Ivanti Neurons for Service Mapping

Administrator Quick Start Guide

Table of Contents

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as “Ivanti”) and may not be disclosed or
copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document, nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.ivanti.com.

Copyright © 2023, Ivanti. All rights reserved.

Rev 04/23

Getting started

Ivanti Neurons for Service Mapping provides visibility into your cloud or data-center network topology, enabling you to view infrastructure relationships, app dependencies, communication flows, and service mappings related to both ITSM and ITOM processes.

> **NOTE**: You can use Ivanti Neurons for Service Mapping as a standalone product or integrate it into your existing Ivanti Neurons for ITSM environment. This guide provides instructions for setting up Service Mapping as a standalone product only. To integrate with ITSM, contact your Ivanti representative.

To get started using Ivanti Neurons for Service Mapping, first review your welcome email from Ivanti containing both the URL to the application website and the temporary credentials for logging in for the first time.

Once you're logged in, you need to configure the application for your environment before using it. The broad steps for doing this are as follows:

- Import CIs in bulk or add them manually to the application.
- Create departments and locations.
- Create user groups and roles and add users to the application.
- Configure the discovery options.

Add CIs to the application

You need to add CI (asset) records to the application, either by importing in bulk or by adding manually. Once the application is set up for your environment, you can also use a discovery scan to add CIs. For details, see the "Add CIs through Auto Discovery" section below.

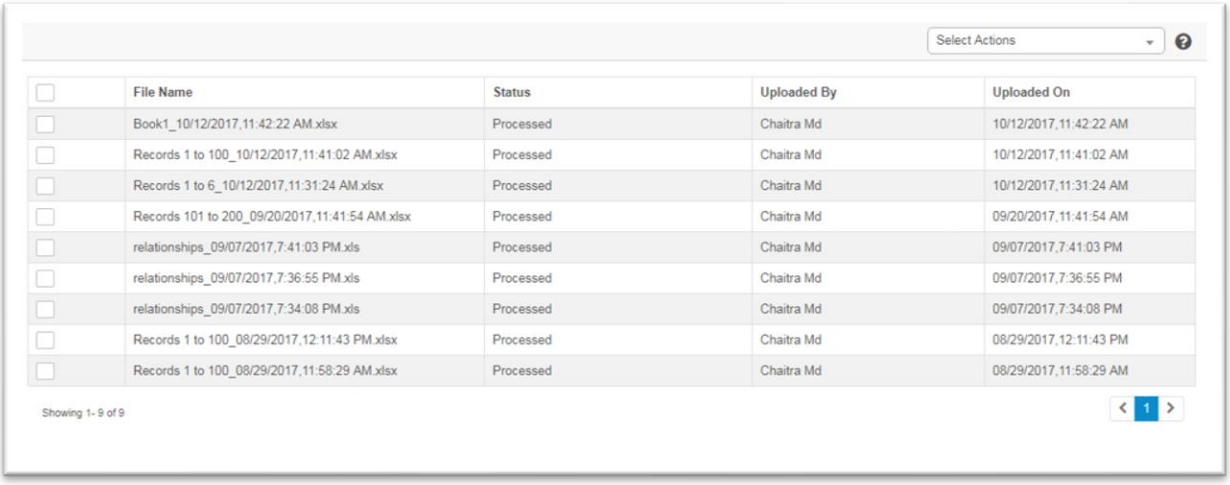
This section also includes procedures for enabling the editing of a CI record, as well as adding an existing property to a CI record.

To import CIs in bulk

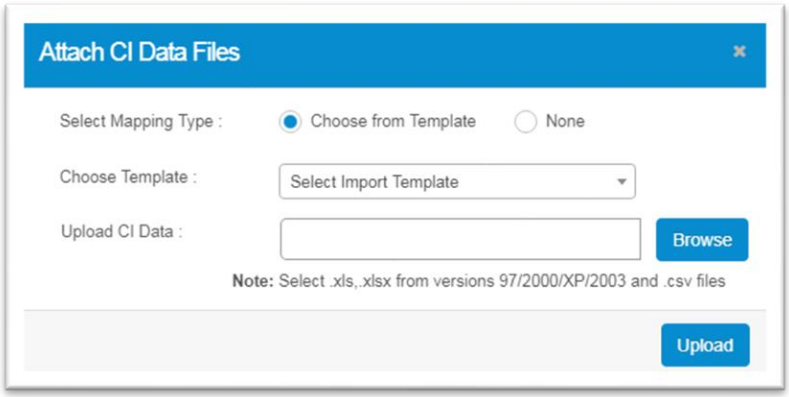
You can import CI record details and relations from .XLS, .XLSX, and .CSV files.

1. In the left navigation pane, click **Discovery Scan > Import Data Files**.

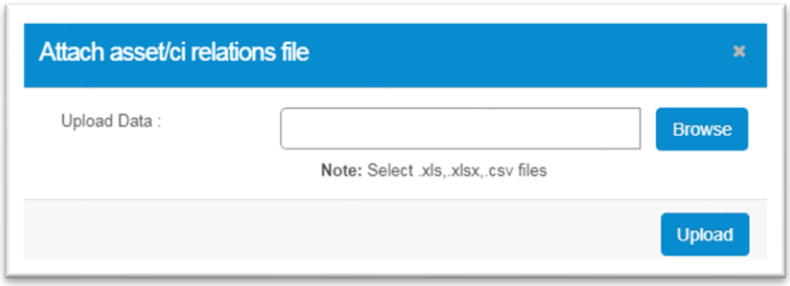
   Note that after the data file is uploaded, you'll see the name of the uploaded file, the current status of the file, the name of the user who uploaded the file, and the data and time of the upload. Click the file in the list to see the imported CI records.



2. To upload a data file containing CI details:
   - From the **Select Actions** drop-down, select **Import CIs**. The Attach CI Data Files dialog displays.



   - Select the required type of mapping. If the mapping type is **Choose from Template**, also select the relevant template from the **Choose Template** drop-down.
   - Click **Browse** to select the file, then click **Upload**.
3. To upload assets and the relationship between two CIs from a data file:
   - From the **Select Actions** drop-down, select **Import Asset/CI Relations**.

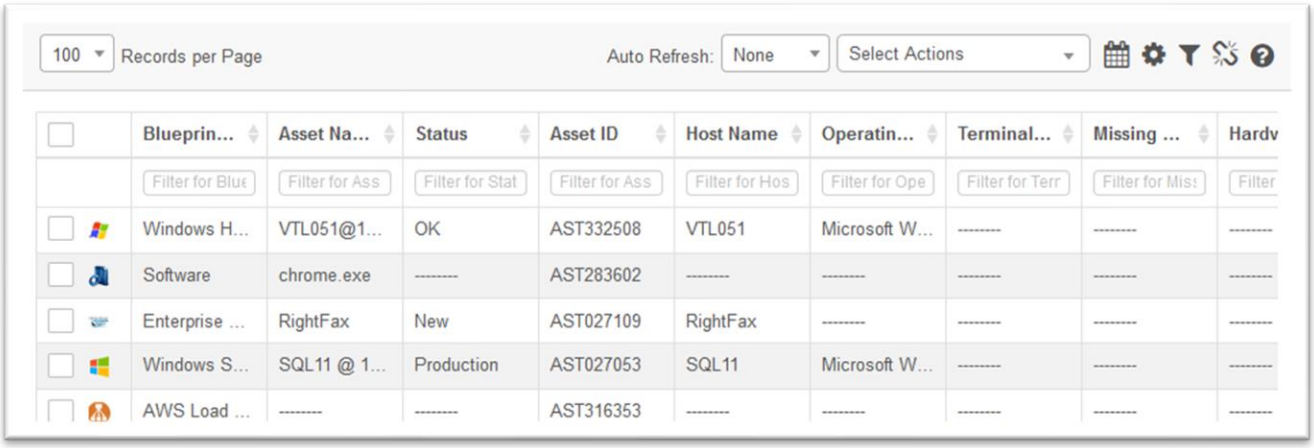


   - Click **Browse** to select the file, the click **Upload**.

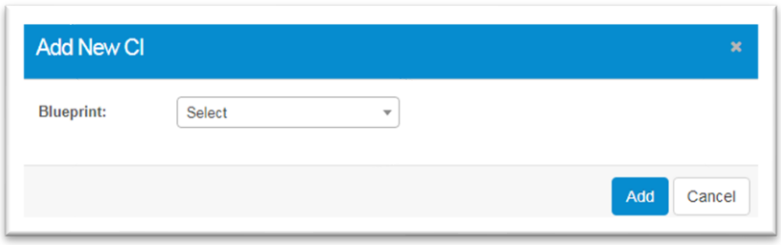
To add new CIs manually

You can add new CI records manually without importing via a data file or performing a discovery scan.

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.



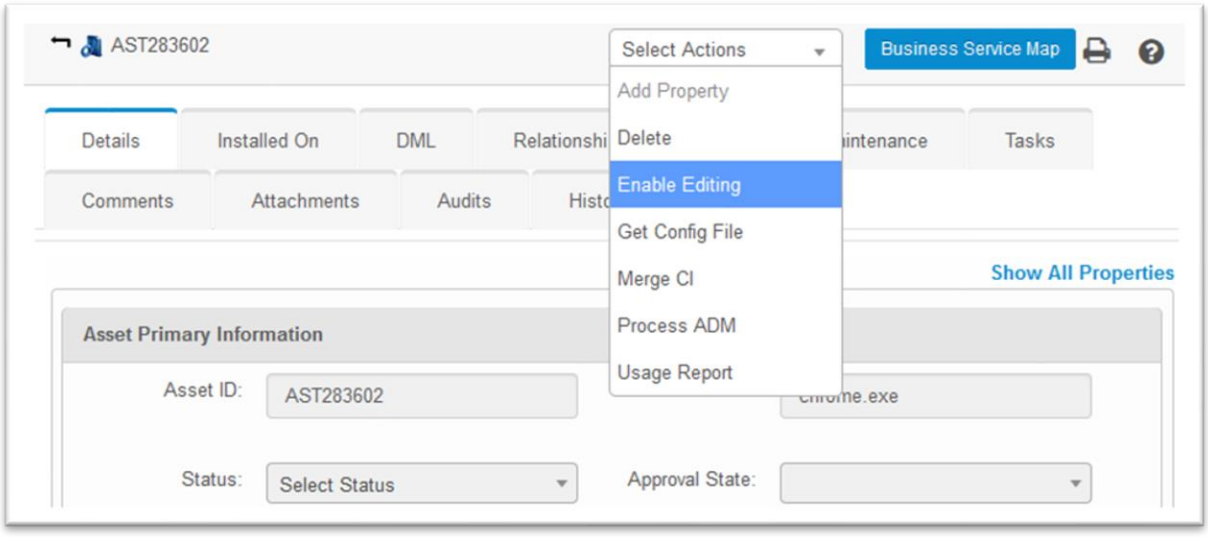
2. From the **Select Actions** drop-down, select **New**.
3. Select the required **blueprint**, then enter the appropriate values for this blueprint type. Note that parameters display according to the selected type. A notification email is sent to the configured user regarding the CI creation.



To enable editing for CI records

You can edit CI records to update the properties, associations, relationships, etc. When a CI is moved to the CMDB, the edit feature is disabled, so you must first enable the editing function.

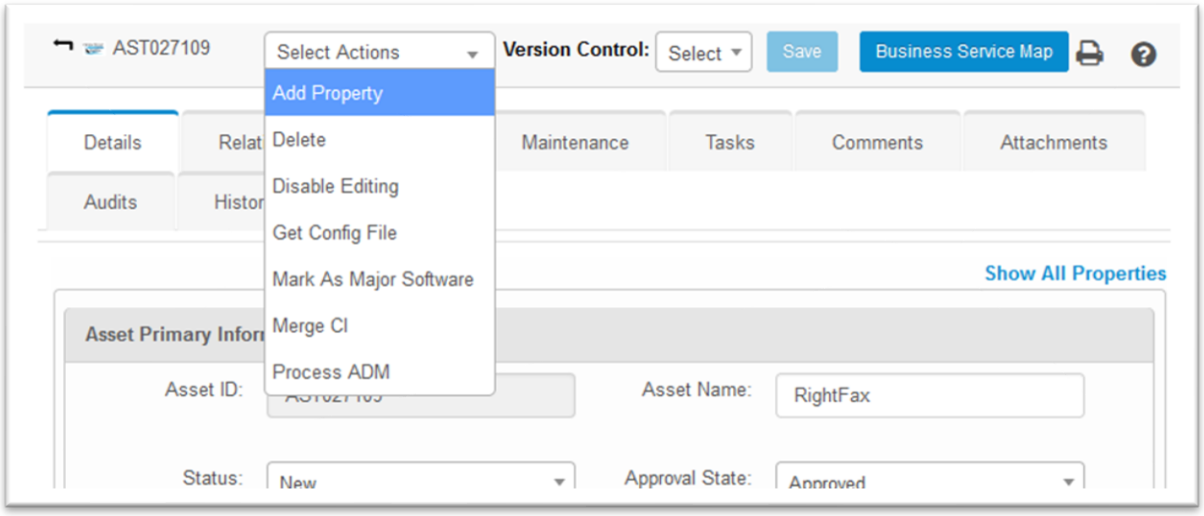
1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. Click the CI record you want to edit.
3. From the **Select Actions** drop-down, select **Enable Editing**, then click **Yes**. This action enables you to edit the CI record's values for its disabled parameters.



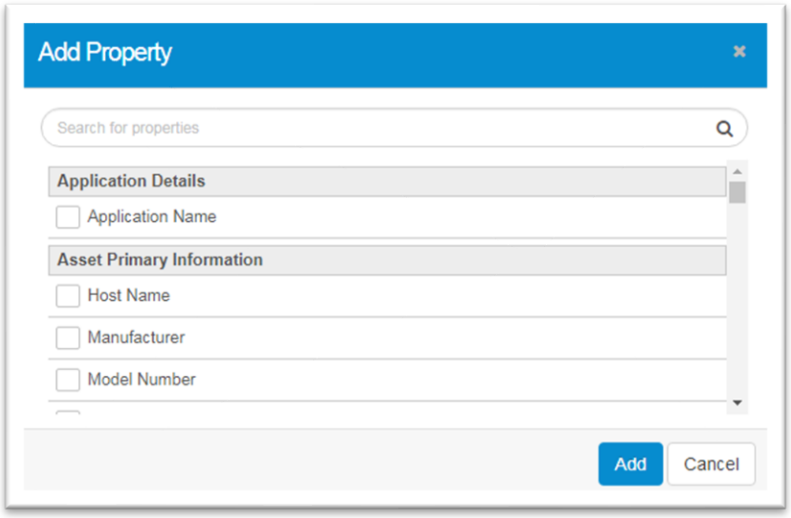
To add an existing property to a CI

You must first enable editing for a CI record before you can add a property. For details, see the procedure above.

