Monitoring Microsoft Office 365

Beta Version

Microsoft: Office 365 *BETA* PowerPack version 100

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Microsoft Office 365 services in the ScienceLogic platform.

> **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 Microsoft Office 365?

Office 365 is Microsoft's suite of subscription-based productivity software and services. It includes web-based versions of the Microsoft Office software applications (e.g., Word, Excel, PowerPoint), cloud-hosted versions of Microsoft Office server platforms (e.g., Exchange, SharePoint, Skype for Business), cloud-based file storage (OneDrive), social networking (Yammer), and more.

What Does the Microsoft: Office 365 *BETA* PowerPack Monitor?

The *Microsoft: Office 365 *BETA** PowerPack enables you to discover, model, and monitor Office 365 services. The *Microsoft: Office 365 *BETA** PowerPack includes:

- An example credential you can use to create credentials to connect to the Office 365 service

- Dynamic Applications that discover and monitor the Office 365 service
- Device Classes for each of the Office 365 services, plus a generic service Device Class
- Event Policies for alert conditions in the Office 365 services

Chapter 2

Configuring Microsoft Office 365 Monitoring

Overview

The following sections describe how to configure the ScienceLogic platform to monitor Microsoft Office 365 services:

- *Configuring Office 365 Monitoring Using a SOAP/XML Credential*
- *Creating a Microsoft Office 365 Virtual Device*
- *Discovering the Microsoft Office 365 Component Devices*
- *Viewing Microsoft Office 365 Component Devices*

Configuring Office 365 Monitoring Using a SOAP/XML Credential

To create a SOAP/XML credential that allows the ScienceLogic platform to access Microsoft Office 365, you need the following information from your Office 365 account:

- Active Directory username and password for an administrative user
- Secret Key
- Client ID
- Tenant ID (GUID)
- Subscription ID

Before creating the SOAP/XML credential, you must first create (or already have) a client Active Directory application and an associated Active Directory administrative user in Microsoft Azure from which to capture the above information. You can then enter the required information when configuring the SOAP/XML credential in the ScienceLogic platform. The following sections describe these processes:

- *Creating a Client Active Directory Application in Azure for Office 365*
- *Configuring a SOAP/XML Credential for Office 365*

Creating a Client Active Directory Application in Azure Classic Portal

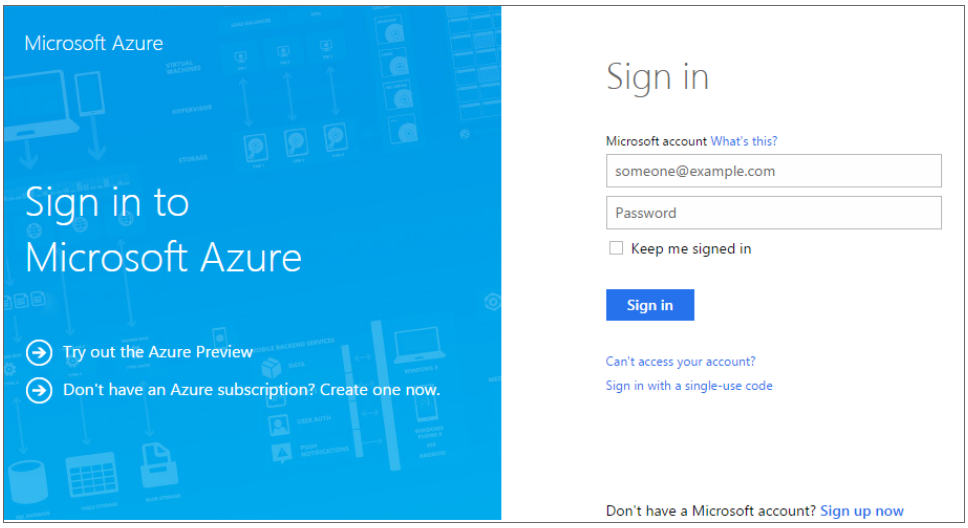
When configuring a SOAP/XML credential in the ScienceLogic platform to access Microsoft Office 365, you must know your Office 365 Subscription ID and the Client ID, Secret Key, and Tenant ID (GUID) of an Active Directory web application that can be used to authenticate your Office 365 account. This Active Directory application must have permission to access the Microsoft Office 365 Management APIs as an administrative user.

This section describes:

- How to create a new Active Directory application in the Azure Classic portal
- How to configure the Active Directory application so that it can access the Microsoft Office 365 Management APIs as an administrative user
- Where you can find the information about the Active Directory application that you will need to configure the SOAP/XML credential in the ScienceLogic platform.

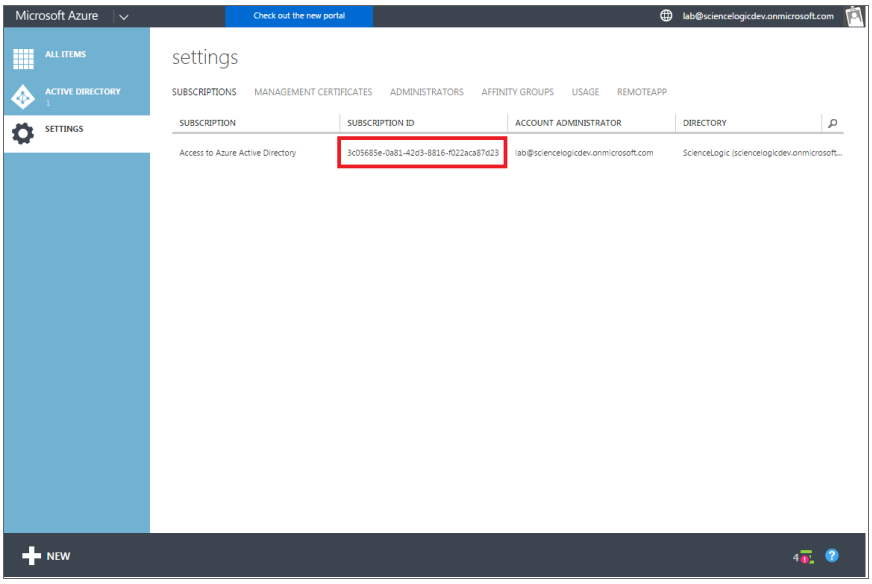
To create a client Active Directory application in the Azure Classic portal:

