Cisco Secure Cloud Analytics

ISE Integration Guide

Table of Contents

Secure Cloud Analytics ISE Integration Overview

Cisco Secure Cloud Analytics can now retrieve user attribution data from Cisco Identity Services Engine (ISE) using pxGrid. This integration enables user activity reporting in the Secure Cloud Analytics Event Viewer. The following diagram provides a sample architectural overview of Secure Cloud Analytics integration with ISE.
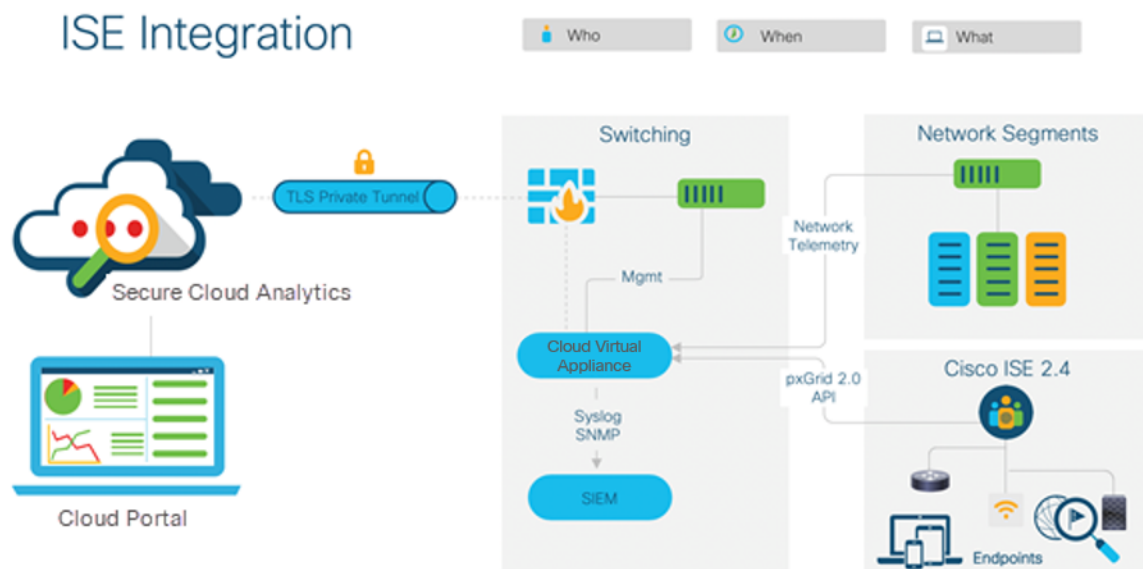
This guide describes how to configure:

- ISE Passive Identity Connector (ISE-PIC) with Active Directory (AD), mapped to Windows Management Instrumentation (WMI), so that ISE-PIC retrieves user sessions from AD.
- a Secure Cloud Analytics sensor to retrieve user information.

> ℹ️
> - You must have ISE version 2.4 or greater to integrate with Secure Cloud Analytics.
> - Secure Cloud Analytics requires the Monitoring (MnT) and pxGrid personas to be enabled on the same node. Due to this requirement, we only support small and medium ISE deployments. Large deployments are not supported. For more information on ISE deployments, refer to Performance and Scalability Guide for Cisco Identity Services Engine.

Procedure Overview

For a successful integration, make sure you complete the following procedures:

1. Review the **ISE Integration Prerequisites**.

2. Follow the instructions in **Configuring ISE-PIC** to passively retrieve user sessions.

   If you use ISE for access control, skip this section.

3. Ensure your sensor is up-to-date by **Verifying the Secure Cloud Analytics Sensor Version**

4. Follow the instructions in **Integrating with ISE** to configure the integration. You can choose to configure using the web portal or manually.

ISE Integration Prerequisites

To integrate Secure Cloud Analytics with ISE, deploy the following:

Component	Required	Notes
Identity Services Engine (ISE)	Yes	Version 2.4 or greater
Secure Cloud Analytics sensor	Yes	Version 5.1.0 or greater
ISE Passive Identity Connector (ISE-PIC)	Optional	Configure if using Windows Management Instrumentation (WMI) to passively retrieve user sessions from a Microsoft Active Directory (AD) server, or other user identity providers, into ISE.

