TrustSec Configuration Guide

TrustSec With Easy Connect Configuration Guide

TrustSec
Software-Defined
Segmentation

Table of Contents

Easy Connect

Introduction

Network segmentation is essential for protecting critical business assets, but traditional segmentation approaches involve operational complexity and can be difficult to introduce to existing environments gracefully. Balancing the demands for agility and security requires a new approach.

With TrustSec, controls are defined simply using endpoint roles, not IP addresses. By classifying systems using human-friendly logical groups, security rules can be defined using these groups, which are more flexible and much easier to manage than using IP address-based controls. These security groups can be used to simplify firewall rules, web security appliance policies and the access control lists used in switches, WLAN controllers and routers.

Security Groups can also be used to enable software-defined segmentation, allowing segmentation patterns to be implemented and changed without reconfiguring network devices or redesigning the network.

This configuration guide covers how managed endpoints can be mapped into Security Groups using Easy Connect, a passive identity method.

Easy Connect simplifies network access control and segmentation by allowing the assignment of Security Group Tags to endpoints without requiring 802.1X on those endpoints, whether using wired or wireless connectivity.

Active Directory logins are used to map user information onto network connections, which are then used for authorizing users on the network even when the Identity Services Engine (ISE) is not involved in the authentication process. Consequently, this authorization method only supports devices that authenticate with a Domain Controller. Easy Connect can also be used as a backup authentication method to 802.1X, to ensure that managed assets are classified even when an 802.1X supplicant is not correctly configured. This can dramatically reduce help desk calls.

The purpose of this document is to show how Easy Connect can be used to enable software defined segmentation with TrustSec, without dependencies on the use of 802.1X.

Easy Connect and 802.1X can both be used on the same ISE platform and there are no restrictions on having 802.1X and Easy Connect co-existing.

The Easy Connect functionality is provided in ISE release 2.1

Summary of Operation

A switch has an access port configured for Mac Authentication Bypass (MAB), or configured for 802.1X with MAB backup. A windows endpoint without an 802.1X supplicant is connected to that access port and the switch generates a MAB RADIUS Access-Request message to ISE incorporating the endpoint MAC address in the username field. If used in a backup scenario, 802.1X would first timeout before the switch falls back into MAB mode. ISE initially replies with a RADIUS Access-Accept message allowing limited access so the endpoint can still communicate with Active Directory (AD). The user/username is not known at this stage.

The user using the Windows endpoint then logs onto the AD domain. ISE learns of the username and session information from AD via the use of Windows Management Instrumentation (WMI) messaging (otherwise known as PassiveID). Through binding this information from AD, information from the MAB session and information from RADIUS Accounting messages, ISE can then send a RADIUS CoA (Authorize-Only) to the switch to re-authenticate the user. When the subsequent second RADIUS Access-Request message is received, ISE has all the information it needs in the session directory to authorize the user and give Full Access with an assigned Security Group Tag (SGT).

Once the ISE session directory includes an IP address and a SGT for a session, that information can be sent to network devices to be used in TrustSec operation. For instance, if the Network Access Device (NAD) supports TrustSec then the IP address and SGT sent in the RADIUS Accept-Accept message from ISE will be stored in the NAD for TrustSec classification, and the SGT used in enforcement if enabled. If TrustSec enforcement is enabled in other parts of the network then the IP-to-SGT mapping could be sent from the NAD towards those enforcement points using TrustSec propagation. Alternatively, ISE can send the IP-to-SGT mapping directly to network devices via SSH or SXP, which negates the need for the NAD to support TrustSec.

This guide covers the SXP use case. If SXP is enabled in ISE, then the IP-to-SGT map is stored in the SXP Mappings Table. That mapping is then immediately forwarded to SXP destinations (TrustSec network enforcement points) as defined in the SXP Devices table.

The network enforcement points can use the received IP-to-SGT mapping to enforce policy sourced from and destined to that user/endpoint.

Figure 1: ISE Uses The IP Address To Bind User Mappings Learned From AD (PassiveID) and MAB Information From Access Switch:

