



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
Activate Using a Bash Script	3
Azure Configuration	5
Create an Azure Resource Group	5
Obtain the Azure Active Directory URL and Subscription ID	5
Create an Azure AD Application	6
Grant Access to an Application	6
Create an Azure Storage Account to Store Flow Log Data	7
Create a blob storage account	7
Enable internet access to the blob storage account	8
Generate an Azure Storage Account Shared Access Signature URL	8
Enable Azure Network Watcher	8
Register Insights Provider	9
Enable Azure NSG 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	11
Additional Resources	13
Contacting Support	14
Change History	15

Public Cloud Monitoring Configuration for Microsoft Azure

Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud 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) 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 NSG 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** Azure Active Directory (AD) role and **Owner** role for all monitored subscriptions. If that is not possible, contact your Azure AD administrator to ensure that:

1. The user is able to create app registrations. This is allowed by default for member users, although some Azure ADs 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.

Activate Using a Bash Script

We have developed an experimental Bash script that automates the configuration instructions.

You can download the script from the Secure Cloud Analytics web portal.

Go to **Settings > Integrations > Azure > About**.

To enable the Bash script:

1. Log in to your Azure portal.
2. Click the console icon next to the search bar to launch Azure Cloud Shell. Click **Bash** to open a bash console.
3. Upload the script using the Upload/Download files button.
4. Execute the script with `bash azure_setup.sh` and follow the instructions.



- The script will enable monitoring for all the subscriptions it can discover.
- The script will direct all Network Security Groups of a given location to store their flow logs to the storage account provided.

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 Azure AD URL and subscription ID. See [Obtain the Azure Active Directory URL and Subscription ID](#) for more information.
- Create an AD application, then grant access to the application. See [Create an Azure AD Application](#) and [Grant Access to an Application](#) for more information.
- Create a storage account for the flow log data, then generate a SAS URL. See [Create an Azure Storage Account to Store Flow Log Data](#) and [Generate an Azure Storage Account Shared Access Signature URL](#) for more information.
- Enable Network Watcher, register Insights provider, and enable flow logs. See [Enable Azure Network Watcher](#), [Register Insights Provider](#), and [Enable Azure NSG 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 into your Azure portal.
2. Select **Resource Groups**.
3. Click **Add**.
4. Enter a **Resource group name**.
5. Select your **Subscription**.
6. Select a **Resource group location**.
7. Click **Review + create**.
8. Click **Create**.


Obtain the Azure Active Directory URL and Subscription ID

To provide Secure Cloud Analytics access to Azure metadata services, obtain your Azure Active Directory (AD) URL and Azure subscription ID. Record this information; you will upload this information to the Secure Cloud Analytics web UI at the end of this process to complete your integration with Azure.


1. Log into your Azure portal.
2. Select **Azure Active Directory > Overview**.
3. Copy your Primary domain (e.g., example.onmicrosoft.com) and paste it into a plaintext editor. This is the Azure AD URL.
4. Select **Subscriptions**, then select your subscription.
5. Copy the subscription ID and paste it into a plaintext editor.

Create an Azure AD Application

After you obtain the Active Directory 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 Active Directory instance. You can monitor multiple subscriptions in an Active Directory instance by assigning roles to the application. See [Grant Access to an Application](#) for more information.

1. Log into your Azure portal.
2. Select **Azure Active Directory > App Registrations > New Registration**.
3. In the **Name** field, enter `swc-reader`. Leave the others as default.
4. Copy the **Application (client) ID** and paste it into a plain text editor.
5. Select **Certificates and Secrets > New Client Secret**.
6. In the **Description** field, enter `SWC Reader`.
7. In the **Expires** drop-down, select an appropriate expiration date or accept the default value.
8. Click **Add**.
9. Copy the application key **Value** and paste it into a plaintext editor.

 Copy the application key now, as you cannot view the key after you navigate away from this page.

Grant Access to an Application

After you register the `swc-reader` app in AD, 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. Log into your Azure portal.
2. Select **Subscriptions**, then select your subscription.

3. Select **Access Control (IAM)**.
4. Select **Add > Add role assignment**.
5. In the **Role** drop-down, select **Monitoring Reader**.
6. In the **Assign access to** drop-down, select **User, group, or service principal**.
7. In the **Search by name or email address** field, enter `swc-reader`.
8. Click **Save**.

