ASSET SYNCHRONIZATION GUIDE

Nozomi Networks - Cisco ISE Asset Synchronization Instructions

This procedure describes how to configure the Cisco ISE asset synchronization with the Nozomi Networks Guardian, which consists of the following:

- Configuring the Cisco ISE data integration into the Nozomi Networks Guardian
- Configuring the Cisco ISE to receive asset identification from Nozomi Networks
  - Creating the seven (7) Endpoint Custom Attributes
  - Creating the Profiler Condition to match assets from Nozomi Networks
  - Creating the first Profiling Policy to detect asset changes
  - Creating the second Profiling Policy to detect asset changes

Prerequisites:

- Cisco ISE
  - Minimum: 2.4.x
  - Recommended: 2.7.x
- Nozomi Networks Guardian: v21.9

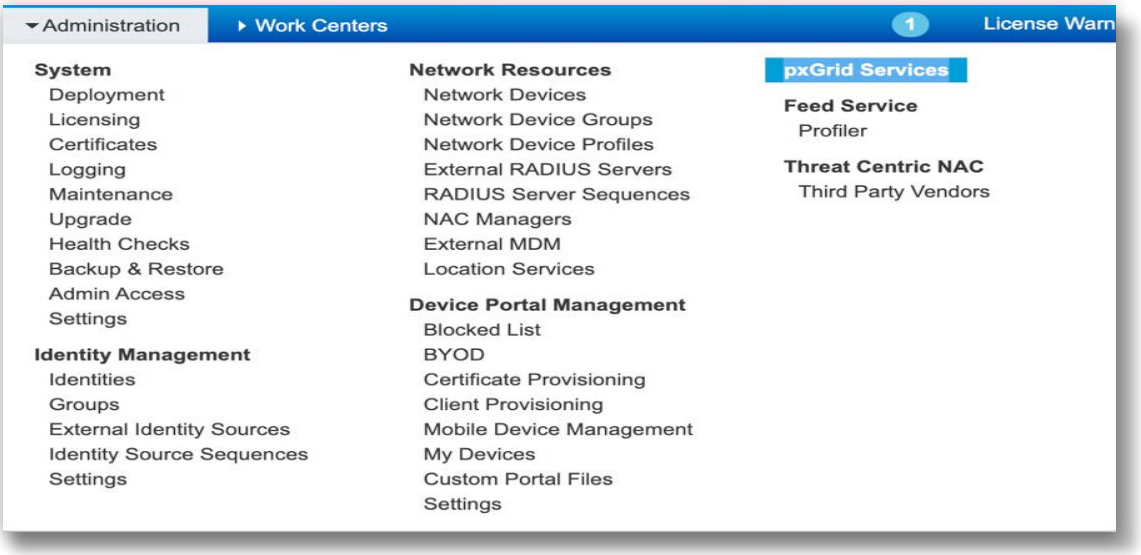
Part 1 - Configuring the Cisco ISE Data Integration in the Nozomi Networks Guardian

From the Nozomi Networks Guardian UI, perform the following steps to configure the Cisco ISE data integration into Guardian:

1. Generate Certificate Signing Requests (CSRs) using one of the following methods:
   a. **Recommended:** Use your Certificate Authority (CA) to generate CSRs, if supported. **See step 2**.
   b. **Optional:** If your CA does not allow you to generate CSRs, use OpenSSL through the Guardian shell to generate your CSR and private key. **See step 3**.
   c. **Alternative:** Use any other tool capable of generating CSRs.

2. **(Recommended)** Use a Self-Signed Certificate issued by the Cisco ISE to generate CSRs as follows:

   a. Log into the ISE GUI and navigate to **Administration > pxGrid Services**.



   b. Select **Certificates** at the top of the screen.

   c. Select **Generate a single certificate (without a certificate signing request)**.

   d. Enter the requested information in the appropriate fields.

      Note: Include all relevant IP and DNS information as SANs.

   e. Select **PEM** as the certificate format.

   f. Enter a certificate password, if any.

      Note: This password is required in the **Configuring the Cisco ISE to receive asset identification from Nozomi Networks** procedure.

   g. Click **Create** and download the archive.

   h. Extract the archive into a directory on your local computer.

      Note: Certificates issued by the Cisco ISE are not perpetual and should be renewed prior to expiration.

