

Monitoring Microsoft Azure

Microsoft: Azure PowerPack version 105

Table of Contents

Introduction	3
What is Azure?	4
What Does the Microsoft: Azure PowerPack Monitor?	. 4
What are Azure Locations?	. 5
Installing the Microsoft: Azure PowerPack	6
Configuring Azure for Monitoring	. 8
Configuring an Azure Active Directory Application	. 9
Creating an Active Directory Application in the Azure Portal	9
Adding the Microsoft Graph and Windows Azure Active Directory APIs	11
Generating the Secret Key	14
Locating the Application ID	15
Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID	15
Locating the Subscription ID	16
Adding Reader or Contributor Access to the Active Directory Application	17
Setting Up a Proxy Server	
Creating a SOAP/XML Credential for Azure	20
Load-Balancing an Account with Multiple Subscriptions	22
Testing the Azure Credential	23
Discovering Azure Resources	25
Creating an Azure Virtual Device	25
Aligning the Azure Dynamic Applications	26
Discovering Azure Component Devices	27
Viewing Azure Component Devices	29
Relationships Between Component Devices	31

Chapter

1

Introduction

Overview

This manual describes how to monitor Microsoft Azure resources that are managed with Azure Resource Manager (ARM) in the ScienceLogic platform using the *Microsoft: Azure* PowerPack.

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

The following sections provide an overview of Microsoft Azure and the Microsoft: Azure PowerPack:

What is Azure?	4
What Does the Microsoft: Azure PowerPack Monitor?	4
What are Azure Locations?	5
Installing the Microsoft: Azure PowerPack	6

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What is Azure?

Azure is a Microsoft service that provides both infrastructure and platform capabilities for cloud computing. Azure enables users to build, deploy, and manage applications and services using Microsoft data centers, and offers users numerous capabilities such as website hosting, virtual machine creation, data management, business analytics, and media services.

Microsoft offers two methods for managing Azure resources: Azure Resource Manager (ARM) portal and the Azure Classic portal.

What Does the Microsoft: Azure PowerPack Monitor?

To monitor Microsoft ARM resources using the ScienceLogic platform, you must install the *Microsoft: Azure* PowerPack. This PowerPack enables you to discover, model, and collect data about ARM resources.

The Microsoft: Azure PowerPack includes:

- Example credentials you can use as templates to create SOAP/XML credentials to connect to ARM
- Dynamic Applications to discover, model, and monitor performance metrics and/or collect configuration data for the following ARM resources:
 - Active Directory tenants
 - Application gateways
 - Load balancers
 - Network security groups
 - Recovery Services vaults
 - Resource groups
 - SQL databases
 - SQL servers
 - Storage accounts
 - Traffic Manager profiles
 - Virtual machines
 - Virtual network subnets
 - Virtual networks
 - VPN gateways
- Device Classes for each Azure data center location and all of the ARM resources the ScienceLogic platform
 monitors
- Event Policies and corresponding alerts that are triggered when ARM resources meet certain status criteria

What are Azure Locations?

An Azure location is an individual data center located in a specific geographic locale. The Dynamic Applications in the *Microsoft: Azure* PowerPack create a "location" component device for each discovered data center location.

The PowerPack supports the following Azure data center locations:

- Australia East (New South Wales)
- Australia Southeast (Victoria)
- Brazil South (Sao Paulo)
- Canada Central (Toronto)
- Canada East (Quebec)
- Central India (Pune)
- Central US (lowa)
- East Asia (Hong Kong)
- East US (Virginia)
- East US 2 (Virginia)
- Germany Central (Frankfurt)
- Germany Northeast (Magdeburg)
- Japan East (Saitama)
- Japan West (Osaka)
- Korea Central (Seoul)
- Korea South (Busan)
- North Central US (Illinois)
- North Europe (Ireland)
- South Central US (Texas)
- South India (Chennai)
- Southeast Asia (Singapore)
- US DoD Central (for Microsoft Azure Government only)
- US DoD East (for Microsoft Azure Government only)
- US Gov Arizona (for Microsoft Azure Government only)
- US Gov Iowa (for Microsoft Azure Government only)
- US Gov Texas (for Microsoft Azure Government only)
- US Gov Virginia (for Microsoft Azure Government only)
- UK South (London)
- UK West (Cardiff)

- West Central US
- West Europe (Netherlands)
- West India (Mumbai)
- West US (California)
- West US 2

Installing the Microsoft: Azure PowerPack

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

NOTE: If you are already using the ScienceLogic platform to monitor Azure Classic and/or ARM resources, you must upgrade to the latest version of the *Microsoft: Azure Classic* PowerPack before using the *Microsoft: Azure* PowerPack to monitor ARM resources.

NOTE: The following instructions describe how to install the *Microsoft*: Azure PowerPack for the first time. If you are upgrading to the latest version from a previous version, see the *Microsoft*: Azure PowerPack Release Notes for specific upgrade instructions.

To download and install a PowerPack:

TIP: By default, installing a new version of a PowerPack overwrites all content in that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the *System Administration* manual.)

