Configure Switch with SXP and IBNS 2.0 for Identity-Based Networks

Contents

Introduction

Prerequisites

- Components Used

Background Information

- Identity Control Policy Configuration Overview

Configure

- Switch Configuration
- ISE Configuration
  - Step 1: Create Authentication and Authorization policies on ISE
  - Step 2: Configure a SXP Device on ISE
  - Step3: Configure Global Password under SXPSettings

Verify

Troubleshoot

- Log Explanation

Introduction

This document describes procedures to configure Cisco Switches with SXP and IBNS 2.0 for Identity-Based Networking.

Prerequisites

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) version 3.3 patch 4
- Cisco Catalyst switch 3850

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

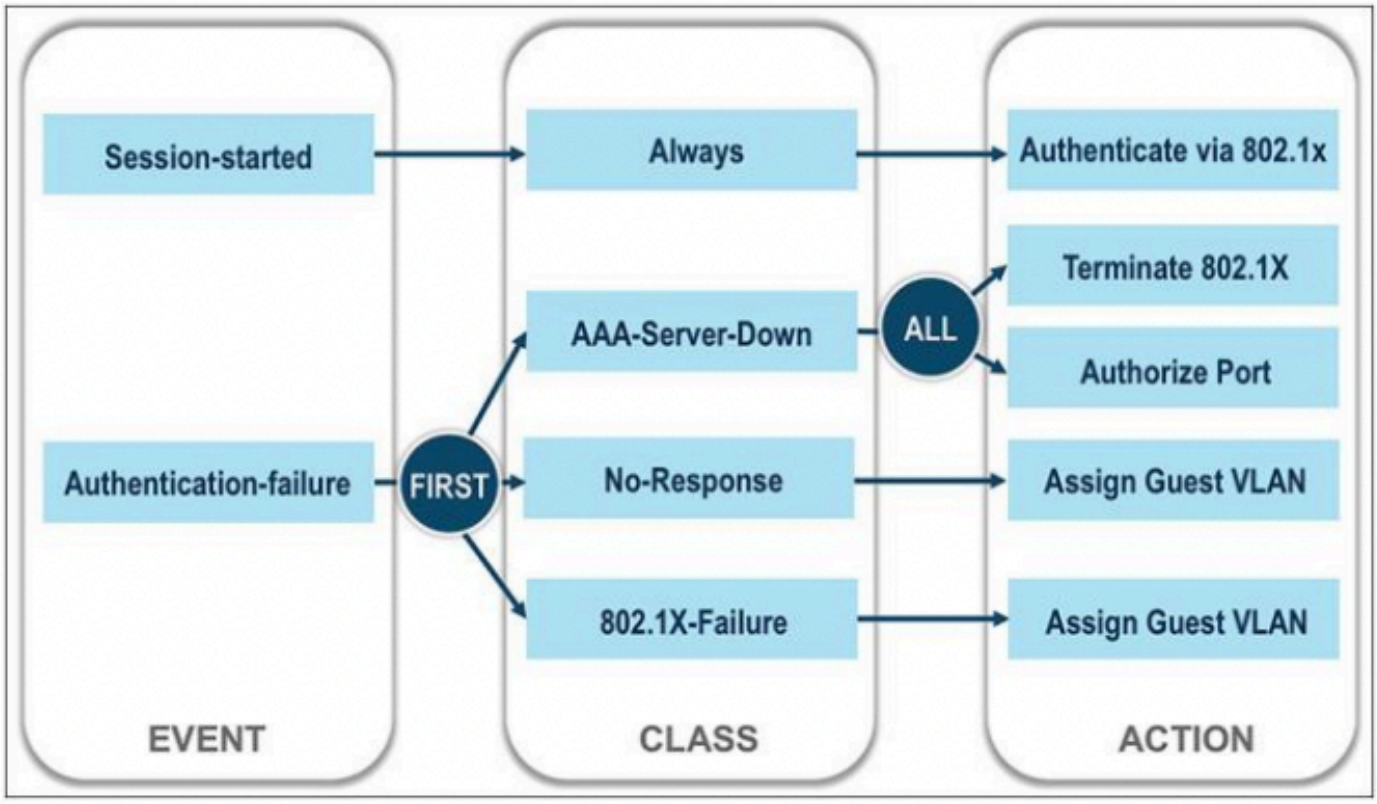
Background Information

Identity control policies define the actions that the Access Session Manager performs in response to specific conditions and endpoint events. Using a consistent policy language, various system actions, conditions, and events can be combined to form these policies.

