Encrypted Traffic Analytics in Cisco SD-Access Fabrics

Prescriptive Deployment Guide

September, 2019

Table of Contents

Introduction 4

About The Solution 4

What is new in this version of the Encrypted Traffic Analytics in Cisco SD-Access Fabrics Perscrptive Deployment Guide 4

About This Guide 5

What is Not Covered in This Document 5

Define 6

Supported Devices and Versions 6

Supported Devices for Enabling Network as a Sensor with Encrypted Traffic Analytics 6

Supported Devices for Enabling Network as a Sensor 7

ETA Deployment Components 7

Software-Defined Access and Cisco DNA Center 7

NetFlow 8

Cisco Stealthwatch 8

Cisco Cognitive Intelligence 8

Encrypted Traffic Analytics 8

Stealthwatch Security Analytics Application 8

Cisco Catalyst 9300 Series Switches 8

Cisco Catalyst 9400 Series Switches 9

Cisco 4000 Series Integrated Services Router 9

Cisco ASR 1000 Series Aggregation Services Router 9

Design 11

Enabling ETA and FNF in a Cisco SD-Access fabric 11

Cisco Stealthwatch Security Analytics service on Cisco DNA Center 12

Deploy 15

Topology and Network infrastructure 15

Process: Integrating Cognitive Intelligence with Stealthwatch 16

Procedure 1: Configure the Stealthwatch Management Console for Cognitive Intelligence integration 16

Process: Provisioning ETA and FNF using SSA with Cisco DNA Center 18

Procedure 1: Install Stealthwatch Security Analytics application in Cisco DNA Center 18

Procedure 2 – Adding SMC to Cisco DNA Center 20

Procedure 3 – Provision Devices for ETA and FNF using SSA 21

Operate 27

Navigating the Stealthwatch Security Insight Dashboard 27

Alarming Hosts 27

Top Alarming Hosts 27

Alarms by Type 28

Today’s Alarms 28

Cognitive Intelligence ... 28
Flow Collection Tend ... 29
Top Applications ... 29
Host Groups ... 30
Inside Hosts ... 30
Configuring a Host Group ... 30
Crypto Audit ... 33
Preform a Crypto Audit Using the ETA Cryptographic Audit tool ... 33
Perform a Crypto Audit using Flow Search ... 36
Investigate suspicious activity for malware through Cognitive Intelligence ... 40
Useful Commands ... 46
About this guide ... 51
Feedback & Discussion ... 51
Appendix A—Hardware and software used for validation ... 52
Appendix B—Glossary ... 53
Appendix C—Deploy ETA and FNF using templates ... 54
Procedure 1 - Create templates for wired and wireless provisioning ... 54
Procedure 2 – Configure the template ... 57
Procedure 3 - Create a network profile ... 60
Procedure 4 – Provision ETA and FNF on the SD-Access edge nodes ... 61
Procedure 5 – Template for ETA and FNF removal ... 64
Appendix D: References ... 66

Introduction

About The Solution

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. Encrypted traffic has increased by more than 90 percent annually

Encryption technology has enabled much greater privacy and security for enterprises and individuals that use the Internet to communicate and transact business online. Mobile, cloud, and web applications rely on well implemented encryption mechanisms that use keys and certificates to ensure security and trust. However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.

Traditional flow monitoring, as implemented in the Cisco® Network as a Sensor (NaaS) solution and through the use of Flexible NetFlow (FNF), provides a high-level view of network communications by reporting the addresses, ports, and byte and packet counts of a flow. In addition, intraflow metadata, or information about events that occur inside of a flow, can be collected, stored, and analyzed within a flow monitoring framework. This data is especially valuable when traffic is encrypted, because deep-packet inspection is no longer viable. This intraflow metadata, called Encrypted Traffic Analytics (ETA), is derived by using new data elements or telemetry that is independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows.

ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud-based global visibility.

ETA extracts two main data elements: The Initial Data Packet (IDP) and the Sequence of Packet Length and Time (SPLT).

For more information about Encrypted Traffic Analytics, see the complete ETA white paper.

What is new in this version of the Encrypted Traffic Analytics in Cisco SD-Access Fabrics Perscrptive Deployment Guide

In earlier guides, templates were used within Cisco DNA Center to provision, both ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. In this guide, the new Cisco Stealthwatch Security Analytics (SSA) service within Cisco DNA Center v 1.3 is used.

In earlier guides, only the Cisco Catalyst® 9300 and 9400 switches were discussed as they were the only switching platforms to support ETA. In this version of the guide, coverage has been expanded to include the provisioning of flexible NetFlow in support of Network as a Sensor (NaaS) on the Cisco Catalyst® 3850 and 3650 switches.

Note that the Cisco Catalyst® 3850 and 3650 switches do not support ETA,

Cisco ASR1000 and ISR4000 series border routers are now supported and will be provisioned for ETA and FNF. Only borders having a role as **ANYWHERE** or **EXTERNAL** with a default route will be supported for ETA and FNF provisioning.

Finally, a dedicated Design Guide is now available for ETA when used in both Cisco SD-Access fabrics as well as traditional network environments. This document has only a brief design section addressing the Cisco Stealthwatch Security Analytics Service. For complete design considerations, please refer to the new Encrypted Traffic Analytics Design Guide.

About This Guide

This document provides guidance to enable Naas with ETA inside a Software Defined-Access (SDA) fabric, providing cryptographic assessment of the cipher suites used for TLS-encrypted communications, as well as the ability to identify malicious traffic patterns within the encrypted traffic of an SD-Access fabric.

This deployment guide provides guidance when using the Stealthwatch Security Analytics service within Cisco DNA Center to deploy NaaS and ETA configuration inside an SDA Fabric.

What is Not Covered in This Document

Although this deployment guide is about enabling NaaS and ETA functionality in a Software Defined-Access (SDA) fabric, this guide does not cover deployment scenarios outside of the fabric. This guide also does not address initial deployment of Stealthwatch or Cisco DNA Center and a Cisco SD-Access fabric.

This guide does not go in depth into the design of the solution, instead that will be in the in a separate guide which can be located here.

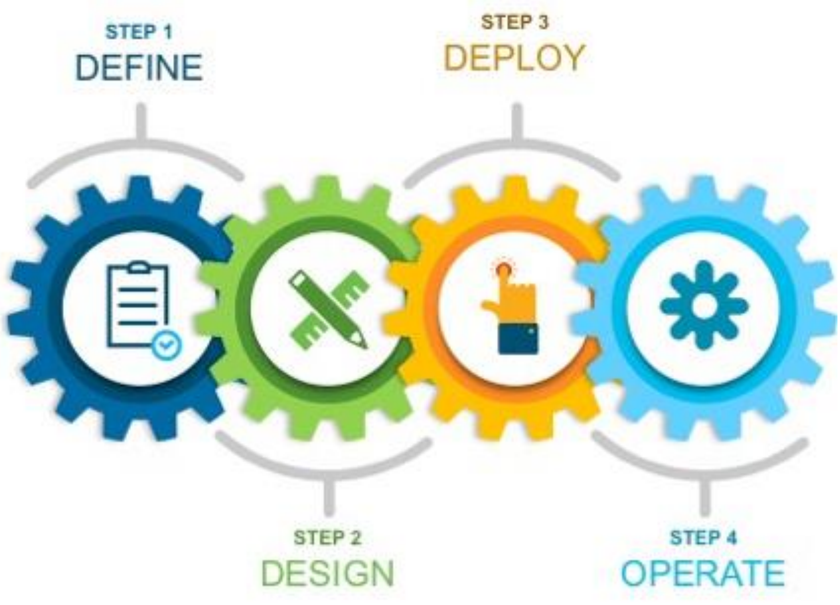


Figure 1 Implementation Flow

This document contains four major sections:

- The **Define** section defines supported platforms as well as components of the solution.
- The **Design** section describes and provides insight about the solution.
- The **Deploy** section provides information about configurations and best practices.
- The **Operate** section shows how to use and troubleshoot the solution.

Define

This section provides a high-level overview of the ETA and Stealthwatch solution and its components.

Supported Devices and Versions

Stealthwatch and Cisco DNA Center Supported Versions

The following table lists the minimum version and components required for Cisco Stealthwatch and Cisco DNA Center in order to deploy NaaS and ETA using the SSA Application.

Product Family	Minimum Version	Validated Version	Product Components Required	License/Capacity Required
Stealthwatch Enterprise	6.10.2	7.0	• Stealthwatch Management Console •Flow Collector	See Stealthwatch Management Console VE and Connector Flow VE Installation and Configuration Guide.
Cisco DNA Center	1.3.1	1.3.1	N/A	N/A

Supported Devices for Enabling Network as a Sensor with Encrypted Traffic Analytics

The following table lists the supported devices, minimum version, and license and platform requirements for enabling Network as a Sensor with Encrypted Traffic Analytics.

Product Family	Minimum Version	Validated Version	License Required	Platforms
Catalyst 9300	IOS-XE 16.6.4	IOS-XE 16.9.3 IOS-XE 16.11.1	DNA Advantage	• C9324 • C9348
Catalyst 9400	IOS-XE 16.6.4	IOS-XE 16.9.3 IOS-XE 16.11.1	DNA Advantage	• C9404 • C9407 • C9410

Product Family	Minimum Version	Validated Version	License Required	Platforms
ISR 4k	IOS-XE 16.6.4	IOS-XE 16.11.1	Either of the following: • DNA Advantage (16.9) • SEC/K9	• 4221 • 4321 • 4331 • 4351 • 4431 • 4451
ASR 1k	IOS-XE 16.6.4	IOS-XE 16.11.1	Either of the following: • DNA Advantage (16.9) • SEC/K9	• 1001-X • 1001-HX • 1002-X • 1002-HX

Catalyst 9500 and 9600 devices are not supported for ETA.

Supported Devices for Enabling Network as a Sensor

The following table lists the supported devices and the minimum version and license requirements for enabling Network as a Sensor.

Product Family	**Minimum Version**	**License Required**
Catalyst 9200	IOS-XE 16.9.1	DNA Advantage
Catalyst 3850	IOS-XE 16.9.1	DNA Advantage
Catalyst 3650	IOS-XE 16.9.1	DNA Advantage

ETA Deployment Components

Software-Defined Access and Cisco DNA Center

Cisco Digital Network Architecture (Cisco DNA™) provides a roadmap to digitization and a path to realize immediate benefits of network automation, assurance, and security. Cisco's SD-Access architecture is the Cisco DNA evolution from traditional campus LAN designs.SD-Access uses Cisco DNA Center for designing, provisioning, applying policy, and providing campus wired and wireless network assurance for an intelligent network. Fabric technology, an integral part of SD-Access, introduces programmable overlays, enabling easy to-deploy network virtualization across the wired and wireless campus. In addition to network virtualization, fabric technology provides software-defined segmentation and policy enforcement based on user identity and group membership. Software-defined segmentation is seamlessly integrated using Cisco Group Based Policy technology, providing micro-segmentation through the use of scalable groups within a virtual network. Using Cisco DNA Center to automate the creation of virtual networks reduces operational expenses, as well as reducing risk, due to Cisco DNA Center's integrated security and improved network performance provided by the assurance and analytics capabilities.

NetFlow

NetFlow is a standard that defines data elements exported by network devices that describe the “conversations” on the network. NetFlow is unidirectional, and each device on the network can export different NetFlow data elements. When processed, NetFlow data can tell you the important details in network transactions involving data communication between endpoints, information about when the conversation occurred, how long it lasted, and what protocols were used. It is a Layer 3, possibly Layer 2 depending on where it’s enabled or match conditions, network protocol that you can easily enable on wired and wireless devices for visibility into the network flows, as well as enhanced network anomaly and malware detection.

For more information, see the Cisco IOS NetFlow web page

Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection of raw packets—to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analyzed to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms that watch behavior and identify suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behavior are matched. For more information, see the Cisco Stealthwatch web page.

For more information, see the Cisco Stealthwatch web page.

Cisco Cognitive Intelligence

Cisco Cognitive Intelligence finds malicious activity that has bypassed security controls or entered through unmonitored channels (including removable media) and is operating inside an organization’s environment. Cognitive Intelligence is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure.

For more information, see the Cisco Cognitive Intelligence web page.

Encrypted Traffic Analytics

Encrypted Traffic Analytics is a Cisco IOS-XE feature that uses advanced behavioral algorithms to identify malicious traffic patterns through analysis of intraflow metadata of encrypted traffic, detecting potential threats hiding in encrypted traffic.

For more information, see the Cisco Encrypted Traffic Analytics web page.

Stealthwatch Security Analytics Application

Stealthwatch Security Analytics or SSA is a service introduced in version 1.3 of Cisco DNA Center. It offers configuration automation of network devices for NaaS and ETA enablement without the need for manual entry or templates.

Cisco Catalyst 9300 Series Switches

The Cisco® Catalyst 9300 Series Switches are Cisco’s lead stackable enterprise switching platform built for security, Internet of Things (IoT), mobility, and cloud. They are the next generation of the industry’s most widely deployed switching platform.

The 9300 Series forms the foundational building block for Software-Defined Access (SD-Access), Cisco's lead enterprise architecture.

At 480 Gbps, the 9300 Series is industry's highest-density stacking bandwidth solution with the most flexible uplink architecture. It is the first platform optimized for high-density 802.11ac Wave 2 and sets new maximums for network scale.

These switches are also ready for the future, with an x86 CPU architecture and more memory, enabling them to host containers and run third-party applications and scripts natively within the switch. The switches are based on the Cisco Unified Access™ Data Plane (UADP) 2.0 architecture, which not only protects your investment but also allows a larger scale and higher throughput as well as enabling Encrypted Traffic Analytics.

For more information, see the Cisco Catalyst 9300 Series Switches web page.

Cisco Catalyst 9400 Series Switches

The Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise access switching platform, built for security, IoT, and cloud. The platform provides unparalleled investment protection with a chassis architecture that is capable of supporting up to 9 Tbps of system bandwidth and unmatched power delivery for high-density IEEE 802.3BT (60W Power over Ethernet [PoE])

The 9400 Series delivers state-of-the-art high availability with capabilities such as uplink resiliency and N+1/N+N redundancy for power supplies. The platform is enterprise-optimized with an innovative dual-serviceable fan tray design and side-to-side airflow and is closet-friendly with a depth of approximately 16 inches (41 cm).

A single system can scale up to 384 access ports with your choice of 1 Gigabit Ethernet copper Cisco UPOE® and PoE+ options. The platform also supports advanced routing and infrastructure services, SD-Access capabilities, and network system virtualization. These features enable optional placement of the platform in the core and aggregation layers of small to medium-sized campus environments.

For more information, see the Cisco Catalyst 9400 Series Switch web page.

Cisco 4000 Series Integrated Services Router

The Cisco 4000 Series ISRs have revolutionized WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, the routers specifically address the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the Internet.

The Cisco® 4000 Series contains six platforms: the 4451, 4431, 4351, 4331, 4321 and 4221 ISRs.

For more information see the Cisco 4000 Series web page.

Cisco ASR 1000 Series Aggregation Services Router

The Cisco ASR 1000 Series aggregates multiple WAN connections and network services, including encryption and traffic management, and forwards them across WAN connections at line speeds from 2.5 to 200 Gbps. The routers contain both hardware and software redundancy in an industry-leading high-availability design.

The ASR 1000 Series supports Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The ASR 1000 Series Embedded Services Processors (ESPs), which are based on Cisco Flow Processor technology, accelerate many advanced features such as crypto-based access security; Network Address Translation (NAT), threat defense with zone-based firewall, deep packet inspection, Cisco Unified Border Element, and a diverse set of data-center-interconnect features. These services are implemented in Cisco IOS XE without the need for additional hardware support.

For more information, see the Cisco ASR 1000 Series web page.

Design

In many campus networks before the availability of SD-Access, NetFlow monitoring was typically performed at either the distribution layer of the network or at the uplink ports from the access layer switches, providing a distributed and scalable means of monitoring traffic entering or leaving the access layer.

SD-Access uses fabric technology to significantly change the campus architecture, driving the need to reconsider how FNF is deployed. Fabric technology in the campus enables the use of virtual networks (overlay networks) running on top of a physical network (underlay network) to create alternative topologies to connect devices. The underlay network is defined by the physical switches and routers that are part of the SD-Access network. An overlay network is created on top of the underlay to create a virtualized network. The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks in addition to isolation from the underlay network. The SD-Access fabric implements virtualization by encapsulating user traffic over IP packets that are sourced and terminated at the boundaries of the fabric. The encapsulation technology used is Virtual Extensible LAN (VXLAN).

With the Cisco SD-Access fabric technology in the campus, all IP traffic traversing the fabric is encapsulated with a VXLAN header appended to the frame. With the VXLAN header present, the original IP header of endpoint traffic is no longer visible for FNF inspection, and as a result only information about the outer VXLAN header is available and as a result, the means by which the fabric is monitored needs to be changed.

With SD-Access and the use of VXLAN encapsulation, what had previously been considered the distribution layer, and to an extent even the core, is now part of the underlay network and are considered to be intermediate nodes. As all traffic traversing the underlay is now encapsulated with a VXLAN header, provisioning the underlay network for FNF, whether at intermediate nodes or uplinks from edge nodes, is not an option, and it will be provisioned at the fabric edge nodes' access ports for wired endpoints or VLANs for wireless endpoints. Additionally, it is possible to monitor communications leaving the fabric at the external border towards the Internet if an ASR1000 or ISR 4000 router is present.

Prior to the introduction of ETA and Stealthwatch version 6.9.2 with Cognitive Intelligence integration, encrypted traffic analysis was not available with traditional NetFlow. However, with ETA enabled on Cisco Catalyst 9300 and 9400 Series Switches and Cisco routers running minimally Cisco IOS-XE 16.6.4, additional data elements such as the IDP and SPLT in encrypted communications are exported in ETA records in addition to flexible NetFlow records. These ETA data elements provide information about encrypted communications using HTTPS for the purpose of cryptographic assessment or “crypto audit” and malware detection without the need to decrypt the traffic.

Although ETA will produce NetFlow data by itself, FNF must also be provisioned for analysis of encrypted traffic by Cognitive Intelligence for malware detection, because ETA sends only information about the IDP and SPLT collected by the switch. For full NetFlow statistics containing connection and peer information, such as number of bytes, packet rates, round-trip times, and so on, you must also configure FNF.

Enabling ETA and FNF in a Cisco SD-Access fabric

Prior to DNA Center 1.3.1, templates were used within Cisco DNA Center to provision, both ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. In this guide, the new Cisco Stealthwatch Security Analytics (SSA) service within Cisco DNA Center v 1.3.1 is used exclusively for provisioning ETA and FNF. The SSA service can also be used to remove ETA and FNF configuration from a previously provisioned device.

Note that although the Cisco SSA application is the preferred method for provisioning ETA and FNF in Cisco DNA Center1.3.1 and later, it is still possible to use templates as documented in the previous guides and contained in the appendix of the new ETA for Cisco SD-Access Deployment Guide. However, when using templates, there is no support for provisioning border routers in the Cisco SD-Access fabric. Manual configuration of ETA and FNF via CLI is not supported..

The SSA service is not installed by default in Cisco DNA Center 1.3.1 and must installed manually after upgrade to version 1.3.1 or installation of a new appliance. As part of the installation procedure, it is also necessary to complete the configuration steps to integrate Cisco DNA Center with your Stealthwatch Enterprise deployment. Even though the SSA service is an optional package, it is linked to a specific version of Cisco DNA Center and hence package upgrades will only be available at the time of release of a new version of DNAC.

The Cisco SSA service, dynamically provisions both ETA and FNF for wired and wireless endpoint monitoring on Catalyst 9300, 9400, 3850, and 3650 edge nodes. As the Catalyst 3850 and 3650 switches do not support ETA, only FNF will be configured on these devices. SSA configures both ETA and FNF globally as well as applying the et-analytics configuration and applicable flow monitor (both directions) on the access interface for wired endpoints or VLAN for wireless endpoints.

Although possible to manually configure ETA and FNF on wired VLANs, however not supported by SSA, it is not recommended nor supported by Cisco as the overall scale for ETA processing will effectively be cut in half as ETA records would be processed twice. This caveat applies *only* to wired VLANs.

In addition to the support for Cisco Catalyst switches, the Cisco SSA application includes ETA provisioning support to ASR1000 and ISR 4000 series routers when configured as anywhere, or external borders in a Cisco SD-Access fabric. ETA support for border nodes only applies to routers and does not include the Catalyst 9500 or 9600 when used as a border as ETA is not supported on these platforms.

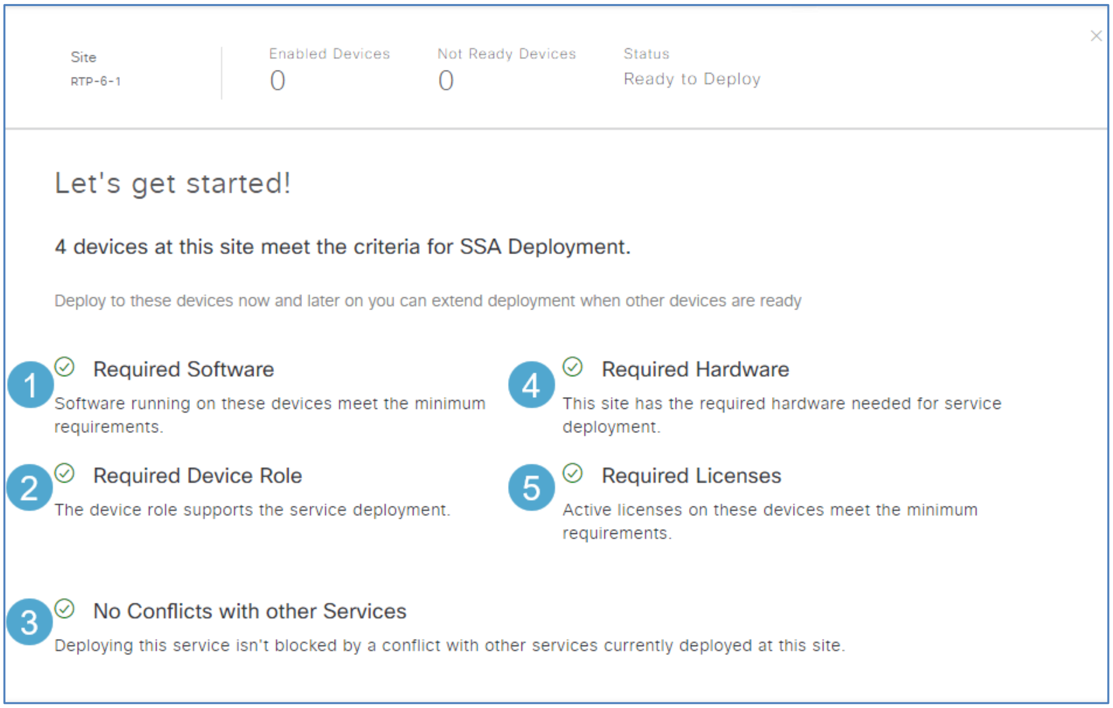
Cisco Stealthwatch Security Analytics service on Cisco DNA Center

The Cisco SSA service was introduced with the release of Cisco DNA Center v1.3 to automate the provisioning of ETA and FNF. The SSA service eliminates the need for the use of templates in provisioning ETA and FNF on network devices that support encrypted traffic analytics, and FNF for Network as a Sensor (NaaS) on those devices lacking ETA support. With this release of the Cisco SSA service, provision occurs on only Cisco SD-Access edge nodes and at ASR or ISR border routers with a default route.

The SSA service performs the following tasks:

- Assess those devices within the fabric to determine deployment readiness
- Enable Stealthwatch Security Analytics through provisioning of ETA and FNF
- Monitor deployment status

Upon launching the SSA service and selecting the site, building, or floor to be provisioned. The following screen displays the steps that were completed as part of the readiness assessment.



Site	Enabled Devices	Not Ready Devices	Status
RTP-6-1	0	0	Ready to Deploy

Let's get started!

4 devices at this site meet the criteria for SSA Deployment.

Deploy to these devices now and later on you can extend deployment when other devices are ready

1 ✓ Required Software
Software running on these devices meet the minimum requirements.

4 ✓ Required Hardware
This site has the required hardware needed for service deployment.

2 ✓ Required Device Role
The device role supports the service deployment.

5 ✓ Required Licenses
Active licenses on these devices meet the minimum requirements.

3 ✓ No Conflicts with other Services
Deploying this service isn't blocked by a conflict with other services currently deployed at this site.

1. Required Software – A minimum version of IOS-XE must be installed on the device. Please refer to the Appendix for more information.

2. Required Device Role – The device role within the Cisco DNA Center inventory must support the deployment model for provisioning that device; for example, supported switches must have a Device Role set to Access, whereas a router must have a Device Role set to Border Router.

3. No conflicts with other Services – A compatibility check is run against other services already configured on the device. The device must not be configured for AVC or other NetFlow configuration.

4. Required Hardware – The device must support either ETA or FNF as deployed for NaaS. Refer to the Appendix for more information.

5. Required License – The device must be licensed for DNA Advantage.

If all the criteria are met, the device will be considered ready for provisioning.

The Cisco SSA service assesses the devices by checking the global inventory to determine those devices ready to be provisioned for ETA and FNF or just FNF alone and then has the ability to hierarchically provision devices starting at the All Sites or All Fabrics level. Whether sites or fabrics are selected, it is possible to drill down hierarchically, the most granular selection being at the floor level. All devices at the selected level of the hierarchy can then be provisioned accordingly. It is not possible to individually select devices for provisioning. The Cisco SSA service is also used for disabling devices previously provisioned through the same hierarchical process. In the event that a new line card is added to a modular chassis or new switch to an existing stack, a Resync of the device in the Cisco DNA Center inventory will result in all applicable ports or VLANs of that new device to be configured appropriately.