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:

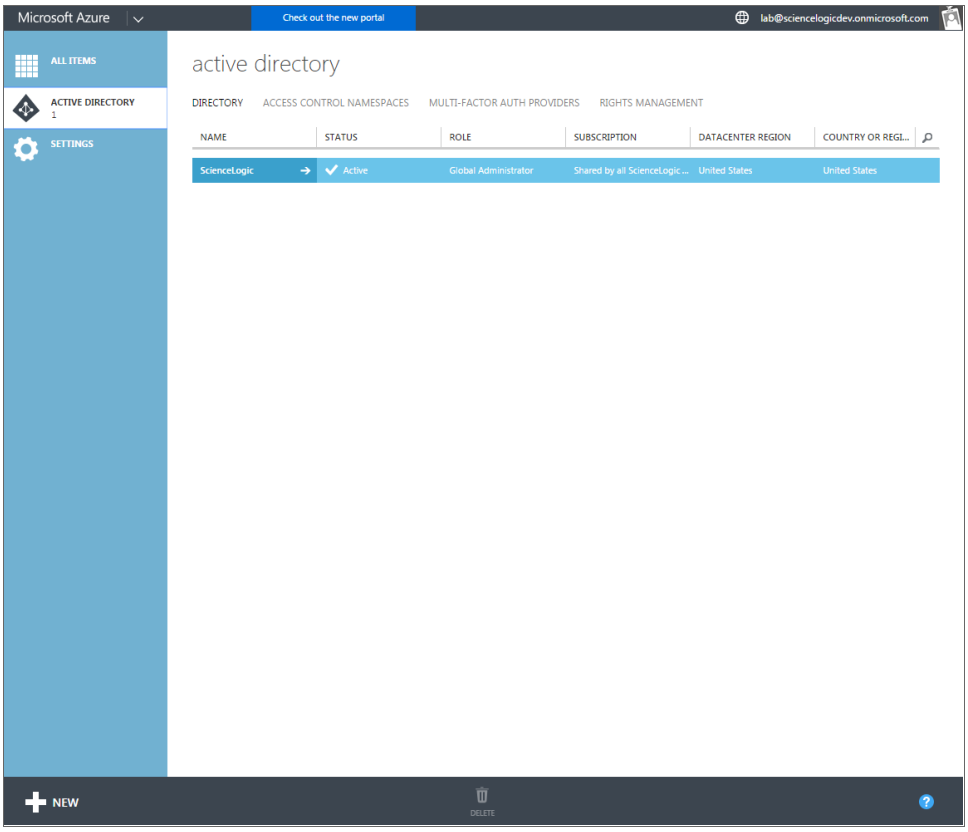


After logging in with your Office 365 administrative username and password, the **All Items** page appears.

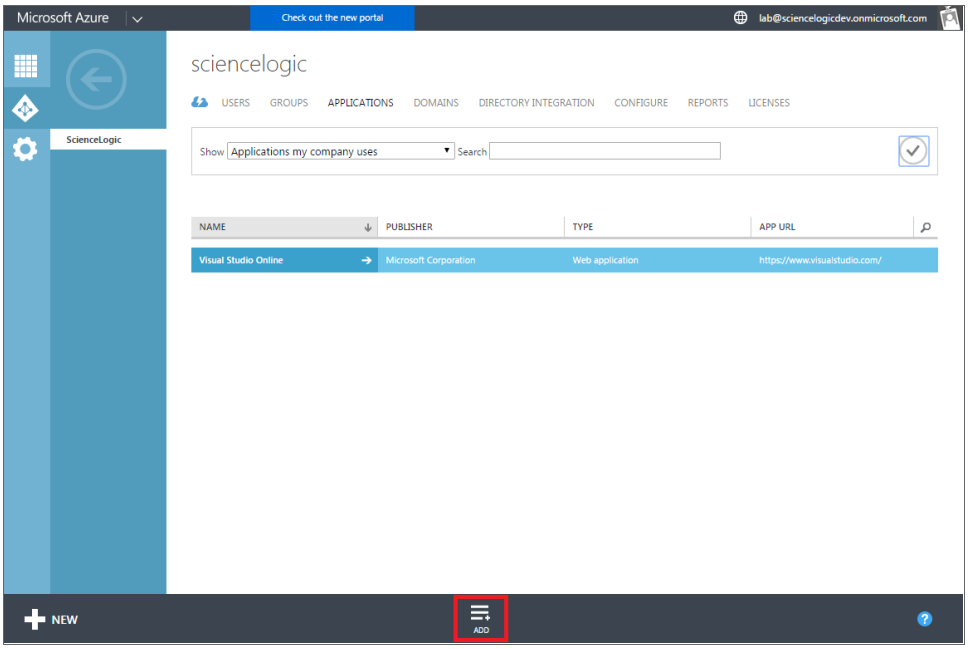
3. From the left panel, click **[Settings]**. The **Settings** page appears.
4. Write down or copy the ***Subscription ID***. *When you create the SOAP/XML credential in the ScienceLogic platform, you must supply the Subscription ID in the Embed Value [%3] field*.



