20 N Wacker Dr Suite 1200
Chicago, IL 60606
(773) 830-4061

NP-Live Module for Forescout

Configuration and Reference Guide

About

The NP-Live Module for Forescout enables integration between CounterACT and NP-Live such that network device configuration files managed by CounterACT can be automatically imported into NP-Live and aggregated into specific workspaces. Currently, Cisco switches are supported through the Forescout Switch Plugin. To request support for other devices, please contact support@network-perception.com. To learn more about NP-Live, please visit https://www.network-perception.com/np-live

Example use case

Compliance and security analysts would like to leverage NP-Live to verify compliance with NERC CIP standards. The NP-Live Module for Forescout will provide the following advantages:

- Automation of the device configuration import workflow
- Better security by keeping a single direct connection to network devices through CounterACT instead of having to add a second connection between NP-Live and network devices
- Receiving automated compliance alerts when device configurations are modified

Additional NP-Live Documentation

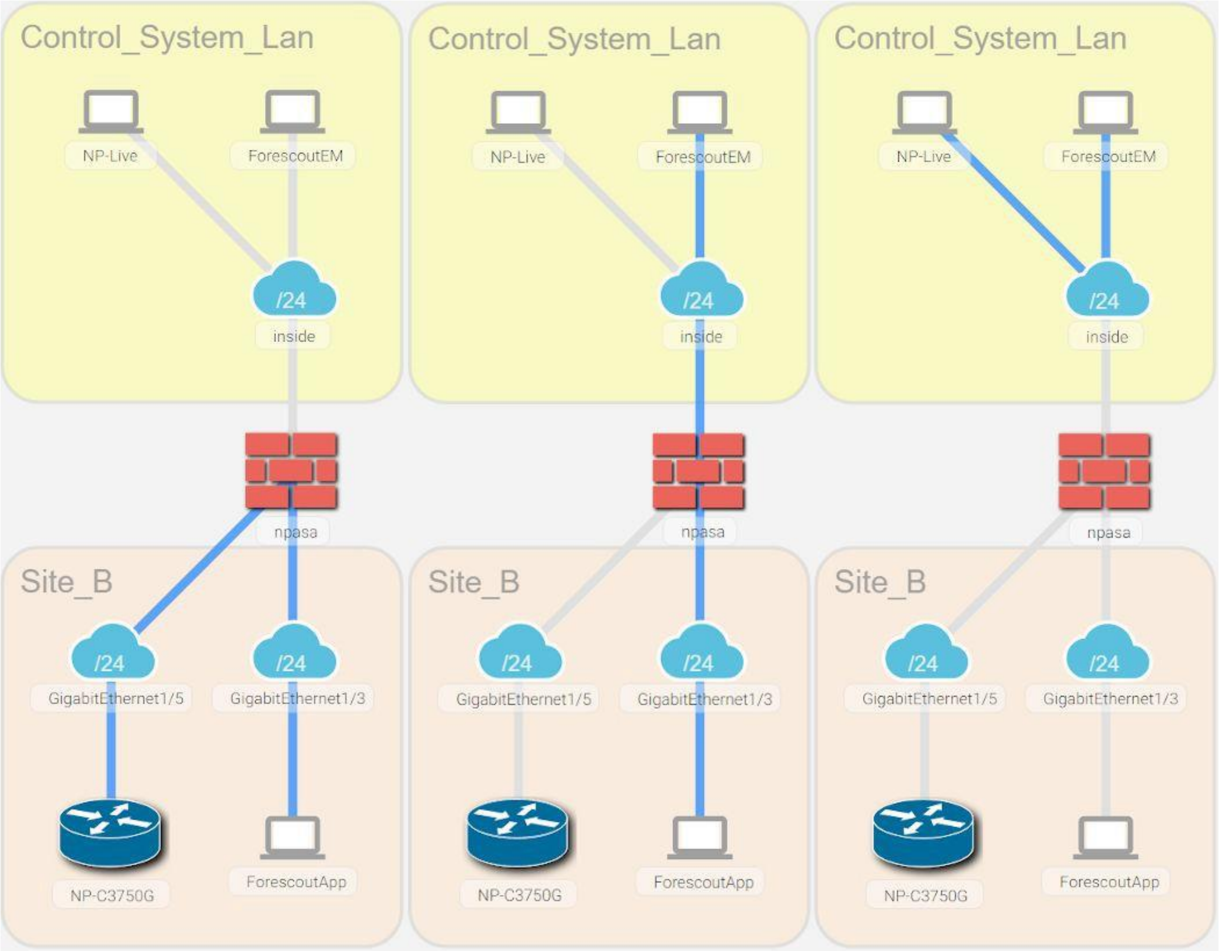
Please visit https://kb.network-perception.com to access to NP-Live knowledge base.