Please refer to the Encrypted Traffic Analytics Design Guide for additional information related to this assessment and how readiness is determined.

The SSA service provisions ETA and FNF on the Cisco Catalyst® 9000 series switches, ASR1000/ISR4000 routers, and only FNF on the Cisco Catalyst® 3850/3650 switches. In the event that a device already has an existing NetFlow configuration such as for Cisco Application Visibility Control (AVC), the device will be considered to have a conflicting service and will be listed as **NOT READY**. With this release of Cisco DNA Center and the SSA service, AVC, reliant upon application based NetFlow reliant on NBAR, and ETA are mutually exclusive and only one or the other may be configured on the device.

SSA provisions the Catalyst® 9300 and 9400 switches with the Flexible NetFlow record, exporter, and monitor along with the et-analytics (ETA) global configurations. The flow monitor and ETA are then applied to the access interfaces for wired users. The fabric interface is always excluded from this configuration as well as any interface that an access point is attached to. If fabric-enabled wireless has been implemented, ETA and FNF will also be configured on the wireless VLANs for monitoring of wireless endpoints.

The SSA service only supports ETA and FNF provisioning for fabric enabled wireless and not CUWN “over the top” deployments where a CAPWAP tunnel is established between a Cisco access point (AP) and Cisco wireless controller (WLC) running in local mode. Fabric enabled wireless monitoring is accomplished through SSA provisioning both ETA and FNF on the wireless VLAN of the Catalyst 9300/9400 edge node. The VLAN must be used for wireless monitoring due to the VXLAN tunnel extending between the Cisco AP and terminating at the access port the AP is physically connected to. The sam holds true for the Catalyst 3850 and 3650 where FNF flow monitors are provisioned on the wireless VLAN.

SSA provisions the Catalyst 3850 and 3650 switches with only the Flexible NetFlow record, exporter, and monitor due to lack of ETA support. As with the Catalyst 9000 series switches, the flow monitor is then applied to the access interfaces for wired users and the wireless VLANs for wireless endpoints while the fabric interface as well as any interface where an access point is attached are always excluded from configuration.

In addition to support for Cisco switches, the SSA service will also provision the Cisco ASR1000 and ISR4000 series of routers when configured as an external or anywhere border router. The SSA service will provision the Flexible NetFlow record, exporter, and monitor along with the et-analytics (ETA) global configuration on the router and then apply the flow monitor and ETA on sub-interfaces (for virtual networks) where a default route has been learned or toward a subnet with a public IP not defined as IP pool in Cisco DNA Center.

Regardless of platform, SSA determines the source interface that will be used for ETA and FNF record exports by looking for the next hop of the flow collector’s IP address specified in Cisco DNA Center. The interface used to source the exports will reside in the underlay and have a route to the flow collector in the global routing table for the underlay. The integrated management interface of a switch or router is never used as the source interface. ETA and FNF record exports will be sent to UDP port 2055 for both ETA and FNF.

Deploy

This section describes the procedures necessary to enable ETA and FNF on devices within a Cisco SD-Access fabric as well as integrating Stealthwatch with Cognitive Intelligence for ETA use. Once completed, this will allow the user to use Stealthwatch and Cognitive Intelligence for crypto audit and malware detection.

With Cisco DNA Center version 1.3.1, automatic provisioning of Cisco devices for ETA and FNF using Cisco DNA Center is supported through the Stealthwatch Security Analytics or SSA service. If running an older version of Cisco DNA Center, the SSA service will not be available. Instead we can make use of templates to provision the fabric edge nodes to enable both ETA and FNF which is shown in the appendix here.

The SSA service provisions devices based off their capabilities and location in fabric. SSA targets access interfaces and fabric wireless vlans of the edge nodes as well as using the external, non-fabric, interface of the external border to give full coverage of a SD-Access fabric. A DNA Advantage license is required for all devices being provisioned by SSA.

If a device is not capable of using ETA, it will only be provisioned for use in NaaS.

Topology and Network infrastructure

This infrastructure depicted below, is running a Cisco SD-Access fabric that consists of three edge nodes, an intermediate switch, and an ISR 4331 as our control plane and border node. The fabric connects to a shared services network that houses Cisco DNA Center, Stealthwatch Management Console, Stealthwatch Flow collector and Cisco ISE.

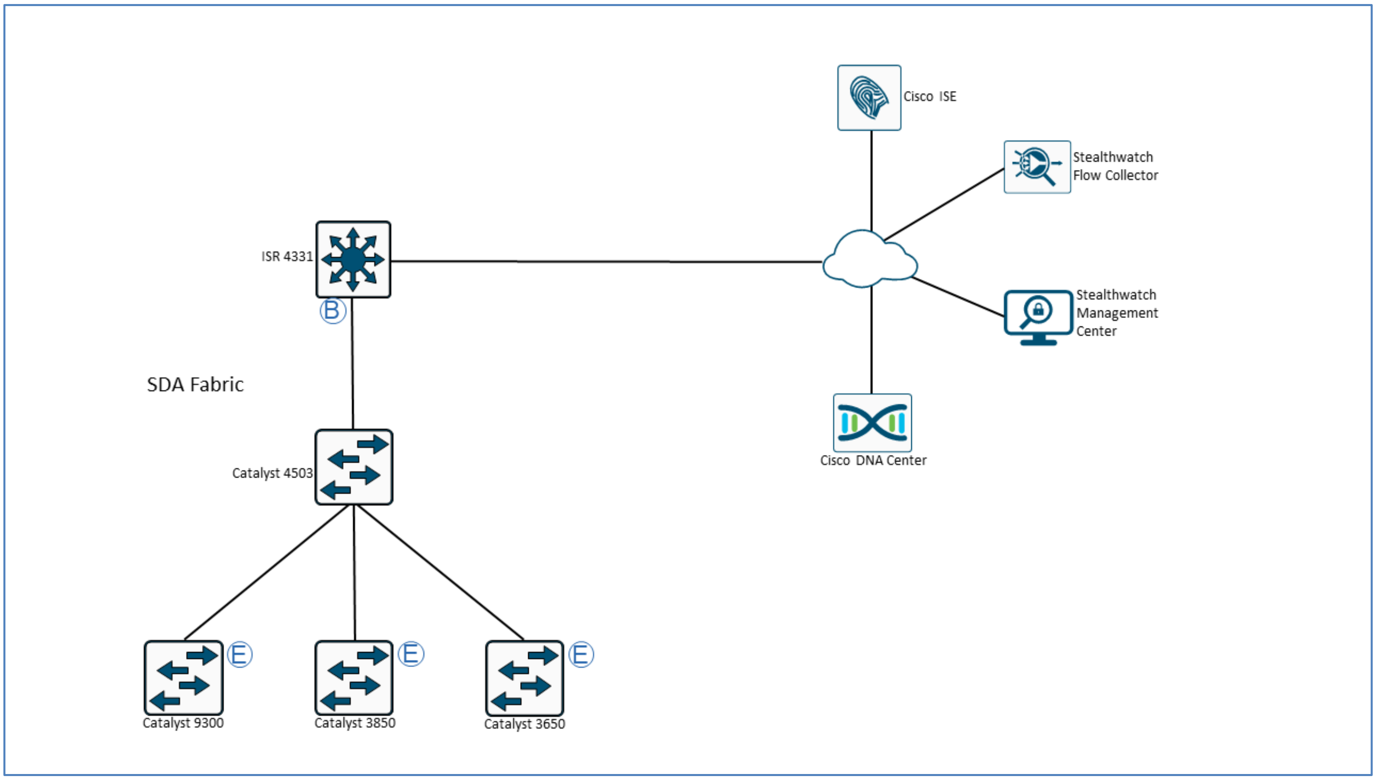


Figure 2 Topology

Process: Integrating Cognitive Intelligence with Stealthwatch

This Process assume that either direct communication or communication via a proxy are permitted from the Stealthwatch Management Console and Flow Collectors to the Cognitive Intelligence Cloud. These communications are all via port 443, and their addresses are:

Service Description	Service URL	Service IP
CTA login page CTA public landing page CTA TAXII service CTA data ingest service	https://cta.eu.amp.cisco.com https://cognitive.cisco.com (alias) https://td.cloudsec.sco.cisco.com/CWSP (alias) https://taxii.cloudsec.sco.cisco.com (alias) https://etr.cta.eu.amp.cisco.com scp+ssh://etr.cta.eu.amp.cisco.com https://etr.cloudsec.sco.cisco.com (alias) scp+ssh://etr.cloudsec.sco.cisco.com (alias)	AWS EIPs: • 34.242.41.248 • 34.242.94.137 • 34.251.54.105 • 34.251.210.21 • 34.255.162.33 • 54.194.49.205 Cisco IPs: • 146.112.59.0/24 • 208.69.38.0/24

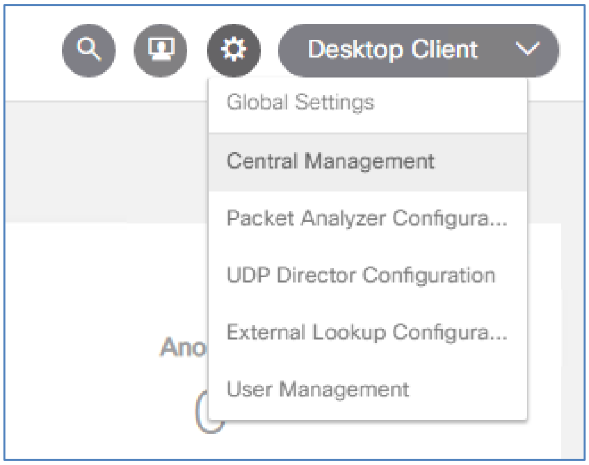
If you use the API offered by Cisco CTA to export your security data into your own SIEM solution, and you reference Cisco's API by IP address and not by URL, Cisco recommends that you change your setting in your SIEM solution to use the URL as high availability is implemented via Domain Name System (DNS).

For additional information, please refer to Cisco Field Notice FN-7205.

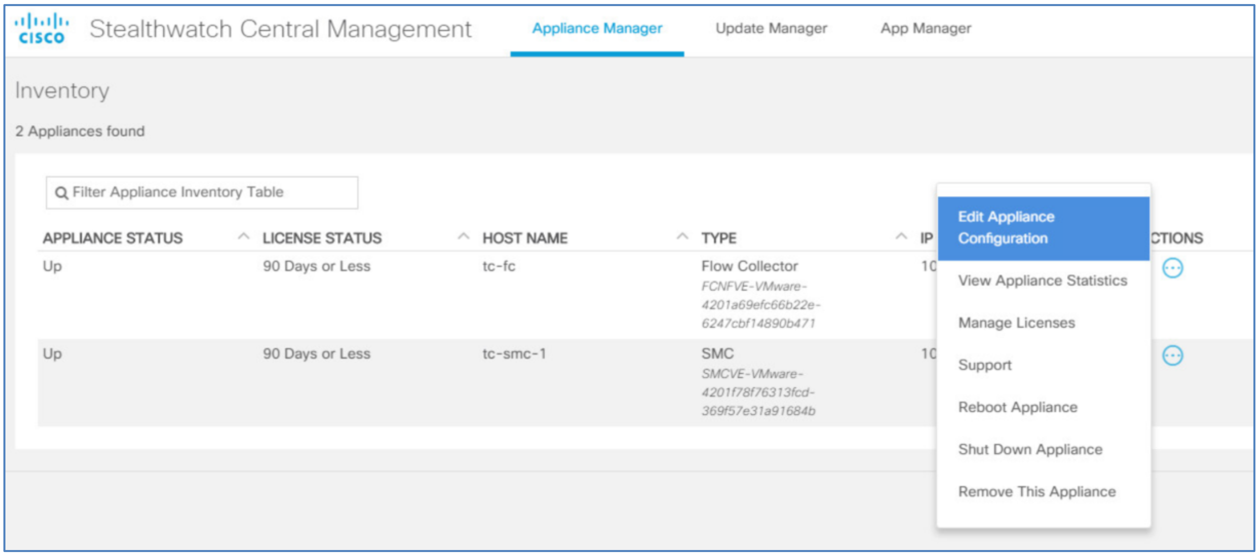
Procedure 1: Configure the Stealthwatch Management Console for Cognitive Intelligence integration

This Procedure documentsb the steps necessary to integrate the Stealthwatch Management Console with the Cognitive Intelligence portal for advanced threat detection enabled by ETA.

1. Log in to the Stealthwatch Management Console and click the global settings icon (gear) at the top right, then select Central Management.


Desktop Client
Global Settings
Central Management
Packet Analyzer Configura...
UDP Director Configuration
External Lookup Configura...
User Management
Ano

2. Click the actions button next to the SMC and select **Edit Appliance Configuration**.

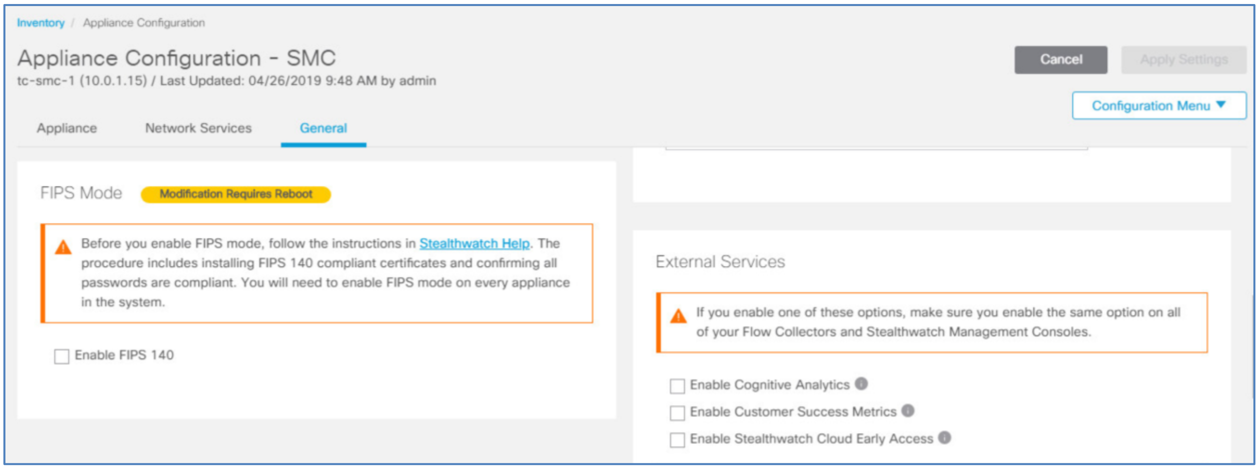


Inventory

2 Appliances found

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP	CTIONS
Up	90 Days or Less	tc-fc	Flow Collector *FCNFVE-VMware-4201a69efc66b22e-6247cbf14890b471*	10	
Up	90 Days or Less	tc-smc-1	SMC *SMCVE-VMware-4201f78f76313fcd-369f57e31a91684b*	10	

3. Select the **General** tab and scroll down to find the External Services section.



Appliance Configuration - SMC

tc-smc-1 (10.0.1.15) / Last Updated: 04/26/2019 9:48 AM by admin

FIPS Mode — Modification Requires Reboot

Before you enable FIPS mode, follow the instructions in Stealthwatch Help. The procedure includes installing FIPS 140 compliant certificates and confirming all passwords are compliant. You will need to enable FIPS mode on every appliance in the system.

□ Enable FIPS 140

External Services

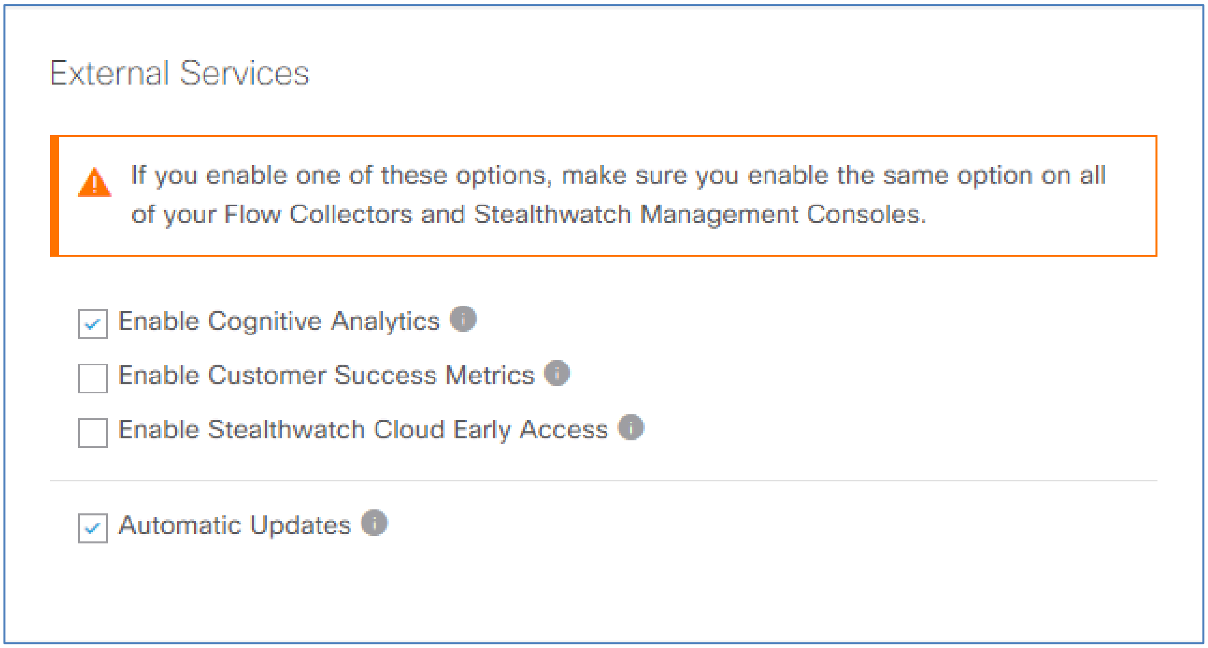
If you enable one of these options, make sure you enable the same option on all of your Flow Collectors and Stealthwatch Management Consoles.

□ Enable Cognitive Analytics

□ Enable Customer Success Metrics

□ Enable Stealthwatch Cloud Early Access

4. Click the checkbox next to **Enable Cognitive Analytics**, optionally click the box for Automatic updates.



External Services

If you enable one of these options, make sure you enable the same option on all of your Flow Collectors and Stealthwatch Management Consoles.

☑ Enable Cognitive Analytics

□ Enable Customer Success Metrics

□ Enable Stealthwatch Cloud Early Access

☑ Automatic Updates

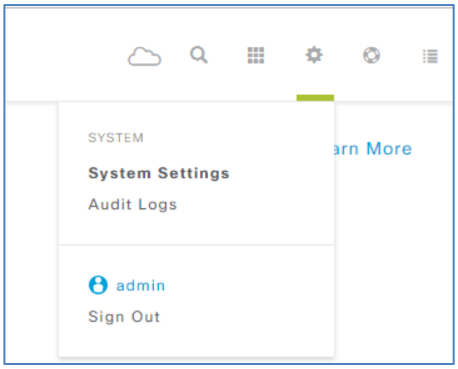
5. Repeat this procedure to enable Cognitive Analytics on each flow collector in your deployment.

Process: Provisioning ETA and FNF using SSA with Cisco DNA Center

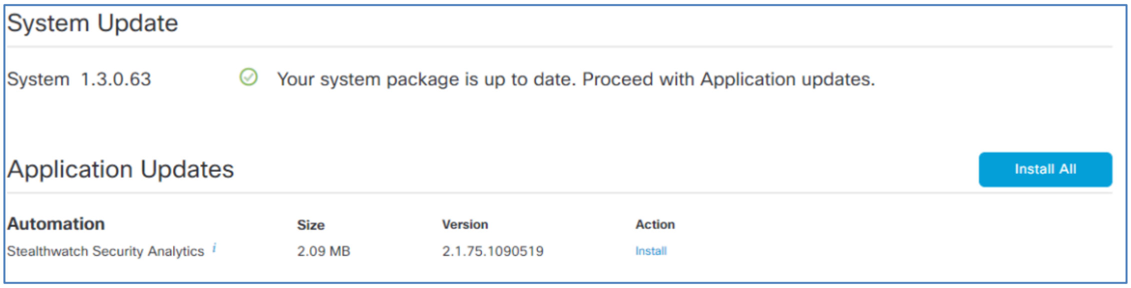
With the Cisco Stealthwatch Security Analytics service, we can now push ETA and FNF configurations to the proper devices without the need for templates or manual entry. This Process will document the steps necessary to install the SSA application and provision devices.

Procedure 1: Install Stealthwatch Security Analytics application in Cisco DNA Center

1. Access Cisco DNA Center and in the top right corner click the Settings icon (gear) and select **System Settings**



2. Select the **SOFTWARE UPDATES** tab and under Application Updates click **INSTALL** next to Stealthwatch Security Analytics.



System Update

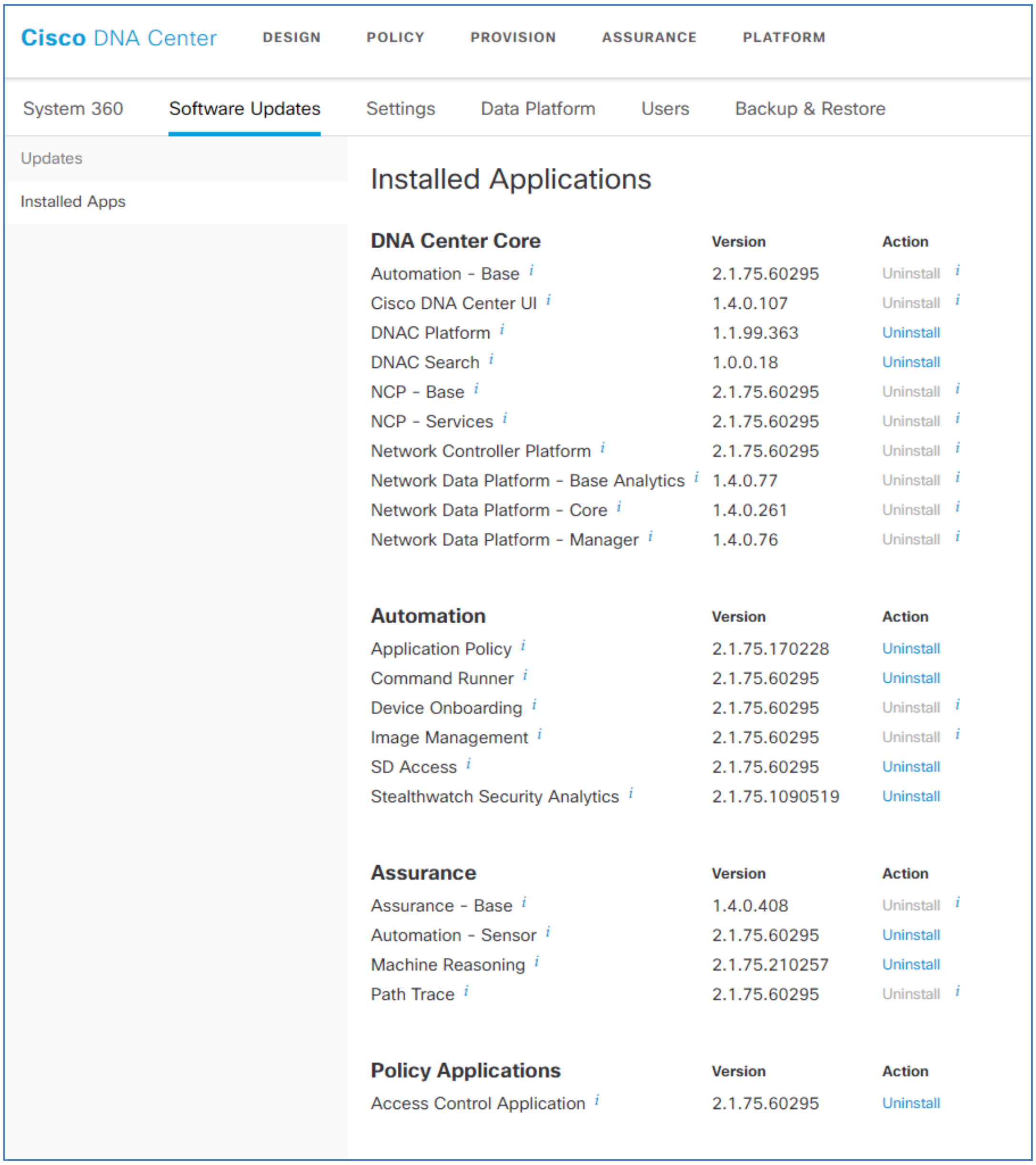
System 1.3.0.63 ✓ Your system package is up to date. Proceed with Application updates.

Application Updates

Install All

Automation	Size	Version	Action
Stealthwatch Security Analytics *i*	2.09 MB	2.1.75.1090519	Install

3. Once completed, Stealthwatch Security Analytics will disappear from under Application Updates. To verify the installation, click **INSTALLED APPS** at the top left corner and see that SSA is now installed under Automation.