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**. The Configuration Items page displays.
2. Click a CI record to open it.



3. From the **Select Actions** drop-down, select **Add Property**.



4. Search for the required property or scroll down the list and select it.
5. When finished, click **Add**.

Create departments and locations

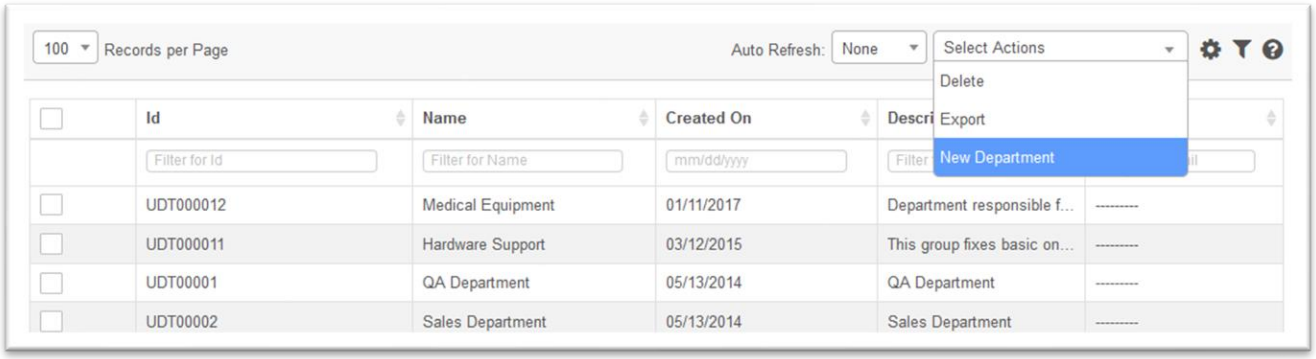
There are several organizational details you need to set up for use within the application—these include departments and locations.

This section also describes how to associate a location with both a CI record and a discovery scan.

To add a department

Use departments to categorize users, groups, and assets.

1. At the top-right corner of the page, click **Admin**. Under the **Organizational Details** heading, click the **Departments** icon. The Departments page displays.

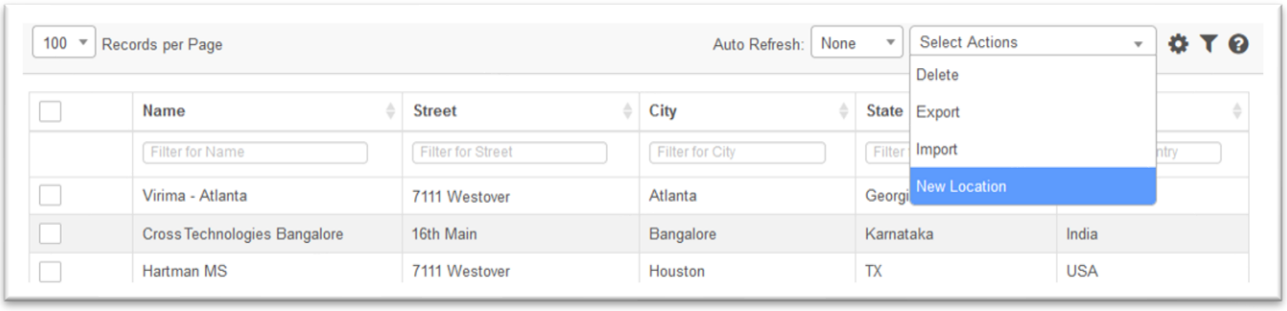


2. From the **Select Actions** drop-down, select **New Department**.
3. Enter the department **name**, a **description** that includes relevant information about the department, and the **email** address of the department. Click **Add**.

To add a location

Add locations to the system, which you can then associate with your CIs and discovery scans.

1. At the top-right corner of the page, click **Admin**. Under the **Organizational Details** heading, click the **Locations** icon. The Locations page displays.

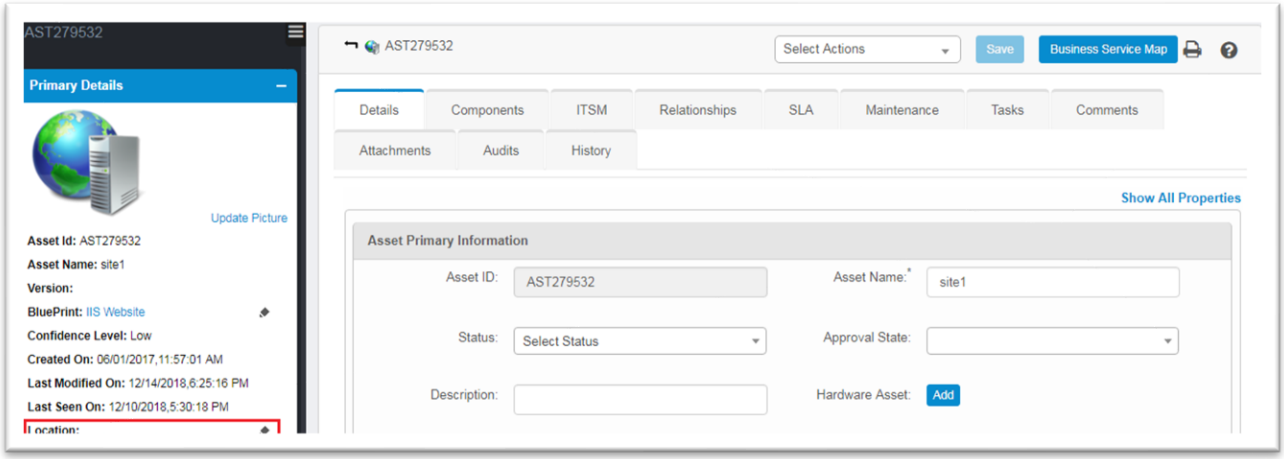


2. From the **Select Actions** drop-down, select **New Location**.
3. Enter the location **name**, a location **type**, the entire **address**, a **contact number**, and **email** address.
4. When finished, click **Add**.

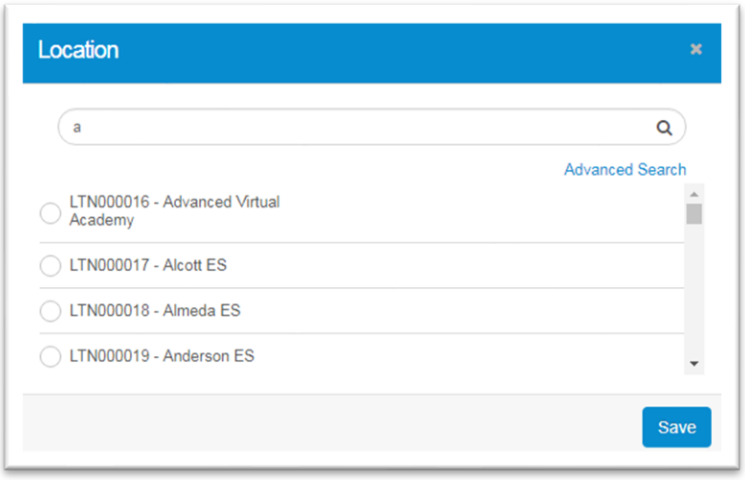
To associate a location with a CI manually

You must first enable editing for a CI record before following this procedure. For details, see the “Add CIs to the application” section above.

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. Click a CI record to open it.



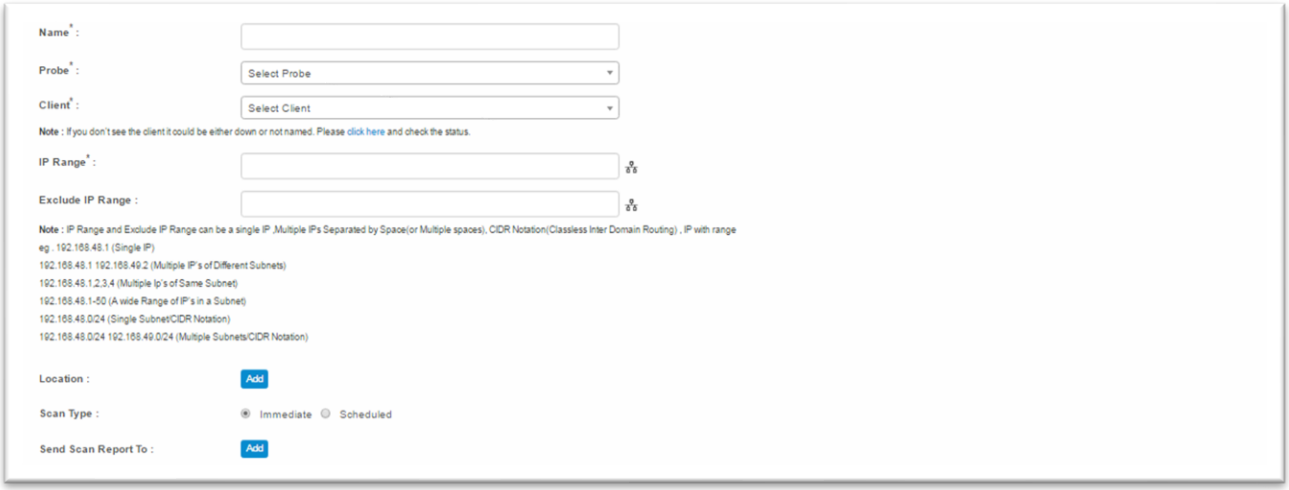
3. Click the **Locations** icon to open the Location dialog.



4. Search for a location, select one from the list, then click **Save**.

To associate a location with a discovery scan

1. In the left navigation pane, click **Discovery Scan > Run a Scan**.
2. Next to **Location** click **Add**, search for the location, select one from the list, then click **Save**.



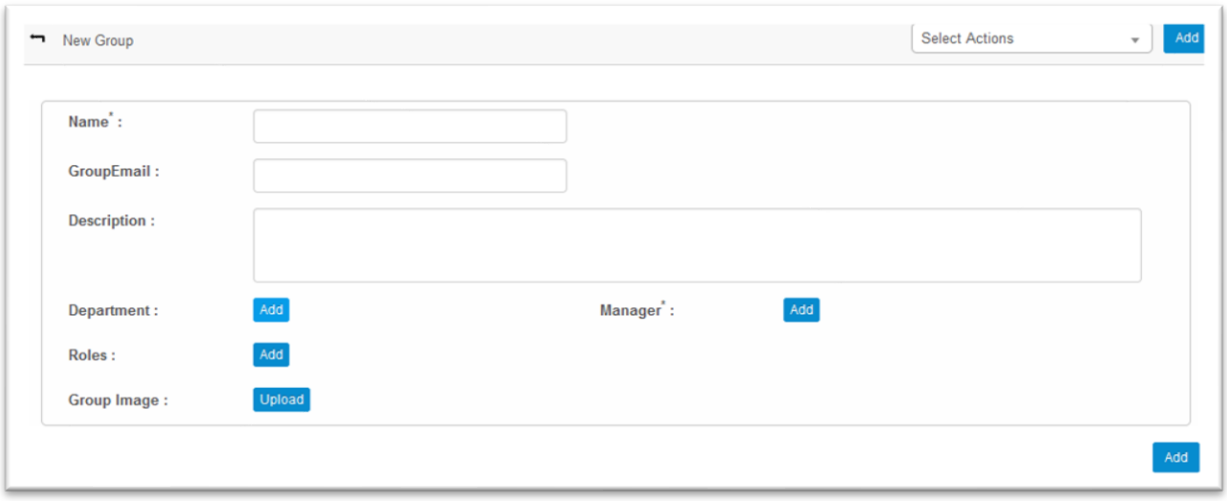
Create user groups, roles, and users

You need to set up user groups and roles for the users who will work within the application. Afterward, you need to select the user-role access to each module. Finally, you can add new users.

To create a user group

1. At the top-right corner of the page, click **Admin**. Under the **Users** heading, click the **User Groups** icon.

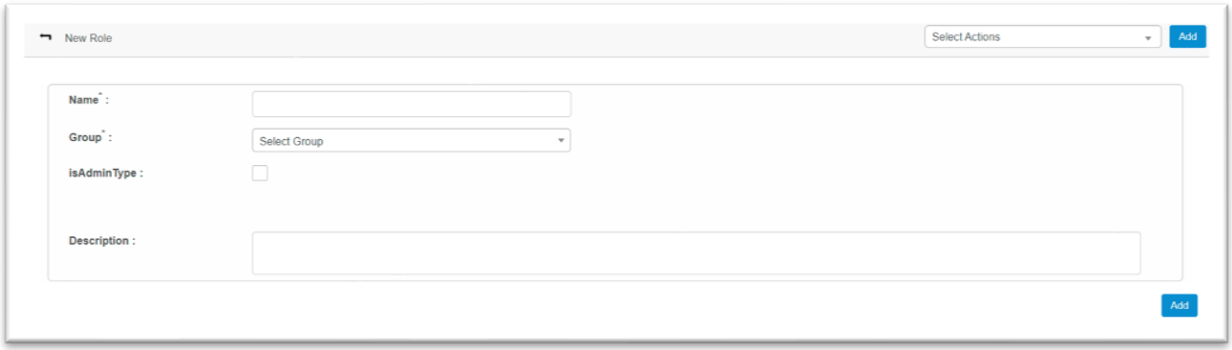
2. From the **Select Actions** drop-down, select **New Group**. The New Group page displays.



3. Enter a **name** for the new group, the group **email** address, and the group's **manager**.
4. Click **Add**.

To create a user role

1. At the top-right corner of the page, click **Admin**. Under the **Users** heading, click the **User Roles** icon.
2. From the **Select Actions** drop-down, select **New Role**. The New Role page displays.