3. **(Optional)** Configure the Cisco ISE integration on the Nozomi Networks Guardian as follows:

   a. Log into the Guardian Web UI and navigate to **Administration > Settings > Data Integration**.

   b. Click + in the top right corner of the screen to add a new integration, then select Cisco ISE from the drop-down menu.

   c. Enter the following configuration information:

      i. To URI: Enter the hostname or IP address of the ISE pxGrid node

      ii. Key Password: Enter the password of the private key that you created when you generated your CSR or that was generated by the Cisco ISE

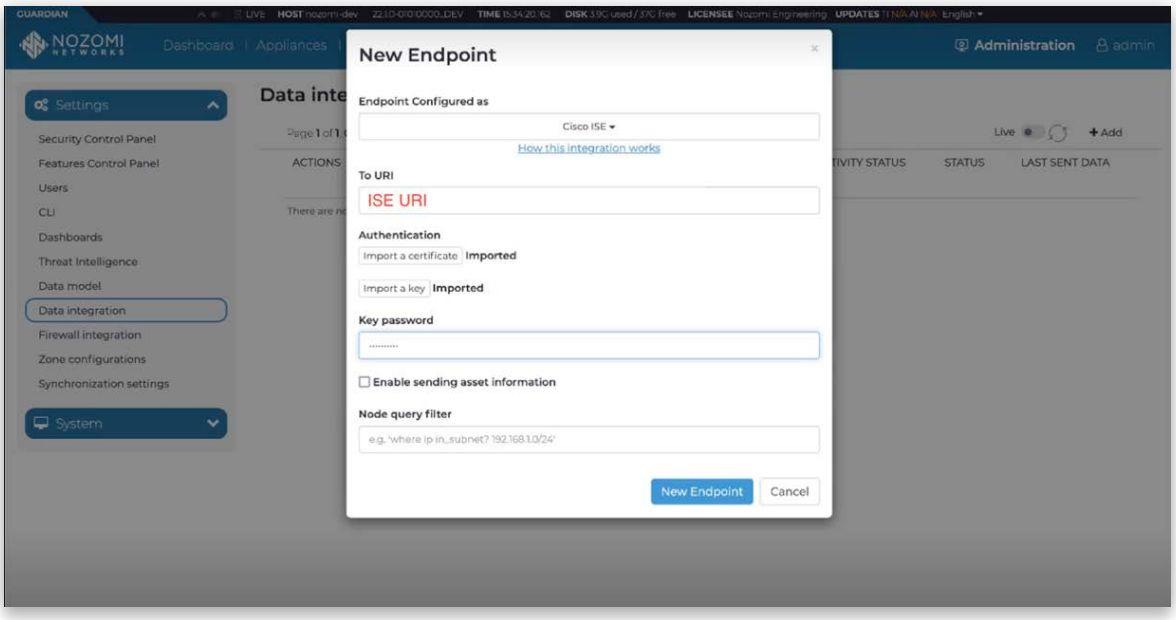
      iii. Import Certificate: Upload your Nozomi Networks Guardian certificate

      iv. Import the Key: Upload your private key file

      v. Assure that the Enable sending asset information checkbox is checked, to ensure that assets will be sent.

Notes:

- High Availability (HA) is not supported at this time. Please integrate with the primary Cisco ISE device.
- Data integration changes asset profiles within your Cisco ISE system. For IT assets discovered by the Nozomi Networks Guardian, this may result in contention with the ISE native profiler. To avoid contention, use the node query filter to send only nodes from your OT network.



Part 2 - Configuring the Cisco ISE to receive asset identification from Nozomi Networks

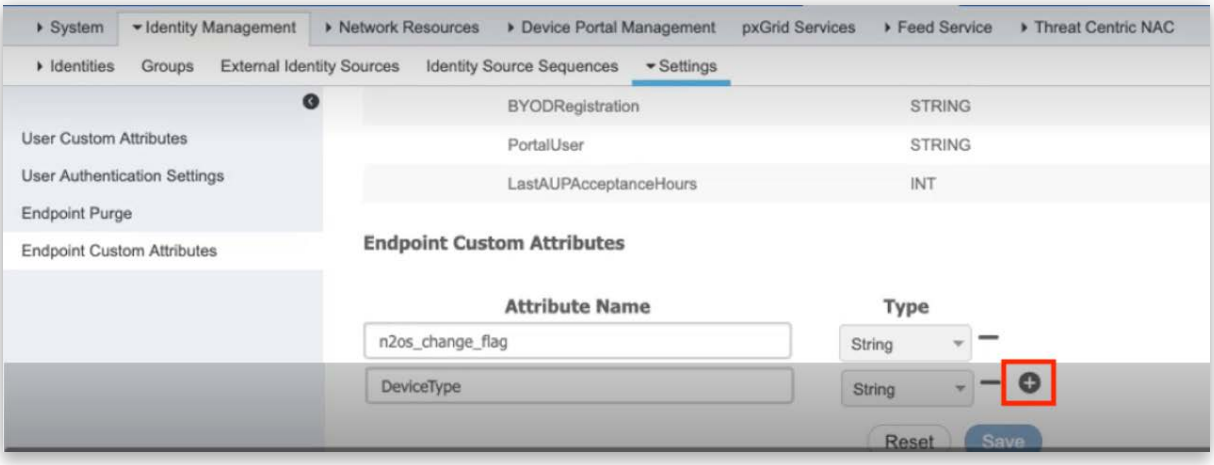
From the Cisco ISE dashboard, perform the following steps to configure the Cisco ISE to receive asset identification from Nozomi Networks.