Installed Applications

DNA Center Core	Version	Action
Automation - Base	2.1.75.60295	Uninstall
Cisco DNA Center UI	1.4.0.107	Uninstall
DNAC Platform	1.1.99.363	Uninstall
DNAC Search	1.0.0.18	Uninstall
NCP - Base	2.1.75.60295	Uninstall
NCP - Services	2.1.75.60295	Uninstall
Network Controller Platform	2.1.75.60295	Uninstall
Network Data Platform - Base Analytics	1.4.0.77	Uninstall
Network Data Platform - Core	1.4.0.261	Uninstall
Network Data Platform - Manager	1.4.0.76	Uninstall

Automation	Version	Action
Application Policy	2.1.75.170228	Uninstall
Command Runner	2.1.75.60295	Uninstall
Device Onboarding	2.1.75.60295	Uninstall
Image Management	2.1.75.60295	Uninstall
SD Access	2.1.75.60295	Uninstall
Stealthwatch Security Analytics	2.1.75.1090519	Uninstall

Assurance	Version	Action
Assurance - Base	1.4.0.408	Uninstall
Automation - Sensor	2.1.75.60295	Uninstall
Machine Reasoning	2.1.75.210257	Uninstall
Path Trace	2.1.75.60295	Uninstall

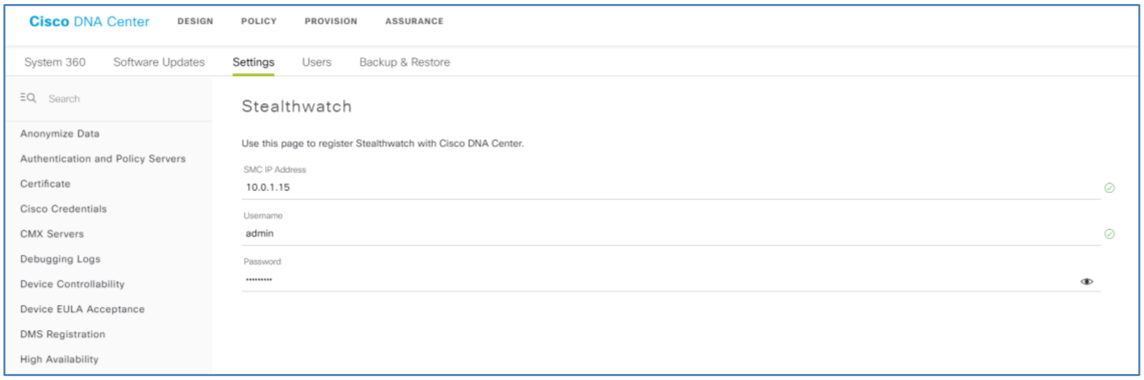
Policy Applications	Version	Action
Access Control Application	2.1.75.60295	Uninstall

Procedure 2 – Adding SMC to Cisco DNA Center

With the SSA Application installed, we now need to link our Stealthwatch Deployment with Cisco DNA Center.

1. Navigate back to **System Settings** and click the **Settings** tab.

2. Click **Stealthwatch** and enter the information for your Stealthwatch Management Console. Once completed click **Apply** at the bottom right corner.



Stealthwatch

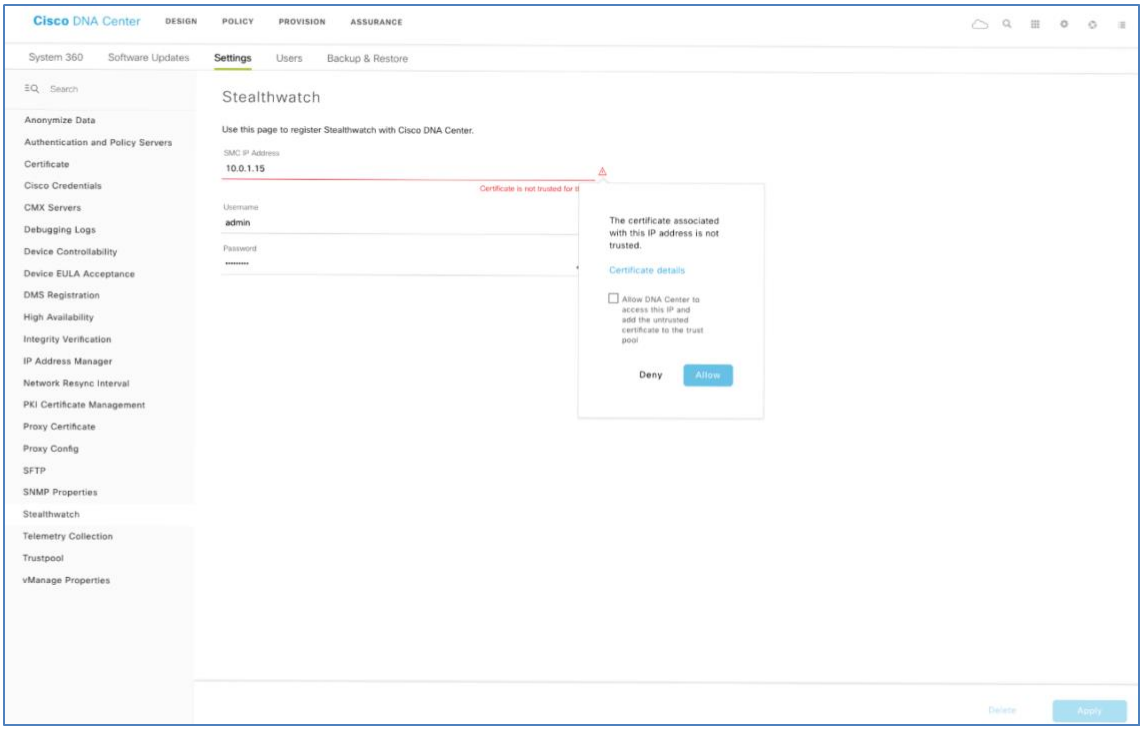
Use this page to register Stealthwatch with Cisco DNA Center.

SMC IP Address: 10.0.1.15

Username: admin

Password: •••••••••

3. If the IP address to which you are attempting to connect does not have a certificate signed by an official Certificate Authority, an alert appears. By default, the Stealthwatch Management Console ships with a self-signed certificate, which is not trusted. If not trusted as in the example below and you wish to continue, you can click on the red triangle next to the SMC IP Address and select Allow.



Stealthwatch

Use this page to register Stealthwatch with Cisco DNA Center.

SMC IP Address: 10.0.1.15

Certificate is not trusted for t

Username: admin

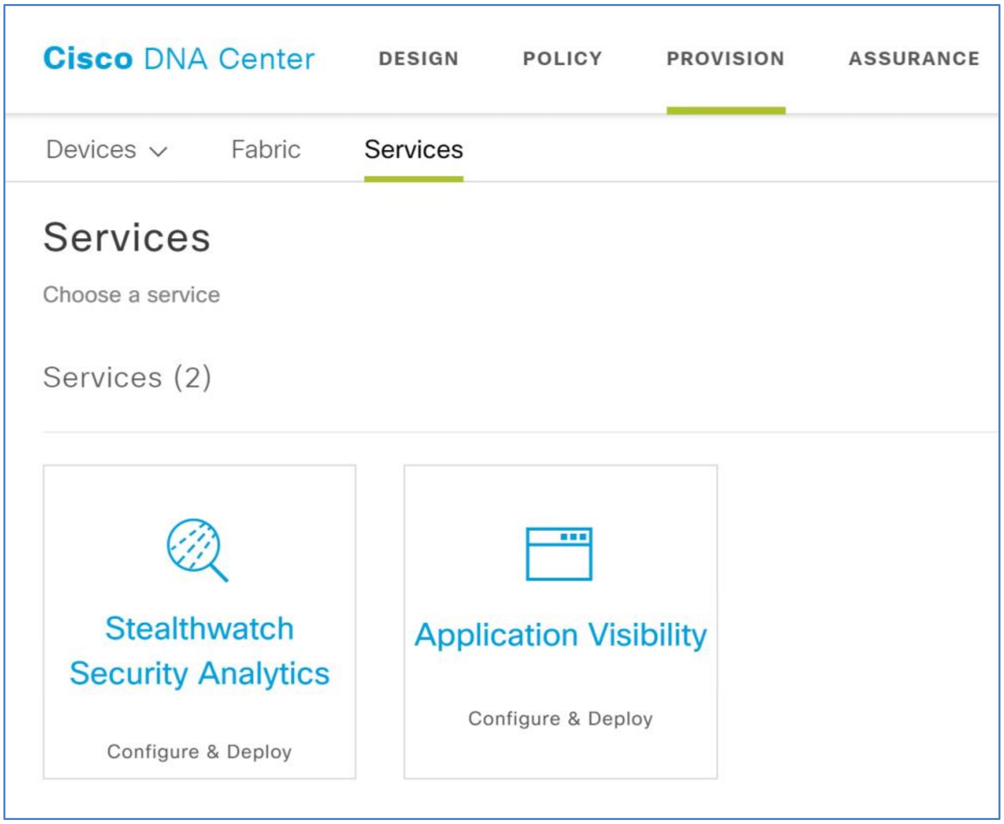
Password: •••••••••

The certificate associated with this IP address is not trusted.

□ Allow DNA Center to access this IP and add the untrusted certificate to the trust pool

Procedure 3 – Provision Devices for ETA and FNF using SSA

1. In Cisco DNA Center navigate to the Provision Page and click the **SERVICES** tab. Then select Stealthwatch Security Analytics service.

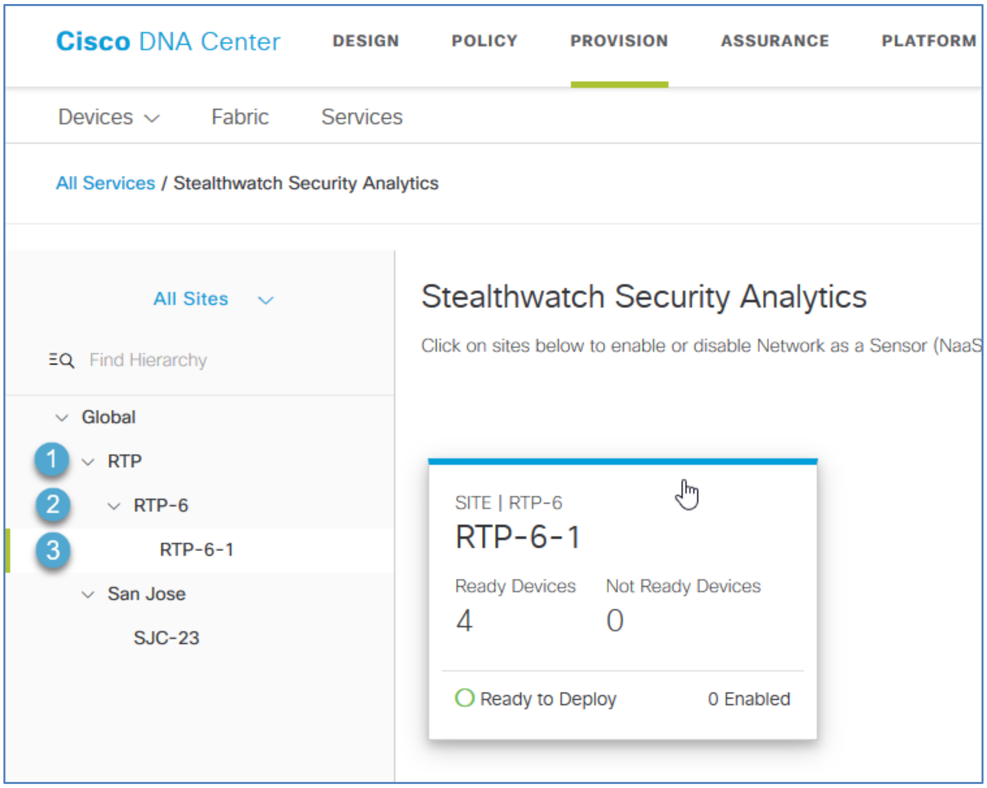


Services

Choose a service

Services (2)

2. As in the next screen, choose the Site (1), Building (2), or Floor (3) you would like to provision for ETA and FNF. Then click the site card.



Stealthwatch Security Analytics

Click on sites below to enable or disable Network as a Sensor (NaaS

SITE | RTP-6

RTP-6-1

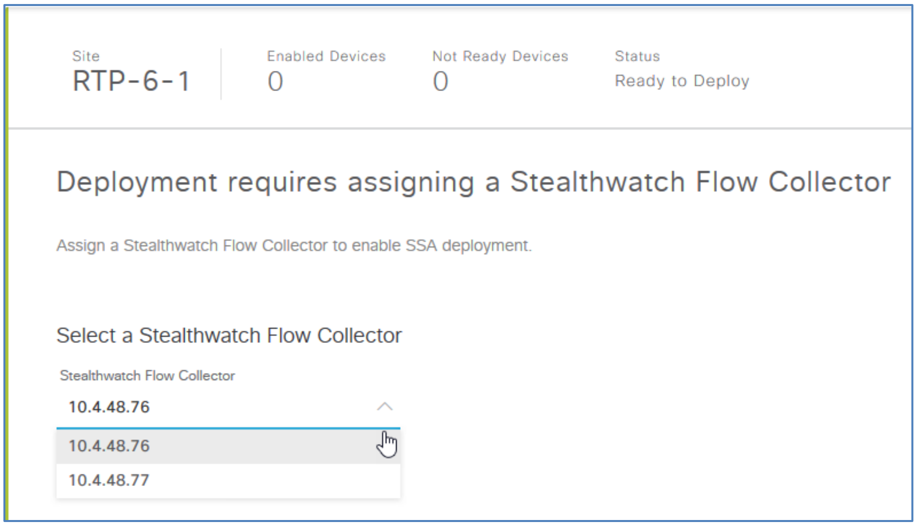
Ready Devices	Not Ready Devices
4	0

○ Ready to Deploy 0 Enabled

Site selection is hierarchal in nature, meaning that the higher levels will include all eligible devices on all floors or buildings that are underneath it.

3. The readiness check window opens. Click **Get Started** at the bottom right. In the flow collector assignment screen that appears, at the drop down, select the flow collector you would like to send FNF and ETA data then click **Next**.

The flow collector information will be pre-populated in the drop down as a result of the Stealthwatch Management Console integration performed earlier



Site
RTP-6-1

Enabled Devices
0

Not Ready Devices
0

Status
Ready to Deploy

Deployment requires assigning a Stealthwatch Flow Collector

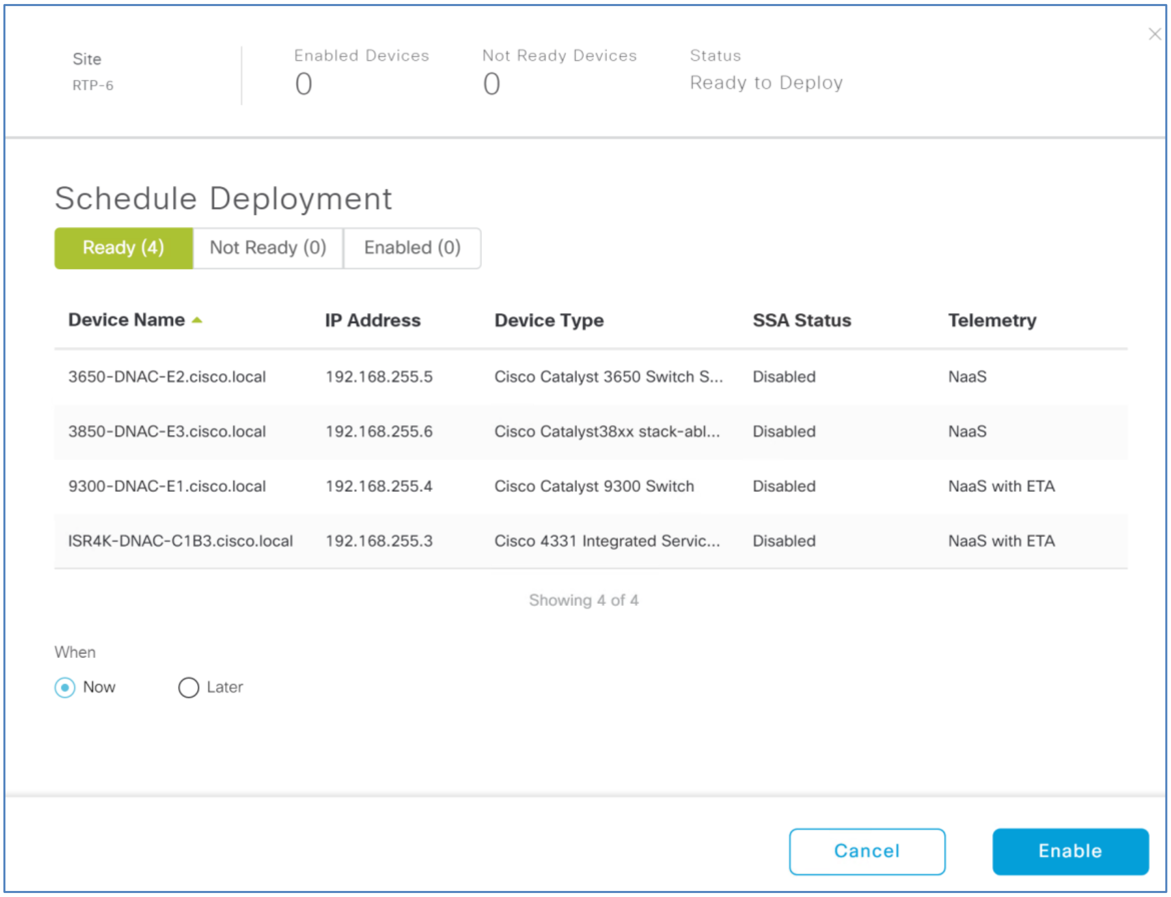
Assign a Stealthwatch Flow Collector to enable SSA deployment.

Select a Stealthwatch Flow Collector

Stealthwatch Flow Collector
10.4.48.76

4. In the next screen, you will see the devices determined by the SSA service to be ready, with their information and the type of telemetry that the device will be provisioned with. We see in the example deployment the Catalyst 3650 and 3850 are not ETA capable therefore they will only be provisioned with FNF as a Network as a Sensor configuration.

> Notice the Catalyst 4503, depicted in the earlier topology diagram, does not show up in the SSA application. This is because Cisco DNA Center has identified this switch as an intermediate node and assigned its device role as distribution, therefore it has no use in the SSA application.



Site
RTP-6

Enabled Devices
0

Not Ready Devices
0

Status
Ready to Deploy

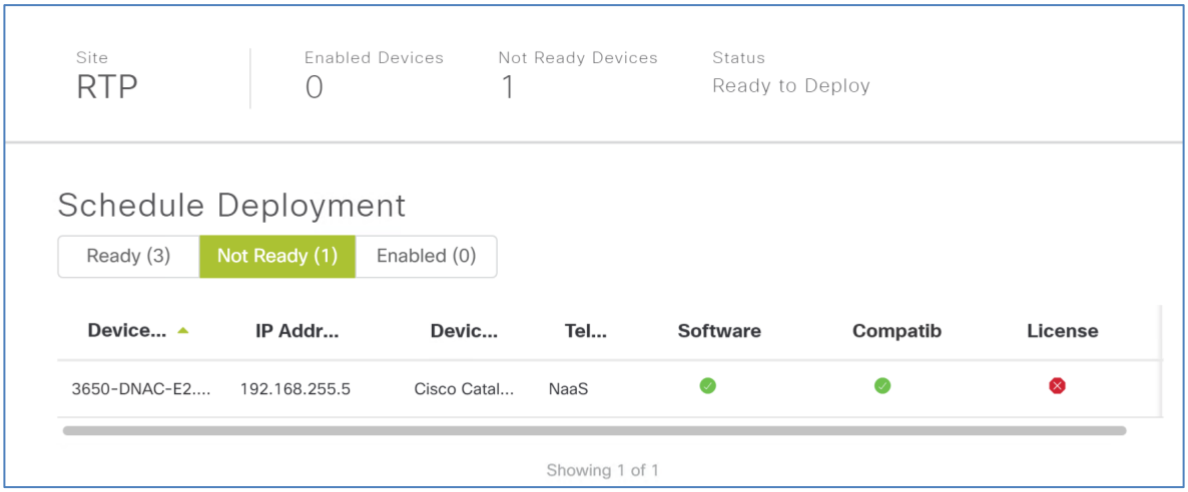
Schedule Deployment

Device Name ▲	IP Address	Device Type	SSA Status	Telemetry
3650-DNAC-E2.cisco.local	192.168.255.5	Cisco Catalyst 3650 Switch S...	Disabled	NaaS
3850-DNAC-E3.cisco.local	192.168.255.6	Cisco Catalyst38xx stack-abl...	Disabled	NaaS
9300-DNAC-E1.cisco.local	192.168.255.4	Cisco Catalyst 9300 Switch	Disabled	NaaS with ETA
ISR4K-DNAC-C1B3.cisco.local	192.168.255.3	Cisco 4331 Integrated Servic...	Disabled	NaaS with ETA

Showing 4 of 4

When
● Now ○ Later

5. If you click the **Not Ready** tab you will see a list of your devices that are not ready and the reason why, whether due to the software version, device compatibility or licensing.



Site
RTP

Enabled Devices
0

Not Ready Devices
1

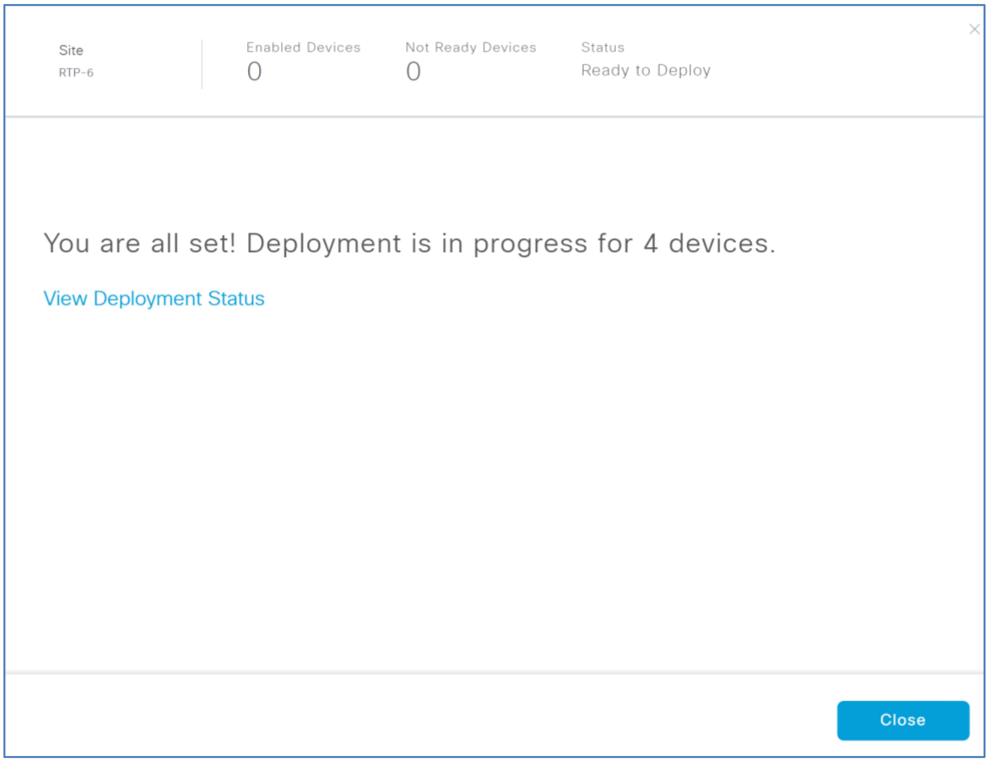
Status
Ready to Deploy

Schedule Deployment

Device... ▲	IP Addr...	Devic...	Tel...	Software	Compatib	License
3650-DNAC-E2....	192.168.255.5	Cisco Catal...	NaaS	✓	✓	✗

Showing 1 of 1

6. If you have all the devices wanted for your deployment in the Ready section, click the **Enable** button to have Cisco DNA Center automatically provision the devices for FNF and if capable ETA. The deployment process begins.



Site
RTP-6

Enabled Devices
0

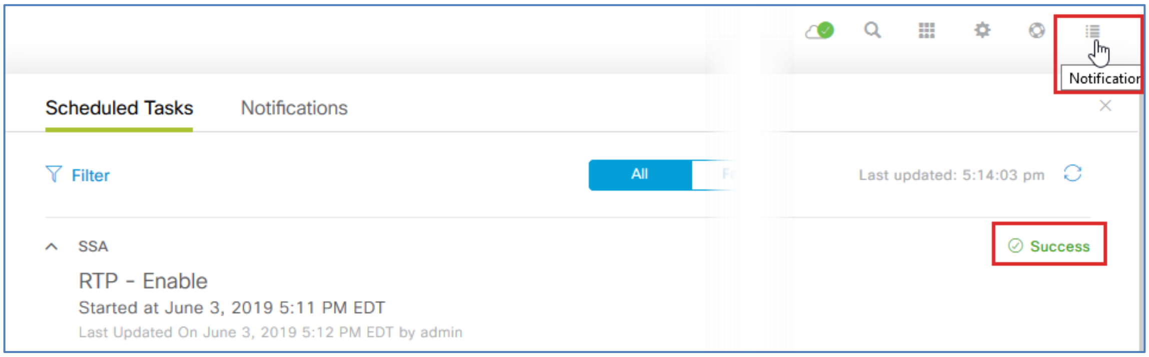
Not Ready Devices
0

Status
Ready to Deploy

You are all set! Deployment is in progress for 4 devices.

View Deployment Status

7. To verify, click **View Deployment Status** from above to see the task has been completed successfully or select the **Notifications** icon as seen below.