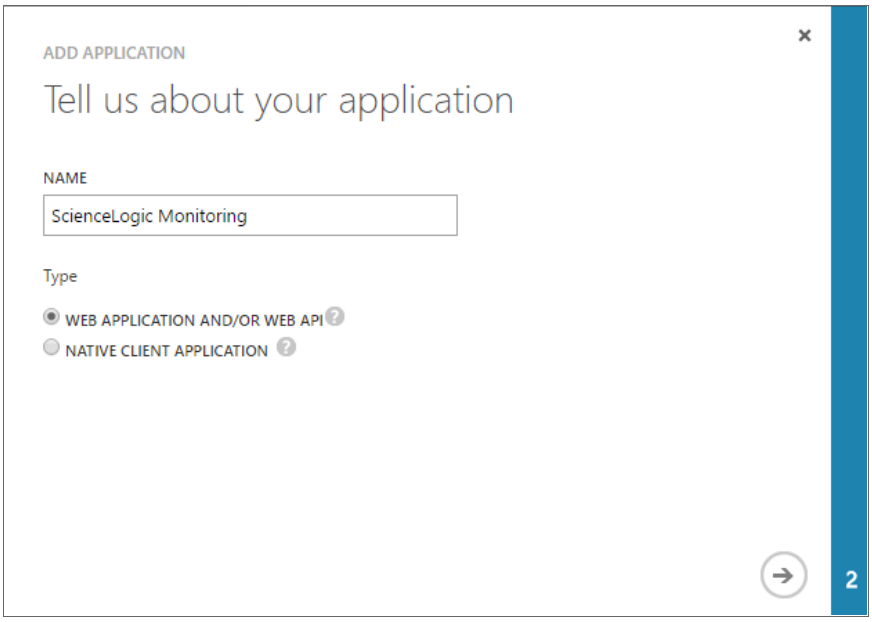
5. From the left panel, click **[Active Directory]**. The **Active Directory** page appears:



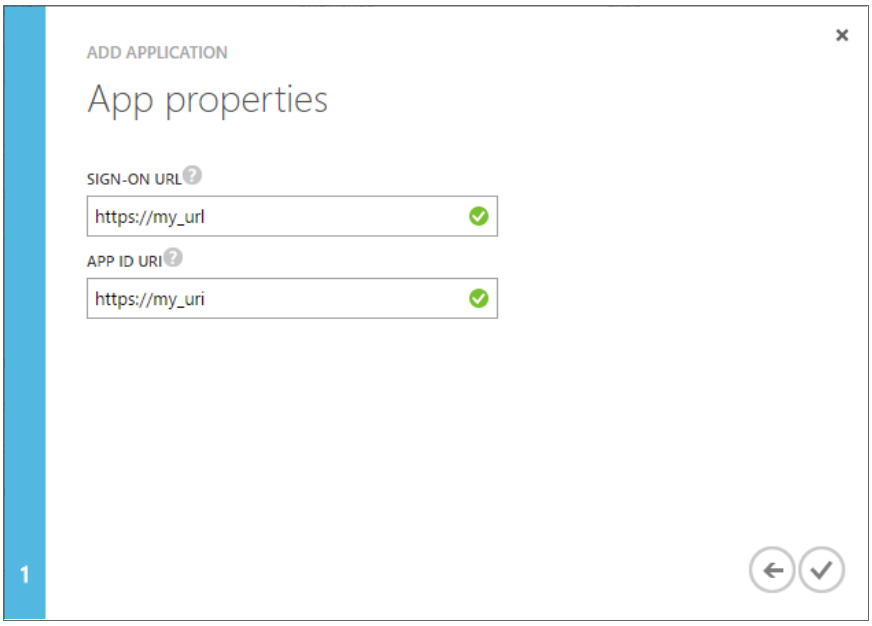
6. Click the ***Name*** of the Active Directory you want to use, then click the **[Applications]** tab. The **Applications** page appears.
7. Click the **[Add]** button.



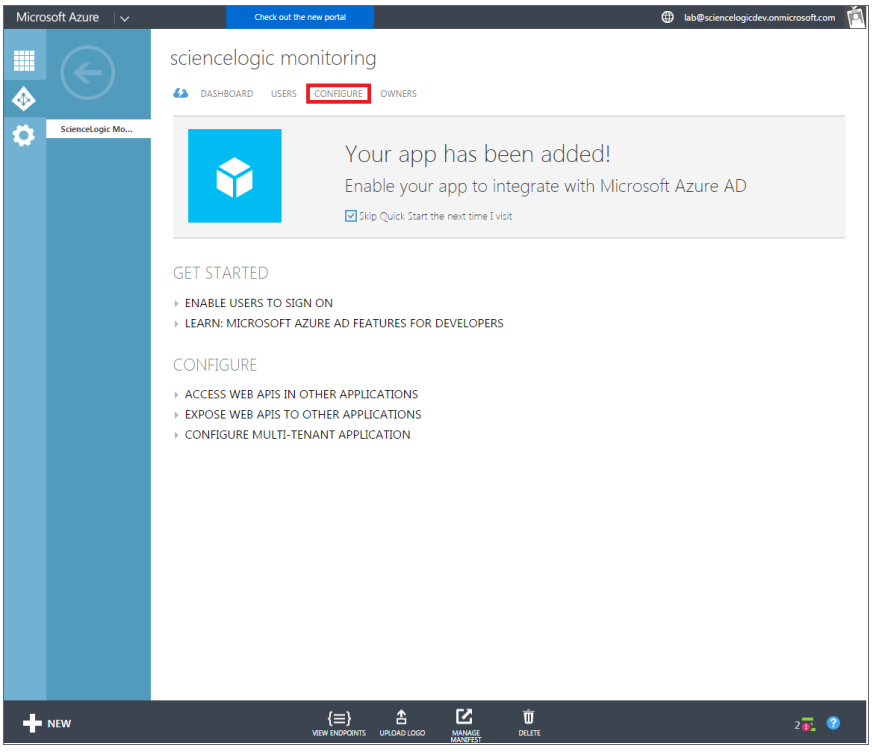
8. At the prompt, click **[Add an application my organization is developing]**. The **Add Application** modal page appears.
9. Enter a ***Name*** for the application and select the **[Web Application and/or Web API]** radio button, then click the right-arrow button to continue.



