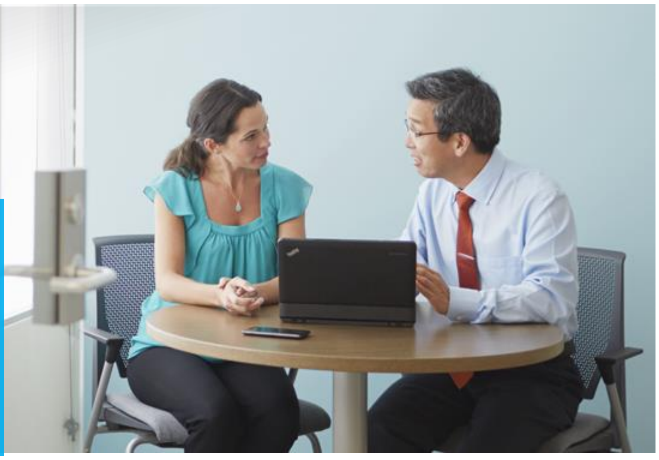
Microsoft

Assessment Setup Guide



Introduction

Setting up and configuring On-Demand assessments is a complex process. There are several steps to complete in a specific order to ensure successful assessment setup and execution. This article aims to provide the details required that are applicable across all the On-Demand assessments available on Services Hub.

This article is organized in four major sections which should be followed in order to ensure successful configuration and execution of On-Demand assessments.

Getting Started with On-Demand Assessments

Establish connectivity to Azure Log Analytics

Configure Microsoft On-Demand Assessment(s)

Working with assessment results

There are also configuration details applicable to each individual assessment that are referred to in the *Configure Microsoft On-Demand Assessment(s)* section of this article with links to the relevant content.

Ensure that you have reviewed the information in the assessment(s) prerequisites and configuration documentation before continuing the setup in this document. Download the prerequisites for your assessment(s) at https://docs.microsoft.com/en-us/services-hub/health/assessment-prereq-docs if not already downloaded.

For general information about On-Demand assessments, see the Assessment FAQs.

This document was last updated on August 28, 2019. To ensure you have the latest version of this document, check here: https://go.microsoft.com/fwlink/?linkid=860142

Table of Contents

Getting Started with On-Demand Assessments 3

Azure Subscription 3

Services Hub Registration 4

Linking of the Azure Subscription and Log Analytics workspace to Services Hub workspace 5

Add the Assessment(s) in Services Hub 8

Providing Access to Azure Log Analytics workspace 9

Establish connectivity to Azure Log Analytics 10

Log Analytics Gateway for Azure Monitor Setup 12

Download and install the Log Analytics Gateway 13

Microsoft Monitoring Agent Setup 13

Download and install the Microsoft Monitoring Agent (MMA) setup file from Azure Log Analytics 15

Microsoft Monitoring Agent Upgrade 19

Setup and configure Log Analytics using SCOM 21

Offline – Disconnected Environment 23

Internet Access Machine 24

Data Collection Machine 24

Configure Microsoft On-Demand Assessment(s) 25

Configuring the required Group Policy Objects 26

Verify the solution is downloaded on the data collection machine 27

Creation of the Assessment Scheduled Task 28

Download On-Demand Assessment Prerequisites 30

Working with Assessment Results 30

Validate Successful Assessment 31

Services Hub Assessment Page 33

Downloading the reports from Services Hub 33

Remediation Plan creation in Service Hub 33

Additional Azure Log Analytics Information... 36

Getting Started with On-Demand Assessments

Assessments are available through the Services Hub to help you assess and optimize the availability, security, and performance of your on-premises, hybrid, and cloud Microsoft technology environments. These assessments use Microsoft Azure Log Analytics, which is designed to give you simplified IT and security management across your environment.

Note: *On average, it takes two hours to initially configure your environment to run an On-Demand Assessment. After you run an assessment you can review the recommendations in Azure Log Analytics. This will provide you with a prioritized list of recommendations, categorized across six focus areas. This allows you and your team to quickly understand risk levels, the health of your environments, act to decrease risk, and improve your overall IT health.*

Use the following checklist to ensure all steps in this section are completed before moving onto the next section.

- ✓ Azure Subscription
- ✓ Services Hub Registration
- ✓ Link Azure Subscription and Log Analytics Workspace to Services Hub
- ✓ Add the assessment(s) in Services Hub
- ✓ Provide access to Azure Log Analytics workspace

Sign up for On-Demand Assessment Initial Setup and Configuration Service

An initial setup and configuration service with a Microsoft engineer is available to simplify the assessment setup process as part of the Microsoft Unified Support base contract offering. We help you link, enable, install, and configure a Services Hub On-Demand Assessment. To learn more, see our Data Sheet. You can get started by clicking 'Sign up' on the top right tile of your Services Hub dashboard under 'Setup & Configuration'. This sends an email to your Microsoft representative to request scheduling of this service.

Whether using the On-Demand Assessment – Setup and Config Service or not, all the steps in this article and the assessment(s) prerequisites documents needs to be completed to ensure successful setup and execution of On-Demand assessments.   Complete the steps in this guide, then select an On-Demand Assessment from the table of contents on the left, under Getting Started with On-Demand Assessments, to see details, configuration instructions, and links to download data sheets and detailed prerequisites for selected On-Demand Assessments.

Azure Subscription

On-Demand Assessments ingest their recommendations and supporting details into Azure Log Analytics. The Azure Log Analytics service requires an Azure subscription owned by the organization. If there is already an Azure subscription, then a customer representative (their registered email address) with the required Azure Log Analytics access and/or Azure Subscription access will need to be invited to the Services Hub workspace by the TAM.

If there is no Azure subscription, Microsoft will sponsor one for the customer. The ideal owner for the sponsored subscription is the main point of contact IT professional that will be working with the assessment results. There are a couple of options to have a sponsored Azure subscription provisioned.

The preferred option is to share an organizational email address to be provisioned as owner of a no-cost Azure sponsorship with the organization's TAM. Once the Azure sponsorship is created, an email with an invitation to activate the subscription will be sent to the provided organizational email address. Activate the Azure subscription through the link provided in the email. This account will be invited to the Services Hub workspace by the TAM.

An alternative option is to request for one directly by creating a support ticket by contacting Services Hub Support and providing an organizational email address to be provisioned as owner of a no-cost Azure sponsorship.

Note*: Customers can choose to use any Azure Subscription for this purpose as long as the user has the required Azure Subscription and/or Log Analytics role to perform the required actions. The Azure Subscription can be an EA or Pay-As-You-Go or trial azure subscriptions. Azure subscriptions created merely due to presence of Office 365 licenses cannot be used as they don't have active azure credits.*

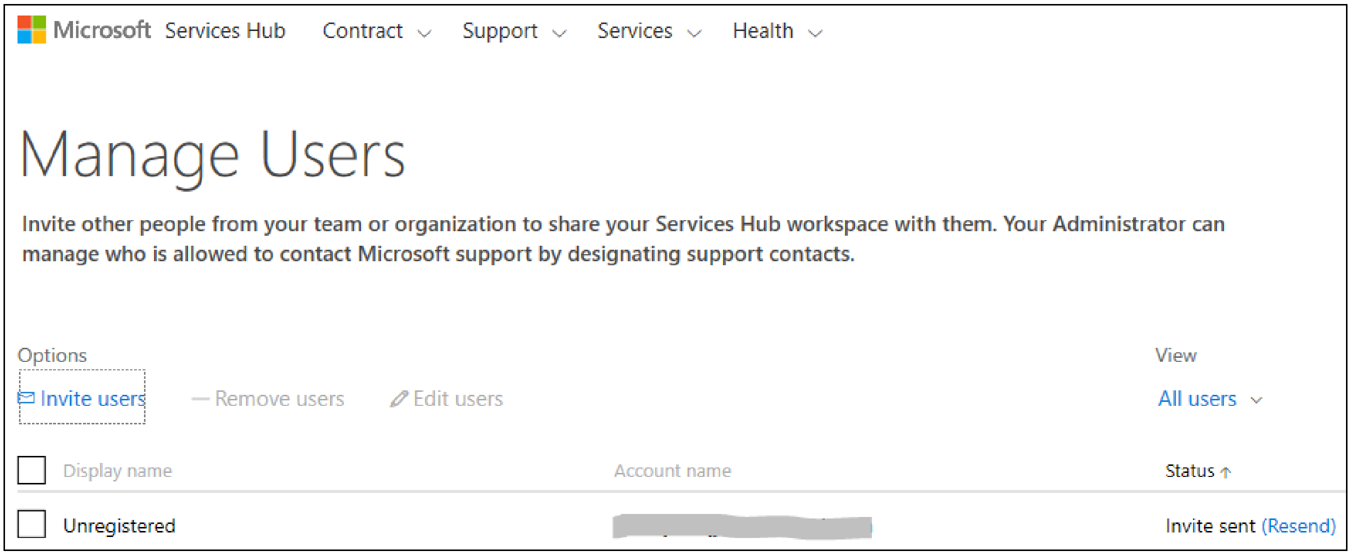
Tip*: No-cost sponsored Azure subscriptions requested from Services Hub Support by default have a validity of 1 year. These subscriptions can be extended before expiry if needed in case of renewals. You can read more about how to manage these subscriptions in this Azure Rollover article.*

Services Hub Registration

The customer with the required access must be registered with the Services hub. Additionally, if the assessment will include a PFE lead delivery, then the PFE must also be registered with the Services Hub.

TAM tasks:

1. The TAM invites customer and PFE (for engineer lead assessment deliveries). Log in to Services Hub using Microsoft Edge and go to **Contract > Manage Users**.
2. Add customers email addresses and PFE with alias@Microsoft.com and ensure the **Health** and **Plans** options are selected to allow the user to see the assessment tab and create a remediation plan.



Manage Users

Invite other people from your team or organization to share your Services Hub workspace with them. Your Administrator can manage who is allowed to contact Microsoft support by designating support contacts.

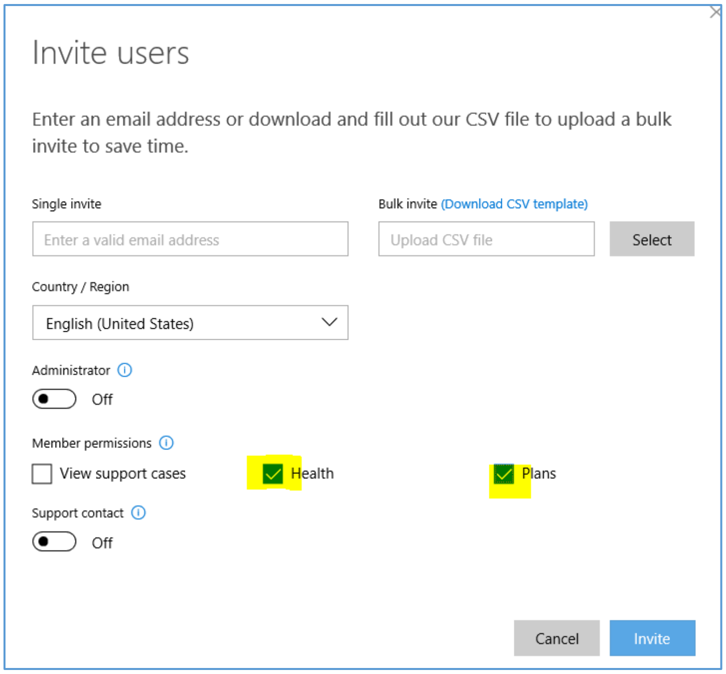
Options

Invite users — Remove users Edit users

View

All users

□	Display name	Account name	Status ↑
□	Unregistered	[redacted]	Invite sent (Resend)



Invite users

Enter an email address or download and fill out our CSV file to upload a bulk invite to save time.

Single invite: Enter a valid email address

Bulk invite (Download CSV template): Upload CSV file [Select]

Country / Region: English (United States)

Administrator ⓘ: Off

Member permissions ⓘ

□ View support cases ☑ Health ☑ Plans

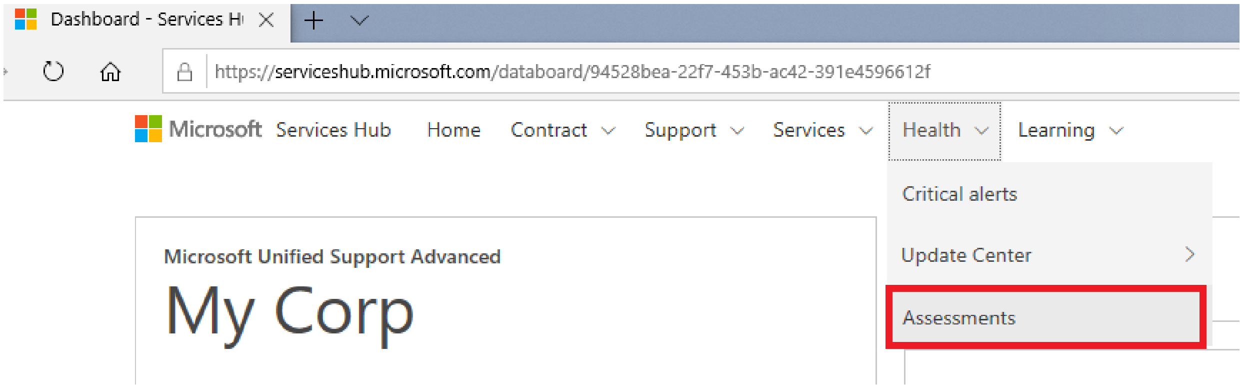
Support contact ⓘ: Off

Customer and PFE registration tasks:

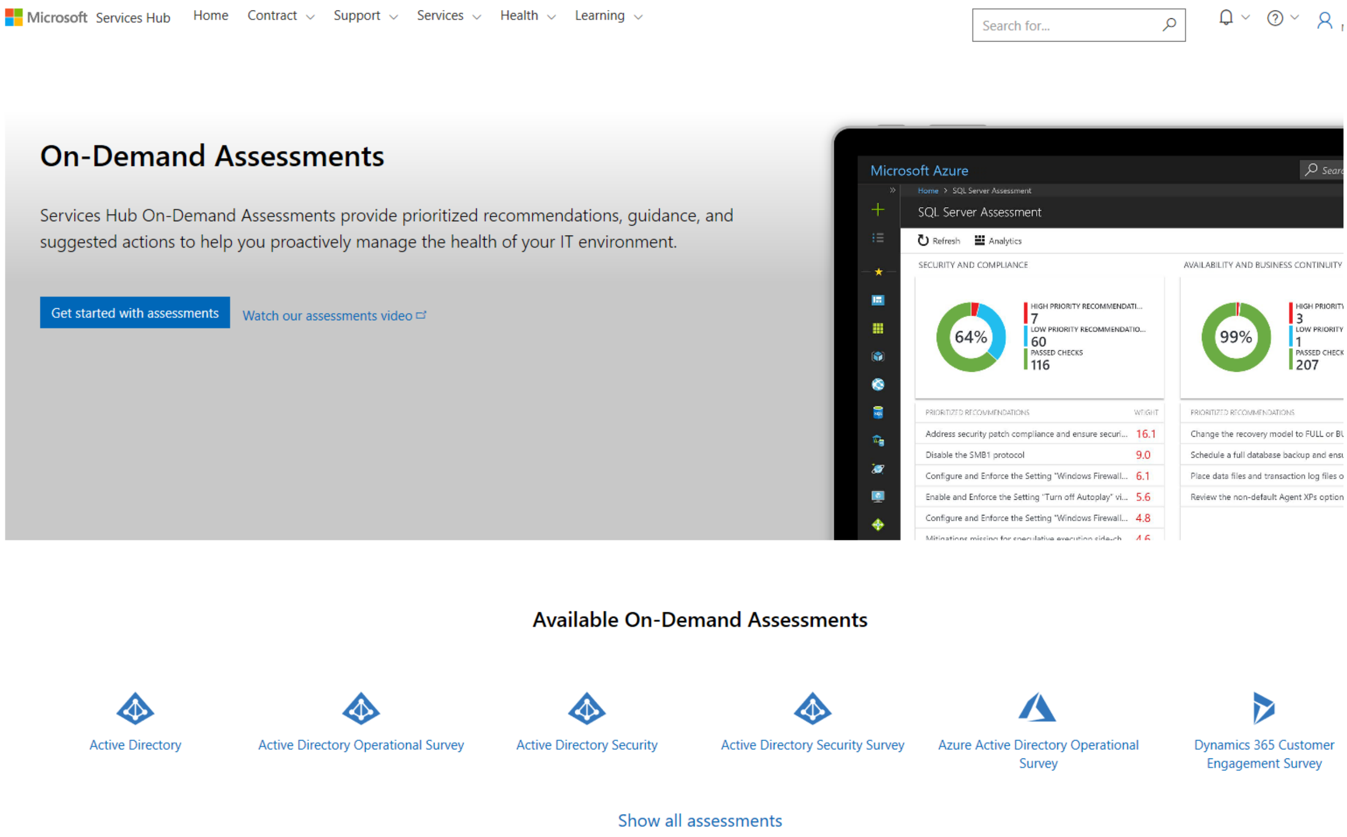
1. Review your email inbox for an email from your TAM inviting you to register on Services Hub
2. Click the link in the email whose URL begins with https://serviceshub.microsoft.com/account/register?registrationId=<uniqueID>