You also need the following information to complete your configuration:

- ISE server IP address and hostname

Configuring ISE-PIC

If you are using Active Directory (AD) for access control, configure ISE-PIC on your policy service node (PSN). Then, configure your AD credentials and WMI on your domain. Finally, test live authentications from the ISE UI.

> ℹ️ Active Directory is the most common identity provider. For more information on supported identity providers, refer to the ISE-PIC Administrator Guide.

ISE-PIC Integration Overview

The basic workflow, using WMI to passively retrieve user sessions from an AD server into ISE, involves the following steps:

1. A user logs into a workstation and is authenticated via AD.
2. WMI notifies ISE Passive Identity about this authentication.
3. ISE adds the binding `Username:IP_Address` to its Session Directory.
4. ISE retrieves the AD User Groups and Attributes.
5. ISE saves this information into its Session Directory.
6. ISE instructs WMI to probe for the current user status.

See https://msdn.microsoft.com/en-us/library/aa384642(v=vs.85).aspx for more information on WMI.

The following diagram describes this workflow.
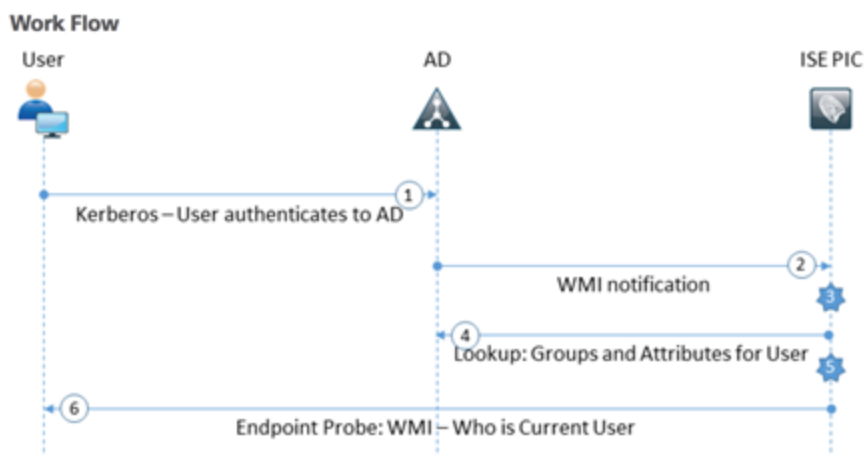
Configure ISE-PIC on your policy service node

Before You Begin

- Make sure you have the AD join password from when you configured AD as an external Identity Store.

Procedure

1. From the ISE UI, select **Administration > System > Deployment**.
2. Select your PSN node.
3. Select **Enable Passive Identity Service**.
4. Click **Save**.

Configure your domain with AD credentials and WMI

Procedure

1. From the ISE UI, select **Work Centers > PassiveID > Providers**.
2. Select your main Active Directory node.
3. Select the PassiveID tab.
4. Select the domain, then click **Edit**.
5. Enter the AD join **Password** that you configured when you configured AD as an external Identity Store.
6. Click **Save**.
7. Click **Test** to verify your credentials. You have the following options:
    - If you receive a message stating that the connection was successfully established, continue to the next step.
    - If you receive an error message, check your password and try again.
8. Select the PassiveID tab.
9. Select the domain, then click **Config WMI**.
10. Wait several minutes for the configuration to complete.
11. When the configuration finishes, click **OK**.

Verify live authentications

Procedure

- From the ISE UI, select **Work Centers > PassiveID > Overview > Live Sessions**. If your configuration is correct, live authentications display here. If it is not, verify your configuration.

Verifying the Secure Cloud Analytics Sensor Version

For ISE UI integration, you must deploy a Secure Cloud Analytics sensor, version 5.1.0 or greater. This allows the sensor to communicate with ISE over pxGrid 2.0 to receive user session information.

