

# **Monitoring Microsoft Office 365**

Microsoft: Office 365 PowerPack version 105

# Table of Contents

Introduction	
What is Microsoft Office 365?	
What Does the Microsoft: Office 365 PowerPack Monitor?	
Installing the Microsoft: Office 365 PowerPack	5
Configuration and Discovery	
Configuring Office 365 Monitoring	
Creating an Office 365 Active Directory Application in the Azure Portal	8
Adding API Permissions to the Application	
Generating the Secret Key	13
Granting Admin Consent on Enterprise Applications	
Creating a SOAP/XML Credential for Microsoft Office 365	14
Creating a SOAP/XML Credential for Microsoft Office 365 in the SL1 Classic User Interface	
Testing Your Office 365 Credential	
Testing Your Office 365 Credential in the SL1 Classic User Interface	18
Discovering Office 365 Devices	19
Creating a Microsoft Office 365 Virtual Device	
Configuring the Office 365 Device Template	21
Aligning the Device Template to Your Office 365 Virtual Device	
Viewing Microsoft Office 365 Component Devices	
Relationships Between Component Devices	

# Chapter

# 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:

Import PowerPack™		×
Browse for file	Browse Import	

- 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	13
Granting Admin Consent on Enterprise Applications	13
Creating a SOAP/XML Credential for Microsoft Office 365	14
Creating a SOAP/XML Credential for Microsoft Office 365 in the SL1 Classic User Interface	15
Testing Your Office 365 Credential	17
Testing Your Office 365 Credential in the SL1 Classic User Interface	
Discovering Office 365 Devices	19
Creating a Microsoft Office 365 Virtual Device	
Configuring the Office 365 Device Template	21
Aligning the Device Template to Your Office 365 Virtual Device	22
Viewing Microsoft Office 365 Component Devices	
Relationships Between Component Devices	

# 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 <u>https://portal.azure.com</u> 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.

Home > App registrations				
App registrations				\$ ×
+ New registration ( Endpoints X Troubleshooting ) 🖤 Got feedback?				
Welcome to the new and improved App registrations (now Generally Available). See what	i's new →			
Looking to learn how it's changed from App registrations (Legacy)? Learn more Still want to use App registrations (Legacy)? Go back and tell us why     All applications     Overed applications     Start typing a name or Application ID to filter these results				
DISPLAY NAME	APPLICATION (CLIENT) ID	CREATED ON	CERTIFICATES & SECRETS	
	This account isn't listed as an owner of any applications in this directory. View all applications in the directory			

- 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.

Register an ap	plication
* Name	-
	lay name for this application (this can be changed later).
ScienceLogic Monito	
ScienceLogie Monit	
Supported acc	ount types
	plication or access this API?
0	organizational directory only (azureteamsciencelogic (Default Directory))
<ul> <li>Accounts in any</li> </ul>	organizational directory
<ul> <li>Accounts in any</li> </ul>	organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
Help me choose	
Redirect URI (c	ptional)
	entication response to this URI after successfully authenticating the user. Providing this now is e changed later, but a value is required for most authentication scenarios.
Web	✓ e.g. https://myapp.com/auth
optional and it can b	be changed later, but a value is required for most authentication scenarios.

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.

Home > App registrations > ScienceLog	ic Monitoring - Office 365		
ScienceLogic Monitoring	- Office 365		\$
Search (Ctrl+,/) ≪	🛅 Delete 🔀 Endpoints		
🗮 Overview	Welcome to the new and improved App registrations. Looking to learn ho	wit's changed from App registrations (Legacy)? Learn more	×
📣 Quickstart			
Manage	Display name : ScienceLogic Monitoring - Office 365	Supported account types : My organization only	
sranding	Application (client) ID :	Redirect URIs : Add a Redirect URI	
Authentication	Directory (tenant) ID :	Managed application in : ScienceLogic Monitoring - Office 365	
💡 Certificates & secrets	Object ID :	*	
API permissions		*	
Expose an API	Call APIs	Documentation	
Owners		Microsoft identity platform	
🔟 Manifest		Authentication scenarios Authentication libraries	
Support + Troubleshooting	💵 💿 s 🛌 🚸	Code samples Microsoft Graph	
X Troubleshooting		Glossary Help and Support	
New support request	Build more powerful apps with rich user and business data from Microsoft services and your own company's data	methodie polybox	
New support request	sources.		
	View API Permissions		
	Sign in users in 5 minutes		

