



Cisco Secure Cloud Analytics

Microsoft Azure Integration Quick Start Guide



Table of Contents

Public Cloud Monitoring Configuration for Microsoft Azure	3
Azure User Roles	3
Azure Configuration	4
Create an Azure Resource Group	4
Obtain the Microsoft Entra ID URL	4
Create a Microsoft Entra ID Application	5
Add API Permissions to an Application	5
Grant Access to an Application	6
Create an Azure Storage Account to Store Flow Log Data	6
Create a Blob Storage Account	7
Enable Internet Access to the Blob Storage Account	7
Grant Azure Storage Account Access	7
Enable Azure Network Watcher	8
Register Insights Provider	9
Enable Azure Flow Logs	9
Secure Cloud Analytics Configuration with Azure	10
Configure Secure Cloud Analytics to Ingest Flow Log Data from Azure	10
Azure Permissions Required for Secure Cloud Analytics Integration	12
Additional Resources	14
Contacting Support	15
Change History	16

Public Cloud Monitoring Configuration for Microsoft Azure

Cisco Secure Cloud Analytics public cloud monitoring is a visibility, threat identification, and compliance service for Microsoft Azure. Secure Cloud Analytics consumes network traffic data, including Network Security Group (NSG) or Virtual network (VNet) flow logs, from your Azure public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics consumes flow logs directly from your Azure storage account, and uses an application to gain additional context.

Azure User Roles

We recommend configuring the integration as a user with the **Global Administrator** Microsoft Entra ID role and **Owner** role for all monitored subscriptions. If that is not possible, contact your Microsoft Entra ID administrator to ensure that:

1. The user is able to create app registrations. This is allowed by default for member users, although some Microsoft Entra IDs may disable this. If this is guest user or app registration has been disabled, the **Application Developer** role must be assigned to the user.
2. For each monitored subscription, the user has access to the following Azure resources: authorization, network, storage accounts, and monitoring. These require the **User Access Administrator** and **Contributor** roles be assigned to the user.

See [Azure Permissions Required for Secure Cloud Analytics Integration](#) for more information.

Azure Configuration

To configure Azure to generate and store flow log data:

- Have at least one resource group to monitor. See [Create an Azure Resource Group](#) for more information.
- Obtain your Microsoft Entra ID URL. See [Obtain the Microsoft Entra ID URL](#) for more information.
- Create an Microsoft Entra ID application, add the proper API permissions, then grant access to the application. See [Create a Microsoft Entra ID Application, Add API Permissions to an Application](#), and [Grant Access to an Application](#) for more information.
- Create a storage account for the flow log data, then grant access. See [Create an Azure Storage Account to Store Flow Log Data](#) and [Grant Azure Storage Account Access](#) for more information.
- Enable Network Watcher, register Insights provider, and enable flow logs. See [Enable Azure Network Watcher](#), [Register Insights Provider](#), and [Enable Azure Flow Logs](#) for more information.

Create an Azure Resource Group

First, make sure you have one or more resource groups that you want to monitor. You can use existing resource groups, or create a new resource group and populate it with resources, such as virtual machines.

1. Log in to your Azure portal.
2. Select **More Services > General > Resource Groups**.
3. Click **Create**.
4. Choose your **Subscription** from the drop-down list.
5. Enter a **Resource group name**.
6. Choose a **Region** from the drop-down list.
7. Click **Review + create**.
8. Click **Create**.


Obtain the Microsoft Entra ID URL

To provide Secure Cloud Analytics access to Azure metadata services, obtain your Microsoft Entra ID URL. Record this information; you will upload this information to the Secure Cloud Analytics web portal at the end of this process to complete your integration with Azure.


1. In your Azure portal, select **More Services > All > Microsoft Entra ID**.
2. On the Overview page, copy your Primary domain, `example.onmicrosoft.com`, and paste it into a plaintext editor. This is the `Microsoft Entra ID` URL used in the [Configure in Secure Cloud Analytics](#) section.

Create a Microsoft Entra ID Application

After you obtain the Microsoft Entra ID URL and subscription ID, create an application to allow Secure Cloud Analytics to read metadata from your resource groups. Copy the application key after you finish creating the application.

 Create **only one application** per Microsoft Entra ID instance. You can monitor multiple subscriptions in an Microsoft Entra ID instance by assigning roles to the application. See [Grant Access to an Application](#) for more information.

1. In your Azure portal, select **Microsoft Entra ID > App Registrations**.
2. Click **New registration**.
3. In the **Name** field, enter `xdra-reader`. Leave the others as default.
4. Copy the **Application (client) ID** and paste it into a plain text editor. This is the `Application ID` used in the [Configure in Secure Cloud Analytics](#) section.
5. Select **Certificates and Secrets > New Client Secret**.
6. In the **Description** field, enter `Cisco XDR Reader`.
7. In the **Expires** drop-down list, choose an appropriate expiration date or accept the default value.
8. Click **Add**.
9. Copy the value and paste it into a plaintext editor. This is the `Application Key` used in the [Configure in Secure Cloud Analytics](#) section.

 You cannot view the key after you navigate away from this page.

