



Monitoring Microsoft Azure

Microsoft: Azure PowerPack version 103

Table of Contents

Introduction	1
Overview	1
What is Azure?	1
What Does the Microsoft: Azure PowerPack Monitor?	2
What are Azure Locations?	2
Installing the Microsoft: Azure PowerPack	3
Configuring Azure for Monitoring	5
Overview	5
Configuring an Azure Credential	5
Creating an Active Directory Application in the Azure Portal	6
Adding the Microsoft Graph and Windows Azure Active Directory APIs	8
Generating the Secret Key	10
Locating the Application ID	12
Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID	13
Locating the Subscription ID	15
Adding Contributor Access to the Active Directory Application	15
Setting Up a Proxy Server	17
Creating a SOAP/XML Credential for Azure	18
Discovering Azure Services and Devices	21
Overview	21
Creating an Azure Virtual Device	21
Aligning the Azure Dynamic Applications	22
Discovering Azure Component Devices	23
Viewing Azure Component Devices	25
Relationships Between Component Devices	27

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.

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

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:

- An example credential you can use as a template 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:
 - Resource groups
 - Blob storage
 - Queue storage
 - Table storage
 - Virtual machines
 - Virtual networks
 - Virtual network subnets
 - Recovery Services vaults
 - Network security groups
 - Active Directory tenants
 - Traffic Manager profiles
 - SQL databases
 - SQL servers
 - Load balancers
- 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

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)
- US Gov Iowa
- US Gov Virginia
- 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 version 103 of the *Microsoft: Azure PowerPack*.

NOTE: To install version 103 of the *Microsoft: Azure PowerPack*, your ScienceLogic system must be upgraded to the 8.3.0 or later release.

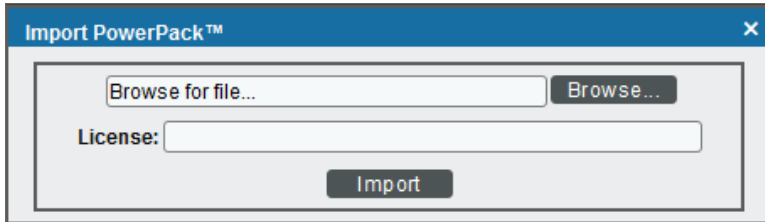
NOTE: If you are upgrading to version 103 of the *Microsoft: Azure PowerPack* from a previous version, ScienceLogic recommends that you first disable your existing device component tree.

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.

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*.

Configuring Azure for Monitoring

Overview

To configure the ScienceLogic platform to monitor Microsoft Azure, you must first create a SOAP/XML credential. This credential allows the platform (specifically, the Dynamic Applications in the *Microsoft: Azure PowerPack*) to communicate with your Azure account.

Configuring an Azure Credential

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
- 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 application with Contributor access. You can then enter the required information about the application when configuring the SOAP/XML credential in the platform.

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

The following sections describe these processes:

- [Creating an Active Directory Application in Azure](#)
- [Adding Permissions to the Microsoft Graph and Windows Azure Active Directory APIs](#)
- [Generating the Secret Key](#)
- [Locating the Application ID](#)
- [Locating the OAuth 2.0 Token Endpoint URL and Tenant ID](#)
- [Locating the Subscription ID](#)
- [Adding Contributor Access to the Active Directory Application](#)
- [Setting Up a Proxy Server](#) (optional)
- [Creating a SOAP/XML Credential for Azure](#)

Creating an Active Directory Application in the Azure Portal

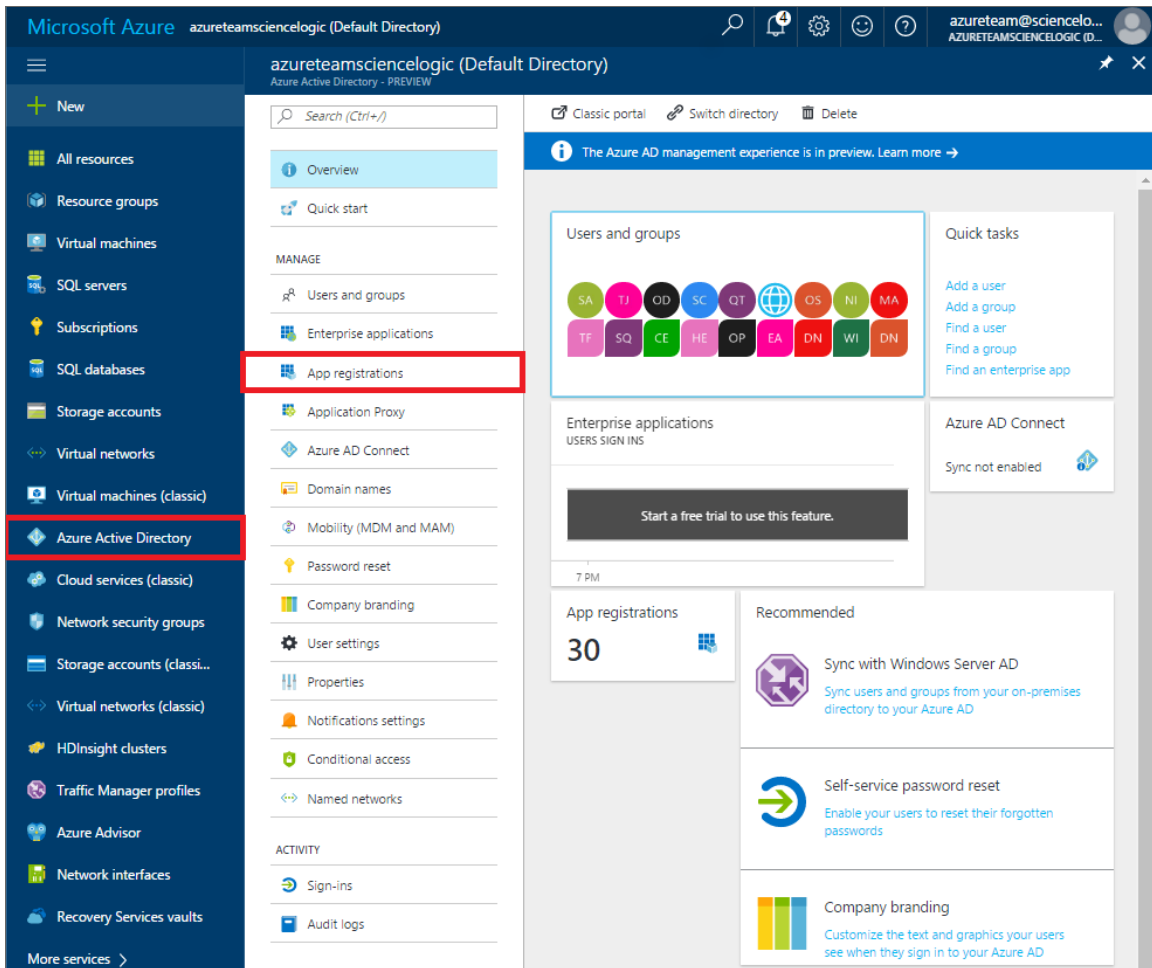
When configuring a SOAP/XML credential in the ScienceLogic platform, you must provide the application ID, subscription ID, OAuth 2.0 token endpoint URL, tenant ID, and secret key of the Azure Active Directory application you will use to authenticate your Azure account.