Verify your sensor's version

Before You Begin

- SSH log into your sensor.

Procedure

- At the command line, enter the following command and press Enter.

```
cat /opt/obsrvbl-ona/version
```

If the console displays a version that is not 5.1.0 or greater, redeploy it using an ISO image downloaded from the Secure Cloud Analytics UI. See the Secure Cloud Analytics Sensor Installation Guide for more information.

If you do not want to redeploy the sensor, you can instead backup your sensor's configuration, upgrade the sensor package manually, and restore the configuration.

> ⚠ Performing this procedure incorrectly may place your sensor in an unusable state.

Upgrade a sensor's package to the current version

Before You Begin

- SSH log into your sensor.

Procedure

1. From the command line, enter the following command and press Enter to stop the sensor service. If prompted, enter the root password.

```
sudo systemctl stop obsrvbl-ona.service
```

2. Enter the following command and press Enter to backup the `config.auto` configuration file.

```
sudo cp /opt/obsrvbl-ona/config.auto .
```

3. Enter the following command and press Enter to backup the `config.local` configuration file.

   ```
   sudo cp /opt/obsrvbl-ona/config.local .
   ```

4. Enter the following command and press Enter to remove the sensor service package.

   ```
   sudo apt remove --purge ona-service
   ```

5. Enter the following command and press Enter to download the latest sensor service package.

   ```
   sudo wget https://assets-
   production.obsrvbl.com/ona-packages/obsrvbl-ona/v5.1.1/ona-
   service_UbuntuXenial_amd64.deb
   ```

6. Enter the following command and press Enter to install the sensor service package.

   ```
   sudo apt install ./ona-service_UbuntuXenial_amd64.deb
   ```

7. Enter the following command and press Enter to change file ownership settings on the `config.auto` configuration file.

   ```
   sudo chown obsrvbl_ona: config.auto
   ```

8. Enter the following command and press Enter to change file ownership settings on the `config.local` configuration file.

   ```
   sudo chown obsrvbl_ona: config.local
   ```

9. Enter the following command and press Enter to restore the `config.auto` configuration file.

   ```
   sudo cp config.auto /opt/obsrvbl-ona/config.auto
   ```

10. Enter the following command and press Enter to restore the `config.local` configuration file.

    ```
    sudo cp config.local /opt/obsrvbl-ona/config.local
    ```

11. Enter the following command and press Enter to restart the sensor service.

    ```
    sudo systemctl restart obsrvbl-ona.service
    ```

Integrating with ISE

To configure the Secure Cloud Analytics sensor to integrate with ISE, follow the instructions for one of the following procedures:

- **Configure ISE using the Web Portal (Recommended)**
- **Manual Configuration for Integrating with ISE**

Configure ISE using the Web Portal (Recommended)

Make sure you complete the preceding procedures before you configure the integration. For details, refer to **Procedure Overview**.

> **i** You can find more details regarding the ISE deployment types, roles and personas in the <u>Cisco ISE Installation Guide</u>.

Enable pxGrid on one or more ISE nodes

1. Log into the ISE UI as an administrator.
2. Click the ≡ (**Menu**) icon and choose **Administration > System > Deployment**.
3. Locate nodes with pxGrid persona enabled.

> **i** We require you to have the pxGrid and MnT personas enabled on the selected node for the integration.

4. If pxGrid is disabled, refer to the *Deploy Cisco pxGrid Node* section of the <u>Cisco ISE Administrator Guide</u>.

Enable certificate-based approval of new accounts

1. In the ISE UI, click the ≡ (**Menu**) icon and choose **Administration > pxGrid Services > Settings**.
2. Check the **Automatically approve new certificate-based accounts** check box, then click **Save**.

> **i** We recommend configuring automatic approval. Manual approval of the pxGrid clients is possible, refer to the *Configure Cisco pxGrid Settings* section of the <u>Cisco ISE Administrator Guide</u> for more information.