Add API Permissions to an Application

After you create the `xdra-reader` application in Microsoft Entra ID, add the API permissions to it, which allows Secure Cloud Analytics to support Entra ID detections.

1. In your Azure portal, select **Microsoft Entra ID > Manage > App registrations**.
2. Search for `xdra-reader` in **All applications**, and then select the `xdra-reader` application.

3. Select **Manage > API permissions > Add a permission > Microsoft Graph > Application permissions**.
4. Under **Select permissions**, check the `AuditLog.Read.All` permission check box.
5. Click **Add permissions**.
6. In the **Configured permissions** table on the **API permissions** pane, click **Grant admin consent** to approve the permission for the `xdra-reader` application.



Create only one application per Entra ID instance. Multiple subscriptions in the same instance can be monitored by a single application via role assignments, as described later.

Grant Access to an Application

After you register the `xdra-reader` app in Microsoft Entra ID, assign the Monitoring Reader role to it, which allows it to read metadata from your resource groups. Perform the following procedure for each subscription you want to monitor.

1. In your Azure portal, select **More Services > General > Subscriptions** and select your subscription.
2. Select **Access Control (IAM)**.
3. Select **Add > Add role assignment**.
4. In the **Role** drop-down list, choose **Monitoring Reader**,
5. Click **Next**.
6. Under **Members > Assign access to**, select **User, group, or service principal**, then click **Select members**.
7. In the **Search** field, enter `xdra-reader`, then click **Next**.
8. Click **Next**, then click **Review + assign**.
9. Repeat these steps for each current subscription you want to monitor.

Create an Azure Storage Account to Store Flow Log Data

After you assign the Monitoring Reader role to the `xdra-reader` application, create a storage account to store the flow log data. Create a binary large object (blob) storage account in the same location as your resource groups.



You can reuse an existing Storage Account if it can store blobs and is in the same location as your resource groups.

After you create the blob storage account, ensure that the firewall rules allow access to the storage account from the internet, so that Secure Cloud Analytics can properly integrate with your Azure deployment.

Create a Blob Storage Account

1. In your Azure portal, select **More Services > Storage > Storage Accounts**.
2. Click **Add**.
3. Select your **Subscription**.
4. Select the **Resource group** you want to monitor.
5. Enter a **Storage account name**.
6. Choose the same **Region** for the storage account as the resource group you specified.
7. In the **Preferred storage type** drop-down menu, choose `Azure Blob Storage` or `Azure Data Lake Storage Gen 2`.
8. Select `Standard` or `Premium` for **Performance**, depending on how often you plan to have blobs accessed within the storage account.
9. Choose a **Redundancy** option from the drop-down menu, based on your organization's requirements.
10. Click **Review + create**.
11. Click **Create**.

Enable Internet Access to the Blob Storage Account

1. From the blob storage account, select the **Networking** tab.
2. In the **Public network access** section, select `Enable`.
3. In the **Public network access scope** section, select `Enable from all networks`.
4. Click **Save**.

Grant Azure Storage Account Access

After you create a storage account, add permissions to enable Secure Cloud Analytics to retrieve the flow log data from the storage account.

1. In your Azure portal, select **More Services > Storage > Storage Accounts**.
2. Select the storage account configured to store flow log data.
3. Select **Access Control (IAM)**.

4. Click **Add > Add role assignment**.
5. Select the `Storage Blob Data Reader` role, then click **Next**.

If you use custom roles, make sure the role has the following required permissions:

`Microsoft.Storage:`

- Actions -

 Other: `Generate User Delegation Key`


Read: `Get Blob Container`

Read: `List of Blob Containers`

- Data Actions -

Read: `Read Blob`

6. In the **Assign access to** field, select `User`, `group`, or `service principal`.
7. In the **Members** field, click **Select members**.
8. In the **Select members** drawer, select the application created in the [Create a Microsoft Entra ID Application](#) section, `xdra-reader`, then click **Select**.
9. Click **Next**.
10. Review the settings, then click **Next**.
11. Click **Review + assign**.
12. Repeat these steps for each storage account containing flow logs.

 If restricting access to this storage account based on IP, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > Azure > About** to see the list of public IPs used by Secure Cloud Analytics.

Enable Azure Network Watcher

After you grant storage access, enable Network Watcher in the region containing your resource groups, if you have not already enabled it. Azure requires Network Watcher to enable flow logs for your network security groups.

1. In your Azure portal, select **More Services > Networking > Network Watcher**.
2. On the **Overview** page, click **Create**.
3. Choose your **Subscription** from the drop-down list.
4. Choose your **Region** from the drop-down list.
5. Click **Add**.

Register Insights Provider

Before activating flow logs, enable the `microsoft.insights` provider.

1. In your Azure portal, select **More Services > General > Subscriptions** and select your subscription.
2. Under the **Settings** section, click **Resource Providers**.
3. Highlight the `microsoft.insights` provider, then click **Register**.
4. Repeat the steps for each subscription you want to monitor.

Enable Azure Flow Logs

After you enable Network Watcher, enable flow logs for one or more resources you want to have monitored.



