Monitoring Microsoft Office 365

Microsoft: Office 365 PowerPack version 104

Table of Contents

Introduction 3
What is Microsoft Office 365? 3
What Does the Microsoft: Office 365 PowerPack Monitor? 4
Installing the Microsoft: Office 365 PowerPack 5
Configuration and Discovery 7
Configuring Office 365 Monitoring 8
Creating an Office 365 Active Directory Application in the Azure Portal 8
Adding API Permissions to the Application 11
Generating the Secret Key 14
Granting Admin Consent on Enterprise Applications 14
Creating a SOAP/XML Credential for Microsoft Office 365 15
Testing Your Office 365 Credential 17
Testing Your Office 365 Credential in the SL1 Classic User Interface 18
Discovering Office 365 Devices 19
Creating a Microsoft Office 365 Virtual Device 19
Configuring the Office 365 Device Template 20
Aligning the Device Template to Your Office 365 Virtual Device 21
Viewing Microsoft Office 365 Component Devices 22
Relationships Between Component Devices 24

Chapter 1

Introduction

Overview

This manual describes how to monitor Microsoft Office 365 services in SL1 using the Dynamic Applications in the *Microsoft: Office 365* PowerPack.

The following sections provide an overview of Microsoft Office 365 and the *Microsoft: Office 365* PowerPack:

What is Microsoft Office 365? 3

What Does the Microsoft: Office 365 PowerPack Monitor? 4

Installing the Microsoft: Office 365 PowerPack 5

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 (including Word, Excel, and PowerPoint), cloud-hosted versions of Microsoft Office server platforms (such as Exchange, SharePoint, and Skype for Business), cloud-based file storage (OneDrive), social networking (Yammer), and more.

What Does the Microsoft: Office 365 PowerPack Monitor?

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

- Dynamic Applications that discover, model, and collect data for the following Office 365 resources:
    - Azure Information Protection
    - Bookings
    - Dynamics 365
    - Dynamics CRM Online Service
    - Dynamics Marketing
    - Exchange Online Archiving Service
    - Exchange Online Protection Service
    - Exchange Online Service
    - Exchange Online Threat Protection
    - Generic Service
    - Identity Service
    - Intune
    - Mobile Device Management
    - Office Applications Service
    - Office Online Service
    - Office Subscription
    - OneDrive for Business Service
    - Planner
    - Platform Service
    - Portal
    - Power BI for Office 365 Service
    - Power BI Service
    - Project Online Service
    - Project Pro Service
    - Rights Management Service
    - SharePoint Online
    - Skype for Business
    - Social Engagement
    - StaffHub

    - Sway
    - Teams
    - Yammer Enterprise

- Device Classes for each type of Office 365 resource monitored, plus a generic service Device Class
- Event Policies that are triggered when Office 365 resources meet certain status criteria
- A Device Template that helps align Dynamic Applications to devices
- Sample Credentials for discovering Office 365 resources
- A Credential Test to ensure that your Office 365 credential works as expected

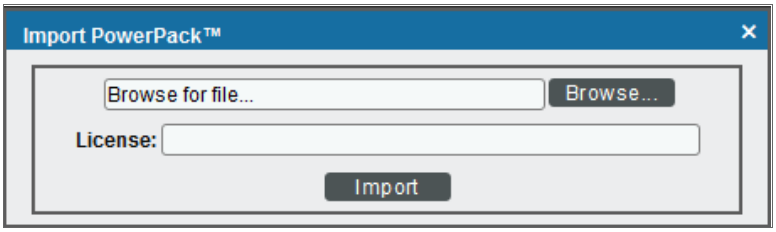
Installing the Microsoft: Office 365 PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Microsoft: Office 365* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of 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.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
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 appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal 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. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure Microsoft Office 365 services for monitoring by SL1 using the *Microsoft: Office 365* PowerPack:

Configuring Office 365 Monitoring 8
Creating an Office 365 Active Directory Application in the Azure Portal 8
Adding API Permissions to the Application 11
Generating the Secret Key 14
Granting Admin Consent on Enterprise Applications 14
Creating a SOAP/XML Credential for Microsoft Office 365 15
Testing Your Office 365 Credential 17
Testing Your Office 365 Credential in the SL1 Classic User Interface 18
Discovering Office 365 Devices 19
Creating a Microsoft Office 365 Virtual Device 19
Configuring the Office 365 Device Template 20
Aligning the Device Template to Your Office 365 Virtual Device 21
Viewing Microsoft Office 365 Component Devices 22
Relationships Between Component Devices 24

Configuring Office 365 Monitoring

To create a SOAP/XML credential that allows SL1 to access Microsoft Office 365, you must provide the following information about an Office 365 application that is already registered with an Active Directory tenant in Microsoft Azure:

- Application ID
- Tenant ID
- Secret Key

To capture the above information, you must first create or use an existing an Office 365 application that is registered with Azure Active Directory. The application must have access permissions for Office 365 Management APIs and Microsoft Graph APIs. You can then enter the required information about the application when configuring the SOAP/XML credential in SL1. The registered application and the ScienceLogic credential allow SL1 to retrieve information from Office 365.

The following sections describe how to create a registered application, add the appropriate API permissions, and capture the application ID, tenant ID, and secret key.

Creating an Office 365 Active Directory Application in the Azure Portal

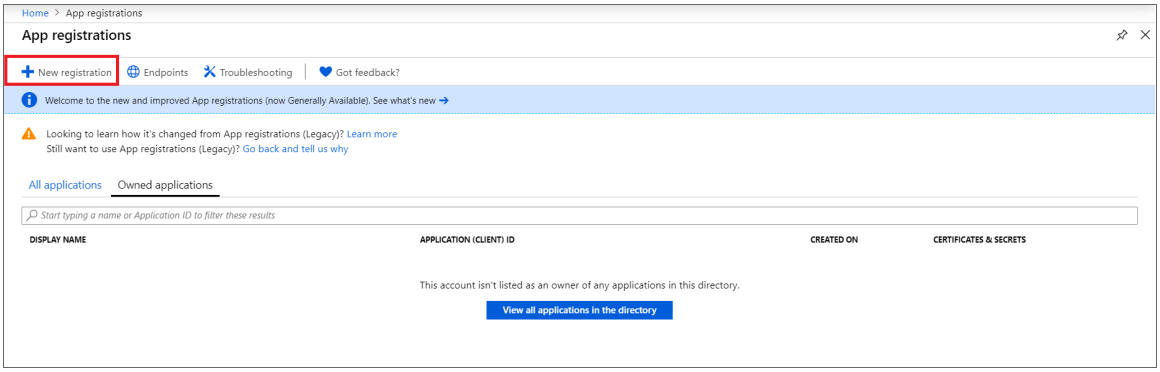
When configuring a SOAP/XML credential in SL1, you must provide the application ID, tenant ID, and secret key of an Office 365 application that is registered with Azure Active Directory. You use this registered application to authenticate your Office 365 account.

