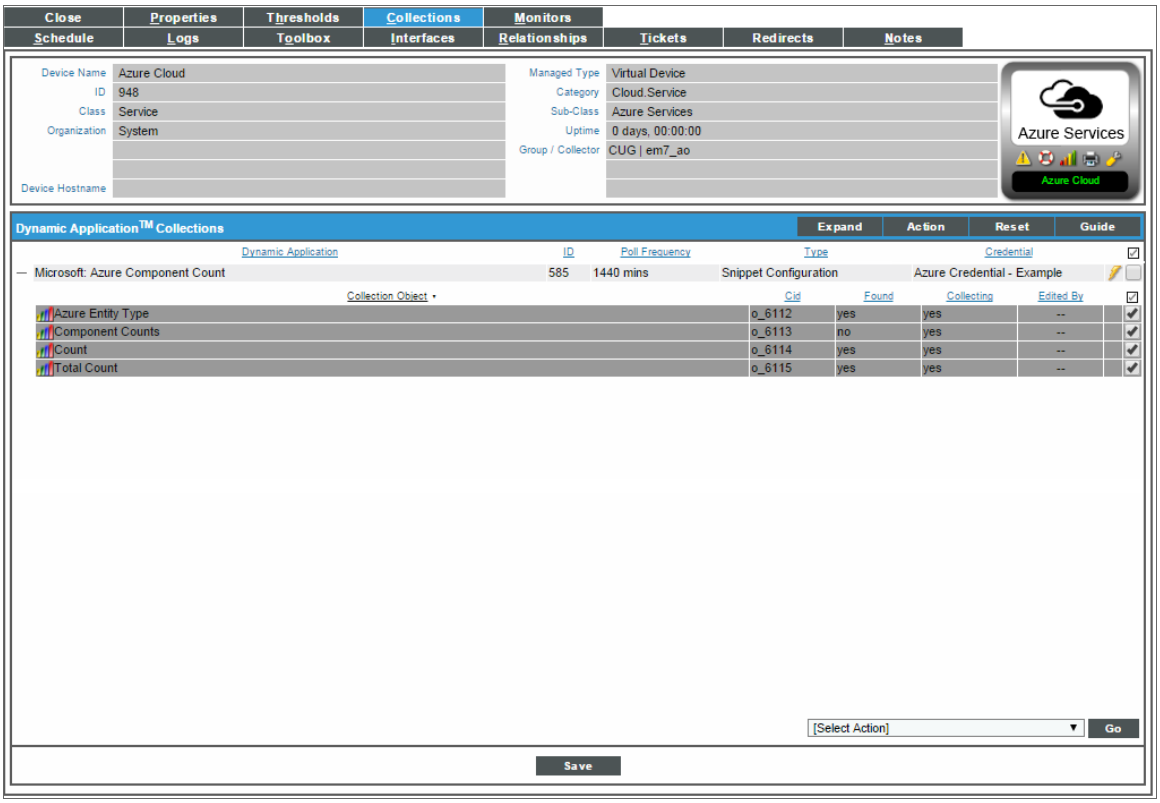
2. Click the wrench icon ( ) for your Azure virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page displays.
4. Click **[Actions]** and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment**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



   - In the ***Dynamic Applications*** field, select the *Microsoft: Azure Component Count* Dynamic Application.
   - 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. The Dynamic Application appears on the **Dynamic Application Collections** page.
7. If you want to run collection immediately, click the lightning bolt icon ( ) for the "Microsoft: Azure Component Count" Dynamic Application. The **Run Dynamic App** modal page displays.
8. After the Dynamic Application has run, close the **Run Dynamic App** modal page.