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



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

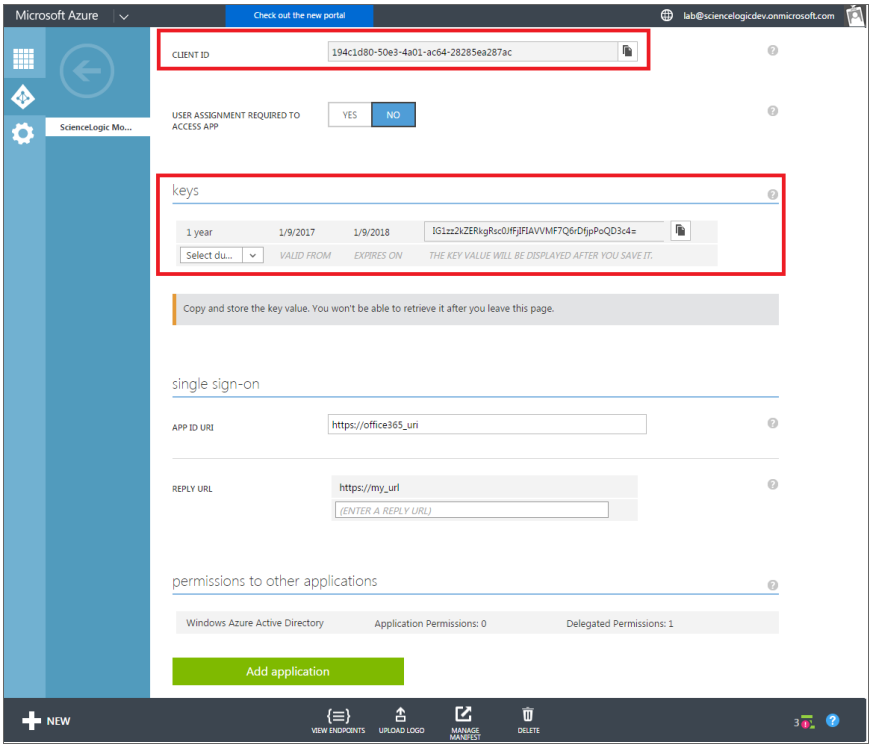


14. The **Properties** page appears. Write down or copy the ***Client ID***. *When you create the SOAP/XML credential in the ScienceLogic platform, you must supply the Client ID in the Embed Value [%1] field*.

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

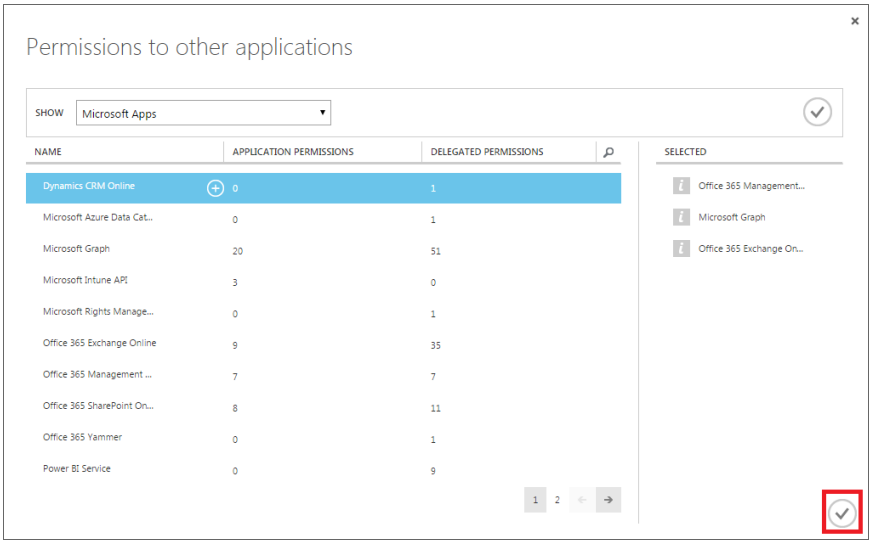
15. On the **Properties** page, in the **Keys** section, select a time duration from the drop-down menu to create a ***Secret Key***, then click **[Save]**. After saving, write or copy the ***Secret Key***. *When you create the SOAP/XML credential in the ScienceLogic platform, you must supply the Secret Key in the Embed Value [%4] field.*

CAUTION: ScienceLogic recommends that you write or copy the ***Secret Key*** before proceeding, as the key value will be hidden after you leave this page.