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

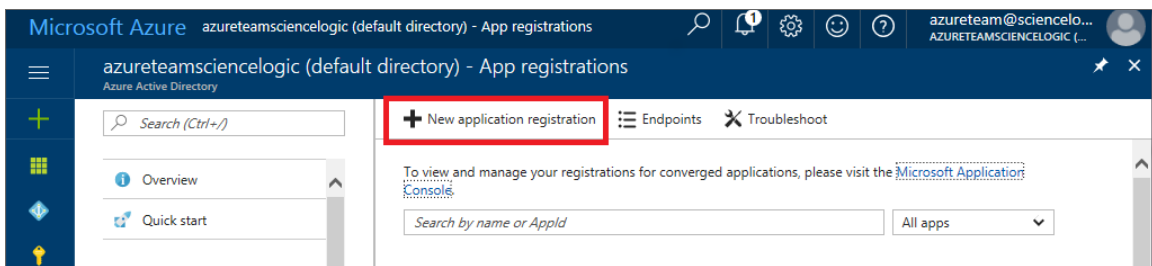
To create an Active Directory application in the Azure Portal:

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

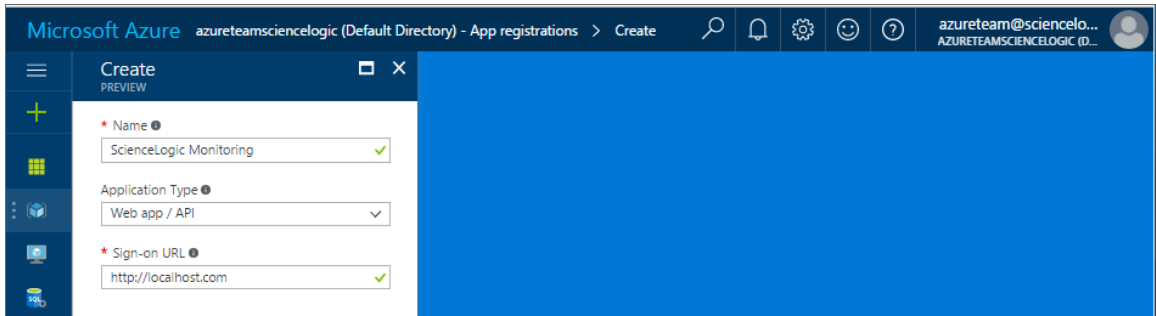
- From the left panel, click **[Azure Active Directory]**, then click **App registrations**. The **App registrations** page appears:



- 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.



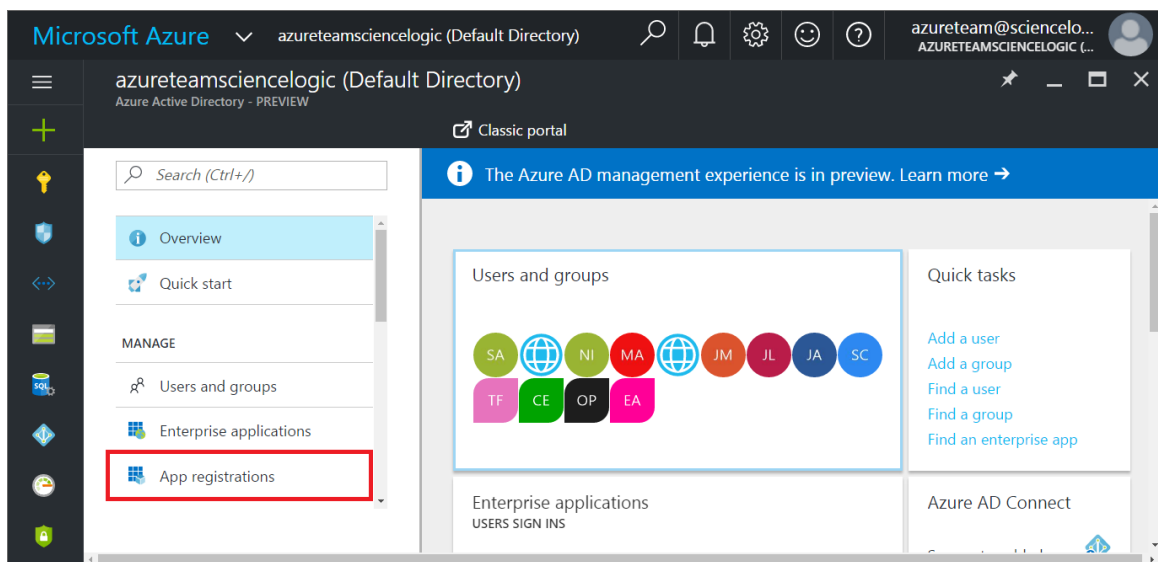
5. A message appears confirming that your application was added.

Adding the Microsoft Graph and Windows Azure Active Directory APIs

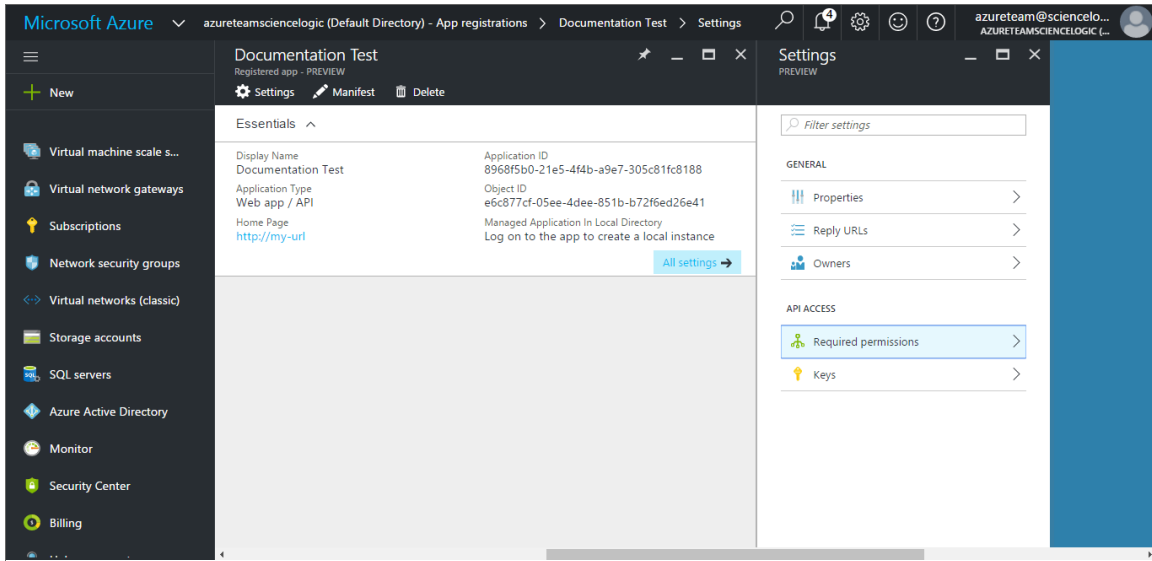
You must add the Microsoft Graph and Windows Azure Active Directory application programmable interfaces (APIs) to the Azure Active Directory application you will use to authenticate your Azure account. At a minimum, the Microsoft Graph and Windows Azure Active Directory APIs must have permission to read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