1. Go to **Administration > Identity Management > Settings > Endpoint Custom Attributes** to create the required endpoint custom attributes in the Cisco ISE.

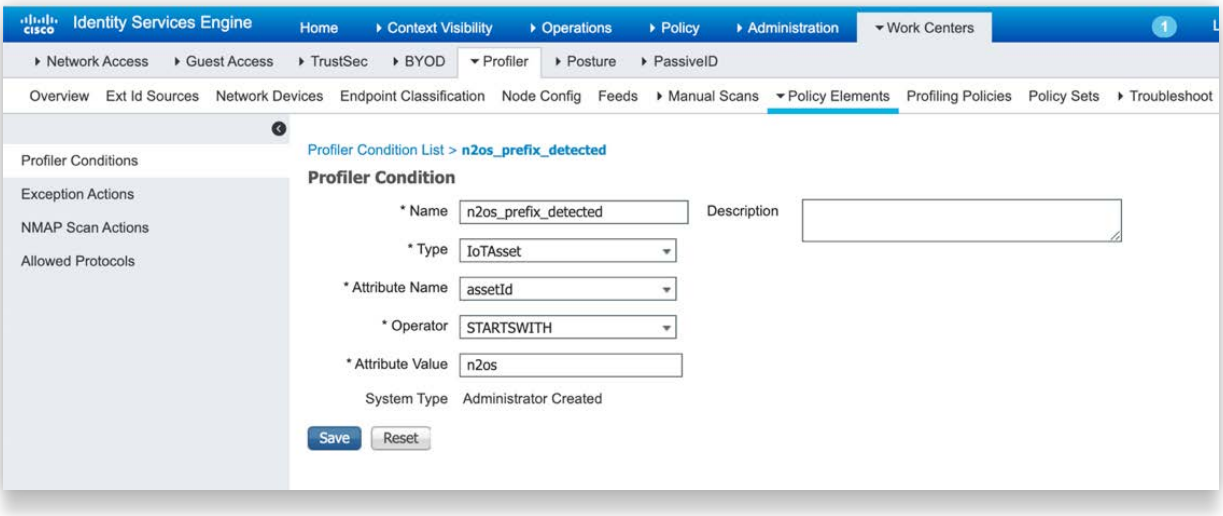
   Note: These attributes are used to receive asset details from the Nozomi Networks Guardian. The type of each attribute is String.

   Attributes List:

   a. n2os_change_flag
   b. n2os_operating_system
   c. n2os_product_name
   d. n2os_vendor
   e. n2os_type
   f. n2os_appliance_site
   g. n2os_zone