Control policies are applied on interfaces and are primarily responsible for managing endpoint authentication and activating services on sessions. Each control policy is made up of one or more rules and a

decision strategy that determines how those rules are evaluated.

A control policy rule includes a control class (a flexible condition statement), an event that triggers the condition evaluation, and one or more actions. While administrators define which actions are triggered by specific events, some events come with predefined default actions.

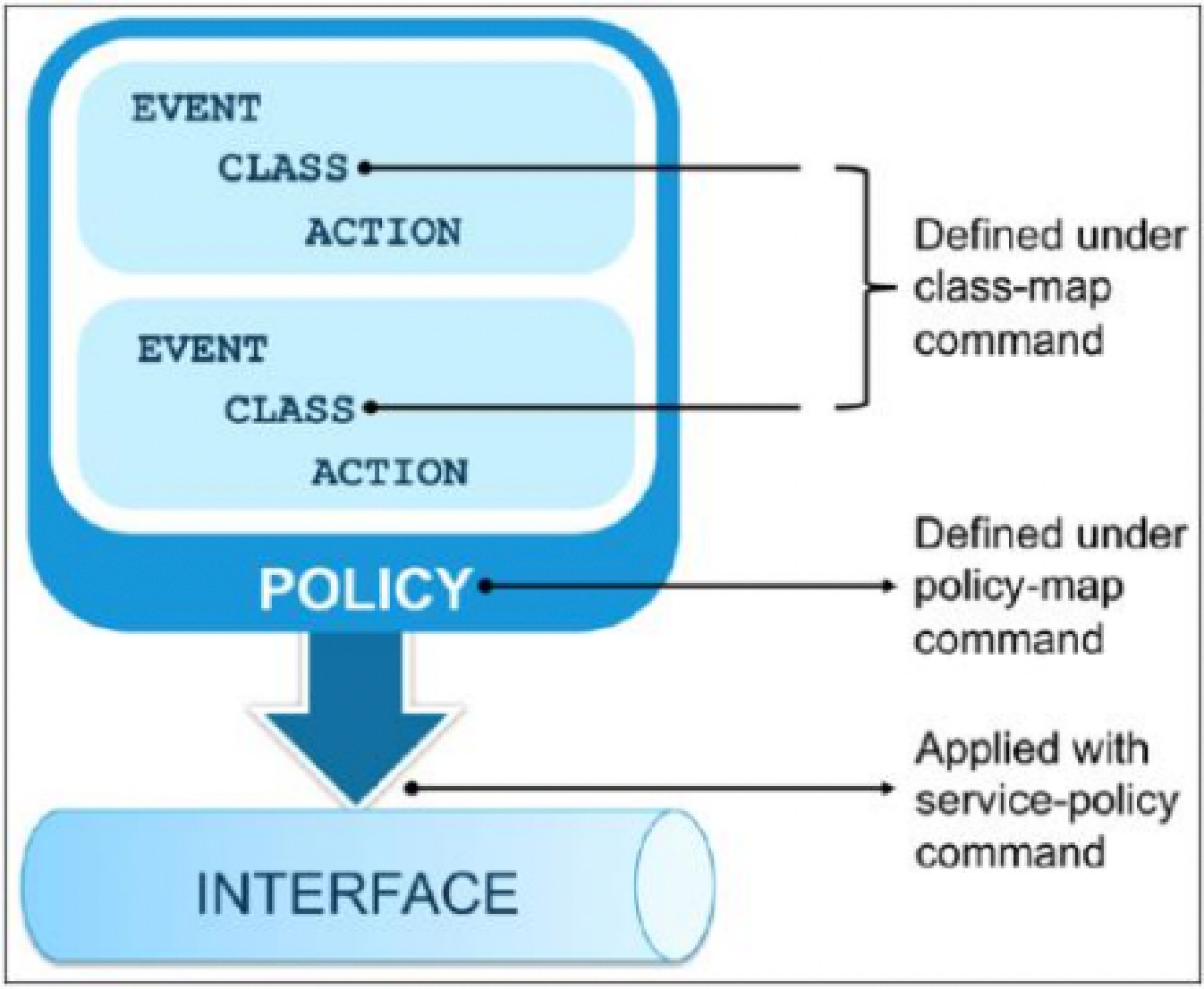


Identity Control Policy

Identity Control Policy Configuration Overview

Control policies define system behavior using an event, a condition, and an action. Configuring a control policy involves three main steps:

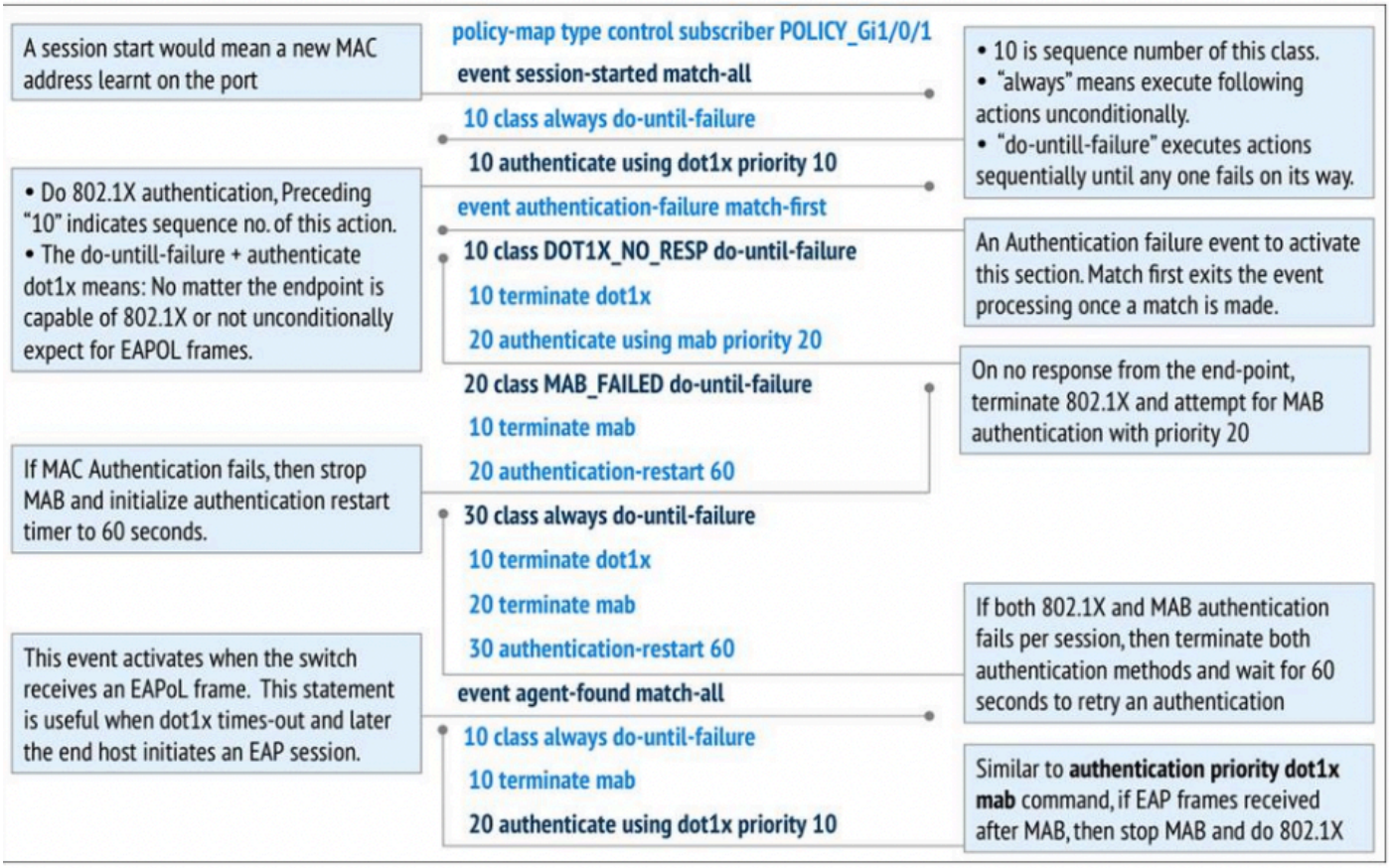
1. Create control classes:
   A control class defines the conditions required to activate a control policy. Each class can have multiple conditions that evaluate as true or false. You can set whether *all*, *any*, or *none* of the conditions must be true for the class to be considered true. Alternatively, administrators can use a default class that has no conditions and always evaluates as true.
2. Create the control policy:
   A control policy contains one or more rules. Each rule includes a control class, an event that triggers the condition check, and one or more actions. Actions are numbered and executed in order.
3. Apply the control policy:
   Finally, apply the control policy to an interface to activate it.