# 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.

Home > App registrations > ScienceLo	gic Monitoring - Office 365 - API permissions	Request API permissions		
ScienceLogic Monitoring     Science(Crit+/)     Search (Crit+/)     Goverview     Quickstart     Manage     Branding     Authentication	g - Office 365 - API permissions           API permissions           Applications are authorized to use APIs by requesting permisgrant/deny access.           + Add a permission           API / PERMISSIONS NAME           • Microsoft Graph (1)	Select an API Microsoft APIs APIs my organization Commonly used Microsoft APIs Microsoft Graph Take advantage of the tremendous amount	: of data in Office 365, Enterprise Mobility + ), Excel, Intune, Outlock/Exchange, OneDrive,	<ul> <li>▲</li> <li>●</li> <li>●</li></ul>
	UserRead These are the permissions that this application requests stat able permissions dynamically through code. See best practi	Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Key Vault Manage your key vaults as well as the keys. secrets, and certificates within your Key Vaults
Coviners     Manifest     Support + Troubleshooting     X Troubleshooting	Grant consent As an administrator, you can grant consent on behalf of all s means that end users will not be shown a consent screen w Grant admin consent for azureteamsciencelogic (Default D	Azure Service Management Programmatic access to much of the functionality available through the Azure portal	Secure, massively scalable object and data lake storage for unstructured and semi-structured data	Content of the second s
New support request		Office 365 Management APIs Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity	S SharePoint Interact remotely with SharePoint data	Skype for Business Integrate real-time presence, secure messaging, calling, and conference capabilities

- 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.

н	ome > App registrations > ScienceLogic Mo	nitoring - Office 365 - API permissions	Request API permissions	×
×	ScienceLogic Monitoring	- Office 365 - API permissions	CAILAPIs	
	Search (Ctrl+/) ≪	API permissions	Device     DeviceManagementApps	- 1
	🐺 Overview	Applications are authorized to use APIs by requesting grant/deny access.	DeviceManagementConfiguration	
	📣 Quickstart	+ Add a permission	DeviceManagementManagedDevices	
	Manage	API / PERMISSIONS NAME	DeviceManagementRBAC	
-	<ul> <li>Branding</li> <li>Authentication</li> </ul>	✓ Microsoft Graph (1)	DeviceManagementServiceConfig	. 1
1	Y Certificates & secrets	User.Read	▼ Directory (1)	- I
-	→ API permissions	These are the permissions that this application request able permissions dynamically through code. See best	Directory.Read.All Yes	
-	Expose an API	tore permissions dynamically through code. See best	Directory.ReadWrite.All Read and write directory data 👔	- 1
	Owners Manifest	Grant consent	▶ Domain	
-	Support + Troubleshooting	As an administrator, you can grant consent on behalf or means that end users will not be shown a consent scre	▶ EduAdministration	
	X Troubleshooting	Grant admin consent for azureteamsciencelogic (Defa	▶ EduAssignments	
-	New support request		► EduRoster	
			Externalitem	-
				Ŷ
			Add permissions Discard	