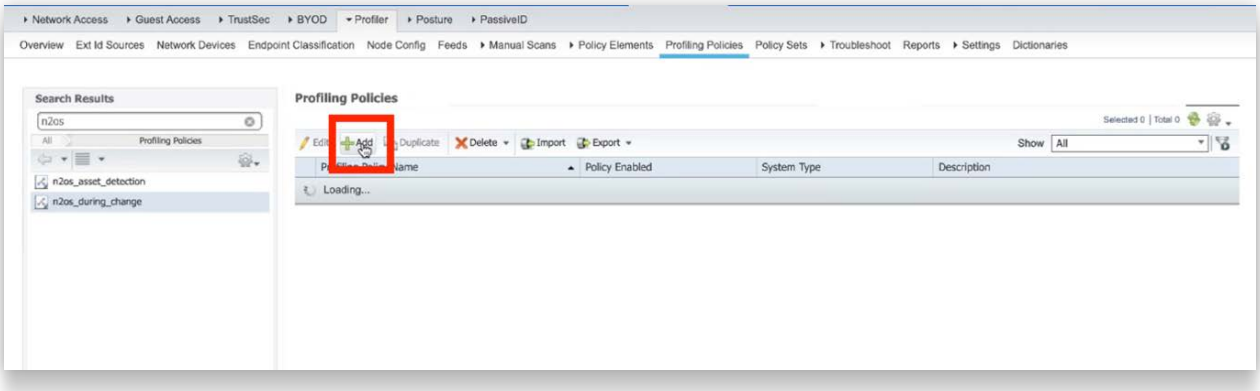


2. Go to **Work Centers > Profiler > Policy Elements > Profiler Conditions > Add** to create a Profiler Condition to match the n2os assetIds (Nozomi Networks assets).



3. Go to **Work Centers > Profiler > Profiling Policies > Add** to create the Profiling Policies to receive attribute updates within the Cisco ISE.

   Note: We create two Profiling Policies as a workaround so that the Cisco ISE can process Nozomi Networks asset updates due to an issue in the pxGrid API. The Cisco ISE can then oscillate between the two policies.



4. Create the following Profiling Policies::

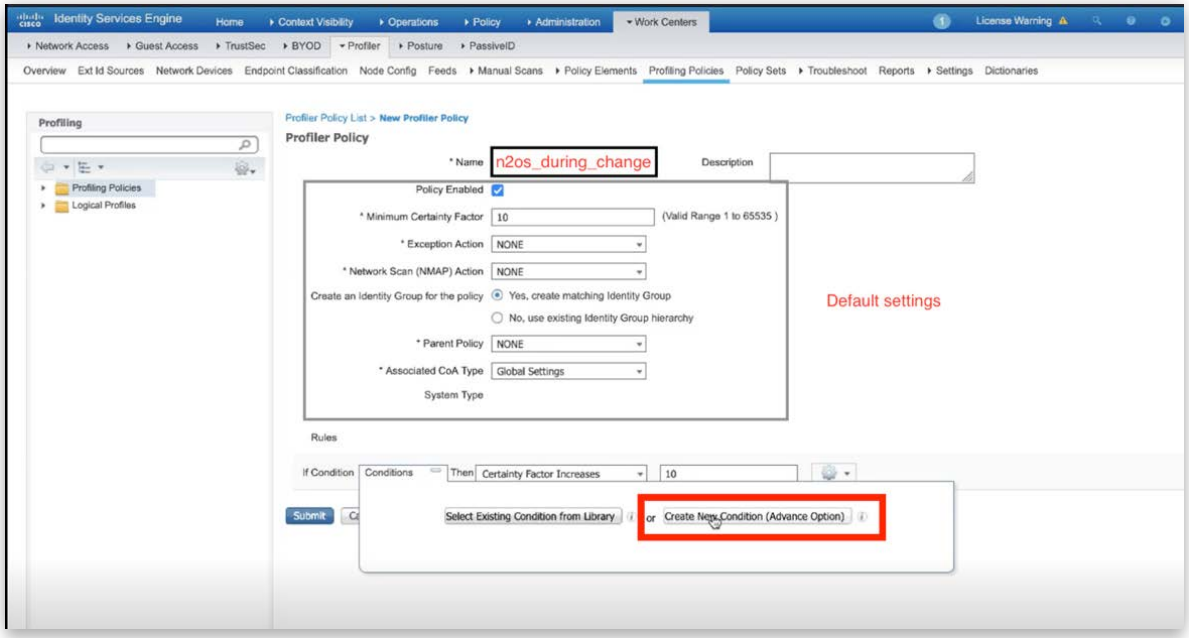
   a. **Profiling Policy 1** (Initial profiling policy).

      i. Name: **n2os_during_change**

      ii. Minimum Certainty Factor: **10**

      iii. Leave all other values at their default, as shown below:

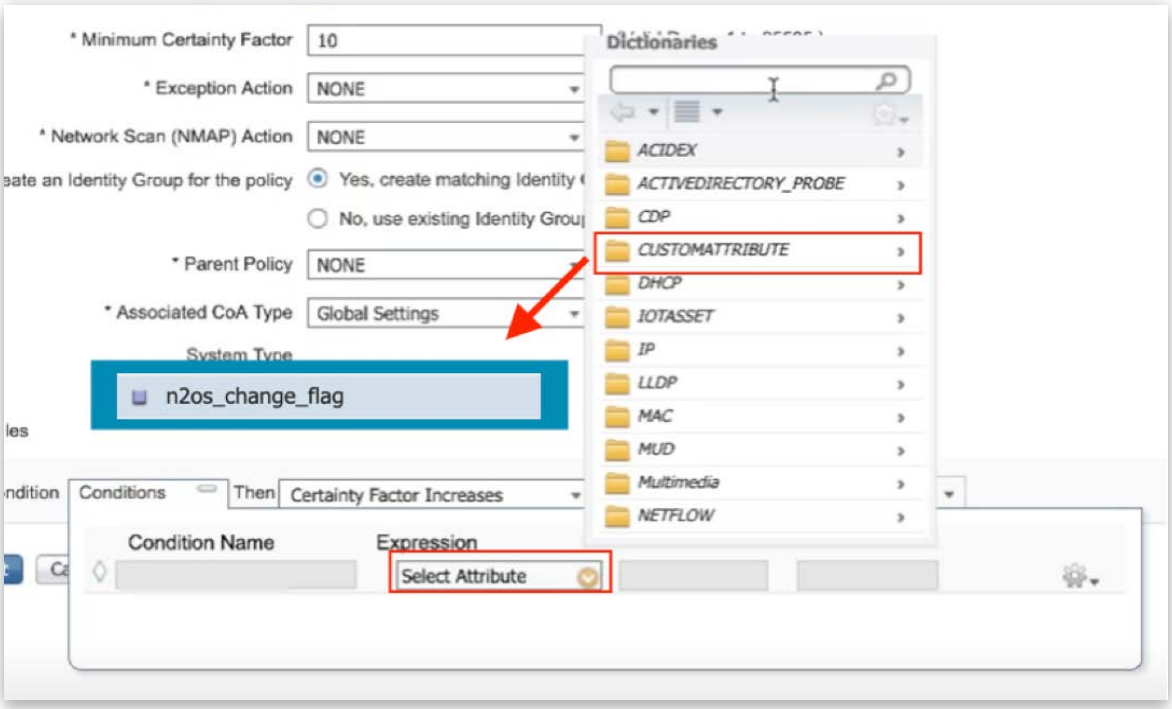
      - Policy Enabled: **checked**
      - Minimum Certainty Factor: **10**
      - Exception Action: **None**
      - Network Scan (NMAP) Action: **None**
      - Create an Identity Group for the Policy: **Yes, create matching identity group**
      - Parent Policy: **None**
      - Associated CoA Type: **Global Setting**



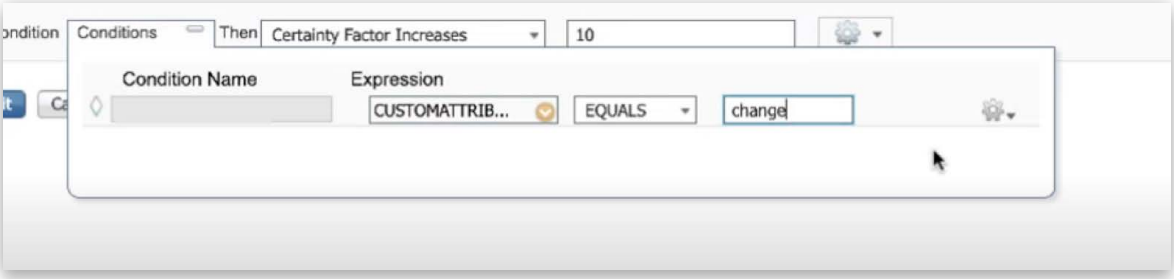
   iv. In the Rules section click **Conditions**, then **Create New Condition (Advance Option)**

   v. From the Conditions pane, click the **Select Attribute** dropdown to open the **Dictionaries** window

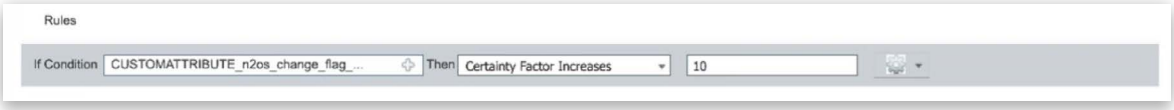
   vi. Use the **Dictionaries** window to select **CUSTOMATTRIBUTE > n2os_change_flag**.



vii. In the **Expression** field, select operator as **EQUALS**, then set the match value to **change.**



viii. From the **Rules > If Condition**, select the **Then** condition as **Certainty Factor Increases**, with a value to **10**.



b. **Profiling Policy 2** - To be applied when the change flag is in its **Done** state