9. On the **Dynamic Application Collections** page, click the plus icon ( ) for the "Microsoft: Azure Component Count" Dynamic Application. The Dynamic Application row expands to display a list of Collection Objects:



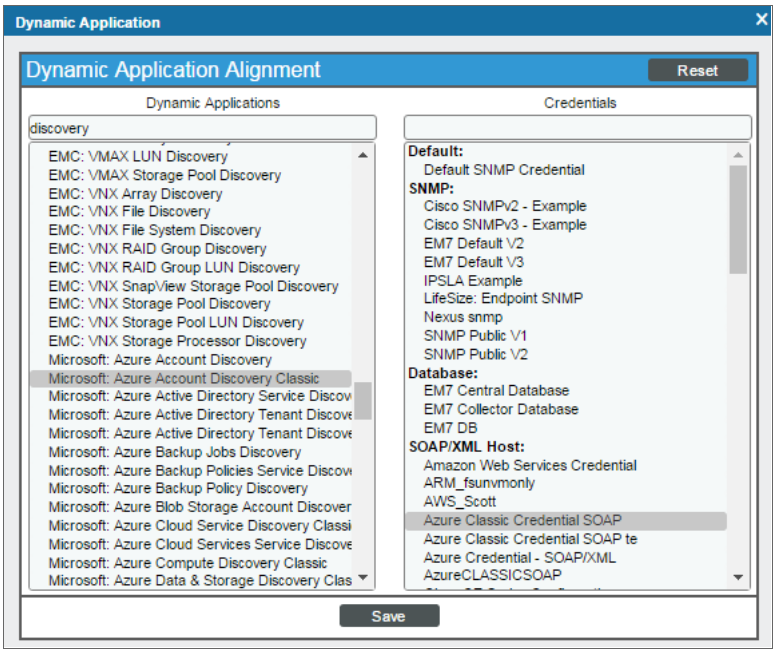
10. Click the ***Total Count*** graph icon ( ). The Microsoft: Azure Component Count configuration report displays a count of all of the Azure component devices.

Discovering Azure Component Devices

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

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 **[Actions]** and select *Add Dynamic Application* from the menu.

5. In the **Dynamic Application Alignment** modal page:



- In the ***Dynamic Applications*** field, select the "Microsoft: Azure Account Discovery Classic" Dynamic Application.
- 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 Classic" Dynamic Application with the Azure virtual device, the Dynamic Application creates a component device representing the Azure account.

The ScienceLogic platform then automatically aligns several other Dynamic Applications to the account component device. These additional Dynamic Applications discover and create component devices for each location used by the Azure account, as well as any security and identity management services and/or Traffic Manager services used by the account.

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

- Networking services
  - Virtual Networks services
    - Virtual networks
- Compute services
  - Virtual Machines services
    - Virtual machines
  - Cloud Services
    - Cloud services

- Data & Storage services
    - SQL Database services
        - SQL servers
            - SQL databases
    - Storage services
        - Storage accounts
            - Storage containers
            - Storage queues
            - Storage tables
- Hybrid Integration services
    - Service Bus services
        - Namespaces

NOTE: The ScienceLogic platform also creates relationships between Azure cloud services and associated virtual machines, if applicable.

Under the Security & Identity component device, the ScienceLogic platform discovers the following component devices:

- Active Directory Services
    - Active Directory tenants

NOTE: At present, the ScienceLogic platform can discover only a single Active Directory tenant per Azure account.

Under the Traffic Manager Service component device, the ScienceLogic platform discovers the following component device(s):