16. Click the **[Add application]** button.

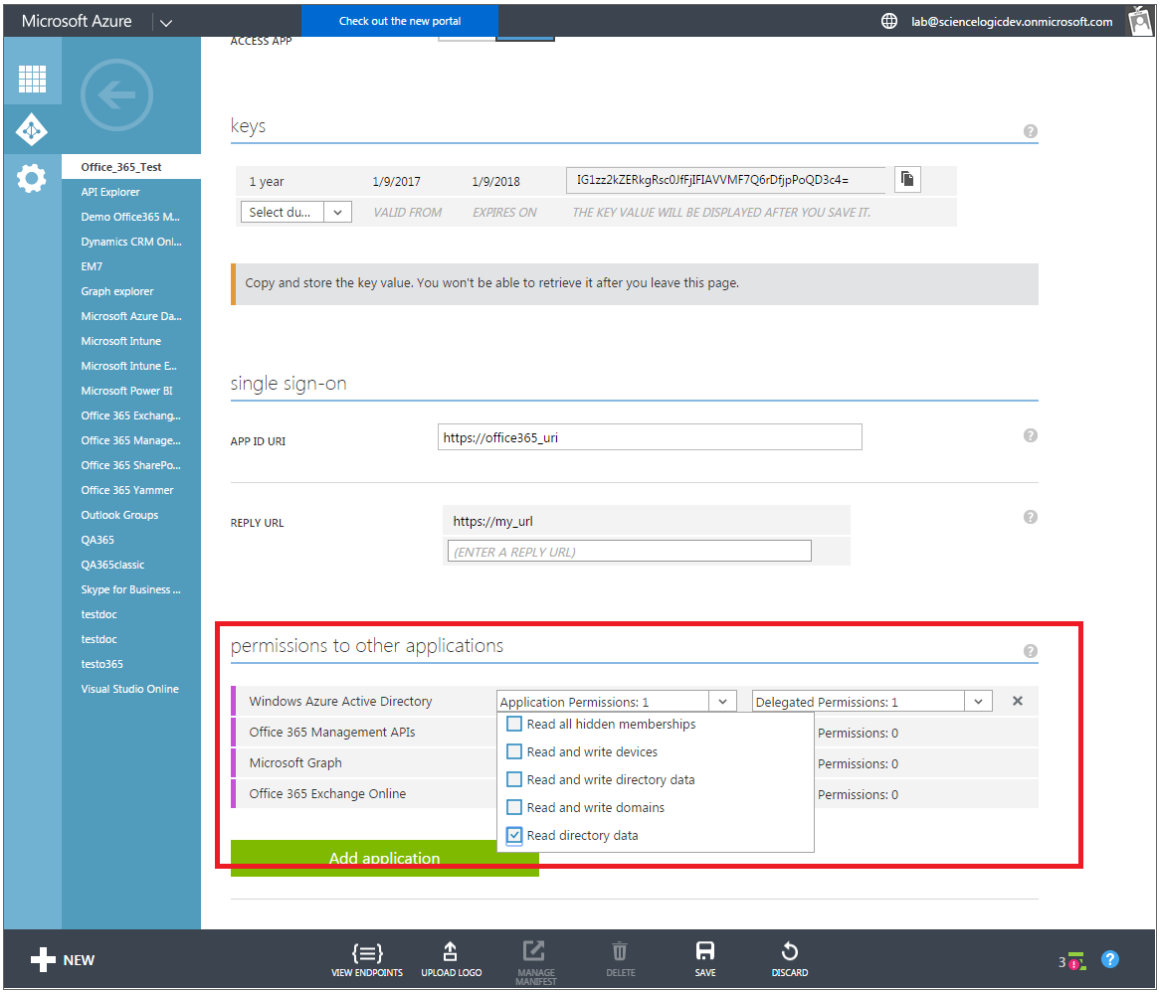
17. The **Permissions to other applications** modal page appears. From the list, select the following applications:



- Office 365 Management APIs
- Windows Azure Active Directory
- Microsoft Graph
- Office 365 Exchange Online (if monitoring Exchange Online services)

When you are finished, click the checkmark button.

18. On the **Properties** page, go to the **Permissions to Other Applications** section. For each selected application, hover over the ***Application Permissions*** field to make a drop-down menu appear. Then make the following selections:

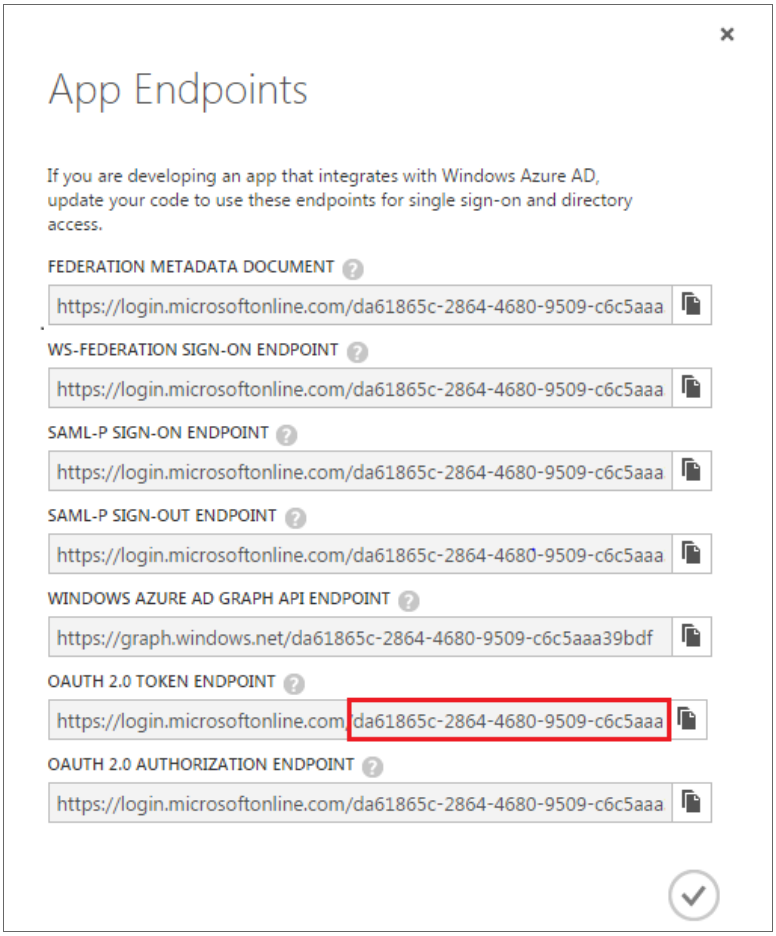


- ***Office 365 Management APIs***. Select all seven Read permissions (and any other permissions desired).
- ***Windows Azure Active Directory***. Select *Read Directory Data* (and any other permissions desired).
- ***Microsoft Graph***. Select *Read Directory Data* (and any other permissions desired).
- ***Office 365 Exchange Online***: Select any permissions desired.

When you are finished, click **[Save]**.