Generate pxGrid certificate

1. In the ISE UI, click the ≡ (**Menu**) icon and choose **Administration > pxGrid Services > Client Management > Certificates**.

2. In the **I want to** drop-down list, select **Generate a single certificate (without a certificate signing request)**.

3. In the **Common Name (CN)** field, enter a name for the sensor, example sca_sensor.

4. In the **Certificate Download Format** drop-down list, select **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)**.

5. In the **Certificate Password** field, enter a temporary (single-use), strong certificate password to encrypt the private key.

6. Click **Create** to download a ZIP archive with the certificate and encrypted private key.

> ℹ️
> - The Common Name does not have to match the sensor name. The name is visible on the pxGrid clients list when you go to **Administration > pxGrid Services > Client Management > Clients**.
>
> - PxGrid requests will fail if there is another pxGrid client with the same name registered to ISE already.
>
> - You should not generate more than one certificate with the same Common Name. During certificate renewal, go to **Administration > pxGrid Services > Client Management > Clients** and remove the existing pxGrid client. Then you can generate a new certificate with the same Common Name.

Enable Secure Cloud Analytics Sensor for ISE

1. Log in to the Secure Cloud Analytics web portal.

2. Go to **Settings** > **Integrations** > **ISE**.

3. Select the sensor you want to configure with ISE.

4. In the **Certificate password** field, use the password created in step 5 of the previous section.

5. Upload the ZIP file downloaded in step 6 of the previous section.

6. Click **Submit**. After successfully configuring the integration, the sensor status icon turns green. This may take up to 30 minutes and depends on the ISE session

volume.

7. After the status icon turns green, go to **Investigate** > **Event Viewer** > **ISE**. Confirm ISE events are shown.

Troubleshooting

There are a few common problems that can prevent the integration from working.

Before You Begin

- SSH into the sensor and log in as an administrator.

Procedure

If the Secure Cloud Analytics portal did not integrate with ISE, check the sensor file at `/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log`, and review it for error messages. We have provided details in each of the following sections.

- `Name or service not known`: refer to **DNS issues**
- `SSLCertVerificationError`: refer to **Certificate issues**
- `No sessions since...`: refer to **No sessions**

DNS issues

Check the sensor file at `/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log`. If it shows lines with `Name or service not known`, the sensor cannot resolve the configured ISE server hostname (for example: ise.example.org).

Try the following:

- Replace the server name with its associated IP address in the web interface, or
- Access the sensor over SSH and add an entry to the `/etc/hosts` file.

Certificate issues

Check the sensor file at `/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log`. If it shows lines with `SSLCertVerificationError`, the ISE server may be presenting the sensor with a certificate for a hostname other than the one you configured.

Try the following:

- Log into the ISE server interface and check the certificate. Re-configure the certificate with the correct hostname.
- Reconfigure the ISE server with the IP address instead of the hostname.

No sessions

Check the sensor file at `/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log`. If it shows lines with shows `No sessions since...`, then the setup is correct but there are no sessions available from pxGrid.

Confirm the following:

- The ISE server is configured to integrate with Active Directory, RADIUS, TACACS, or similar.

- There are active sessions being logged in the ISE server.

- The time is correct on the ISE server and the sensor.

Manual Configuration for Integrating with ISE

> ℹ️ If you configured ISE using the previous section, Configure ISE using the Web Portal (Recommended), you do not need to manually configure the integration.

Make sure you complete the preceding procedures before you configure the integration. For details, refer to **Procedure Overview**.

Requirements

To configure the on-premises sensor to query an ISE server for session data, you need the following:

- a client certificate

- a client key in RSA format and a passphrase to decrypt the client key

- a server certificate and chain

Generate the certificate bundle

Before You Begin

- Log in to your Secure Cloud Analytics portal.