- Traffic Manager Profiles

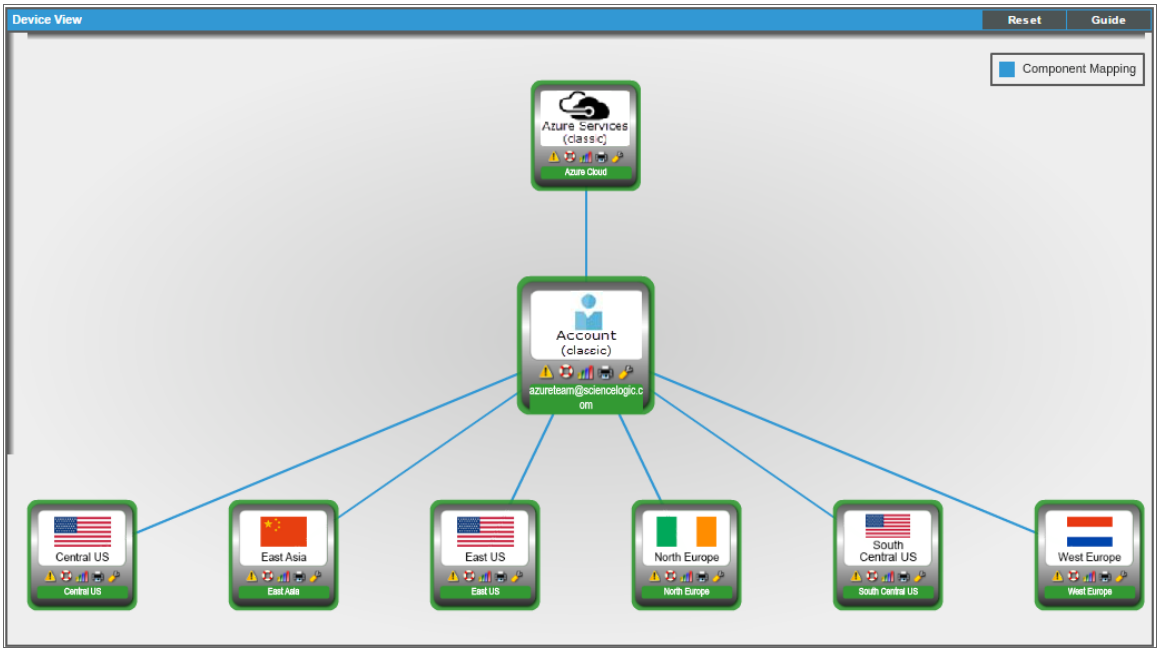
NOTE: The ScienceLogic platform might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

Viewing Azure Component Devices

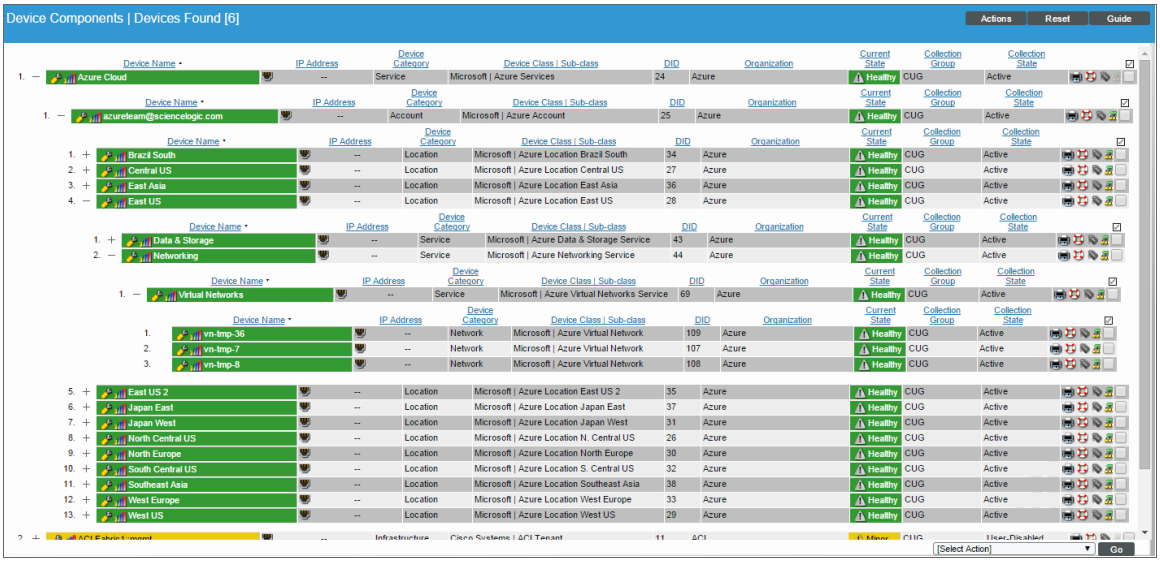
In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the Azure service and all associated component devices in the following places in the user interface:

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.