19. Click **[View Endpoints]**. The **App Endpoints** modal page appears.

20. The ***OAuth 2.0 Token Endpoint URL*** contains a GUID that is used as a ***Tenant ID***. Copy or write down the GUID/Tenant ID. *When you create the SOAP/XML credential in the ScienceLogic platform, you must supply the Tenant ID in the URL and Embed Value [%2] fields*.



Configuring a SOAP/XML Microsoft Office 365 Credential

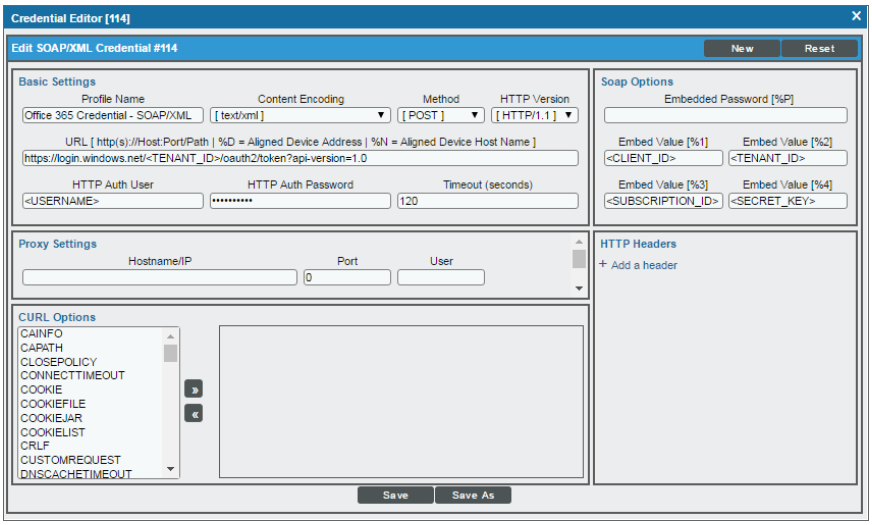
To configure the ScienceLogic platform to monitor Microsoft Office 365, you must first create a SOAP/XML credential. This credential allows the platform (specifically, the Dynamic Applications in the *Microsoft: Office 365 *BETA** PowerPack) to communicate with your Office 365 account.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential to access Microsoft Office 365:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **Office 365 Credential - SOAP/XML** credential, then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears.

3. Enter values in the following fields:



Basic Settings

- ***Profile Name***. Enter a name for the Microsoft Office 365 credential.
- ***Content Encoding***. Select *text/xml*.
- ***Method***. Select POST.
- ***HTTP Version***. Select HTTP/1.1.
- ***URL***. Enter "https://login.windows.net/<TENANT_ID>/oauth2/token?api-version=1.0", replacing <TENANT_ID> with your Office 365 Tenant ID.
- ***HTTP Auth User***. Enter the Office 365 administrator username.
- ***HTTP Auth Password***. Enter the Office 365 administrator password
- ***Timeout (seconds)***. Enter "120".

Proxy Settings

- ***Hostname/IP***. Leave this field blank.
- ***Port***. Enter "0".
- ***User***. Leave this field blank.

CURL Options

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

SOAP Options

- ***Embedded Password [%P]***.
- ***Embed Value [%1]***. Enter the Office 365 Client ID.

- ***Embed Value [%2]***. Enter the Office 365 Tenant ID.
- ***Embed Value [%3]***. Enter the Office 365 Subscription ID.
- ***Embed Value [%4]***. Enter the Office 365 Secret Key.

HTTP Headers

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

NOTE: The Office 365 account username and password that you enter in the credential should belong to a user with "Service Administrator" rights or greater for the Office 365 account.

4. Click the **[Save As]** button.

Creating a Microsoft Office 365 Virtual Device

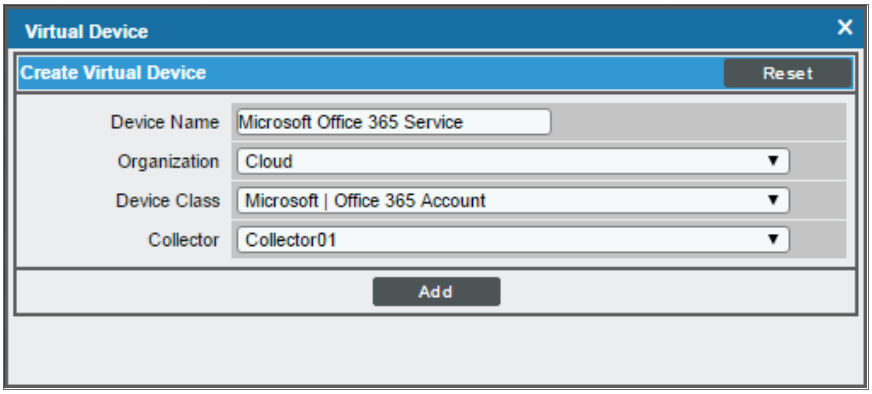
Because the Microsoft Office 365 service does not have an IP address, you cannot discover an Office 365 device using discovery. Instead, you must create a ***virtual device*** that represents the root device for the Office 365 service. A virtual device is a user-defined container that represents a device 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 Office 365 subscriptions you want to monitor, you should create a separate virtual device for each root device. You can also create different organizations for each Office 365 subscription.

To create a virtual device that represents your Office 365 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, you could enter "Microsoft Office 365 Service" 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 | Office 365 Account*.
- ***Collector***. Select the collector group that will monitor the device.