Linking of the Azure Subscription and Log Analytics workspace to Services Hub workspace

1. Log into Services hub with user credentials with the required access. Go to Health -> Assessments.



2. Click on **Get started with assessments**.

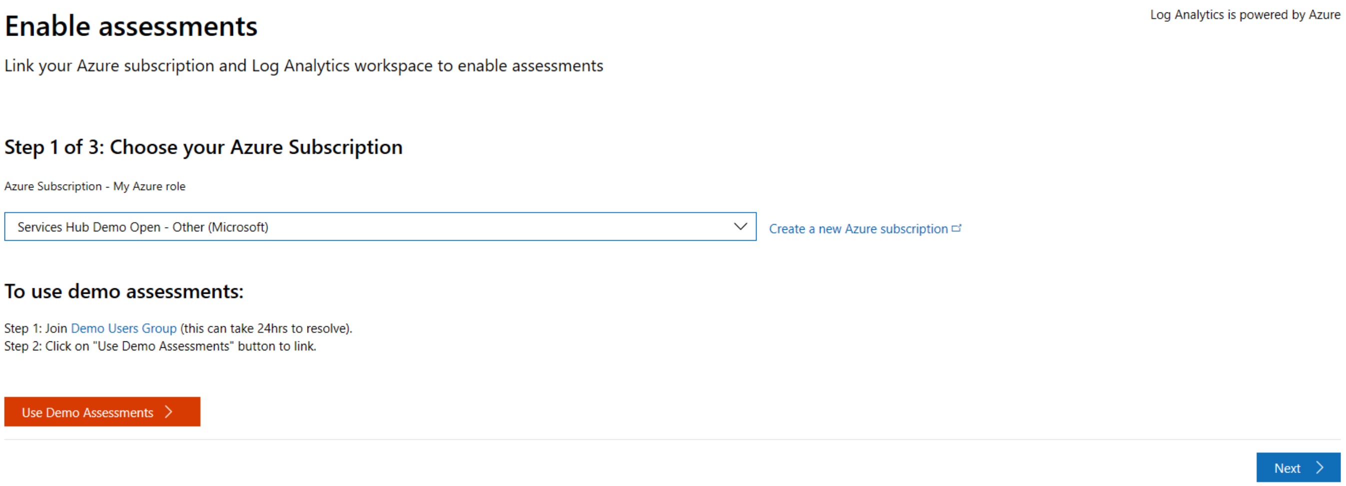

Microsoft Services Hub
Home
Contract
Support
Services
Health
Learning
Search for...
Microsoft Azure
Home > SQL Server Assessment
SQL Server Assessment
Refresh
Analytics
SECURITY AND COMPLIANCE
AVAILABILITY AND BUSINESS CONTINUITY
64%
HIGH PRIORITY RECOMMENDATI...
7
LOW PRIORITY RECOMMENDATIO...
60
PASSED CHECKS
116
99%
HIGH PRIORITY
3
LOW PRIORITY
1
PASSED CHECK
207
PRIORITIZED RECOMMENDATIONS
WEIGHT
Address security patch compliance and ensure securi... 16.1
Disable the SMB1 protocol 9.0
Configure and Enforce the Setting "Windows Firewall... 6.1
Enable and Enforce the Setting "Turn off Autoplay" vi... 5.6
Configure and Enforce the Setting "Windows Firewall... 4.8
Change the recovery model to FULL or BU
Schedule a full database backup and ens
Place data files and transaction log files o
Review the non-default Agent XPs option
Get started with assessments
Watch our assessments video
Active Directory
Active Directory Operational Survey
Active Directory Security
Active Directory Security Survey
Azure Active Directory Operational Survey
Dynamics 365 Customer Engagement Survey
Show all assessments

On-Demand Assessments

Services Hub On-Demand Assessments provide prioritized recommendations, guidance, and suggested actions to help you proactively manage the health of your IT environment.

Available On-Demand Assessments

3. Select the desired Azure subscription from the list and choose next.



Log Analytics is powered by Azure

Enable assessments

Link your Azure subscription and Log Analytics workspace to enable assessments

Step 1 of 3: Choose your Azure Subscription

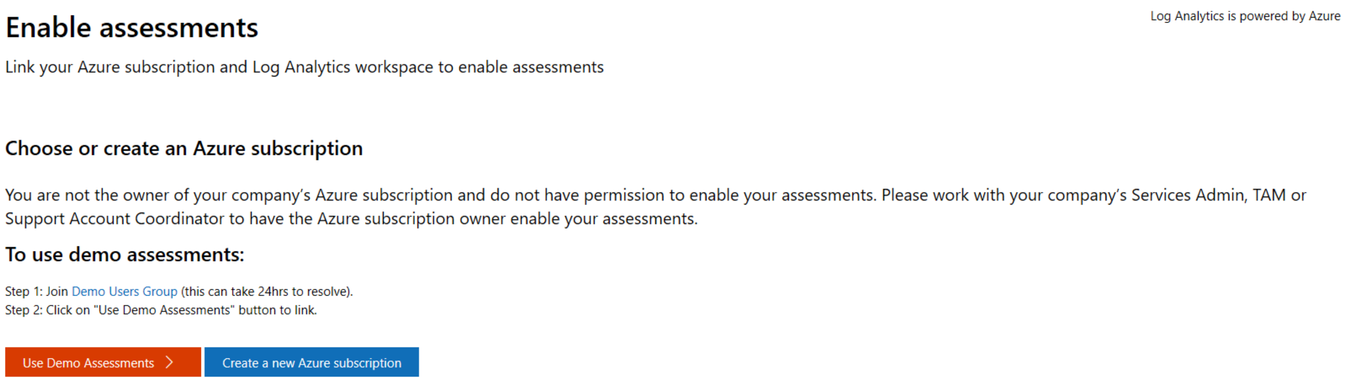
Azure Subscription - My Azure role

Services Hub Demo Open - Other (Microsoft)

To use demo assessments:

Step 1: Join Demo Users Group (this can take 24hrs to resolve).
Step 2: Click on "Use Demo Assessments" button to link.

Organizations that have an Azure subscription but lack the required permissions will see:



Log Analytics is powered by Azure

Enable assessments

Link your Azure subscription and Log Analytics workspace to enable assessments

Choose or create an Azure subscription

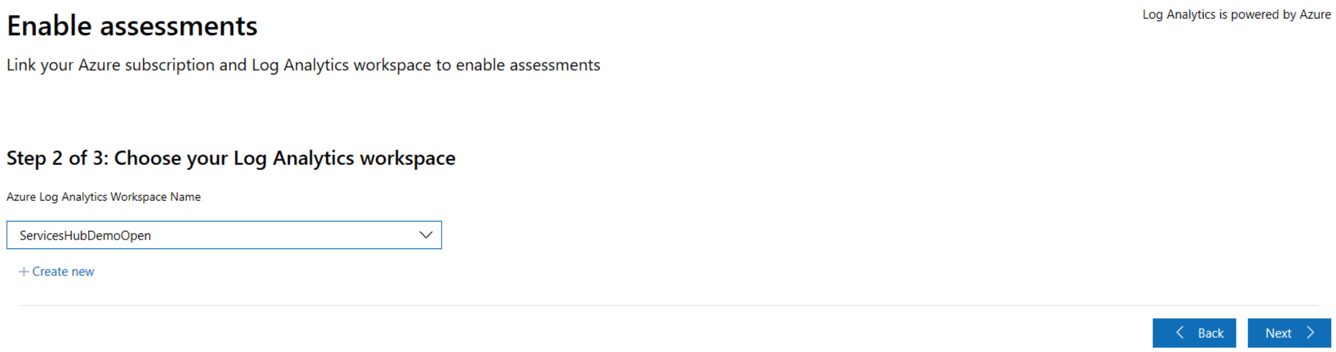
You are not the owner of your company's Azure subscription and do not have permission to enable your assessments. Please work with your company's Services Admin, TAM or Support Account Coordinator to have the Azure subscription owner enable your assessments.

To use demo assessments:

Step 1: Join Demo Users Group (this can take 24hrs to resolve).
Step 2: Click on "Use Demo Assessments" button to link.

Please work with your company's Services Admin, TAM, or Support Account Coordinator to have the customer representative with the required permissions within Azure register on Services Hub and pre-configure your assessments. Organizations without an Azure subscription refer to **Azure Subscription** to get your Microsoft sponsored subscription.

4. Choose the Azure Log Analytics workspace that the assessment(s) you choose will be enabled in. Or use the Create New to create a dedicated workspace for the assessment(s) if desired. Then click next.



Log Analytics is powered by Azure

Enable assessments

Link your Azure subscription and Log Analytics workspace to enable assessments

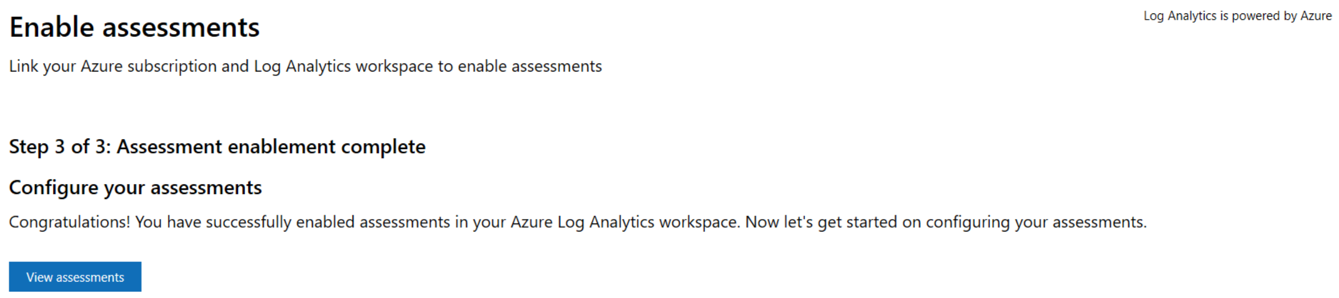
Step 2 of 3: Choose your Log Analytics workspace

Azure Log Analytics Workspace Name

ServicesHubDemoOpen

Note: an Azure Log Analytics workspace may also be created from Azure using the steps documented in this article. [How to Create new Azure Log Analytics Workspace from Azure]

5. At the conclusion of the linking process, click "View assessments".



Log Analytics is powered by Azure

Enable assessments

Link your Azure subscription and Log Analytics workspace to enable assessments

Step 3 of 3: Assessment enablement complete

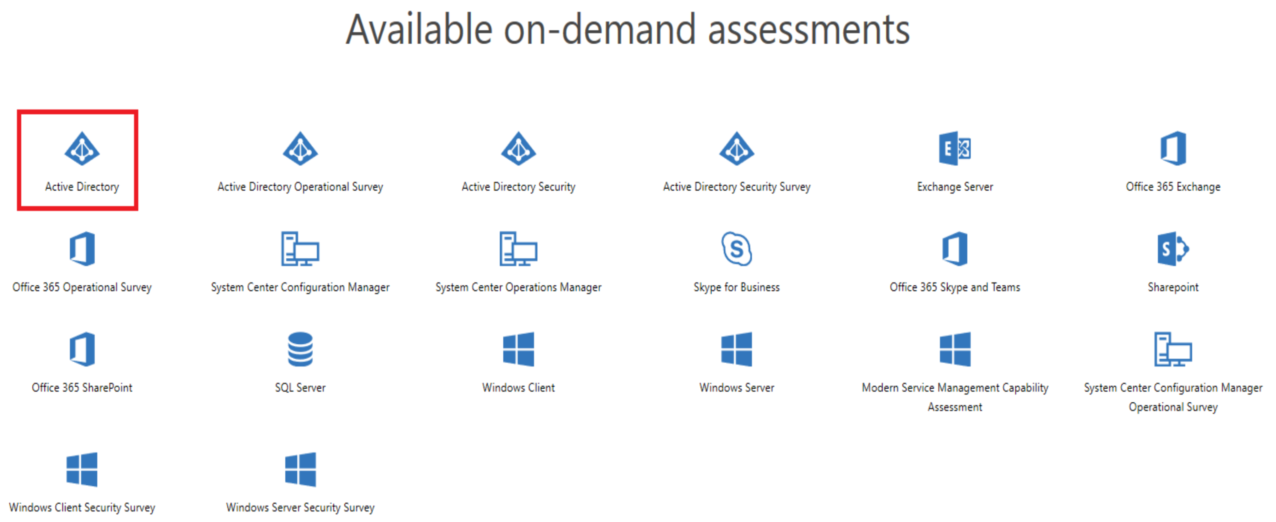
Configure your assessments

Congratulations! You have successfully enabled assessments in your Azure Log Analytics workspace. Now let's get started on configuring your assessments.

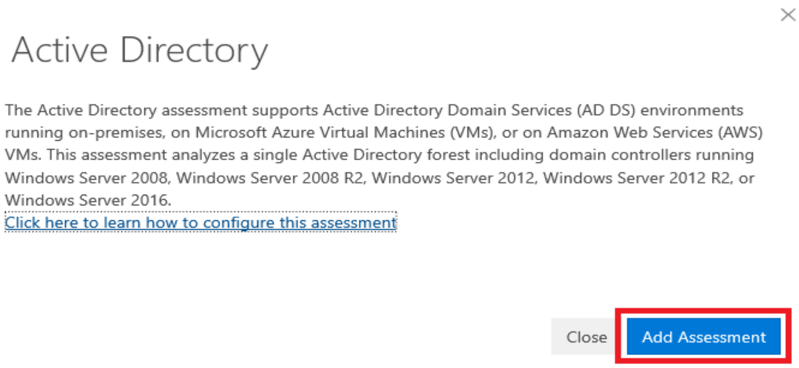
Add the Assessment(s) in Services Hub

To configure an assessment, go to **Services Hub**, **Health**, and **Assessments**. Browse through the assessment catalog and click **Add Assessment** on the assessments that best fit your organization's needs.

Select an assessment of your choice from the list of available assessments and click on Add assessment. For example, Active Directory.



Available on-demand assessments
Active Directory
Active Directory Operational Survey
Active Directory Security
Active Directory Security Survey
Exchange Server
Office 365 Exchange
Office 365 Operational Survey
System Center Configuration Manager
System Center Operations Manager
Skype for Business
Office 365 Skype and Teams
Sharepoint
Office 365 SharePoint
SQL Server
Windows Client
Windows Server
Modern Service Management Capability Assessment
System Center Configuration Manager Operational Survey
Windows Client Security Survey
Windows Server Security Survey



Active Directory

The Active Directory assessment supports Active Directory Domain Services (AD DS) environments running on-premises, on Microsoft Azure Virtual Machines (VMs), or on Amazon Web Services (AWS) VMs. This assessment analyzes a single Active Directory forest including domain controllers running Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016.

Click here to learn how to configure this assessment

The option changes from **Add Assessment** to **View in Azure Log Analytics**. You are now all set for the next steps.

Providing Access to Azure Log Analytics workspace

Granting access to the Log Analytics workspace to Microsoft personnel is necessary for PFE lead deliveries of On-Demand assessments and must be completed by the Azure subscription owner. We recommended you add users as a Log Analytics Reader to grant @microsoft.com users access to your Azure Log Analytics workspace to view your assessments. They will not have access to your Azure subscription.

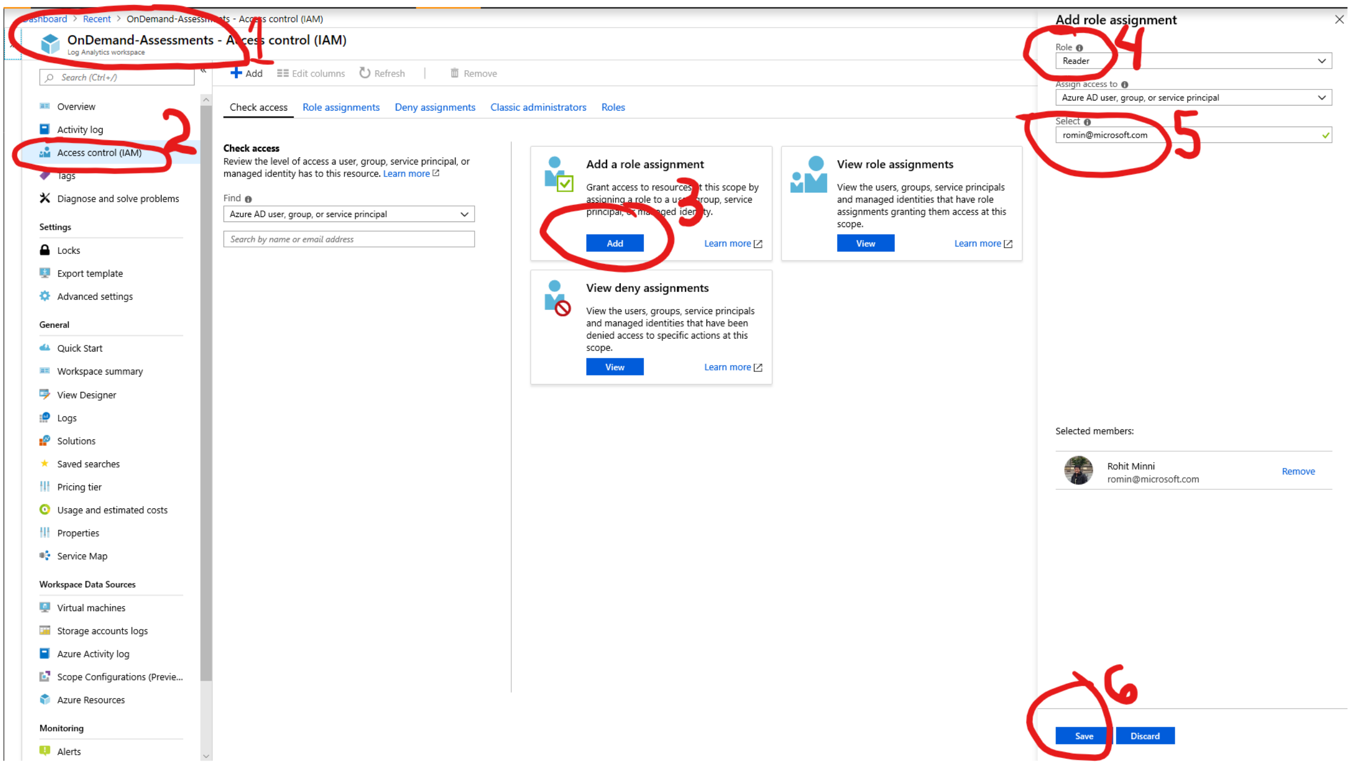
Note: This step is not required for self-consumption of assessments without PFE lead delivery.