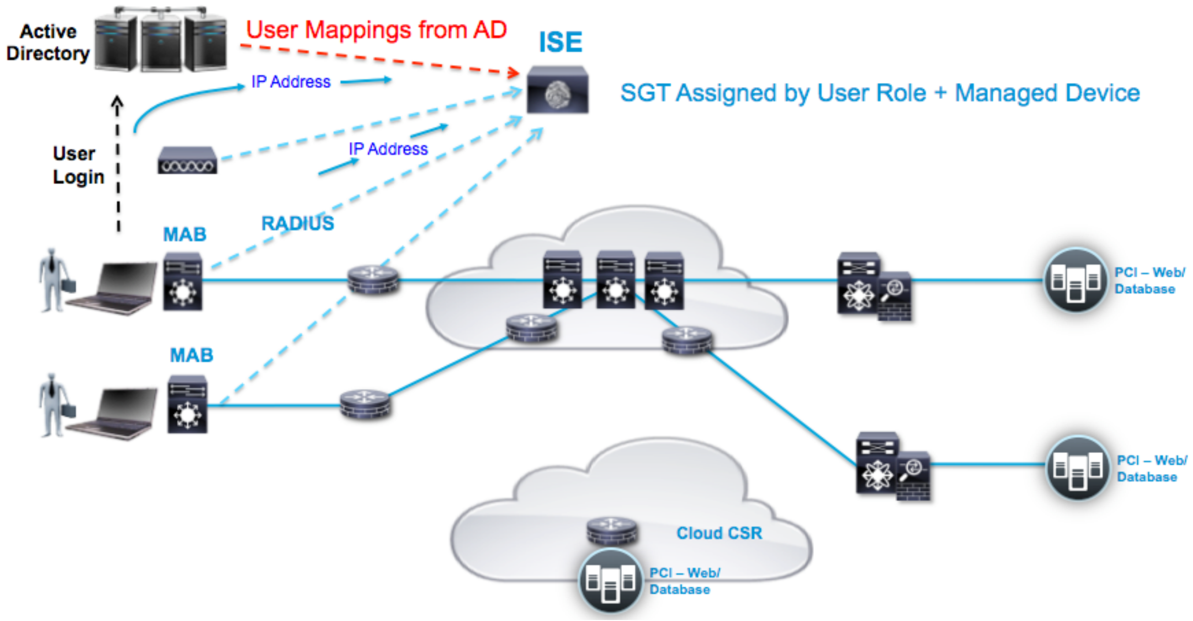
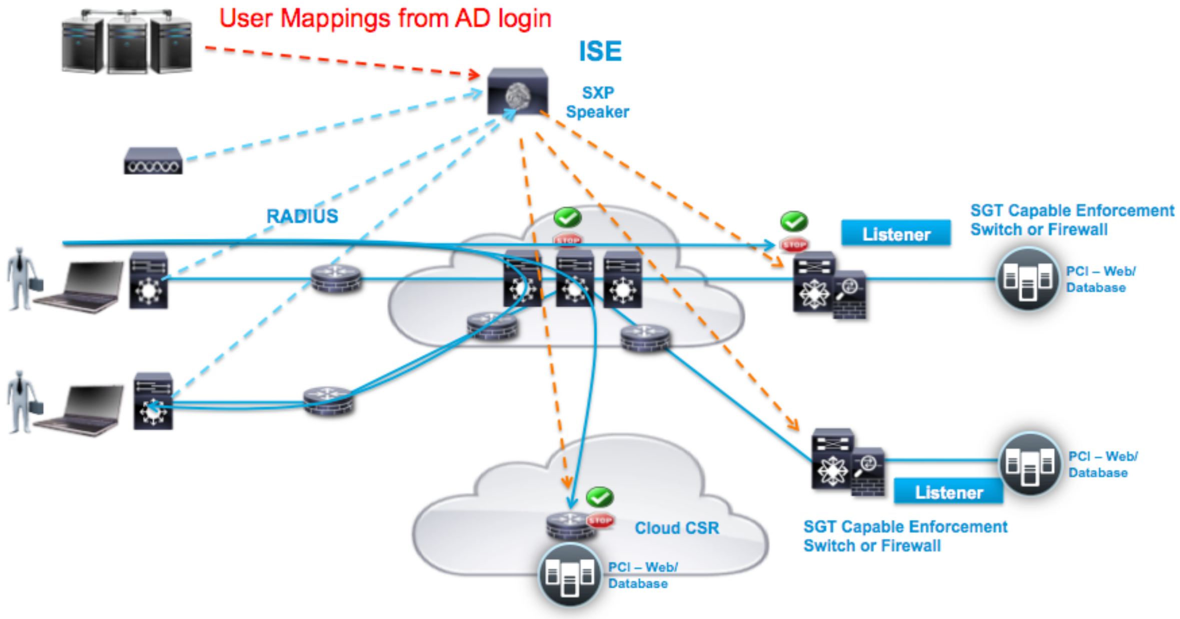


Figure 2: The IP Learned And SGT Assigned Allows the IP-to-SGT Mapping To Be Created and Forwarded To SXP Destinations:



Configuration

Setting Up Active Directory (AD) for PassiveID

AD needs to have WMI messaging enabled.