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

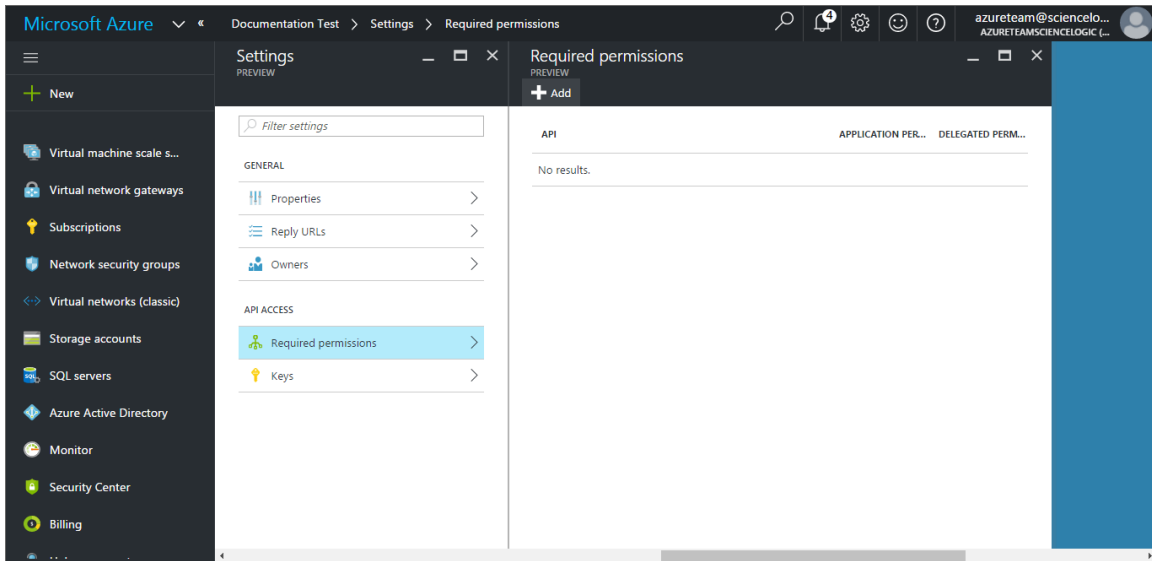
1. Log in to the new Azure portal at <https://portal.azure.com>.
2. In the left pane of the Azure portal, click **[Azure Active Directory]**.
3. Click **[App registrations]**, then click on the name of the Azure Active Directory application you will use to authenticate your Azure account.