Provide access to the Log Analytics workspace by adding an account and granting access as follows:

Azure Portal -> All Resources -> Select the Azure Log analytics workspace linked in Linking of the Azure Subscription and Log Analytics workspace to Services Hub workspace.

Follow the steps indicated in the screenshot to get to the access pane

a. Engineer should be given Log Analytics Reader
b. TAM optionally should be given Log Analytics Reader



Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: Azure AD user, group, or service principal

Search by name or email address

Add a role assignment

Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

View role assignments

View the users, groups, service principals and managed identities that have role assignments granting them access at this scope.

View deny assignments

View the users, groups, service principals and managed identities that have been denied access to specific actions at this scope.

Add role assignment

Role: Reader

Assign access to: Azure AD user, group, or service principal

Select: romin@microsoft.com

Selected members:

Rohit Minni
romin@microsoft.com

##

If the portal doesn't let you invite the email ID you are trying to add, your Azure Active Directory Global Administrator might have blocked Invite Guest Users feature. Please refer to the below article on how to invite guest users [Invite Guest users to your active directory](#)

Establish connectivity to Azure Log Analytics

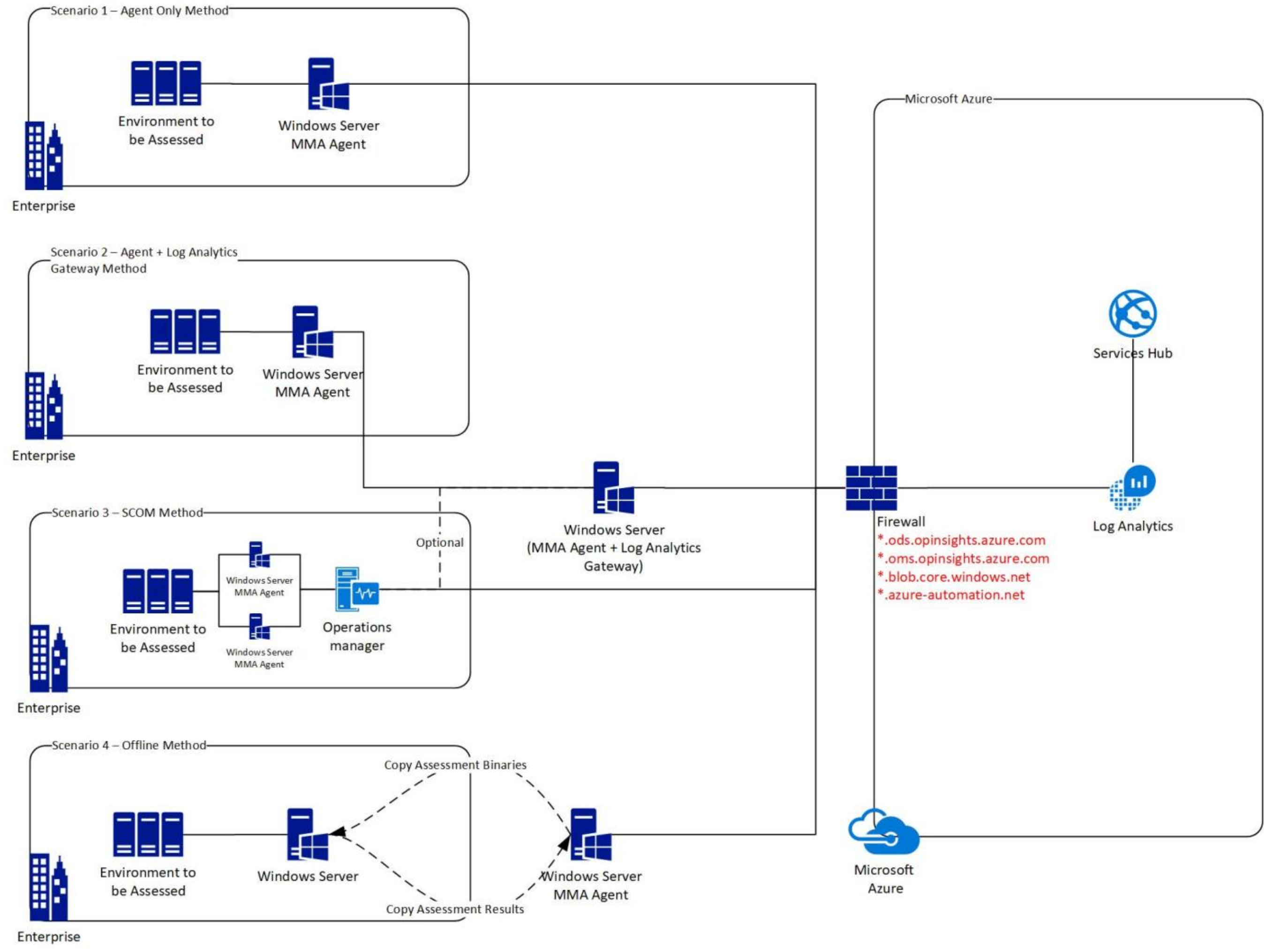
Use the following checklist to ensure all steps in this section are complete.

- ✓ Choose a connectivity option
- ✓ Deploy the connectivity option that fits best for your organization

There are **four scenarios** available to configure the assessment. Determine which scenario fits best for your organization.

- Agent Only Method
- Agent + Log Analytics Gateway Method
- SCOM Method
- Offline – Disconnected environment

The following illustration visually shows the above scenarios:



Agent Only Method

Decision points at a glance:

- When you want to install the Azure Log Analytics agent on the data collection machine, and have it connected to the Internet to upload recommendations and supporting details to your Log Analytics workspace
- Ideal when you only have a single machine in your environment to be dedicated to this setup

This scenario can be used when the data collection machine can contact log analytics directly. It requires one computer that will be designated as the data collection machine which has to be able to access the Internet to upload data to log analytics. This scenario can be used in environments where the Internet connection is not restricted.

Agent + Log Analytics Method

Decision points at a glance:

- When you don't want to expose your data collection machine to the Internet and use a proxy configuration through the Azure Log Analytics gateway

- Ideal when you have 2 separate machines in your environment to be dedicated to this setup

This scenario is the most secure and recommended option to help protect privileged account credentials which are used on the scheduled task configured on the data collection machine needed to run the assessment. This scenario requires two computers. One will be designated as the data collection machine, and the second machine will be the Log Analytics Gateway. In this scenario, the data collection machine has no Internet connection and connects to the Log Analytics Gateway to upload recommendations and supporting data to log analytics. The Log Analytics Gateway must have Internet access.

For information about the Log Analytics Gateway, go to https://go.microsoft.com/fwlink/?linkid=830157.

SCOM Method
Decision points at a glance:

- When you have a SCOM management server configured in your environment and connected to all the targets you wish to assess.

In this configuration SCOM will either act as the gateway itself, or it leverages the Log Analytics Gateway to send data to log analytics.

Offline – Disconnected environment
Decision points at a glance:

- There is zero connection allowed from the assessed environment to the Internet or to any other machine that has Internet access such as the Log Analytics Gateway or proxy.

In this scenario we require two machines

- One is the data collection machine and needs to fulfill prerequisites from the assessment.
- The other is the machine that has Internet access and can upload data to Azure Log Analytics.
    - This machine can be running any supported version of Windows Server or Windows Client that can run the Microsoft Management Agent.

Log Analytics Gateway for Azure Monitor Setup

If the Log Analytics Gateway and data collection machine scenario are chosen, then on the designated Log Analytics gateway machine, you must install and configure both the Log Analytics Gateway and the Microsoft Monitoring Agent.

For detailed information about the Log Analytics gateway including system requirements, network configuration requirements, download, and installation instructions, see the following. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/gateway

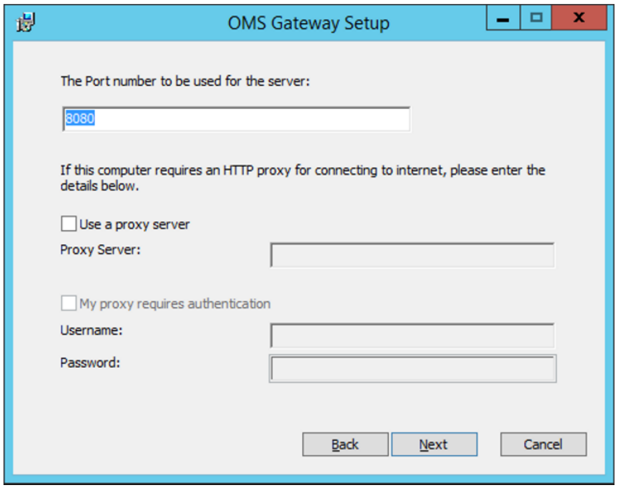
Follow the instructions in the sections below to set up both components.

Note: The Log Analytics Gateway computer does not need to be joined to an Active Directory Domain Service or Azure Active Directory to perform its job of proxying recommendations and supporting details from the data collection computer and Azure Log Analytics.

Download and install the Log Analytics Gateway

On the designated OMS Gateway computer, complete the following:

1. Download the Setup file from https://go.microsoft.com/fwlink/?linkid=837444
2. On the **Welcome** page, click **Next**.
3. On the **License Agreement** page, select **I accept the terms in the License Agreement** to agree to the EULA, and then click **Next**.
4. On the **Port and Proxy Address** page, do the following:
   - Type the TCP port number to be used for the Log Analytics Gateway. Setup opens this port number from Windows firewall. The default value is **8080**.


OMS Gateway Setup

The Port number to be used for the server:

8080

If this computer requires an HTTP proxy for connecting to internet, please enter the details below.

□ Use a proxy server

Proxy Server:

□ My proxy requires authentication

Username:

Password:

   - [**Optional**] If the server on which the Log Analytics Gateway resides needs to go through a proxy, input the proxy address where the Log Analytics Gateway needs to connect. For example, *myorgname.corp.contoso.com:80*. This is an optional value. If it is blank, the Log Analytics Gateway will try to connect to the Internet directly. Otherwise, the Log Analytics Gateway will connect through your internal proxy. If your proxy requires authentication, you can provide a username (domain\user) and password. (**NOTE**: If you do not provide a domain for the user, it will not work).
   - Click **Next**.
5. On the **Destination Folder** page, either retain the default folder location of **%ProgramFiles%\OMS Gateway**, or type the location where you want to install, and then click **Next**.
6. On the **Ready to install** page, select **Install**. A User Account Control dialog box might appear requesting permission to install. If so, click **OK**.
7. After Setup completes, click **Finish**. You can verify that the service is running by opening the **Services.msc** snap-in and checking the status of the service called **OMS Gateway**.

Note. It is required to install the Microsoft Monitoring Agent on the Log Analytics Gateway and configure it with the same log analytics workspace that you will configure on the data collection machine. Follow the instructions in the next section in this document, Microsoft Monitoring Agent Setup

Microsoft Monitoring Agent Setup

The Microsoft Monitoring Agent must be installed and configured on the data collection machine. It must also be installed on the Log Analytics Gateway if deploying that scenario.

For detailed information about the Microsoft Monitoring Agent including system requirements, network firewall configuration requirements, download, and installation instructions, see the following. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

The information below list the proxy and firewall configuration information required for the Linux and Windows agent to communicate with Log Analytics within the Azure commercial cloud. For complete and up to date information on the networking requirements for the MMA as well as networking requirements for Azure Government or other sovereign Azure Log Analytics services, see the following article. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent#network-firewall-requirements

Agent Resource	**Ports**	**Direction**	**Bypass HTTPS inspection**
*.ods.opinsights.azure.com	Port 443	Outbound	Yes
*.oms.opinsights.azure.com	Port 443	Outbound	Yes
*.blob.core.windows.net	Port 443	Outbound	Yes
*.azure-automation.net	Port 443	Outbound	Yes

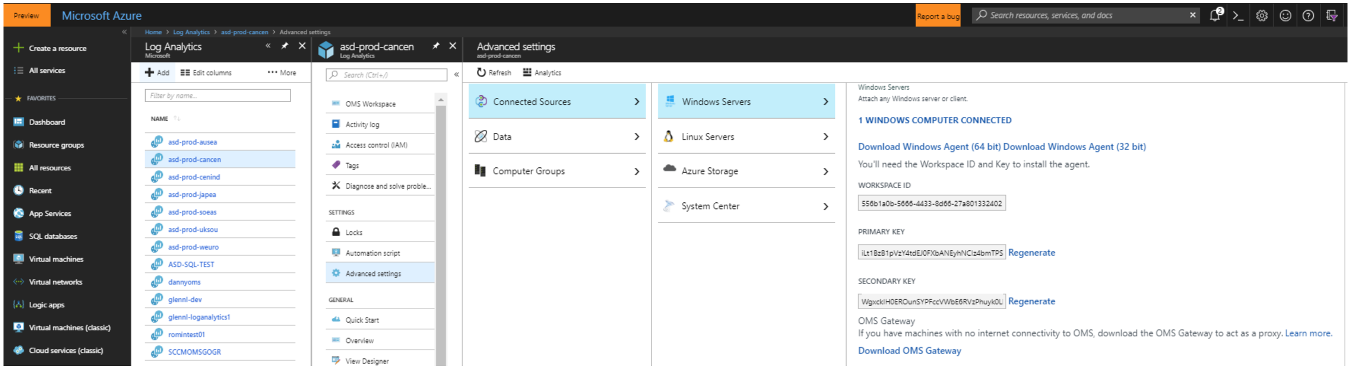
Download and install the Microsoft Monitoring Agent (MMA) setup file from Azure Log Analytics

On the designated data collection machine and Log Analytics Gateway (if using) complete the following steps. If Log Analytics Gateway scenario is being deployed, then install and configure the MMA on the gateway first.

Note. If the collection machine does not have an Internet connection, perform the first 3 steps from an Internet Connected machine.

1. In the Azure portal, go to log analytics, select your workspace and click the **Advanced Settings** Icon.

2. Click **Connected Sources**, and then select **Windows Servers**.



Windows Servers
Attach any Windows server or client.

1 WINDOWS COMPUTER CONNECTED

Download Windows Agent (64 bit) Download Windows Agent (32 bit)
You'll need the Workspace ID and Key to install the agent.

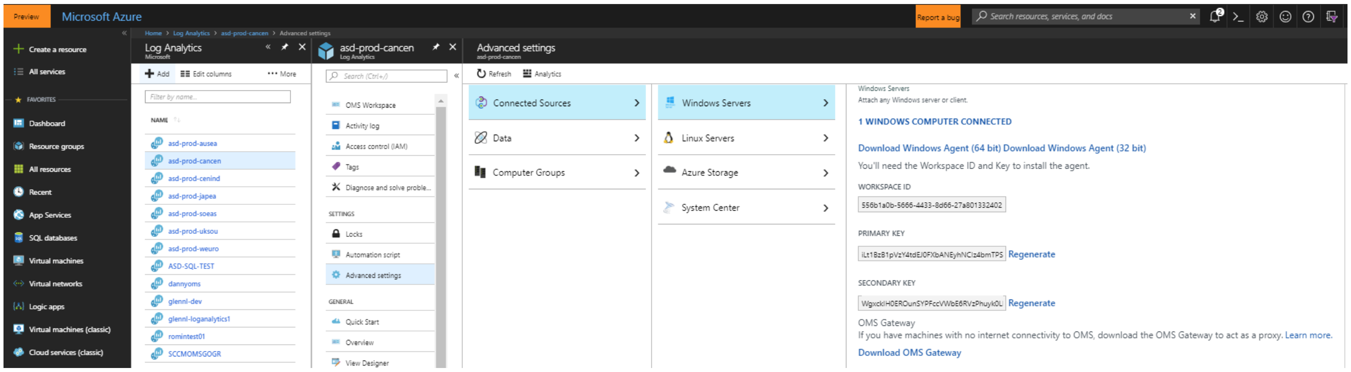
WORKSPACE ID
556b1a0b-5666-4433-8d66-27a801332402

PRIMARY KEY
iLt1BzB1pVzY4tdEJ0FXbANEyhNCIz4bmTPS Regenerate

SECONDARY KEY
WgxckIH0EROunSYPFccVWbE6RVzPhuyk0L Regenerate

OMS Gateway
If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. Learn more.
Download OMS Gateway

3. Click the **Download Windows Agent** link that is applicable to your computer processor type to download the setup file. If the agent is downloaded on another machine, copy the Setup file over to the data collection machine or Log Analytics Gateway server.