- 1. Download the PowerPack from the ScienceLogic Customer Portal.
- 2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
- 4. The **Import PowerPack** dialog box appears:

Import PowerPack™		×
Browse for file	Browse]

- 5. Click the [Browse] button and navigate to the PowerPack file.
- 6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter

Z

Configuring Azure for Monitoring

Overview

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

NOTE: The Microsoft: Azure PowerPack can monitor Microsoft Azure resources and Microsoft Azure Government resources.

Configuring an Azure Active Directory Application	
Creating an Active Directory Application in the Azure Portal	
Adding the Microsoft Graph and Windows Azure Active Directory APIs	11
Generating the Secret Key	14
Locating the Application ID	
Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID	
Locating the Subscription ID	
Adding Reader or Contributor Access to the Active Directory Application	17
Setting Up a Proxy Server	
Creating a SOAP/XML Credential for Azure	20
Load-Balancing an Account with Multiple Subscriptions	
Testing the Azure Credential	

Configuring an Azure Active Directory Application

To create a SOAP/XML credential that allows the ScienceLogic platform to access Microsoft Azure, you must provide the following information about an Azure application that is already registered with an Azure AD tenant:

- Application ID
- Subscription ID (if monitoring a single subscription)
- OAuth 2.0 token endpoint URL
- Tenant ID
- Secret key

To capture the above information, you must first create (or already have) an application that is registered with Azure Active Directory. The registered application must have Reader or Contributor access. You can then enter the required information about the application when configuring the SOAP/XML credential in the platform. The registered application and the ScienceLogic credential allow the platform to retrieve information from Microsoft Azure.

TIP: For details on registering an Azure application with Azure AD, see https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications.

Creating an Active Directory Application in the Azure Portal

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

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

To create an application in Azure and register it with Azure Active Directory:

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

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

Microsoft Azure azuretear	nsciencelogic (default directory) - App	o registra	ations	𝒫 Search resources			×	₽>_	\$ 0	banderton@sciencelo
	azureteamsciencelogic (d	efault o	directory) - App registrations							* ×
+ New	 Overview 	*	New application registration	🗄 Endpoints 🗙 Troubleshoot						
🔳 Dashboard 🕴 🇴	💅 Quick start	1.	To view and manage your registrati Console.	ons for converged applications, plea	se visit the	Microsoft Applicati	on			
III resources	MANAGE		Search by name or Appld		~	My apps	*			
📦 Resource groups	g ^R Users and groups	1								
S App Services	Enterprise applications		DISPLAY NAME	APPLICATION TYPE	APPLICAT	ION ID				
Function Apps	Devices (Preview)		No results.							
🧟 SQL databases	App registrations									
🧷 Azure Cosmos DB	Application proxy									
Virtual machines	Licenses	1.								
💠 Load balancers	Azure AD Connect									
Storage accounts	Domain names Mobility (MDM and MAM)									
🐡 Virtual networks	Password reset									
Azure Active Directory	Company branding									
Monitor	User settings									
🧙 Advisor	HI Properties	¥								
→ ✓ More services >										

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

Micro	osoft Azure azureteamsciencelogic (d	efault directory) - App registrations	Q	Q	>_	ŝ	\odot	?	banderton@science.cence.		ļ
	azureteamsciencelogic (default Azure Active Directory	directory) - App registration:	S							* ×	
+	Overview	New application registration	₩ End	points	*™	roubles	noot				
	🥳 Quick start	To view and manage your registrat	ions for c	onverge	ed appli	cations,	please	isit the	Microsoft Application		
	MANAGE	Search by name or Appld						✓	My apps 🗸	·	
	x ^R Users and groups										
٢	Enterprise applications	DISPLAY NAME			APPLIC	ATION TY	PE AI	PPLICATI	ON ID		
<i>«</i> >>	Devices (Preview)	No results.									
201	Registrations										
2	B Application proxy										

4. Enter a **Name** for the application and select Web app / API in the **Application Type** field. In the **Sign-On URL** field, enter any valid URL, then click the **[Create]** button.

Micro	osoft Azure « Create		Q	Q	>_	ŝ	\odot	?	banderton@sciencelo
	Create	□ ×							
+	* Name 0 ScienceLogic Monitoring	~							
	Application type 0	•							
	Web app / API	*							
8	http://localhost.com	~							
<i>«</i>									
X									
<i>`@</i> ?	Create								

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

Adding the Microsoft Graph and Windows Azure Active Directory APIs

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

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

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

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

M	icrosoft Azure 🗸 🗤	zureteamsciencelogic (Default Directory) - App	registrations > Documentation Test > Settings		ureteam@sciencelo
≡		Documentation Test Registered app - PREVIEW	* _ ¤ ×	Settings _	
+	New	🔅 Settings 💉 Manifest 🗴 Delete			
		Essentials 🔨			
	Virtual machine scale s	Display Name Documentation Test	Application ID	GENERAL	
	Virtual network gateways	Application Type Web app / API	Object ID	Properties	>
Ŷ	Subscriptions	Home Page http://my-url	Managed Application In Local Directory Log on to the app to create a local instance	🗮 Reply URLs	>
	Network security groups		All settings 🔿	Owners	>
«· »	Virtual networks (classic)			API ACCESS	
=	Storage accounts			🖧 Required permissions	>
-	SQL servers			💡 Keys	>
•	Azure Active Directory				
۲	Monitor				
٥	Security Center				
0	Billing				
		4		1	