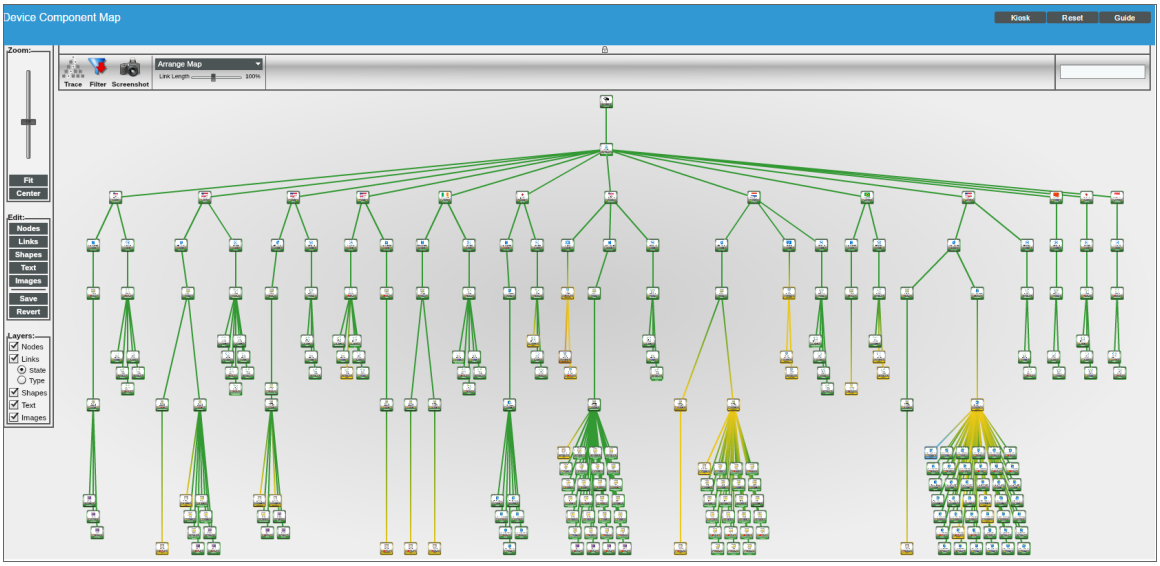
- The **Device View** modal page displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



- 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.



Chapter 4

Troubleshooting

Troubleshooting Error Messages

The following error messages can be generated during collection for the Azure Dynamic Applications.

Error / Message	Cause / Resolution
Failed to connect to Microsoft Azure.	There is a problem with your internet connection or internal network. Alternatively, the Microsoft Azure Portal might be down or the login to the Azure portal was unsuccessful, possibly due to an incorrect credential. Verify that the correct Dynamic Application and credential are aligned to the device and are being used to connect to the API.
A connection with Microsoft Azure was not established.	Your login attempt to Azure was unsuccessful. Alternatively, Azure is experiencing an outage.
Failed to connect to the Microsoft Azure Portal with the following error: Invalid credential type.	You attempted to connect to Azure using a credential type other than SOAP/XML.
Failed to connect to the Microsoft Azure Portal with the following error: Azure subscription ID not provided in credential.	The credential does not include the correct Azure Subscription ID. Refer to the sample credentials provided by the Microsoft: Azure Classic PowerPack.
Failed to connect to the Microsoft Azure Portal with the following error: Azure username is not provided in credential.	The credential does not include a correct username. Refer to the sample credentials provided by the Microsoft: Azure Classic PowerPack.
Failed to connect to the Microsoft Azure Portal with the following error: Azure password is not provided in credential.	The credential does not include a correct password. Refer to the sample credentials provided by the Microsoft: Azure Classic PowerPack.