Windows Servers
Attach any Windows server or client.

1 WINDOWS COMPUTER CONNECTED

Download Windows Agent (64 bit) Download Windows Agent (32 bit)
You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID
556b1a0b-5666-4433-8d66-27a801332402

PRIMARY KEY
iLt1BzB1pVzY4tdEJ0FXbANEyhNCIz4bmTPS Regenerate

SECONDARY KEY
WgxckIH0EROunSYPFccVWbE6RVzPhuyk0L Regenerate

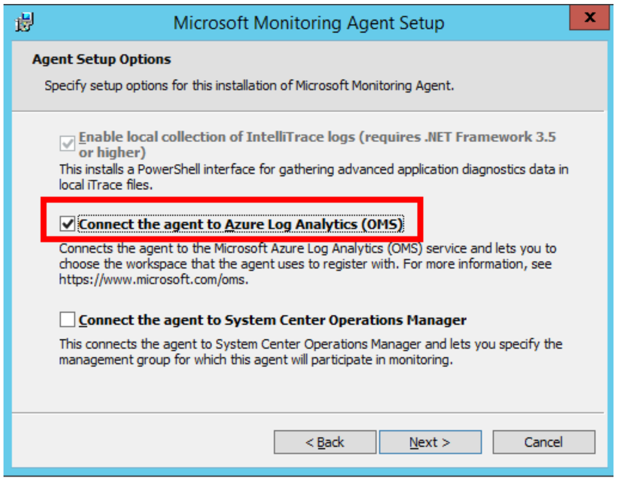
OMS Gateway
If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. Learn more.
Download OMS Gateway

Note. If a monitoring client was installed for System Center Operations Manager (SCOM), the setup only offers to Upgrade the agent, preserving existing settings. The upgrade for SCOM agent does not include any of the configuration steps below.

The next steps apply to installations where no monitoring client was installed for SCOM.
Refer to the Microsoft Monitoring Agent Upgrade section in this document when you are performing an upgrade of the Monitoring Agent for SCOM.

4. Run Setup to install the agent.
5. On the **Welcome** page, click **Next**.

6. On the **License Terms** page, read the license and then click **I Agree**
7. On the **Destination Folder** page, change or keep the default installation folder and then click **Next**.
8. On the **Agent Setup Options** page, choose the **Connect the agent to Azure Log Analytics (OMS)** option. Click **Next**.



Agent Setup Options

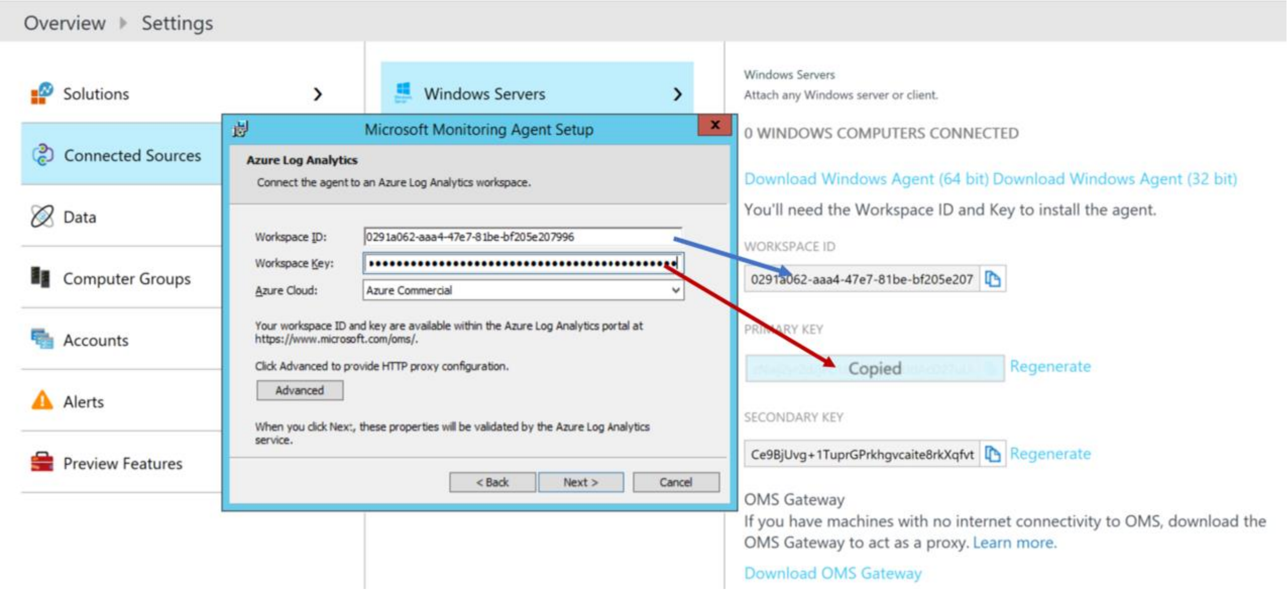
Specify setup options for this installation of Microsoft Monitoring Agent.

☑ Enable local collection of IntelliTrace logs (requires .NET Framework 3.5 or higher)
This installs a PowerShell interface for gathering advanced application diagnostics data in local iTrace files.

☑ Connect the agent to Azure Log Analytics (OMS)
Connects the agent to the Microsoft Azure Log Analytics (OMS) service and lets you to choose the workspace that the agent uses to register with. For more information, see https://www.microsoft.com/oms.

□ Connect the agent to System Center Operations Manager
This connects the agent to System Center Operations Manager and lets you specify the management group for which this agent will participate in monitoring.

9. On the Overview, Settings Dashboard page, click **Connected Sources**, and then copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal. (Hint: Click the copy button then paste in the corresponding **Agent Setup** field).
Select **Azure Commercial** or if you are using an Azure US Government cloud select **Azure US Government** from the **Azure Cloud** drop down menu and click **OK**.
10. If you are currently installing the agent on the data collection machine and using an Log Analytics Gateway deployment scenario, or if your company requires access through a proxy server, click the **Advanced** button to provide **HTTP proxy** configuration. If you do not use any of the above, click **Next** and go to **step 12**.



Azure Log Analytics

Connect the agent to an Azure Log Analytics workspace.

Workspace ID: 0291a062-aaa4-47e7-81be-bf205e207996
Workspace Key: ••
Azure Cloud: Azure Commercial

Your workspace ID and key are available within the Azure Log Analytics portal at https://www.microsoft.com/oms/.

Click Advanced to provide HTTP proxy configuration.

When you click Next:, these properties will be validated by the Azure Log Analytics service.

Windows Servers
Attach any Windows server or client.

0 WINDOWS COMPUTERS CONNECTED

Download Windows Agent (64 bit) Download Windows Agent (32 bit)

You'll need the Workspace ID and Key to install the agent.

WORKSPACE ID
0291a062-aaa4-47e7-81be-bf205e207

PRIMARY KEY
Copied Regenerate

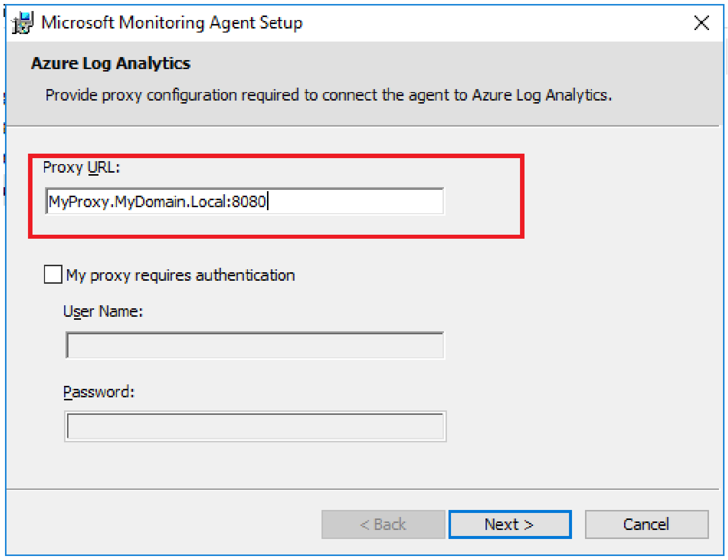
SECONDARY KEY
Ce9BjUvg+1TuprGPrkhgvcaite8rkXqfvt Regenerate

OMS Gateway
If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. Learn more.

Download OMS Gateway

11. Specify the fully qualified domain name (FQDN) or the IP address and port of the Log Analytics Gateway.

If you use a proxy server instead of an Log Analytics Gateway, add the information for your proxy server and if required, authentication credentials (not required for the Log Analytics Gateway), then click **Next** twice.



Microsoft Monitoring Agent Setup

Azure Log Analytics

Provide proxy configuration required to connect the agent to Azure Log Analytics.

Proxy URL:

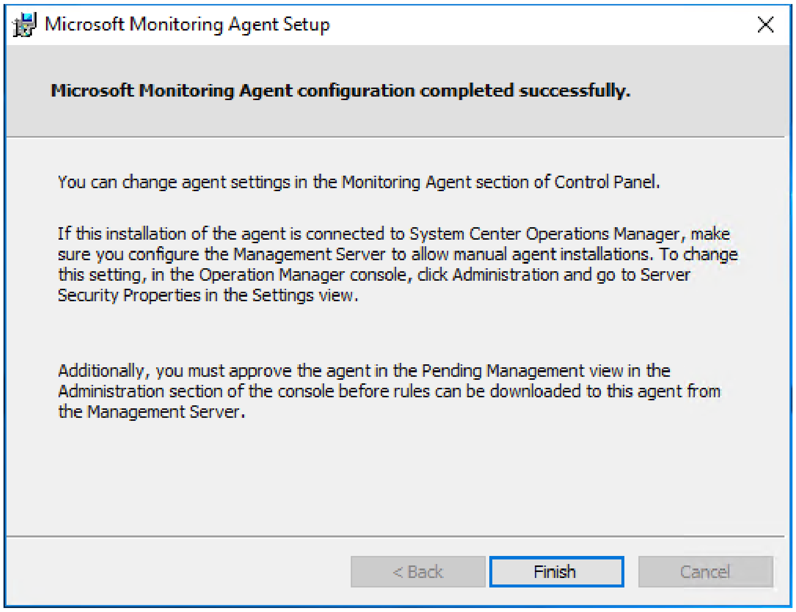
MyProxy.MyDomain.Local:8080

□ My proxy requires authentication

User Name:

Password:

12. On the **Microsoft Update** page, optionally select **Use Microsoft Update when I check for updates (recommended)**, then click **Next**.
13. On the **Ready to Install** page, review your choices, and then click **Install**.
14. On the **Microsoft Monitoring Agent configuration completed successfully** page, click **Finish**.



Microsoft Monitoring Agent Setup

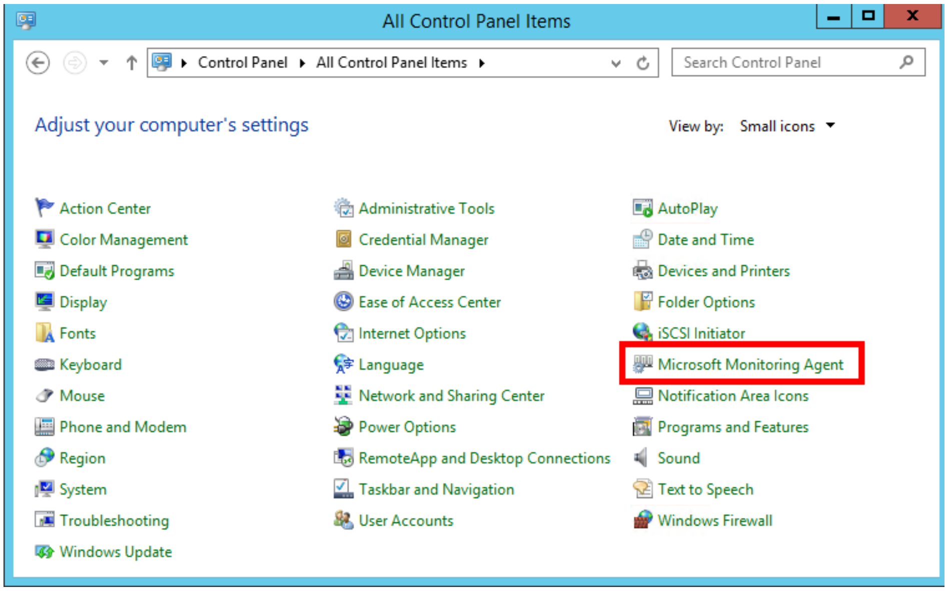
Microsoft Monitoring Agent configuration completed successfully.

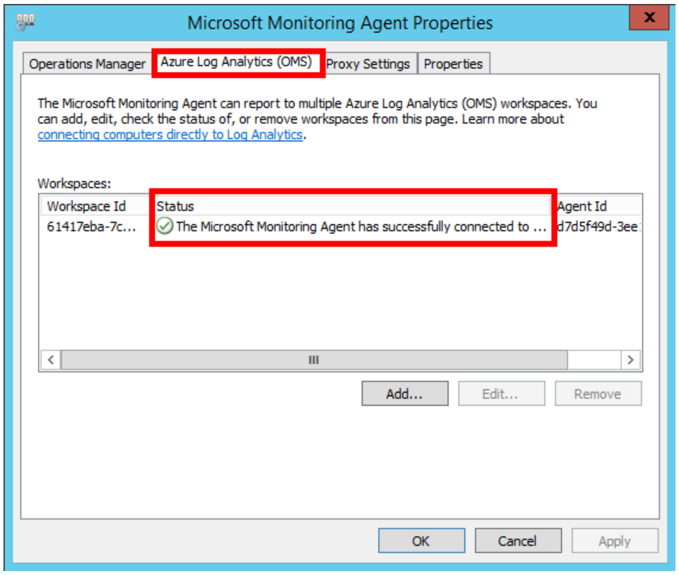
You can change agent settings in the Monitoring Agent section of Control Panel.

If this installation of the agent is connected to System Center Operations Manager, make sure you configure the Management Server to allow manual agent installations. To change this setting, in the Operation Manager console, click Administration and go to Server Security Properties in the Settings view.

Additionally, you must approve the agent in the Pending Management view in the Administration section of the console before rules can be downloaded to this agent from the Management Server.

15. When complete, the **Microsoft Monitoring Agent** appears in **Control Panel**. You can review your configuration there and verify that the agent is connected to Azure Log Analytics. When connected to Log Analytics, the agent displays a message stating: **The Microsoft Monitoring Agent has successfully connected to the log analytics service**.





The Microsoft Monitoring Agent can report to multiple Azure Log Analytics (OMS) workspaces. You can add, edit, check the status of, or remove workspaces from this page. Learn more about connecting computers directly to Log Analytics.

Workspaces:

Workspace Id	Status	Agent Id
61417eba-7c...	✓ The Microsoft Monitoring Agent has successfully connected to ...	d7d5f49d-3ee

Note. If you have been installing the Microsoft Monitoring Agent on the Log Analytics Gateway, you need to repeat the installation steps above on the data collection machine.

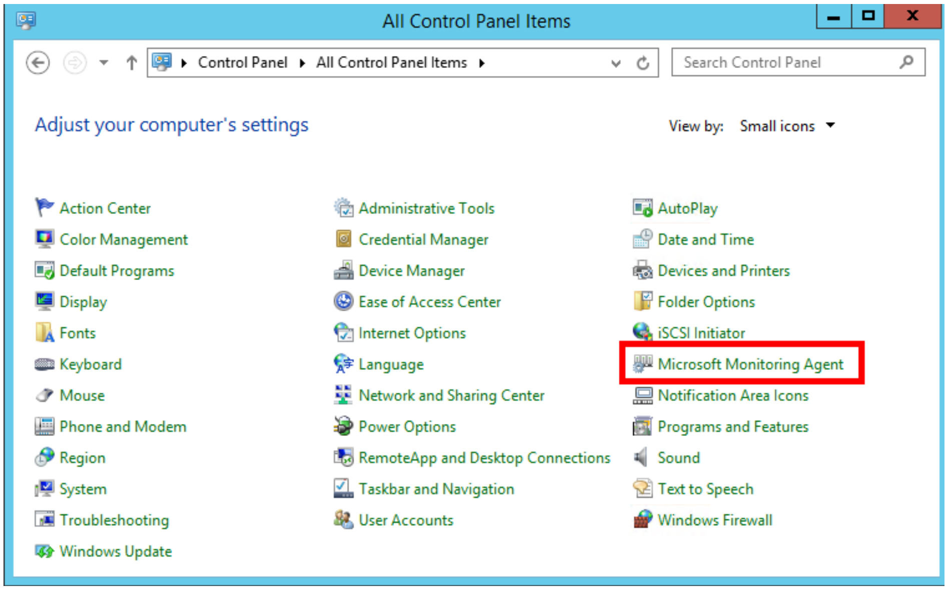
After setting up the data collection machine, continue with the setup of the assessment as outlined in the Configure Microsoft On-Demand Assessments(s) section of this article.