Follow the ISE 2.1 admin guide for setting this up on AD:

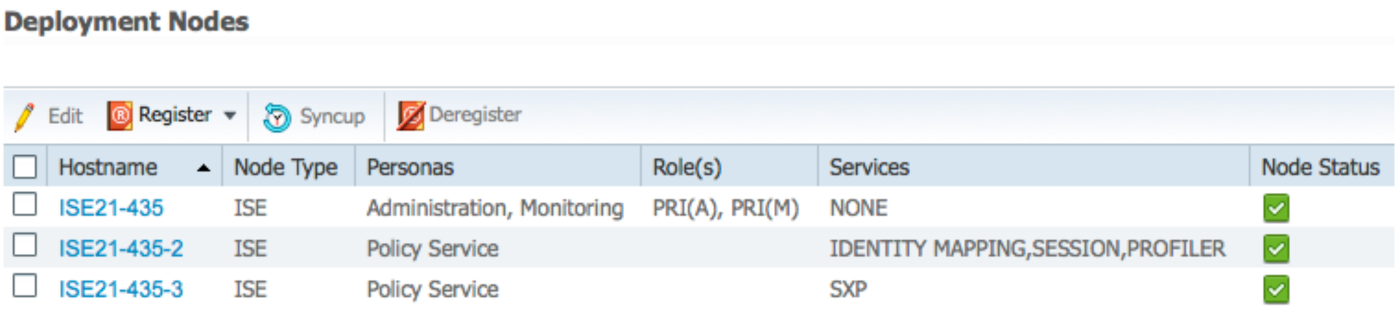
http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_01101.html#task_3580FB80B8394E078393C71E4AA1233B

Setting Up ISE

Enabling SXP and PassiveID

It is recommended to keep SXP and PassiveID functionality on different ISE instances. This is configured under Administration > System > Deployment.

In this small deployment example, PassiveID (Identity Mapping) is enabled on the ISE instance with the PSN Session and Profiler services. SXP is enabled on a dedicated ISE instance:



Deployment Nodes

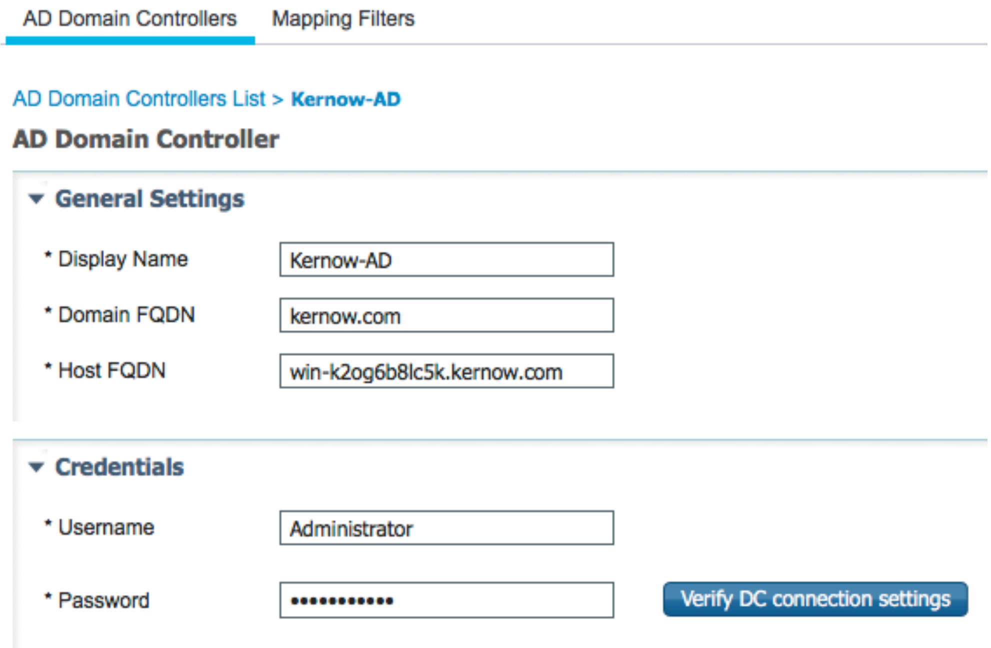
□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
□	ISE21-435	ISE	Administration, Monitoring	PRI(A), PRI(M)	NONE	✓
□	ISE21-435-2	ISE	Policy Service		IDENTITY MAPPING,SESSION,PROFILER	✓
□	ISE21-435-3	ISE	Policy Service		SXP	✓

Note: pxGrid is not a requirement for Easy Connect and therefore does not need to be enabled. If enabled, it can be used to export mappings to other systems.

Adding PassiveID to ISE

This section details how to add PassiveID within ISE so there can be interaction with AD via WMI messaging. AD should have previously been added to ISE using Administration > Identity Management > External Identity Sources > Active Directory.