Example Architecture Diagram

The following network diagram represents where the NP-Live server and the Forescout Enterprise Manager would be located (Control System LAN) with respect to the switch device and the Forescout Appliance (Site B).

The sequence of network flows is highlighted from left to right:

1. The Forescout Appliance connects to the Cisco switch and downloads the latest version of the running configuration
2. The Forescout Enterprise Manager retrieves the downloaded configuration from the Forescout Appliance
3. The NP-Live Module inside the Forescout Enterprise Manager pushes the configuration files to the NP-Live server



Requirements

- Forescout version 8.1 or later
- NP-Live version 2.1 or later

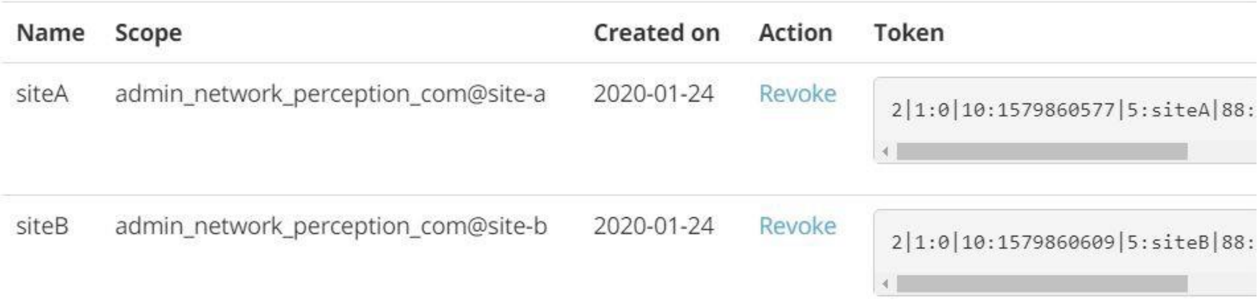
Installing the NP-Live Module

Download the Forescout Extended Module for NP-Live from https://updates.forescout.com. Start your Forescout Console and login into Enterprise Manager. Then open “Options”, select “Modules”, and install the fpi.

Configuring the NP-Live Module

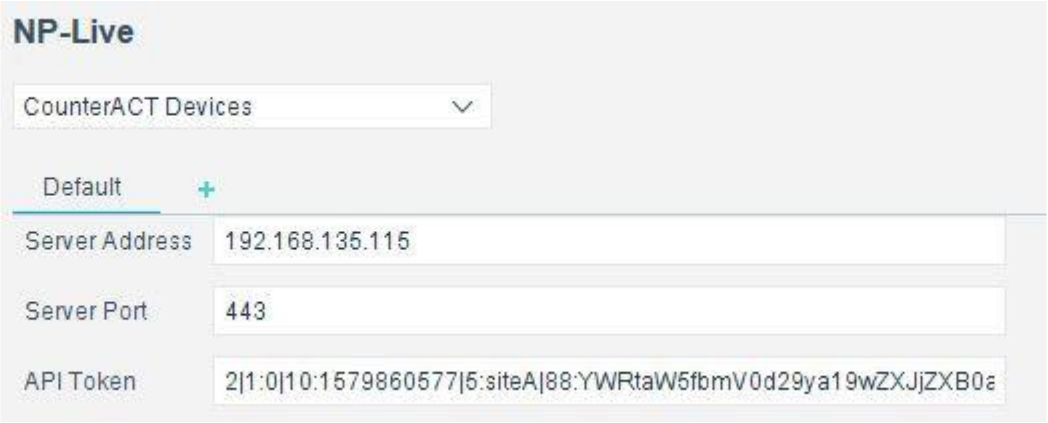
The NP-Live configuration aggregation policy is dependent on the running-config host property. Appendix 5 of the Switch Plugin Configuration Guide discusses the details of resolving the host property for running-config.