Create an Azure Storage Account to Store Flow Log Data

After you assign the Monitoring Reader role to the `swc-reader` app, 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. Log into your Azure portal.
2. Select **Storage Accounts**.
3. Click **Add**.
4. Select your **Subscription**.
5. Select the **Resource group** you want to monitor.
6. Enter a **Storage account name**.
7. Select the same **Location** for the storage account as the resource group you specified.
8. Select `Storage v2 (general purpose)` for the **Account kind**.
9. Select a **Replication** option from the drop-down, based on your organization's requirements.
10. Select the `Hot` or `Cool` access tier, depending on how often you plan to have blobs accessed within the storage account.
11. Click **Review + create**.
12. Click **Create**.

Enable internet access to the blob storage account

1. From the blob storage account, select the **Firewalls and virtual networks** setting.
2. Select **Allow access from** `All networks`, then save your changes.

Generate an Azure Storage Account Shared Access Signature URL

After you create a storage account, generate a shared access signature (SAS) for the storage account to allow Secure Cloud Analytics permission to retrieve the flow log data from the storage account. Then, copy the Blob service SAS URL. Secure Cloud Analytics uses the Blob service SAS URL to retrieve the flow log data from the storage account.



SAS permissions are time-limited, based on configuration. If your SAS permissions expire, Secure Cloud Analytics cannot retrieve flow log data from the storage account.

1. Log into your Azure portal.
2. Select **More Services > Storage > Storage Accounts**.
3. Select the storage account configured to store flow log data.
4. Select **Shared access signature**.
5. In the **Allowed services** field, select the **Blob**.
6. In the **Allowed resource types** field, select **Service, Container, and Object**.
7. In the **Allowed permissions**, select **Read and List**.
8. Enter a **Start time** corresponding to your current time.
9. Enter an **End time** corresponding to at least one year from the current time.
10. In the **Allowed protocols** field, select the **HTTPS only**.
11. Click **Generate SAS and connection string**.
12. Copy the **Blob service SAS URL** and paste it into a plaintext editor.



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 generate the blob storage SAS URL, 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. Log into your Azure portal.
2. Select **Network Watcher > Overview**.
3. Select the regions list to expand it.
4. Select the menu for the region containing your resource groups, then select **Enable Network Watcher**.

Register Insights Provider

Before activating NSG Flow Logs, enable the `microsoft.insights` provider.


1. Log into your Azure portal.
2. Go to **Subscriptions**, and select your subscription name.
3. Click **Settings > Resource Providers**.
4. Highlight the `microsoft.insights` provider, then click **Register**.

Enable Azure NSG Flow Logs

After you enable Network Watcher, enable network security group (NSG) flow logs for one or more network security groups. These network security groups should correspond with the resource groups you want to monitor.

 Blob storage accounts do not support NSG flow log retention periods.

1. Log into your Azure portal.
2. Select **Network Watcher > NSG flow logs**.
3. Select a network security group to display the Flow Logs settings page.
4. In the **Flow Logs version** field, select `Version 2`.
5. Select the blob **Storage account** for which you configured an SAS in **Generate an Azure Storage Account Shared Access Signature URL**.
6. Select `Off` for the **Traffic Analytics** status.

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

7. In the **Retention (days)** field, enter a retention time for the logs.
8. Click **Save**.
9. Repeat steps 2 through 8 for each network security group for which you want to enable flow logging.

Secure Cloud Analytics Configuration with Azure

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

- [Azure AD URL](#)
- [Subscription ID](#)
- [Application ID](#)
- [Application Key](#)
- [Blob service SAS URL](#)

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 **Azure AD URL**.
5. Enter the Azure **Application ID**.
6. Enter the Azure **Application Key**.
7. Select the **Azure Cloud** environment from the drop-down list.
8. Click **Create**.
9. Click **Storage Access**.
10. Click **New Integration**.
11. Enter the **Blob Service SAS URL** in the **API Key** field.
12. Click **Create**.
13. Select Subscriptions and ensure that your subscription is listed.

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 Azure Active Directory URL and Subscription ID	default permission of member user	default permission of guest user to obtain AD URL, add guest user to Cognitive Services User role to obtain Subscription ID
Create an Azure AD Application	default permission of member user to create the AD 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
Generate an Azure Storage Account Shared Access Signature URL	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

Enable Azure NSG Flow Logs	add member user to Network Contributor role	add guest user to Network Contributor role
-----------------------------------	---	--

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/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for a 60-day Free Trial
- <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>
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

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 Contacting Support section. Added note for public IPs. Updated document title.
4_1	January 11, 2023	Removed the Azure Activity Log Storage section.
4_2	April 21, 2023	Corrected cross-reference links were needed.

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)