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

Microsoft Azure 🗸 «	Documentation Test > Settings > Required	permissions	
	Settings _	Required permissions	_ 🗆 ×
+ New		+ Add	
	○ Filter settings	API	APPLICATION PER DELEGATED PERM
Virtual machine scale s	GENERAL	No results.	
Virtual network gateways	Properties >		
💡 Subscriptions	∏ Reply URLs		
🏮 Network security groups	📸 Owners >		
🐡 Virtual networks (classic)	API ACCESS		
Storage accounts	& Required permissions		
sQL servers	🕈 Keys 📏		
Azure Active Directory			
🕒 Monitor			
Security Center			
 Billing 			
• ··· ·	٠		•

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

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

Microsoft Azure ∨ « Setting	ıs > Required	l permissions > Add API a	ccess > Select ar	n API \mathcal{P} \mathfrak{G} \mathfrak{G} \mathfrak{G} azureteam@sciencelo \mathfrak{G}
=		dd API access	_ 🗖 ×	Select an API _
+ New				
LEGATED P	RM	1 Select an API Microsoft Graph	>	Search for other applications with Service Principal name
Virtual network gateways				Windows Azure Active Directory (Microsoft Azure ActiveDirectory)
💡 Subscriptions		2 Select permissions	>	Microsoft Graph
🏺 Network security groups				Windows Azure Service Management API Office 365 Management APIs
Virtual networks (classic)				
Storage accounts				
🔜 SQL servers				
Azure Active Directory				
🐣 Monitor				
Security Center				
Ø Billing		Done		Select
· · · · · · · · · · · · · · · · · · ·	1			

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

Microsoft Azure 🗸 « Se	iettings > Requ	uired permissions > Add API ac	ccess > Enable Ac	cess 🔎 🗘 🐯 😳 곗	azureteam@sciencelo
_ = _	- - ×	Add API access	_ 🗆 ×	Enable Access	_ 🗆 ×
+ New					
	TED PERM	Select an API	~	Read and write calendars in all mailboxes	🔮 Yes 🔺
Virtual machine scale s		Microsoft Graph	•	Read contacts in all mailboxes	🔮 Yes
Virtual network gateways		-		Read and write contacts in all mailboxes	🔮 Yes
💡 Subscriptions		2 Select permissions 1 role, 0 scope	>	Read all groups	🔮 Yes
🏮 Network security groups				Read and write all groups	🔮 Yes
Virtual networks (classic)				✓ Read directory data	🔮 Yes
Storage accounts				Read and write directory data	🔮 Yes
				Read and write devices	🔮 Yes
				Read all users' full profiles	🔮 Yes
Azure Active Directory				Read and write all users' full profiles	🔮 Yes
😁 Monitor				Read and write all user mailbox settings (preview)	🔮 Yes 🗸
Security Center					
O Billing		Done		Select	
· · · · · · · · · · · · · · · · · · ·					•

- 8. Click [Done] to save.
- 9. Repeat these steps for the Windows Azure Active Directory API. To do so, choose Windows Azure Active Directory (rather than Microsoft Graph) in step 6.
- 10. After you add the Microsoft Graph and Windows Azure Active Directory APIs, return to the **Required permissions** pane and click **[Grant Permissions]**.

Generating the Secret Key

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

To generate a secret key:

- 1. In the left pane of the Azure portal (<u>https://portal.azure.com</u>), click **Active Directory**, then click **App** registrations.
- 2. Click the application name.
- 3. In the **Settings** pane, click **[Keys]**.

Micr	OSOft Azure 《 Azure Stack > Setting	ıs	Q	Q	>_ ĝ		?	banderton@sciencelo AZURETEAMSCIENCELOGIC (
	Azure Stack Registered app		* 🗆	×	Setting	gs		∎ ×
+	Settings 🖍 Manifest 🛅 Delete				, <i>♀</i> Filte	er settings		
	Essentials 🔨				GENERA	L		
	Display name Azure Stack	Application ID			Pr	operties		>
	Application type Web app / API	Object ID			j≣ Re	eply URLs		>
(Home page https://management.local.azurestack.exter	Managed application in local directory Azure Stack	1		 O	wners		>
<i>«</i>			All settings	→	API ACCI	ss		
						equired pe	rmissions	;
2					📍 Ke	eys		>
>	4	_			TROUBL	SHOOTING	+ SUPPOR	τ τ -

- 4. In the Keys pane, enter a name in the Key Description field and select a duration in the Expires field.
- 5. Click [Save] to generate the secret key.

Micro	osoft Azure « Azure Stack	> Settings > H	Keys		୍ମ ଦ ≻_ 🕸 😳 ଡି	banderton@sciencelo AZURETEAMSCIENCELOGIC (
≡	Settings	□ ×	Keys			□ ×
+			R Save X Discard			
	GENERAL		DESCRIPTION	EXPIRES	VALUE	
	Properties	>	No results.			
(🗮 Reply URLs	>	Key description	Duration 🗸	Value will be displayed on save	
8	🏰 Owners	>				
<i>«</i> ?>	API ACCESS					
2	💑 Required permissions	>				
2	📍 Keys	>				
>	TROUBLESHOOTING + SUPPORT	•				•

6. Copy and save the key value.

2

Locating the Application ID

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

To locate the Application ID:

- 1. In the left pane of the Azure portal (https://portal.azure.com), click [Azure Active Directory].
- 2. Click **[App registrations]**, then click on the name of the Active Directory application you will use to authenticate your Azure account. The Application ID appears in the **Essentials** section.