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

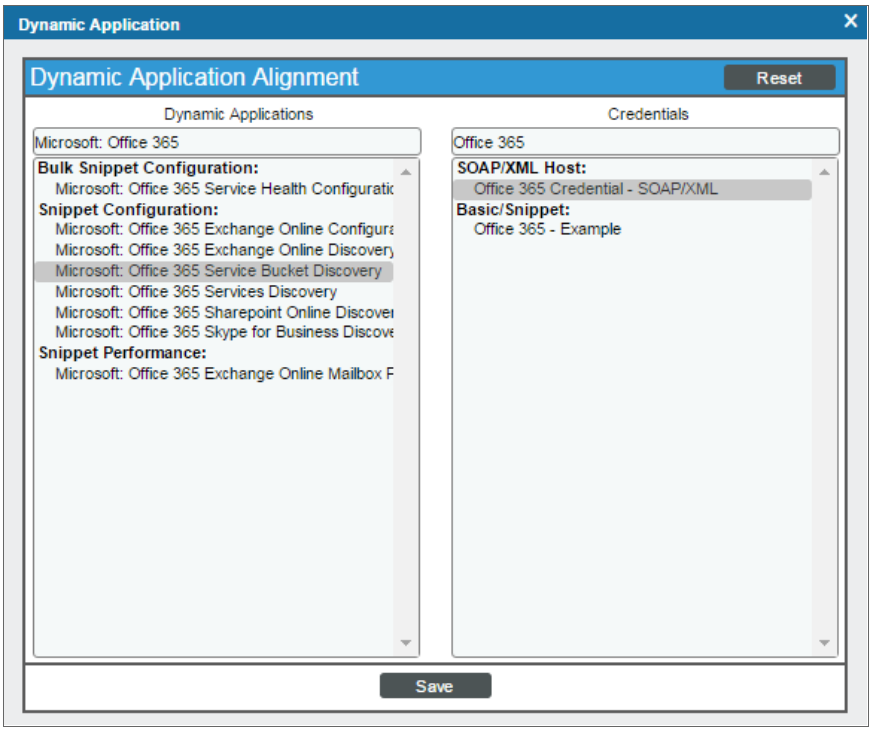
Discovering Microsoft Office 365 Component Devices

To discover and model the components of your Office 365 service, you must manually align the *Microsoft: Office 365 Service Bucket Discovery* Dynamic Application with the Office 365 virtual device. When you do so, the *Microsoft: Office 365 Service Bucket Discovery* Dynamic Application uses the virtual device as the root component device representing the Office 365 account and creates child component devices for each Office 365 service used by that account.

To align the *Microsoft: Office 365 Service Bucket Discovery* Dynamic Application to your Office 365 virtual device, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Click the wrench icon ( ) for your Office 365 virtual device.
3. In the **Device Administration** panel, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
4. Click the **[Action]** button and select *Add Dynamic Application* from the menu.

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



   - In the ***Dynamic Applications*** field, select the *Microsoft: Office 365 Service Bucket Discovery* Dynamic Application.
   - In the ***Credentials*** field, select the *credential you created for your Office 365 service*.

6. Click the **[Save]** button to align the Dynamic Application with the Office 365 virtual device and discover the Office 365 service.

Several minutes after discovery has completed, the following Dynamic Applications from the *Microsoft: Office 365 *BETA** PowerPack should automatically align to the service:

- Microsoft: Office 365 Exchange Discovery
- Microsoft: Office 365 Skype for Business Discovery
- Microsoft: Office 365 Sharepoint Online Discovery
- Microsoft: Office 365 Services Discovery

These Dynamic Applications will create child component devices for each service used by the Office 365 account.

To verify that these Dynamic Applications were automatically aligned during discovery, wait several minutes for the Office 365 service to be discovered and then repeat steps 1-3. The additional Dynamic Applications should appear on the **Dynamic Application Collections** page.

If they do not, then repeat steps 4-6, selecting the missing Dynamic Application(s) in the ***Dynamic Applications*** field on the **Dynamic Application Alignment** modal page.

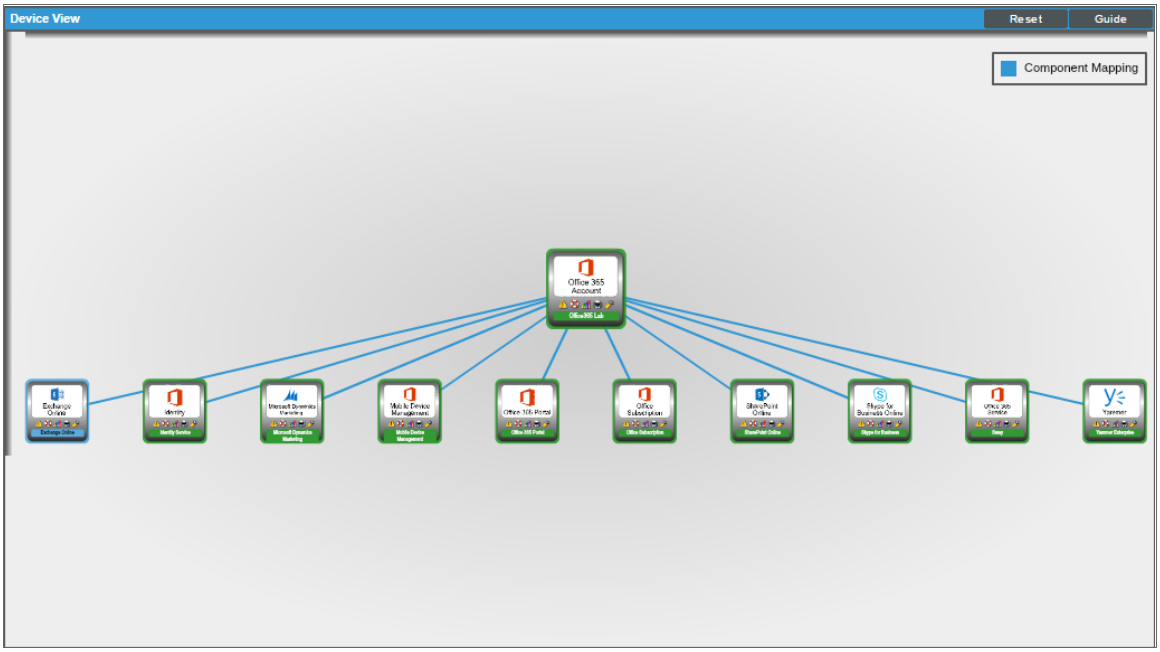
Viewing Microsoft Office 365 Component Devices

When the ScienceLogic platform performs collection for the Microsoft Office 365 virtual device, the platform will create component devices that represent each application in your Office 365 service.

