eyeExtend for ServiceNow Configuration Guide v3.2.4

1 September 2023

eyeExtend for ServiceNow Configuration Guide v3.2.4

About the Forescout Platform eyeExtend for ServiceNow Integration

Forescout Platform eyeExtend for ServiceNow® enables the exchange of information between the Forescout Platform and the ServiceNow cloud service, as well as the integration of IT Service Management and Security Operations in ServiceNow. ServiceNow sends action requests to the Forescout Platform and triggers policy actions.

Forescout Platform eyeExtend for ServiceNow enables you to:

- Send selected tags to ServiceNow. You can configure and schedule mapping to the Configuration Management Database (CMDB).
- Import device properties and get real-time updates from ServiceNow.
- Create incidents in ServiceNow and receive real-time updates for them.
- Provide a Web service for ServiceNow to send action requests.

  Use the policy engine to report ServiceNow incidents, take action on devices and issue action requests in ServiceNow workflows and business rules. For information about policies, see Policy Manager in the Forescout Platform Administration Guide.

Forescout App for Asset Management

The Forescout App for Asset Management supports integration between the Forescout Platform and ServiceNow. The bi-directional data exchange between the Forescout Platform and ServiceNow enriches and supplements the Configuration Management Database (CMDB).

By adding or updating device properties on the ServiceNow CMDB configuration item tables, the Forescout Platform triggers the ServiceNow workflow by applying Forescout policies. These policies are based on the Forescout Platform properties, and the properties exchanged with the ServiceNow instance.

The data exchange:

- Identifies devices on network segments using Forescout Appliance(s).
- Updates ServiceNow tables with device properties captured by the Forescout Platform.
- Imports device properties from ServiceNow.

This app includes tables, import sets, and scripts required by the Forescout App for IT Incidents and the Forescout App for SOC Incidents. These additional objects let the app push updates to the Forescout Platform. For more information, see the Forescout App for Asset Management Installation Guide.

Forescout App for IT Incidents

ServiceNow Information Technology (IT) personnel can use the Forescout App for IT Incidents to create incidents in ServiceNow from the Forescout Platform via an Action.

The Forescout App for IT Incidents sends action requests to the Forescout Platform, based on controls available in the ServiceNow Incident table.

For update events, use a business rule to send information about an IT incident to the Forescout Platform. The information sent for the incident includes the incident number, category, subcategory, impact, urgency, priority, short description, and state.

This app is dependent on the Forescout App for Asset Management. For more information, see the Forescout App for IT Incidents Installation Guide.

Forescout App for SOC Incidents

ServiceNow Security Operations Center (SOC) personnel can use the Forescout App for SOC Incidents to create incidents in ServiceNow from the Forescout Platform via an action.

The Forescout App for SOC Incidents sends action requests to the Forescout Platform based on controls available in the ServiceNow Security Incident table.

The Forescout App for SOC Incidents contains a business rule for sending information about a SOC incident to the Forescout Platform, in the event of an update. The information sent for a SOC incident includes the incident number, category, subcategory, business impact, priority, short description, and state.

This app is dependent on the Forescout App for Asset Management, and the Security Incident Response plugin from ServiceNow. For more information, see the Forescout App for SOC Incidents Installation Guide.

Service Graph Connector for Forescout

ServiceNow IT Operations and Security teams can use Service Graph Connector for Forescout to quickly and reliably ingest Forescout device data into the CMDB and streamline the correlation of Forescout Platform data with other data sources for a comprehensive data repository.

The Service Graph Connector for Forescout leverages Forescout Platform continuous IT, IoT and OT device visibility and rapidly provides rich, real-time device properties, classification, configuration and network context to ServiceNow CMDB by complying with the ServiceNow Common Service Data Model (CSDM). This enables IT Operations and Security teams to get a

current view of networked assets, track their movement and remediate or retire them as required.

Note: For the Service Graph Connector to function properly, run the "Normalize MAC Address" script in the ServiceNow instance.

This Service Graph Connector for Forescout is dependent on the Forescout App for Asset Management for user credentials validation. For more information, see the Service Graph Connector for Forescout Installation Guide.

The table below provides a comparison between the Service Graph Connector for Forescout and the Forescout App for Asset Management.

Functionality	Service Graph Connector for Forescout	Forescout App for Asset Management
Data Import	Batch requests – default value; 100	Single request
Data Processing	Parallel	Serial – one request at a time
Request Response	Single HTTP response for the batch request	Single request result
Data Transformation	IntegrationHub ETL	Script based
Add/Update CMDB	Automatic add/update CMDB	Requires policy to query [Host Status in CMDB] to add/update asset

Service Graph Connector for Forescout (ServiceNow Application) and Forescout Advanced Control Settings

The Service Graph Connector for Forescout is a ServiceNow application and limited by the available processing resources in the ServiceNow instance. The number of available processing resources varies depending on the ServiceNow instance workload. If more endpoints are sent to the Service Graph Connector than it can process, those endpoints are not be mapped into the CMDB.

You may configure the Forescout Platform Advanced Control Settings for Service Graph Rate and Batch size.

The Service Graph Rate adds the ability to adjust how many endpoints per second to send to the Service Graph Connector. The Service Graph Batch Size dictates the maximum batch size when sending endpoints to the Service Graph Connector. For information about how to configure these settings, see Configure General Settings.

About the eyeExtend for ServiceNow Module

The Forescout Platform eyeExtend for ServiceNow Module integrates with ServiceNow instances to provide complete visibility of assets, so that you can send selected host information from the Forescout Platform to ServiceNow instances and trigger actions based on properties.

Forescout Platform eyeExtend for ServiceNow:

- Let's you use Policies and actions provided by the Forescout Platform eyeExtend module to update your current asset information (such as switch port, open ports, or VLAN) to ServiceNow. You can also use action indents and ticketing. See ServiceNow Policy Templates.
- Combines with Forescout App for Asset Management, Forescout App for IT Incidents, Forescout App for SOC Incidents, and Service Graph Connector for Forescout, to provide a complete Forescout Platform - ServiceNow integration.

Note: The minimum Forescout requirements for the ServiceNow integration described in this publication are the Forescout Platform eyeExtend Module and the Forescout App for Asset Management. For example, Forescout policies and actions provided by the Forescout Platform eyeExtend module are used to populate the import set table in the Forescout App for Asset Management with Forescout data, and then the application transfers the data to the ServiceNow CMDB.

You can get these apps at the ServiceNow Store at https://store.servicenow.com (search for Forescout on the site).

Note: The user guides are located in the right pane under Supporting Links & Docs.
Important: You must install and configure both the Forescout Platform and ServiceNow to work with the features described here.

Forescout Platform eyeExtend for ServiceNow and Certification Compliance Mode

Forescout eyeExtend for ServiceNow supports Certification Compliance Mode. For information about this mode, refer to Certification Compliance in the *Forescout Platform Installation Guide*.

About Forescout Platform eyeExtend for ServiceNow and Support for Dual Stack Environments

The Forescout Platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. Endpoints with both Ipv4 and IPv6 are detected for the properties, actions, and policies provided by this eyeExtend module.