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

Home > App registrations > Sciencelog	gic Monitoring - Office 365 oring - Office 365   API permissions 🛷 …	Request API permissions	×
<b>-</b>		K All APIs	
	🕐 Refresh 🔰 🕂 Got feedback?	> Security/incident	<b>^</b>
Overview	A You are editing permission(s) to your application, users will have to consent even if	/ SecurityIncuent	
🝊 Quickstart		✓ ServiceHealth (1)	
💉 Integration assistant		ServiceHealth.Read.All ① Yes	
Manage	The "Admin consent required" column shows the default value for an organization.	Read service health	
Branding & properties	where this app will be used. Learn more	> ServiceMessage	
<ul> <li>Authentication</li> </ul>	Configured permissions		
Certificates & secrets	Applications are authorized to call APIs when they are granted permissions by users,	ServicePrincipalEndpoint	
Token configuration	all the permissions the application needs. Learn more about permissions and conser	> ShortNotes	
<ul> <li>API permissions</li> </ul>	+ Add a permission 🗸 Grant admin consent for uajms		
<ul> <li>Expose an API</li> </ul>	API / Permissions name Type Description	> Sites	
K App roles	✓ Microsoft Graph (2)	> TeamMember	
A Owners	Directory.Read.All Application Read directory data		
8 Roles and administrators   Preview	User.Read Delegated Sign in and read user profile	> TeamsActivity	
Manifest		> TeamsAppInstallation	
Support + Troubleshooting	To view and manage permissions and user consent, try Enterprise applications.		- 1
Troubleshooting		> TeamsApp	
New support request		> TeamSettings	
New support request		/ reannancenings	
		> TeamsTab	-
		Add permissions Discard	
4		Add permissions Discard	

- 6. On the API permissions page, click [Grant admin consent for [Directory Name]].
- 7. 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].

Home > azureteamsciencelogic (Default	Directory) - App registrations > ScienceLogic Monitoring - Office 365 - Certificates & secrets
💡 ScienceLogic Monitoring	- Office 365 - Certificates & secrets
Search (Ctrl+/)	Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
<ul> <li>Overview</li> <li>Quickstart</li> </ul>	Certificates
Manage	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.
🧰 Branding	T Upload certificate
Authentication	No certificates have been added for this application.
💡 Certificates & secrets	
<ul> <li>API permissions</li> </ul>	THUMBPRINT START DATE EXPIRES
Expose an API	
Owners	Client secrets
Manifest	A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
Support + Troubleshooting	+ New client secret
★ Troubleshooting	DESCRIPTION EXPIRES VALUE
New support request	No client secrets have been created for this application.

- 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 <u>the Microsoft documentation on</u> 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 **Credentials** page (Manage > Credentials).
- 2. Locate the sample credential you want to use, click its **[Actions]** icon (--) and select **Duplicate**. A copy of the credential, called appears.
- 3. Click the **[Actions]** icon (--) for the copied credential and select **Edit**. The **Edit Credential** modal page appears.
- 4. Enter values in the following fields:

redential					
Name* Office 365 Credential Exam	nple copy			Credential Te	iter
II Organizations	Select the organizations the credential	pelongs to * 👻	Timeout (ms) 120000	Select Credential Test	
Content Encoding text/xml	Method ~ POST	HTTP Versia ~ http:/1.1	20	Select Collector	
uRL* https://%D				IP or Hostname to test*	
HTTP Auth User		HTTP Auth Password			
Proxy Hostname/IP		Proxy Port O			
Proxy User		Proxy Password			
optional Embedded Password [%P]					
Embed Value [%1] <app_id></app_id>		Embed Value [%2] <tenant_id></tenant_id>			
					Save & Close

- Name. Type a new name for the Microsoft Office 365 credential.
- All Organizations. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the What organization manages this service? drop-down field to align the credential with those specific organizations.

- URL. Type "https://%D".
- HTTP Auth User. Leave this field blank.
- HTTP Auth Password. Leave this field blank.
- **Proxy 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.
- **Proxy 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.
- **Proxy 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.
- **Proxy 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.
- 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. The following headers are added by default:
  - Content-Type: application/json. 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".
- **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".
- 4. For all other fields, use the default values.
- 5. Click the [Save & Close] button.

NOTE: If you would like to test your credential using the Credential Tester panel, click [Save & Test]. For detailed instructions on using the Credential Tester panel, see the Testing Your Office 365 Credential section.