Mi	crosoft Azure 🗸 «	Documentation Test	
≡		Documentation Test Registered app - PREVIEW	* _ 🗆 ×
+	New	🔅 Settings 💉 Manifest 菌 Delete	
	Virtual networks (clas	Essentials A	
=	Storage accounts	Display Name Documentation Test	Application ID
2	SQL servers	Application Type Web app / API	Object ID
: 🚸	Azure Active Directory	Home Page http://my-url	Managed Application In Local Directory Log on to the app to create a local instance
0	Monitor		All settings ->
0	Security Center		
0	Billing		
	Help + support		

3. Copy and save the *Application ID*.

Locating the OAuth 2.0 Token Endpoint URL and the Tenant ID

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

To locate the OAuth 2.0 token endpoint URL and the tenant ID:

1. In the left pane of the Azure portal (<u>https://portal.azure.com</u>), click [Azure Active Directory].

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

Microsoft Azure 🗸 🗸	azureteamsciencelogic (Default Director	y) - App registrations	> Endpoints	¢ ک	ŝ	② ⑦ azuret	eam@sciencelo
ncelogic (Default Dir	rectory) - App registrations		*	_ 🗖	×	Endpoints PREVIEW	_ 🗆 ×
+	+ Add 🗄 Endpoints				A	SAML-P SIGN-ON ENDPO	
6	Search by name or Appld		All apps	~		https://login.windows.n	net/
<>	DISPLAY NAME	APPLICATION TYPE	APPLICATION ID			SAML-P SIGN-OUT ENDP	POINT
-	QA QATesting	Web app / API				https://login.windows.n	net/
R ,	AA AD Auth/Avail Test	Native				MICROSOFT AZURE AD G	
sqt 🚸	SM ScienceLogic Monitoring	Native Web app / API				https://graph.windows.	
(C) lications	FS fsuntodel	Web app / API				OAUTH 2.0 TOKEN ENDP	OINT
<u>a</u>	AR arm_dev	Web app / API				https://login.windows.n	
• ect	FS fsuntraining	Web app / API				OAUTH 2.0 AUTHORIZAT	
· · ·	DE devwebtest	Web app / API				https://login.windows.n	
>	FS fsuntraining2	Web app / API					Ť

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

For example, in the following OAuth 2.0 token endpoint URL, the GUID is in bold: https://login.windows.net/**eg58975d-1953-5509-4654-b5d4bbga22ceg**/oauth2/token

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

Locating the Subscription ID

If you are monitoring only a single Azure subscription, you must provide the Subscription ID of the Azure Active Directory application you will use to authenticate your account when you configure your SOAP/XML credential for Azure in the ScienceLogic platform.

NOTE: If you are monitoring an account with multiple child subscriptions, you can skip this section.

To locate the Subscription ID:

1. In the left pane of the Azure portal (https://portal.azure.com), click [Subscriptions].

2. Copy and save the **Subscription ID** of the subscription where you created the Azure Active Directory application you will use to authenticate your account.

Microsoft Azure 🗸 Sub	scriptions	𝒫 ⊈ ঊ ☺	azureteam@sciencelo
	Subscriptions azureteamsciencelogic (Default Directory)		* _ 🗆 ×
+ New	+ Add		
Storage accounts (class			
🚯 Traffic Manager profile 🛛	Search to filter items		
🚯 Traffic Manager profiles	SUBSCRIPTION ^ SUBSCRIPTION ID	ROLE CURRENT SPEND	SUBSCRIPTION S ^
W tranic Manager promes	😳 Eng - Azure Team	Account admin Not available	
Virtual networks			
💿 Virtual machine scale s			
🛃 Virtual network gateways			
📍 Subscriptions			
🏮 Network security groups			
↔ Virtual networks (classic)			
Storage accounts			
-			

Adding Reader or Contributor Access to the Active Directory Application

To allow ScienceLogic to access your Azure account, you must specify the type of access the user whose information you will use in your SOAP/XML credential has to the Active Directory application used to authenticate your account.

You can select one of the following access roles:

- Reader. This read-only user can view everything but cannot make changes.
- Contributor. This user can read and manage everything in Azure except access rights.

NOTE: You must have Contributor access to collect performance data for Azure storage queues, tables, and blobs.