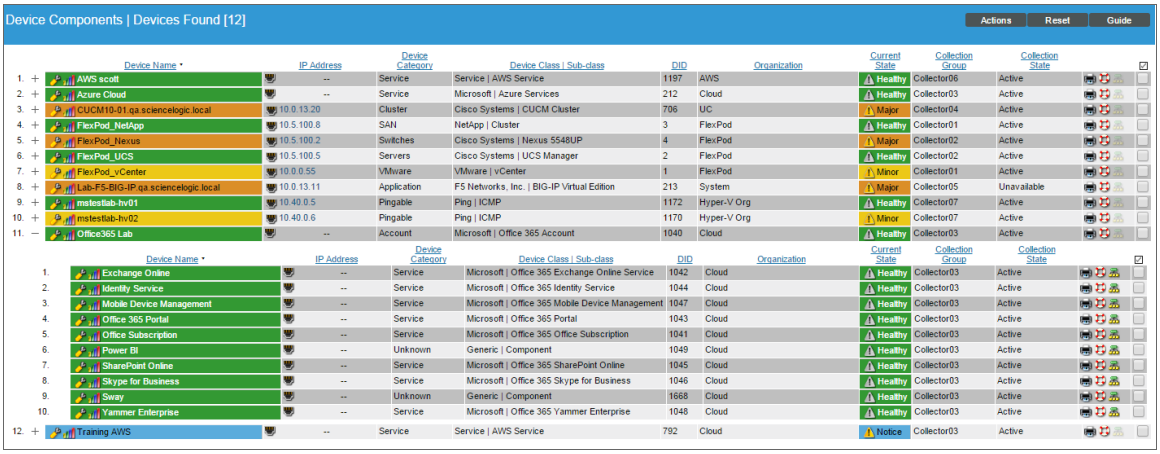
NOTE: Most Office 365 applications (e.g., Exchange Online, Skype for Business) have their own designated Device Classes and icons in the ScienceLogic platform. If a service does not have its own specific Device Class, it will have a Device Class of "Office 365 Generic Service" and an icon for generic Office 365 Service component devices.

In addition to the **Device Manager** page, you can view the Office 365 service and all associated component devices in the following places in the user interface:

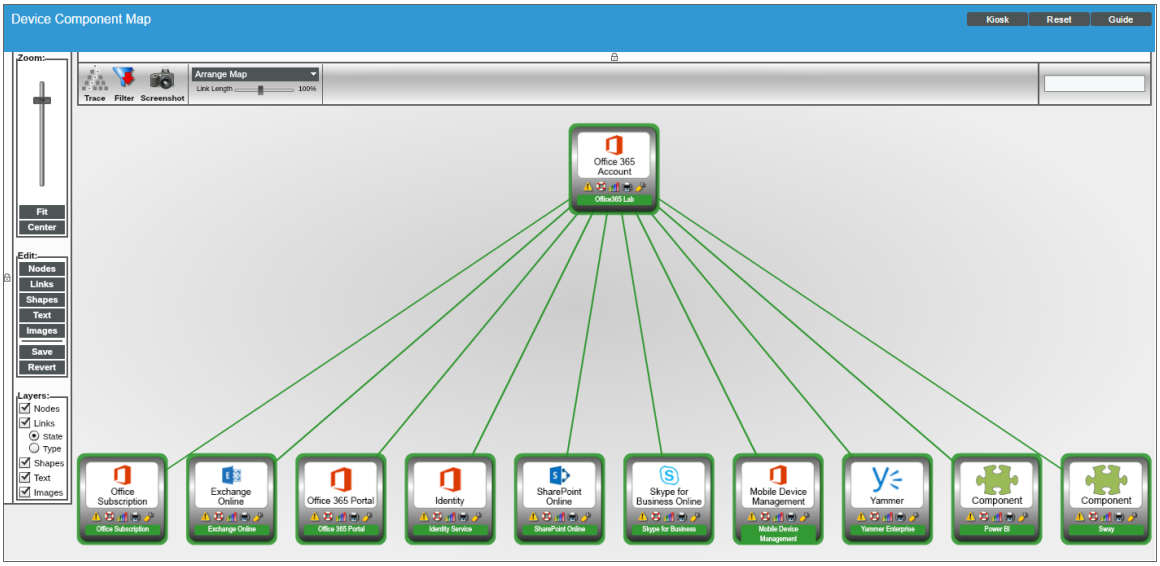
- The **Device View** modal page (click the bar-graph icon [] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page with the selected device the 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 your Office 365 service, find the Office 365 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 your Office 365 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.



Monitoring Microsoft Office 365 Alerts and Events

The *Microsoft: Office 365 *BETA** PowerPack includes a Dynamic Application, *Microsoft: Office 365 Service Health Configuration*, which monitors the overall health of each Office 365 service managed in the ScienceLogic platform. This Dynamic Application also creates events and triggers alerts in the following scenarios:

- Critical: Indicates a service disruption. This usually means users cannot access their email, documents, or presence information.
- Major: Indicates that a service incident is in the process of being resolved.
- Minor: Indicates the service is slow, sluggish, or occasionally unresponsive for brief periods.
- Notice: Indicates that steps have been completed to resolve the service incident, but some service actions might take longer than normal to complete. Additionally, indicates when a report of the service incident has been published.
- Healthy: Indicates that the service is available and has suffered no incidents during the reporting time period.

NOTE: For more information about events and alerts, including how to view and respond to them, see the ***Events*** manual.

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