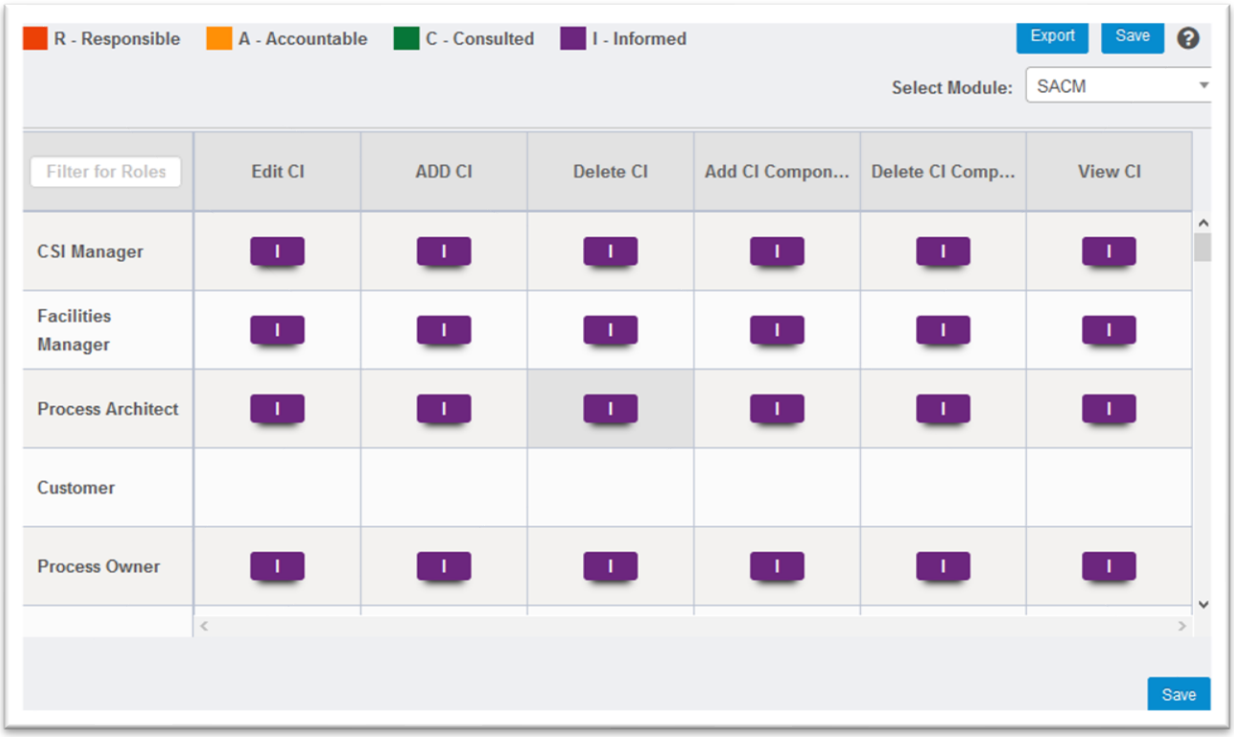


3. Enter the **name** of the new user role and associate it with a user **group**.
4. Enter a **description** of the role, as well as the assigned **module**.
5. Click **Add**.

Once a role is added, you must then configure a RACI matrix for each module to give read/write permissions to the users with that role. For details, see the next procedure.

To select user-role access to modules

1. At the top-right corner of the page, click **Admin**. Under the **Others** heading, click the **Role Access** icon.



2. From the **Select Module** drop-down, select a module.
3. In each provided privilege box, select the appropriate user-role access. Available options are color coded along the top of the page.
4. When finished, click **Save**.

NOTE: Click the **Export** button to export and view the configured RACI matrix for a module in Excel file format. An email with the attachment will be sent to the logged-in user.

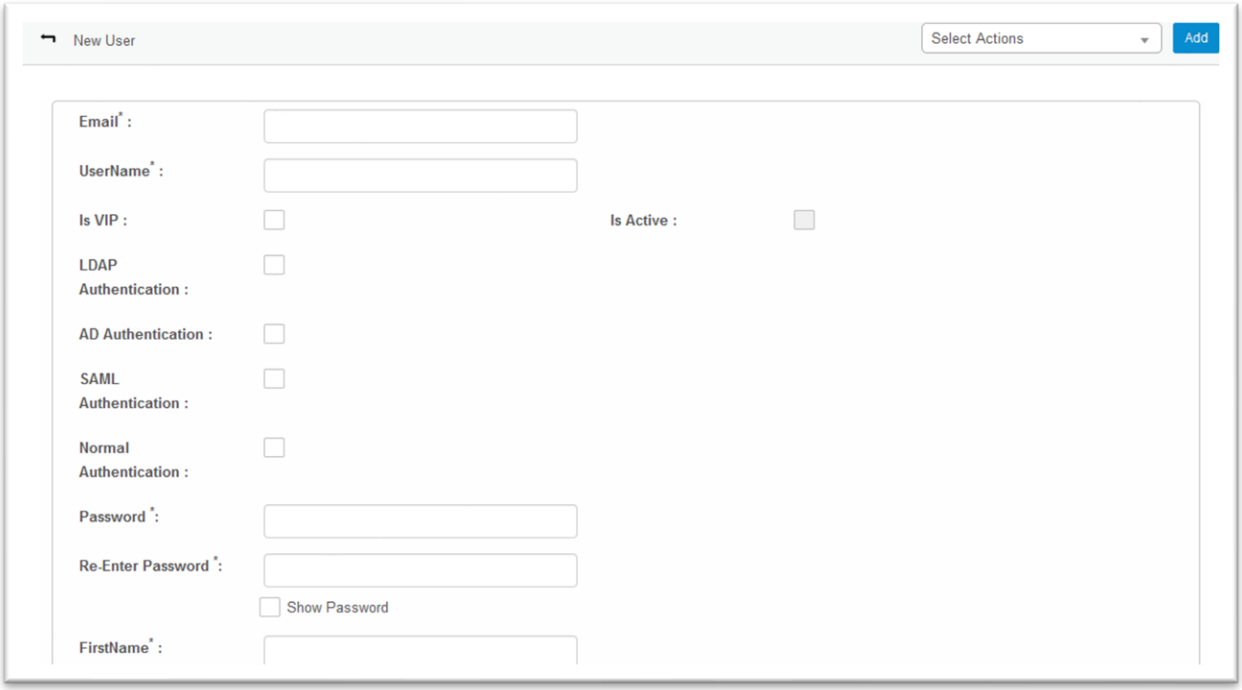
To add a new user

When adding a user, you can also select one or more user roles for them.

1. At the top-right corner of the page, click **Admin**. Under the **Users** heading, click the **Users** icon.

   The Access Management page displays, listing the following information about configured users: email address, username, display name, contact number, name of the associated user role, user status (true or false), and an ID generated by the application.

2. From the **Select Actions** drop-down, select **New User**. The New User page displays.



3. Enter the user's **email** address and their **username** for logging into the application.
4. Select the **Is VIP** option to enable VIP privileges.
5. Select the **authentication** to give the user, then enter those settings. A user can have only one type of authentication. If you don't require authentication, then enter a **password** and share it with the user.
6. Enter the user's **name** and **display name** in the application, as well as their contact information.
7. Add a **location**, **role**, **department**, and **group** for this user. A user can be assigned multiple user roles and belong to multiple groups.
8. Add **report to** information, upload a **profile picture** if needed, and add a **landing page**, which the user will view immediately after login.
9. Select the **language** for viewing the UI.
10. When finished, click **Add**.

Configure discovery options

You can use Ivanti Neurons for Service Mapping in environments that are cloud-only, on-premises, or a combination of both.

For on-premises environments, you must deploy a discovery agent to at least one data center server that will conduct a "probe" or discovery scan for other devices on the network and begin mapping the relationships. For instructions on how to deploy the discovery agent, contact your Ivanti representative.

You can also view and edit discovery options for each client (which is the server that has the discovery agent installed) and add new client credentials that will be used during the scan.

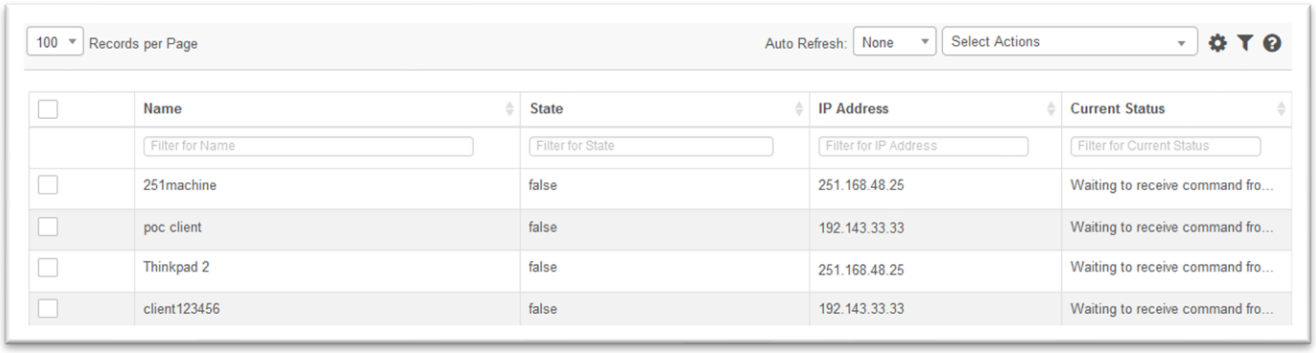
For cloud-only environments, APIs do the discovery work by default, so no agents are required.

To edit client discovery options

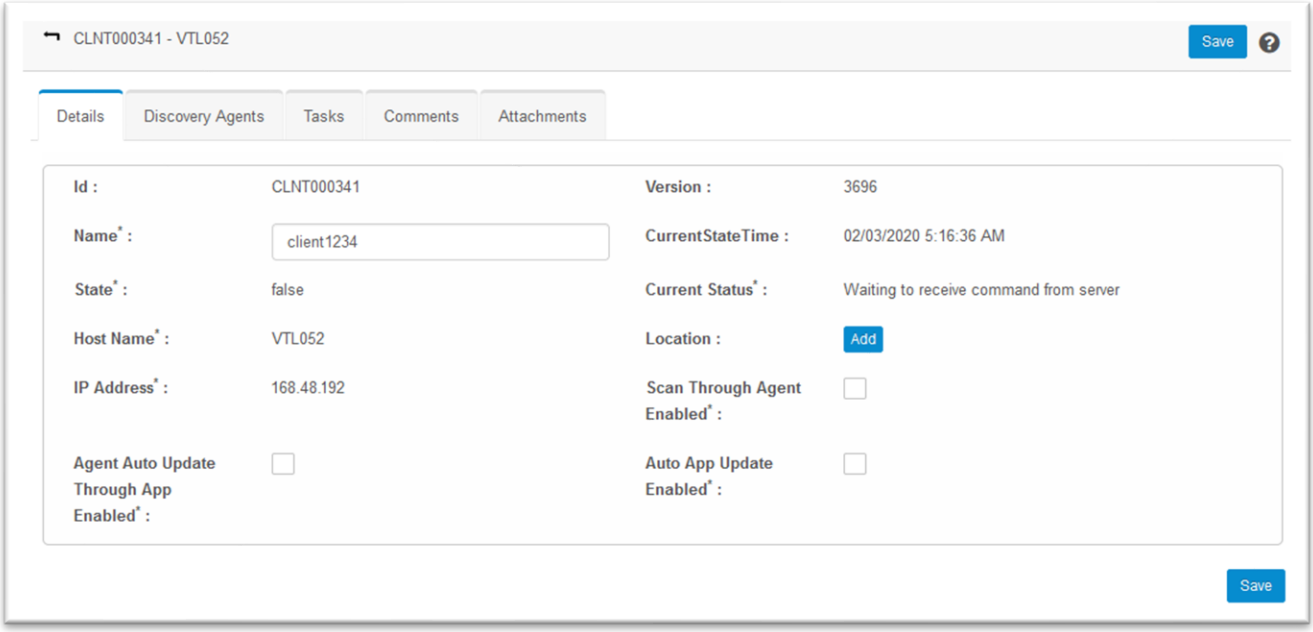
The discovery agent discovers each client host's communication method within your enterprise network. If you have multiple data centers in different locations, the discovery agent must be installed on one server at every data center.

1. At the top-right corner of the page, click **Admin**. Under the **Discovery** heading, click the **Client** icon. The Client page displays.

   The **state** of the client can be **false**, meaning the discovery agent isn't currently functional, or **true**, meaning the agent is functional.



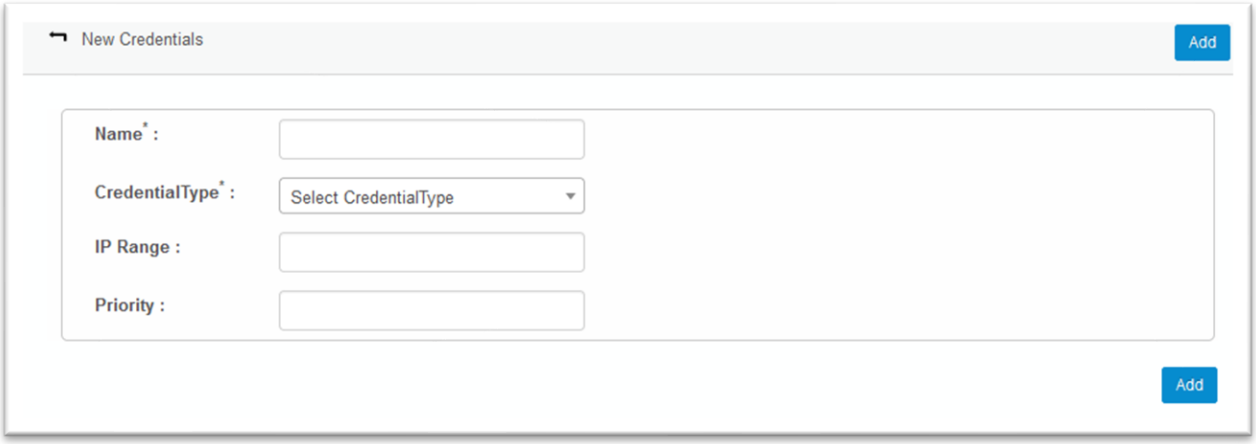
2. Click a client in the list to view and modify its details. If a **location** is absent, click **Add** to provide one.
3. When finished, click **Save**.



To add a new client credential

You must define the authentication of servers and other network components in your monitored network environment to confirm their identity.

1. At the top-right corner of the page, click **Admin**. Under the **Discovery** heading, click the **Credentials** icon.
2. From the **Select Actions** drop-down, select **New Credentials**. The New Credentials page displays.



3. Enter a **name** for the credential and select the required **type** from the Credential Type drop-down.
4. Optional settings include the IP range and priority.
5. Click **Add**.

Setting up an enterprise service map

An enterprise service is a type of blueprint within the application. Blueprints are CI categories that define the overall type and structure of a CI and include its properties. (An “enterprise service” may also be known as a business service or enterprise application.)

The only difference between an enterprise service and a regular application that runs on a host is the scale of applicability. Any application that serves as a front-end for other departmental users or external users can be termed an “enterprise service.”

This section outlines how to set up an enterprise service map and associate all of its dependent resources such as hardware, software, and any other supporting infrastructure.