Identity Control Policy Configuration

The **authentication display new-style** command converts the legacy configurations in to new style.

switch#authentication display new-style



Interpreting Identity Control Policy

Configure

Switch Configuration

WS-C3850-48F-E#show run aaa

!

aaa authentication dot1x default group radius local

aaa authorization network default group radius local

username admin password 0 xxxxxx

!

!

!

!

radius server ISE1

address ipv4 10.127.197.xxx auth-port 1812 acct-port 1813

pac key xxxx@123

```
!
!
aaa group server radius ISE2
server name ISE1
!
!
!
!
aaa new-model
aaa session-id common
!
aaa server radius dynamic-author
client 10.127.197.xxx server-key xxxx@123
dot1x system-auth-control
!
WS-C3850-48F-E#show run | in POLICY_Gi1/0/45
policy-map type control subscriber POLICY_Gi1/0/45
service-policy type control subscriber POLICY_Gi1/0/45
WS-C3850-48F-E#show run | sec  POLICY_Gi1/0/45
policy-map type control subscriber POLICY_Gi1/0/45
event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
event authentication-failure match-first
  5 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
```

```
   20 authenticate using mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  40 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-policy type control subscriber POLICY_Gi1/0/45
WS-C3850-48F-E#show run interface gig1/0/45
Building configuration...
Current configuration : 303 bytes
!
interface GigabitEthernet1/0/45
switchport access vlan 503
switchport mode access
access-session host-mode single-host
access-session closed
access-session port-control auto
mab
no cts role-based enforcement
dot1x pae authenticator
```

service-policy type control subscriber POLICY_Gi1/0/45

end

WS-C3850-48F-E#show run cts

!

cts authorization list ISE2

cts sxp enable

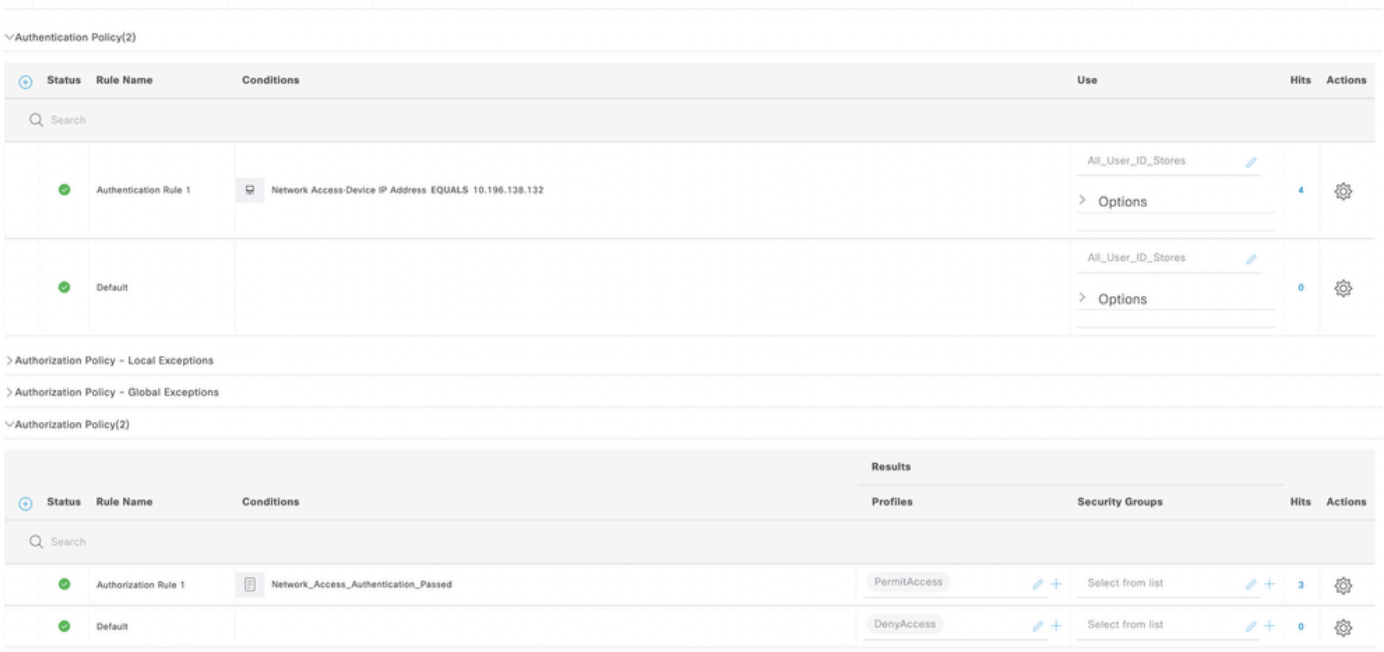
cts sxp connection 10.127.197.xxx password none mode peer speaker hold-time 0 0