To specify access roles to the Azure Active Directory application:

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

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

Microsoft Azure 🗸 s	ubscriptions >	Eng - Azure Team - Access	control (I	AM)			¢ 🖓 🕸		eam@sciencel reamsciencelogic	
≡		* - □	×	Eng - Azure Team -	Access o	ontrol	(IAM)		* -	□ ×
+ New						🕂 Add	🐁 Roles			
😑 Storage accounts (cl						_				
_	URRENT SPEND	SUBSCRIPTION S ^		Overview		0	You can control access to your Azu custom roles. You can also use grou access. Learn more			Z
🚯 Traffic Manager prof	lot available	📀 Active 🛛		Access control (IAM)						
Virtual networks			·	🔀 Diagnose and solve problem:		USER		ROLE	ACCESS	
Virtual machine scal				SETTINGS			arm_dev	Contributor, Reader	Assigned	
🗟 Virtual network gate				Programmatic deployment			Azure Team azureteam@sciencelogic.com	Owner	Assigned	
Subscriptions				Resource groups			azure_team	Contributor	Assigned	
🏮 Network security gr				Resources				Contributor	Assigned	
Virtual networks (cla				Usage + quotas		•	fsuntest	Contributor, Reader	Assigned	
🧱 Storage accounts				Management certificates			fsuntraining	Contributor	Assigned	
👼 SQL servers				My permissions		-				
Azure Active Directory				Properties		Î	fsuntraining2	Contributor	Assigned	
Monitor				Resource locks	•	i	gisela_app	Contributor	Assigned	
Security Center	4						-			

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

Microsoft Azure 🗸 🗧	Subscriptions > Eng - Azure Team - Acce	ess control (IAM) >	Add access	> Selo	ect a n	ole	© 10 ج	azureteam@sciencelo
≡	AM)		* -		×	Add access	_ 🗆 ×	Select a role _
+ New	😪 Roles							
Storage accounts (cl					-			î
😵 Traffic Manager prof 🛛	You can control access to your Azure resour custom roles. You can also use groups in yo access. Learn more	rces using built-in role our Azure Active Directe	s or your own ory to control	Z		Select a role Contributor	>	Owner 🖲
🛞 Traffic Manager prof						Add users		Contributor
Virtual networks		ROLE	ACCESS		L	Z None selected	>	
🧕 Virtual machine scal	arm_dev	Contributor, Reader	Assigned					Reader 🛛
 Virtual network gate Subscriptions 	Azure Team azureteam@sciencelogic.com	Owner	Assigned					API Management Service Contri 0
 Subscriptions Network security gr 	azure_team	Contributor	Assigned					Application Insights Component 0
Virtual networks (cla	fsuntest	Contributor, Reader	Assigned					
Storage accounts	fsuntraining	Contributor	Assigned					Automation Operator 0
SQL servers	fsuntraining2	Contributor	Assigned					BizTalk Contributor
Azure Active Directory	-		<u> </u>					
Monitor	gisela_app	Contributor	Assigned			ОК	_	• • • • • • • • • • • • • • • • • • •
Security Center	4				T			

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

6. Click [OK].

Microsoft Azure	e 🗸 Subscriptions > Eng - Azure Te	am - Access control (IAM) > Add a	access > Ada	d users		¢ ي م	3 😳 🕐 azureteam@sciencelo Azureteamsciencelogic (
\equiv m - Access of	control (IAM)	*	_ 🗖		d access	_ 🗖 ×	Add users _ 🗖	×
+	🕂 Add 🔹 Roles						+ Invite	
				*			Select	-
•		ure resources using built-in roles or your oups in your Azure Active Directory to co			Select a role Contributor	~	Search by name or email address	1
•					2 Add users	>	AM amaida amaida@azureteamsciencelogic.o	
	USER	ROLE ACCESS			None selected		AS asdasdas tsuser@azureteamsciencelogic.on.	
•	arm_dev	Contributor, Reader Assigne	ed					
ent ent	AT Azure Team azureteam@sciencelogic.com	Owner Assigne	ed				azureteam@sciencelogic.com	
	azure_team	Contributor Assigne	ed				AZ azureadmin@sciencelogic.com	
 ♥ ↔> 	fsuntest	Contributor, Reader Assigne	d				BP bpage bpage@azureteamsciencelogic.on.	
	•	, , , , , , , , , , , , , , , , , , , ,		1			CE California Employeesf01e2a00	
s -	fsuntraining	Contributor Assigne	•d					- •
≅ . ◆	fsuntraining2	Contributor Assigne	ed				Selected Azure Team	>
e	gisela_app	Contributor Assigne	ed		ОК		Select	
0	-			*				•

Setting Up a Proxy Server

Depending on your needs, you can optionally enable the ScienceLogic platform to connect to Azure through a third-party proxy server. With this configuration, the ScienceLogic platform connects to the proxy server, which then connects to Azure relays information to the proxy server and the platform then retrieves that information from the proxy.

NOTE: You can connect to Azure via a proxy server regardless of whether you are monitoring a single subscription or an account with multiple child subscriptions. You can connect to both Microsoft Azure and Microsoft Azure Government via a proxy server.

NOTE: The Microsoft: Azure PowerPack is certified to work with SQUID version 3.5.12 proxy servers.

If you choose to use this configuration, you will first need to set up the proxy server. To do so:

NOTE: For the following steps, you must have openssh-server.x86_64 and telnet installed.