The broad steps for setting up an enterprise service map are these:

- Identify the enterprise service.
- Create the CI blueprint types. Blueprints are CI categories that define the overall type and structure of a CI and include its properties.
- Add an enterprise service CI to the CMDB.
- Identify underlying assets and their IP addresses.
- Add CIs through Auto Discovery.
- Create the CI relationships.
- Add the relationships between the enterprise service and the associated CIs.
- Tag the CIs, which is the best way of identifying a CI’s relationship to a service.

Identify the enterprise service

An enterprise service can be identified by the common name used in your company for an enterprise application (for example, RF Cloud).

As this is an abstraction of the existing application, you’ll need to add this CI manually into the application as explained in the “Add an enterprise service to the CMDB” section below.

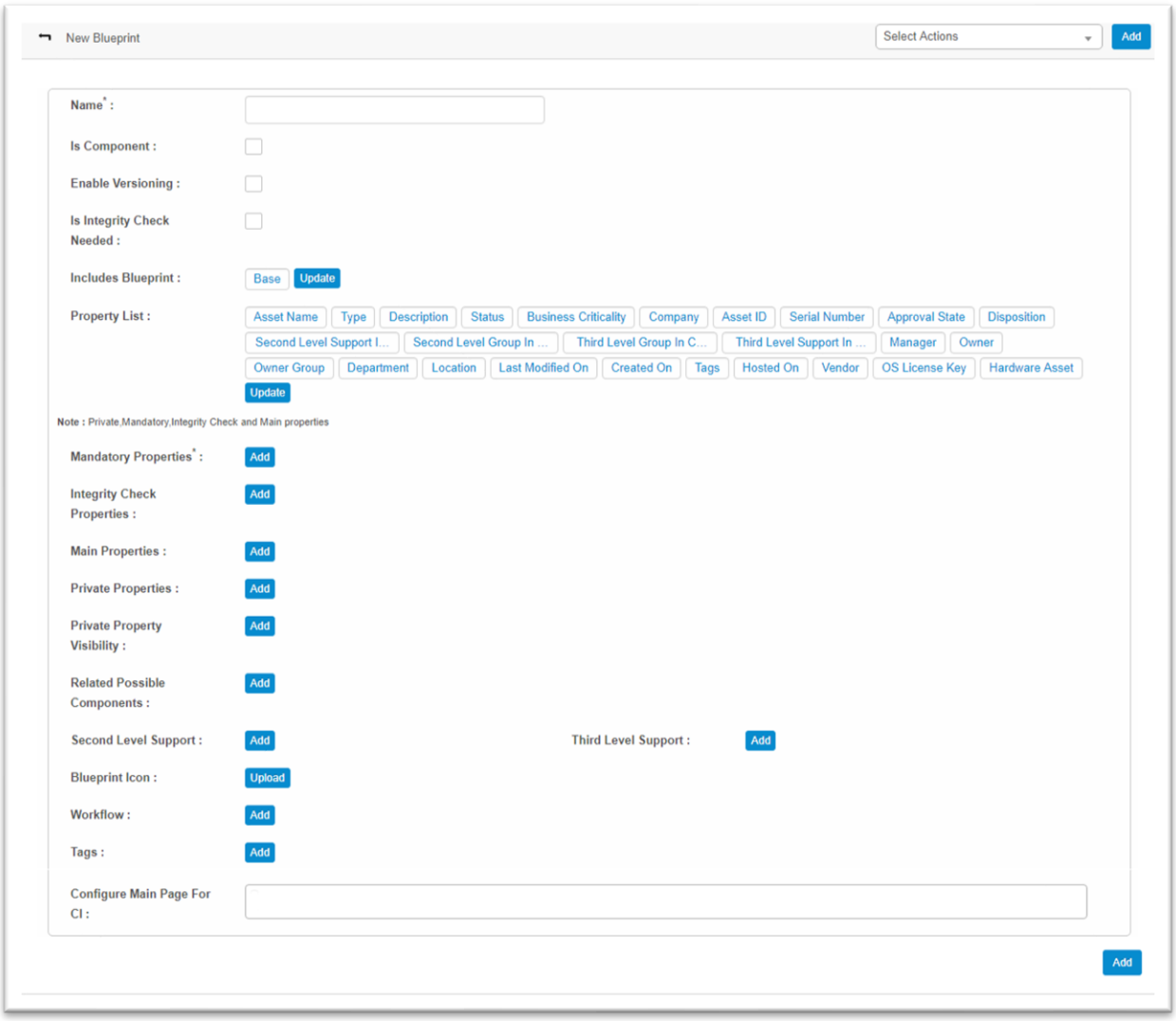
Create the CI blueprint types

You need to create the blueprint types for the CI records, which define the overall type and structure of a CI, including its properties.

This section also includes a procedure for adding new properties to an existing blueprint.

To create a new blueprint

1. At the top-right corner of the page, click **Admin**. Under the **SACM** heading, click the **Blueprints** icon. The Blueprints page displays.
2. From the **Select Actions** drop-down, select **New Blueprint**. The New Blueprint page displays.



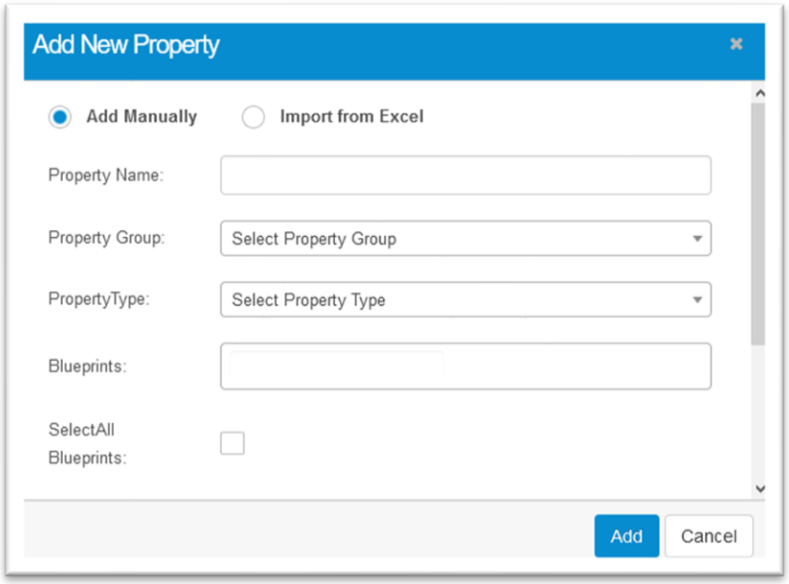
3. Enter a **name** for this blueprint based on the nature of the CI.
4. Select the **Is Component** option if the blueprint will be part of the main CI. Note that this component will be displayed during CI configuration.
5. Select the **Enable Versioning** option to turn on version control. This option updates the blueprint version automatically when you update an associated CI with the status of “Production.”
6. Select the **Is Integrity Check Needed** option to ensure that the corresponding properties are present in the CI. In case of absence, a notification will be sent to the configured user.
7. Click **Update** to include new blueprints that are absent in the base.
8. From the given **property list**, click **Update** if you want to add new properties to the list.

9. Click **Add** to update the values of the following parameters:
    - **Mandatory Properties**: Properties that will be the mandatory fields when adding a new CI to this blueprint.
    - **Integrity Check Properties**: These properties are mandatory if the **Is Component** option is enabled.
    - **Main Properties**
    - **Private Properties**: Properties that are added or marked as private can be viewed only by specified assigned roles.
    - **Private Property Visibility**: Display roles to whom the private properties are visible.
    - **Related Possible Components**: The components of the parent CI. For example, the Network Adapter blueprint is a component of the parent Windows Server blueprint.
    - **Second Level Support**: Configure a user to receive notifications that they can act upon accordingly.
    - **Blueprint Icon**: Click **Upload** to select an image representing the blueprint.
    - **Workflow**: Associate a configured, required workflow for the blueprint. A notification is sent to the configured user when the workflow is triggered.
    - **Tags**: Define a color code for the parent CIs to facilitate an easy search of the corresponding CI/discovered asset existing in the CMDB.
    - **Configure Main Page for CI**: Click in the text box to select the page for the blueprint.
10. When finished, click **Add**.

To add new properties to a blueprint

You can add properties to a blueprint type by creating them manually or by importing from an Excel file.

1. At the top-right corner of the page, click **Admin**. Under the **SACM** heading, click the **Add New Property** icon. The Add New Property dialog displays.



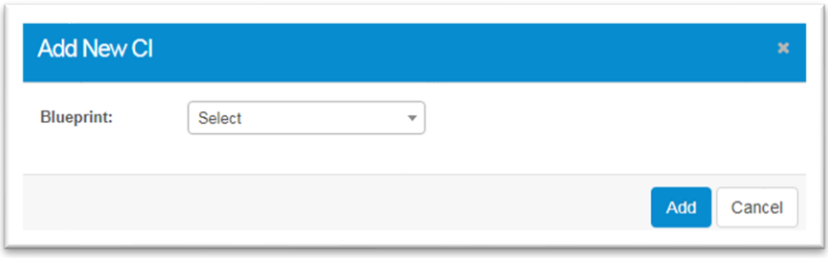
2. To add properties manually:
   - Click the **Add Manually** option.
   - Enter the new property **name**, then select the property **group** and **type** from the drop-downs.
   - Select a blueprint from the **Blueprints** drop-down.
   - Scroll down and select the **Is Mandatory** option to define the property as a mandatory parameter.
   - Click the + icon to save the entered property details.
   - Repeat the above instructions to save more properties.
   - When finished, click **Add**.
3. To add properties by importing from Excel:
   - Click the **Import from Excel** option.
   - Click **Browse** to select an Excel workbook with the property information, then click **Upload**.

Add an enterprise service CI to the CMDB

You now need to add the new enterprise service CI to the CMDB.

To add an enterprise service CI to the CMDB

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. From the **Select Actions** drop-down, select **New**.
3. From the **Blueprint** drop-down, select the blueprint type, then enter the appropriate values for the selected type.



4. Click **Add**. Note that parameters are displayed according to the blueprint type selected. A notification email is sent to the configured user regarding the CI creation.

Identify underlying assets and their IP addresses

After adding the enterprise service, you need to identify the IP addresses of the underlying infrastructure items such as physical servers, workstations, routers, web servers, etc. that are associated with that service. If you do not have this information, contact the support person for the enterprise service. The IP addresses are required for Auto Discovery.

> **NOTE:** If you don't know the IP addresses, there is another way of finding assets related to an enterprise service based on the name of the process or Windows service. This procedure is explained in the "Tag the CIs" section below.

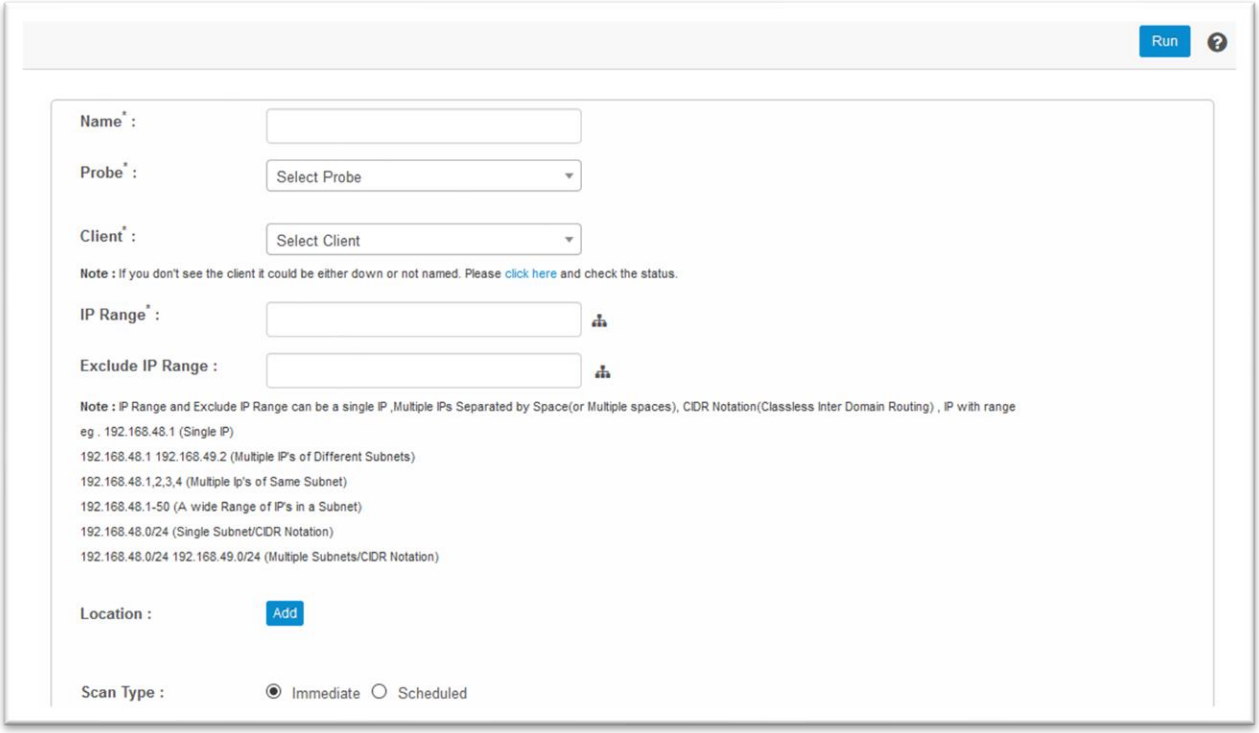
Add CIs through Auto Discovery

You can use Discovery scanning to populate your CMDB. Discovery scans search the network for all attached computers and devices, then populate the CMDB with information about each device's configuration, provisioning, and status. Discovery also reports on any software that is running (Software Instances), and the IP connections between the systems, thereby establishing their relationships.

To run a discovery scan

This feature enables you to identify the devices that are connected and communicating within a network environment. Discovery identifies device types, the host name, and other relevant information of the device based on the probe selected for the scan. Discovery also provides an option to schedule scans.

1. In the left navigation pane, click **Discovery Scan > Run a Scan**.
2. Enter a **name** for the scan.



3. From the **Probe** drop-down, select the required probe for the scan. To define a certificate scan, do the following:
   - From the **Probe** drop-down, select **Certificate Scan**.
   - From the **Client** drop-down, select the name of the client, then enter the **certificate path**.
   - In the **IP Range** box, enter the IP address range to be included in the scan.
   - In the **Exclude IP Range** box, enter the IP address range to be excluded from the scan.
   - Click the icon to scan the entire subnet mask of the corresponding IP addresses.
   - The default **scan type** option is **Immediate**. To schedule a scan, see the next procedure.
   - Click **Add** to update the **location** and to select users to send the **scan report** to.
4. In the top-right corner of the page, click **Run** to execute the scan as configured.