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

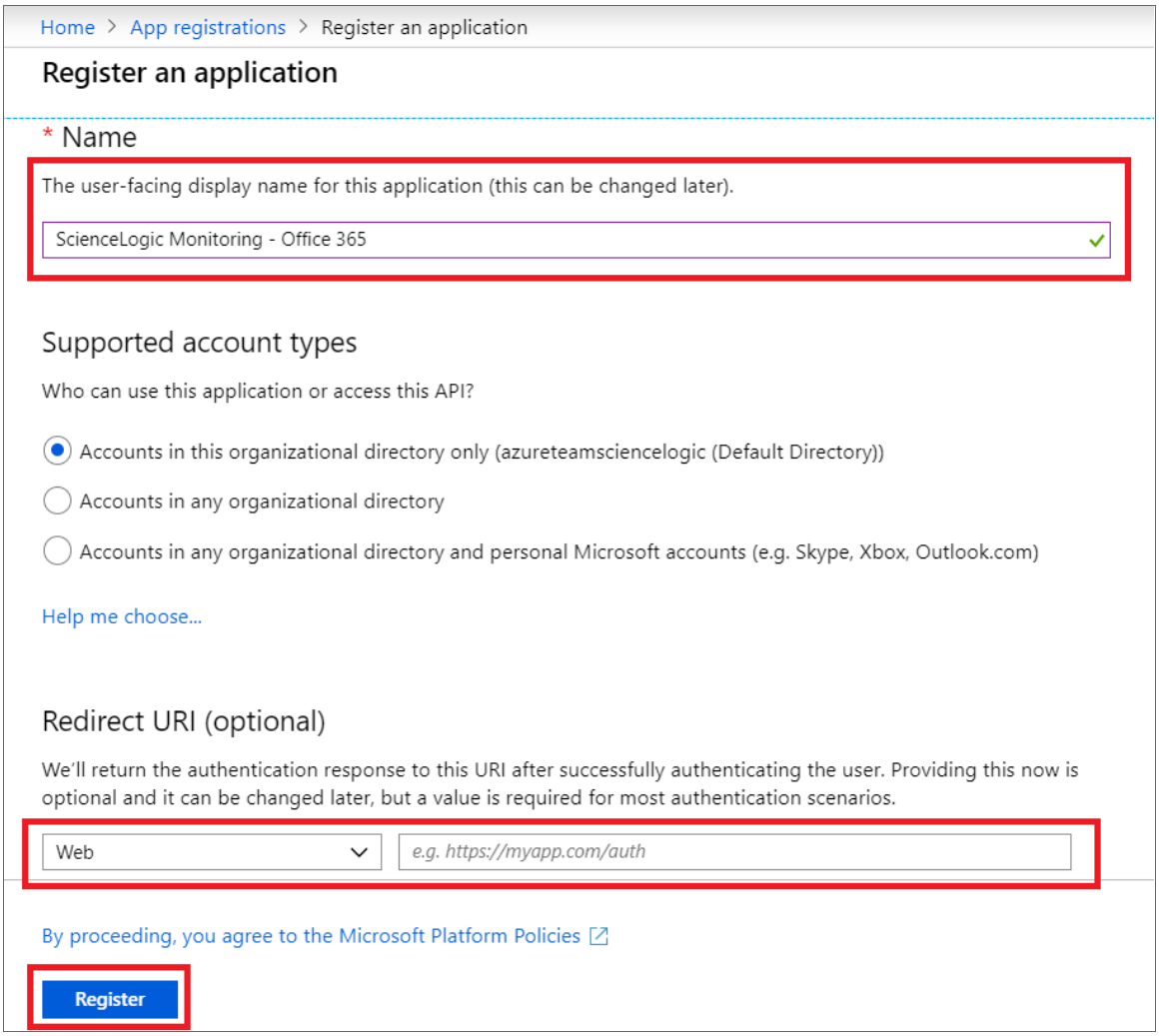
To create an Office 365 application on the Azure portal and register it with Azure Active Directory:

1. Log in to the Azure portal at https://portal.azure.com and type "App registrations" in the **Search** field at the top of the window.
2. From the search results, select *App registrations*. The **App registrations** page appears.

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

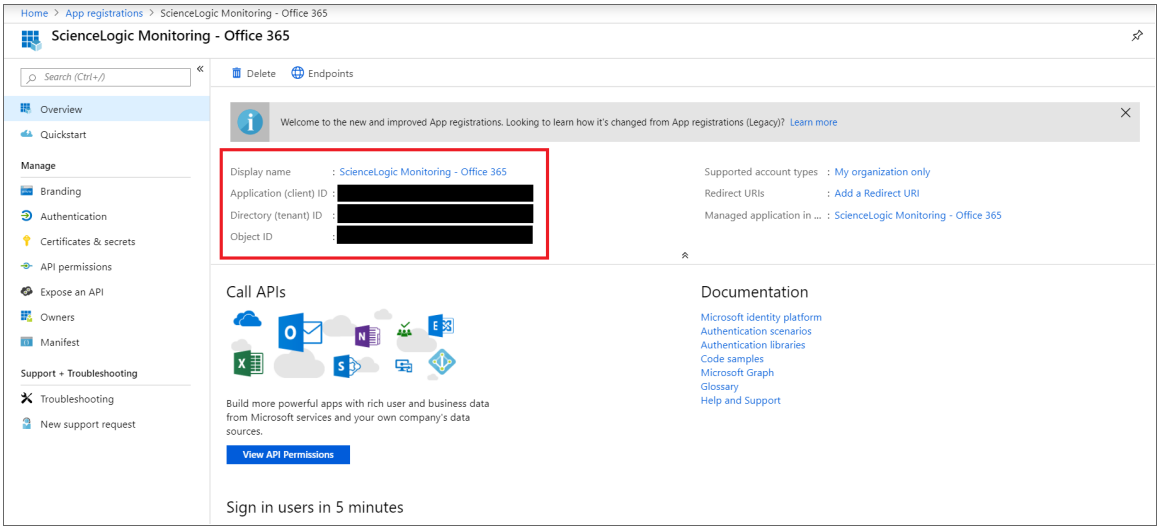


4. When the **Register an application page** appears, enter your application's registration information:
   - ***Name***. Type a name for the application.
   - ***Supported account types***. Select the account types that you want to be supported in your application.
   - ***Redirect URI (optional)***. Select *Web* in the drop-down menu and type a valid URL. For example: https://localhost.com.