1. Using SSH, connect to the proxy server.

2. Run the following commands in the command-line interface:

```
sudo apt-get install squid3
cd /etc/squid3
sudo cp squid.conf squid.conf.bak
sudo rm squid.conf
sudo touch squid.conf
sudo vim squid.conf
```

- 3. Do one of the following, depending on your needs:
 - If you want to connect to the proxy server using basic authentication, add the following lines to the new squid.conf file:

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/passwords
auth_param basic realm proxy
acl authenticated proxy_auth REQUIRED
http_access allow authenticated
http_port [port number]
visible_hostname [hostname]
sudo htpasswd -c /etc/squid3/passwords [username]
[password]
[password]
```

• If you do not want to use basic authentication to connect to the proxy server, add the following lines to the new squid.conf file:

```
http_access allow all
http_port [port number]
visible hostname [hostname]
```

4. Restart the SQUID service:

sudo service squid3 restart

5. Using SSH, connect to the ScienceLogic collector, then telnet to the opened port on the proxy server to verify that the proxy server is set up properly.

Creating a SOAP/XML Credential for Azure

After you note the application ID, subscription ID, OAuth 2.0 token endpoint URL, tenant ID, and secret key of the application (that is registered with Azure Active Directory) that you will use to authenticate your Azure account, you can create a SOAP/XML credential for Azure in the ScienceLogic platform. This credential allows the Dynamic Applications in the *Microsoft: Azure* PowerPack to communicate with your Azure subscriptions.

If you want to connect to your Azure account through a third-party proxy server, you must also add the proxy information in the credential. This applies to both Microsoft Azure and Microsoft Azure Government.

The *Microsoft: Azure* PowerPack includes three sample credentials you can use as templates for creating SOAP/XML credentials for Azure. They are:

- Azure Credential Government, for users who subscribe to Microsoft Azure Government
- Azure Credential Proxy, for users who connect to Azure through a third-party proxy server
- Azure Credential SOAP/XML, for users who do not use a proxy server

To create a SOAP/XML credential for Azure:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the Azure Credential Proxy, the Azure Credential SOAP/XML, or the Azure Credential -

Government credential, and then click its wrench icon (*P*). The **Edit SOAP/XML Credential** modal page appears:

Credential Editor [77]	×
Edit SOAP/XML Credential #77	New Reset
Basic Settings Profile Name Content Encoding Method HTTP Version Azure Credential - Proxy [text/xml] [POST] [HTTP/1.1] URL [https://Host:Port/Path %D = Aligned Device Address %N = Aligned Device Host Name] [https://login.windows.net/ <tenant_id>/oauth2/token?api-version=1.0 HTTP Auth User HTTP Auth Password Timeout (seconds) 120</tenant_id>	Soap Options Embedded Password [%P] Embed Value [%1] Embed Value [%2] <client_id> <tenant_id> Embed Value [%3] Embed Value [%4] <subscription_id> <secret_key></secret_key></subscription_id></tenant_id></client_id>
Proxy Settings Hostname/IP Port User Password (HOST-OR-IP () <proxy_user> ••••••••• CAINFO () <proxy_user> ••••••••• CAINFO () () <proxy_user> CONFORCTIMEOUT () () COOKIEFILE () () () COOKIEFILE () () COOKIELJAR () () CUSTOMREQUEST () () DINSCACHETIMEOUT () ()</proxy_user></proxy_user></proxy_user>	HTTP Headers + Add a header
Save As	

3. Enter values in the following fields:

Basic Settings

- Profile Name. Type a new name for the Azure credential.
- Content Encoding. Select text/xml.
- Method. Select POST.
- HTTP Version. Select HTTP/1.1.
- URL. Type the OAuth 2.0 token endpoint URL for the Azure Active Directory application.
- HTTP Auth User. Leave this field blank.

- HTTP Auth Password. Leave this field blank.
- Timeout (seconds). Type "120".

Proxy Settings

- Hostname/IP. If you are connecting to Azure via a proxy server, type the server's hostname or IP address. Otherwise, leave this field blank.
- **Port**. If you are connecting to Azure via a proxy server, type the port number you opened when *setting* up the proxy server. Otherwise, leave this field blank.
- **User**. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator username. Otherwise, leave this field blank.
- **Password**. If you are connecting to Azure via a proxy server using basic authentication, type the server's administrator password. Otherwise, leave this field blank.

CURL Options

• CURL Options. Do not make any selections in this field.

SOAP Options

- Embedded Password [%P]. Leave this field blank.
- Embed Value [%1]. Type the Application ID for the Azure Active Directory application.
- Embed Value [%2]. Type the Tenant ID for the Azure Active Directory application.
- **Embed Value [%3]**. If you are monitoring only a single Azure subscription, type the Subscription ID for the Azure Active Directory application. If you are monitoring multiple subscriptions, leave this field blank.
- Embed Value [%4]. Type the secret key for the Azure Active Directory application.

HTTP Headers

- HTTP Headers. If you are using Microsoft Azure, you can leave this field blank. If you are using Microsoft Azure Government, this field contains the text "AZGOV", so you can differentiate credentials.