Last updated: 5:14:03 pm

SSA

RTP - Enable

Started at June 3, 2019 5:11 PM EDT

Last Updated On June 3, 2019 5:12 PM EDT by admin

Success

Operate

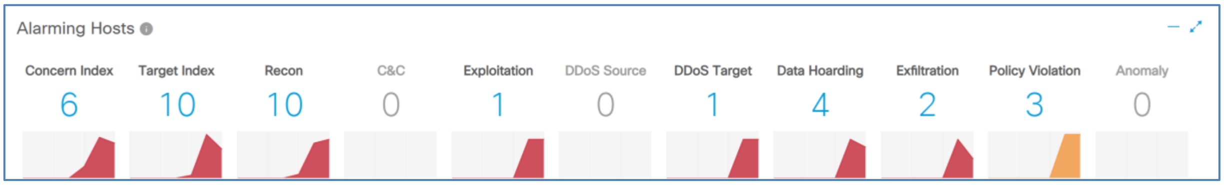
Navigating the Stealthwatch Security Insight Dashboard

The insight dashboard displays a variety of information regarding the status of the network. The following section gives a brief overview of the different parts of this dashboard

The Security Insight Dashboard will be the first page shown once logged into the Stealthwatch Management Console.

Alarming Hosts

At the top of the page, the Alarming Hosts shows the number of hosts that are currently alarming within a certain category.



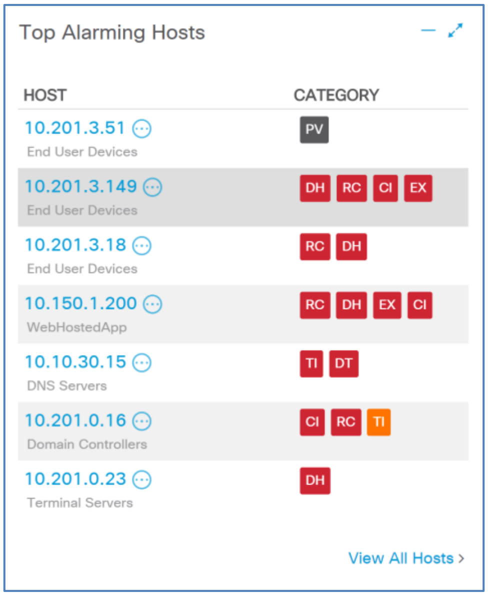
Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
6	10	10	0	1	0	1	4	2	3	0

The numbers are color-coded based on the overall severity of activity for the given alarm category. Beneath the number there is a trend graph that shows the total number of hosts that have generated alarms in the category, each day, for the past 7 days. Clicking on a number will pull up a list of all hosts currently generating alarms in the category.

Top Alarming Hosts

This section displays the top 7 alarming hosts in your environment. This is based on the overall amount of alarming behavior it has been a part of.



Top Alarming Hosts

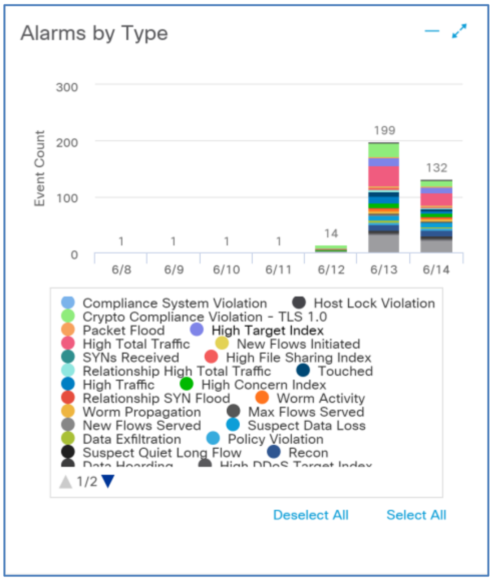
HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 WebHostedApp	RC DH EX CI
10.10.30.15 DNS Servers	TI DT
10.201.0.16 Domain Controllers	CI RC TI
10.201.0.23 Terminal Servers	DH

View All Hosts ›

You can mouse over the listed categories on the right to show the percentage of alarms over a normal host. Additionally, you can click the ellipsis (…) to dig down deeper into that host’s activities.

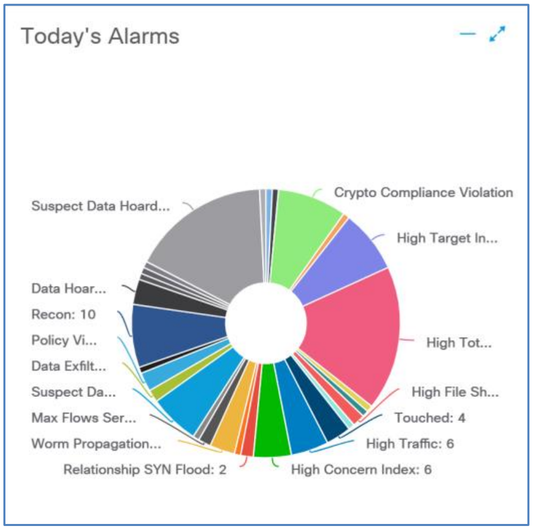
Alarms by Type

This is a graphical representation of the past week's alarms broken down by day and alarm type.



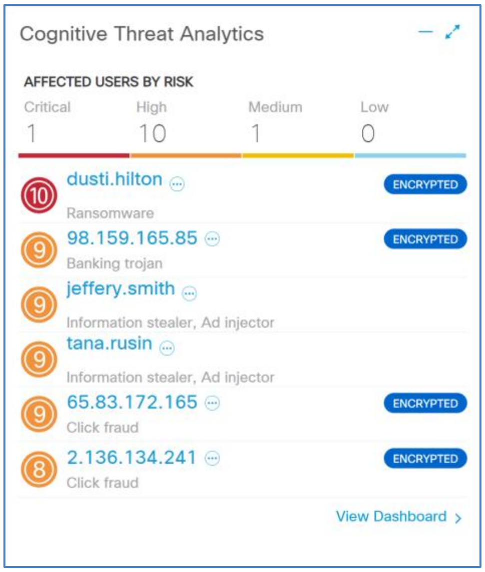
Today's Alarms

This pie chart provides an overview of all alarms that have occurred in the present day. You can click on any of the Alarm types in the chart to see the correlating alarm details for the day.



Cognitive Intelligence

Provides Stealthwatch with enhanced capabilities allowing for Encrypted Traffic Analytics.



Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low
1	10	1	0

10 dusti.hilton ENCRYPTED
Ransomware

9 98.159.165.85 ENCRYPTED
Banking trojan

9 jeffery.smith
Information stealer, Ad injector

9 tana.rusin
Information stealer, Ad injector

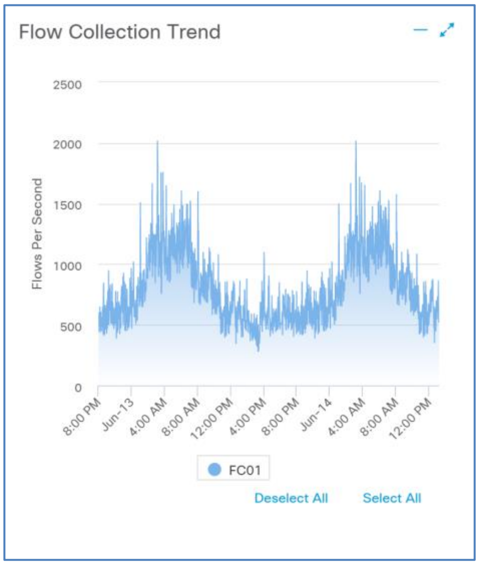
9 65.83.172.165 ENCRYPTED
Click fraud

8 2.136.134.241 ENCRYPTED
Click fraud

View Dashboard >

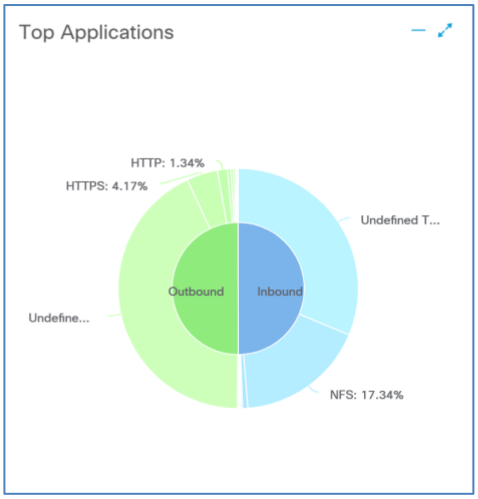
Flow Collection Tend

This chart shows the rate of NetFlow collection for all Flow Collectors over the past 48 hours. In deployments with multiple Collectors, you can select which appliance to see the collection trend for that particular collector.



Top Applications

This pie chart shows the top inbound and outbound application traffic types seen across the network.



Host Groups

Host Groups are containers of hosts or IP addresses that share attributes and policies. This allows you to better inform Stealthwatch about your network policy structure relative to user/server organizational groupings making it more efficient to establish acceptable communication patterns.

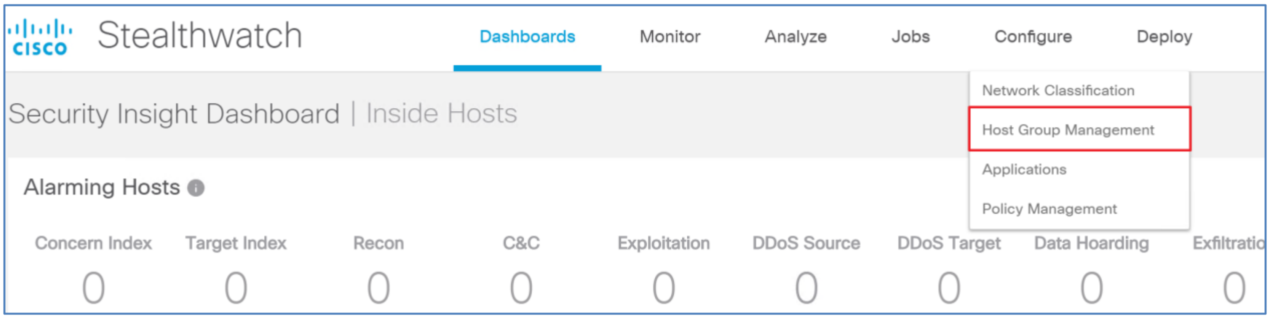
For example, if DHCP servers are configured within a host group, Stealthwatch knows they are legitimate. If a rogue DHCP server appears with an address outside the hostgroup and starts handing out addresses, Stealthwatch will be able to quickly raise an alert.

Inside Hosts

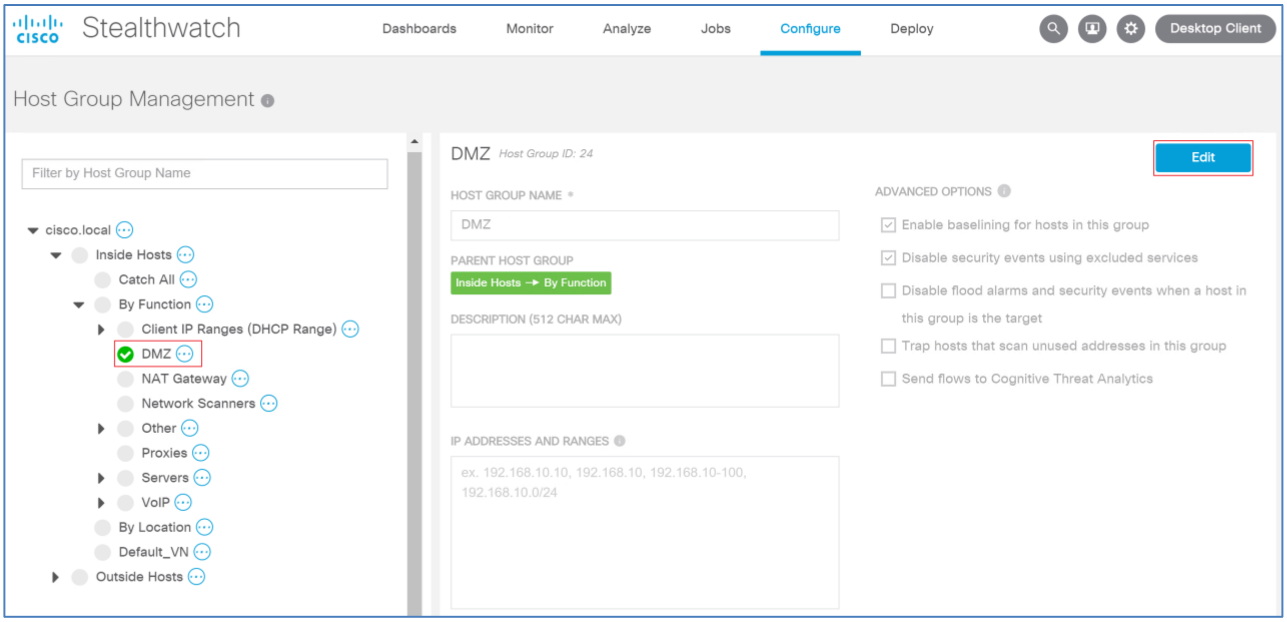
Inside Hosts are an integral part of Stealthwatch, they allow Stealthwatch to know what IP Addresses and Host Groups are considered internal to the network and which are not. By default, all RFC 1918 ranges are in the Inside Hosts/Catch All group. If using an IP range that is not covered by that spectrum for the internal network, it is important to add it to Inside Hosts so Stealthwatch does not report on inaccurate information.

Configuring a Host Group

1. Log into the Stealthwatch Management Console.
2. At the top hover over **Configure** and select **Host Group Management**



3. Inside the **Host Group Management** page, you will see there are already some pre-defined Host Groups. If wanted, you can configure these by selecting a group and clicking **Edit**.



DMZ *Host Group ID: 24*

HOST GROUP NAME * DMZ

PARENT HOST GROUP Inside Hosts → By Function

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES ex. 192.168.10.10, 192.168.10, 192.168.10-100, 192.168.10.0/24

ADVANCED OPTIONS

☑ Enable baselining for hosts in this group

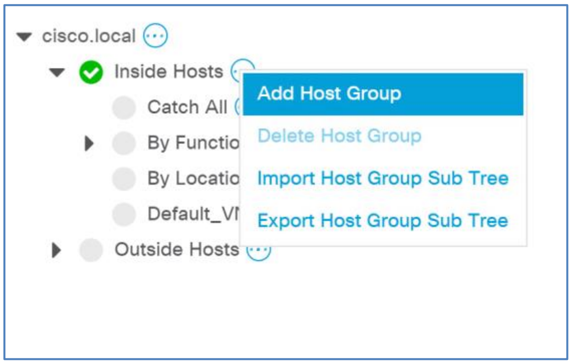
☑ Disable security events using excluded services

☐ Disable flood alarms and security events when a host in this group is the target

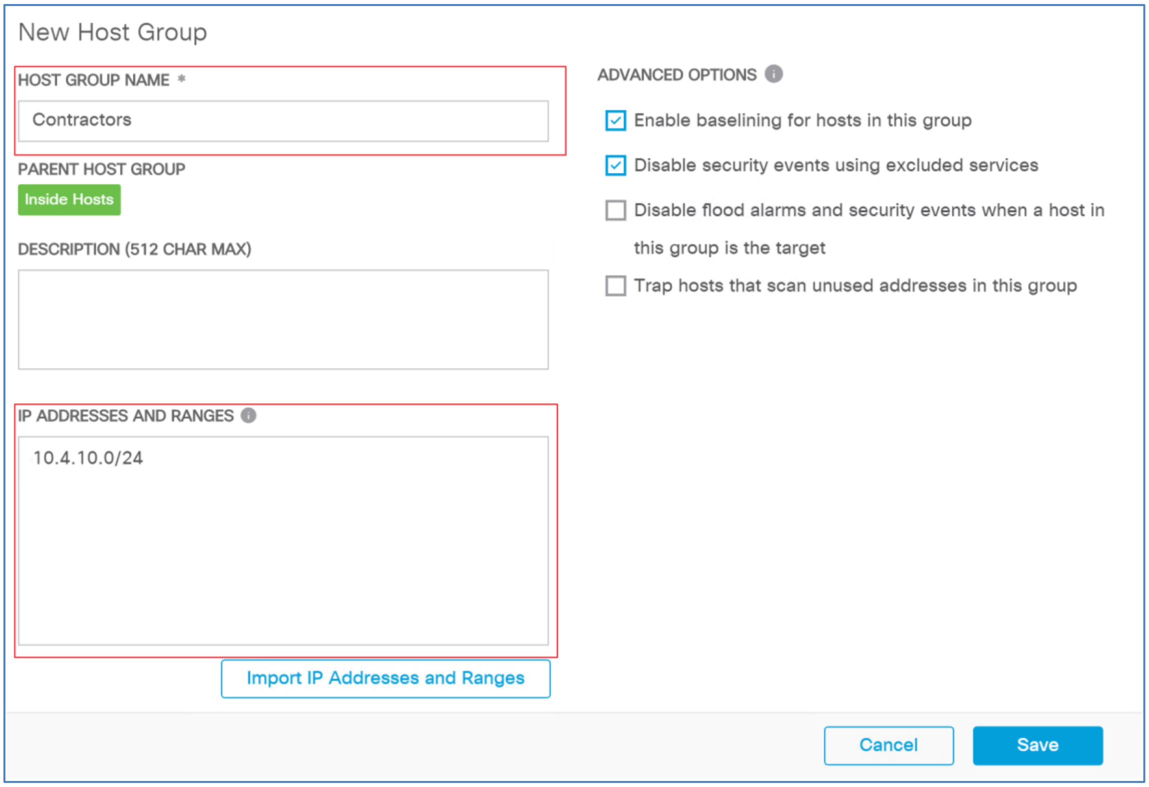
☐ Trap hosts that scan unused addresses in this group

☐ Send flows to Cognitive Threat Analytics

4. You can create a new group by clicking the ellipsis (…) next to the hierarchy you would like to add the group to and selecting **Add Host Group**.



In the resulting menu enter the group name under **Host Group Name** and then enter the IP range under the **IP Addresses and Ranges** section and click **Save**.



New Host Group

HOST GROUP NAME *

Contractors

PARENT HOST GROUP

Inside Hosts

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES

10.4.10.0/24

ADVANCED OPTIONS

☑ Enable baselining for hosts in this group

☑ Disable security events using excluded services

□ Disable flood alarms and security events when a host in this group is the target

□ Trap hosts that scan unused addresses in this group

Crypto Audit

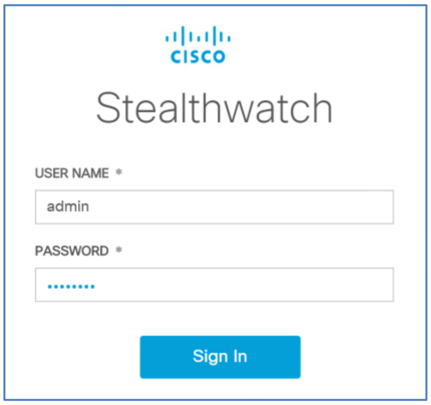
Crypto Audit is a useful tool to detect which cryptography version and cipher suite is being used within your network.

Preform a Crypto Audit Using the ETA Cryptographic Audit tool

Currently the Crypto Audit tool runs against the server-side flows in the selected host group. Therefor it is recommended to create or add internal servers into an inside host group to run the audit against.

> If wanting to see both client-side and server-side orientation see Perform a Crypto Audit using Flow Search.

1. To start a crypto audit log into the **Stealthwatch Management Console**.

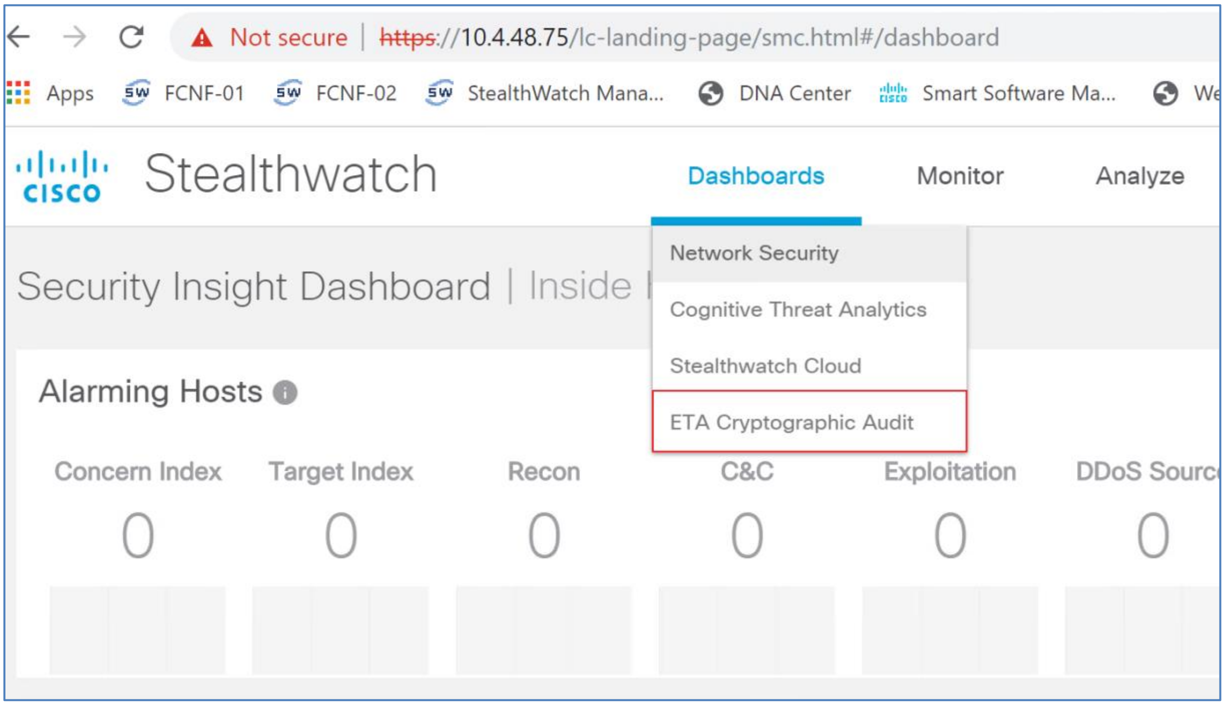


Stealthwatch

USER NAME * admin

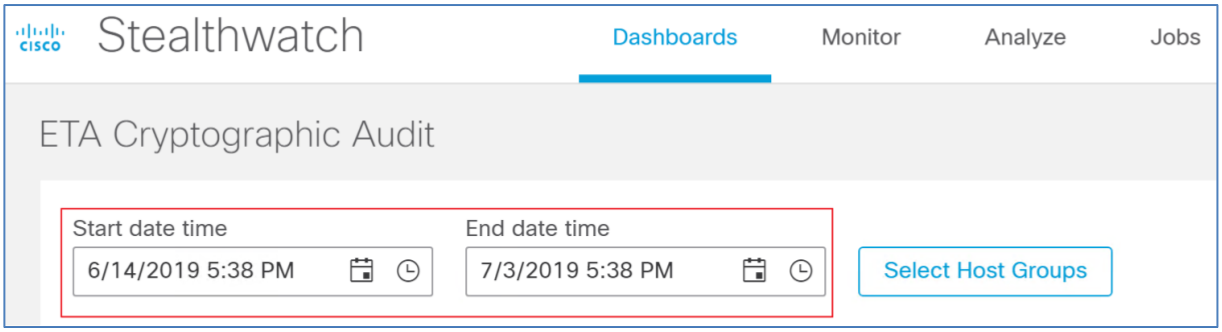
PASSWORD * ••••••••

2. Hover over **Dashboards** and select **ETA Cryptographic Audit**.



Not secure | ~~https~~://10.4.48.75/lc-landing-page/smc.html#/dashboard

3. In the Cryptographic Audit tool select the date and time you wish to run the audit.

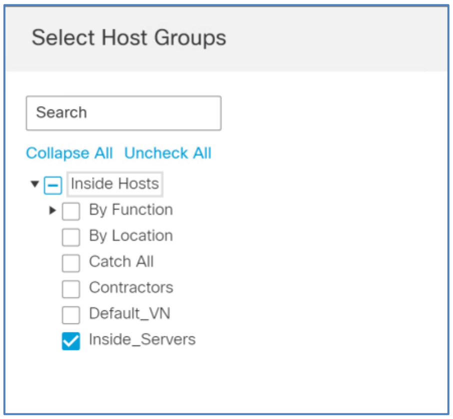


ETA Cryptographic Audit

Start date time: 6/14/2019 5:38 PM

End date time: 7/3/2019 5:38 PM

4. Click Select Host Group and pick the group you wish to run the audit for and click Apply.



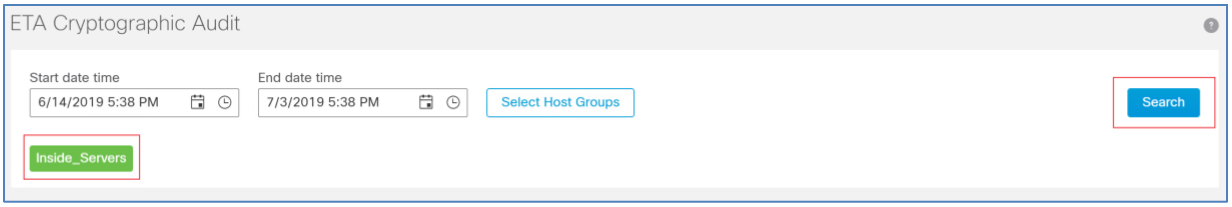
Select Host Groups

Search

Collapse All Uncheck All

- ⊟ Inside Hosts
  - □ By Function
  - □ By Location
  - □ Catch All
  - □ Contractors
  - □ Default_VN
  - ☑ Inside_Servers