5. Click the **[Register]** button. The **Overview** page for your new application appears.

6. On the **Overview** page for your new application, copy and save the values in the *Application (client) ID* and *Directory (tenant) ID* fields. You will need these values when creating your Office 365 credential in SL1.

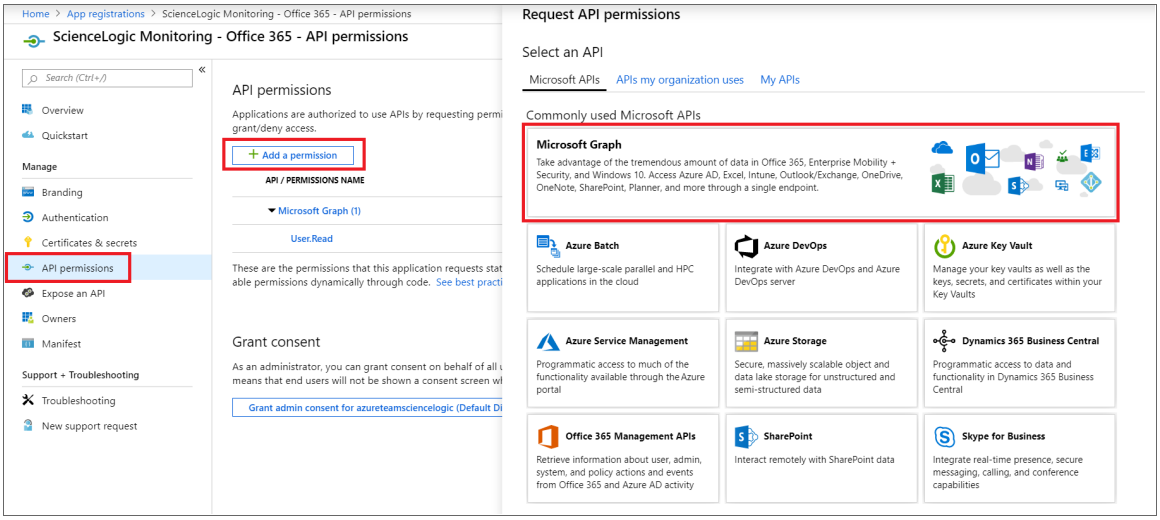


Adding API Permissions to the Application

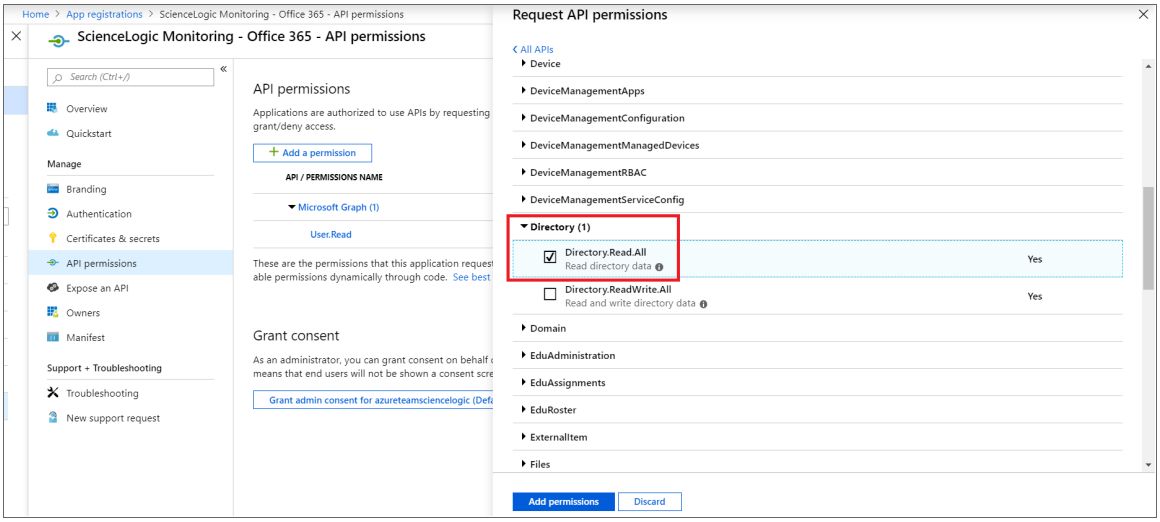
Your Office 365 application must have access permissions for Microsoft Graph APIs and Office 365 Management APIs to be monitored in SL1.

To add API permissions to application:

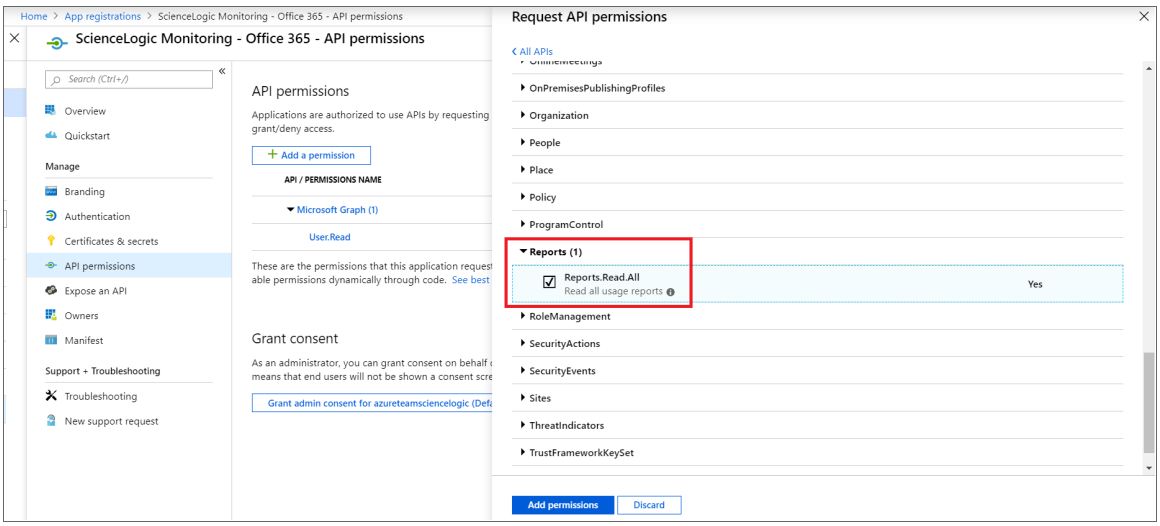
1. From the page for your new application, click **[View API Permissions]**.
2. Click **[Add a permission]**, then click the **Microsoft Graph** option.