To configure the module, API Tokens have to be first generated within NP-Live. The API Tokens window can be access through the Import > New Connector menu inside an existing workspace. These tokens are then used to configure the Forescout Extended Module for NP-Live.



Name	Scope	Created on	Action	Token
siteA	admin_network_perception_com@site-a	2020-01-24	Revoke	2|1:0|10:1579860577|5:siteA|88:
siteB	admin_network_perception_com@site-b	2020-01-24	Revoke	2|1:0|10:1579860609|5:siteB|88:

The default tab provides specifies the API token that is used when no other appliance specific configuration are made. In this instance, the default workspace is associated with the API token "siteA."



NP-Live

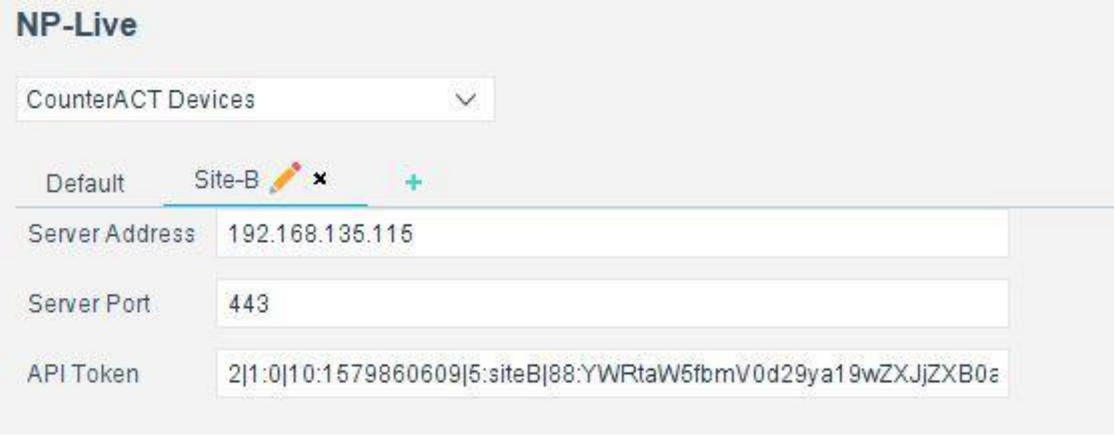
CounterACT Devices

Server Address: 192.168.135.115

Server Port: 443

API Token: 2|1:0|10:1579860577|5:siteA|88:YWRtaW5fbmV0d29ya19wZXJjZXB0a

To better scope file upload, each CounterACT Appliance could be configured with a unique API Token. Since each API Token' scope is a specific workspace, the assigned assets to a CounterACT device would only be available within the respective scope.