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

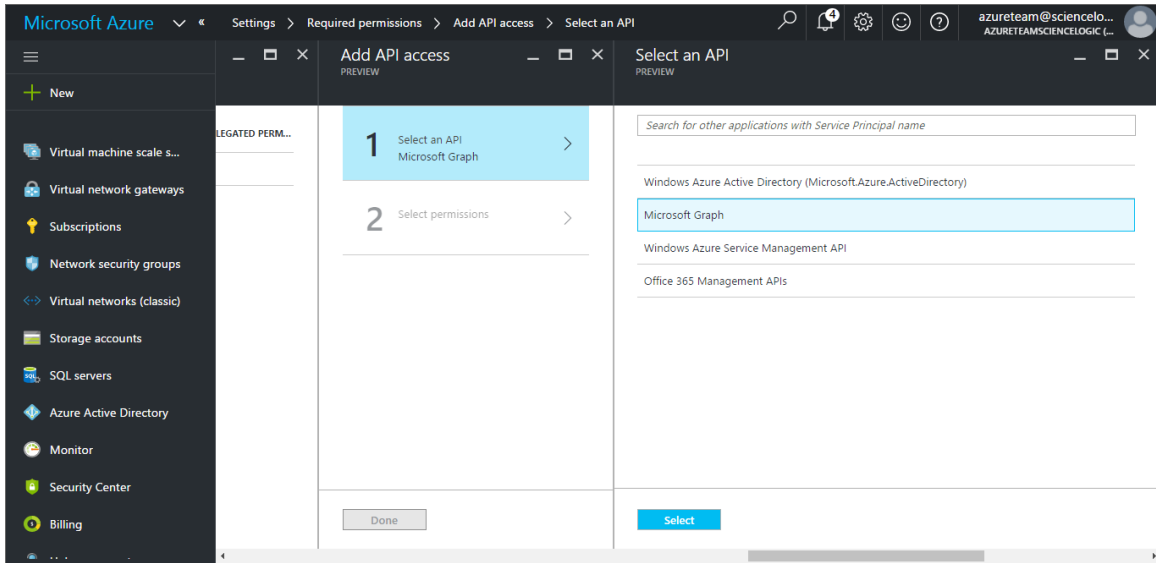


5. In the **Required permissions** pane, click **[Add]**.

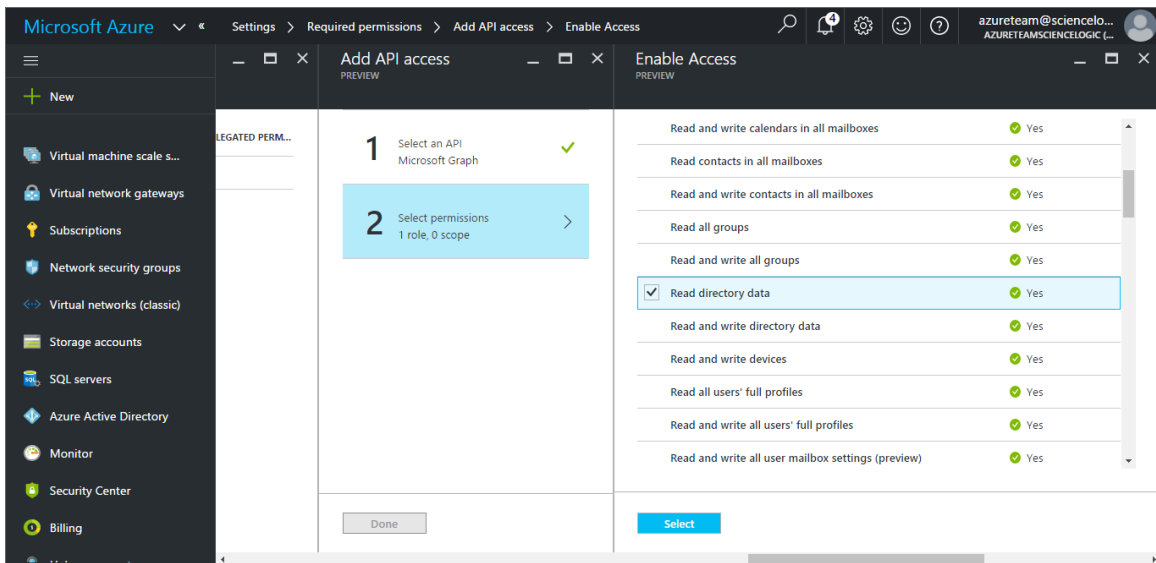


6. In the **Add API access** pane, click **[Select API]**.

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



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



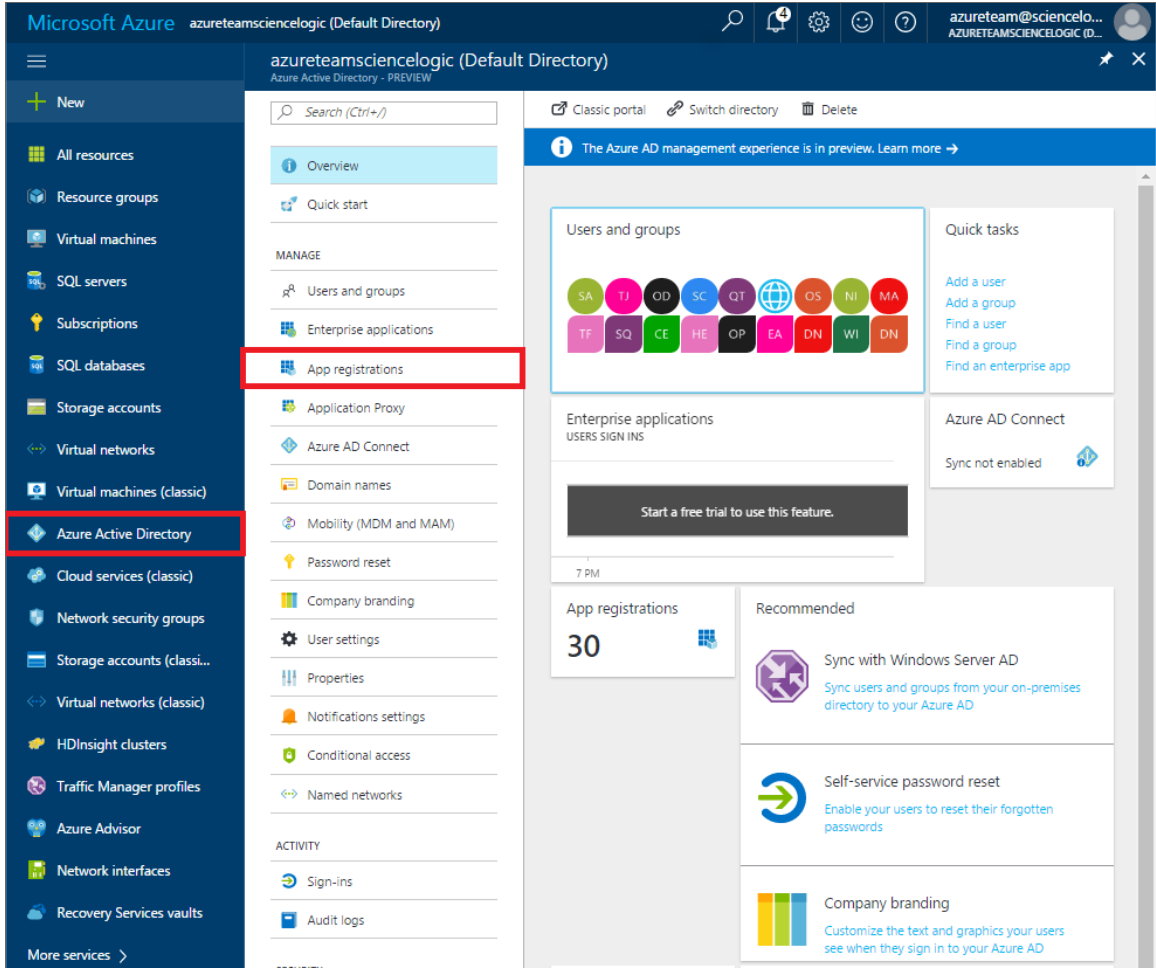
9. Click **[Done]** to save.
10. Repeat these steps for the Windows Azure Active Directory API. To do so, choose *Windows Azure Active Directory* (rather than *Microsoft Graph*) in step 7.

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.

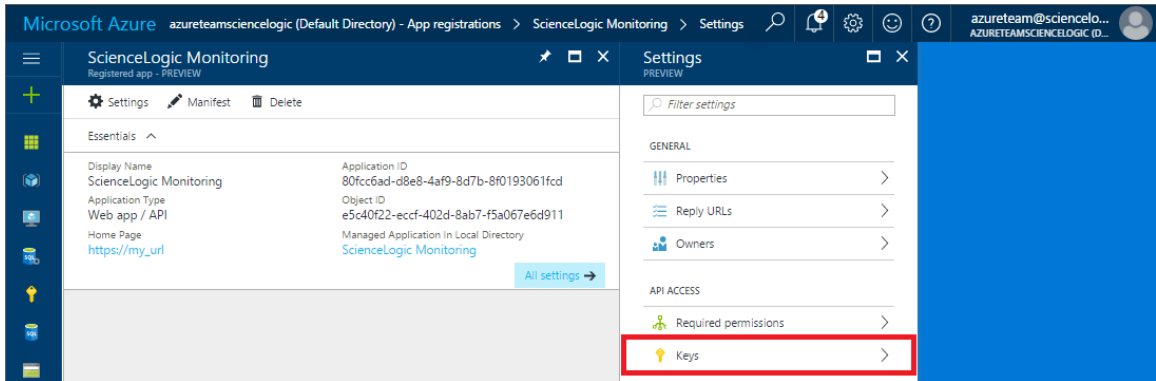
To generate a secret key:

1. In the left pane of the Azure portal (<https://portal.azure.com>), click **Active Directory**, then click **App registrations**. The **App registrations** page appears:

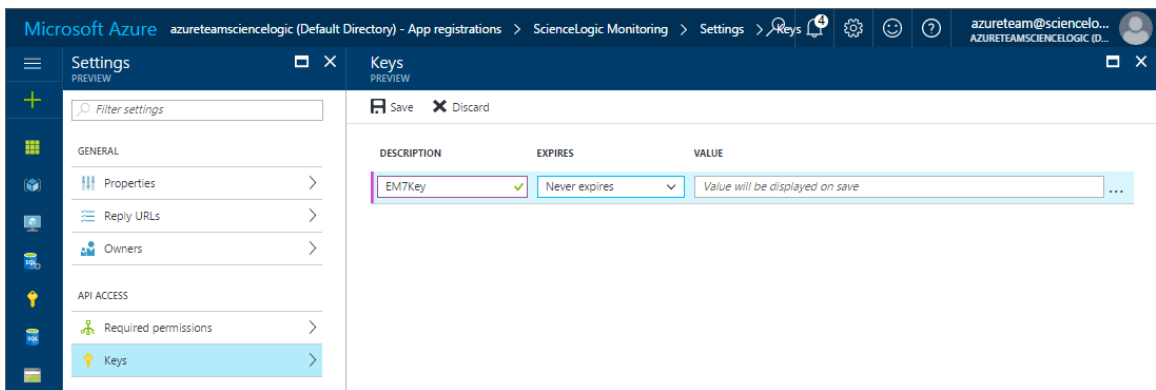


2. Click the application name.

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.