Microsoft Monitoring Agent Upgrade

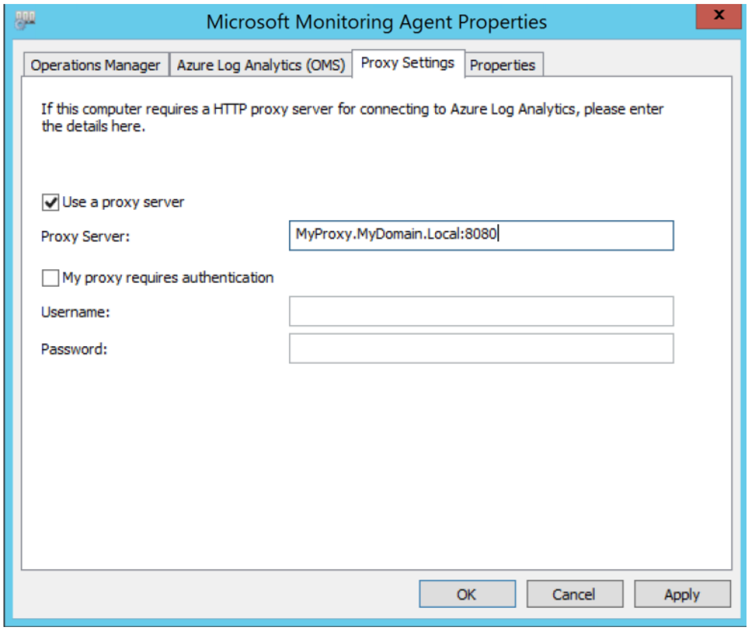
If a monitoring agent is already installed, the Microsoft Monitoring Agent setup will only display the upgrade option. The upgrade will keep the existing configuration and adds a new option to configure a Log Analytics workspace.

Follow the steps below to perform an upgrade and configure the agent for the log analytics Workspace.

1. Run Setup to install the agent.
2. On the **Welcome** page, click **Next**.
3. On the **License Terms** page, read the license and then click **I Agree**
4. On the **begin Upgrade** page, click **Upgrade**.
5. On the **Completion** page, click **Finish.**
6. Once the agent installation completed, go to the **Control Panel.**



7. Click **Microsoft Monitoring Agent**
8. If the Log Analytics Gateway scenario is chosen or a Proxy server is in place go to the **Proxy Settings** tab When this scenario is not used go to step 9.


Microsoft Monitoring Agent Properties
Operations Manager
Azure Log Analytics (OMS)
Proxy Settings
Properties
OK
Cancel
Apply

If this computer requires a HTTP proxy server for connecting to Azure Log Analytics, please enter the details here.

☑ Use a proxy server

Proxy Server: MyProxy.MyDomain.Local:8080

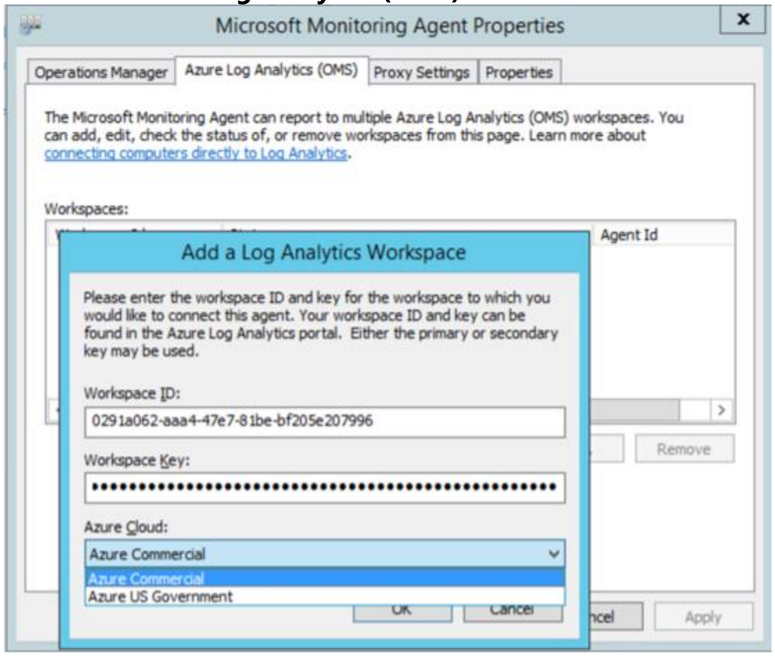
□ My proxy requires authentication

Username:

Password:

Select **Use a proxy server** and specify the fully qualified domain name (FQDN) or the IP address and port of the Log Analytics Gateway.
If you use a proxy server instead of an Log Analytics Gateway, add the information for your proxy server and if required, authentication credentials (not required for the Log Analytics Gateway), then Select **Apply**

9. Select the **Azure Log Analytics (OMS)** tab and click **Add…**


Microsoft Monitoring Agent Properties
Operations Manager
Azure Log Analytics (OMS)
Proxy Settings
Properties
Workspaces:
Agent Id
Remove
ncel
Apply
Add a Log Analytics Workspace
OK
Cancel

The Microsoft Monitoring Agent can report to multiple Azure Log Analytics (OMS) workspaces. You can add, edit, check the status of, or remove workspaces from this page. Learn more about connecting computers directly to Log Analytics.

Please enter the workspace ID and key for the workspace to which you would like to connect this agent. Your workspace ID and key can be found in the Azure Log Analytics portal. Either the primary or secondary key may be used.

Workspace ID: 0291a062-aaa4-47e7-81be-bf205e207996

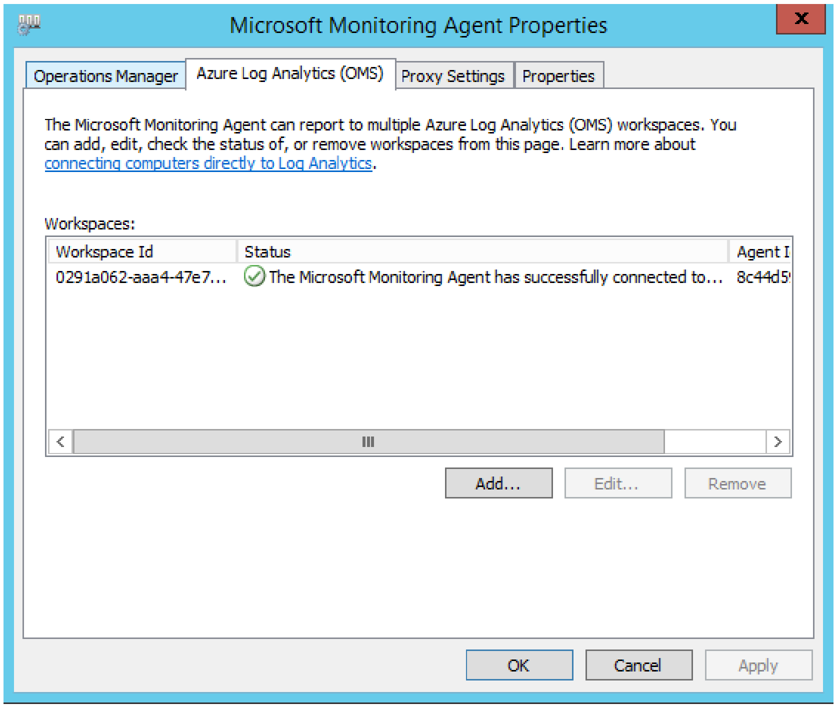
Workspace Key: ••

Azure Cloud: Azure Commercial

Azure Commercial
Azure US Government

10. Copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal. (Hint: Click the copy button then paste in the corresponding **Agent Setup** field). Select **Azure Commercial** or, if you are using an Azure US Government cloud select **Azure US Government** from the **Azure Cloud** drop down menu and click **OK**.

11. An exclamation mark will be visible in the Workspaces pane. Click **Apply**. This will stop and start the agent, and the Workspaces pane should look like the following example after a few seconds.



Microsoft Monitoring Agent Properties
Operations Manager
Azure Log Analytics (OMS)
Proxy Settings
Properties

The Microsoft Monitoring Agent can report to multiple Azure Log Analytics (OMS) workspaces. You can add, edit, check the status of, or remove workspaces from this page. Learn more about connecting computers directly to Log Analytics.

Workspaces:

Workspace Id	Status	Agent I
0291a062-aaa4-47e7...	✓ The Microsoft Monitoring Agent has successfully connected to...	8c44d5

12. Click **OK** to finish the Microsoft Monitoring Agent upgrade for log analytics.

After setting up the data collection machine, continue with the setup of the assessment as outlined in the Configure Microsoft Unified Support Solutions section of this document.

Setup and configure Log Analytics using SCOM

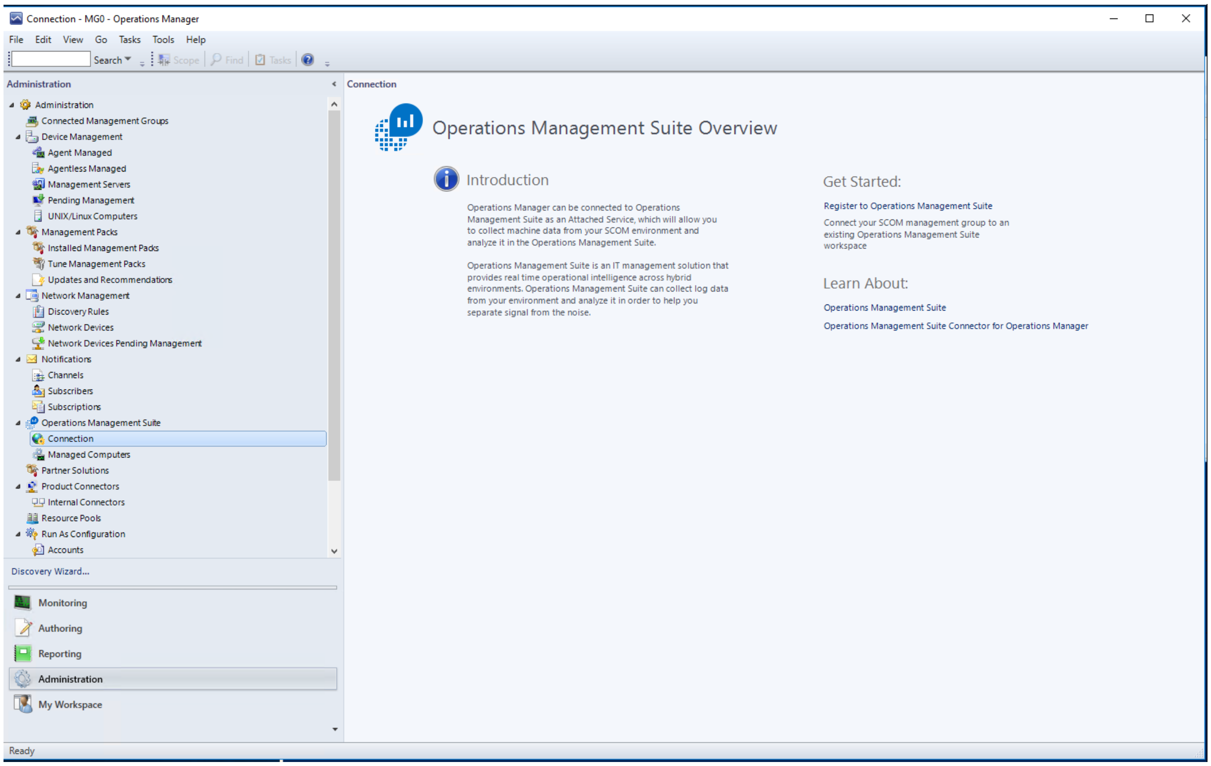
If SCOM is already in use and you want to use SCOM and the already installed agents, follow the steps in this section. In this configuration SCOM will either act as the gateway or it leverages the OMS Gateway itself to send data to log analytics.

Pre-requisites

The SCOM 2012 SP1 UR6 (UR7 for proxy/gateway support) or SCOM 2012 R2 UR2 (UR3 for proxy/gateway support) agent is the minimum version required to fully support log analytics functionality.

If you are using multi homing of log analytics workspaces, we would suggest that you not use the agent that comes with SCOM but use the Microsoft Monitoring Agent from Microsoft Update/log analytics workspace instead. The current Microsoft Monitoring Agent version is backwards compatible and supported with all SCOM
2012 R2/2016 management groups.

1. On the SCOM Administration Console go to **Administration** -> **Operations Management Suite** -> **Connection**



Operations Management Suite Overview

Introduction

Operations Manager can be connected to Operations Management Suite as an Attached Service, which will allow you to collect machine data from your SCOM environment and analyze it in the Operations Management Suite.

Operations Management Suite is an IT management solution that provides real time operational intelligence across hybrid environments. Operations Management Suite can collect log data from your environment and analyze it in order to help you separate signal from the noise.

Get Started:

Register to Operations Management Suite

Connect your SCOM management group to an existing Operations Management Suite workspace

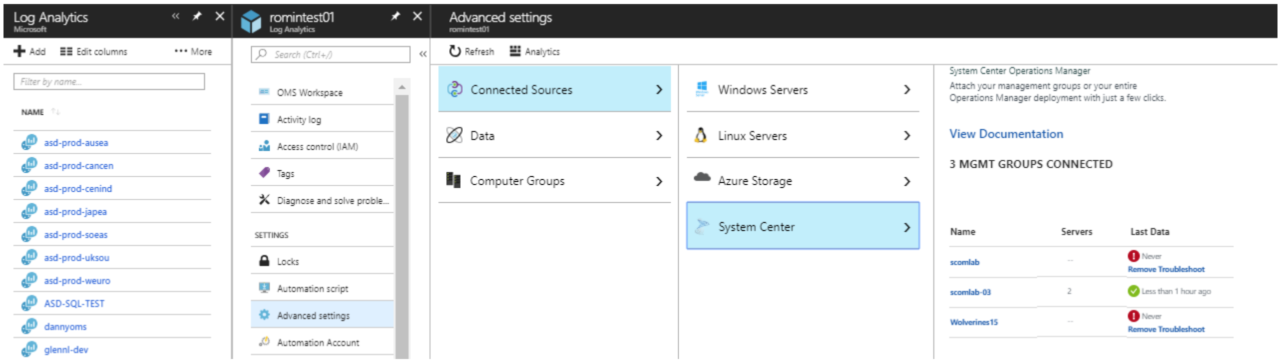
Learn About:

Operations Management Suite

Operations Management Suite Connector for Operations Manager

2. Click on **Register to Operations Management Suite**
   A login window will appear. Log in with an account that has administrative rights to connect to the log analytics workspace. Select the proper workspace (if there is more than one) and click **Next**. In the **Confirm the settings** window click on **Create.**

3. Go to the log analytics workspace.



System Center Operations Manager

Attach your management groups or your entire Operations Manager deployment with just a few clicks.

View Documentation

3 MGMT GROUPS CONNECTED

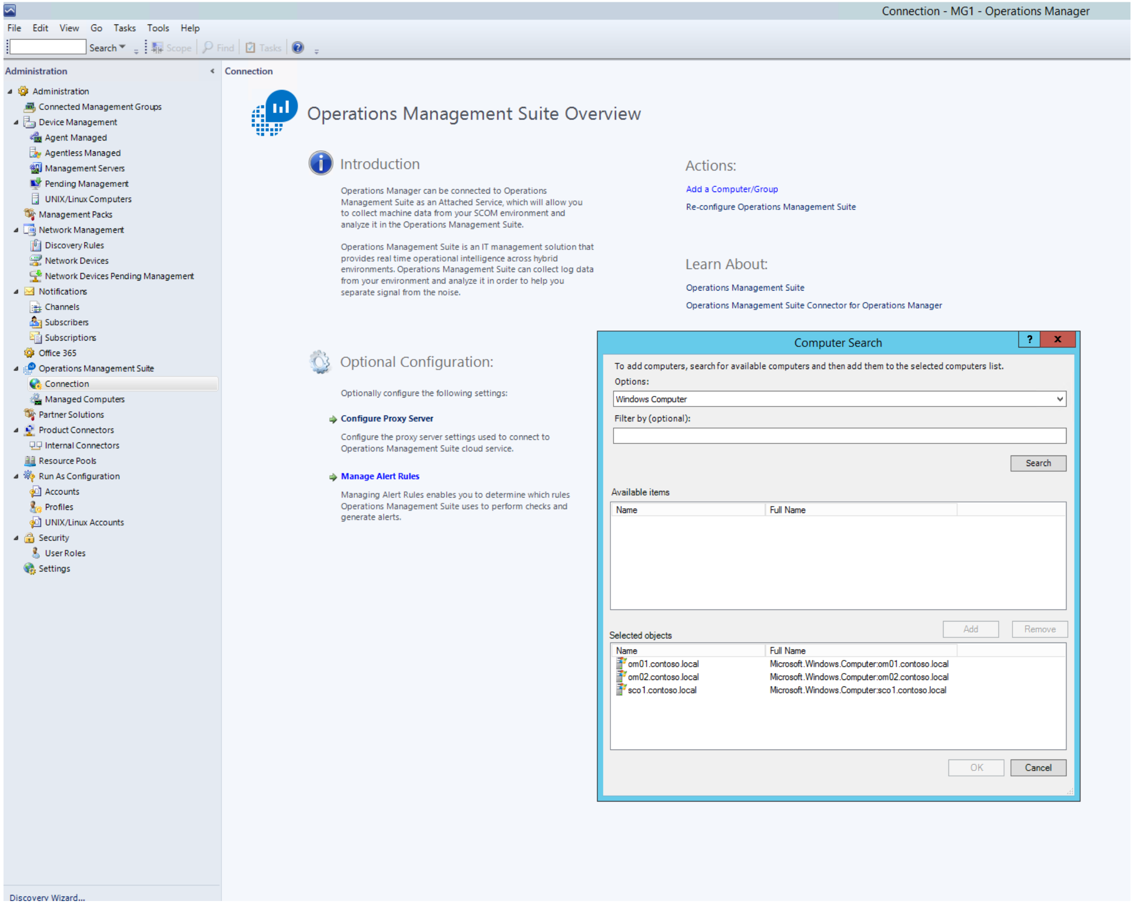
Name	Servers	Last Data
scomlab	--	Never Remove Troubleshoot
scomlab-03	2	Less than 1 hour ago
Wolverines15	--	Never Remove Troubleshoot

4. From the log analytics workspace, to confirm that the Management Group is connected, go to **Advanced Settings** -> **Connected Sources** -> **System Center**:

Back in the SCOM Administration Console you need to opt-in the agents for log analytics/OMS:

1. Go to **Administration -> Operations Management Suite -> Connection**

2. In the right pane, click on **Add a Computer/Group** below **Actions**:



Operations Management Suite Overview

Introduction

Operations Manager can be connected to Operations Management Suite as an Attached Service, which will allow you to collect machine data from your SCOM environment and analyze it in the Operations Management Suite.