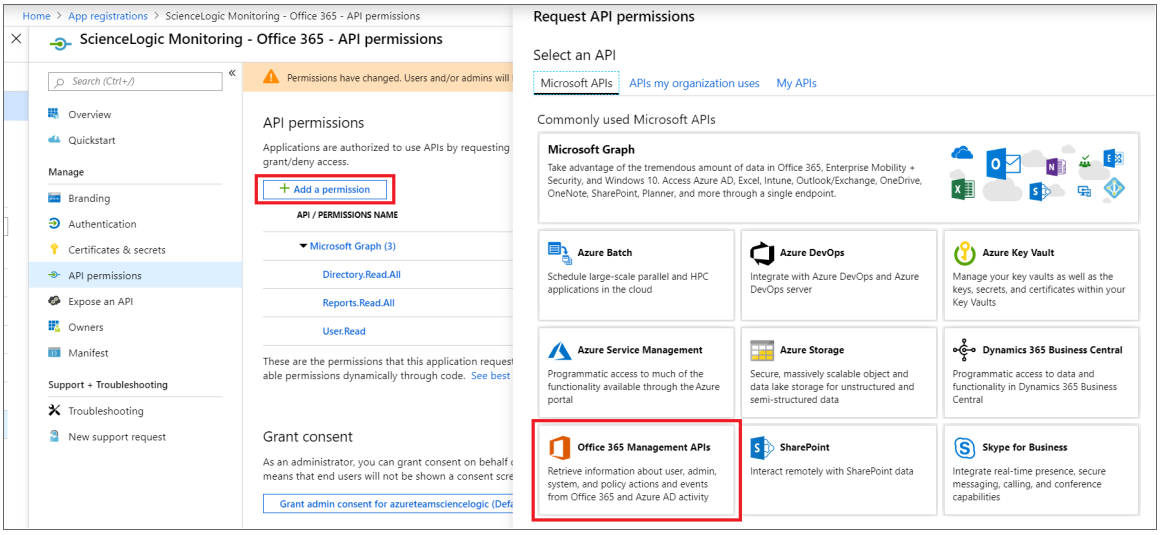
3. In the **Request API permissions** pane, click **Application permissions**.
4. Click the arrow next to **Directory** to open the sub-menu, and then select the checkbox for the *Directory.Read.All* permission.



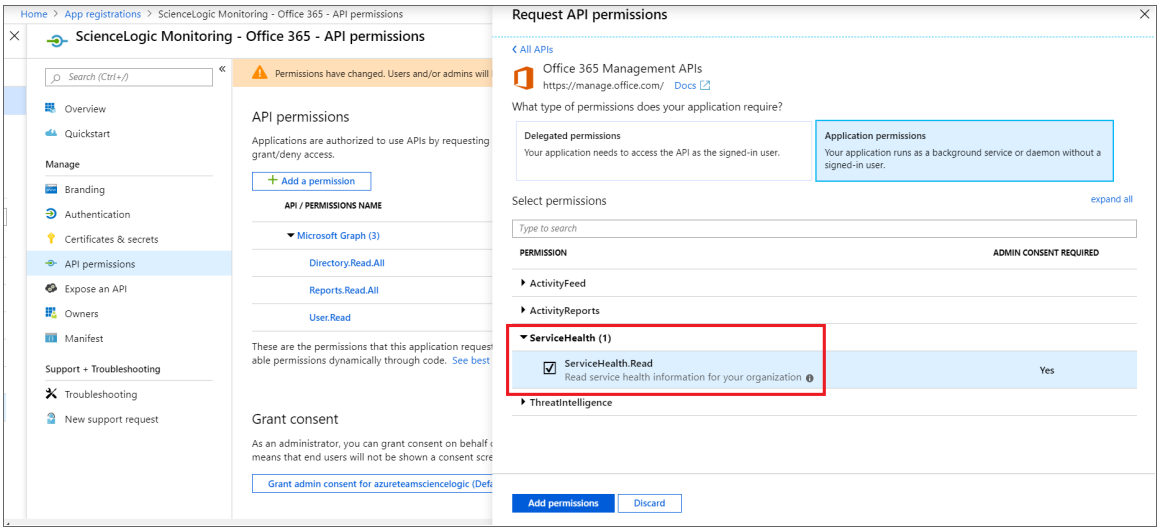
5. Click the arrow next to **Reports** to open the sub-menu, and then select the checkbox for the *Reports.Read.All* permission.



6. Click the **[Add permissions]** button.
7. On the **API permissions** page, click **[Add a permission]**, and then click the *Office 365 Management APIs* option.



8. In the **Request API permissions** pane, click **Application permissions**.
9. Click the arrow next to **ServiceHealth** to open the sub-menu, and then select the checkbox for the *ServiceHealth.Read* permission.