There are several types of scans available, based on your network environment. They include:

- **Deep Host Scan**: Enables you to view entire details of the host including IP address, OS type, MAC address, device basic details, software running instances, etc.
- **Host Type Scan**: Enables you to view the host type present in the network environment.
- **Basic Host Scan**: Enables you to view basic details of a device.
- **Windows Basic AD Scan**: Enables you to view basic details of a device present under an AD server.
- **Windows Deep AD Scan**: Enables you to view basic details of every device present under an AD server with AD structures present under diverse types of hosts in the network environment.
- **IP Connection Scan**: Enables you to view IP connection details.
- **Website Discovery**: Enables you to view web URL inputs and relevant information.
- **Port Scan**: Enables you to ping the existing ports in the network environment.

- **Medical Device Scan**: Enables you to view details of medical devices present in a monitored network environment.

Upon a successful scan, the results are displayed on the **Discovery Assets** page. In the left navigation pane, click **Discovery Scan > Discovered Assets** to see the results.

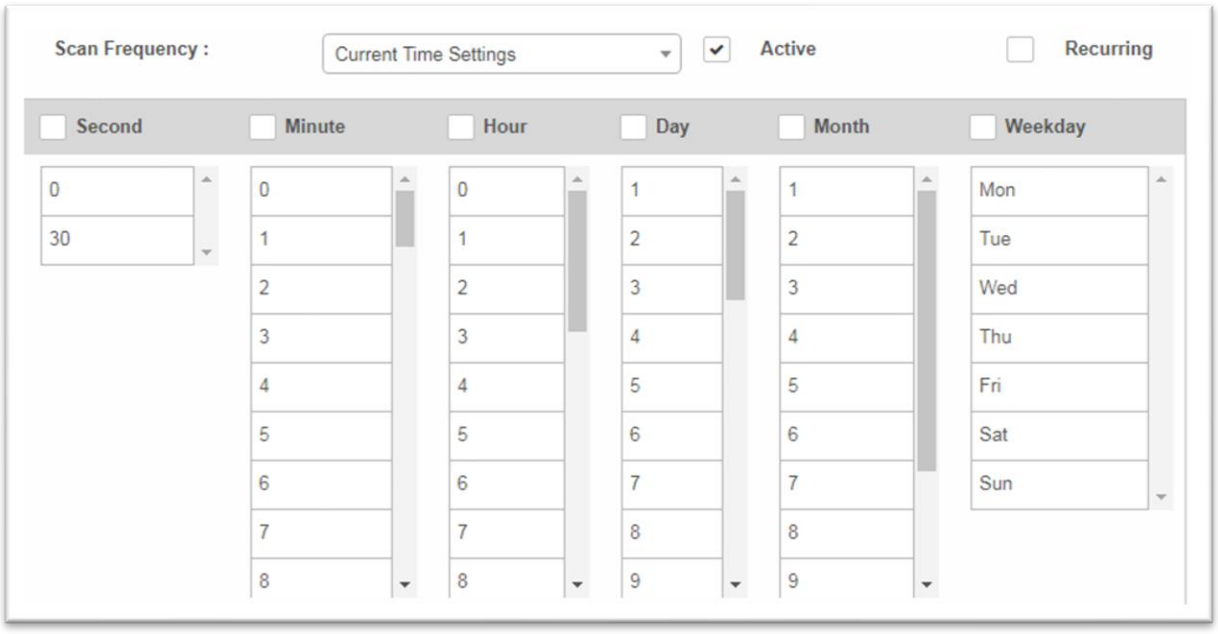
The following actions can be performed on discovered assets:

- **Delete**: Delete assets from the application.
- **Move to CMDB**: Move assets into the CMDB, where you can perform additional functionalities such as incident management, etc. For details, see the "Move CIs to the CMDB" section below. If you want to integrate with Ivanti Neurons for ITSM, you can view discovered assets from the ITSM console. For more information, contact your Ivanti representative.
- **Re-scan**: Repeat the scan process on the discovered assets.

To schedule a discovery scan

When creating a scan, you have the option to schedule it to recur at certain times.

1. For **scan type**, select the **Scheduled** option.



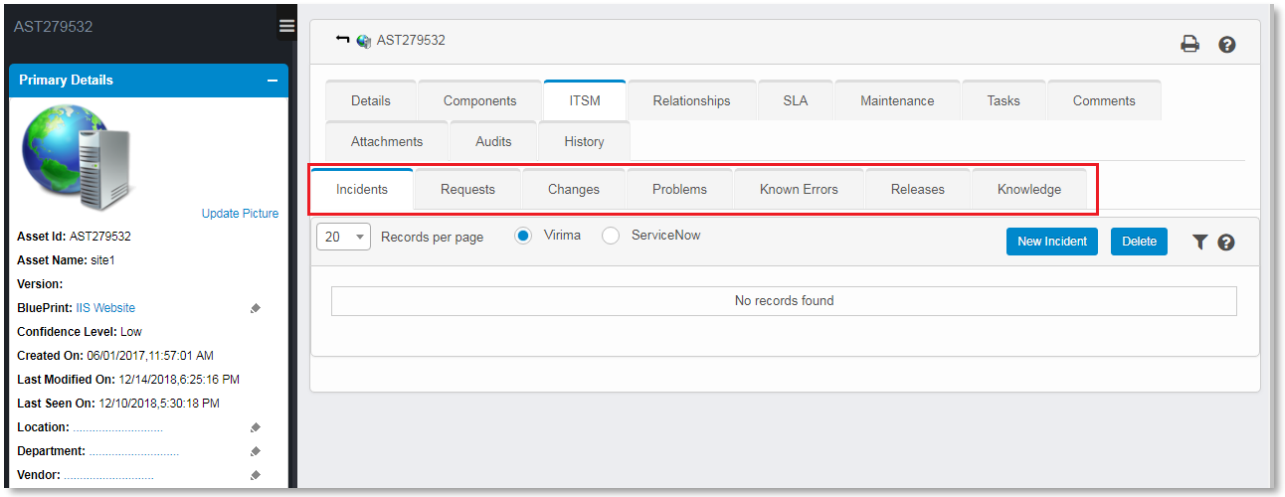
2. From the **Current Time Settings** drop-down, select the scan frequency for executing the scan.
3. Select options for **Active** and **Recurring** (to repeat the scan according to the defined time).
4. Select the time interval option (second, minute, hour, etc.) according to the time selected in the Current Time Setting drop-down.
5. Click **Run** to execute the scan as configured.

Move CIs to the CMDB

Newly discovered CIs must be manually moved to the CMDB before you can proceed with ITSM activities related to:

- Incident management
- Change management
- Problem management
- Knowledge management
- Release management
- Request management

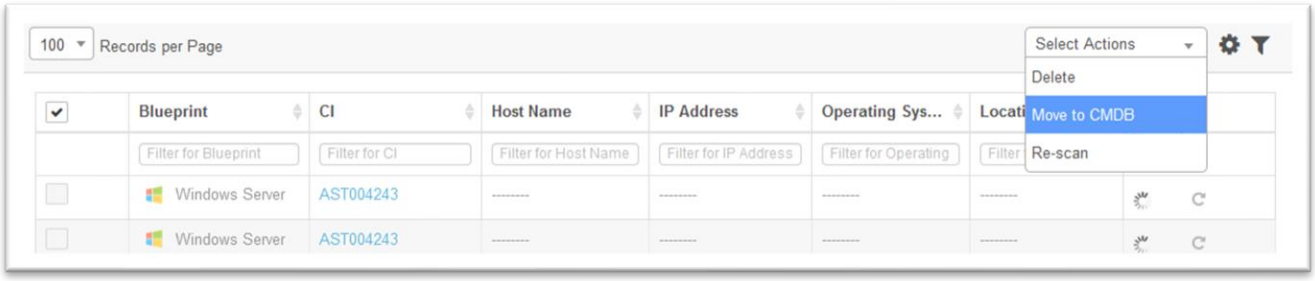
If you're using Ivanti Neurons for ITSM, it's possible to integrate service mapping capabilities into the ITSM console. For more information, contact your Ivanti representative.



Note that you can also use business rules to automatically promote CIs and updates to the CMDB. For details, see the "Business rules" section below.

To move CIs to the CMDB

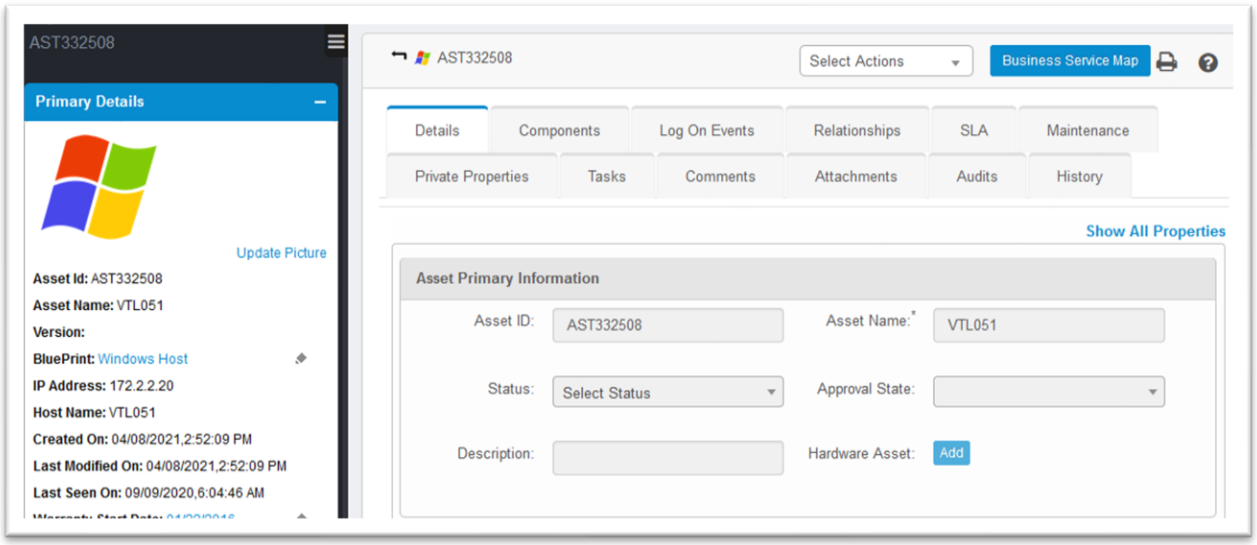
1. In the left navigation pane, click **Discovery Scan > Discovered Assets**. The Discovery Assets page displays.
2. Select individual CIs to move or click the top checkbox to move all of the CIs in the list.



3. From the **Select Actions** drop-down, select **Move to CMDB**.
4. Confirm the action to move the CIs.

Discovered assets that are moved to the CMDB display on the **Configuration Items** page. Navigate to that page by clicking **ITSM > Configuration Management > Configuration Items**.

Click an asset in the list to view its details as shown below:



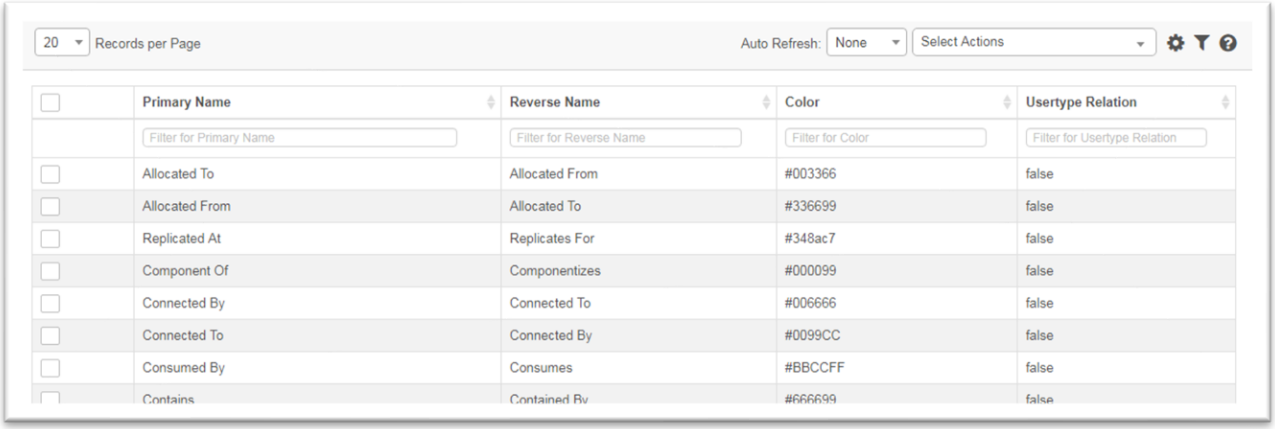
The CI page also includes tabs that provide information related to components, relationships, SLAs, etc.

Create and view CI relationships

You can manually create CI relationships with existing sources and targets. You can then view a graphical presentation of those relationships as part of an enterprise service map.

To create CI relationships

1. At the top-right corner of the page, click **Admin**. Under the **SACM** heading, click the **Relationship Types** icon. The Relationship Types page displays.

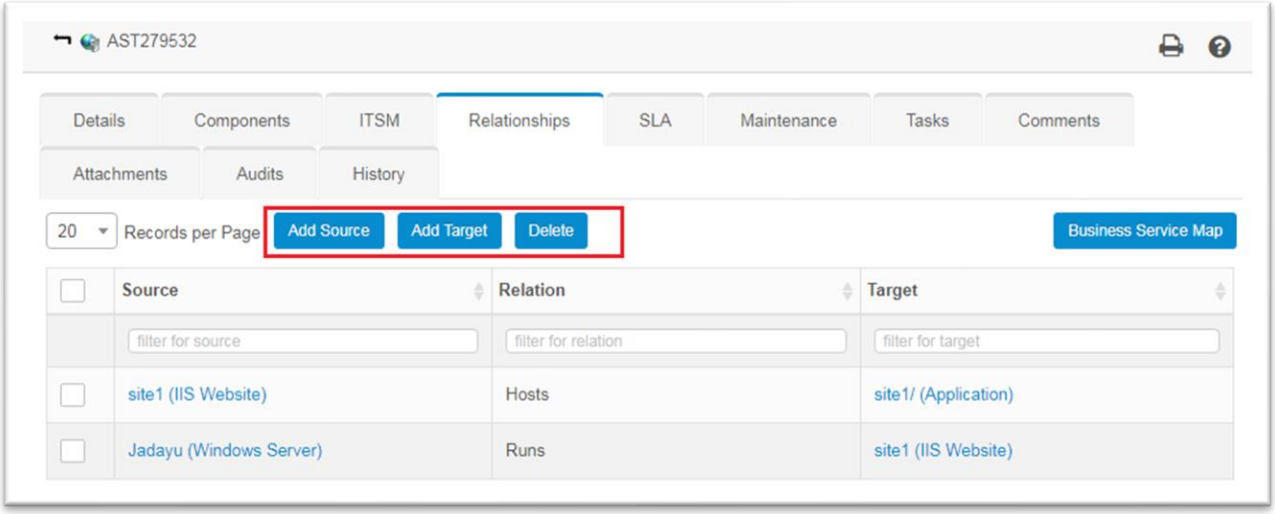


2. From the **Select Actions** drop-down, select **New Relationship Type**.

3. Enter a **primary name**, which defines the relationship from the source to the target.
4. Enter a **reverse name**, which defines the relationship from the target to the source.
5. Set the color to represent the relationship between the source and target and vice versa.
6. Select the **Usertype Relation** option to associate the relationship with the relevant user. If this option is not selected, the corresponding relationship cannot be associated with any user.
7. Click **Add** to update the relationship and display the updates on the Relationship Types page.