- 4. Click [Save As].
- 5. In the confirmation message, click [OK].

Load-Balancing an Account with Multiple Subscriptions

When monitoring an account with multiple child subscriptions, instead of discovering all child subscriptions in a single dynamic component map under their parent account, you can load-balance subscriptions and their components across multiple Data Collectors.

To do this:

• The Collector Group that discovers a group of subscriptions can contain only one Data Collector. You cannot use multiple Data Collectors to discover the Azure components in a single dynamic component map or discover the same device in multiple dynamic component maps.

2

- To group multiple Azure subscriptions into a single dynamic component map, you need to create a shared credential for that group of subscriptions.
- To create the credential:
 - Perform all of the steps in the section on Configuring an Azure Active Directory Application.
 - Align each subscription in the group with the same application that you registered with Azure AD.
 - In the credential, enter the application ID in the *Embed Value* [%1] field.
 - In the credential, leave the *Embed Value [%3]* field blank.
- During discovery, use this credential to discover the group of subscriptions.
- During discovery, specify the Data Collector you want to use for the group of subscriptions.
- The discovered subscriptions will reside in a common dynamic component map.
- Repeat these steps for each group of subscriptions.

Testing the Azure Credential

The ScienceLogic platform includes a Credential Test for Microsoft Azure. Credential Tests define a series of steps that the platform can execute on demand to validate whether a credential works as expected.

The Azure Credential Test can be used to test a SOAP/XML credential for monitoring Azure using the Dynamic Applications in the *Microsoft: Azure* PowerPack. The Azure Credential Test performs the following steps:

- Test Port Availability. Performs an NMAP request to test the availability of the Azure endpoint HTTPS port.
- Test Name Resolution. Performs an nslookup request on the Azure endpoint.
- Make connection to Azure account. Attempts to connect to the Azure service using the account specified in the credential.
- Make Azure Active Directory Request. Verifies that the Azure Active Directory service can be queried.

NOTE: The Azure Credential Test has not been certified for use with credentials that use a proxy server.

To test the Azure credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).

2. Locate the Azure Credential Test and click its lightning bolt icon (//). The Credential Tester modal page appears:

Credential Tester [BETA] ×
Test Type	[Azure Credential Test]
Credential	Azure Credential - SOAP/XML
Hostname/IP	
Collector	RS-ISO-DCU-33
	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 (2) 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".

Chapter

Discovering Azure Resources

Overview

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

Creating an Azure Virtual Device	25
Aligning the Azure Dynamic Applications	
Discovering Azure Component Devices	
Viewing Azure Component Devices	
Relationships Between Component Devices	

Creating an Azure Virtual Device

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

To create a virtual device that represents your Azure service:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Click the **[Actions]** button and select Create Virtual Device from the menu. The Virtual Device modal page appears.

3. Enter values in the following fields:

Virtual Device		×
Create Virtual Device		Reset
Device Name	Azure Cloud	
Organization	Azure	•
Device Class	Microsoft Azure Services	T
Collector	CUG	•
	Add	

- Device Name. Enter a name for the device. For example, "Azure Cloud".
- **Organization**. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.
- Device Class. Select Microsoft | Azure Services.
- Collector. Select the collector group that will monitor the device.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how the ScienceLogic Platform monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on Load-Balancing an Account with Multiple Subscriptions.

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

Aligning the Azure Dynamic Applications

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

- **Discovery**. These Dynamic Applications poll Azure for new instances of services or changes to existing instances of services.
- **Configuration**. These Dynamic Applications retrieve configuration information about each service instance and retrieve any changes to that configuration information.
- Performance. These Dynamic Applications poll Azure for performance metrics.

When configuring the ScienceLogic platform to monitor Azure services, you can manually align Dynamic Applications to discover Azure component devices.

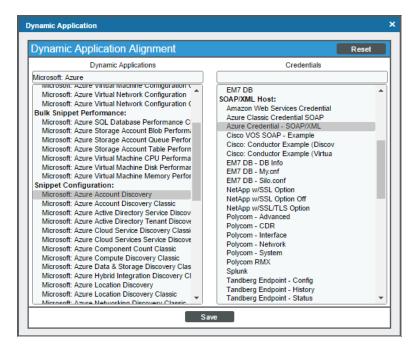
Discovering Azure Component Devices

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

TIP: When monitoring an account with multiple child subscriptions, ScienceLogic recommends that you first review your device capacity and load limits to determine the best method for implementation prior to discovery. For details, see the section on *Load-Balancing an Account with Multiple Subscriptions*.

To manually align the "Microsoft: Azure Account Discovery" Dynamic Application:

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



- In the Dynamic Applications field, select Microsoft: Azure Account Discovery.
- In the **Credentials** field, select the credential you created for your Azure service.
- 6. Click **[Save]** to align the Dynamic Application with the Azure virtual device.

When you align the "Microsoft: Azure Account Discovery" Dynamic Application with the Azure virtual device, the ScienceLogic platform does one of the following, depending on your subscription model:

- If you are monitoring an account with multiple child subscriptions, the platform creates a root component device representing the Azure account and one or more child component devices representing all of your Azure subscriptions.
- If you are monitoring a single subscription, the platform creates a root component device representing your Azure subscription.

TIP: When monitoring an account with multiple child subscriptions, you can load-balance how the ScienceLogic Platform monitors your Azure components by discovering groups of subscriptions and their components across multiple collectors. For details, see the section on Load-Balancing an Account with Multiple Subscriptions.

The ScienceLogic platform then automatically aligns several other Dynamic Applications to the subscription component devices. These additional Dynamic Applications discover and create component devices for Active Directory tenants, Traffic Manager profiles, and each location used by the Azure account.

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

- Application Gateway Services
 - Application Gateways
- Resource Groups Services
 - Resource Groups
- Storage Services
 - Storage Accounts
- Virtual Machines Services
 - Virtual Machines
- Virtual Network Services
 - VPN Gateways
 - Virtual Networks
 - Virtual Network Subnets
- SQL Server Services
 - SQL Servers
 - SQL Databases
- Recovery Service Vaults Services
 - Recovery Service Vaults
- Network Security Group Services
 - Network Security Groups

- Load Balancer Services
 - Load Balancers

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

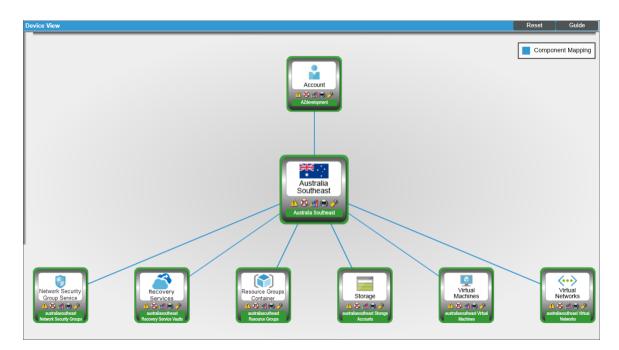
NOTE: When discovering a large number of component devices, such as when discovering an account with multiple child subscriptions, the discovery process can cause the appearance of numerous critical events with the message, "Large backlog of asynchronous jobs detected". This will occur only during the initial discovery session.

Viewing Azure Component Devices

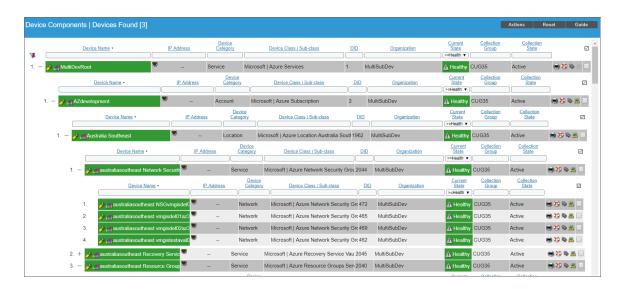
In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the Azure service and all associated component devices in the following places in the user interface:

NOTE: If you are using both the *Microsoft: Azure* and *Microsoft: Azure Classic* PowerPacks to monitor resources in the same Azure subscription, duplicate Active Directory and SQL database component devices will appear in the ARM and Classic component maps in the ScienceLogic platform.

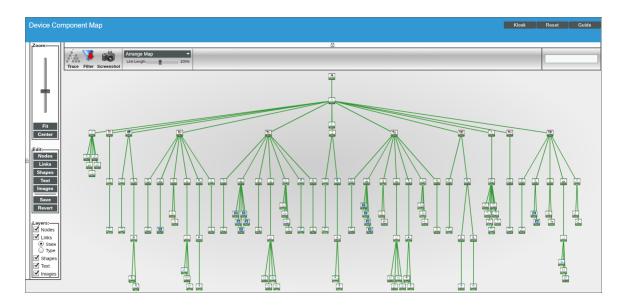
• The **Device View** modal page (click the bar-graph icon [**1**] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



• The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with an Azure service, find the Azure virtual device and click its plus icon (+):



The Component Map page (Views > Device Maps > Components) allows you to view devices by root
node and view the relationships between root nodes, parent components, and child components in a map.
This makes it easy to visualize and manage root nodes and their components. The ScienceLogic platform
automatically updates the Component Map as new component devices are discovered. The platform also
updates each map with the latest status and event information. To view the map for an Azure service, go to
the Component Map page and select the map from the list in the left NavBar. To learn more about the
Component Map page, see the Views manual.



Relationships Between Component Devices

In addition to parent/child relationships between component devices, the ScienceLogic platform also creates relationships between the following component devices:

- Virtual Machines and Storage Accounts
- Virtual Machines and Network Security Groups
- Virtual Machines and Resource Groups
- Virtual Machines and Virtual Networks
- Virtual Machines and Subnets
- Application Gateways and Subnets
- Application Gateways and Resource Groups
- VPN Gateways and Subnets
- VPN Gateways and Resource Groups
- Storage Accounts and Resource Groups
- Virtual Networks and Resource Groups
- SQL Servers and Resource Groups
- SQL Databases and Resource Groups
- Traffic Manager Profiles and Resource Groups
- Azure Traffic Managers and Traffic Managers
- Network Security Groups and Resource Groups
- Network Security Groups and Virtual Network Subnets
- Recovery Service Vaults and Resource Groups

Additionally, the platform can automatically build relationships between Azure component devices and other associated devices:

• If you discover Cisco Cloud Center devices using the Dynamic Applications in the Cisco: Cloud Center PowerPack version 103 or later, the platform will automatically create relationships between Azure Virtual Machines and Cisco Cloud Center applications.

© 2003 - 2018, 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