Error / Message	Cause / Resolution
Failed to connect to the Microsoft Azure Portal with the following error: Azure application client ID is not provided in credential.	The SOAP/XML credential does not include a correct client ID. Refer to the sample credentials provided by the Microsoft: Azure Classic PowerPack.
Failed to connect to the Microsoft Azure Portal with the following error: Azure application tenant ID is not provided in credential. (Alternatively, failed to retrieve Active Directory tenant information from Azure.)	The SOAP/XML credential does not include a correct tenant ID. Refer to the sample credentials provided by the Microsoft: Azure Classic PowerPack. Alternatively, Azure could be experiencing an outage, you might be experiencing internal network issues, or the API authentication was incorrect.
Failed to retrieve subscription information from Azure.	The credential does not include the correct Azure Subscription ID, or the subscription is not configured in the Microsoft Azure Portal.
Failed to connect to the Microsoft Azure Portal with the following error: Failed to get token with the current SOAP credential set, invalid client ID, URL, username or password.	The alignment or credential is incorrect.
Failed to connect to the Microsoft Azure Portal with the following error: Azure application's token endpoint is not provided in credential.	Ensure that the Azure SOAP/XML credential has a valid token endpoint in the ***URL*** field.
Failed to connect to the Microsoft Azure Portal with the following error: Azure application key is not provided in the credential.	Ensure that the Azure SOAP/XML credential contains an application key in the ***Embed Value [%4]*** field.
Failed to retrieve an authentication token from Azure.	Ensure that all values in the SOAP/XML credential are correct.
Azure diagnostics are not enabled for the Azure virtual machines in a storage account.	In the portal for classic Azure virtual machines, go to Settings. In the Monitor sections, go to Diagnostics. For each diagnostic you want to enable, set the Status to "On" and then save.
No Azure performance metrics were found.	For storage components, ensure that diagnostics are enabled in the Azure portal.
The Azure virtual machine is configured with an unknown size.	There is a mismatch between the configuration sizes in Azure and what the ScienceLogic snippet expects. Report this issue to ScienceLogic.
Failed to parse the following time stamp for an Azure performance counter.	Ensure that the device is generating performance information. Alternatively, ensure that the device still exists.

Error / Message	Cause / Resolution
Failed to retrieve a list of "Affinity Group" objects from Azure.	There could be an internal Azure issue with the affinity group object, or there could be potential alignment or credential issues. Verify the object still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to retrieve the collection of storage accounts from Azure	There could be an internal Azure issue with the storage objects, or there could be potential alignment or credential issues. Verify the storage account still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to retrieve primary keys for storage account from Azure	There could be an internal Azure issue with the storage objects, or there could be potential alignment or credential issues. Verify the storage account still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to instantiate the BlobService for the storage account	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Alternatively, this could indicate an Azure outage.
Failed to retrieve the list of blobs for the storage container from Azure	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Alternatively, this could indicate an Azure outage.
Failed to instantiate the QueueService for the storage account	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Alternatively, this could indicate an Azure outage.
Failed to instantiate the TableService for the storage account	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Alternatively, this could indicate an Azure outage.
Failed to retrieve the collection of blobs for the storage container	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Verify the blob still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to retrieve the collection of queues for the storage account from Azure	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Verify the queue still exists in the Azure portal. Alternatively, this could indicate an Azure outage.

Error / Message	Cause / Resolution
Failed to retrieve the collection of tables for the storage account	In the portal for Storage Accounts Classic, go to Settings > Diagnostics. Set the Status for each option you want to "On" and then save. Verify the table still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to retrieve the collection of containers for the storage account from Azure	Verify the container still exists in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to retrieve the collection of disks from Azure	Verify the disks still exist in the Azure portal. Alternatively, this could indicate an Azure outage.
Failed to query performance counters in the storage account	There is a mismatch of performance counters between Azure and the Dynamic Application. Report this issue to ScienceLogic.

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