



TrustSec Configuration Guide

TrustSec with Meraki MS320 Switch Configuration Guide



Table of Contents

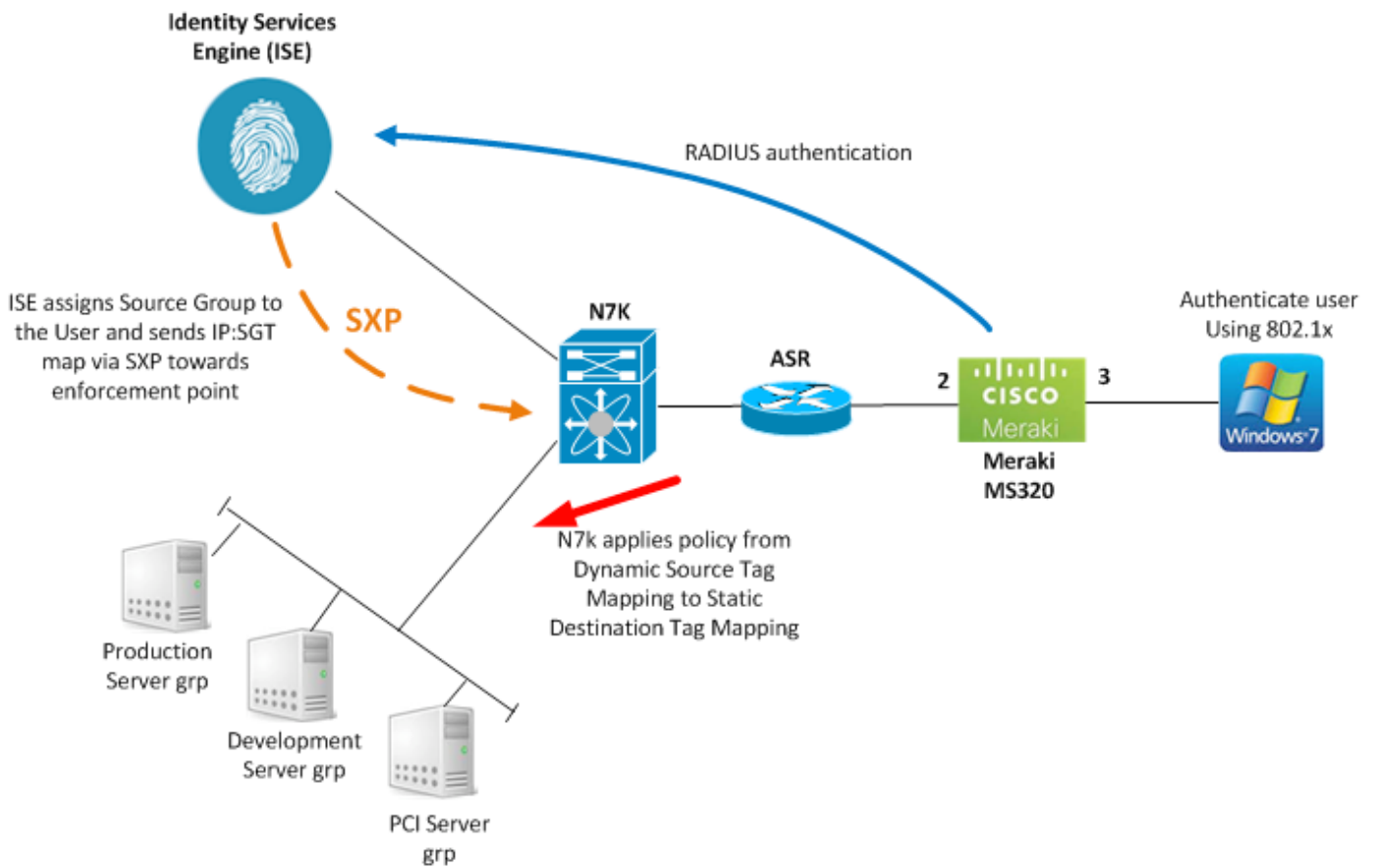
TrustSec with Meraki MS320 Switch	3
Introduction.....	3
Summary of Operation	3
Configuration	4
Meraki Dashboard Configuration	4
Switch Summary	4
Switch Ports	5
Access Policy	7
DHCP Server Configuration	8
Routing and DHCP Configuration (Not Added)	8
OSPF Configuration (Not Added).....	9
ASR Trunk Port Configuration	9
ISE Authorization Table	9
Operation.....	10
Connect / Authenticate Client	10
SXP Mapping and Propagation.....	10
TrustSec Enforcement	11