Operations Management Suite is an IT management solution that provides real time operational intelligence across hybrid environments. Operations Management Suite can collect log data from your environment and analyze it in order to help you separate signal from the noise.

Actions:

Add a Computer/Group

Re-configure Operations Management Suite

Learn About:

Operations Management Suite

Operations Management Suite Connector for Operations Manager

Optional Configuration:

Optionally configure the following settings:

Configure Proxy Server

Configure the proxy server settings used to connect to Operations Management Suite cloud service.

Manage Alert Rules

Managing Alert Rules enables you to determine which rules Operations Management Suite uses to perform checks and generate alerts.

Computer Search

To add computers, search for available computers and then add them to the selected computers list.

Options: Windows Computer

Filter by (optional):

Available items

Name	Full Name

Selected objects

Name	Full Name
om01.contoso.local	Microsoft.Windows.Computer:om01.contoso.local
om02.contoso.local	Microsoft.Windows.Computer:om02.contoso.local
sco1.contoso.local	Microsoft.Windows.Computer:sco1.contoso.local

3. Select the **object type** (**Windows Computer** or **Groups**) and optionally leave the **Filter** field empty to return all objects of the type selected

Collected data from any agent that is running the scheduled task is sent back to the SCOM Management Server which in turn will upload to the log analytics/OMS Workspace

Note: the SCOM Management Group might connect directly to the log analytics service or through the OMS Gateway. The OMS Gateway in the picture above is used for certain solutions that cannot leverage SCOM.

Reference: https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-om-agents

After setting up the data collection machine, continue with the setup of the assessment as outlined in the Configure Microsoft On-Demand Assessments(s) section of this article.

Offline – Disconnected Environment

Data Collection has no Internet access and not possible to use OMS Gateway

This scenario can be used to assessment a completely disconnected environment. I.e., there is zero network connectivity from the assessed environment to the Internet or to any other machine that has Internet access. This scenario requires additional configuration and steps that are outlined below.

Requirements: In this scenario we require two machines

- One is the data collection machine and needs to fulfill prerequisites from the assessment.
- The other is the machine that has Internet access and can upload data to Azure Log Analytics.
  - This machine can be running any supported version of Windows Server or Windows Client that support the Microsoft Monitoring Agent.

To successfully execute On-Demand assessments via this method, an offline secure file copy process is necessary to transfer files to and from the Internet connected machine and the environment being assessed.

Internet Access Machine

After the agent installation and setup of the assessment are completed, follow the next steps on the machine that has Internet access.

- Open Task Manager
- Open scheduled tasks and drill down to the assessment task
- Set the scheduled task to start manually, removing the weekly schedule.
- Start the scheduled task, this will download the assessment executable and the assessment package.
  - Go to the Working Directory that was entered in the assessment setup. <Working Directory>\XXAssessment Where XX is different for each assessment.
  - A numbered folder will appear. As soon as you see this folder, stop the OMSAssessment.exe process in Task Manager.
- Copy the folder "OMSAssessment" folder that is created in "<working directory>\XXAssessment" to a USB drive or other method of your choice to copy content to the data collection machine
- Go to: C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State\Resources
  1. Search for execpkg
  2. Find the assessment package for the technology you need, open the file location and copy that Execpkg file to the same location as where you stored the "OMSAssessment" folder.

This concludes the actions on the machine with Internet access until we want to upload data.

Data Collection Machine

Create a folder on the local drive that has enough free disk space to store all collected data, up to 10GB.

For instance: C:\MicrosoftAssessment

Create a directory for collection of data.

For instance:

- C:\MicrosoftAssessment\Collect

Copy the Execpkg file and OMSAssessment folder to the C:\MicrosoftAssessment folder.

- Open an elevated CMD Prompt, go to C:\MicrosoftAssessment\OMSAssessment and run the following command:

- OmsAssessment.exe -execPackage C:\MicrosoftAssessment\ADAssessmentPlus.execpkg" -w " C:\MicrosoftAssessment\Collect" -trace Off -headers False -assessmentname "ADAssessment" -discoverysettings "AD" -computername "<DataCollectionMachine>" -target ToolsMachine -op "<Location for the Recommendation files>"

Data collection starts and generate few files named:

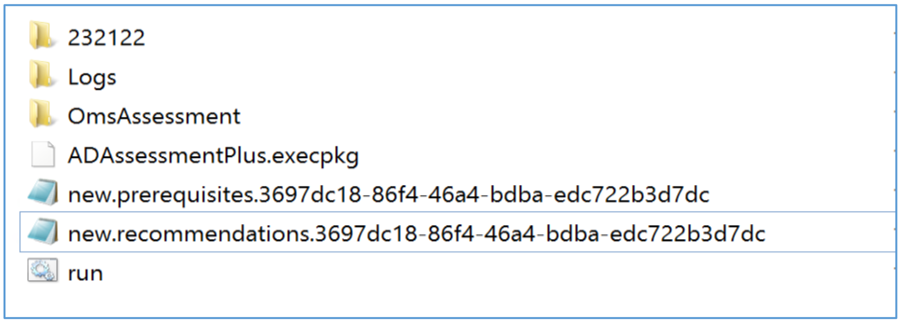
new.prerequisite<assessmentguid>.assessmentrecs

new.recommendations.<assessment guid>.assessmentrecs

When the assessment is finished, the command prompt is back at the input prompt and you should not see anything running.

Copy the files that are named new.* over to the machine with Internet access

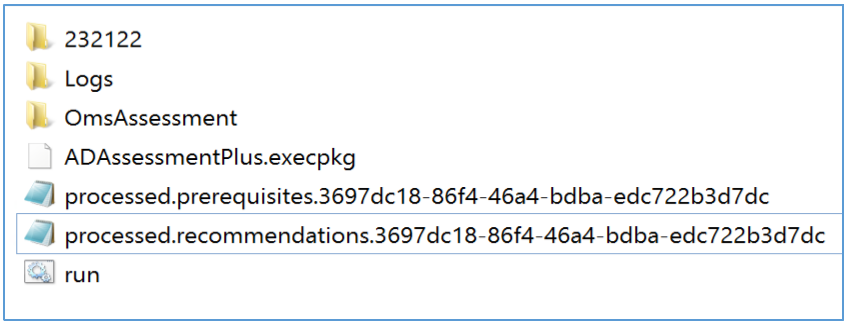
Copy the new.* files in the "<working directory>\XXAssessment"



232122
Logs
OmsAssessment
ADAssessmentPlus.execpkg
new.prerequisites.3697dc18-86f4-46a4-bdba-edc722b3d7dc
new.recommendations.3697dc18-86f4-46a4-bdba-edc722b3d7dc
run

To immediately upload the files: restart the "Microsoft Monitoring Agent" service

If not, the files will be found during the next cycle, within an hour. When they are processed and uploaded to Azure Log Analytics, the name changes from new to processed.



232122
Logs
OmsAssessment
ADAssessmentPlus.execpkg
processed.prerequisites.3697dc18-86f4-46a4-bdba-edc722b3d7dc
processed.recommendations.3697dc18-86f4-46a4-bdba-edc722b3d7dc
run

Review data afterwards on the portal, it may take up to one hours after the data is submitted to show up.

Configure Microsoft On-Demand Assessment(s)

Use the following checklist to ensure all steps in this section are complete.

- ✓ Configure required group policy settings
- ✓ Verify solution is downloaded on the data collection machine

- ✓ Verify environment to be assessment the account running the assessment
- ✓ Create assessment scheduled task

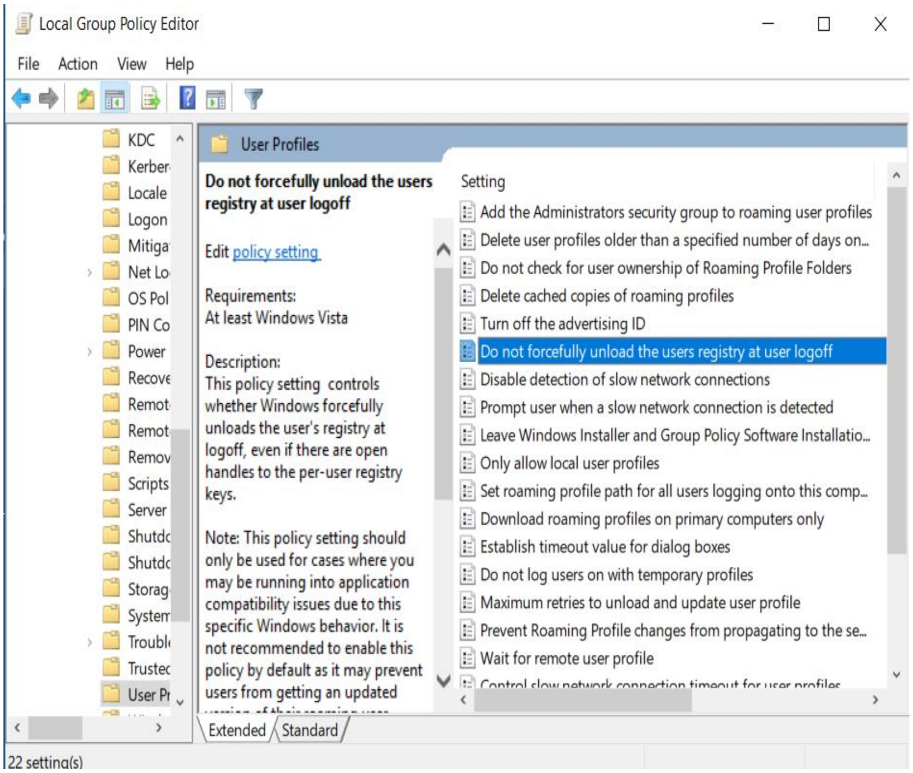
Configuring the required Group Policy Objects

Successful execution of assessment scheduled tasks requires some policy configuration on the data collection machine to mitigate issues/risks known to degrade the successful collection of assessment data from your environment. The following configurations are applicable to all assessments.

Note: there may be policy configuration unique to specific assessments documented in the respective assessment prerequisite documentation.

Start -> Run -> gpedit.msc-> Computer Configuration -> Administrative Template ->

system -> user profile ->Do not forcefully unload the users registry at user logoff -> Click Enable



Do not forcefully unload the users registry at user logoff

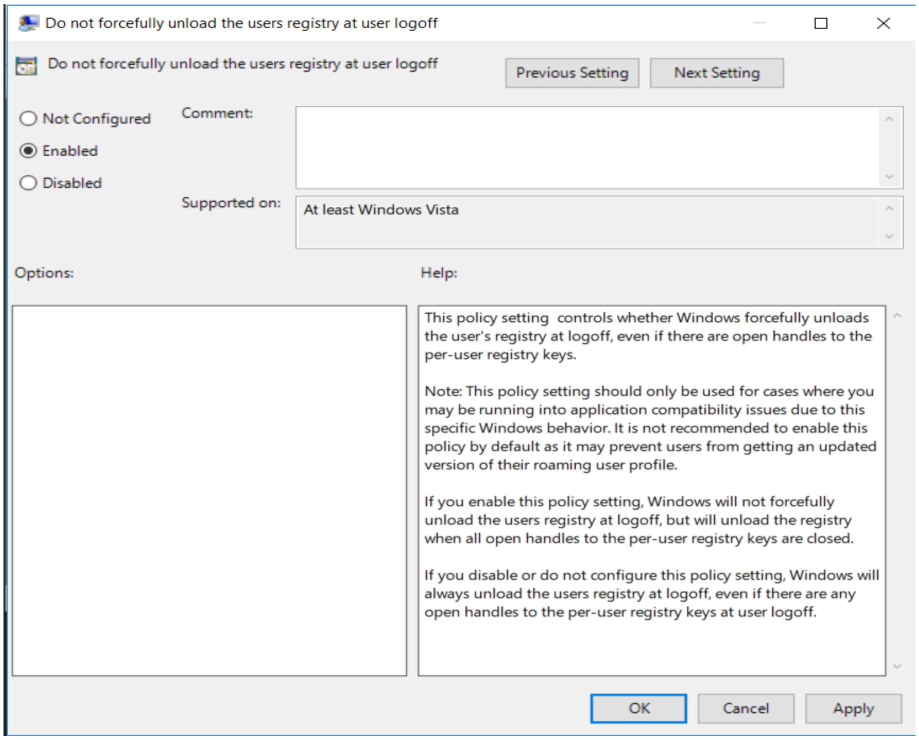
Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting controls whether Windows forcefully unloads the user's registry at logoff, even if there are open handles to the per-user registry keys.

Note: This policy setting should only be used for cases where you may be running into application compatibility issues due to this specific Windows behavior. It is not recommended to enable this policy by default as it may prevent users from getting an updated

Setting
- Add the Administrators security group to roaming user profiles
- Delete user profiles older than a specified number of days on...
- Do not check for user ownership of Roaming Profile Folders
- Delete cached copies of roaming profiles
- Turn off the advertising ID
- Do not forcefully unload the users registry at user logoff
- Disable detection of slow network connections
- Prompt user when a slow network connection is detected
- Leave Windows Installer and Group Policy Software Installatio...
- Only allow local user profiles
- Set roaming profile path for all users logging onto this comp...
- Download roaming profiles on primary computers only
- Establish timeout value for dialog boxes
- Do not log users on with temporary profiles
- Maximum retries to unload and update user profile
- Prevent Roaming Profile changes from propagating to the se...
- Wait for remote user profile
- Control slow network connection timeout for user profiles



Do not forcefully unload the users registry at user logoff

Do not forcefully unload the users registry at user logoff

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

This policy setting controls whether Windows forcefully unloads the user's registry at logoff, even if there are open handles to the per-user registry keys.

Note: This policy setting should only be used for cases where you may be running into application compatibility issues due to this specific Windows behavior. It is not recommended to enable this policy by default as it may prevent users from getting an updated version of their roaming user profile.

If you enable this policy setting, Windows will not forcefully unload the users registry at logoff, but will unload the registry when all open handles to the per-user registry keys are closed.

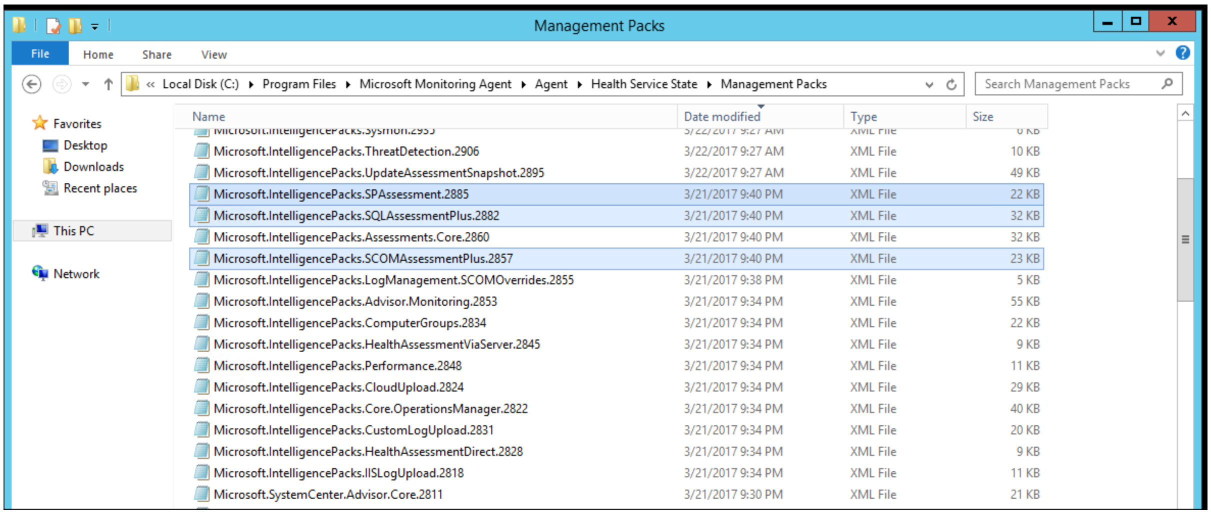
If you disable or do not configure this policy setting, Windows will always unload the users registry at logoff, even if there are any open handles to the per-user registry keys at user logoff.