To add relationships between the enterprise service and associated CIs

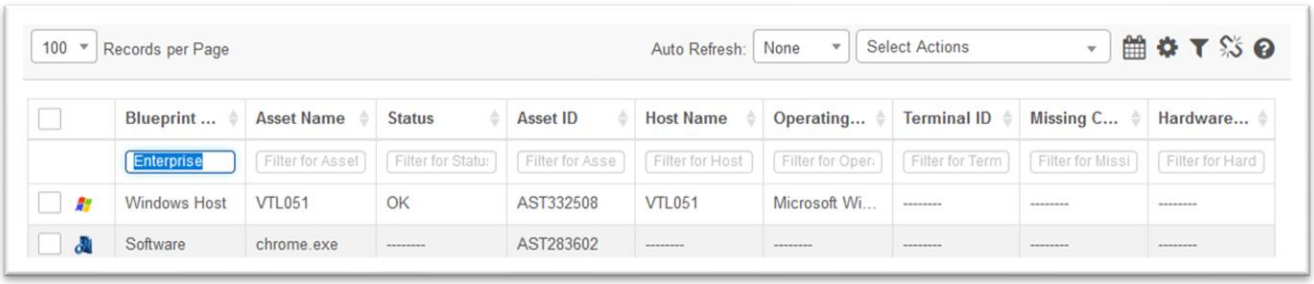
1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. Click a CI in the list to configure the relationship type.
3. Click the **Relationships** tab.



4. Click **Add Source** and/or **Add Target** to configure the relationship type.

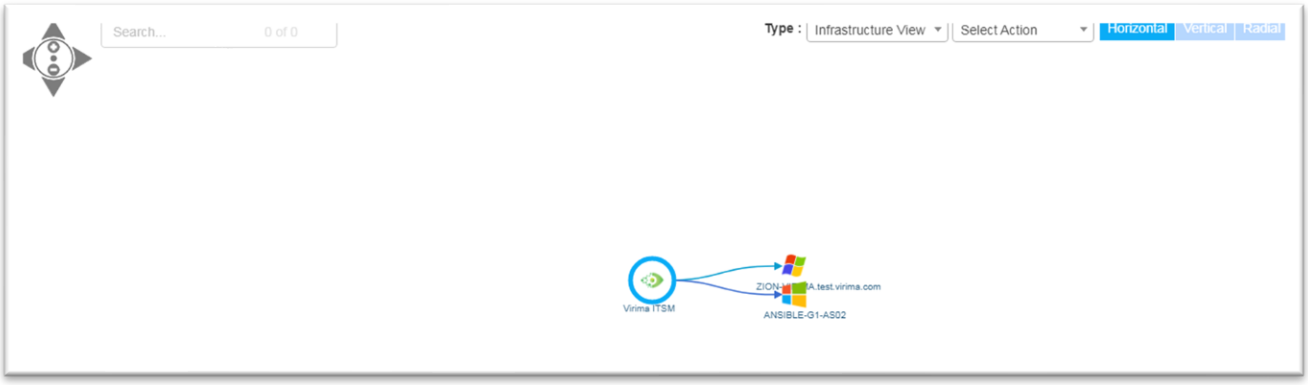
To view the CI relationships in an enterprise service map

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. In the **Records per Page** drop-down, select **All**.
3. In the **Blueprint Name** search box, type **Enterprise** and press **Enter** to display a list of the configured enterprise CIs.



4. Click the required enterprise to view its details.
5. Click the **Relationships** tab, then click the **Business Service Map** button to view the relationship in graphical format in a separate browser window.

A sample enterprise service map looks like this:

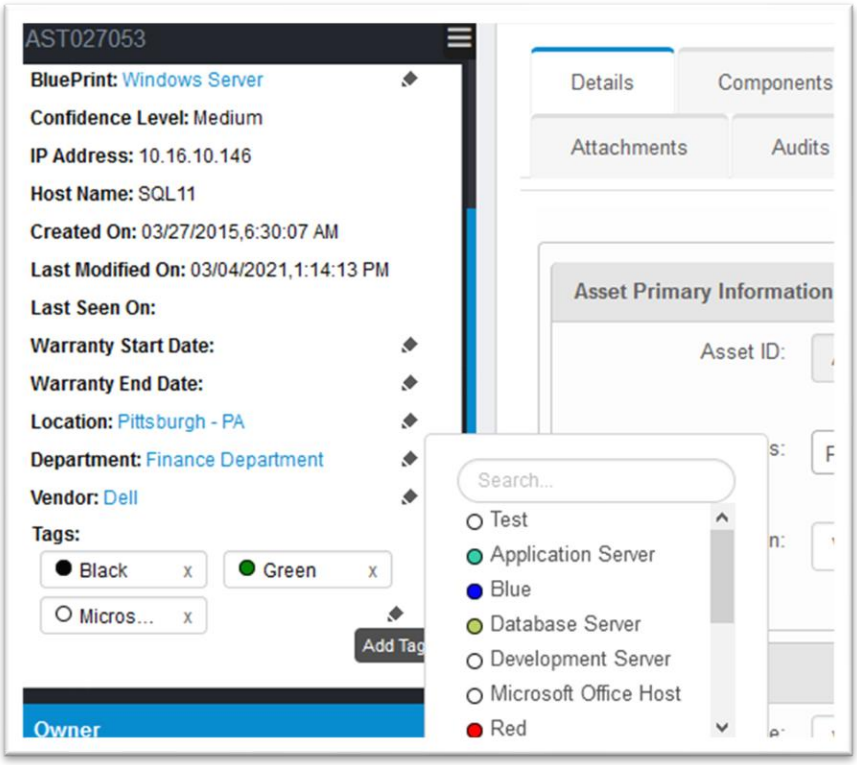


Tag the CIs

A CI can be identified by the unique property information that it contains, such as IP address, host name, etc. The most efficient way of identifying a CI is by using its tags.

To tag a single CI

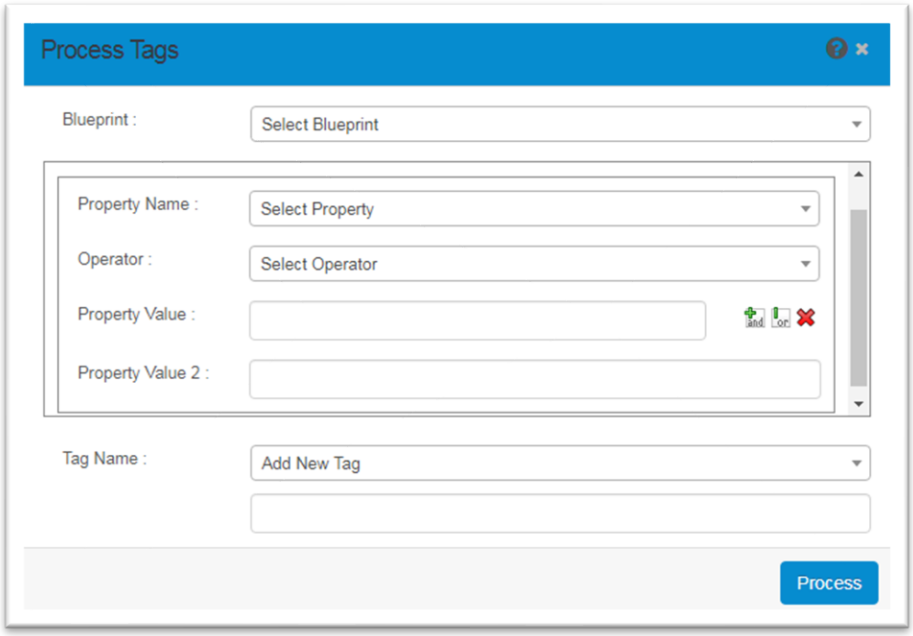
1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**.
2. Click a CI in the list to open the record and configure its relationship types.
3. From the **Select Actions** drop-down, select **Enable Editing**. This enables you to edit the values for the existing parameters of the CI.
4. In the left pane, click the **Add Tag** icon to tag the CI. Enter relevant criteria to search for the required option and/or click the listed option to tag. Click the “x” to remove a tag.



To tag multiple CIs

You can define a tag for identifying CIs according to their process.

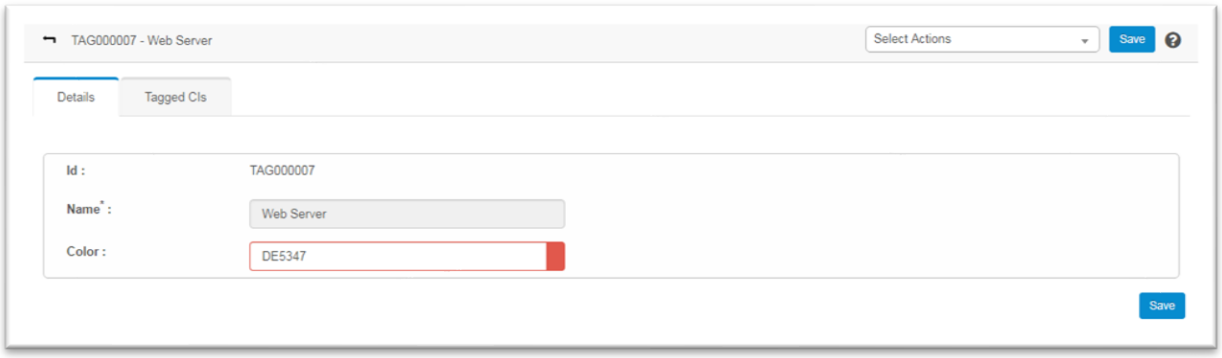
1. At the top-right corner of the page, click **Admin**. Under the **SACM** heading, click the **Process Tags** icon. The Process Tags dialog displays.



2. From the **Blueprint** drop-down, select the required blueprint. The values of the **property name** and **operator** parameters display according to the selected blueprint type.
3. In the **Property Value** boxes, enter values using the  icons as needed.
4. In the **Tag Name** drop-down, select a **name** for the tag. Click **Process**. A notification is sent to the configured user when tag processing is completed.

To view CI grouped tags

1. In the left navigation pane, click **ITSM > Configuration Management > Tags**.
2. Click the configured tag to view the details. The Details CI page displays.



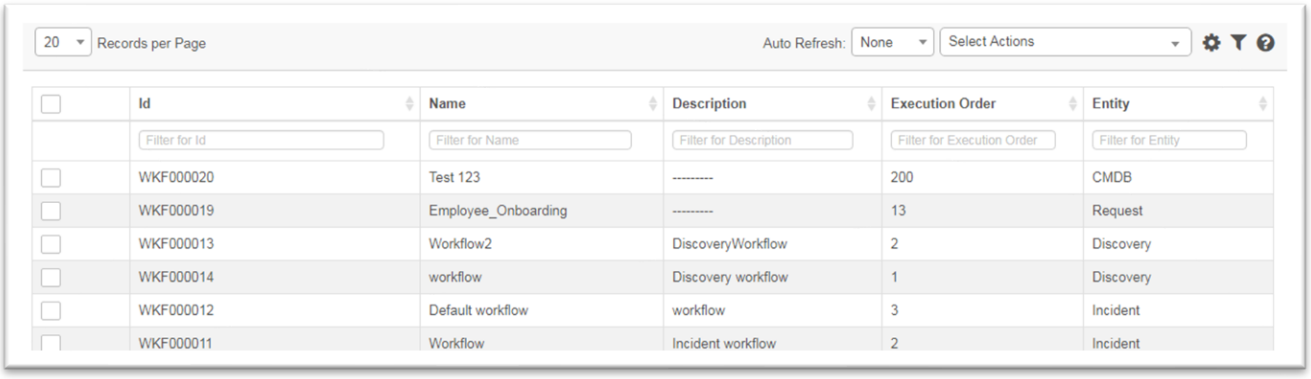
3. Click the **Tagged CIs** tab to view the tag details.

Business rules

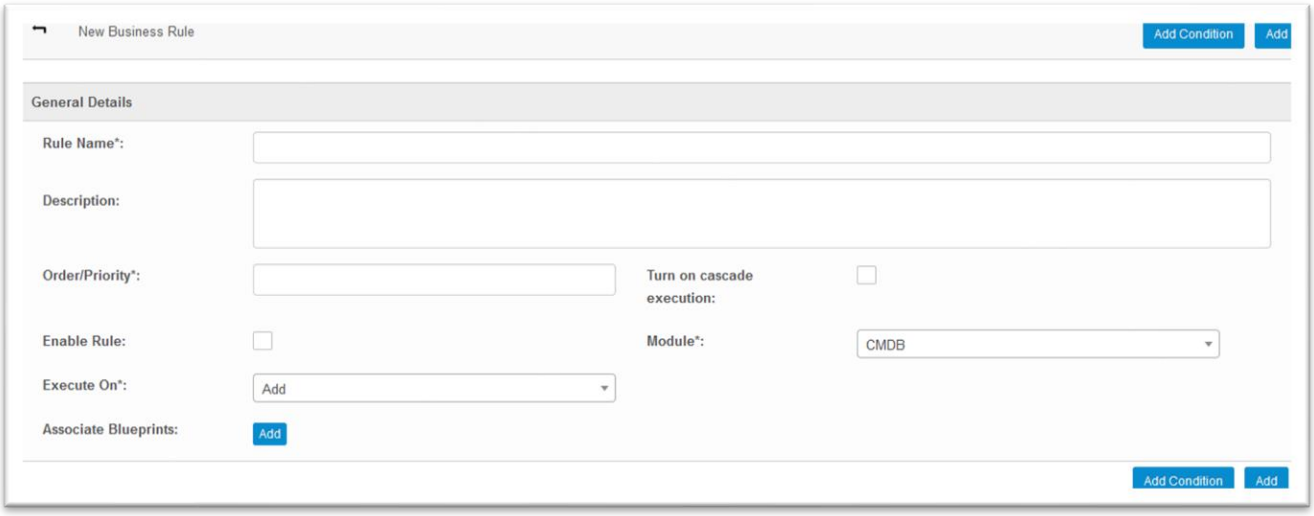
Use business rules to reduce the manual effort of creating/updating records for repeatable actions. For example, you can automate tasks for modifying CI records or creating a new record based on action details when trigger conditions are met.

