Endpoint Insights Configuration

Last Modified on 07.19.24

Before you can collect warranty information with Endpoint Insights, you'll need to configure some settings in the Recast Management Server interface. You'll assign roles to users and configure a Recast Proxy to collect warranty information .

Once RMS configuration and Agent installation are complete, you can manually kick off a warranty scan on your Recast Management Server's **Warranty** page by clicking **Start EI Warranty Scan**. You can also wait for the scan to run automatically overnight.

NOTE: Recast Agents will take time to deploy and report their data back to the ConfigMgr database. By default, the hardware inventory cycle can take **up to 7 days**. Adjusting the time to install and increasing the frequency of reporting back to ConfigMgr can shorten this delay significantly.

Assign an Endpoint Insights Administrator Role

You can grant users and groups Recast permissions by assigning them a specific role, such as an Administrator role. Your Recast software must be connected to Recast Management Server to set up role-based permissions.

Add Active Directory User or User Group

To add an AD user or user group:

1. In your Recast Management Server, navigate to **Administration** > **Permissions**.

2. In the main window, click **Add User** or **Add Group**.

3. In the window that opens, search for your AD name or AD user group and click the **Add** button.

NOTE: You can include a **wildcard (*)** to facilitate your search.

Wildcard examples:

- **John Connor** returns strings that match exactly
- **John C*** returns strings beginning with 'John C', such as '**John C**onnor', '**John C**onnors', and '**John C**ranston'
- ***Connor** returns strings ending with 'Connor', such as 'John **Connor**' and 'Carol O'**Connor**'
- ***Support*** returns strings that include 'Support' plus whatever is on the left and right, such as 'Customer **Support** Team' and 'Enterprise **Support** Group'

Assign User a Role

A user must be assigned at least one role.

To assign a user an administrator's role:

1. On the **Permissions** page, click the Edit icon to the right of the user.

2. Under **Role Assignments**, select **Administrators**.

3. To limit the user's permissions to a set of devices, enable **Limit this user to specific objects** and select a **Service Connection**.

4. If desired, set a specific **Refresh Interval** for repopulating scopes. A longer interval uses fewer resources but also detects new users and devices less frequently.

5. Click **Save**.

To assign a Right Click Tools role using a role template, see Role Templates for Right Click Tools.

Configure a Recast Proxy for Warranty Information Collection

Setting up a Recast Proxy for warranty information collection in Endpoint Insights involves authorizing the proxy in the Recast Management Server (if necessary) and creating a Recast Proxy route. Routes determine which Recast Proxy runs a Recast action.

A Recast Proxy route sends an action to a service account if:

- The route is assigned a role that has permissions to run the action
- The targets of that action fall within the route's assigned scope

For more information, see Route Types.

Proxy Route Prerequisites:

- Recast Management Server installed with Recast Proxy
- Recast Proxy service account has the required permissions to collect warranty information

To create a Recast Proxy route:

1. In your Recast Management Server, navigate to **Administration** > **Routes**.

2. In the main window, click **Create**.

3. Set the route **Type** to **Recast Proxy**.

4. As **Recast Proxy**, select your service account.
5. Set **Role** to **Administrators**.
6. Click **Create**.