cts sxp default source-ip 10.196.138.yyy

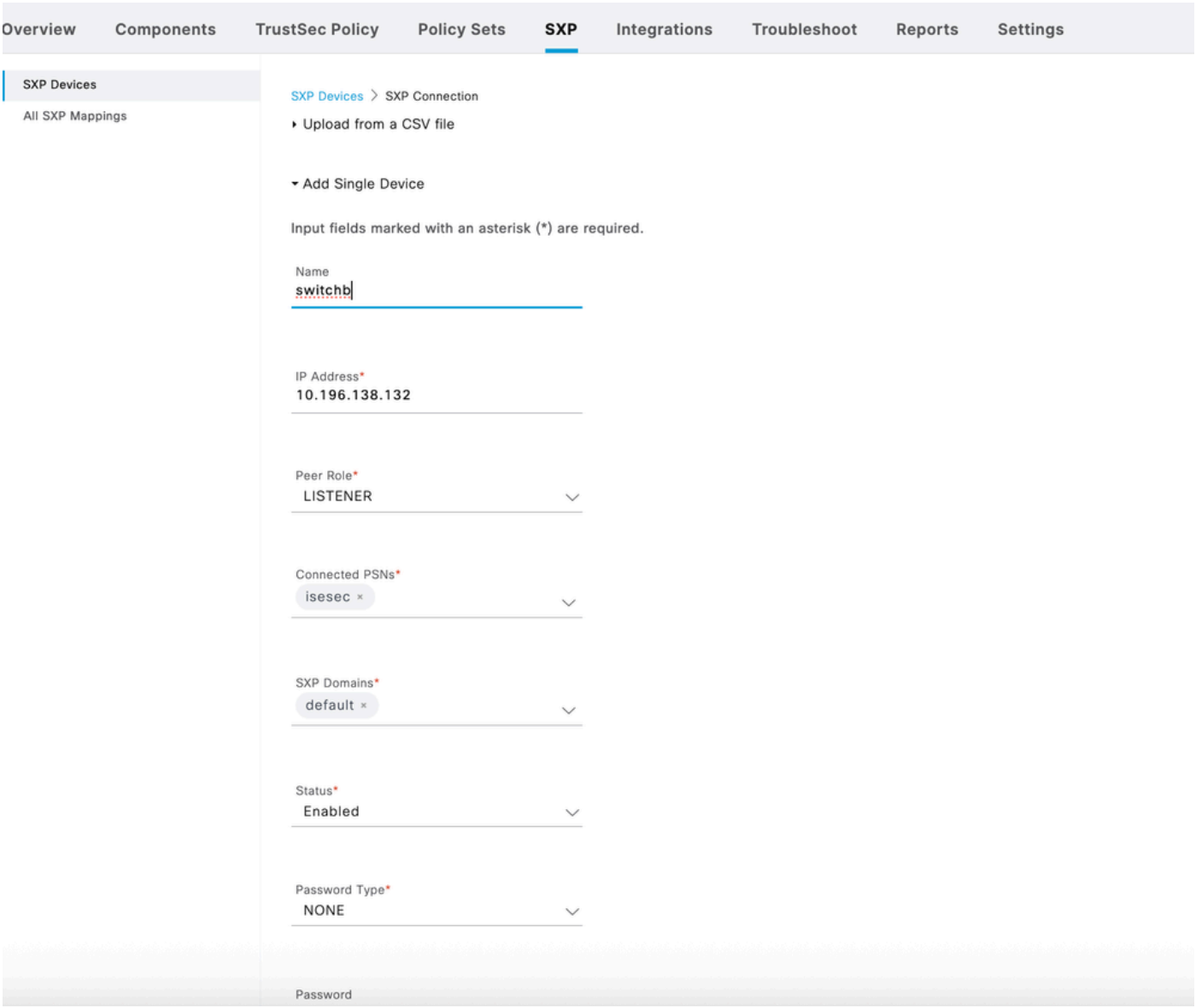
cts sxp default password xxxx@123

ISE Configuration

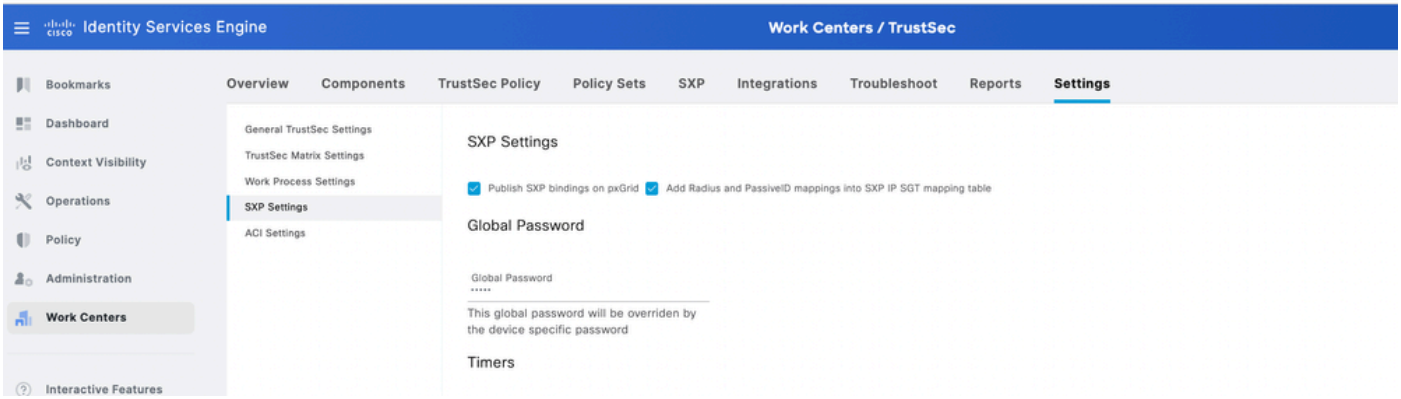
Step 1: Create Authentication and Authorization policies on ISE



Step 2: Configure a SXP Device on ISE



Step 3: Configure Global Password under SXP Settings



Verify

WS-C3850-48F-E#show access-session interface gig1/0/45 details

Interface: GigabitEthernet1/0/45

IIF-ID: 0x1A146F96

MAC Address: b496.9126.decc

IPv6 Address: Unknown

IPv4 Address: Unknown

User-Name: divya123

Status: Authorized

Domain: DATA

Oper host mode: single-host

Oper control dir: both

Session timeout: N/A

Common Session ID: 000000000000000B95163D98

Acct Session ID: Unknown

Handle: 0x6f000001

Current Policy: POLICY_Gi1/0/45

Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_MUST_SECURE (priority 150)

Security Policy: Must Secure

Security Status: Link Unsecured

Server Policies:

Method status list:

Method State

dot1x Authc Success

WS-C3850-48F-E#

WS-C3850-48F-E(config)#do show cts sxp conn

SXP : Enabled

Highest Version Supported: 4

Default Password : Set

Default Key-Chain: Not Set

Default Key-Chain Name: Not Applicable

Default Source IP: 10.196.138.yyy

Connection retry open period: 120 secs

Reconcile period: 120 secs

Retry open timer is running

Peer-Sequence traverse limit for export: Not Set

Peer-Sequence traverse limit for import: Not Set

Peer IP : 10.127.197.xxx

Source IP : 10.196.138.yyy

Conn status : On

Conn version : 4

Conn capability : IPv4-IPv6-Subnet

Conn hold time : 120 seconds

Local mode : SXP Listener

Connection inst# : 1

TCP conn fd : 1

TCP conn password: none

Hold timer is running

Duration since last state change: 0:00:00:22 (dd:hr:mm:sec)