To create a business rule

1. At the top-right corner of the page, click **Admin**, then scroll down to the **Others** heading and click the **Business Rules** icon. The Business Rule page displays.

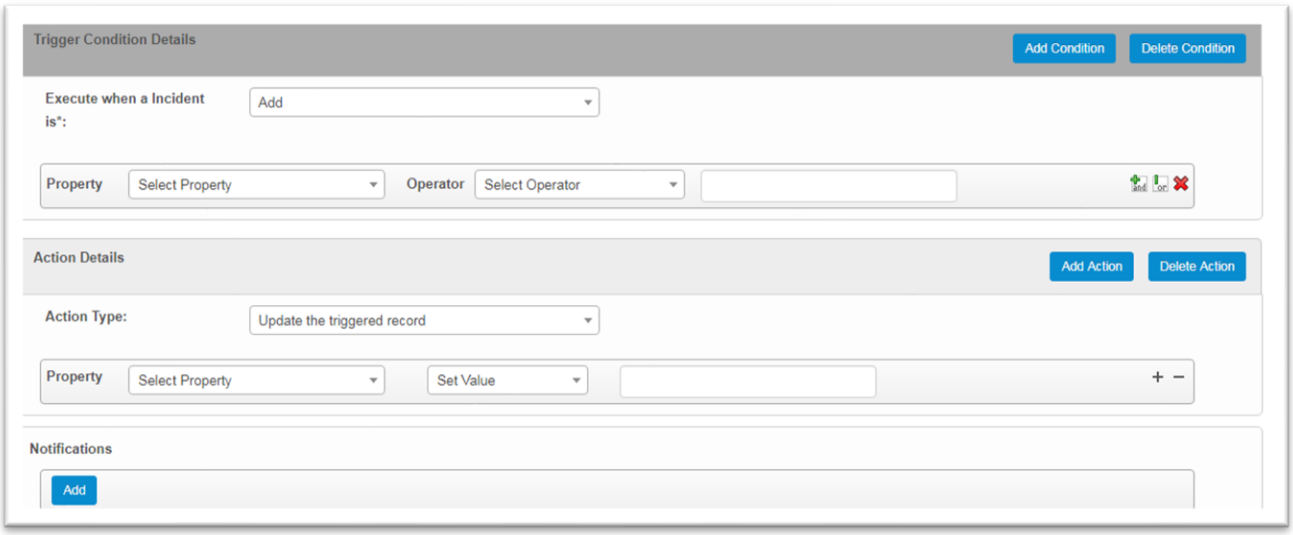


2. From the **Select Actions** drop-down, select **New Business Rule**. The New Business Rule page displays.



3. Enter a **name** for the new rule, as well as a **description**.

4. Enter an **order/priority** number to specify the order of the rules to be executed when there are multiple rules set for the selected module.
5. Select the **Turn on Cascade Execution** option to execute the next enabled business rule based on the order/priority for the same module.
6. Select the **Enable Rule** option to make the rule active.
7. From the **Module** drop-down, select the module for this rule.
8. Select a default for the **Execute on** option.
9. To **associate blueprints** or templates with this rule, click **Add** and select the items.
10. Click the **Add Condition** button.



11. Under **Trigger Condition Details**, select a **property** and an **operator**. Two or more conditions can be combined using the  icons.
12. Click **Add Condition** for each condition you create.
13. Under **Action Details**, select the **action type** to be performed upon triggering the condition.
14. Select a **property** and set a **value** from the drop-downs.
15. Click **Add Action** for each action you define.
16. For **notifications**, click **Add** to send a notification to a user upon triggering a business rule.
17. When finished, click **Add** in the bottom-right corner of the page.

NOTES:

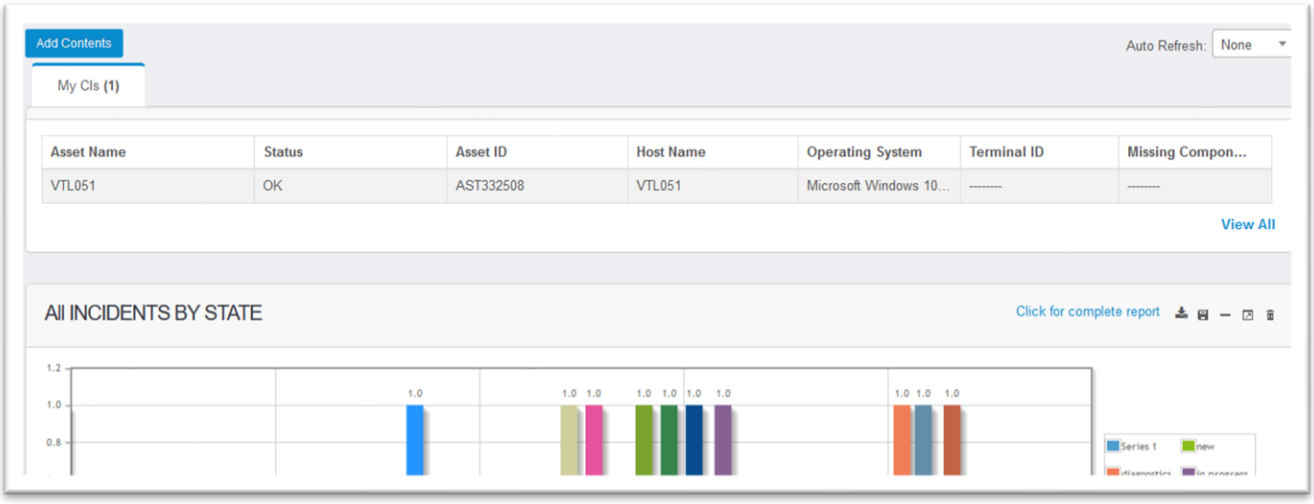
- Two business rules cannot have the same execution order.
- All mandatory fields of an ITSM record should be defined under the **Action Details** area.
- Two or more conditions can be combined using AND or OR logical conditions.

Dashboards

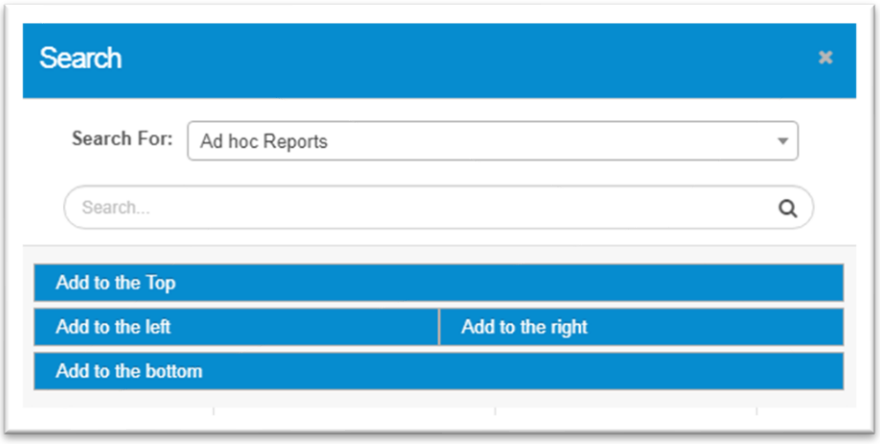
Ivanti Neurons for Service Mapping provides customizable dashboards for all modules where users can add content (such as graphs, change/outage calendars, and KPIs), which provides a high level of information about the module without the need to navigate the module itself.

To view a dashboard

1. In the left navigation pane, you can access dashboards one of several ways:
   - Click **My Dashboard**.
   - Click **Discovery Scan > Dashboard**.
   - Click **ITSM > Configuration Management > Dashboard**.
2. In the top-left corner of the page, click **Add Contents**. The Search dialog displays.

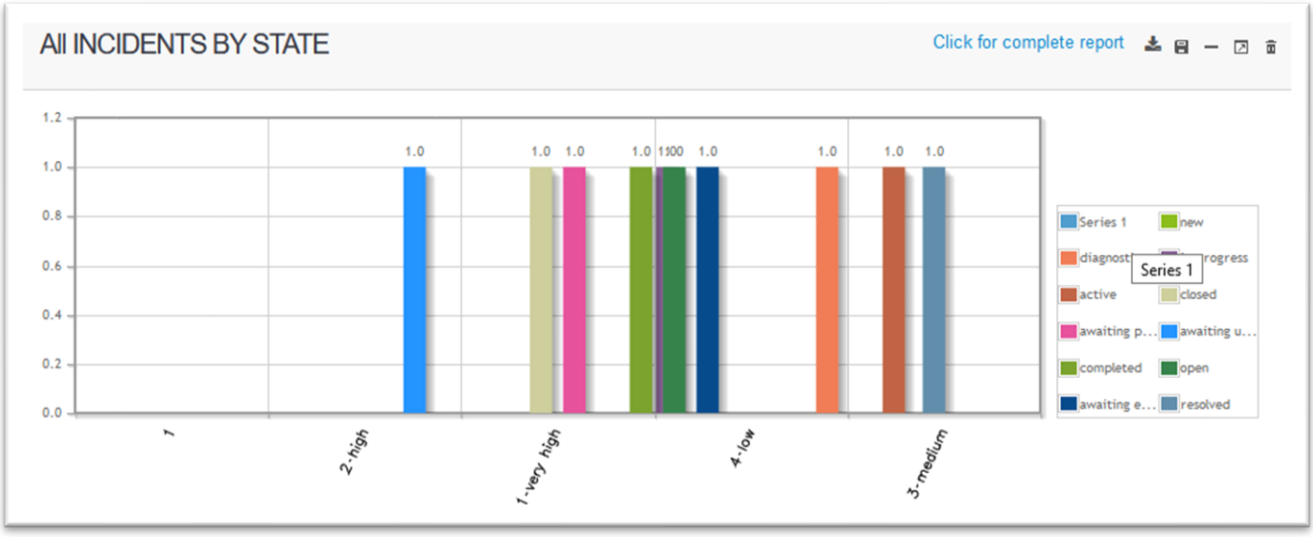


3. From the **Search For** drop-down, select a report type.



4. Enter the search criteria in the given text box, then click the icon. The results will display as per the given search criteria.
5. Click an item, then select one of the options to align the report to the top, bottom, left, or right of the Dashboard page.

A sample dashboard looks like this:



Reports

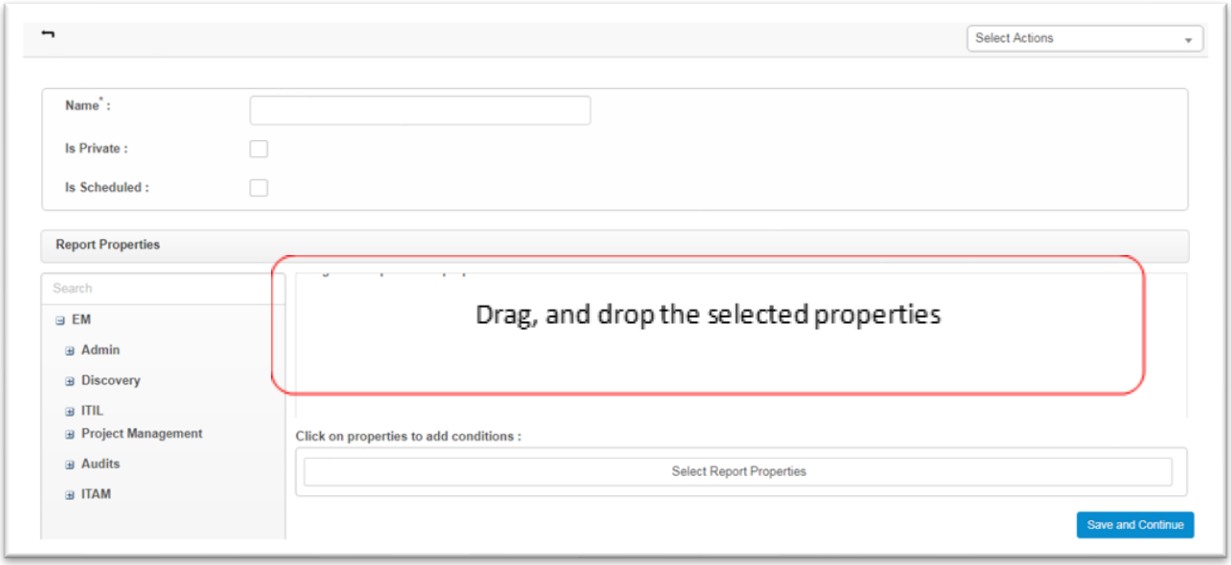
Ivanti Neurons for Service Mapping has a flexible reporting feature that enables you to generate ad-hoc reports by defining a query based on existing module properties.

You can set a schedule for generating ad-hoc reports, which eliminates the need to generate them manually.

Canned reports are also available.

To create and generate a report

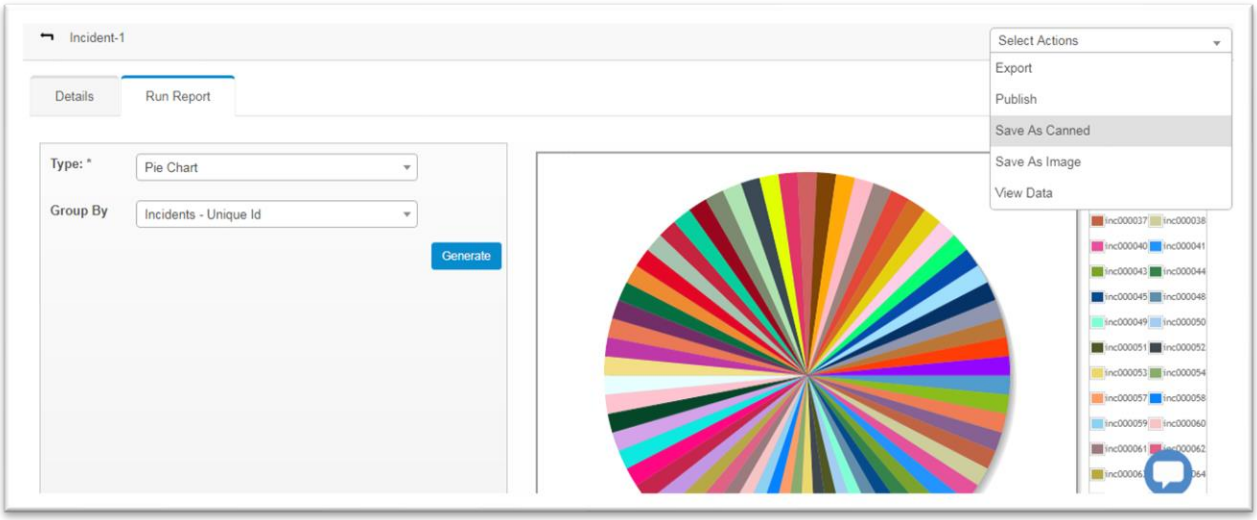
1. In the left navigation pane, click **Reports > Ad-hoc Reports**. The Reports page displays.
2. From the **Select Actions** drop-down, select **New Report**.
3. Enter a **name** for the report.
4. Select the **Is Private** option if the report should be visible to selected users only, then add those users.
5. Select the **Is Scheduled** option if the report should be sent to users according to a specific time and date, then configure that schedule.
6. In the left column, expand the required module heading to create the report.
7. Click the properties of the module to be included in the report, then add any required conditions by clicking the  icons.
8. Drag and drop the selected properties into the given text box.