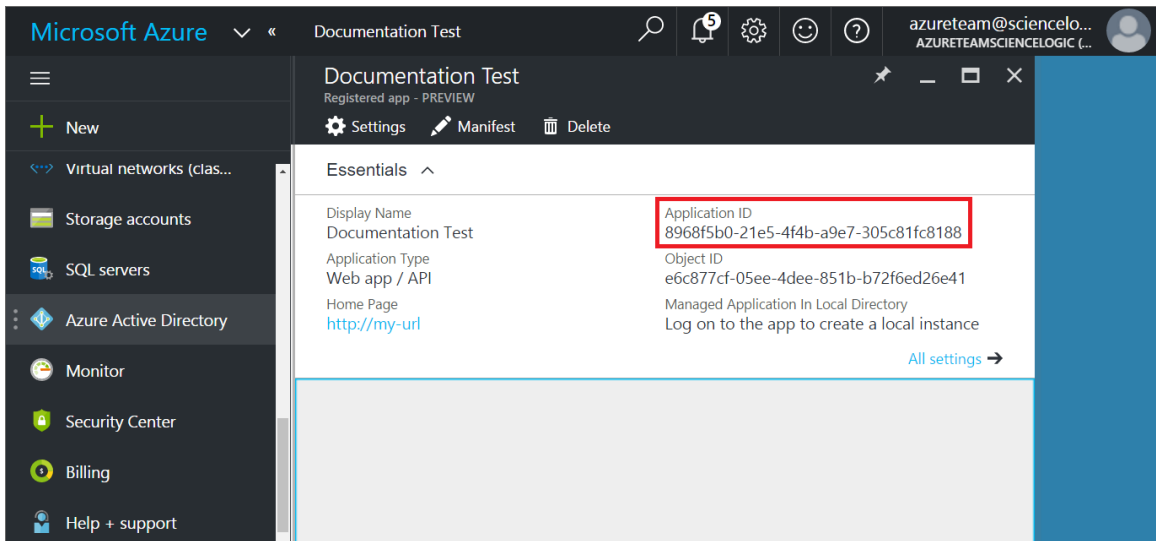
Locating the Application ID

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**.

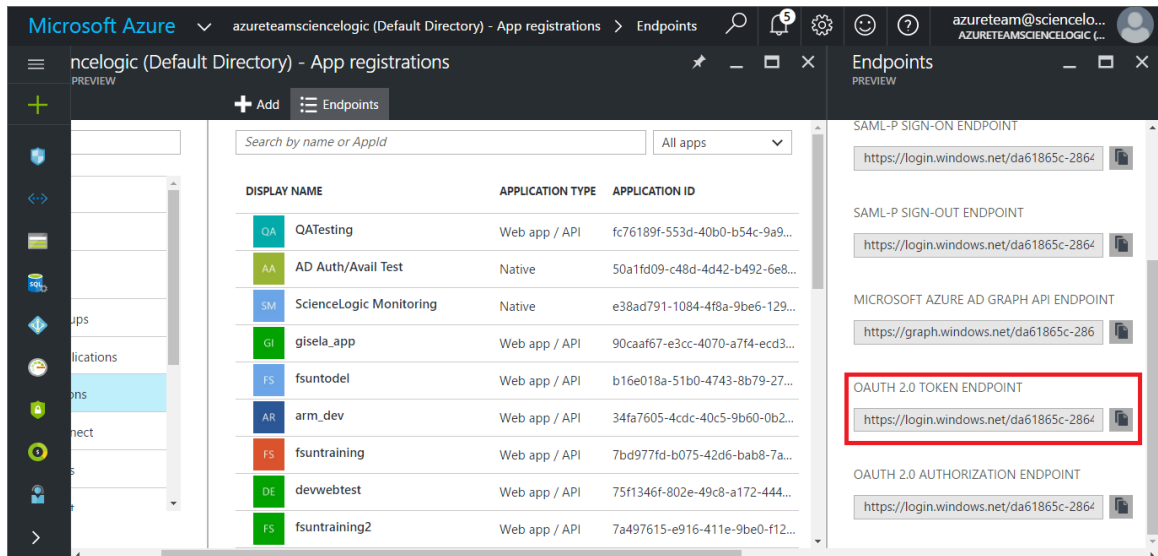
Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID

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]**.

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

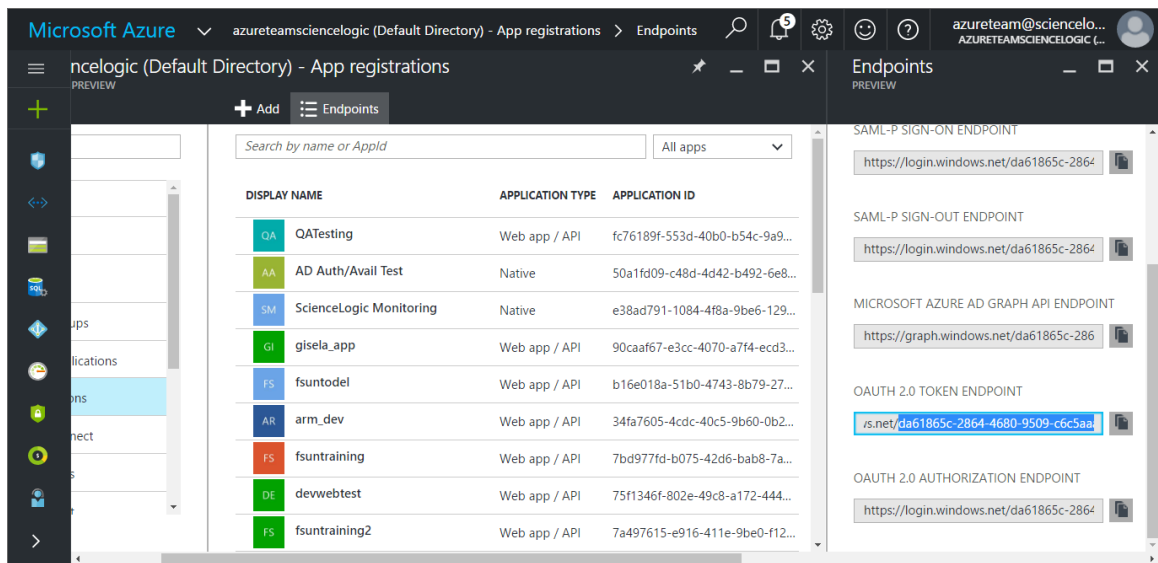


- Copy and save the **OAUTH 2.0 TOKEN ENDPOINT** URL.
- The OAuth 2.0 token endpoint URL contains a GUID, a string of characters in the middle of the URL.