5. You should now see the host groups selected under the Start Date Time. Click Search to start the Crypto Audit.



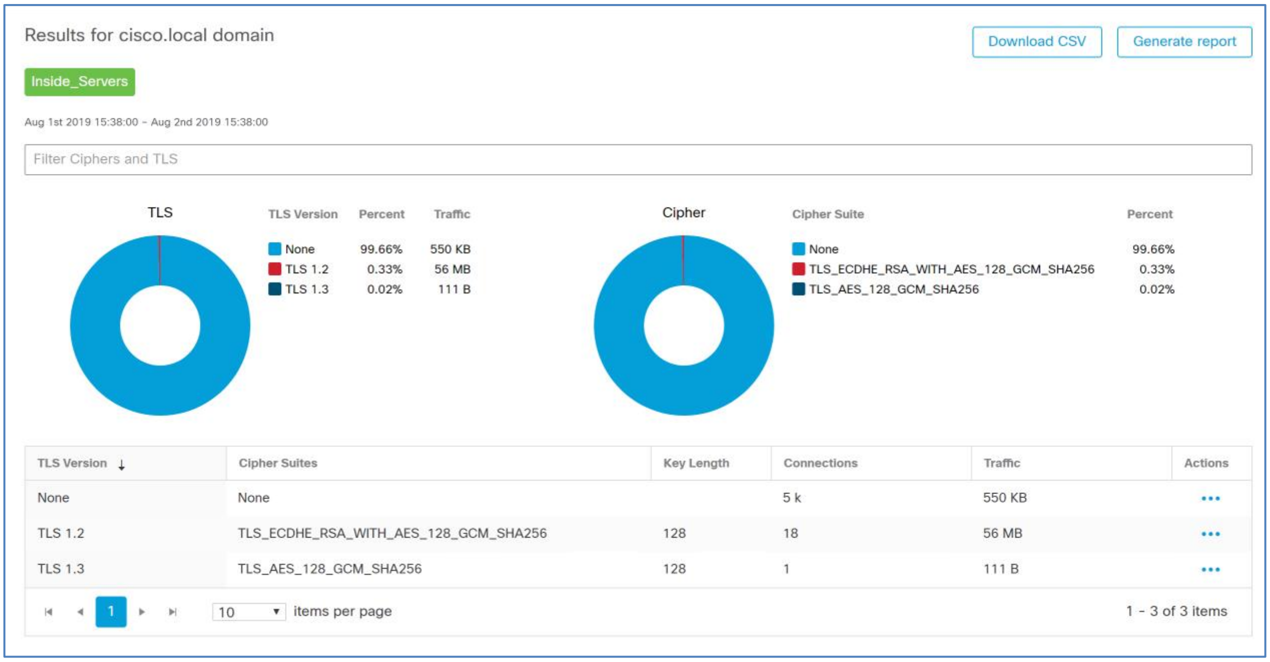
ETA Cryptographic Audit

Start date time: 6/14/2019 5:38 PM

End date time: 7/3/2019 5:38 PM

Inside_Servers

6. You will now see the results of the Crypto Audit showing the TLS version as well as the Cipher Suites being used.



Results for cisco.local domain

Download CSV | Generate report

Inside_Servers

Aug 1st 2019 15:38:00 - Aug 2nd 2019 15:38:00

Filter Ciphers and TLS

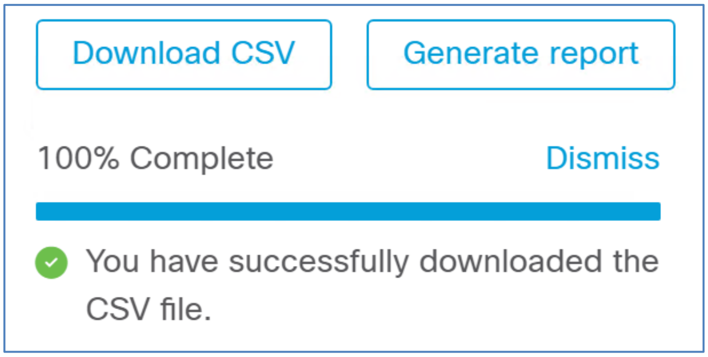
TLS Version	Percent	Traffic
🟦 None	99.66%	550 KB
🟥 TLS 1.2	0.33%	56 MB
■ TLS 1.3	0.02%	111 B

Cipher Suite	Percent
🟦 None	99.66%
🟥 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.33%
■ TLS_AES_128_GCM_SHA256	0.02%

TLS Version ↓	Cipher Suites	Key Length	Connections	Traffic	Actions
None	None		5 k	550 KB	•••
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128	18	56 MB	•••
TLS 1.3	TLS_AES_128_GCM_SHA256	128	1	111 B	•••

7. To export the report, click the download CSV file, this report produces a one-page report per server.

> In the current version of the crypto audit application, the support is limited to 100 servers.



100% Complete

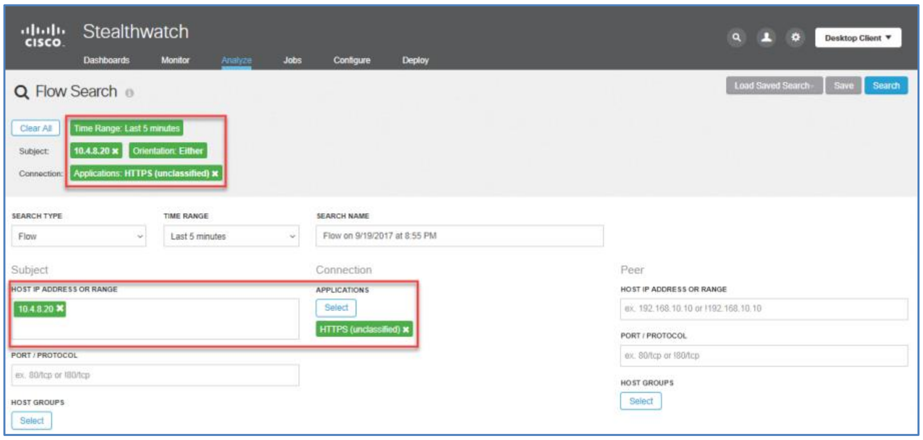
✓ You have successfully downloaded the CSV file.

Perform a Crypto Audit using Flow Search

1. In your browser, access SMC.

2. On the Dashboard, navigate to **ANALYZE > FLOW SEARCH.**

3. On the Flow Search page, create any filters against which you want to search.



Time Range: Last 5 minutes

Subject: 10.4.8.20 Orientation: Either

Connection: Applications: HTTPS (unclassified)

SEARCH TYPE: Flow

TIME RANGE: Last 5 minutes

SEARCH NAME: Flow on 9/19/2017 at 8:55 PM

Subject

HOST IP ADDRESS OR RANGE: 10.4.8.20

PORT / PROTOCOL: ex. 80/tcp or !80/tcp

HOST GROUPS

Connection

APPLICATIONS: HTTPS (unclassified)

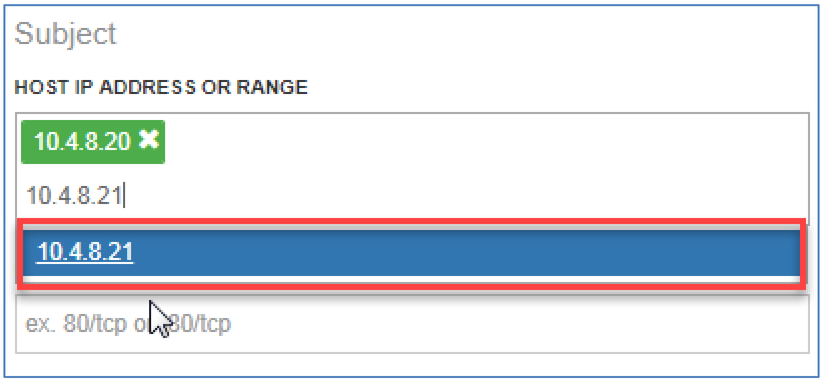
Peer

HOST IP ADDRESS OR RANGE: ex. 192.168.10.10 or !192.168.10.10

PORT / PROTOCOL: ex. 80/tcp or !80/tcp

HOST GROUPS

When you type information such as the IP address, select the box that appears (with the entered text underlined).



Subject

HOST IP ADDRESS OR RANGE

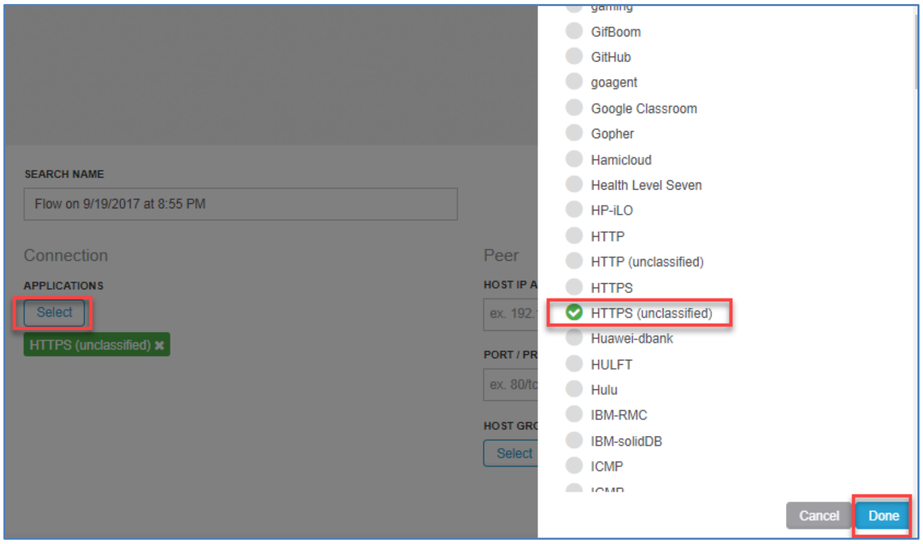
10.4.8.20

10.4.8.21

10.4.8.21

ex. 80/tcp or !80/tcp

4. To select a specific application, click the **SELECT** button. From the pop-up, select the application to filter on (in this case HTTPS has been selected), and then click **DONE.**



SEARCH NAME

Flow on 9/19/2017 at 8:55 PM

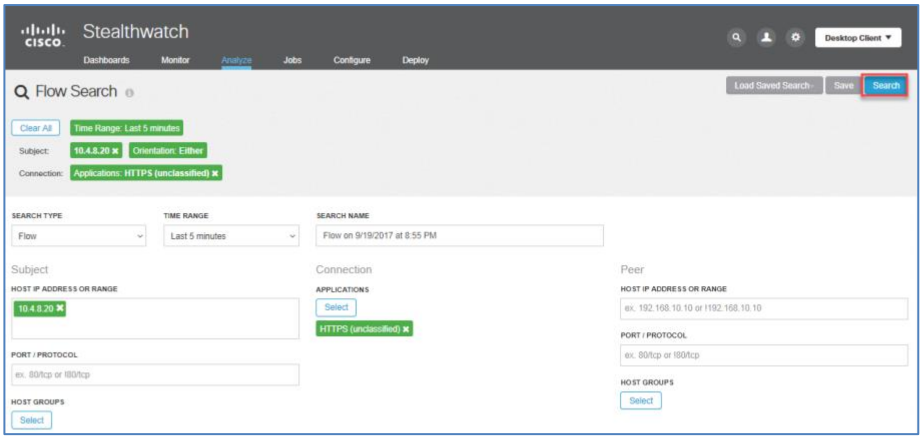
Connection

APPLICATIONS

HTTPS (unclassified)

✓ HTTPS (unclassified)

5. With search criteria defined, click **SEARCH**. The search begins.



Flow Search

Time Range: Last 5 minutes

Subject: 10.4.8.20 Orientation: Either

Connection: Applications: HTTPS (unclassified)

SEARCH TYPE: Flow

TIME RANGE: Last 5 minutes

SEARCH NAME: Flow on 9/19/2017 at 8:55 PM

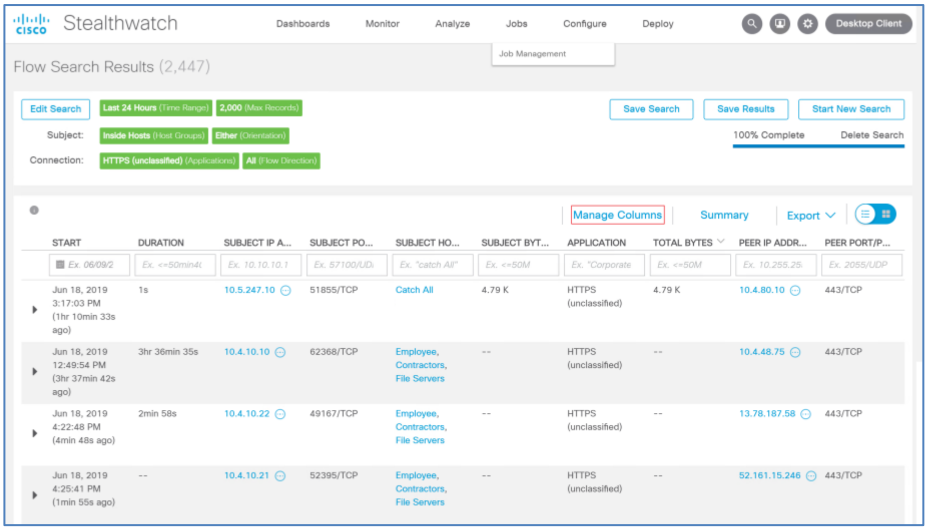
Subject

HOST IP ADDRESS OR RANGE: 10.4.8.20

Connection

APPLICATIONS: HTTPS (unclassified)

6. After the search has completed, the following screen appears, showing HTTPS flows and information derived from the IDP and TLS handshake. Notice that the ETA-specific data elements are not present. To enable the display of that information, click **MANAGE COLUMNS**.



Flow Search Results (2,447)

Last 24 Hours (Time Range) 2,000 (Max Records)

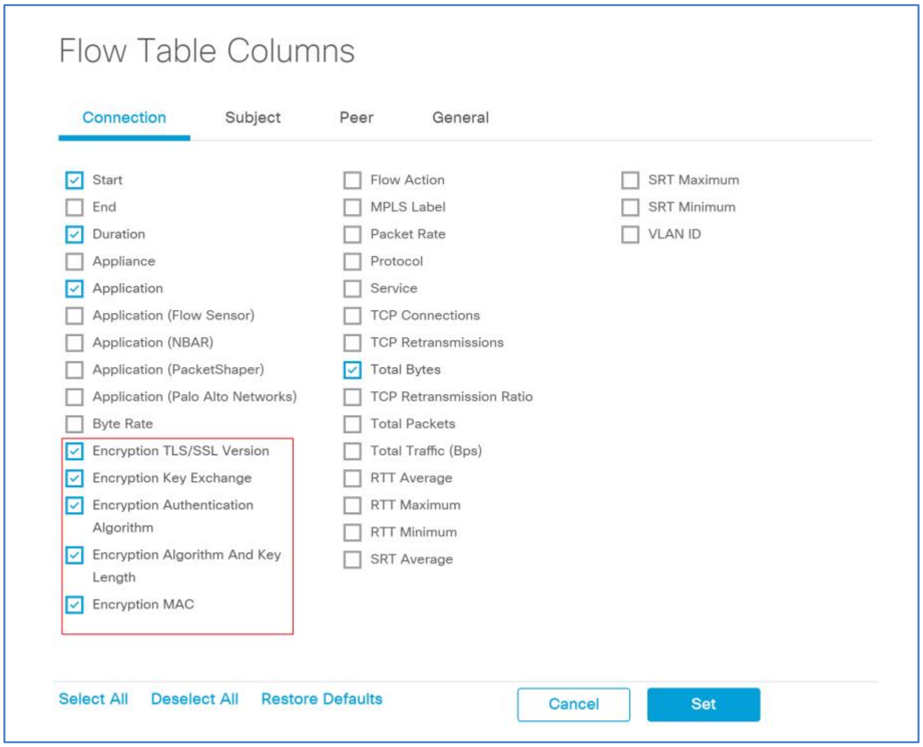
Subject: Inside Hosts (Host Groups) Either (Orientation)

Connection: HTTPS (unclassified) (Applications) All (Flow Direction)

100% Complete

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD/	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25	Ex. 2055/UDP
Jun 18, 2019 3:17:03 PM (1hr 10min 33s ago)	1s	10.5.247.10	51855/TCP	Catch All	4.79 K	HTTPS (unclassified)	4.79 K	10.4.80.10	443/TCP
Jun 18, 2019 12:49:54 PM (3hr 37min 42s ago)	3hr 36min 35s	10.4.10.10	62368/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	10.4.48.75	443/TCP
Jun 18, 2019 4:22:48 PM (4min 48s ago)	2min 58s	10.4.10.22	49167/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	13.78.187.58	443/TCP
Jun 18, 2019 4:25:41 PM (1min 55s ago)	--	10.4.10.21	52395/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	52.161.15.246	443/TCP

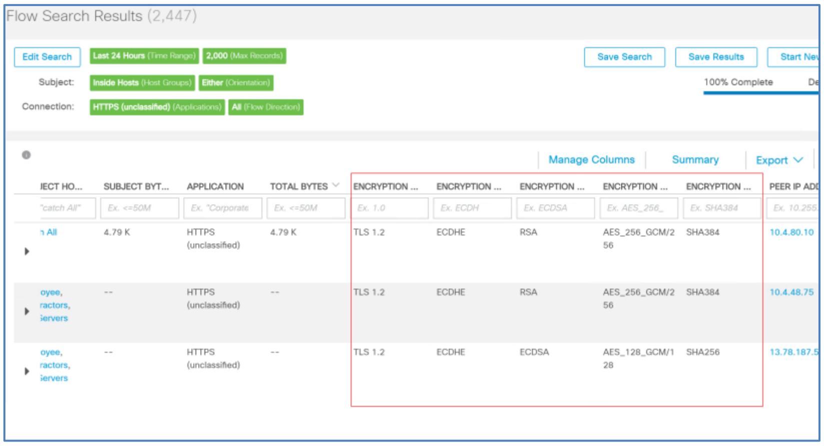
7. A pop-up appears. Scroll down and select the encryption fields to be added to the columns displayed. After selecting all encryption fields, scroll down and click **Set.**



Flow Table Columns

☑ Start
□ End
☑ Duration
□ Appliance
☑ Application
□ Application (Flow Sensor)
□ Application (NBAR)
□ Application (PacketShaper)
□ Application (Palo Alto Networks)
□ Byte Rate
☑ Encryption TLS/SSL Version
☑ Encryption Key Exchange
☑ Encryption Authentication Algorithm
☑ Encryption Algorithm And Key Length
☑ Encryption MAC
□ Flow Action
□ MPLS Label
□ Packet Rate
□ Protocol
□ Service
□ TCP Connections
□ TCP Retransmissions
☑ Total Bytes
□ TCP Retransmission Ratio
□ Total Packets
□ Total Traffic (Bps)
□ RTT Average
□ RTT Maximum
□ RTT Minimum
□ SRT Average
□ SRT Maximum
□ SRT Minimum
□ VLAN ID

8. Once the settings have been saved, the following screen appears, with all the encryption fields selected.



Flow Search Results (2,447)

Edit Search | **Last 24 Hours** (Time Range) | **2,000** (Max Records) | Save Search | Save Results | Start Nev

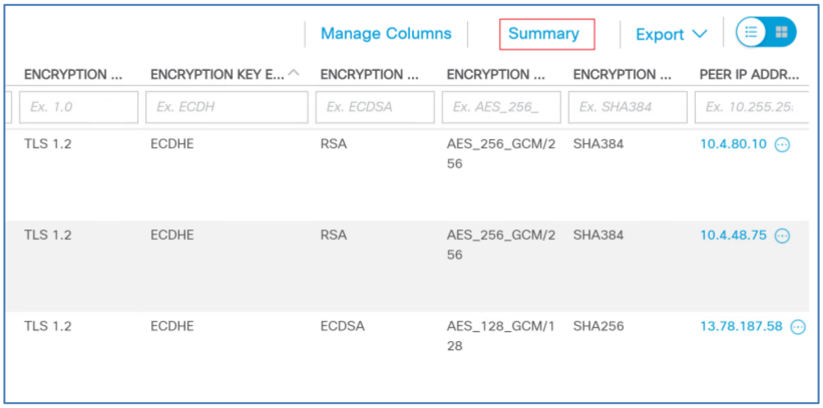
Subject: **Inside Hosts** (Host Groups) **Either** (Orientation) | 100% Complete | De

Connection: **HTTPS (unclassified)** (Applications) **All** (Flow Direction)

Manage Columns | Summary | Export

JECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADI
"catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255
ı All	4.79 K	HTTPS (unclassified)	4.79 K	TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.80.10
oyee, ractors, Servers	--	HTTPS (unclassified)	--	TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.48.75
oyee, ractors, Servers	--	HTTPS (unclassified)	--	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	13.78.187.5

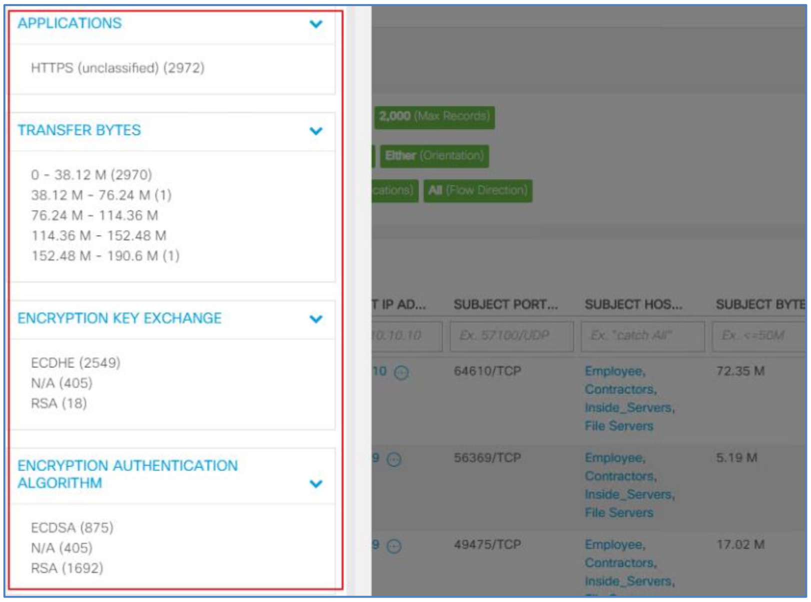
9. To produce an overview of the encryption information from the cipher suite used, click **SUMMARY.**



Manage Columns | Summary | Export

ENCRYPTION ...	ENCRYPTION KEY E...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADDR...
Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255.25
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.80.10
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.48.75
TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	13.78.187.58

10. This will bring up a panel on the side of your screen showcasing the information of the flow search in an organized view.



APPLICATIONS

HTTPS (unclassified) (2972)

TRANSFER BYTES

0 - 38.12 M (2970)
38.12 M - 76.24 M (1)
76.24 M - 114.36 M
114.36 M - 152.48 M
152.48 M - 190.6 M (1)

ENCRYPTION KEY EXCHANGE

ECDHE (2549)
N/A (405)
RSA (18)

ENCRYPTION AUTHENTICATION ALGORITHM

ECDSA (875)
N/A (405)
RSA (1692)

2,000 (Max Records)

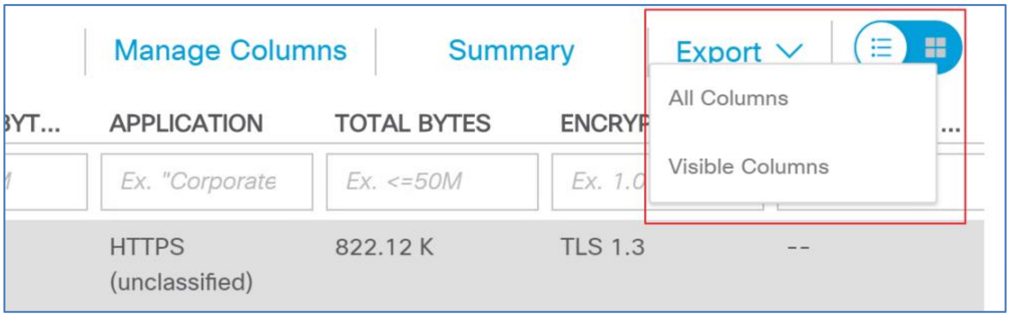
Either (Orientation)

cations) **All** (Flow Direction)

T IP AD...	SUBJECT PORT...	SUBJECT HOS...	SUBJECT BYTE
0.10.10	Ex. 57100/UDP	Ex. "catch All"	Ex. <=50M
10	64610/TCP	Employee, Contractors, Inside_Servers, File Servers	72.35 M
9	56369/TCP	Employee, Contractors, Inside_Servers, File Servers	5.19 M
9	49475/TCP	Employee, Contractors, Inside_Servers,	17.02 M

In the current version of Stealthwatch there is a known bug that is causing the Encryption TLS/SSL Version field from showing up in the summary view.

11. Once finished, you can click Export and choose either ALL COLUMNS or VISIBLE COLUMNS and it will be exported in CSV format to an Excel spreadsheet.