# Creating a SOAP/XML Credential for Microsoft Office 365 in the SL1 Classic User Interface

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 (*P*). The **Edit SOAP/XML Credential** modal page appears.
- 3. Enter values in the following fields:

Credential Editor [102]	×
Edit SOAP/XML Credential #102	New Reset
Basic Settings         Profile Name       Content Encoding       Method       HTTP Version         Office 365 Cred Proxy Example       [ text/xml ]       V       [ POST ]       V       [ HTTP/1.1 ]         URL [ https://Host:Port/Path 1 %D = Aligned Device Address 1 %N = Aligned Device Host Name ]       [ https://%D	Soap Options           Embedded Password [%oP]           ••••••••••••••••••••••••••••••••••••
Proxy Settings         A           Hostname/IP         Port         User           IP         0 <proxy_user< td=""></proxy_user<>	HTTP Headers + Add a header Content-Type: application/json
CURL Options CAINFO CAPATH CLOSEPOLICY CONNECTTIMEOUT COOKIEFILE COOKIELIST CRLF CRLF CUSTOMREQUEST DNSCACHETIMEOUT	%silo_token=Authorization:Bearer       Cogging:False
Save Save As	

#### **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/json. 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 365PowerPack 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 365PowerPack.

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 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 "graph.microsoft.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 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 (*F*). The **Credential Tester** modal page appears:

Credential Tester [	BETA]	×
Test Type	[ Office365 Credential Test ]	T
Credential	Office 365 Credential - SOAP/XML	•
Hostname/IP		
Collector	50C-PATCH-DCU-27	•
	Run Test	

- 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 (C) 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:

Virtual Device		×								
Create Virtual Device		Reset								
Device Name	Microsoft Office 365 Service									
Organization	Cloud	T								
Device Class	Microsoft   Office 365 Account	•								
Collector	Collector01	•								
	Add									

- **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 (*P*). 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.

Device Template Editor   Editing Dynamic	Application Subtemp	lates (Click field label	s to enable/disable then	n)		New	Reset
Templa	te Name Microsoft: Off	ice 365 Template					
Config Interface	CV Policies	Port Policies	Svc Policies	Proc Policies	Dyn Apps		Logs
Subtemplate Selection 1. App: Microsoft: Office 365 Token Not 2. App: Microsoft Office 365 Service of 3. App: Microsoft: Office 365 Perform of 4. App: Microsoft: Office 365 Relation of	Template Application	w applications and up	Align Dynamic A date collection states)	Application With			¥
5. App: Microsoft: Office 365 License and Add New Dynamic App Sub-Template	Microsoft: Office 36	5 Token Manager	Dynamic A	Application			•
		Crec	lentials		P	oll Rate	
	Office 365 Credenti	al - SOAP/XML		•	Every 1 Minute		•
	Durantia Applicatio	Manage Token Graph Token	Enabled V Enabled V	Presentation Object(s)			
	Dynamic Applicatio Raw Data R		save As	· · ·	5 days		

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.

Template [ Microsoft: Off	îce 365 Template ] 🛛 🖂	Save When Ap	plied & Confirme	d Template N	lame Microso	ft: Office 365 Template	
Config	Interface CV I	Policies F	ort Policies	Svc Policies	Proc Polic	ies Dyn Apps	Logs
ccess & Monitoring						Device Preferences	
Device Organization	backend	$\sim$				Auto-Clear Events	Scan All IPs
SNMP Read	APCON_CRED	$\sim$	SNMP Write	None	$\sim$		
Availability Protocol	ТСР	$\sim$	Avail Port	ICMP	$\sim$	Accept All Logs	Dynamic Discovery
Latency Protocol	ТСР	$\sim$	Latency Port	ICMP	$\sim$		
Avail+Latency Alert	Disabled	$\sim$				Daily Port Scans	Preserve Hostname
Collection	Enabled	$\sim$	Collector Grp	CU52			
Coll. Type		$\sim$				Auto-Update	Disable Asset Update
Critical Ping		24					
_						Bypass Interface	
Event Mask	Disabled	$\sim$				Inventory	
evice Retention & Basic							
System Latence	<sup>y</sup>	1	100 ms	Daily Rollup Bandwidth Data	1	<u> </u>	730 days
				Hourly Rollup Bandwidth Data	- JU	I I	90 days
Availabililty Packet Siz	2e <b>4</b>	I	56 bytes	Raw Performance Data		1	7 days
Availability Ping Cou	nt		1 pings				7 days
, ,	1		1 pings	Daily Rollup Performance Data	1		730 days