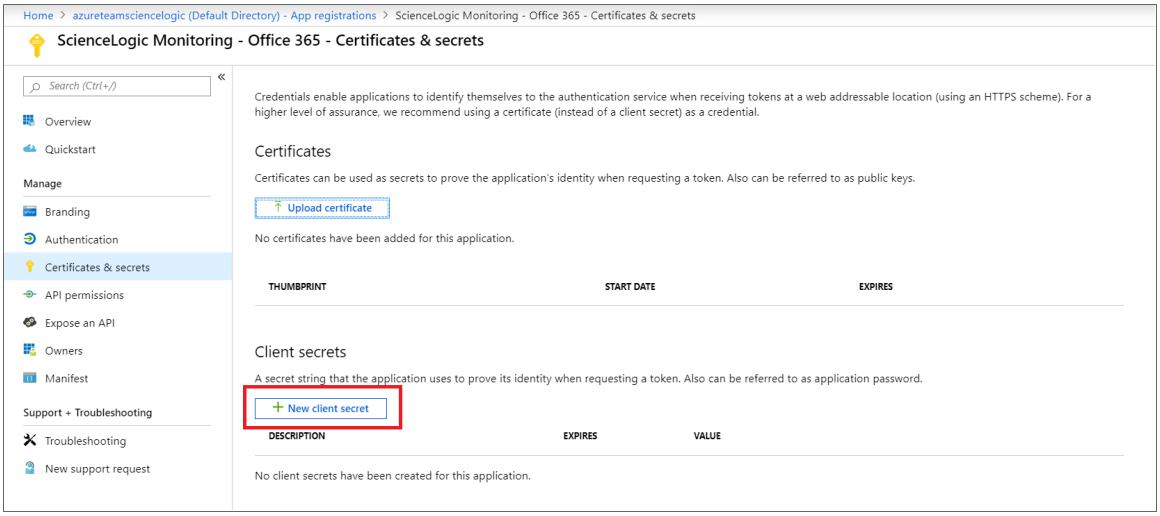
10. Click the **[Add permissions]** button.
11. On the **API permissions** page, click **[Grant admin consent for [Directory Name]]**.
12. A pop-up window appears asking if you grant consent for the required permissions for all accounts in your directory. Click **[Yes]**.

Generating the Secret Key

When configuring a SOAP/XML credential for Office 365 in SL1, you need to provide a secret key for the Office 365 Active Directory application that you will use to authenticate your account.

To generate a secret key:

1. From the Azure portal, type "Active Directory" in the **Search** field at the top of the window.
2. From the search results, select *Azure Active Directory*, and then click **App registrations** on the left pane.
3. Select your Office 365 app from the list.
4. Click **[Certificates & secrets]** on the left pane.
5. In the **Client secrets** pane, click **[+ New client secret]**.



6. In the **Add a client secret** pane, type a name in the ***Description*** field and select a duration in the ***Expires*** field.
7. Click **[Add]** to generate the secret key. A new key value displays in the **Client secrets** pane.
8. Copy and save the key value.

Granting Admin Consent on Enterprise Applications

Your Office 365 Enterprise application must have tenant-wide admin consent to be monitored and pass the credential test by SL1. For more information on granting admin consent, see the Microsoft documentation on granting admin consent in Enterprise apps.

Creating a SOAP/XML Credential for Microsoft Office 365

To configure SL1 to monitor Microsoft Office 365, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *Microsoft: Office 365* PowerPack to communicate with your Office 365 account.

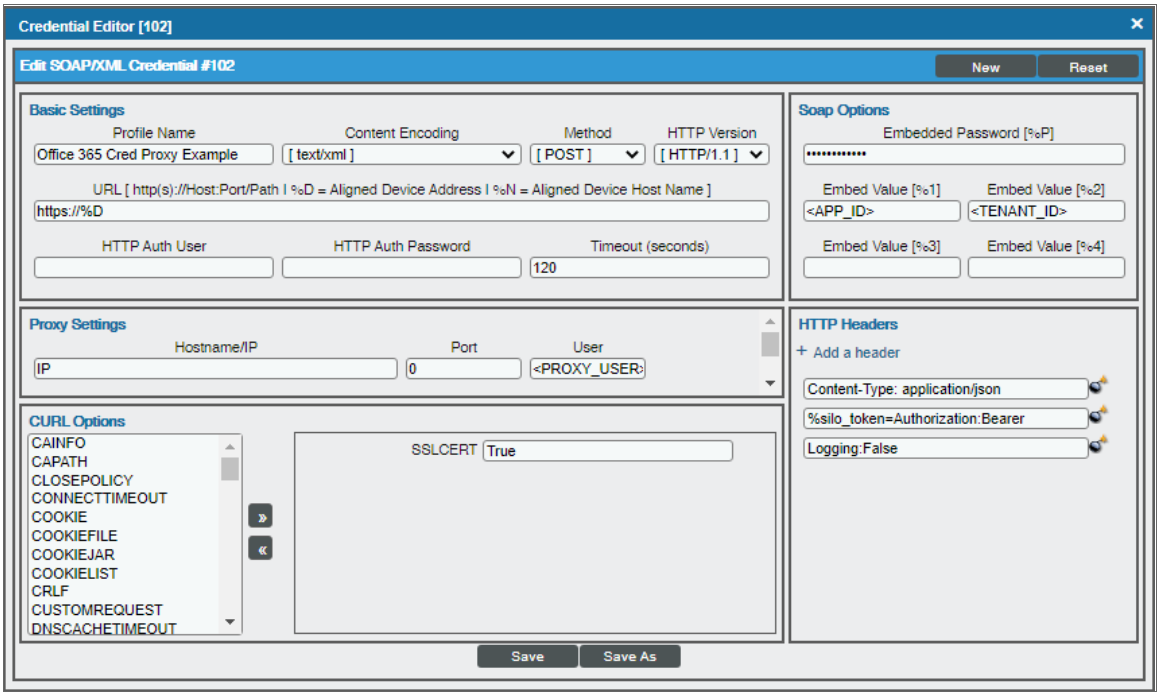
If you want to connect to your Office 365 account through a third-party proxy server, you must also add the proxy information in the credential.

The *Microsoft: Office 365* PowerPack includes two example SOAP/XML credentials that you can use as templates for creating SOAP/XML credentials for Office 365. They are:

- **Office 365 Cred Proxy Example**, for users who connect to Office 365 through a third-party proxy server
- **Office 365 Credential Example**, for all other users

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

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the sample credential you want to use and then click its wrench icon (). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields:



Basic Settings

- ***Profile Name***. Type a new name for the Microsoft Office 365 credential.

- ***URL***. Type "https://%D".
- ***HTTP Auth User***. Leave this field blank.
- ***HTTP Auth Password***. Leave this field blank.

Proxy Settings

- ***Hostname/IP***. If you are connecting to Office 365 via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- ***Port***. If you are connecting to Office 365 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 Office 365 via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- ***Password***. If you are connecting to Office 365 via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

- ***SSL Cert***. The default value of this field is "True". You can also replace this value with your SSL certificate path. If your SSL certificate is expired or if you do not want extra security, set the value of this field to "False".

SOAP Options

- ***Embedded Password [%P]***. Type the secret key for the Office 365 Active Directory application.
- ***Embed Value [%1]***. Type the Application ID for the Office 365 Active Directory application.
- ***Embed Value [%2]***. Type the Tenant ID for the Office 365 Active Directory application.
- ***Embed Value [%3]***. Leave this field blank.
- ***Embed Value [%4]***. Leave this field blank.