Procedure

1. Go to **Settings** > **Integrations** > **ISE**.

2. Follow the instructions on the page to generate a certificate bundle:

   For example, here is a sample file list:

   ```
   CertificateServicesEndpointSubCA-ise_.cer
   CertificateServicesNodeCA-ise_.cer
   ```

```
CertificateServicesRootCA-ise_.cer
SSL.comRootCertificationAuthorityRSA_.cer
SSL.comRSASSLsubCA_.cer
swc-sensor_.cer
swc-sensor_.key
```

> ℹ️ We will use this list of examples in the following instructions.

3. Transfer the relevant files to the target sensor (for example, with WinSCP).

Obtain the client key

1. Run the following command to decrypt the client key. You will also be prompted to enter the passphrase.

```
openssl rsa -in swc-sensor_.key -out decrypted-swc-sensor_.key
```

2. After the decryption, the first line of the file is:

```
-----BEGIN RSA PRIVATE KEY-----
```

Create the certificate chain

1. Identify the client certificate file – `swc-sensor_.cer` from our [example].
2. Link all the certificate files together, excluding the client certificate file:

```
cat CertificateServicesEndpointSubCA-ise_.cer \
CertificateServicesNodeCA-ise_.cer \
CertificateServicesRootCA-ise_.cer \
SSL.comRootCertificationAuthorityRSA_.cer > server_chain.cer
```

Your resulting file should have multiple -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.

Update the configuration

Move the files

Run the following commands to move the client certificate, decrypted client key, and server chain to a permanent location:

---

1. `sudo mkdir /etc/ise_poller`

2. `sudo mv swc-sensor_.cer /etc/ise_poller/ise_client_cert.pem`

3. `sudo mv decrypted-swc-sensor_.key /etc/ise_poller/ise_client_key.pem`

4. `sudo mv server_chain.cer /etc/ise_poller/ise_server_cert.pem`

5. `sudo chown obsrvbl_ona: /etc/ise_poller/*`

6. `sudo chmod 0600 /etc/ise_poller/*`

Configure your sensor

Configure the sensor to point to the files you moved in the previous procedure.

1. Open the file `/opt/obsrvbl-ona/config.local` and add lines as shown in the following example. Make sure you set the `OBSRVBL_ISE_SERVER_NAME` to match your ISE server's primary node:

   `OBSRVBL_ISE_POLLER="true"`

   `OBSRVBL_ISE_SERVER_NAME="your-ise-server.local"`

   `OBSRVBL_ISE_CLIENT_CERT="/etc/ise_poller/ise_client_cert.pem"`

   `OBSRVBL_ISE_CLIENT_KEY="/etc/ise_poller/ise_client_key.pem"`

   `OBSRVBL_ISE_CA_CERT="/etc/ise_poller/ise_server_cert.pem"`

Restart sensor services

1. Run the following command:

   `sudo systemctl restart obsrvbl-ona.service`

Confirm integration

Before You Begin

- Log in to your Secure Cloud Analytics portal.

Procedure

1. Go to **Settings** > **Integrations** > **ISE**.

2. After you complete the configuration, the status icon turns green. This may take up to 30 minutes and depends on the ISE session volume.

3. After the status icon turns green, go to **Investigate** > **Event Viewer** > **ISE**. Confirm ISE events are shown.

Troubleshooting

1. Check the sensor file and review it for error messages:

   `/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log`

   If the file ends with `SSLCertVerificationError` and contains the string `self signed certificate in certificate chain`, the server certificate chain is incomplete. Review the instructions and confirm that all relevant certificates are included in your certificate chain.

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

Revision	Revision Date	Description
1.0	21 November 2019	Initial version.
1.1	4 November 2020	Updated based on updates to Stealthwatch Cloud ISE integration.
1.2	8 July 2021	- Updated sensor version. - Updated steps in "Upgrade a sensor's package to the current version." - Updated integration instructions. Added basic setup and manual configuration. - Updated branded terms.
1.3	6 August 2021	Updated logo.
2.0	24 May 2022	- Added web portal configuration instructions. - Updated steps in the "Upgrade a sensor's package to the current version" section. - Restructured ISE-PIC section.
2.1	4 August 2022	Updated Contacting Support section.
2.2	6 September 2024	Added ISE deployment size support note.

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)