Verify the solution is downloaded on the data collection machine.

Every agent opted-in will receive Management Packs (MPs) from the Log Analytics workspace. The MPs will depend on which assessments are added. For the Microsoft On-Demand assessments, the MPs are named:

Microsoft.IntelligencePacks.<technology>.Assessment

The Microsoft On-Demand assessments MPs will be downloaded as soon as the solution is added to the Log Analytics workspace. The MPs are downloaded into the Management Pack folder of the agent (this is true regardless of the setup – direct, through GW, or through SCOM):

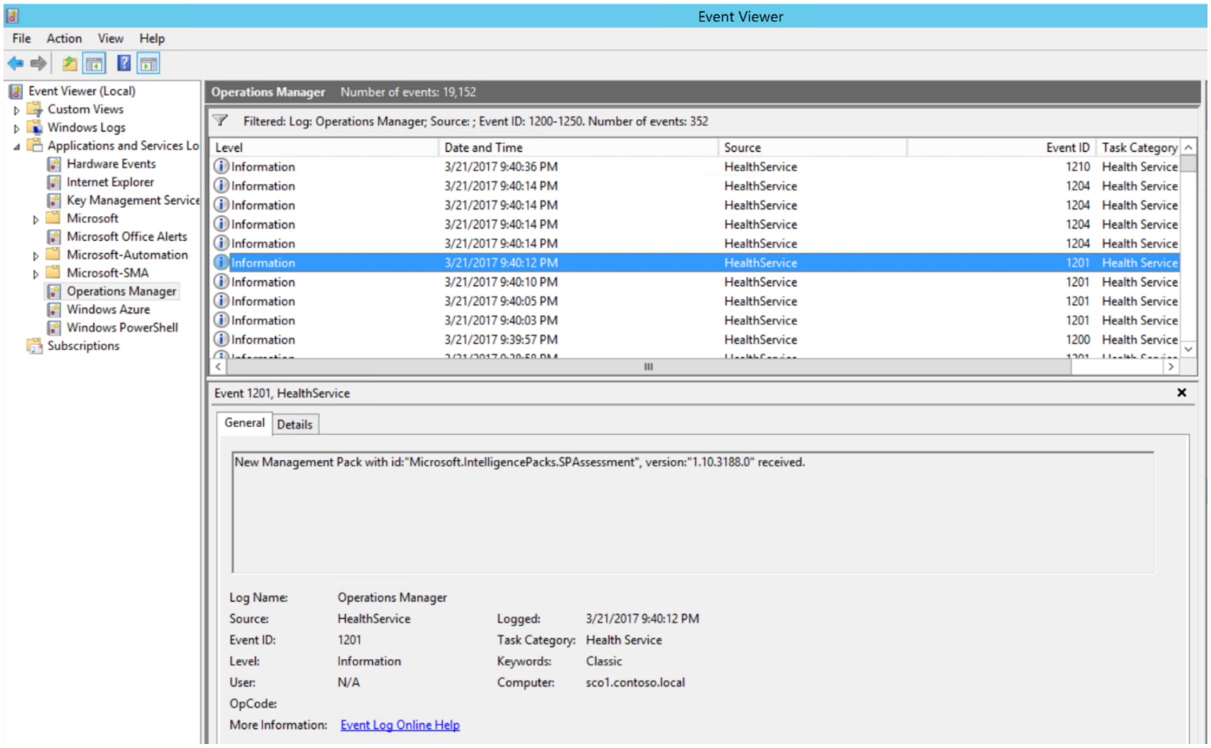


Management Packs

« Local Disk (C:) ▸ Program Files ▸ Microsoft Monitoring Agent ▸ Agent ▸ Health Service State ▸ Management Packs

Name	Date modified	Type	Size
Microsoft.IntelligencePacks.Sysmon.2935	3/22/2017 9:27 AM	XML File	6 KB
Microsoft.IntelligencePacks.ThreatDetection.2906	3/22/2017 9:27 AM	XML File	10 KB
Microsoft.IntelligencePacks.UpdateAssessmentSnapshot.2895	3/22/2017 9:27 AM	XML File	49 KB
Microsoft.IntelligencePacks.SPAssessment.2885	3/21/2017 9:40 PM	XML File	22 KB
Microsoft.IntelligencePacks.SQLAssessmentPlus.2882	3/21/2017 9:40 PM	XML File	32 KB
Microsoft.IntelligencePacks.Assessments.Core.2860	3/21/2017 9:40 PM	XML File	32 KB
Microsoft.IntelligencePacks.SCOMAssessmentPlus.2857	3/21/2017 9:40 PM	XML File	23 KB
Microsoft.IntelligencePacks.LogManagement.SCOMOverrides.2855	3/21/2017 9:38 PM	XML File	5 KB
Microsoft.IntelligencePacks.Advisor.Monitoring.2853	3/21/2017 9:34 PM	XML File	55 KB
Microsoft.IntelligencePacks.ComputerGroups.2834	3/21/2017 9:34 PM	XML File	22 KB
Microsoft.IntelligencePacks.HealthAssessmentViaServer.2845	3/21/2017 9:34 PM	XML File	9 KB
Microsoft.IntelligencePacks.Performance.2848	3/21/2017 9:34 PM	XML File	11 KB
Microsoft.IntelligencePacks.CloudUpload.2824	3/21/2017 9:34 PM	XML File	29 KB
Microsoft.IntelligencePacks.Core.OperationsManager.2822	3/21/2017 9:34 PM	XML File	40 KB
Microsoft.IntelligencePacks.CustomLogUpload.2831	3/21/2017 9:34 PM	XML File	20 KB
Microsoft.IntelligencePacks.HealthAssessmentDirect.2828	3/21/2017 9:34 PM	XML File	9 KB
Microsoft.IntelligencePacks.IISLogUpload.2818	3/21/2017 9:34 PM	XML File	11 KB
Microsoft.SystemCenter.Advisor.Core.2811	3/21/2017 9:30 PM	XML File	21 KB

You can also look at the OperationsManager event log (it's the same for the SCOM agent or the standalone MMA agent) for the events indicating the MPs have been downloaded:



Operations Manager Number of events: 19,152

Filtered: Log: Operations Manager; Source: ; Event ID: 1200-1250. Number of events: 352

Level	Date and Time	Source	Event ID	Task Category
Information	3/21/2017 9:40:36 PM	HealthService	1210	Health Service
Information	3/21/2017 9:40:14 PM	HealthService	1204	Health Service
Information	3/21/2017 9:40:14 PM	HealthService	1204	Health Service
Information	3/21/2017 9:40:14 PM	HealthService	1204	Health Service
Information	3/21/2017 9:40:14 PM	HealthService	1204	Health Service
Information	3/21/2017 9:40:12 PM	HealthService	1201	Health Service
Information	3/21/2017 9:40:10 PM	HealthService	1201	Health Service
Information	3/21/2017 9:40:05 PM	HealthService	1201	Health Service
Information	3/21/2017 9:40:03 PM	HealthService	1201	Health Service
Information	3/21/2017 9:39:57 PM	HealthService	1200	Health Service

Event 1201, HealthService

New Management Pack with id:"Microsoft.IntelligencePacks.SPAssessment", version:"1.10.3188.0" received.

Log Name:	Operations Manager		
Source:	HealthService	Logged:	3/21/2017 9:40:12 PM
Event ID:	1201	Task Category:	Health Service
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	sco1.contoso.local
OpCode:			
More Information:	Event Log Online Help		

After confirming the Microsoft Intelligent Packs have been downloaded for the assessment(s) desired, continue with the setup of the assessment as outlined in the in the next section of this article.

Creation of the Assessment Scheduled Task

This step of the assessment setup and configuration is unique per assessment. At a high level, this phase has 2 steps.

1. Validate and configure the environment being assessed and the account and access required for successful collection per prerequisite documents for the respective assessments.
2. Create the assessment scheduled task for the assessments being configured.

The following table illustrates the high-level assessment account permissions required for successful assessment execution:

Assessment	**Local Administrator on Data Collection Machine**	**Enterprise Administrator**	**Domain Administrator**	**Local Administrator on targets**	**SQL SysAdmin**	**Assessment specific permissions**
Active Directory	✓	✓				https://docs.microsoft.com/en-us/services-hub/health/getting-started-ad#prerequisites
Active Directory Security	✓	✓				https://docs.microsoft.com/en-us/services-hub/health/getting-started-adsecurity#prerequisites
SCCM	✓			✓	✓	https://docs.microsoft.com/en-us/services-hub/health/getting-started-sccm#prerequisites
Exchange	✓		✓ (Optional)	✓		https://docs.microsoft.com/en-us/services-hub/health/getting-started-exchange#prerequisites
SQL	✓			✓	✓	https://docs.microsoft.com/en-us/services-hub/health/getting-started-sql#prerequisites
Windows Server	✓			✓		https://docs.microsoft.com/en-us/services-hub/health/getting-started-windows-server#prerequisites
Windows Client	✓			✓		https://docs.microsoft.com/en-us/services-hub/health/getting-started-windows-client#prerequisites
SharePoint	✓			✓	✓	https://docs.microsoft.com/en-us/services-hub/health/getting-started-sharepoint#prerequisites
Skype for Business	✓		✓ (Optional)	✓	✓ (Optional)	https://docs.microsoft.com/en-us/services-hub/health/getting-started-skype-for-business#prerequisites
SCOM	✓			✓	✓	https://docs.microsoft.com/en-us/services-hub/health/getting-started-scom#prerequisites
Exchange Online	✓					Global Administrator for Office365 with MFA disabled
SharePoint Online	✓					Global Administrator for Office365 with MFA disabled
Skype for Business Online/ Teams	✓					Global Administrator for Office365 with MFA disabled

Complete the assessment setup by following the "Getting Started" documentation for the assessments being configured, then return to this documentation for post setup details below.

[On-Demand Assessment – Active Directory]()

[On-Demand Assessment – AD Security]()

[On-Demand Assessment – Exchange]()

[On-Demand Assessment – SCCM]()

On-Demand Assessment – SCOM

On-Demand Assessment – SharePoint

On-Demand Assessment – Skype for Business

On-Demand Assessment – SQL Server

On-Demand Assessment – Windows Server

On-Demand Assessment – Windows Client

Download On-Demand Assessment Prerequisites

This page contains prerequisites documents for the various Assessment solutions running on Azure Log Analytics and Microsoft Services Hub. These documents will help you prepare your environment to setup and configure the Assessment solution.

On-Demand Assessment Prerequisite Documents

Active Directory

Active Directory Security

System Center Configuration Manager

Exchange Server

SQL Server

Windows Server (Server, Server Security, Hyper-V, Failover Cluster, IIS)

Windows Client

Office 365 Exchange Online

Office 365 Skype and Teams

Office 365 SharePoint Online

System Center Operations Manager

Skype for Business

SharePoint Server

Working with Assessment Results

Assessment recommendations may be reviewed once an assessment scheduled task has run and its recommendations and supporting details ingested into Azure Log Analytics.

Complete the steps in this section to navigate and work with assessment recommendations

- ✓ Validate successful ingestion of recommendations into Azure Log Analytics
- ✓ Review assessment results in Azure Log Analytics
- ✓ Review assessment results on Services Hub assessment dashboard

- ✓ Download assessment reports from Services Hub assessment dashboard
- ✓ Create remediation plan for assessment results from Services Hub

Validate Successful Assessment

Go to data collection machine On-Demand assessment working directory (e.g. c:\ODA) for the configured assessment(s) and click on the assessment folder (example: ADAssessment).

After the conclusion of the assessment execution, several files should be observed. For example:

new.prerequisites.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrecs

new.processingmodel.37508ed7-ad62-485f-9f22-d5d6fae783fd.ad.assessmentpm

new.rawdata.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrawdata

new.recommendations.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrecs

new.trace.37508ed7-ad62-485f-9f22-d5d6fae783fd.adassessment.assessmenttrace

After several minutes, the health service will begin ingesting these files into Azure Log Analytics and rename them to processed as the following set of files illustrates:

processed.prerequisites.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrecs

processed.processingmodel.37508ed7-ad62-485f-9f22-d5d6fae783fd.ad.assessmentpm

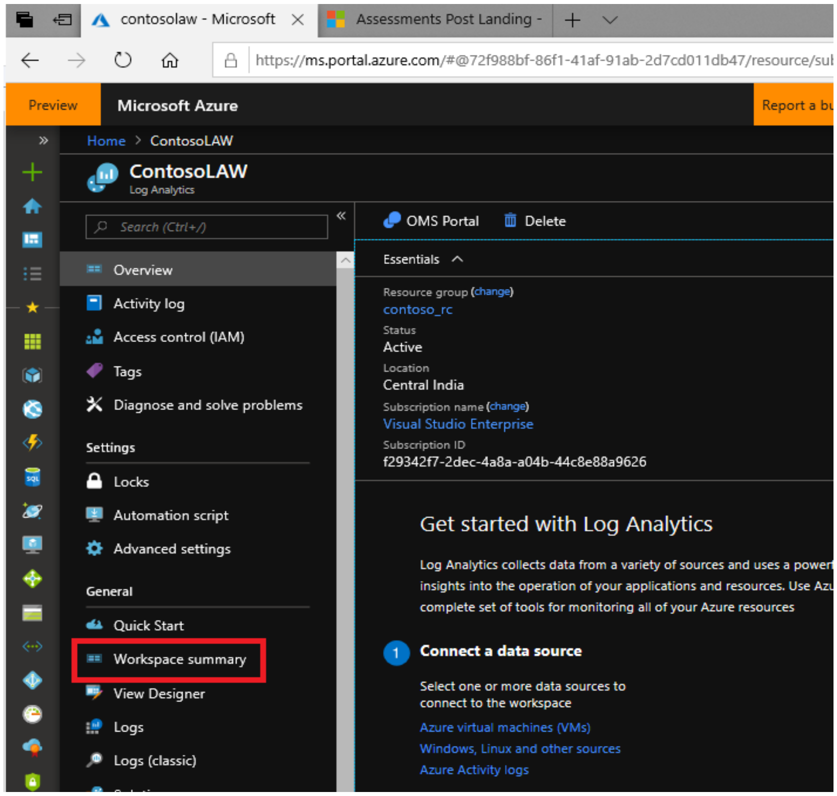
processed.rawdata.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrawdata

processed.recommendations.37508ed7-ad62-485f-9f22-d5d6fae783fd.assessmentadrecs

processed.trace.37508ed7-ad62-485f-9f22-d5d6fae783fd.adassessment.assessmenttrace

After 3 to 4 hours, check if you can view the results from the Azure portal.

All resources > Select Azure Log analytics workspace created > Workspace Summary



contosolaw - Microsoft | Assessments Post Landing -

https://ms.portal.azure.com/#@72f988bf-86f1-41af-91ab-2d7cd011db47/resource/sul

Preview | Microsoft Azure | Report a bu

Home > ContosoLAW

ContosoLAW
Log Analytics

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Locks
- Automation script
- Advanced settings

General

- Quick Start
- Workspace summary
- View Designer
- Logs
- Logs (classic)

OMS Portal | Delete

Essentials

Resource group (change)
contoso_rc
Status
Active
Location
Central India
Subscription name (change)
Visual Studio Enterprise
Subscription ID
f29342f7-2dec-4a8a-a04b-44c8e88a9626

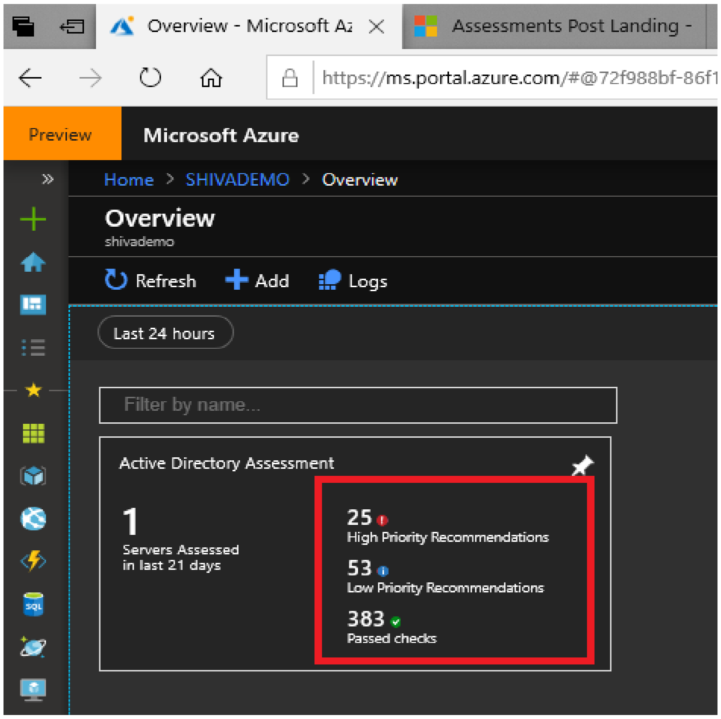
Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerf
insights into the operation of your applications and resources. Use Azu
complete set of tools for monitoring all of your Azure resources

1 Connect a data source

Select one or more data sources to connect to the workspace

Azure virtual machines (VMs)
Windows, Linux and other sources
Azure Activity logs



Overview - Microsoft Az | Assessments Post Landing -

https://ms.portal.azure.com/#@72f988bf-86f1

Preview | Microsoft Azure

Home > SHIVADEMO > Overview

Overview
shivademo

Refresh | Add | Logs

Last 24 hours

Filter by name...