HTTP Headers

- ***HTTP Headers***. The following headers are added by default:
  - ***Content-Type: application/son***. Leave the default value that appears in this field.
  - ***%silo_token-Authorization:Bearer***. Leave the default value that appears in this field.
  - ***Logging:False/True***. The default value of this field is "Logging:False". If you would like your credential to gather event information and errors to display in the **/tmp/0365_error.log** log file, set the value of this field to "Logging:True".

4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Testing Your Office 365 Credential

The *Microsoft: Office 365* PowerPack includes a Credential Test for Office 365. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The "Office 365 Credential Test" can be used to test a SOAP/XML credential for monitoring Office 365 using the Dynamic Applications in the *Microsoft: Office 365* PowerPack.

The "Office 365 Credential Test" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Office 365 endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Office 365 endpoint.
- ***Make connection to Office 365 Management API***. Attempts to connect to the Office 365 Management API using the account information specified in the credential.
- ***Make connection to Office 365 Graph API***. Attempts to connect to the Office 365 Graph API using the account information specified in the credential.

To test the Office 365 credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the SOAP/XML credential that you created, click the **Actions** button (···), and then select *Test*.
3. The **Credential Test Form** modal page appears. Fill out the following fields on this page:

    - ***Credential Select***. This field is pre-populated with the credential you selected
    - ***Select Credential Test***. Select the **Office 365 Credential Test**.
    - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
    - ***IP or Hostname to Test***. Type "manage.office.com".

4. Click **[Run Test]** button to run the credential test. The **Testing Credential** window appears.

    The **Testing Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

    - ***Step***. The name of the step.
    - ***Description***. A description of the action performed during the step.
    - ***Log Message***. The result of the step for this execution of the credential test.
    - ***Status***. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
    - ***Step Tip***. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

Testing Your Office 365 Credential in the SL1 Classic User Interface

The *Microsoft: Office 365* PowerPack includes a Credential Test for Office 365. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

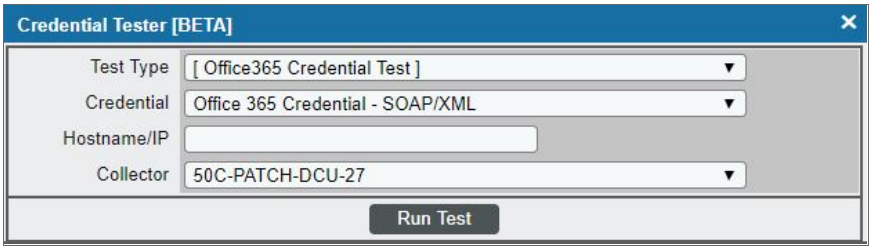
The "Office 365 Credential Test" can be used to test a SOAP/XML credential for monitoring Office 365 using the Dynamic Applications in the *Microsoft: Office 365* PowerPack.

The "Office 365 Credential Test" performs the following steps:

- ***Test Port Availability***. Performs an NMAP request to test the availability of the Office 365 endpoint HTTPS port.
- ***Test Name Resolution***. Performs an nslookup request on the Office 365 endpoint.
- ***Make connection to Office 365 Management API***. Attempts to connect to the Office 365 Management API using the account information specified in the credential.
- ***Make connection to Office 365 Graph API***. Attempts to connect to the Office 365 Graph API using the account information specified in the credential.

To test the Office 365 credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).
2. Locate the **Office 365 Credential Test** and click its lightning bolt icon ( ). The **Credential Tester** modal page appears:



3. Supply values in the following fields:
    - ***Test Type***. This field is pre-populated with the credential test you selected.
    - ***Credential***. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
    - ***Hostname/IP***. Leave this field blank.
    - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
4. Click the **[Run Test]** button. The **Test Credential** window appears, displaying a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:
    - ***Step***. The name of the step.

- ***Description***. A description of the action performed during the step.
- ***Log Message***. The result of the step for this credential test.
- ***Status***. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).
- ***Step Tip***. Mouse over the question mark icon ( ) to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".

Discovering Office 365 Devices

To discover and monitor your Office 365 devices, you must do the following:

- Create a virtual device representing the Office 365 service
- Configure the device template that is included in the *Microsoft: Office 365* PowerPack
- Align the device template to the Office 365 virtual device

Each of these steps is documented in the following sections.

TIP: If you have multiple Office 365 subscriptions you want to monitor, you should create a separate virtual device, credential, and device template for each root device. You can also create different organizations for each Office 365 subscription.

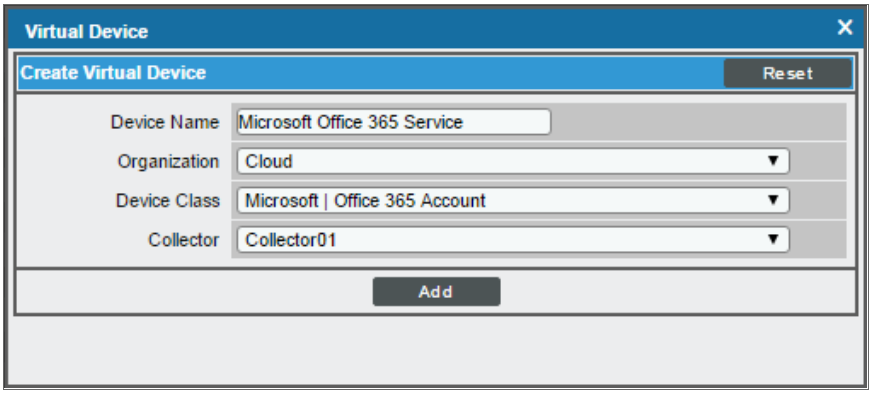
Creating a Microsoft Office 365 Virtual Device

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 SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your Office 365 service:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
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.