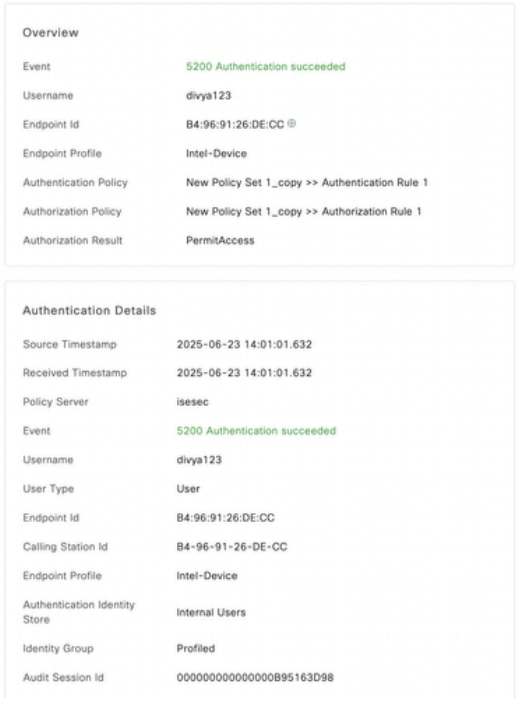
Total num of SXP Connections = 1

0xFF8CBFC090 VRF:, fd: 1, peer ip: 10.127.197.xxx

cdbp:0xFF8CBFC090 <10.127.197.145, 10.196.138.yyy> tableid:0x0

WS-C3850-48F-E(config)#

The live log report shows SGT tag **Guest applied**:

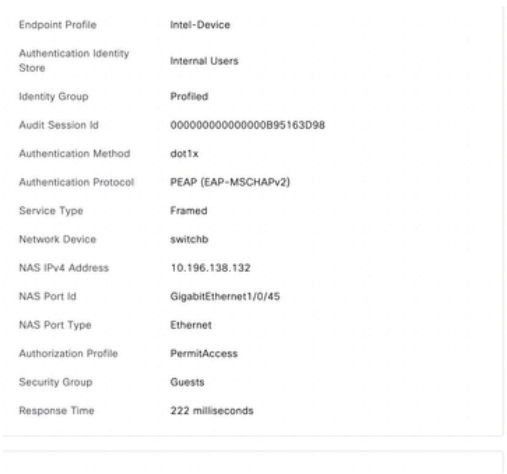


Overview

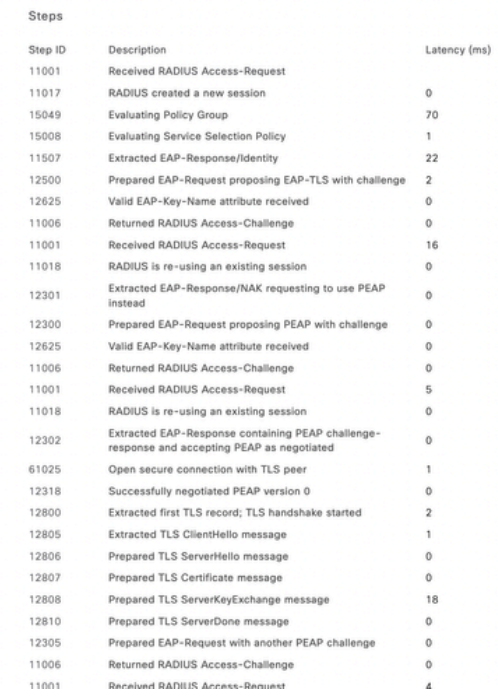
Event	5200 Authentication succeeded
Username	divya123
Endpoint Id	B4:96:91:26:DE:CC
Endpoint Profile	Intel-Device
Authentication Policy	New Policy Set 1_copy >> Authentication Rule 1
Authorization Policy	New Policy Set 1_copy >> Authorization Rule 1
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2025-06-23 14:01:01.632
Received Timestamp	2025-06-23 14:01:01.632
Policy Server	isesec
Event	5200 Authentication succeeded
Username	divya123
User Type	User
Endpoint Id	B4:96:91:26:DE:CC
Calling Station Id	B4-96-91-26-DE-CC
Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98

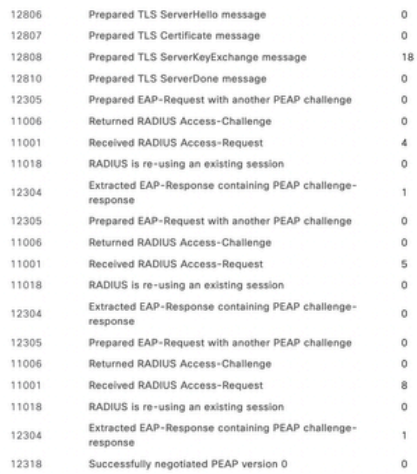


Endpoint Profile	Intel-Device
Authentication Identity Store	Internal Users
Identity Group	Profiled
Audit Session Id	000000000000000B95163D98
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	switchb
NAS IPv4 Address	10.196.138.132
NAS Port Id	GigabitEthernet1/0/45
NAS Port Type	Ethernet
Authorization Profile	PermitAccess
Security Group	Guests
Response Time	222 milliseconds



Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request	
11017	RADIUS created a new session	0
15049	Evaluating Policy Group	70
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	22
12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	16
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	2
12805	Extracted TLS ClientHello message	1
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4



12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	18
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	4
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-response	1
12318	Successfully negotiated PEAP version 0	0

Troubleshoot

Enable this debug on the switch to troubleshoot dot1x issues:

- **debug dot1x all**

Log Explanation

dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x1 >>>>> **EAPoL packet received by switch**
dot1x-packet: length: 0x0000

dot1x-ev:[b496.9126.decc, Gig1/0/45] client detected, sending session start event for b496.9126.decc >>>>> **dot1x client detected**

dot1x-ev:[b496.9126.decc, Gig1/0/45] Dot1x authentication started for 0x26000007 (b496.9126.decc)>>>>> **dot1x started**

%AUTHMGR-5-START: Starting 'dot1x' for client (b496.9126.decc) on Interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting !EAP_RESTART on Client 0x26000007
/>>>>> **Requesting client to restart the EAP Proces**

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting RX_REQ on Client 0x26000007 >>>>> **waiting fot the EAPoL packet fromt he client**

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting AUTH_START for 0x26000007 >>>>> **Starting authentication process**

dot1x-ev:[b496.9126.decc, Gig1/0/45] Sending out EAPOL packet >>>>> **Identity Request**
dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-packet: length: 0x0005
dot1x-packet:EAP code: 0x1 id: 0x1 length: 0x0005
dot1x-packet: type: 0x1
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL packet sent to client 0x26000007

dot1x-ev:[Gig1/0/45] Received pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.000a
dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x0 // Identity Response
dot1x-packet: length: 0x000A

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAPOL_EAP for 0x26000007 >>>>> **EAPoL packet(EAP Response) received, preparing request to server**

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_REQ for 0x26000007 >>>>> **Server response received, EAP Request is being prepared**

dot1x-ev:[b496.9126.decc, Gig1/0/45] Sending out EAPOL packet
dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-packet: length: 0x0006
dot1x-packet:EAP code: 0x1 id: 0xE5 length: 0x0006
dot1x-packet: type: 0xD
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL packet sent to client 0x26000007 >>>>> **EAP request sent out**

dot1x-ev:[Gig1/0/45] Received pkt saddr =b496.9126.decc , daddr = 0180.c200.0003, pae-ether-type = 888e.0100.0006 //EAP response received
dot1x-packet:EAPOL pak rx - Ver: 0x1 type: 0x0
dot1x-packet: length: 0x0006
||
||
||
|| Here a lot of EAPOL-EAP and EAP_REQ events occur as a lot of information is exchanged between the switch and the client
|| If the events after this do not follow, then the timers and the information sent till now need to be checked
||
||
||
dot1x-packet:[b496.9126.decc, Gig1/0/45] Received an EAP Success >>>>> **EAP Success recieved from Server**

dot1x-sm:[b496.9126.decc, Gig1/0/45] Posting EAP_SUCCESS for 0x26000007 >>>>> **Posting EAP Success event**

dot1x-sm:[b496.9126.decc,Gig1/0/45] Posting AUTH_SUCCESS on Client 0x26000007 >>>>> **Posting**

Authentication success

%DOT1X-5-SUCCESS: Authentication successful for client (b496.9126.decc) on Interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-packet:[b496.9126.decc, Gig1/0/45] EAP Key data detected adding to attribute list >>>>> **Additional key data detected sent by server**

%AUTHMGR-5-SUCCESS: Authorization succeeded for client (b496.9126.decc) on Interface Gig1/0/45 AuditSessionID 0A6A258E0000003500C9CFC3

dot1x-ev:[b496.9126.decc, Gig1/0/45] Received Authz Success for the client 0x26000007 (b496.9126.decc) >>>>> **Authorization Success**

dot1x-ev:[b496.9126.decc, Gig1/0/45] Sending out EAPOL packet >>>>> **Sending EAP Success to the client**
dot1x-packet:EAPOL pak Tx - Ver: 0x3 type: 0x0
dot1x-packet: length: 0x0004
dot1x-packet:EAP code: 0x3 id: 0xED length: 0x0004
dot1x-packet:[b496.9126.decc, Gig1/0/45] EAPOL packet sent to client 0x26000007