Active Directory Assessment

1
Servers Assessed in last 21 days

25
High Priority Recommendations

53
Low Priority Recommendations

383
Passed checks

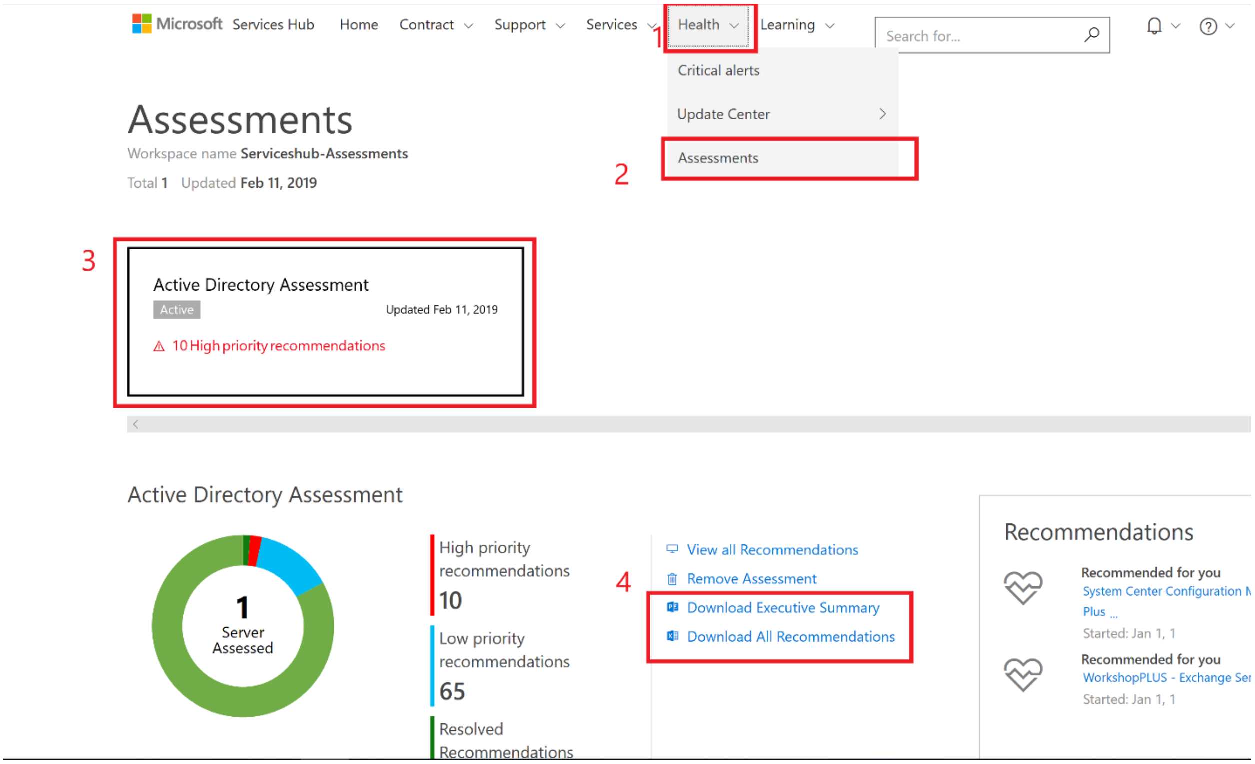
Services Hub Assessment Page

Once you've linked your Services Hub to an Azure Log Analytics workspace and configured an assessment you can access and view your assessment information from the Services Hub. To view your personalized assessment page, select Health from the primary navigation, and then click Assessments. Here you'll find all your configured assessments with top-level data pulled from Azure Log Analytics.

Note: *Only users that have access to Azure Log Analytics will be able to see the assessment data as we are following the security rules in place for Azure Log Analytics. For access, please contact the Azure owner in your organization.*

Downloading the reports from Services Hub

Download the reports from portal. Serviceshub.microsoft.com->Health->Assessment

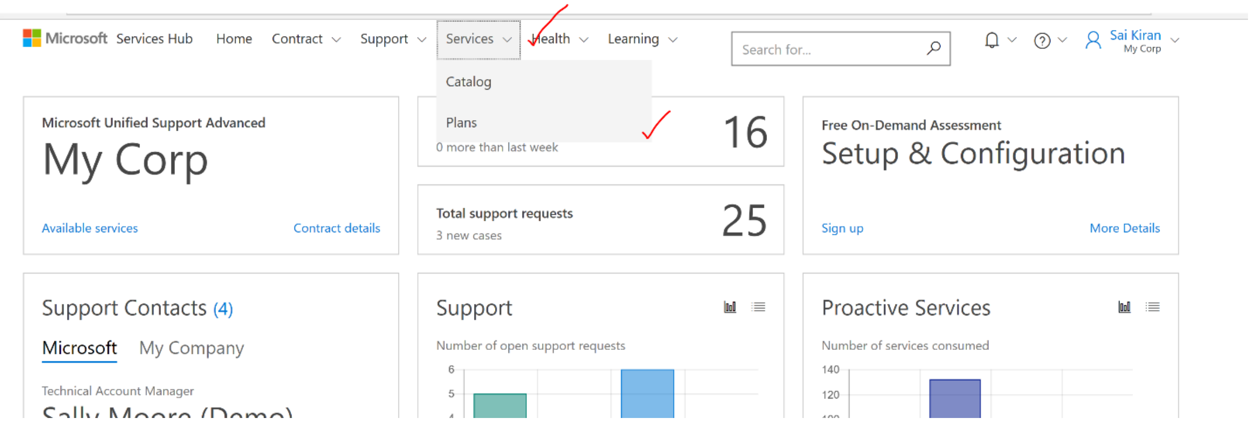


Remediation Plan creation in Service Hub

For creating a remediation plan Please follow the below process:

1. Log into the https://serviceshub.microsoft.com/databoard

   Services > Plan



Microsoft Unified Support Advanced

My Corp

Available services

Contract details

0 more than last week 16

Total support requests 25

3 new cases

Free On-Demand Assessment

Setup & Configuration

Sign up

More Details

Support Contacts (4)

Microsoft My Company

Technical Account Manager

Sally Moore (Demo)

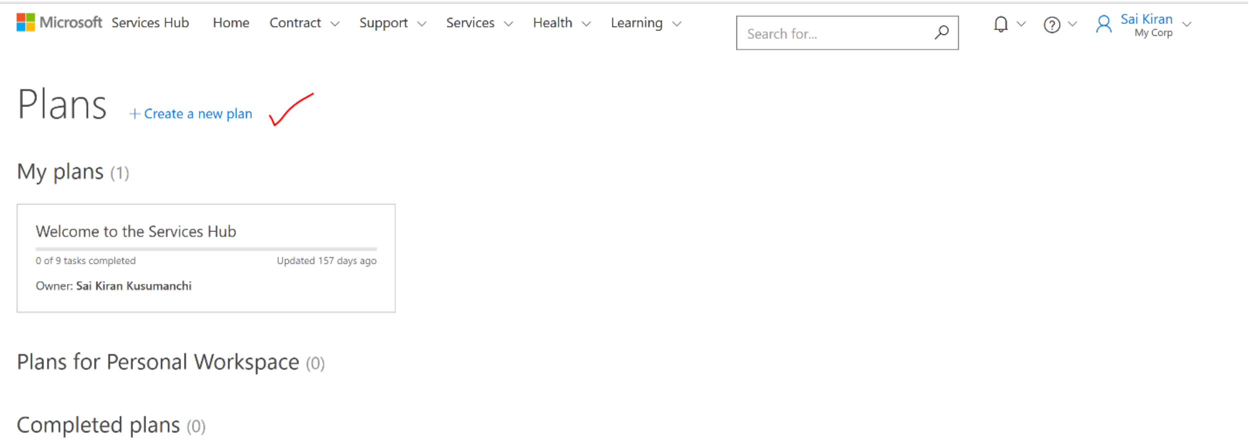
Support

Number of open support requests

Proactive Services

Number of services consumed

2. Click on the +Create a new plan



Plans

My plans (1)

Welcome to the Services Hub

0 of 9 tasks completed Updated 157 days ago

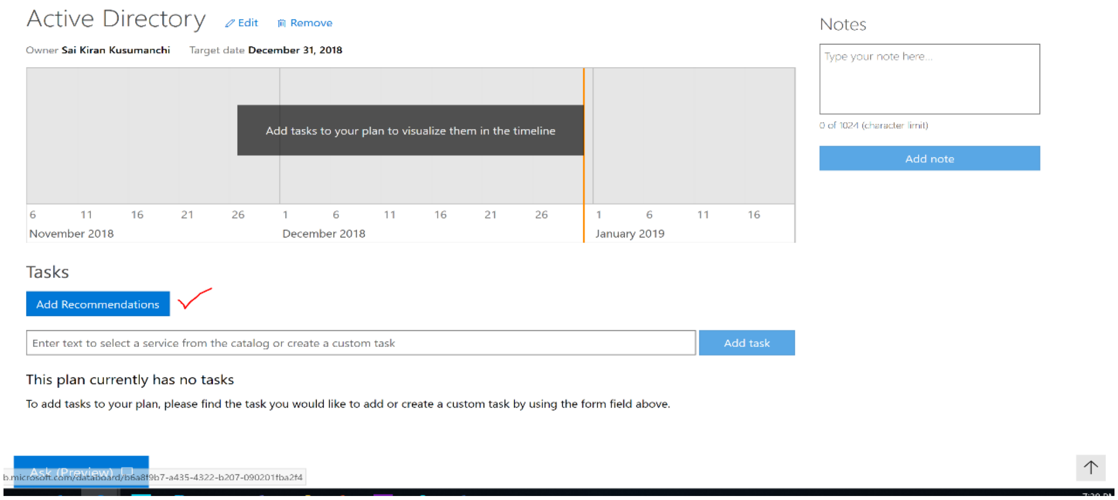
Owner: Sai Kiran Kusumanchi

Plans for Personal Workspace (0)

Completed plans (0)

3. Select Choose an existing template > Choose the respective technology > Click Next
4. Choose the following for the below attributes:
   a. Plan Template: Select the respective technology
   b. Owner: Your email ID
   c. Target Date: Select a future Date by which you want to finish the remediation execution.
   d. Members: Can add members of your org if you want to share the Plan with them.
   e. Click Save

5. Click Add Recommendations



Owner Sai Kiran Kusumanchi Target date December 31, 2018

Add tasks to your plan to visualize them in the timeline

Type your note here...

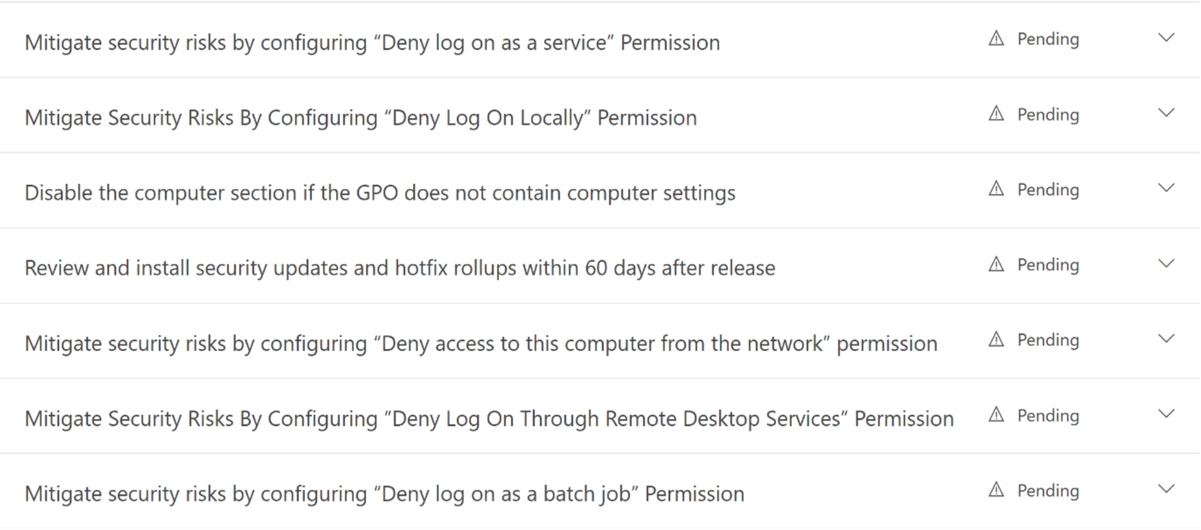
0 of 1024 (character limit)

Enter text to select a service from the catalog or create a custom task

This plan currently has no tasks

To add tasks to your plan, please find the task you would like to add or create a custom task by using the form field above.

6. Once the recommendations are added. It should have all the issues from Azure portal with respect to the Focus areas.



Mitigate security risks by configuring “Deny log on as a service” Permission ⚠ Pending

Mitigate Security Risks By Configuring “Deny Log On Locally” Permission ⚠ Pending

Disable the computer section if the GPO does not contain computer settings ⚠ Pending

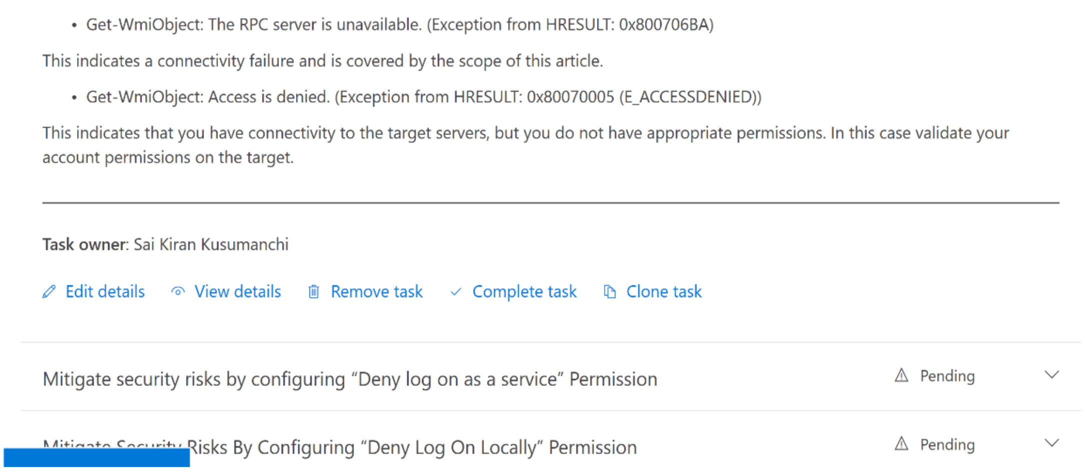
Review and install security updates and hotfix rollups within 60 days after release ⚠ Pending

Mitigate security risks by configuring “Deny access to this computer from the network” permission ⚠ Pending

Mitigate Security Risks By Configuring ”Deny Log On Through Remote Desktop Services” Permission ⚠ Pending

Mitigate security risks by configuring “Deny log on as a batch job” Permission ⚠ Pending

7. Now you can edit the issue, target date, change the status of issue by clicking the individual issues as below:



- Get-WmiObject: The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)

This indicates a connectivity failure and is covered by the scope of this article.

- Get-WmiObject: Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))

This indicates that you have connectivity to the target servers, but you do not have appropriate permissions. In this case validate your account permissions on the target.

Task owner: Sai Kiran Kusumanchi

Mitigate security risks by configuring “Deny log on as a service” Permission ⚠ Pending

Mitigate Security Risks By Configuring “Deny Log On Locally” Permission ⚠ Pending

8. You can use the Remediation plan for tracking the issues progress, assigning the issues to the respective stakeholder.

Additional Azure Log Analytics Information

Azure Log Analytics Site Focus Area: Insights and Analytics: Gain immediate insights across workloads

- Overview Video
- Gaining insights with Microsoft Azure Log Analytics

Azure Log Analytics Site Focus Area: Security and Compliance: Respond faster to security threats

- Overview Video
- Managing security and compliance with Microsoft Azure Log Analytics

Azure Log Analytics Site Focus Area: Automation and Control: Enable consistent control and compliance

- Overview Video
- Demo guide

Azure Log Analytics Site Focus Area: Protection and Recovery: Ensure availability of apps and data

- Overview Video