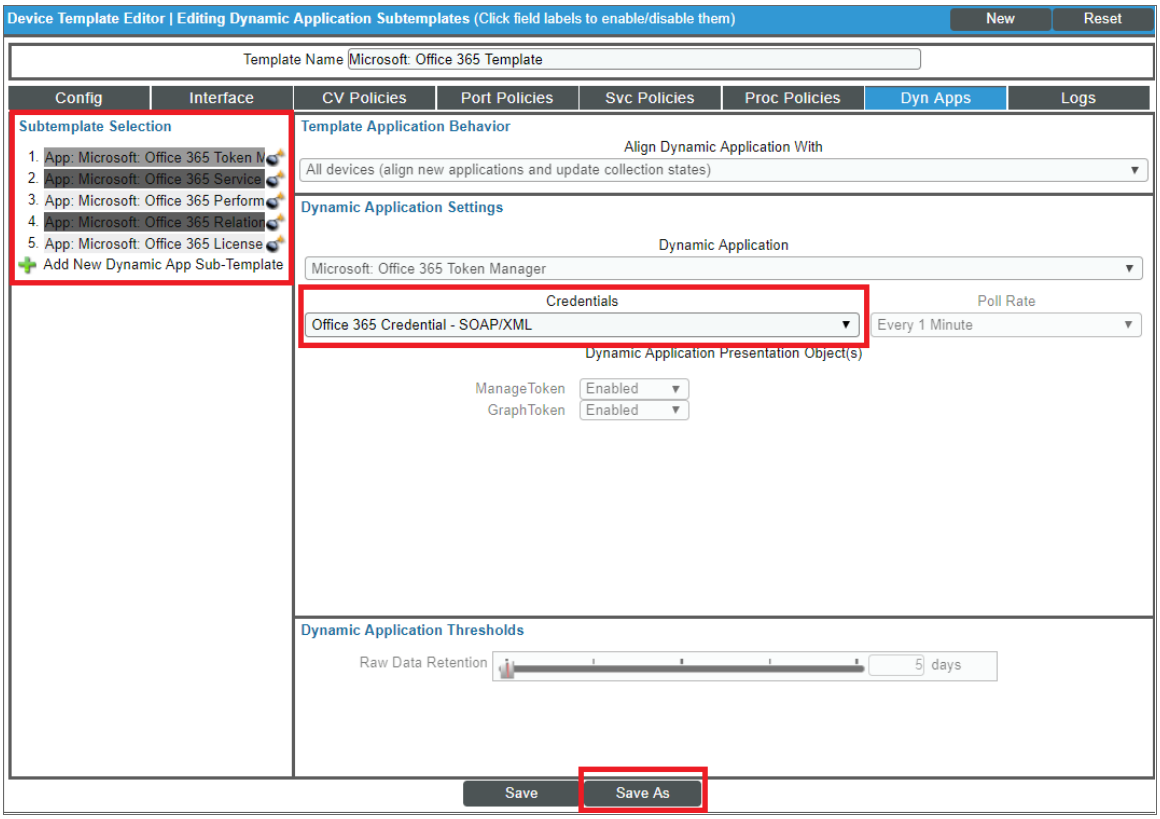
Configuring the Office 365 Device Template

The *Microsoft: Office 365* PowerPack includes the "Microsoft: Office 365 Template", which you can use to create a device template for your own Office 365 account. This device template enables SL1 to align all of the necessary Dynamic Applications to the Office 365 root component device.

Before you can use the "Microsoft: Office 365 Template", you must give the template a new name and configure it so that each Dynamic Application in the template aligns with the credential you created earlier.

To configure the Office 365 device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
2. Locate the "Microsoft: Office 365 Template" and click its wrench icon ( ). The **Device Template Editor** modal page appears.
3. In the ***Template Name*** field, type a new name for the device template.
4. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
5. In the **Subtemplate Selection** pane, click the first Dynamic Application name, then select your Office 365 credential in the *Credentials* field in the Dynamic Application Settings pane.
6. Repeat step 5 for each of the Dynamic Applications listed in the **Subtemplate Selection** pane.



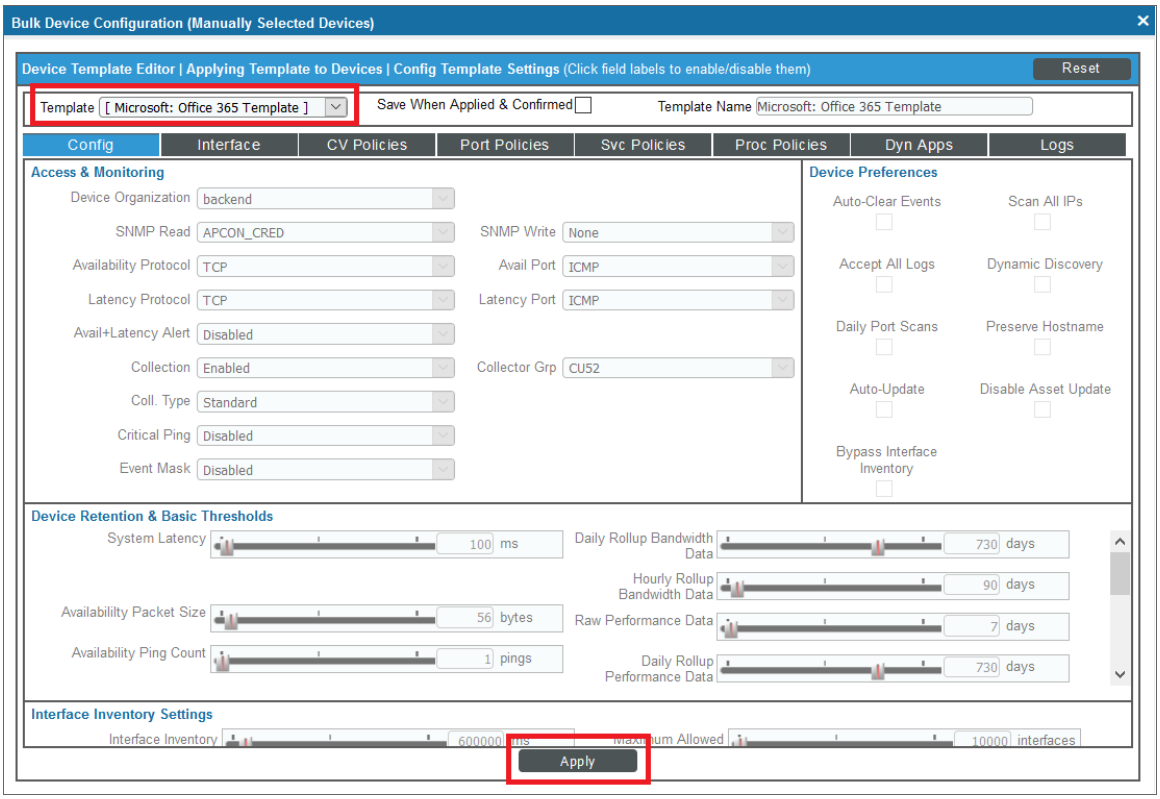
7. When you are finished, click **[Save As]**.