9. Click **Save and Continue**.
10. Click the **Run Report** tab to open the page where you can generate the report.

11. From the **Type** drop-down, select the type of report to be generated. The available types of charts are tabular, bar, line, pie, and donut.
12. From the **Group by** drop-down, select grouped properties to generate an incident report.
13. Click **Generate** to view the report.

A sample report looks like this:



From the **Select Actions** drop-down on this page, you can do the following:

- **Export**: Export and view the report in Excel file format. An email with the attachment will be sent to the logged-in MSP vendor.
- **Publish**: Publish the report in the dashboard of the logged-in MSP vendor.
- **Save as Canned**: Save the report as a canned report with an automatically generated name.
- **Save as Image**: Save the report in an image format. Note that tabular reports can't be saved as an image.
- **View Data**: View the data that has been accumulated for generating the report.

To view a canned report

1st, 2nd, and 3rd level users can view canned reports, but end users cannot view them.

1. In the left navigation pane, click **Reports > Canned Reports**. The Canned Reports page displays.
2. Click a report in the list to open it.

To delete or export a report from this page, select the checkbox next to the report, then use the **Select Actions** drop-down to delete or export the record.

Data export

This feature enables you to export and view configured CIs in Excel file format. An email with the attachment is sent to the logged-in application user.

You also have the option of creating a custom export.

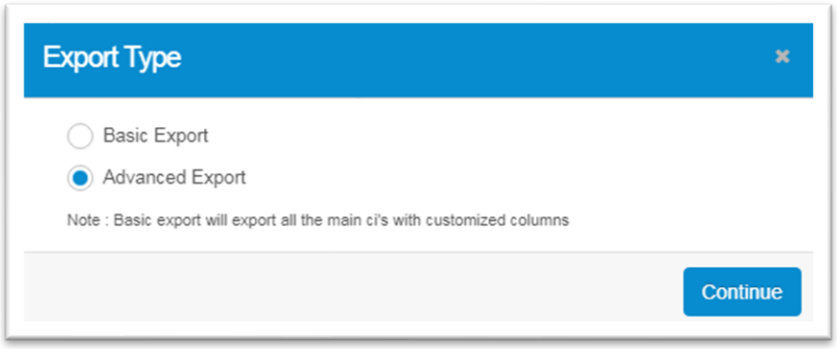
To export CI data to Excel

1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**. The Configuration Items page displays.
2. Select individual CIs to export or click the top checkbox to export all of the CIs in the list.
3. From the **Select Actions** drop-down, select **Export**. Click **Basic Export**, then confirm the export to receive an email with an Excel attachment consisting of CI details. Note that CI properties are *not* included in the report.

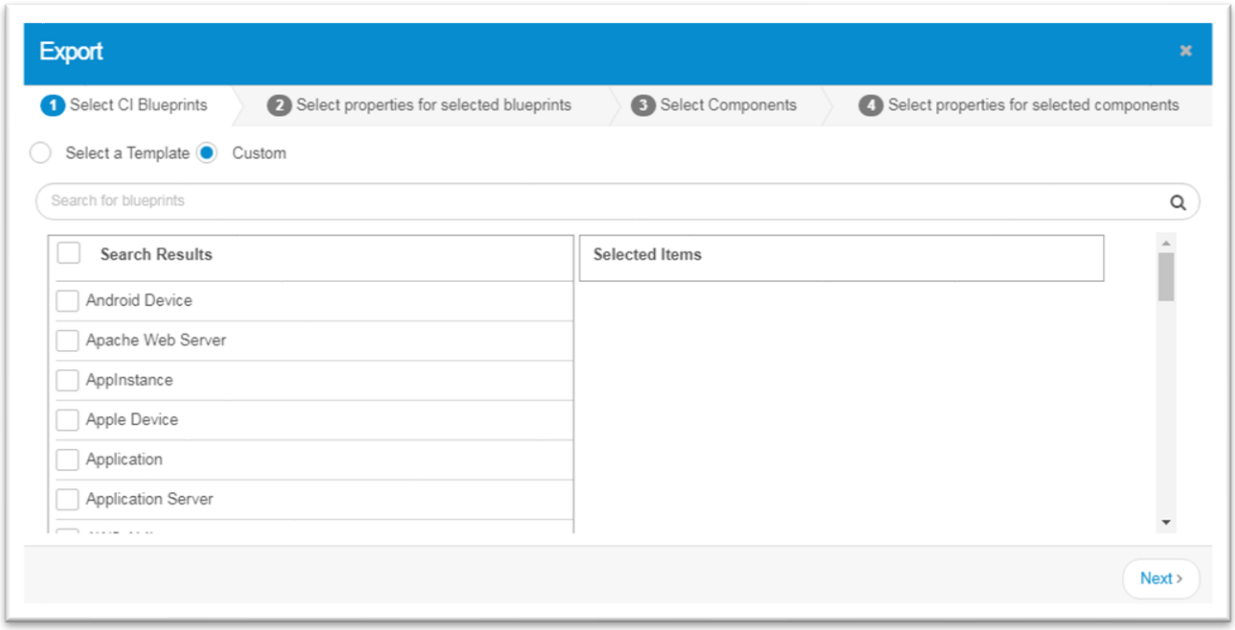
To create a custom export of CI data

A custom export enables you to include CI components and other properties in the export.

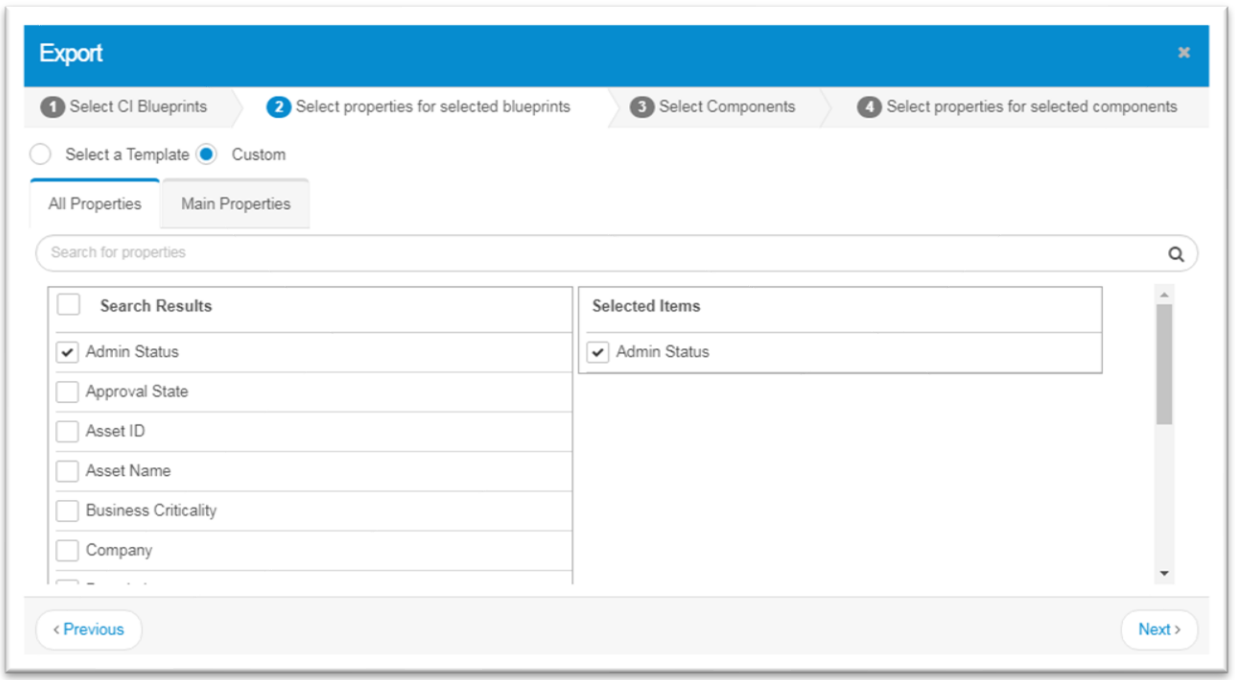
1. In the left navigation pane, click **ITSM > Configuration Management > Configuration Items**. The Configuration Items page displays.
3. From the **Select Actions** drop-down, select **Export**. The Export Type dialog displays.



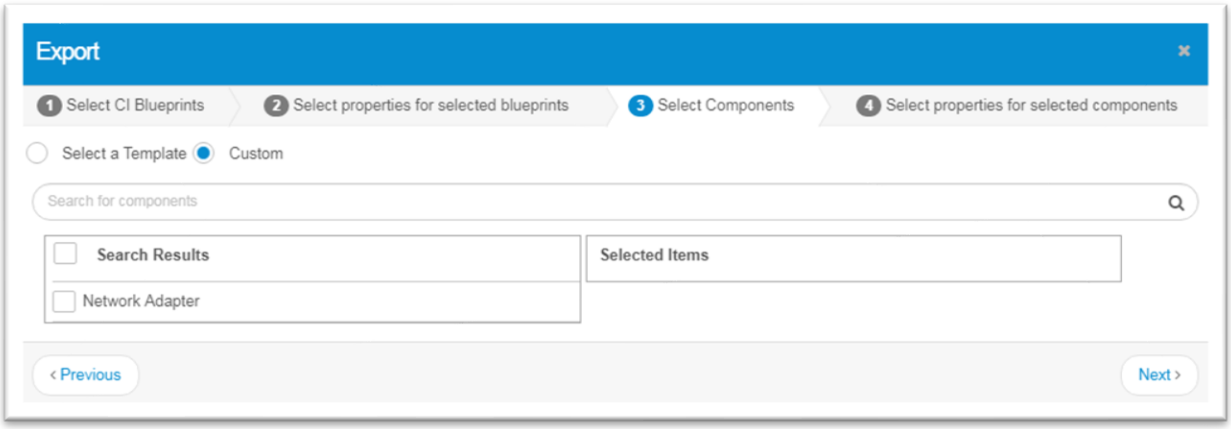
4. Click **Advanced Export** and click **Continue**. The Export dialog displays. There are two export methods: **Select Template** and **Custom**.
5. The **Select Template** method enables you to export CI data from the existing options in the application:
   - From the **Select Template** drop-down, select the required option.
   - Click **Export**.
6. The **Custom** method enables you to customize your exported CI report based on CI blueprints, properties for selected CI blueprints, components, and properties for selected components:
   - Select the required CI blueprints and click **Next**.



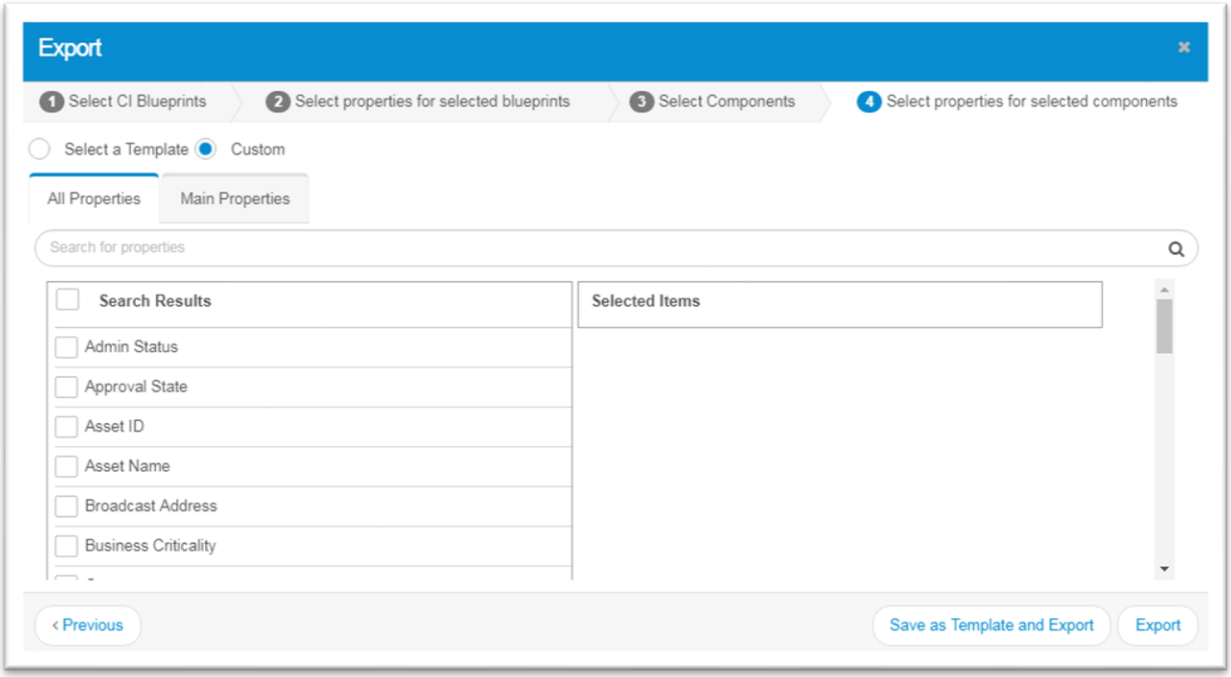
- Select the required properties for the selected blueprints, then click **Next**.



- Select the required components, then click **Next**.



- Select the required properties for the selected components. You can save the selected blueprint options as a template to export by clicking **Save as Template and Export**, entering a template name, then clicking **Save**. The template name will be displayed in the Select Template option of the Export.



- Click **Export**. Note that with the Export option, no template is saved.