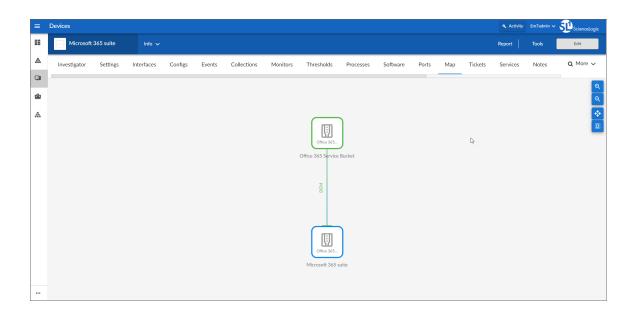
# Viewing Microsoft Office 365 Component Devices

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:

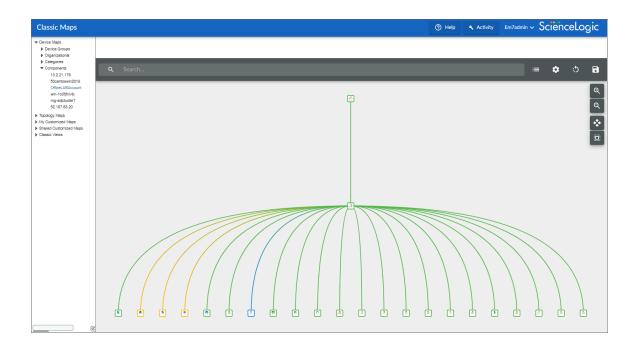
• The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.



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 (+).