Aligning the Device Template to Your Office 365 Virtual Device

After you have configured the Office 365 device template so that each Dynamic Application in the template aligns with your Office 365 credential, you can use that template to align the Dynamic Applications to the virtual device that you created to act as the root device for your Office 365 environment. When you do so, SL1 discovers and models all of the components in your Office 365 service.

To align the Office 365 device template to the Office 365 virtual device:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager in the SL1 classic user interface).
2. On the **Device Manager** page, select the checkbox for the Office 365 virtual device.
3. In the ***Select Actions*** field, in the lower right corner of the page, select the option *MODIFY by Template* and then click the **[Go]** button. The **Device Template Editor** page appears.
4. In the ***Template*** drop-down list, select your Office 365 device template.
5. Click the **[Apply]** button, and then click **[Confirm]** to align the Dynamic Applications to the root component device.



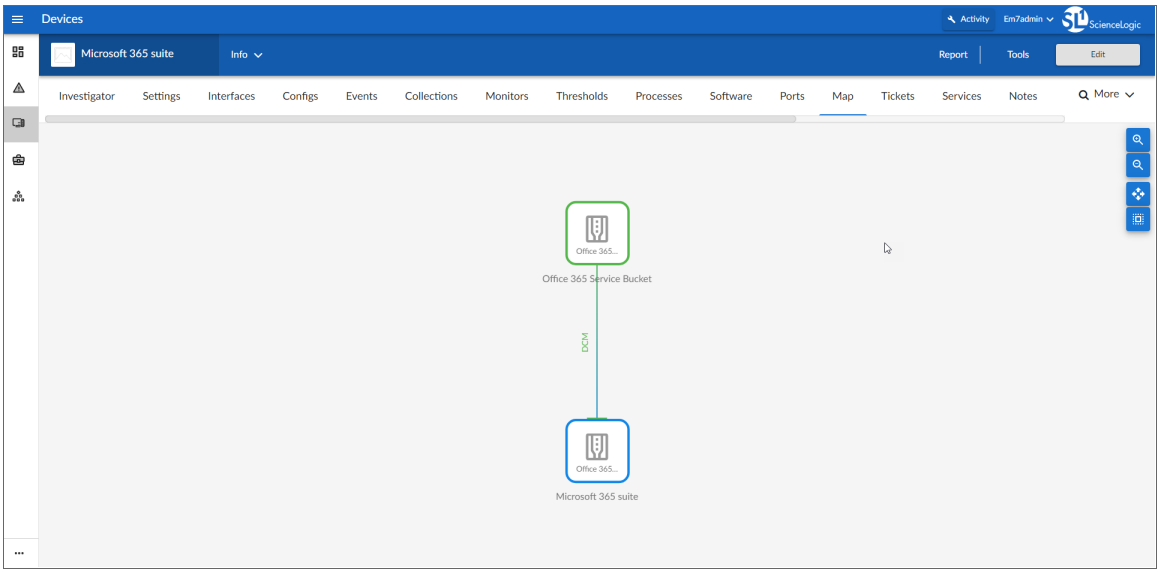
Viewing Microsoft Office 365 Component Devices

When SL1 performs collection for the Microsoft Office 365 virtual device, SL1 will create component devices that represent each application in your Office 365 service.

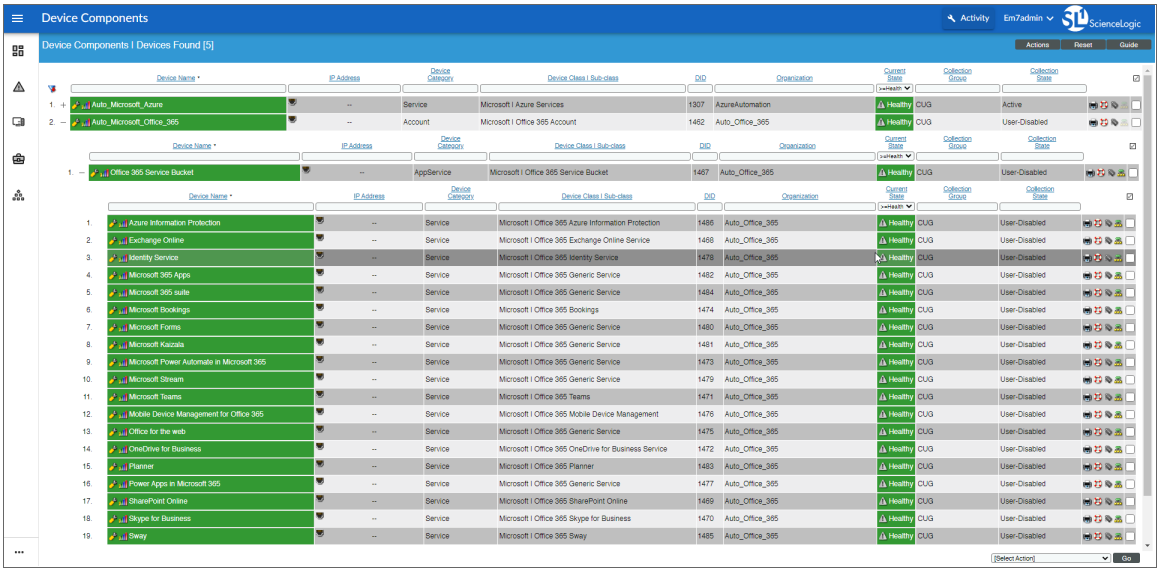
NOTE: Most Office 365 applications, such as Exchange Online and Skype for Business, have their own designated Device Classes and icons in SL1. If a service does not have its own specific Device Class, it will have a Device Class of "Office 365 Generic Service" and an icon for generic Office 365 Service component devices.

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

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** 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 listed devices reloads the page to make the selected device the primary device.



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page displays all root devices and component devices 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 (Classic Maps > 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. SL1 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

Relationships Between Component Devices

In addition to parent/child relationships between component devices, SL1 also creates relationships between Office 365 component devices and other associated devices:

- If you discover Azure devices using the Dynamic Applications in the *Microsoft: Azure* PowerPack version 110 or later, SL1 will automatically create relationships between Office 365 Active Directory tenants and Azure Active Directory tenants.

© 2003 - 2021, 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