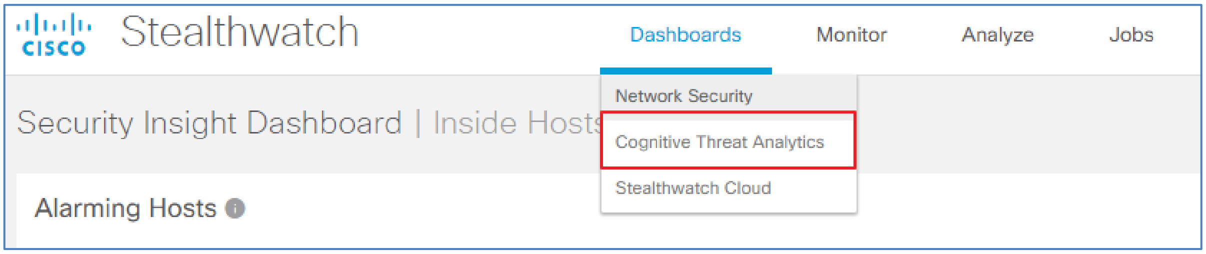


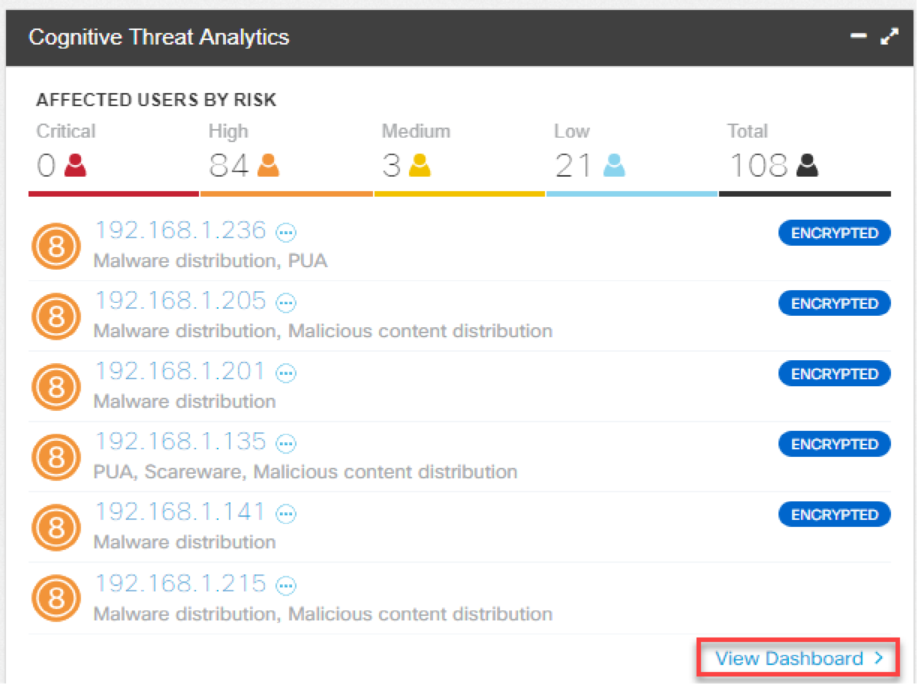
Investigate suspicious activity for malware through Cognitive Intelligence

The following information is meant to serve as a brief example of navigating the Cognitive Intelligence user interface in investigating infected hosts and suspicious activity. For complete information regarding portal administration and the fields displayed, refer to the Cisco ScanCenter Administrator Guide.

1. Access to the Cognitive Intelligence portal is integrated within the Stealthwatch Security Insight Dashboard. Within the SMC Dashboard, under Dashboards, access to the portal is available by selecting Cognitive Intelligence or by scrolling down to the Cognitive Intelligence widget as shown below and clicking View Dashboard.

   In the Cognitive Intelligence widget in SMC, a summary of "Affected Users by Risk" can be seen. The blue "Encrypted" bubble next to each IP address signifies that this had been classified as a result of ETA data elements within the Cognitive Intelligence Cloud.





Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low	Total
0	84	3	21	108

8 192.168.1.236 — ENCRYPTED
Malware distribution, PUA

8 192.168.1.205 — ENCRYPTED
Malware distribution, Malicious content distribution

8 192.168.1.201 — ENCRYPTED
Malware distribution

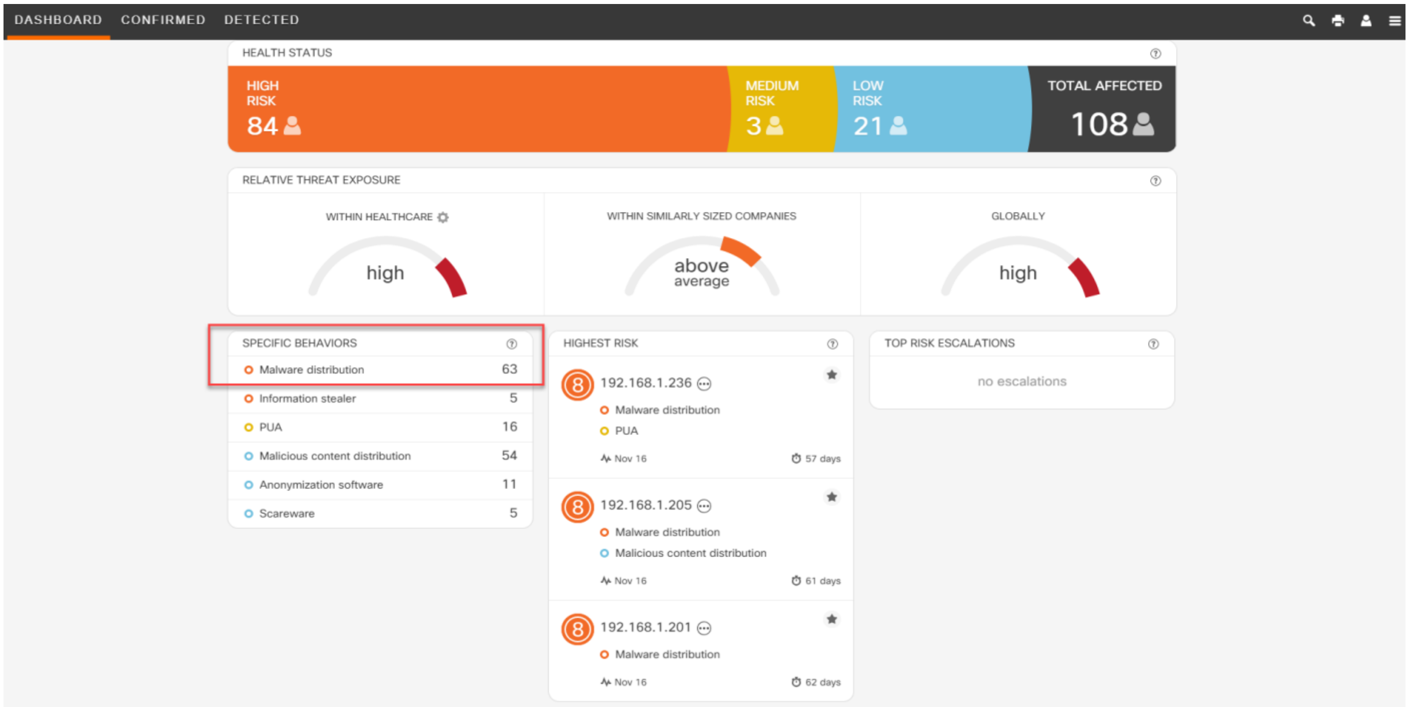
8 192.168.1.135 — ENCRYPTED
PUA, Scareware, Malicious content distribution

8 192.168.1.141 — ENCRYPTED
Malware distribution

8 192.168.1.215
Malware distribution, Malicious content distribution

View Dashboard >

2. Within the Cognitive Intelligence portal, the first view accessed is the Dashboard view. From this view, you can quickly view the overall health status of your network. Clicking any of the specific behaviors, such as **MALWARE DISTRIBUTION**, displays a summary of compromised or suspicious endpoints.



DASHBOARD CONFIRMED DETECTED

HEALTH STATUS

HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL AFFECTED
84	3	21	108

RELATIVE THREAT EXPOSURE

WITHIN HEALTHCARE	WITHIN SIMILARLY SIZED COMPANIES	GLOBALLY
high	above average	high

SPECIFIC BEHAVIORS

Malware distribution	63
Information stealer	5
PUA	16
Malicious content distribution	54
Anonymization software	11
Scareware	5

HIGHEST RISK

8 192.168.1.236
Malware distribution
PUA
Nov 16 — 57 days

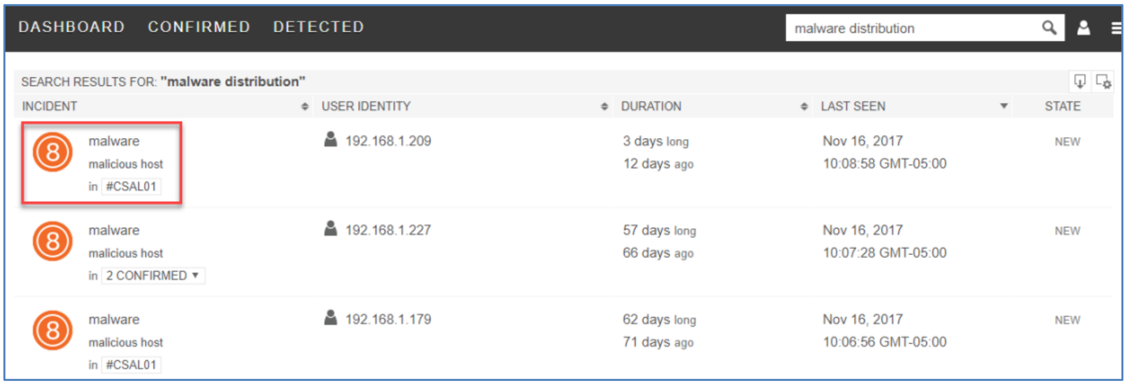
8 192.168.1.205
Malware distribution
Malicious content distribution
Nov 16 — 61 days

8 192.168.1.201
Malware distribution
Nov 16 — 62 days

TOP RISK ESCALATIONS

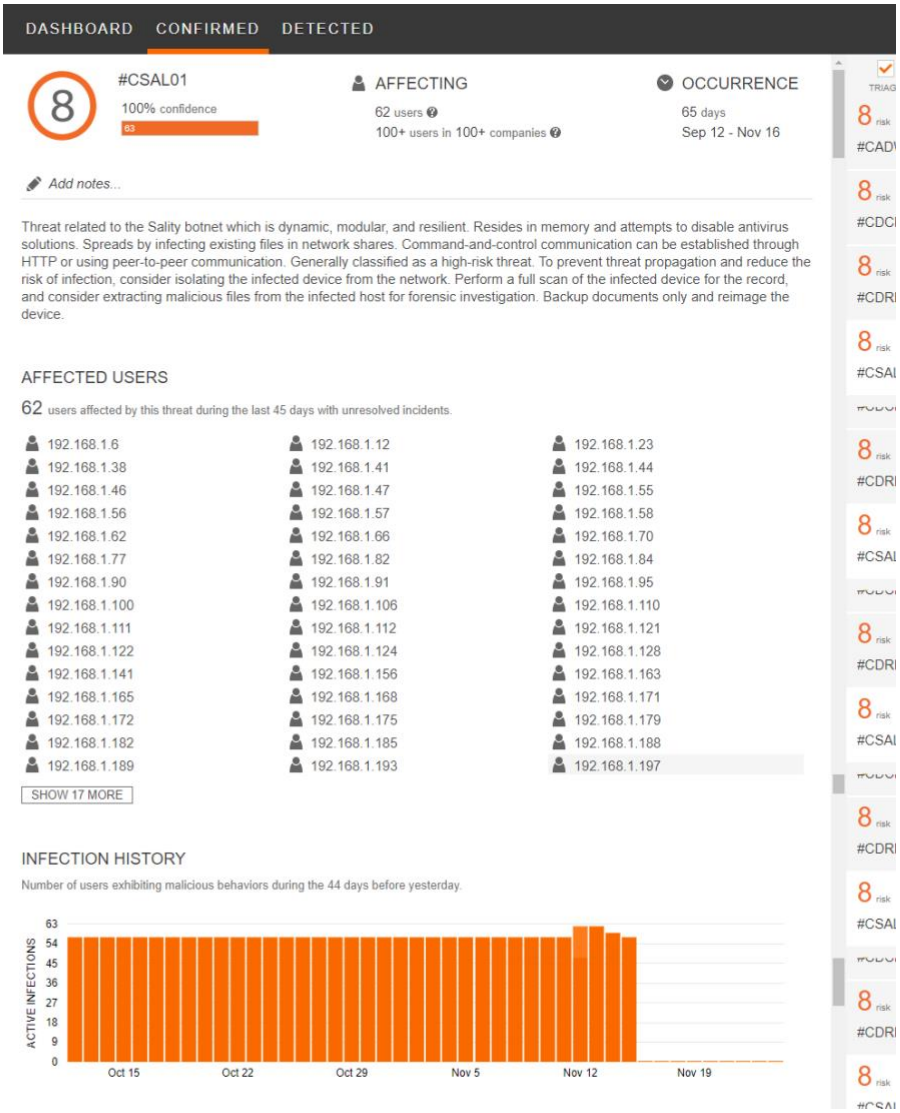
no escalations

3. With the summary information displayed, selecting the malware detected provides a description of the malware as well as a summary of infected devices in your network.



SEARCH RESULTS FOR: **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	STATE
8 malware malicious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2017 10:08:58 GMT-05:00	NEW
8 malware malicious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2017 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2017 10:06:56 GMT-05:00	NEW



#CSAL01

100% confidence

63

AFFECTING

62 users

100+ users in 100+ companies

OCCURRENCE

65 days

Sep 12 - Nov 16

Add notes...

Threat related to the Sality botnet which is dynamic, modular, and resilient. Resides in memory and attempts to disable antivirus solutions. Spreads by infecting existing files in network shares. Command-and-control communication can be established through HTTP or using peer-to-peer communication. Generally classified as a high-risk threat. To prevent threat propagation and reduce the risk of infection, consider isolating the infected device from the network. Perform a full scan of the infected device for the record, and consider extracting malicious files from the infected host for forensic investigation. Backup documents only and reimage the device.

AFFECTED USERS

62 users affected by this threat during the last 45 days with unresolved incidents.

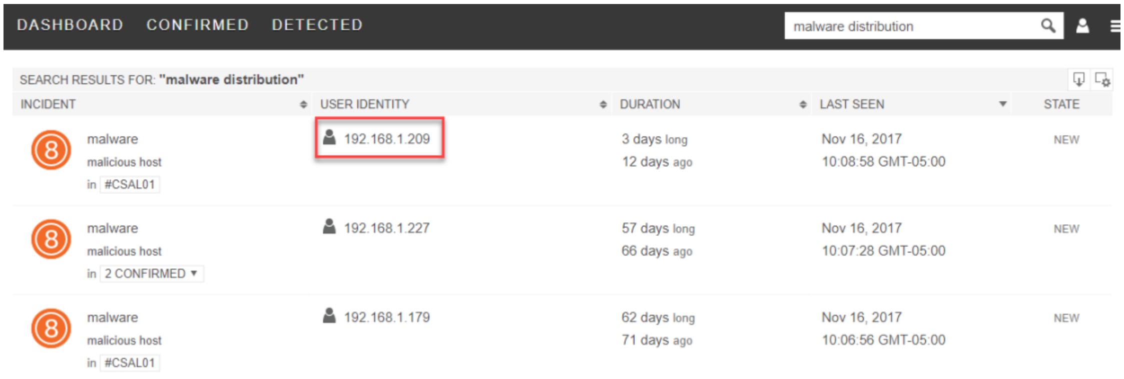
192.168.1.6	192.168.1.12	192.168.1.23
192.168.1.38	192.168.1.41	192.168.1.44
192.168.1.46	192.168.1.47	192.168.1.55
192.168.1.56	192.168.1.57	192.168.1.58
192.168.1.62	192.168.1.66	192.168.1.70
192.168.1.77	192.168.1.82	192.168.1.84
192.168.1.90	192.168.1.91	192.168.1.95
192.168.1.100	192.168.1.106	192.168.1.110
192.168.1.111	192.168.1.112	192.168.1.121
192.168.1.122	192.168.1.124	192.168.1.128
192.168.1.141	192.168.1.156	192.168.1.163
192.168.1.165	192.168.1.168	192.168.1.171
192.168.1.172	192.168.1.175	192.168.1.179
192.168.1.182	192.168.1.185	192.168.1.188
192.168.1.189	192.168.1.193	192.168.1.197

SHOW 17 MORE

INFECTION HISTORY

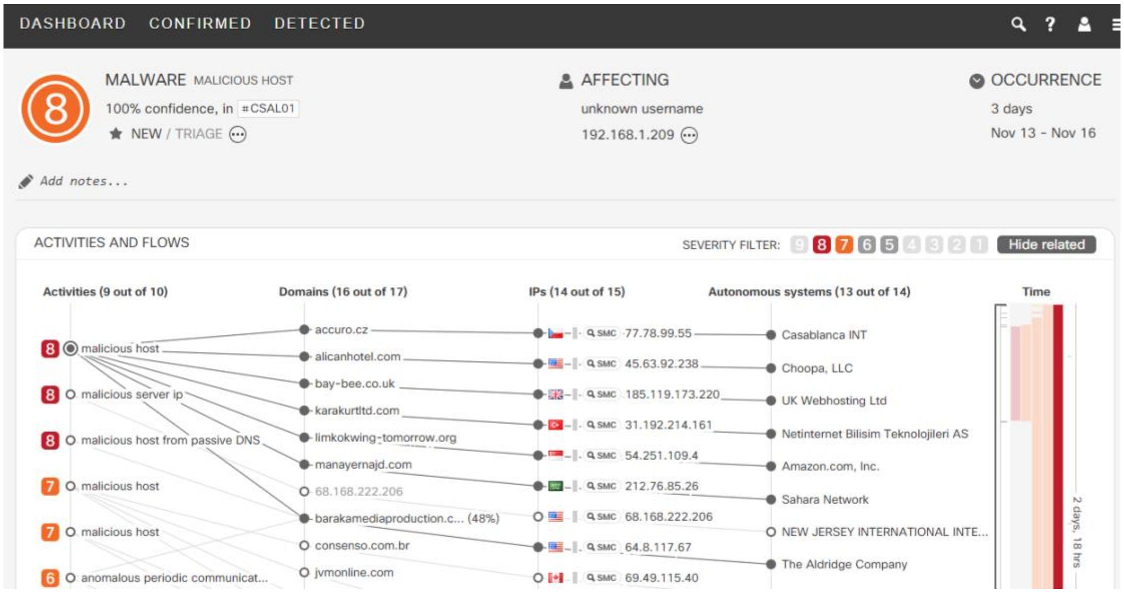
Number of users exhibiting malicious behaviors during the 44 days before yesterday.

4. From the summary information it is also possible for you to click an endpoint to view a histogram of activity leading up to the current security risk level (level 8 in this case).



SEARCH RESULTS FOR: **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	STATE
8 malware malicious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2017 10:08:58 GMT-05:00	NEW
8 malware malicious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2017 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2017 10:06:56 GMT-05:00	NEW



8 MALWARE MALICIOUS HOST
100% confidence, in #CSAL01
NEW / TRIAGE

AFFECTING
unknown username
192.168.1.209

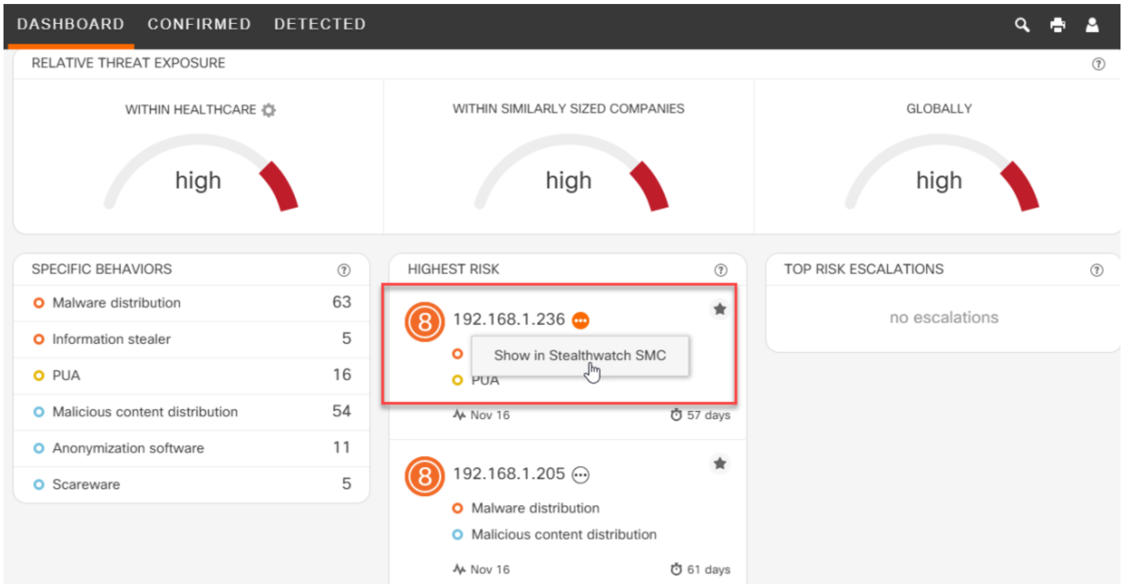
OCCURRENCE
3 days
Nov 13 - Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

5. At the Cognitive Intelligence dashboard, it is also possible to view information that Stealthwatch has collected regarding an infected endpoint. To do so, click the **Show in Stealthwatch SMC** pop-up box that appears when placing your mouse over the endpoint.



DASHBOARD CONFIRMED DETECTED

RELATIVE THREAT EXPOSURE

WITHIN HEALTHCARE: high

WITHIN SIMILARLY SIZED COMPANIES: high

GLOBALLY: high

SPECIFIC BEHAVIORS

Malware distribution	63
Information stealer	5
PUA	16
Malicious content distribution	54
Anonymization software	11
Scareware	5

HIGHEST RISK

8 192.168.1.236

Show in Stealthwatch SMC

PUA

Nov 16 57 days

8 192.168.1.205

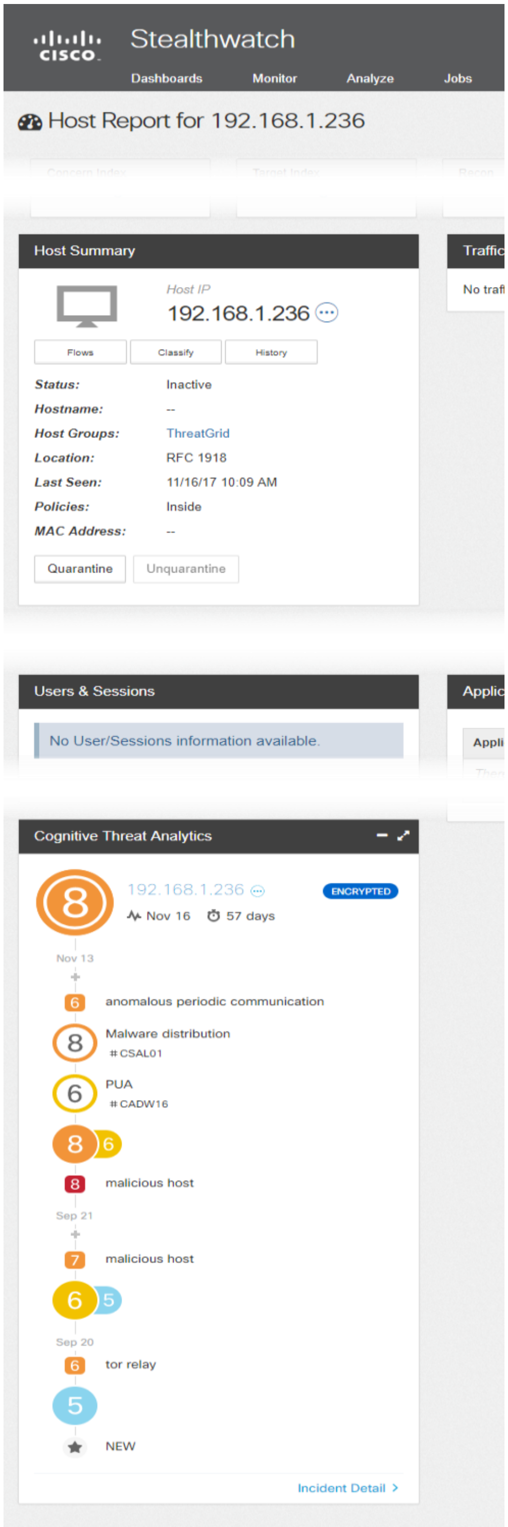
Malware distribution

Malicious content distribution

Nov 16 61 days

TOP RISK ESCALATIONS

no escalations



Host Report for 192.168.1.236

Host Summary

Host IP
192.168.1.236

Status:	Inactive
Hostname:	--
Host Groups:	ThreatGrid
Location:	RFC 1918
Last Seen:	11/16/17 10:09 AM
Policies:	Inside
MAC Address:	--

Users & Sessions

No User/Sessions information available.

Cognitive Threat Analytics

8 192.168.1.236
Nov 16 57 days

Nov 13
6 anomalous periodic communication
8 Malware distribution
#CSAL01
6 PUA
#CADW16
8 6
8 malicious host
Sep 21
7 malicious host
6 5
Sep 20
6 tor relay
5
NEW

For further information regarding navigation of the Cognitive Intelligence user interface, refer to the "Threats Tab" section of the Cisco ScanCenter Administrator Guide.

Useful Commands

This section goes through commands to help verify and troubleshoot your configurations.