•	Device Com	ponents								🔦 Activity	Em7admin 🗸	
8	Device Compo										Actions	Reset Guide
Δ		Device Name *		IP Address	Device Category	Device Class I Sub-class		Orpanization	Current State	Collection Group	Collection State	Ø
_	1. + 🖉 🚮 Aut	_Microsoft_Azure			Service	Microsoft I Azure Services	1307	AzureAutomation	A Healthy CUG		Active	<b>H 10</b> % (5)
30	2 🤌 🚮 Aut	_Microsoft_Office_365	۲		Account	Microsoft I Office 365 Account	1462	Auto_Office_365	A Healthy CU3		User-Disabled	<b>⊜</b> ₿%
5		Device Name *		IP Address	Device Category	Device Class I Sub-class	212	Organization		Collection Group	Collection State	E
9	1. – 🎤	Office 365 Service Bucket	Ĩ	·	AppService	Microsoft I Office 365 Service Bucket	1467	Auto_Office_365	A Healthy CUG		User-Disabled	10 <b>10</b> 10 <u>10</u>
0 0 0 0		Device Name •		IP Address	Device Celevory	Device Class I Sub-class		2 <u>Organization</u>	Current State	Collection Group	Collection State	
	1.	Azure Information Protection			Service	Microsoft I Office 365 Azure Information Protection	1486	Auto_Office_365	A Healthy CUG		User-Disabled	m 23 % 85
	2.	Exchange Online		۰. ۳	Service	Microsoft I Office 365 Exchange Online Service	1468	Auto_Office_365	A Healthy CUG		User-Disabled	
	З.	🚰 🚮 Identity Service			Service	Microsoft I Office 365 Identity Service	1478	Auto_Office_365	Healthy CUG		User-Disabled	10 <b>2</b> N 20
	4.	مَنْ Microsoft 365 Apps		· · ·	Service	Microsoft I Office 365 Generic Service	1482	Auto_Office_365	A Healthy CUG		User-Disabled	<b>₩</b> ₽8&
	6.	Microsoft 365 suite 👔 👉		۰. ۳	Service	Microsoft I Office 365 Generic Service	1484	Auto_Office_365	A Healthy CUG		User-Disabled	10 <b>10</b> 10 <b>10</b> 10
	6.	🖋 📶 Microsoft Bookings		۰. 🛡	Service	Microsoft I Office 365 Bookings	1474	Auto_Office_365	A Healthy CUG		User-Disabled	<b>11 12 10 15</b>
	7.	Microsoft Forms 🖌 🖌		×	Service	Microsoft I Office 365 Generic Service	1480	Auto_Office_365	A Healthy GUG		User-Disabled	📾 🍀 🗞 🙈
	8.	🥜 🚛 Microsoft Kaizala		·	Service	Microsoft I Office 365 Generic Service	1481	Auto_Office_365	A Healthy CUG		User-Disabled	🖶 🏷 🗞 😹 (
	9.	Microsoft Power Automate in Microsoft 365		·	Service	Microsoft I Office 365 Generic Service	1473	Auto_Office_365	A Healthy CUG		User-Disabled	🖶 🖉 🖏 📾
	10.	Microsoft Stream 🔥 👔		· ·	Service	Microsoft I Office 365 Generic Service	1479	Auto_Office_365	A Healthy CUG		User-Disabled	10 to 20 10 10 10 10 10 10 10 10 10 10 10 10 10
	11.	🖋 🔐 Microsoft Teams			Service	Microsoft I Office 365 Teams	1471	Auto_Office_365	A Healthy CUG		User-Disabled	10 <b>20</b> 10 <u>26</u>
	12.	nt Mobile Device Management for Office 365		· ·	Service	Microsoft I Office 365 Mobile Device Management	1476	Auto_Office_365	A Healthy CUG		User-Disabled	📾 👯 🗞 🙈
	13.	HOffice for the web		·	Service	Microsoft I Office 365 Generic Service	1475	Auto_Office_365	A Healthy CUG		User-Disabled	10 X N 25
	14.	🤌 📶 OneDrive for Business		· ·	Service	Microsoft I Office 365 OneDrive for Business Service	1472	Auto_Office_365	A Healthy CUG		User-Disabled	📾 👯 🗞 👼
	15.	🧨 🚮 Planner		· · ·	Service	Microsoft I Office 365 Planner	1483	Auto_Office_365	A Healthy CUG		User-Disabled	10 <b>1</b> 0 <b>1</b>
	16.	🤌 📶 Power Apps in Microsoft 365			Service	Microsoft I Office 365 Generic Service	1477	Auto_Office_365	A Healthy CUG		User-Disabled	🖶 🖏 🖏 🐻
	17.	ان 👉 🖌 SharePoint Online		- *	Service	Microsoft I Office 365 SharePoint Online	1469	Auto_Office_365	A Healthy CUG		User-Disabled	📾 🍀 🗞 🙈
	18.	skype for Business 🕹 🕹 🕹		· · ·	Service	Microsoft I Office 365 Skype for Business	1470	Auto_Office_365	A Healthy CUG		User-Disabled	10 N N N N N N N N N N N N N N N N N N N
	19.	🥜 📶 Sway			Service	Microsoft I Office 365 Sway	1485	Auto_Office_365	A Healthy CUG		User-Disabled	📾 😆 🗞 🙈

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 - 2022, 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<sup>™</sup> 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<sup>™</sup> has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic<sup>™</sup> assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic<sup>™</sup> 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 <sup>™</sup> 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<sup>™</sup>
- EM7<sup>™</sup> and em7<sup>™</sup>
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management<sup>™</sup>

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