TrustSec with Meraki MS320 Switch

Introduction

This use case is for customers that wish to utilize Meraki access switches but want to use TrustSec group based policy enforcement.

At the time of writing this guide, the Meraki access switches do not support TrustSec classification, propagation or enforcement. However, the Meraki switches can still be used in a TrustSec deployment by making use of TrustSec functions within other network components.



Summary of Operation

The latest Meraki firmware supports RADIUS Authentication and Accounting. This allows the Meraki access switches to send RADIUS authentication and accounting messages to ISE which provides the capability to build complete sessions for authenticating clients.

If a client successfully authenticates to ISE via a Meraki access switch, ISE can be configured to assign a Security Group Tag to the learned client IP address, known as an IP:SGT mapping. ISE can send this mapping to TrustSec enforcement points in the network via Security Group Tag Exchange Protocol (SXP).

The enforcement points then have the ability to enforce policy based on the source group information sent via ISE and the destination group information learned via any supported methods.

As can be seen, the Meraki access switch only takes part in RADIUS messaging, it does not play a part in TrustSec classification, propagation or enforcement. The TrustSec functions within other network components allows the Meraki access switches to be deployed and used within this architecture.

Configuration

Meraki Dashboard Configuration

Switch Summary

The screenshot displays the Meraki dashboard interface for a switch named 'Kernow-Meraki'. The left sidebar shows navigation options: Network-wide, Security appliance, Switch (selected), Wireless, Organization, and Help. The main content area is divided into two columns. The left column lists configuration details for the switch, including LAN IP (10.6.1.2), VLAN (10), Public IP (209.206.52.7), Gateway (10.6.1.1), DNS (10.1.100.2), and other settings like Serial number, Address, Tags, Notes, RSTP root, Firmware, Config, Topology, and L3 routing status. A red notification banner indicates a connection issue with the Cisco Meraki Cloud. The right column provides a summary of the switch's status, including a 'Ports' section with a visual representation of port activity, 'Historical data' for connectivity and client usage, and a 'Clients' table listing active connections.

Description	Usage ▲	MAC address	IP address	VLAN	Port
1 e8:b7:48:7e:5a:15	153.7 MB	e8:b7:48:7e:5a:15	10.6.1.1	10	2

Switch Ports

Summary
Ports
Power
L3 routing
Event log
Location
Tools

Ports | [Configure ports on this switch](#)

Port	Name	Type	VLAN	Current traffic Sent ↓, Received ↑	Total bytes	RSTP state	PoE usage	CDP/LLDP	Link	Status
1		trunk	native 1	-	3.6 MB	Forwarding	-	S-4900-DC	Auto negotiate (1 Gbps)	OK
2		trunk	native 1	-	202.9 MB	Forwarding	-	-	1 Gigabit full duplex	OK
3	UCS vmnic 8	access	10	-	983.3 KB	Disabled	-	-	1 Gigabit full duplex	Warning

Port 1 is purely for management.
 Port 2 is the uplink trunk to the network (ASR).
 Port 3 is the access port where the 802.1x client is connected.