1. Verify Flow Monitor configuration by using the command **SHOW FLOW MONITOR *[MONITOR NAME]*.** Make sure the monitor is active by the status indicating **ALLOCATED.**

> SSA-FNF-MON is the default Flow Monitor name given by the SSA application. Replace this in the command if using a different name for your Flow Monitor.

```
9300-DNAC-E1#show flow monitor SSA-FNF-MON
Flow Monitor SSA-FNF-MON:
 Description:        User defined
 Flow Record:        SSA-FNF-REC
 Flow Exporter:      SSA-FNF-EXP
  Cache:
  Type:                  normal (Platform cache)
  Status:                allocated
  Size:                  10000 entries
 Inactive Timeout:     15 secs
 Active Timeout:       60 secs
```

2. If ETA is configured independently of FNF, verify the ETA monitor cache by using the **SHOW FLOW MONITOR *[MONITOR NAME]* CACHE**

> If configuring both ETA and FNF on the same interface, you may disregard this step as when issuing the command, you will see that no cached entries are present. This is expected behavior due to how the ETA and FNF flow monitors are programmed on the interface. Instead use the "show flow monitor [monitor name] cache" command.

```
9300-DNAC-E1#show flow monitor SSA-FNF-MON cache
Cache type:                               Normal (Platform cache)
Cache size:                                10000
Current entries:                               7
Flows added:                               52139
    —Active timeout    (  1800 secs)        8155
Flows aged:                                52132
    —Inactive timeout   (    15 secs)      43977

IPV4 DESTINATION ADDRESS:  107.152.26.219
IPV4 SOURCE ADDRESS:       10.4.8.20
IP PROTOCOL:               6
```

```
TRNS SOURCE PORT:           52174
TRNS DESTINATION PORT:      443
counter bytes long:         9236
counter packets long:       56
timestamp abs first:        22:55:59.963
timestamp abs last:         23:18:23.963
interface input:            Null
interface output:           Null
```

3. Verify ETA flow exports by using the command SHOW FLOW EXPORTER ETA-EXP STATISTICS.

```
9300-DNAC-E1#show flow exporter eta-exp statistics
Flow Exporter eta-exp:
Packet send statistics (last cleared 08:23:31 ago):
Successfully sent:          4853

Client send statistics:
Client: Flow Monitor eta-mon
Records added:            7548
   —sent:                 7548
Bytes added:              6062810
   —sent:                 6062810
```

4. Use the command SHOW PLATFORM SOFTWARE FED SWITCH ACTIVE FNF ET-ANALYTICS-FLOW-DUMP to verify SPLT and IDP are exporting to the flow collector.

```
9300-DNAC-E1#show platform software fed active fnf et-analytics-flow-dump
 ET Analytics Flow dump

 =================
 Total packets received     :4606354
 Excess packets received    :1278
 Excess syn received        : 647831
 Total eta records added    : 635371
 Current eta records        : 0
 Total eta splt exported    : 616991
 Total eta IDP exported     : 616991

 (Index:0) 10.4.10.10, 10.4.48.75, protocol=6, source port=61793, dest port=443, flow
 done=u
 SPLT: len = 3, value = (1282,256)(35328,34304)(128,0)
 IDP: len = 557, value = 45:0:2:2d:13:a4:40:0:80:6
```

5. Check to see which interfaces et-analytics has been enabled on with the command SHOW PLATFORM SOFTWARE ET-ANALYTICS INTERFACES.

```
9300-DNAC-E1#show platform software et-analytics interfaces
ET-Analytics interfaces
 GigabitEthernet1/0/1
 GigabitEthernet1/0/2
 GigabitEthernet1/0/3
 GigabitEthernet1/0/19
 GigabitEthernet1/0/20
 GigabitEthernet1/0/21
 GigabitEthernet1/0/22
 GigabitEthernet1/0/46
 GigabitEthernet1/0/47
 GigabitEthernet1/0/48
ET-Analytics VLANs
 1023,1025
```

IOS-XE Router Commands

1. Verify the ETA service has initialized with the command SHOW PLATFORM HARDWARE QFP ACTIVE FEATURE ET-ANALYTICS DATA RUNTIME.

```
RS11-4331#show platform hardware qfp active feature et-analytics data runtime
ET-Analytics run-time information:

Feature state                : initialized (0x00000004)
Inactive timeout             : 15 secs (default 15 secs)
Flow CFG information         :
instance ID                  : 0x0
feature ID                   : 0x0
feature object ID            : 0x0
chunk ID                     : 0x4
```

2. Verify the ETA flow statistics with the command SHOW PLATFORM HARDWARE QFP ACTIVE FEATURE ET-ANALYTICS DATA STATS FLOW.

```
RS11-4331#show platform hardware qfp active feature et-analytics data stats
Flow
```

```
ET-Analytics Stats:
 Flow statistics:
 feature object allocs : 19257
 feature object frees : 19235
 flow create requests : 787668
 flow create matching : 768411
 flow create successful: 19257
 flow create failed, CFT handle: 0
 flow create failed, getting FO: 0
 flow create failed, malloc FO : 0
 flow create failed, attach FO : 0
 flow create failed, match flow: 0
 flow create failed, set aging : 150
 flow ageout requests : 19218
 flow ageout failed, freeing FO: 0
 flow ipv4 ageout requests : 0
 flow ipv6 ageout requests : 0
 flow whitelist traffic match : 0
```

3. Verify the ETA export statistics with the command **SHOW PLATFORM HARDWARE QFP ACTIVE FEATURE ET-ANALYTICS DATA STATS EXPORT**

```
RS11-4331# show platform hardware qfp active feature et-analytics data stats
Export

ET-Analytics 10.4.48.70:2055 Stats:
 Export statistics:
 Total records exported : 88554
 Total packets exported : 45553
 Total bytes exported : 33287148
 Total dropped records : 0
 Total dropped packets : 0
 Total dropped bytes : 0
 Total IDP records exported :
 initiator->responder : 77092
 responder->initiator : 11636
 Total SPLT records exported:
```

```
initiator->responder : 77075
responder->initiator : 11633
Total SALT records exported:
initiator->responder : 0
responder->initiator : 0
Total BD records exported :
initiator->responder : 0
responder->initiator : 0
Total TLS records exported :
initiator->responder : 3835
responder->initiator : 3815
```

About this guide

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.

Appendix A—Hardware and software used for validation

This guide was validated using the following hardware and software.

SSA Functionality	Version	License
Catalyst 9300	16.11.1 & 16.9.3	DNA-Advantage
Catalyst 3850	16.11.1	DNA-Advantage
Catalyst 3650	16.11.1	DNA-Advantage
ISR 4331	16.11.1	DNA-Advantage
Cisco DNA Center	1.3.1	N/A
Stealthwatch Management Center	7.0	N/A

Appendix B—Glossary

ASR Aggregation services router

AWS Amazon Web Services

DNS Domain Name System

ETA Encrypted Traffic Analytics

FNF Flexible Netflow

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol secure

IDP Initial Data Packet

IP Internet Protocol

ISE Cisco Identity Service Engine

ISR Integrated Services Router

LAN local area network

NaaS Network as a Sensor

NBAR Network-Based Application Recognition

SDA Software Defined Access

SPLT Sequence of packet length and time

SSA Stealthwatch Security Analytics

SPLT Sequence Packet Length Time

VLAN Virtual local area network

Appendix C—Deploy ETA and FNF using templates

Deployment details

This section describes those procedures necessary to enable ETA and FNF on edge nodes within an SD-Access fabric. It consists of the processes for enabling ETA and FNF on Cisco Catalyst 9300 and 9400 Series fabric edge switches for wired or wireless users, after which you can use the Stealthwatch and Cognitive Intelligence user interfaces for crypto audit and malware detection. With Cisco DNA Center version 1.2 and lower, automatic provisioning through the Cisco DNA Center user interface is not supported. Instead, templates can be used to provision the fabric edge nodes to enable both ETA and FNF.

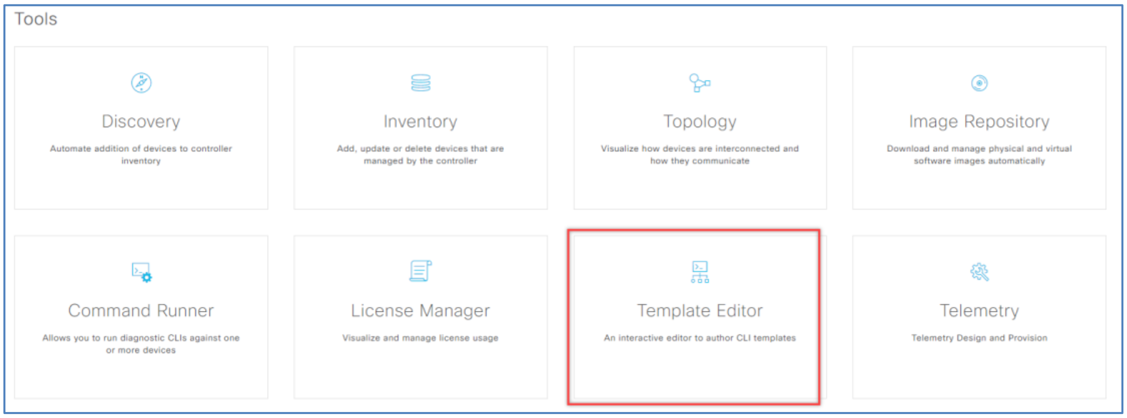
Process: Creating Cisco DNA Center templates for provisioning ETA and FNF

Provisioning ETA and FNF in an SD-Access fabric using templates is a three-step process. The first step involves the creation of the wired and wireless template using the Template Editor within Cisco DNA Center. Once the templates have been created, we need to create a network profile under the Design Workflow in Cisco DNA Center and assign the appropriate sites to the profile. The final step is to provision those devices with this new network profile.

In Cisco DNA Center 1.1.X, there is a restriction that only one CLI template per device type per site is allowed. Cisco DNA Center 1.2 introduced a feature known as *composite templates that will remove that restriction. The use of composite templates and Cisco DNA Center 1.2 has not been validated.*

Procedure 1 - Create templates for wired and wireless provisioning

1. Access Cisco DNA Center and scroll down to the **Tools** section and select **Template Editor**



Tools

Discovery
Automate addition of devices to controller inventory

Inventory
Add, update or delete devices that are managed by the controller

Topology
Visualize how devices are interconnected and how they communicate

Image Repository
Download and manage physical and virtual software images automatically

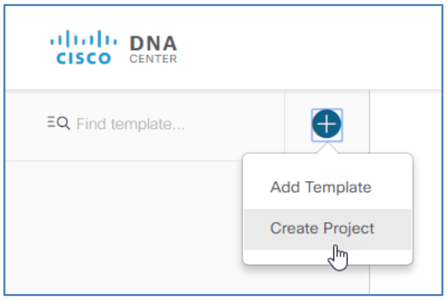
Command Runner
Allows you to run diagnostic CLIs against one or more devices

License Manager
Visualize and manage license usage

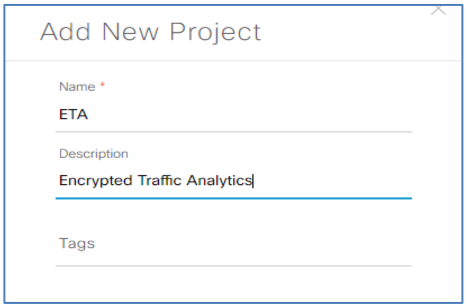
Template Editor
An interactive editor to author CLI templates

Telemetry
Telemetry Design and Provision

2. Click the **+** sign > **Create Project**. The project provides a logical grouping of templates.



3. The Add New Project dialog box opens for you to complete. At the bottom, click **ADD**


Add New Project

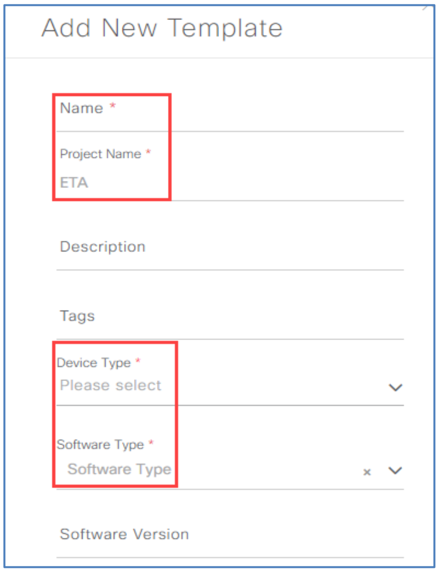
Name *
ETA

Description
Encrypted Traffic Analytics

Tags

4. Repeat Step 2 but select **ADD TEMPLATE**.

5. The Add New Template dialog box opens for you to complete. Add a Name for the new template. A single template will be created to address both wired and wireless provisioning. If more than one project exists, a drop-down is available to select the correct Project Name; otherwise the project created earlier is auto-filled.


Add New Template

Name *

Project Name *
ETA

Description

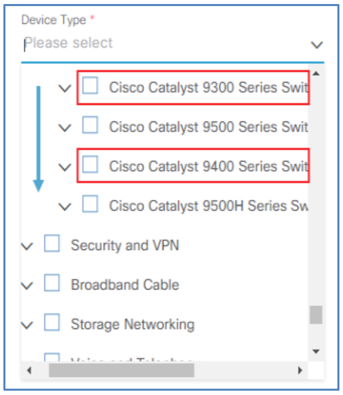
Tags

Device Type *
Please select

Software Type *
Software Type

Software Version

6. Click the arrow to select the correct Device Type. Scroll down and click the arrow next to Switches and Hubs. Scroll down and select either Cisco Catalyst 9300 Series Switches or Cisco Catalyst 9400 Series Switches.

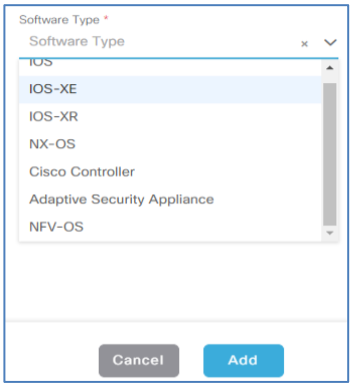


Device Type *

Please select

- □ Cisco Catalyst 9300 Series Swit
- □ Cisco Catalyst 9500 Series Swit
- □ Cisco Catalyst 9400 Series Swit
- □ Cisco Catalyst 9500H Series Sw
- □ Security and VPN
- □ Broadband Cable
- □ Storage Networking

7. Next click the arrow to select the correct Software Type. Scroll down and select IOS-XE. Once you are finished, click **ADD**.

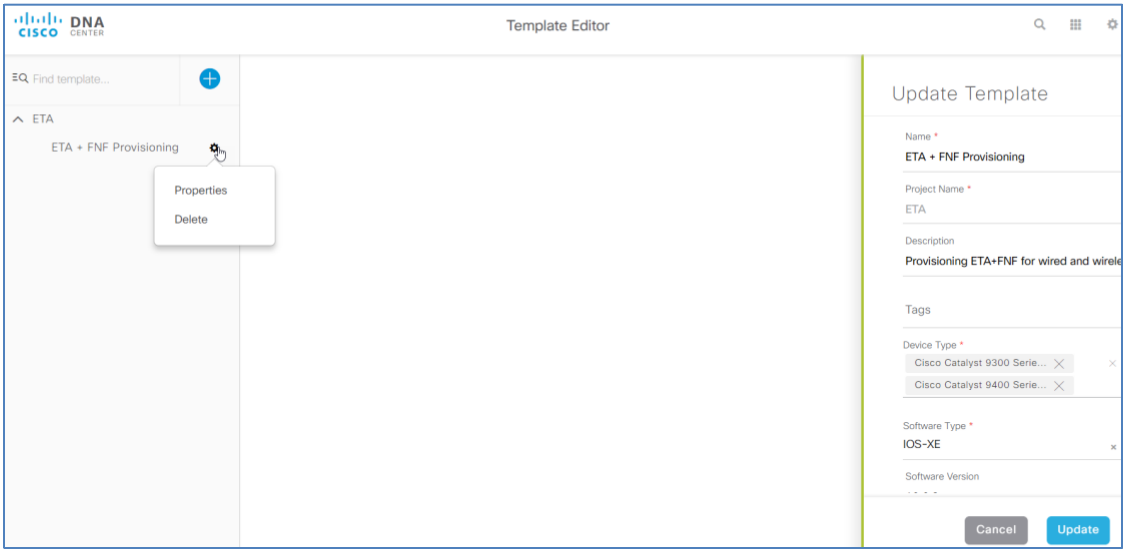


Software Type *

Software Type

- IOS
- IOS-XE
- IOS-XR
- NX-OS
- Cisco Controller
- Adaptive Security Appliance
- NFV-OS

8. To view and confirm your template properties, from the Template Editor, click the gear next to the template you just defined, and select **PROPERTIES**.



Update Template

Name *
ETA + FNF Provisioning

Project Name *
ETA

Description
Provisioning ETA+FNF for wired and wirele

Tags

Device Type *
Cisco Catalyst 9300 Serie...
Cisco Catalyst 9400 Serie...

Software Type *
IOS-XE

Software Version

Procedure 2 – Configure the template

In this procedure we will configure the actual commands used in the template to provision ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. The sample template provided below can be copied and pasted directly into the Cisco DNA Center Template Editor window.

```
et-analytics
ip flow-export destination $fc $fc_port
flow record fnf-rec
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
flow exporter fnf-exp
destination $fc
transport udp $fc_port
template data timeout 30
option interface-table
option application-table timeout 10
flow monitor fnf-mon
exporter fnf-exp
cache timeout active 60
record fnf-rec
interface $wired_interface
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable
vlan configuration $wireless_vlan
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable
vlan configuration $wireless_guest_vlan
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output

et-analytics enable
```

The dollar sign signifies that a user entry is required, and the text following the dollar sign will populate the user entry area when provisioning the device, as we discuss below. For further information regarding the Template Editor, please go to https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/user_guide/b_dnac_ug_1_1/b_dnac_ug_1_1_chapter_01111.html.

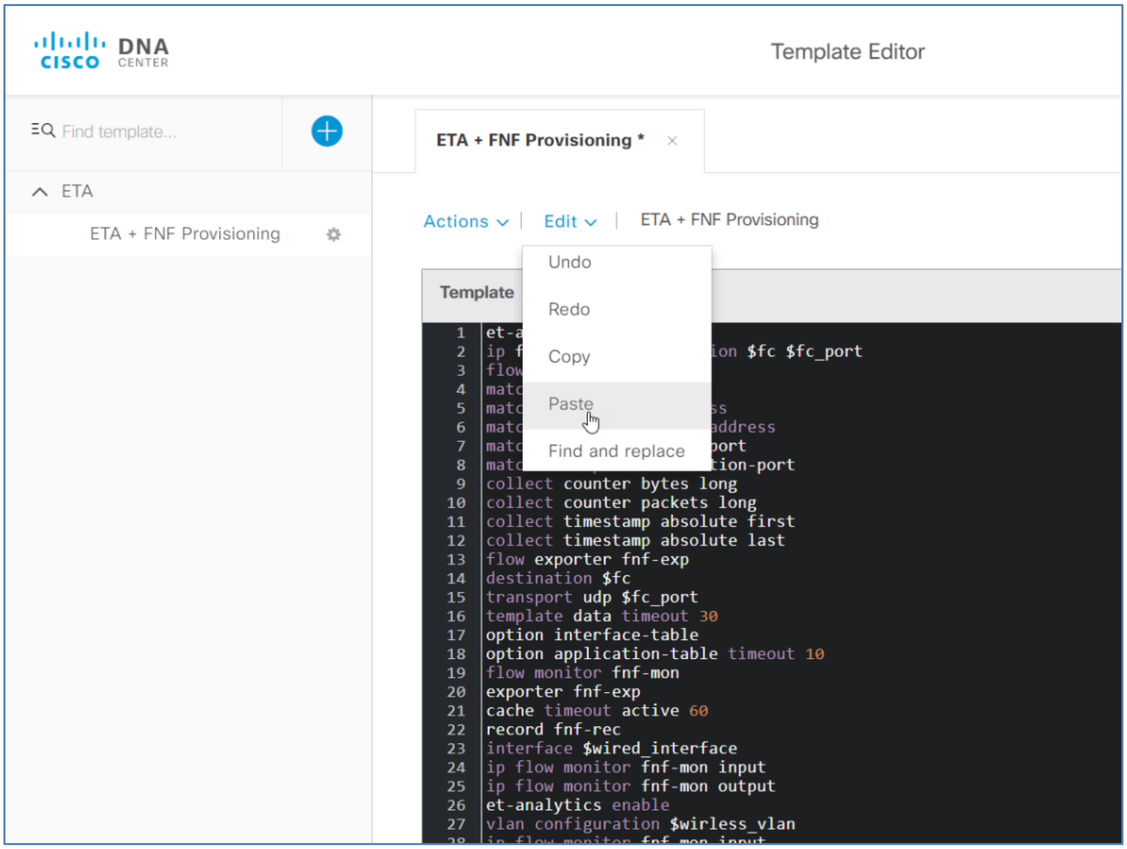
When you provision the switches using the template example above, you will need to provide the information in the following table.

Table 1 Values needed for template example

Field	Value
$fc	Flow Collector IP address
$fc_port	Flow Collector UDP port
$wired_interface	Interface(s) to be configured. If configuring a range, include the keyword range and use normal range syntax. `Example: range Gi1/0/1-24,Gi2/0/1`
$wireless_vlan	Wireless VLAN(s) to be configured. Use normal VLAN range syntax. `Example: 1028-1030,1032`
$wireless_guest_vlan	Wireless guest VLAN to be configured.

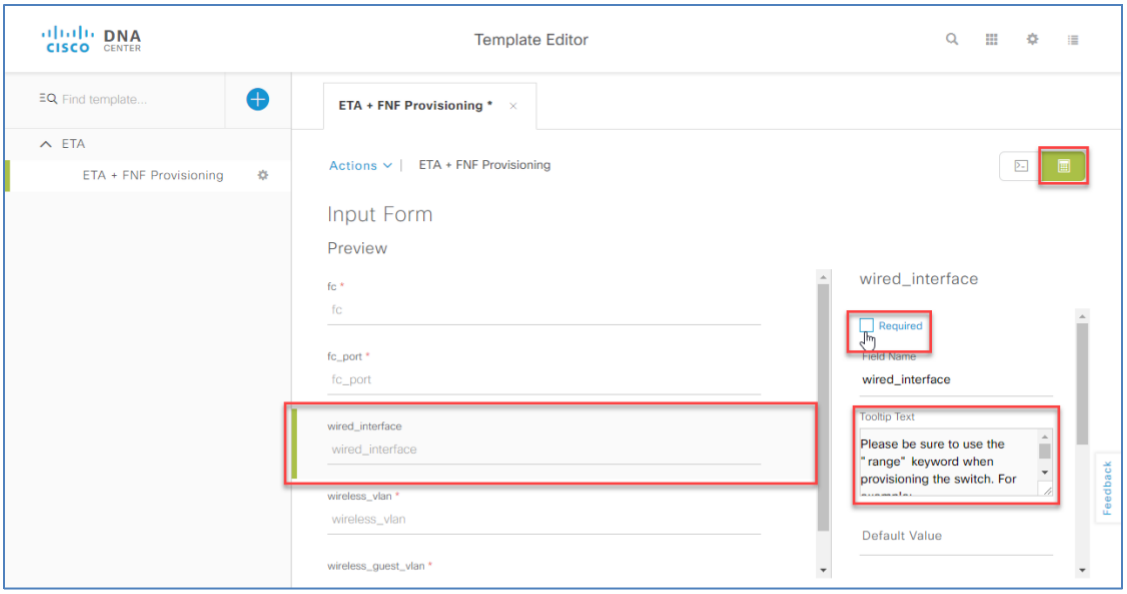
1. Based on the example provided above, either create your customized template in a text editor or simply copy the example above.

2. From the Template Editor, select the template you just created > click **EDIT** > select **PASTE** to paste in the commands from the template example above. This results in the text being populated as seen below.



```
et-a
ip f                    ion $fc $fc_port
flow
matc
matc                    ss
matc                    address
matc                    port
matc                    tion-port
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
flow exporter fnf-exp
destination $fc
transport udp $fc_port
template data timeout 30
option interface-table
option application-table timeout 10
flow monitor fnf-mon
exporter fnf-exp
cache timeout active 60
record fnf-rec
interface $wired_interface
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable
vlan configuration $wirless_vlan
ip flow monitor fnf-mon input
```

3. By default, any of the text strings following the $ sign that you will input information for are mandatory fields. You can change them to be optional by clicking the Form Editor icon in the top right corner of the Template Editor window. Select the field you wish to change, and de-select the Required box. The red asterisk as seen in the Form Editor indicates that the field is mandatory. There is also a box labeled Tooltip Text where you can add any optional tips for that field. Repeat these steps for any additional field you want to make optional.