We support Network Security Group (NSG) and Virtual network (VNet) flow logging.

1. In your Azure portal, select **More Services > Networking > Network Watcher**.
2. Select **Logs > Flow Logs**.
3. Click **Create**.
4. Select your **Subscription**.
5. Select **Flow Log type (Network Security Group / Virtual Network)**.
6. Click **Select target resources** and confirm the selections.
7. Select the blob storage account to store the logs.
8. In the **Retention (days)** field, enter a retention time for the logs.
9. Click **Review + create**.



Secure Cloud Analytics does not require enabling Traffic Analytics, but you can enable it if your organization wants the functionality.

10. Repeat the steps for each resource you want to monitor.

Secure Cloud Analytics Configuration with Azure

Enter the following information in the Secure Cloud Analytics web portal to complete your integration with Azure:

- [Microsoft Entra ID URL](#)
- [Application ID](#)
- [Application Key](#)

Configure Secure Cloud Analytics to Ingest Flow Log Data from Azure

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > Azure > Credentials**.
3. Click **Add New Credentials**.
4. Enter your `Microsoft Entra ID URL`.
5. Enter the `Application ID`.
6. Enter the `Application Key`.
7. Choose the **Azure Cloud** environment from the drop-down list.
8. Click **Create**.
9. Select **Settings > Integrations > Azure > Storage Access** and ensure that your storage accounts are listed in the **Azure RBAC** table.

Azure RBAC

Below are the Azure role-based access control (Azure RBAC) storage accounts configured to retrieve flow log data using your Azure credentials. We recommend using this method for accessing flow logs.

Name	Last Success Time
testvnetflowlogs	2025-10-09 19:06:56 UTC

20 Per Page 1-1 of 1 results << 1/1 >>

10. To verify Secure Cloud Analytics is receiving data from your storage accounts, select **Settings > Sensors** and scroll to the **Azure Sensors** section to view your **Azure (RBAC)** storage accounts.

Azure Sensors

 Azure (RBAC): testvnetflowlogs <input type="button" value="Delete"/>	 Azure: labflowlogs <input type="button" value="Delete"/>
--	--



It can take up to 10 minutes for Azure RBAC storage accounts to display in the Secure Cloud Analytics portal. Any existing Azure sensors using the Shared Access Signature (SAS) method will go offline, and then you can click **Delete** to remove the SAS sensors.

Azure Permissions Required for Secure Cloud Analytics Integration

The following table details the role memberships required to configure Azure for integration with Secure Cloud Analytics:

Action	Permission required for member user (native tenant member)	Permission required for guest user (collaboration guest)
Create an Azure Resource Group	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Obtain the Microsoft Entra ID URL	default permission of member user	default permission of guest user to obtain Microsoft Entra ID URL, add guest user to Cognitive Services User role to obtain Subscription ID
Create a Microsoft Entra ID Application	default permission of member user to create the Microsoft Entra ID application registration, default permission of member user to generate a client secret if the user created the application registration	add guest user to Application Developer role
Grant Access to an Application	default permission of member user, if user created the application registration	add guest user to Application Developer role
Create an Azure Storage Account to Store Flow Log Data	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Grant Azure Storage Account Access	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Enable Azure Network Watcher	add member user to Network Contributor role	add guest user to Network Contributor role

<p>Enable Azure Flow Logs</p>	<p>add member user to Network Contributor role</p>	<p>add guest user to Network Contributor role</p>
--	--	---

For more information on roles and permissions, search for the following terms on Microsoft's Azure documentation:

- Guest and member user permissions
- Application Developer role
- Cognitive Services User role
- Monitoring Contributor role
- Network Contributor role
- Storage Account Contributor role

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
 - To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
 - To open a case by email: tac@cisco.com
 - For phone support: 1-800-553-2447 (U.S.)
 - For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	December 6, 2018	Initial version.
1_1	March 20, 2019	Updated to remove mentions of beta.
1_2	November 1, 2019	Updated with activity log storage information and additional role information.
1_3	January 10, 2019	Updated with removal of flow log retention configuration.
1_4	August 26, 2020	Update with information about internet access for blob storage account.
1_5	16 October 2020	Updates based on UI update.
1_6	February 2, 2021	Updates for how to create the storage account.
2_0	November 3, 2021	Updated product branding.
3_0	June 1, 2022	Restructured and updated configuration instructions.
4_0	August 1, 2022	Added <i>Contacting Support</i> section. Added note for public IPs. Updated document title.
4_1	January 11, 2023	Removed the <i>Azure Activity Log Storage</i> section.
4_2	April 21, 2023	Corrected cross-reference links.

5_0	February 26, 2025	<p>Added <i>Add API Permissions to an Application</i> section.</p> <p>Updated configuration instructions to match Azure UI updates.</p>
5_1	March 21, 2025	<p>Updated the <i>Enable Azure Flow Logs</i> section to include VNet flow logging support.</p>
6_0	November 6, 2025	<p>Updated configuration instructions throughout the guide to support Azure RBAC. Removed the <i>Activate Using a Bash Script</i> section.</p>

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