NP-Live

CounterACT Devices

Default | Site-B

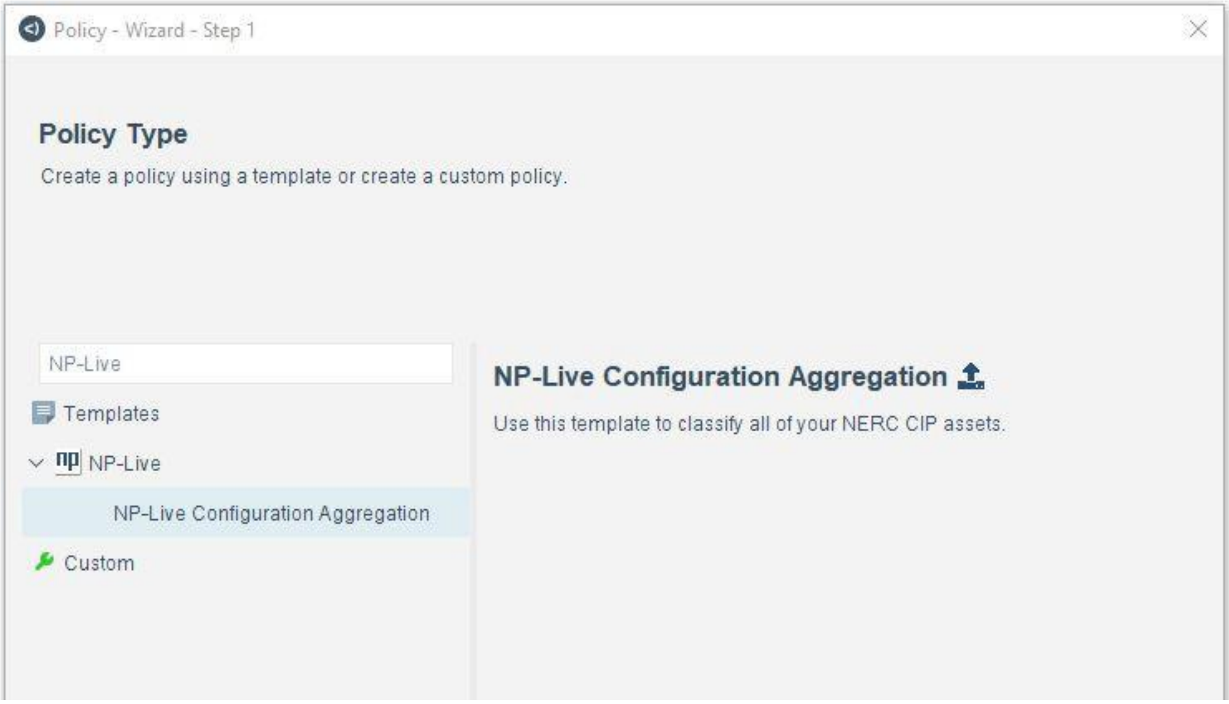
Server Address: 192.168.135.115

Server Port: 443

API Token: 2|1:0|10:1579860609|5:siteB|88:YWRtaW5fbmV0d29ya19wZXJjZXB0a

The configuration above will scope the assets belonging to the CounterACT Appliance named "Site-B" by API Token "siteB."

Create NP-Live Policies Using Templates



Policy - Wizard - Step 1

Policy Type

Create a policy using a template or create a custom policy.

NP-Live

Templates

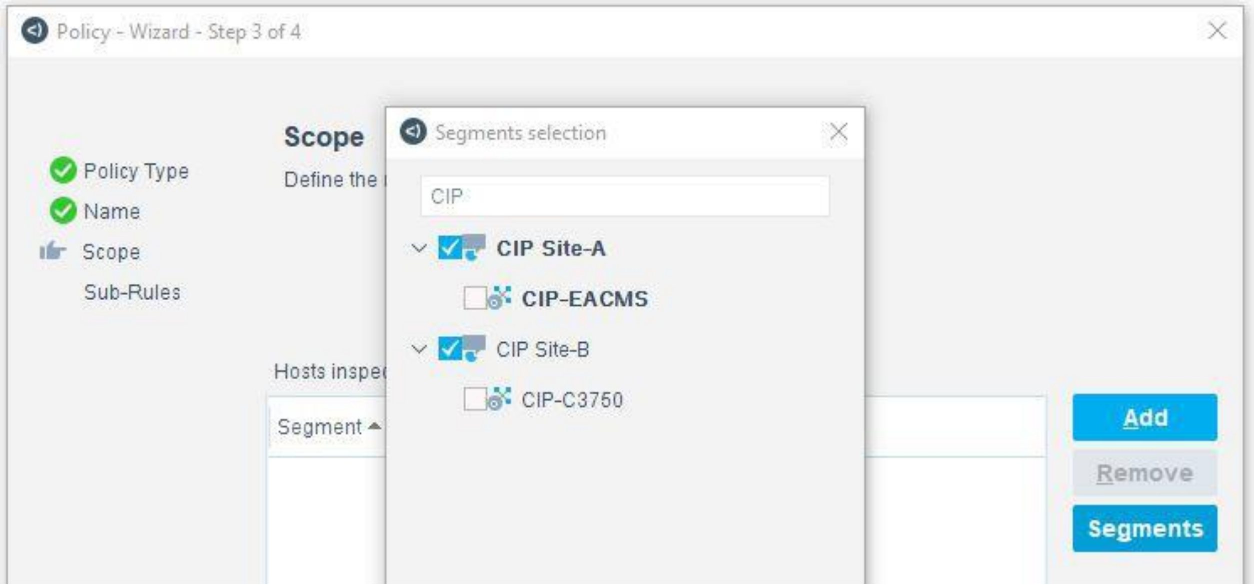
NP-Live

NP-Live Configuration Aggregation

Custom

NP-Live Configuration Aggregation

Use this template to classify all of your NERC CIP assets.



Contact

Please contact support@network-perception.com for any question or to request more information.