Switch ports:	<input type="text" value="Kernow-Meraki/2"/>
Name:	<input type="text"/>
Tags:	<input email-alerts="" phone""="" type="text" value="eg. "/>
Enabled:	<input type="text" value="enabled"/>
RSTP:	<input type="text" value="enabled"/>
STP guard:	<input type="text" value="disabled"/>
PoE:	<input type="text" value="disabled"/>
Link:	<input type="text" value="1Gbps (auto)"/>
Port schedule:	<input type="text" value="Unscheduled"/>
Isolation:	<input type="text" value="disabled"/>
Type:	<input type="text" value="trunk"/>
Native VLAN:	<input type="text" value="1"/>
Allowed VLANs: ⓘ	<input type="text" value="1,10"/>

Switch ports:	<input type="text" value="Kernow-Meraki/3"/>
Name:	<input type="text" value="UCS vmnic 8"/>
Tags:	<input email-alerts="" phone""="" type="text" value="eg. "/>
Enabled:	<input type="text" value="enabled"/>
RSTP:	<input type="text" value="disabled"/>
PoE:	<input type="text" value="disabled"/>
Link:	<input type="text" value="1Gbps (auto)"/>
Port schedule:	<input type="text" value="Always on"/>
Isolation:	<input type="text" value="disabled"/>
Type:	<input type="text" value="access"/>
Access policy:	<input type="text" value="For ISE"/>
VLAN:	<input type="text" value="10"/>
Voice VLAN: ⓘ	<input type="text"/>

Access Policy

As can be seen in the port 3 configuration above, the access policy is set as 'For ISE'. This policy is added in the dashboard as follows where 10.1.101.41 is the IP address of the Identity Services Engine (ISE).

The ISE RADIUS server is added for authentication and accounting is enabled:

Access policies

Name

RADIUS servers ⓘ

#	Host	Port	Secret	Actions
1	<input type="text" value="10.1.101.41"/>	<input type="text" value="1812"/>	<input type="text" value="....."/>	⊕ × <input type="button" value="Test"/>

[Add a server](#)

RADIUS testing ⓘ

RADIUS CoA support ^{BETA} ⓘ

RADIUS accounting

RADIUS accounting servers

#	Host	Port	Secret	Actions
1	<input type="text" value="10.1.101.41"/>	<input type="text" value="1813"/>	<input type="text" value="....."/>	⊕ × <input type="button" value="Test"/>

[Add a server](#)

Host Mode ⓘ

Access policy type ⓘ

Guest VLAN ⓘ

Voice VLAN clients

Switch ports There is currently [1 Switch port](#) using this policy

[Remove this access policy](#)

[Add an access policy](#)

DHCP Server Configuration

DHCP servers

DHCP servers

Configure DHCP servers DHCP servers running on layer 3 switches in this network can be configured on the [Routing and DHCP](#) page.

Email alerts

Default DHCP server policy

Note: Switches with configured DHCP servers are *always* allowed.

Blocked DHCP servers 

DHCP servers for the last day ▾

Description	MAC	VLAN	Subnet	IP	Last seen ▾	Recent packet	Policy	Seen by	+
e8:b7:48:7e:5a:15	e8:b7:48:7e:5a:15	10	10.6.1.0/24	10.1.100.2 (relay: 10.6.1.1)	18 hours	view packet	allowed	Kernow-Meraki	

Routing and DHCP Configuration (Not Added)

Routing and DHCP

Interfaces and static routes

This section includes all existing static routes and L3 interfaces configured in your network.

You have not configured any static routes or L3 interfaces.

Warm spares

This section displays any warm spares that you've configured within the network. This feature adds L3 redundancy to non-stacking gateway switches.

You have not configured any warm spares.

OSPF Configuration (Not Added)

Open Shortest Path First (OSPF) routing

OSPF

Disabled 

ASR Trunk Port Configuration

The following configuration resides on the ASR router interface connected to the Meraki MS320 switch:

```
interface GigabitEthernet0/1/5
description Connected to Meraki MS320 port 2
no ip address
negotiation auto
!
interface GigabitEthernet0/1/5.1
encapsulation dot1Q 10
ip address 10.6.1.1 255.255.255.0
ip helper-address 10.1.100.2
```

ISE Authorization Table

ISE contains the following authorization table entry.

The condition checks if the user logging into the network is a member of the TSEngineering group in AD. If yes then permit access and assign the TSEngineering security group.


Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies 

▶ Exceptions (1)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	TSEng	if Kernow-AD:ExternalGroups EQUALS kernow.com/Users/TSEngineering	then PermitAccess AND TSEngineering

Operation

Connect / Authenticate Client

When the client is connected/authenticated, ISE shows the following entry in the Live Log:

Time	Status	Details	Network Device	Identity	Endpoint ID
Jun 27, 2017 02:48:50.495 PM	✓		Kernow-MerakiMS320	KERNOWtseng1	00:50:56:8F:89:8F

Authorization Profiles	Endpoint Profile	Authentication Policy	Authorization Policy
PermitAccess,TSEngineering	VMWare-Device	Default >> Dot1X >> Default	Default >> TSeng

So, the TSeng authorization table entry has been hit/selected and therefore the TSEngineering security group has been assigned.

SXP Mapping and Propagation

After a successful authentication, ISE tracks the IP:SGT mapping of the user. Static mappings have also been added to ISE for the DC servers. All these mappings are placed in the ISE SXP table:

All SXP Mappings

Rows/Page: 5 / 1 / 1 Go

Refresh Add SXP Domain filter Manage SXP Domain filters Filter

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
10.1.100.3/32	11_Dev_Srvrs (11/000B)	10.1.101.42	Local	sxp-4948-dc	ISE21-435-3
10.1.100.4/32	14_PCI_Srvr (14/000E)	10.1.101.42	Local	sxp-4948-dc	ISE21-435-3
10.1.140.2/32	19_Prod_srvr (19/0013)	10.1.101.42	Local	sxp-4948-dc	ISE21-435-3
10.6.1.10/32	TSEngineering (17/0011)	10.1.101.42,10.6.1.2	Session	default	ISE21-435-3

Static Mappings for DC Servers (rows 1-3)

Dynamic Mapping for Meraki User (row 4)

With an SXP connection deployed between ISE and the N7k, the mappings are propagated to the N7k:

```
Kernow-N7k# show cts role-based sgt-map
```

```
IP ADDRESS      SGT          VRF/VLAN      SGT CONFIGURATION
10.1.100.3      11(11_Dev_Srvrs)  vrf:1         Learnt from SXP peer:10.3.3.1
10.1.100.4      14(14_PCI_Srvr)  vrf:1         Learnt from SXP peer:10.3.3.1
10.1.140.2      19(19_Prod_srvr) vrf:1         Learnt from SXP peer:10.3.3.1
10.6.1.10       17(TSEngineering) vrf:1         Learnt from SXP peer:10.1.101.42
```

```
Kernow-N7k#
```

TrustSec Enforcement

Once the N7k learns of mappings, it downloads the TrustSec policy from ISE for groups it needs to protect. The TrustSec policy matrix in ISE includes a policy to deny traffic from the TSEngineering group to the PCI_Srvr group:

Production Matrix		Populated cells: 16						
		Edit + Add ✖ Clear 🚀 Deploy 👁 Monitor All - Off 📄 Import 📄 Export 📄 View						
Destination ▶	Source ▲	11_Dev_Srvrs 11/000B	14_PCI_Srvr 14/000E	19_Prod_srvr 19/0013	AAA_555_Test 555/022B	Assembly_Plant 104/0068	Auditors	
Unknown								
TSMarketing 16/0010								
TSEngineering 17/0011		✔ Permit_All	✔ Deny IP	✔ Permit_All				
TrustSec_Device								

The N7k shows this policy in residence once it has been downloaded from ISE:

```
Kernow-N7k# show cts role-based policy sgt 17 dgt 14
```

```
sgt:17(TSEngineering)
dgt:14(14_PCI_Srvr)  rbacl:Deny IP
deny ip
Kernow-N7k#
```

The policy is active on the N7k with counters showing traffic being denied from the TSEngineering group to the PCI_Srvr group. This is blocking the user logged onto the network (via dot1x on the Meraki switch) from accessing the PCI Servers in the DC:

```
Kernow-N7k# show cts role-based counters sgt 17 dgt 14
```

```
RBACL policy counters enabled  
Counters last cleared: Never
```

```
sgt:17(TSEngineering) dgt:14(14_PCI_Srvr)    [6]  
rbacl:Deny IP  
    deny ip [6]  
Kernow-N7k#
```

Hence the Meraki access switch can be used in a TrustSec deployment even though the switch itself does not support TrustSec capabilities today.