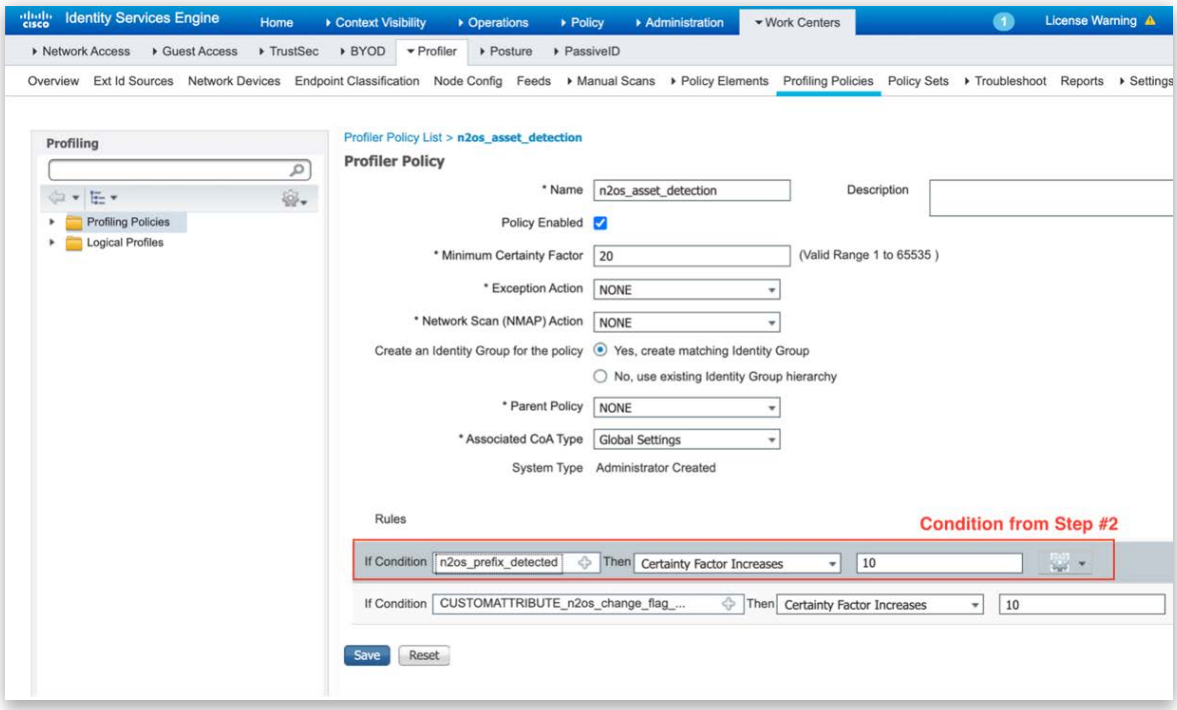
   i. Name: **n2os_asset_detection**

   ii. Minimum Certainty Factor: **20**

   iii. Leave all of the following values at their default

   - Policy Enabled: **checked**
   - Minimum Certainty Factor: **10**
   - Exception Action: **None**
   - Network Scan (NMAP) Action: **None**
   - Create an Identity Group for the Policy: **Yes, create matching identity group**
   - Parent Policy: **None**
   - Associated CoA Type: **Global Settings**

   iv. Configure two rules when creating the second Profiling Policy:



Rule 1

- If Condition: **n2os_prefix_detected** (Profiler Condition created earlier, shown above)
- Then: **Certainty Factor Increases**
- Value: **10**

Rule 2

- If Condition: **n2os_change_flag NOTEQUALS change**
- Then: **Certainty Factor Increases**
- Value: **10**

Two Profiling Policies are created so that the Nozomi Networks sourced assets in the Cisco ISE can oscillate between the two policies, which is needed for the Cisco ISE to process the Nozomi Networks Guardian asset updates sent via pxGrid.

Checklist

Confirm that you have performed the steps below to sync Cisco ISE assets with the Nozomi Networks Guardian.

Nozomi Networks Guardian UI

- [ ] Configure the Cisco ISE Data Integration into the Nozomi Networks Guardian

Cisco ISE Dashboard

- [ ] Create the seven (7) Endpoint Custom Attributes
- [ ] Create the Profiler Condition to match assets from Nozomi Networks
- [ ] Create the first Profiling Policy to detect asset changes
- [ ] Create the second Profiling Policy to detect asset changes

SYNC-GUIDE-CISCO-ISE-8.5x11-001