For example, in the following OAuth 2.0 token endpoint URL, the GUID is in bold:

`https://login.windows.net/df69864c-2864-4680-5565-c6c5aafbf31bdf/oauth2/token`

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

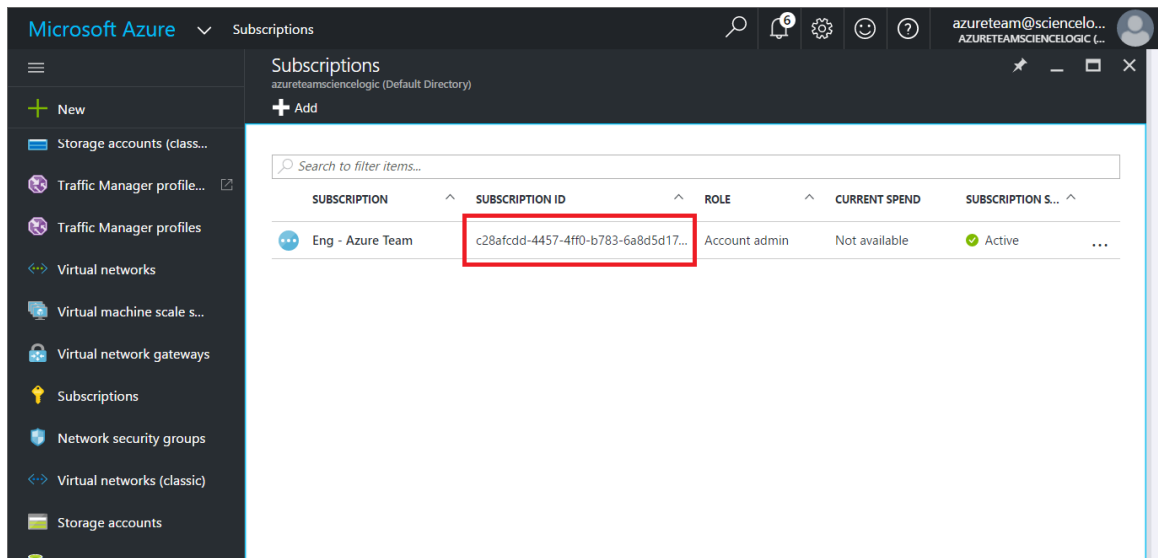


Locating the Subscription ID

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

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.



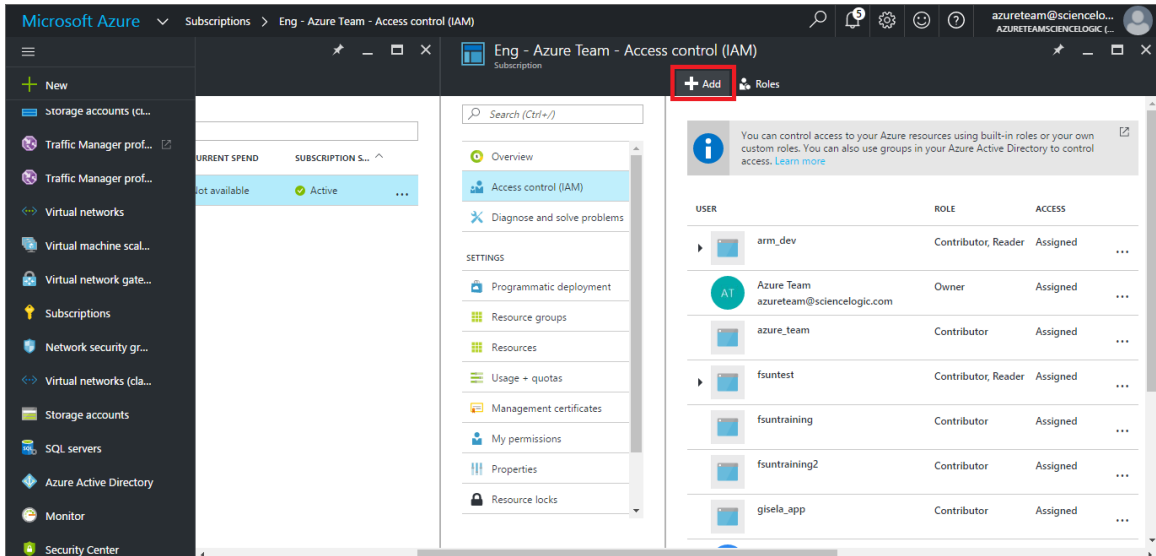
Adding Contributor Access to the Active Directory Application

To allow ScienceLogic to access your Azure account, you need to add Contributor access to the Active Directory application you will use to authenticate your account.

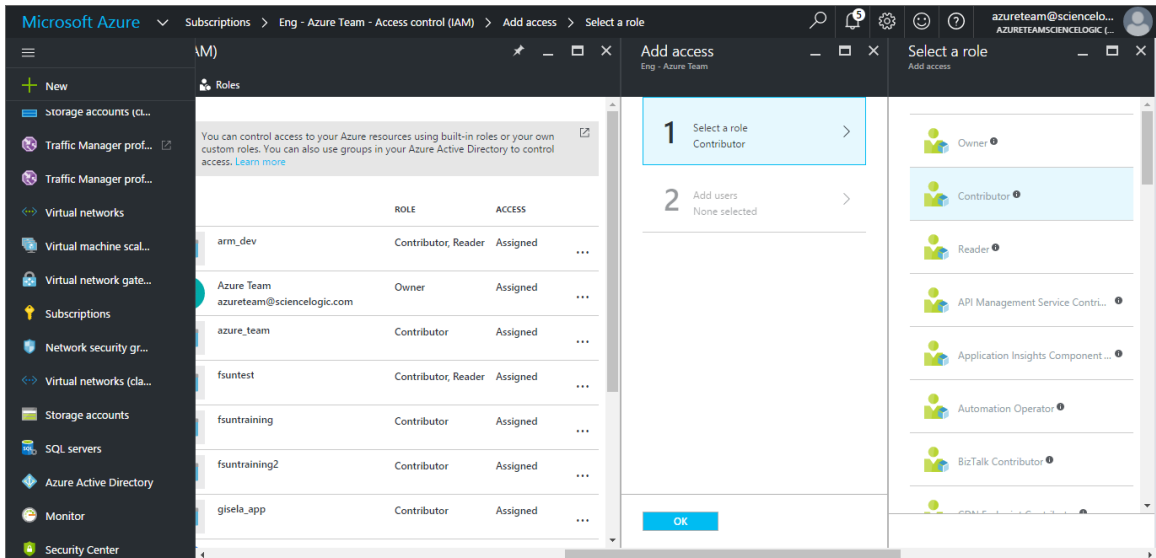
To add Contributor access to the Azure Active Directory application:

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

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

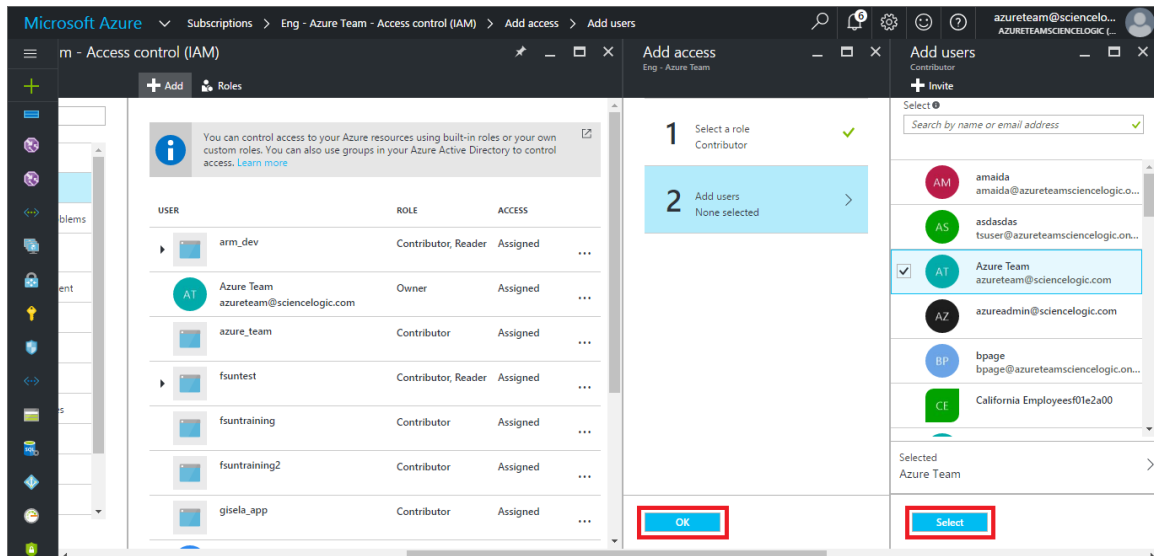


4. In the **Select a role** pane, select *Contributor*.



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

6. Click **[OK]** to add Contributor access to the application.



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: 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.

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.

To create a SOAP/XML credential for Azure:

1. Go to the **Credential Management** page (System > Manage > Credentials).

- Locate the sample SOAP/XML credential included in the *Microsoft: Azure PowerPack*, called **Azure Credential - SOAP/XML**, then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears:

- 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].** Type the Subscription ID for the Azure Active Directory application.
- **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]**.

Discovering Azure Services and Devices

Overview

The following sections describe the steps required to discover Microsoft Azure services and component devices in the ScienceLogic platform:

- [Creating an Azure Virtual Device](#)
- [Aligning the Azure Dynamic Applications](#)
- [Viewing Azure Component Devices](#)

Creating an Azure Virtual Device

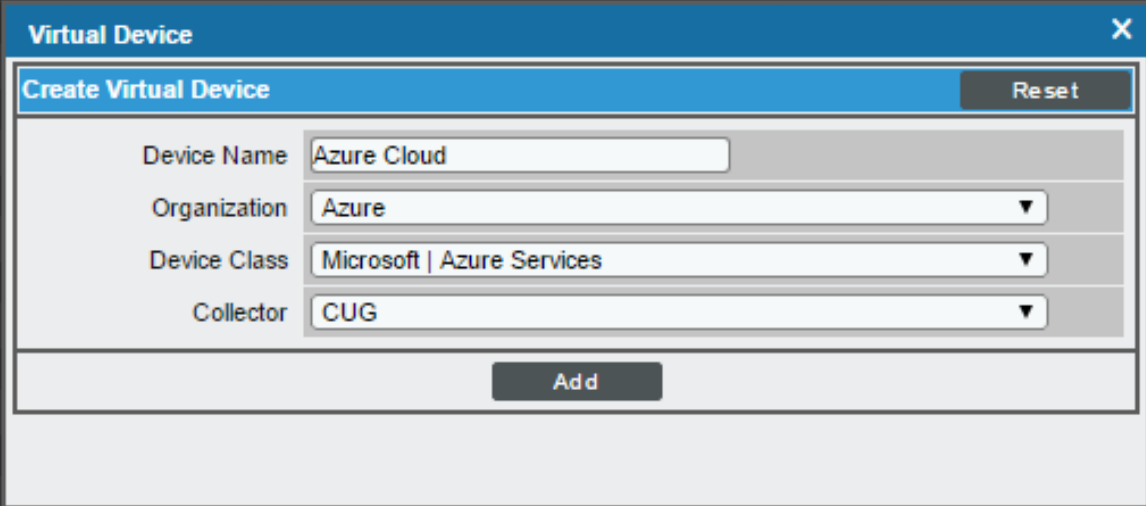
Because the Azure service does not have a static IP address, you cannot discover an Azure device using discovery. Instead, you must create a **virtual device** that represents the Azure service. A virtual device is a user-defined container that represents a device or service that cannot be discovered 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 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 the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.

3. Enter values in the following fields:



The screenshot shows a 'Virtual Device' dialog box with a 'Create Virtual Device' form. The form has four fields: 'Device Name' (text input with 'Azure Cloud'), 'Organization' (dropdown with 'Azure'), 'Device Class' (dropdown with 'Microsoft | Azure Services'), and 'Collector' (dropdown with 'CUG'). There is a 'Reset' button in the top right and an 'Add' button at the bottom center.

- **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.

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:

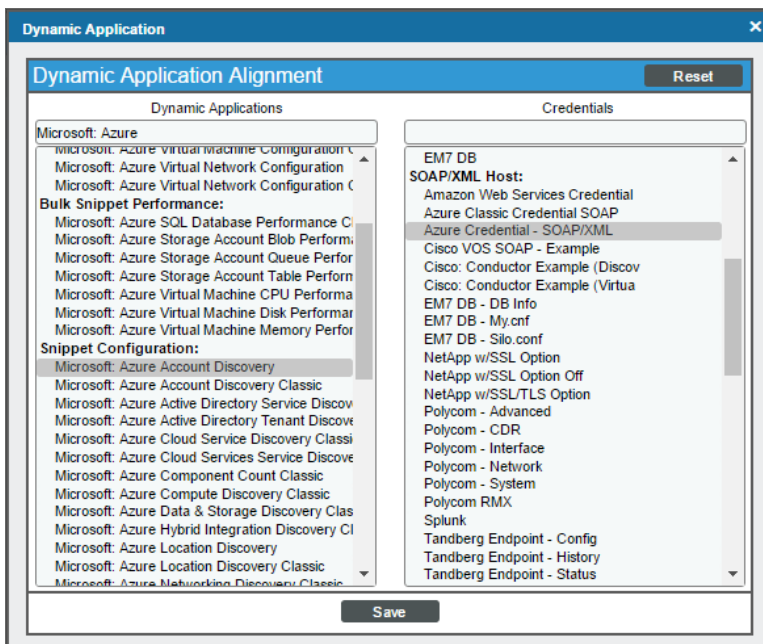
- **Discovery.** These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- **Configuration.** These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- **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. 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 the **[Actions]** button and select *Add Dynamic Application* from the menu.
5. In the **Dynamic Application Alignment** modal:



- In the **Dynamic Applications** field, select the *Microsoft: Azure Account Discovery* 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* 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 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:


- Resource Groups Services
 - Resource Groups
- Storage Services
 - Storage Accounts
 - Storage Tables
 - Storage Queues
 - Storage Containers
 - Storage Blobs
- Virtual Machines Services
 - Virtual Machines
- Virtual Network Services
 - 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