□ Required
Field Name: wired_interface
Tooltip Text: Please be sure to use the " range" keyword when provisioning the switch. For example:

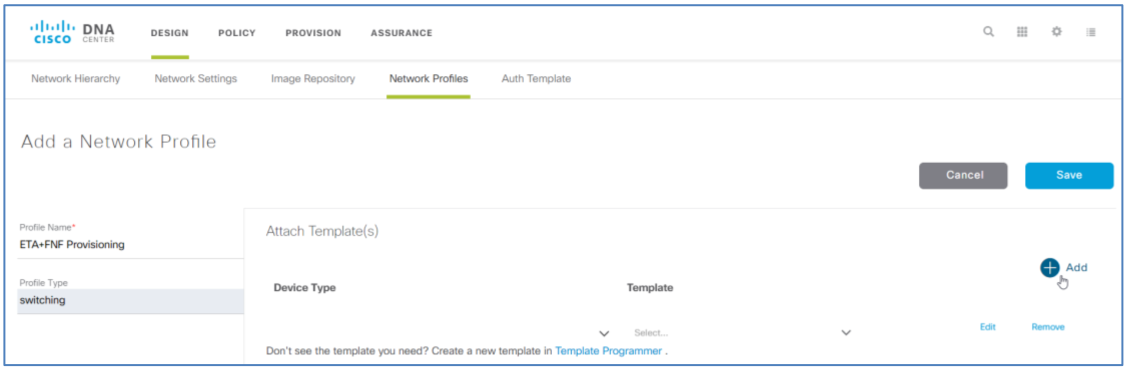
We recommend that the fields for wired interfaces and wireless VLAN be configured as optional.

Procedure 3 - Create a network profile

Now that the template has been defined, the next step is to create a network profile in Cisco DNA Center and assign the template to the profile. Network profiles are assigned to sites that have been previously created in Cisco DNA Center under Design > Network Hierarchy.

1. In Cisco DNA Center, navigate to Design > Network Profiles and click the ADD PROFILE button. In the pop up select Switching.

2. In the Add a Network Profile workflow, enter a profile name and, in the Attach Templates box, click the ADD button.



Add a Network Profile

Profile Name* ETA+FNF Provisioning

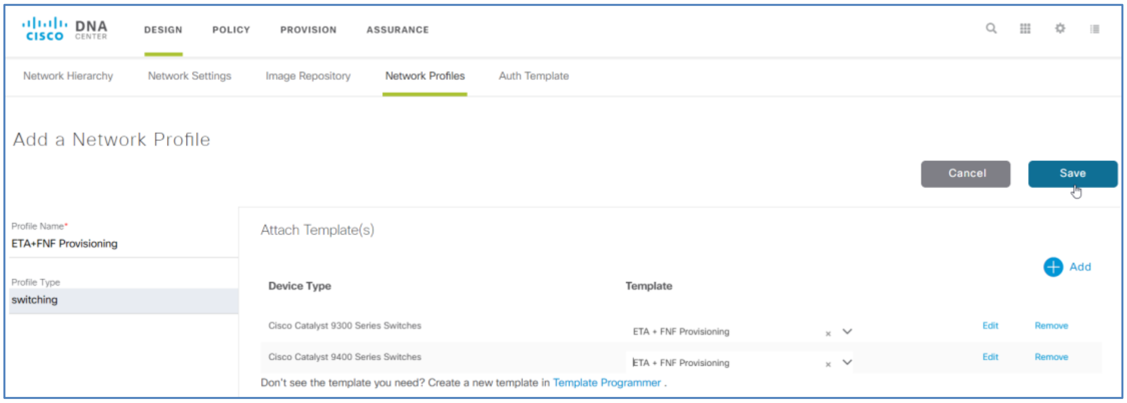
Profile Type switching

Attach Template(s)

Device Type	Template
	Select...

Don't see the template you need? Create a new template in Template Programmer .

3. Click the arrow under Device Type and select the Cisco Catalyst 9300 Series Switches. Then click the drop-down arrow under Template and select the ETA+FNF provisioning template you just created. Click the ADD button again and now select the Cisco Catalyst 9400 Series Switches and the ETA+FNF template. Click SAVE.



Add a Network Profile

Profile Name* ETA+FNF Provisioning

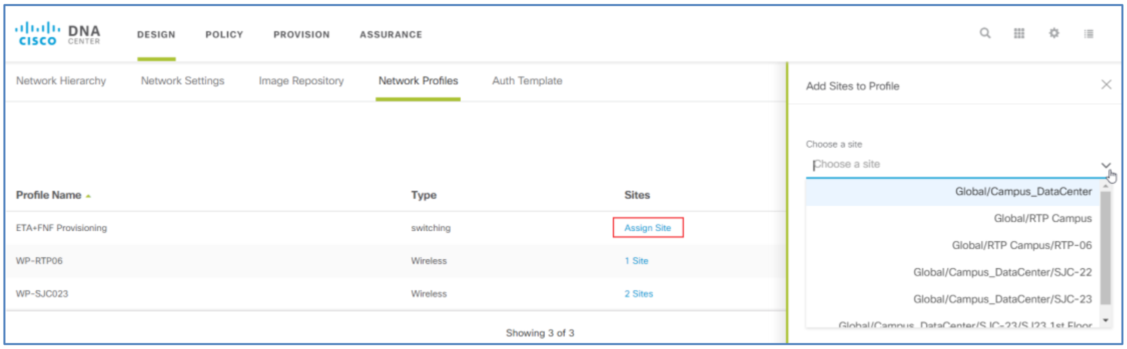
Profile Type switching

Attach Template(s)

Device Type	Template
Cisco Catalyst 9300 Series Switches	ETA + FNF Provisioning
Cisco Catalyst 9400 Series Switches	ETA + FNF Provisioning

Don't see the template you need? Create a new template in Template Programmer .

4. Once the new network profile has been successfully saved, you will assign the sites to which this profile is applicable. Click ASSIGN SITE and then click the arrow for Choose a site. Select the sites for the network profile and click SAVE. Once completed you will see that the ETA+FNF Provisioning profile displays the number of sites you selected.



Profile Name	Type	Sites
ETA+FNF Provisioning	switching	Assign Site
WP-RTP06	Wireless	1 Site
WP-SJC023	Wireless	2 Sites

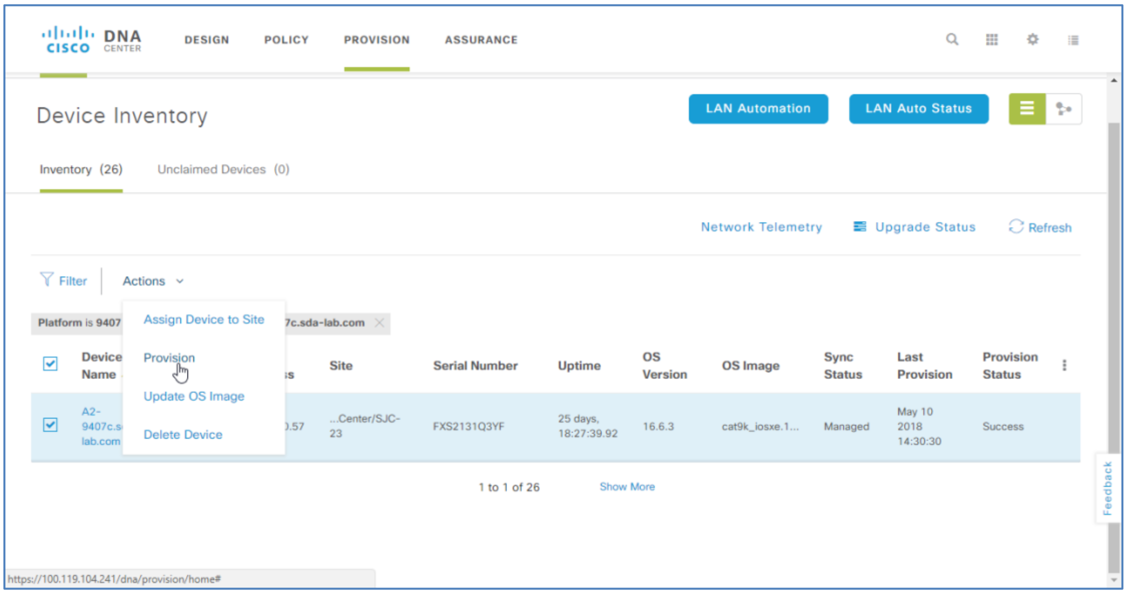
Showing 3 of 3

Global/Campus_DataCenter
Global/RTP Campus
Global/RTP Campus/RTP-06
Global/Campus_DataCenter/SJC-22
Global/Campus_DataCenter/SJC-23
Global/Campus_DataCenter/SJC-23/SJ23 1st Floor

Procedure 4 – Provision ETA and FNF on the SD-Access edge nodes

With the template defined and assigned to a network profile, you are now ready to provision the SD-Access edge nodes.

1. From the Cisco DNA Center home screen, select **Provision** and select the devices you want to provision by checking the box next to each device or selecting all. Click the **Actions** drop-down arrow and select **Provision**

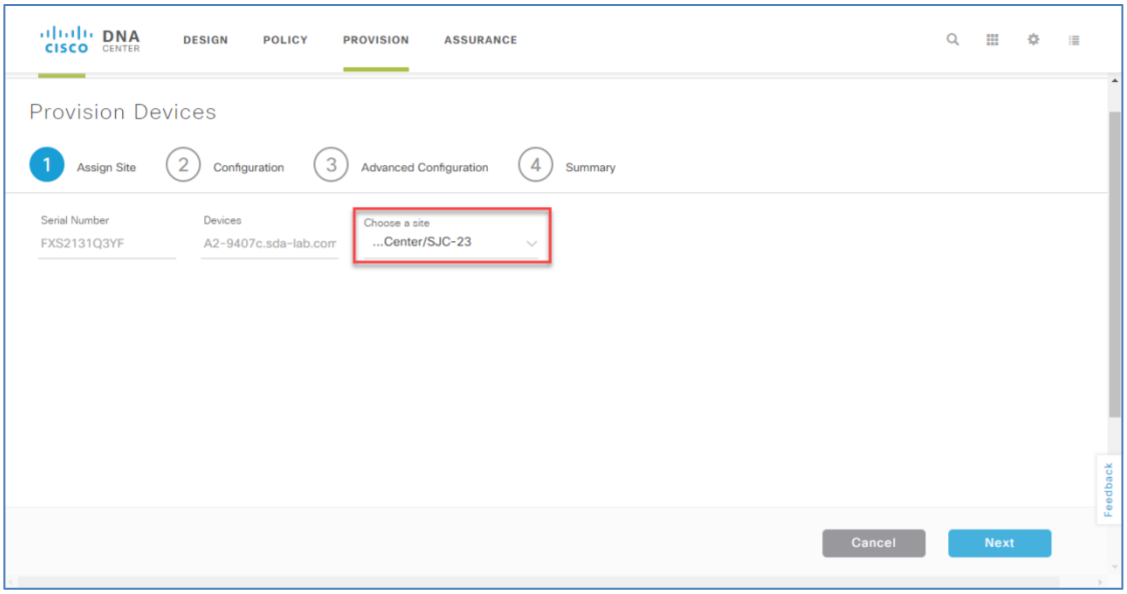


☑	Device Name	…s	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status
☑	A2-9407c.s… lab.com	…0.57	...Center/SJC-23	FXS2131Q3YF	25 days, 18:27:39.92	16.6.3	cat9k_iosxe.1...	Managed	May 10 2018 14:30:30	Success

1 to 1 of 26

https://100.119.104.241/dna/provision/home#

2. The next window, Step 1 Assign Site, opens. The selected devices will appear as well as the corresponding site that they are located in. If the device has not been assigned to a site yet, you will now select the site by clicking the drop-down arrow and choosing the site. Click **Next**.



Provision Devices

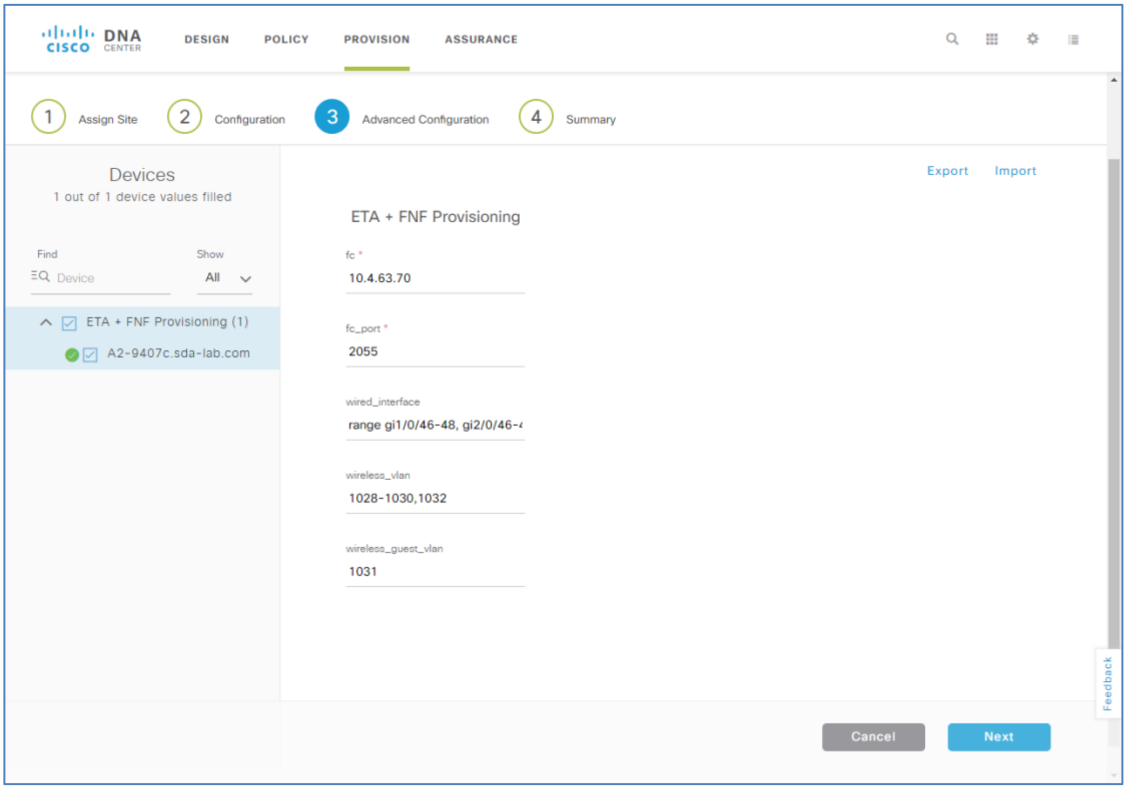
Serial Number: FXS2131Q3YF

Devices: A2-9407c.sda-lab.com

Choose a site: ...Center/SJC-23

3. The next window, Step 2 Configuration, opens. When deploying the template for ETA and FNF, nothing needs to be changed here and you can just click **Next**.

4. The next window Step 3 Advanced Configuration, opens. In the Devices column on the left, you will see the template you just created. Select the box next to the template name or the device(s) listed below it. Provide the required information for the Flow Collector IP address, the UDP port number, and optionally the wired interfaces and appropriate VLANs to be configured. Click **Next**.



Devices

1 out of 1 device values filled

☑ ETA + FNF Provisioning (1)

☑ A2-9407c.sda-lab.com

ETA + FNF Provisioning

fc *: 10.4.63.70

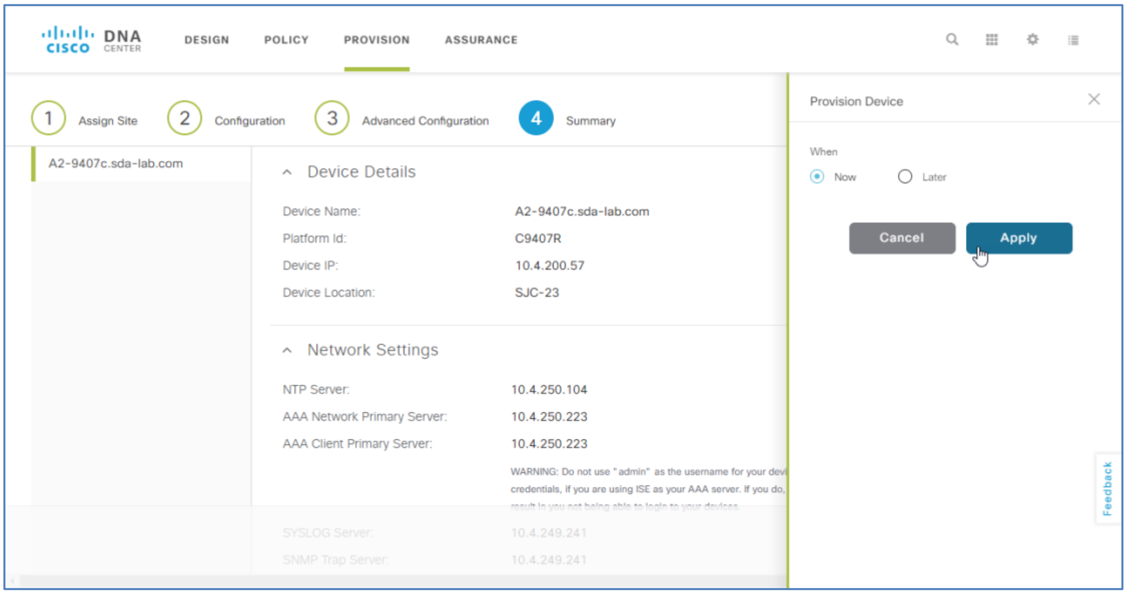
fc_port *: 2055

wired_interface: range gi1/0/46-48, gi2/0/46-4

wireless_vlan: 1028-1030,1032

wireless_guest_vlan: 1031

5. The Step 4 Summary window opens. After verifying the details and the selection of the correct template, click **DEPLOY** and then either Apply now or schedule for later.



A2-9407c.sda-lab.com

Device Details

Device Name: A2-9407c.sda-lab.com
Platform Id: C9407R
Device IP: 10.4.200.57
Device Location: SJC-23

Network Settings

NTP Server: 10.4.250.104
AAA Network Primary Server: 10.4.250.223
AAA Client Primary Server: 10.4.250.223
WARNING: Do not use "admin" as the username for your devi
credentials, if you are using ISE as your AAA server. If you do,
result in you not being able to login to your devices.
SYSLOG Server: 10.4.249.241
SNMP Trap Server: 10.4.249.241

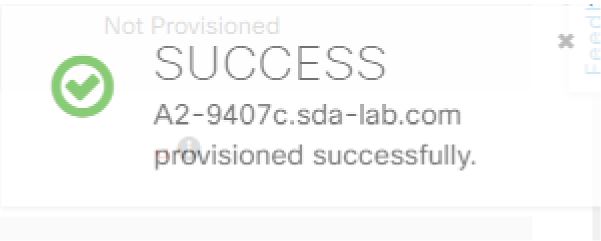
Provision Device

When

● Now ○ Later

Cancel Apply

6. A status message indicating that the provisioning has successfully started will pop-up, and after a few seconds another pop-up indicating that the provisioning successfully completed should appear. If the provisioning does not complete successfully, you will need to review your template for accuracy and rerun the provisioning.

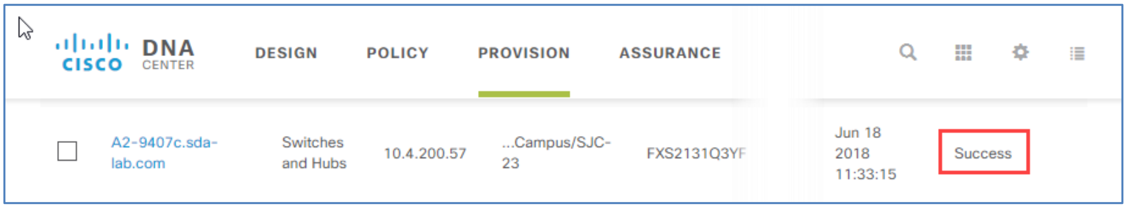

Not Provisioned

SUCCESS

A2-9407c.sda-lab.com provisioned successfully.

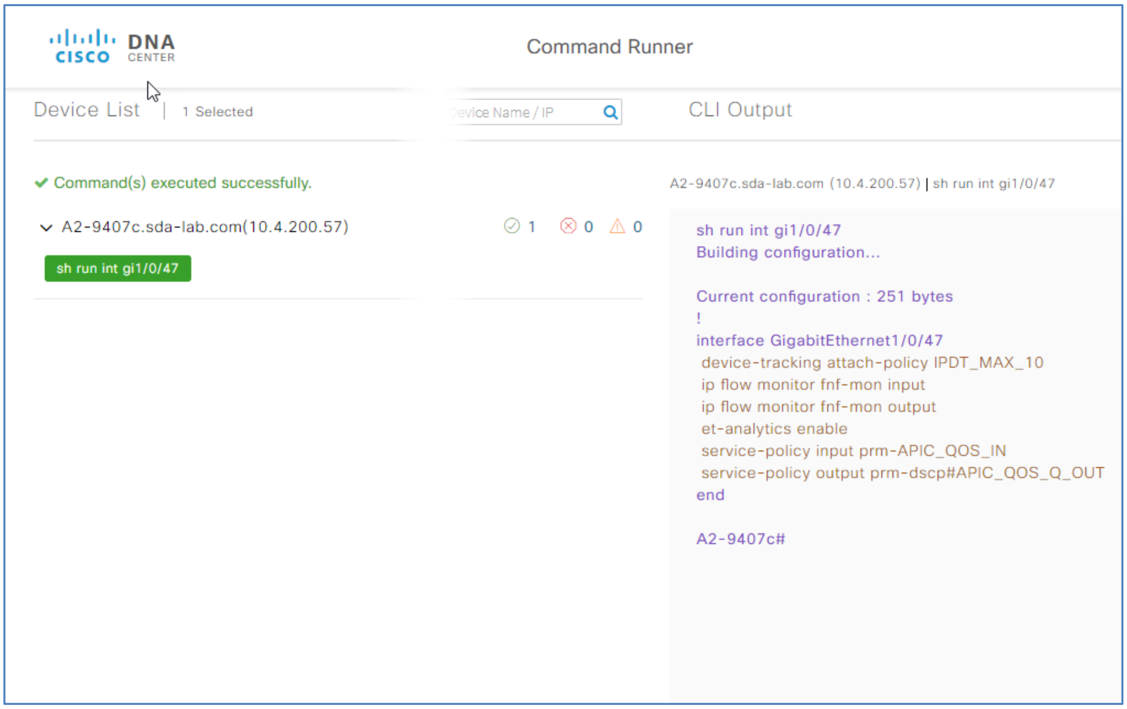
Two of the most common reasons for a template not to be provisioned successfully are that one of the values specified, such as interface or VLAN, doesn't exist or that a conflicting configuration already exists on the interface or VLAN; an example of the latter might be another previously defined flow monitor having been configured.

7. Once successfully provisioned, the device inventory Provision Status column should reflect Success.



□	A2-9407c.sda-lab.com	Switches and Hubs	10.4.200.57	...Campus/SJC-23	FXS2131Q3YF	Jun 18 2018 11:33:15	Success

8. You can then use the Command Runner tool, which can be found in the Tools section of the Cisco DNA Center homepage, to verify that the device has been configured correctly.



✓ Command(s) executed successfully.

A2-9407c.sda-lab.com(10.4.200.57) ✓ 1 ⊗ 0 ⚠ 0

A2-9407c.sda-lab.com (10.4.200.57) | sh run int gi1/0/47

```
sh run int gi1/0/47
Building configuration...

Current configuration : 251 bytes
!
interface GigabitEthernet1/0/47
 device-tracking attach-policy IPDT_MAX_10
 ip flow monitor fnf-mon input
 ip flow monitor fnf-mon output
 et-analytics enable
 service-policy input prm-APIC_QOS_IN
 service-policy output prm-dscp#APIC_QOS_Q_OUT
end

A2-9407c#
```

Procedure 5 – Template for ETA and FNF removal

The following example may be used to create a template to remove the configurations applied with the provisioning template outlined earlier in the document. The same steps will be required as when first creating the provisioning template and assigning it to a network profile however, you will want to create a unique template under the existing project and a new network profile dedicated to the removal of ETA and FNF configuration commands.

```
vlan configuration $wireless_guest_vlan
no et-analytics enable
no ip flow monitor fnf-mon input
no ip flow monitor fnf-mon output
vlan configuration $wireless_vlan
no et-analytics enable
no ip flow monitor fnf-mon input
no ip flow monitor fnf-mon output
Interface range $wired_interface
no et-analytics enable
no ip flow monitor fnf-mon input
no ip flow monitor fnf-mon output
exit
no flow monitor fnf-mon
no flow record fnf-rec
no flow exporter fnf-exp
no et-analytics
```

When provisioning the 9300 and 9400 Series Switches by site, the network profile associated with that site will be used in the provisioning process. During network profile definition, site information is associated with the profile as we discussed in Procedure 3, step 4 in the section entitled "Creating Cisco DNA Center templates for provisioning ETA and FNF." Because only one profile of a type, for example "switching", can be associated with a site, you will need to either modify the original network profile used for provisioning ETA and FNF by removing the sites and then adding them to the new profile or, simply confirming a message that will appear when assigning the sites to the new profile, indicating that the sites will be removed from the old provisioning profile and associated with the new profile for removal of ETA and FNF.

Appendix D: References

Cisco Catalyst 9300 Series Switches

Cisco Catalyst 9400 Series Switches

Cisco Cognitive Threat Analytics

Cisco Cyber Threat Defense CVD

Cisco Cisco DNA Center Template Editor

Cisco Cisco DNA Center User Guide, Release 1.1

Cisco Identity Services Engine web page

Cisco Platform Exchange Grid web page

Cisco Rapid Threat Containment web page

Cisco Security web page

Cisco ScanCenter Administrator Guide

Cisco Stealthwatch Enterprise web page

Cisco Stealthwatch technical reference and specifications

Cisco TrustSec

Encrypted Traffic Analytics Router Configuration Guide

Encrypted Traffic Analytics White Paper

Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide

Stealthwatch Management Console User's Guide

Software-Defined Access Design Guide