

New TrustSec ISE 2.4 Features

Jonathan Eaves, TME
Security Policy & Access

ISE 2.4 meets the needs of expanding TrustSec Deployments

6) Send SGACL CoA from Selective PSN

4) Ability to use FQDN for DNS resolution when adding IPv4 and IPv6 static mappings

2) Selective deployment of IP-SGT mappings to network devices, for example with regional deployments



5) Verify deployment capability. Help with NAD availability issues.

3) Assist in troubleshooting configuration errors in duplicate IP addresses and missing IP-SGT mappings with network devices

1) Support for IPv6-SGT static mappings

Static Mappings for IPv6 Addresses

IP SGT static mapping > 201:0:3238:dfe1:63::fe38/128

IP address(es)

- Add to a mapping group
- Map to SGT individually

SGT *

Send to SXP Domain

Deploy to devices

IP SGT static mapping

1 Selected

Rows/Page

<input type="checkbox"/>	IP address/Host	SGT	Mapping group
<input checked="" type="checkbox"/>	201:0:3238:dfe1:63::fe38/128	Development_Servers (12/000C)	
<input type="checkbox"/>	192.168.1.1	Developers (8/0008)	jofftest3
<input type="checkbox"/>	192.168.1.2	Developers (8/0008)	jofftest3

1) Support for IPv6-SGT static mappings

Selective NAD Deployment

After clicking on “Deploy” on TrustSec matrix page, this pop-up window lets you select or deselect target NADs

2) Selective deployment of IP-SGT mappings to network devices, for example with regional deployments

Deploy IP SGT static mapping

13 Selected

Filter

<input checked="" type="checkbox"/>	Name	IP/Mask	Type
<input checked="" type="checkbox"/>	CTS11	1.2.3.5/32	Group1
<input checked="" type="checkbox"/>	W_CAT	10.56.63.68/32	Working_Devices
<input checked="" type="checkbox"/>	CTS22	1.2.4.2/32	Group2
<input checked="" type="checkbox"/>	CTS10	1.2.3.4/32	Group1
<input checked="" type="checkbox"/>	CTS13	1.2.3.7/32	Group1
<input checked="" type="checkbox"/>	CTS23	1.2.4.3/32	Group2
<input checked="" type="checkbox"/>	iol1	10.1.1.2/32	
<input checked="" type="checkbox"/>	CTS20	1.2.4.0/32	Group2
<input checked="" type="checkbox"/>	CTS21	1.2.4.1/32	Group2
<input checked="" type="checkbox"/>	W_CAT2	10.56.63.66/32	Working_Devices
<input checked="" type="checkbox"/>	CTS12	1.2.3.6/32	Group1
<input checked="" type="checkbox"/>	CTS14	1.2.3.8/32	Group1
<input checked="" type="checkbox"/>	CTS24	1.2.4.4/32	Group2

SGT to IP Conflict Checking

IP SGT static mapping

1 Selected

Rows/Page 5 1 / 1

Refresh Add Trash Edit Move to mapping group Manage groups Import Export **Check status** Deploy

<input type="checkbox"/>	IP address/Host	SGT	Mapping group	Deploy via
<input checked="" type="checkbox"/>	201:0:3238:dfe1:63::fe38/128	Development_Servers (12/000C)		default
<input type="checkbox"/>	192.168.1.1	Developers (8/0008)	jofftest3	-

Found 2 devices to process

Check status process started

About to connect to: Kernow-4500x 10.9.2.2

About to connect to: Kernow-6500 10.8.1.2

Kernow-4500x-IP(10.9.2.2) Configuration downloaded

Kernow-4500x-IP(10.9.2.2) Configuration is up to date

Kernow-6500-IP(10.8.1.2) Configuration downloaded

ERROR: Kernow-6500-IP(10.8.1.2) Configuration needs to be updated. Found 1 missing, 0 with incorrect tag and 1 redundant mappings

Check status process finished

3) Assist in troubleshooting configuration errors in duplicate IP addresses and missing IP-SGT mappings with network devices

FQDN for Static Mapping DNS Lookup

4) Ability to use FQDN for DNS resolution when adding IPv4 and IPv6 static mappings

IP SGT static mapping of hostnames

- Create mappings for all IP addresses returned by DNS query
- Create mappings only for the first IPv4 address and the first IPv6 address returned by DNS query

IP SGT static mapping

Rows/Page 5 / 1

Refresh Add Trash Edit Move to mapping group Manage groups Import Export Check status Deploy

<input type="checkbox"/>	IP address/Host	SGT	Mapping group	Deploy via
<input type="checkbox"/>	201:0:3238:dfe1:63::fe38/128	Development_Servers (12/000C)		default
<input type="checkbox"/>	192.168.1.1	Developers (8/0008)	jofftest3	-
<input type="checkbox"/>	192.168.1.2	Developers (8/0008)	jofftest3	-
<input type="checkbox"/>	jofftest.kernow.com	Production_Servers (11/000B)		-
<input type="checkbox"/>	jofftestip6.kernow.com	Test_Servers (13/000D)		-

Verify Deployment

The image shows two screenshots of the Cisco Identity Services Engine (ISE) interface. The top screenshot displays the 'General TrustSec Settings' page, where the 'Verify TrustSec Deployment' section is highlighted with a green box. This section includes a checkbox for 'Automatic verification after every deploy', a text input for 'Time after deploy process' set to 10 minutes, and a 'Verify Now' button. The bottom screenshot shows the 'Production Matrix' page, where the 'Verify Deploy' button in the toolbar is highlighted with a green box. The matrix table below has columns for various destinations and rows for different sources.

General TrustSec Settings

Verify TrustSec Deployment

Automatic verification after every deploy *i*

Time after deploy process minutes (10-60) *i*

Verify Now

Protected Access Credential (PAC)

Production Matrix

Populated cells: 0

Verify Deploy

Destination	Auditors 9/0009	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Network_Service... 3/0003	PCI_Servers 14/000E	Point_of_Sale_S... 10/000A	Production_Serv... 11/000B	Production_User...
Source	Auditors 9/0009	BYOD 15/000F	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Employees 4/0004	Guests 6/0006	Network_Service... 3/0003	PCI_Servers 14/000E	Point_of_Sale_S... 10/000A	Production_Serv... 11/000B	Production_User...
Auditors 9/0009												
BYOD 15/000F												

5) Verify deployment capability. Help with NAD availability issues.

“Verify deployment” option available on Settings, Matrix, SGT, and SGACL pages

Selective PSN for SGACL CoA

6) Send SGACL CoA from Selective PSN

From the Network Device window, you can select the ISE node from which it will get configurations changes (COA)

TrustSec Notifications and Updates

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other TrustSec devices to trust this device

Send configuration changes to device Using CoA CLI (SSH)

Send from

Ssh Key