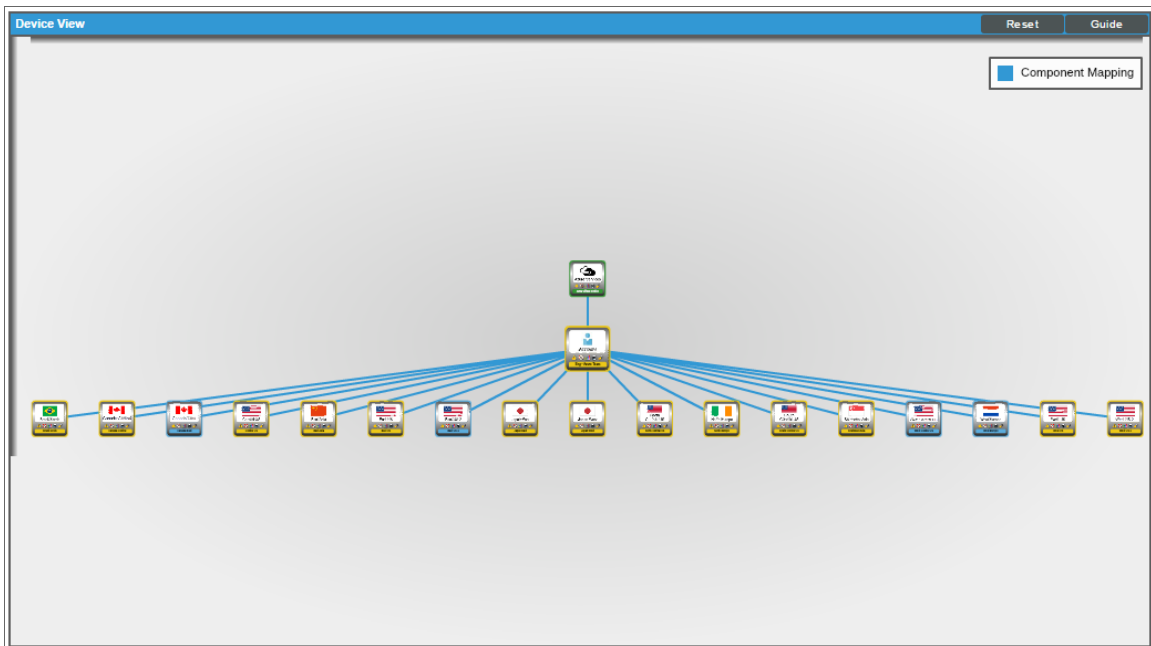
NOTE: The ScienceLogic platform might take several minutes to align these Dynamic Applications and create the component devices in your Azure service.

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.

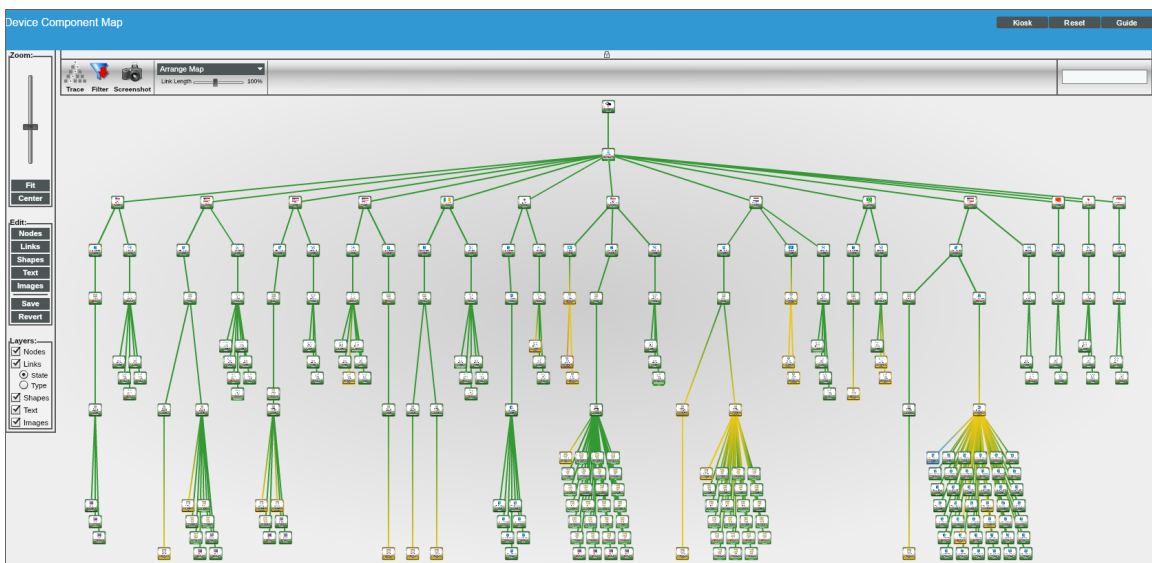
- The **Device View** modal page (click the bar-graph icon  for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device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

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State
Azure Cloud	--	Service	Microsoft Azure Services	24	Azure	Healthy	CUG	Active
azurelearn@sciencelogic.com	--	Account	Microsoft Azure Account	25	Azure	Healthy	CUG	Active
Brazil South	--	Location	Microsoft Azure Location Brazil South	34	Azure	Healthy	CUG	Active
Central US	--	Location	Microsoft Azure Location Central US	27	Azure	Healthy	CUG	Active
East Asia	--	Location	Microsoft Azure Location East Asia	36	Azure	Healthy	CUG	Active
East US	--	Location	Microsoft Azure Location East US	28	Azure	Healthy	CUG	Active
Data & Storage	--	Service	Microsoft Azure Data & Storage Service	43	Azure	Healthy	CUG	Active
Networking	--	Service	Microsoft Azure Networking Service	44	Azure	Healthy	CUG	Active
Virtual Networks	--	Service	Microsoft Azure Virtual Networks Service	69	Azure	Healthy	CUG	Active
vn-imp-36	--	Network	Microsoft Azure Virtual Network	109	Azure	Healthy	CUG	Active
vn-imp-7	--	Network	Microsoft Azure Virtual Network	107	Azure	Healthy	CUG	Active
vn-imp-8	--	Network	Microsoft Azure Virtual Network	108	Azure	Healthy	CUG	Active
East US 2	--	Location	Microsoft Azure Location East US 2	35	Azure	Healthy	CUG	Active
Japan East	--	Location	Microsoft Azure Location Japan East	37	Azure	Healthy	CUG	Active
Japan West	--	Location	Microsoft Azure Location Japan West	31	Azure	Healthy	CUG	Active
North Central US	--	Location	Microsoft Azure Location N. Central US	26	Azure	Healthy	CUG	Active
North Europe	--	Location	Microsoft Azure Location North Europe	30	Azure	Healthy	CUG	Active
South Central US	--	Location	Microsoft Azure Location S. Central US	32	Azure	Healthy	CUG	Active
Southeast Asia	--	Location	Microsoft Azure Location Southeast Asia	38	Azure	Healthy	CUG	Active
West Europe	--	Location	Microsoft Azure Location West Europe	33	Azure	Healthy	CUG	Active
West US	--	Location	Microsoft Azure Location West US	29	Azure	Healthy	CUG	Active

- 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 Machine Disks and Storage Blobs
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups
- Virtual Machines and Virtual Networks
- Virtual Machines and Subnets
- 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

© 2003 - 2017, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

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