Once AD has WMI (PassiveID) enabled, in ISE add the AD under Administration > PassiveID > AD Domain Controllers:


AD Domain Controllers
Mapping Filters
AD Domain Controllers List > Kernow-AD

AD Domain Controller

General Settings

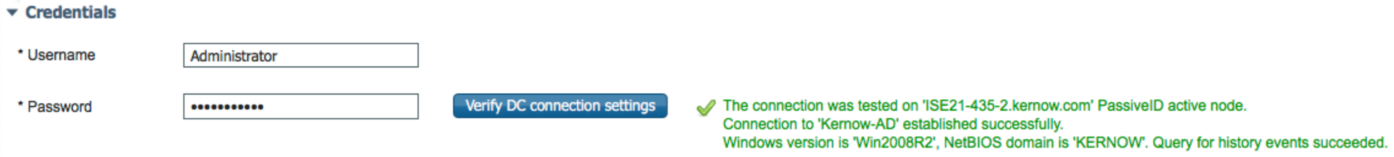
* Display Name	Kernow-AD
* Domain FQDN	kernow.com
* Host FQDN	win-k2og6b8lc5k.kernow.com

Credentials

* Username	Administrator
* Password	••••••••••••

Verify DC connection settings

Note: Use ‘Verify DC connection settings’ to check AD connectivity.

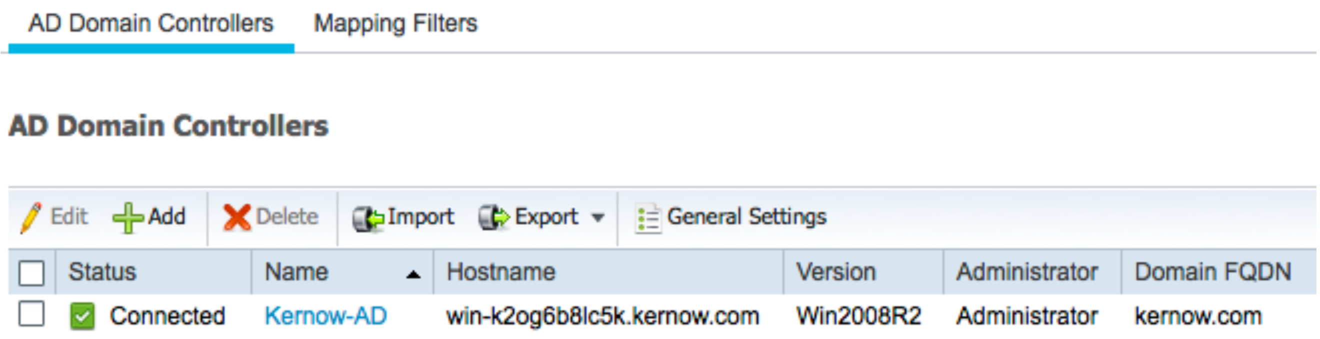


Credentials

* Username	Administrator
* Password	•••••••••••

✓ The connection was tested on 'ISE21-435-2.kernow.com' PassiveID active node.
Connection to 'Kernow-AD' established successfully.
Windows version is 'Win2008R2', NetBIOS domain is 'KERNOW'. Query for history events succeeded.

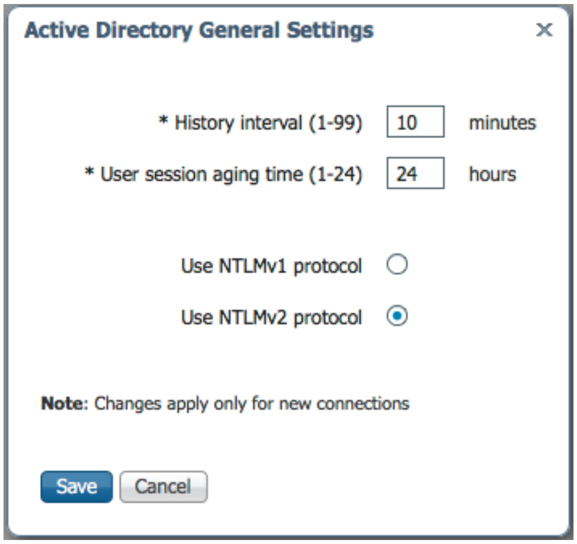
Once saved, the AD Domain Controller should show as ‘Connected’ in the Administration > PassiveID > AD Domain Controllers screen:



AD Domain Controllers

☐	Status	Name ▲	Hostname	Version	Administrator	Domain FQDN
☐	☑ Connected	Kernow-AD	win-k2og6b8lc5k.kernow.com	Win2008R2	Administrator	kernow.com

There are further options to be investigated under the ‘General Settings’ tab that can be seen above:



Active Directory General Settings

* History interval (1-99) 10 minutes

* User session aging time (1-24) 24 hours

Use NTLMv1 protocol ○

Use NTLMv2 protocol ●

Note: Changes apply only for new connections

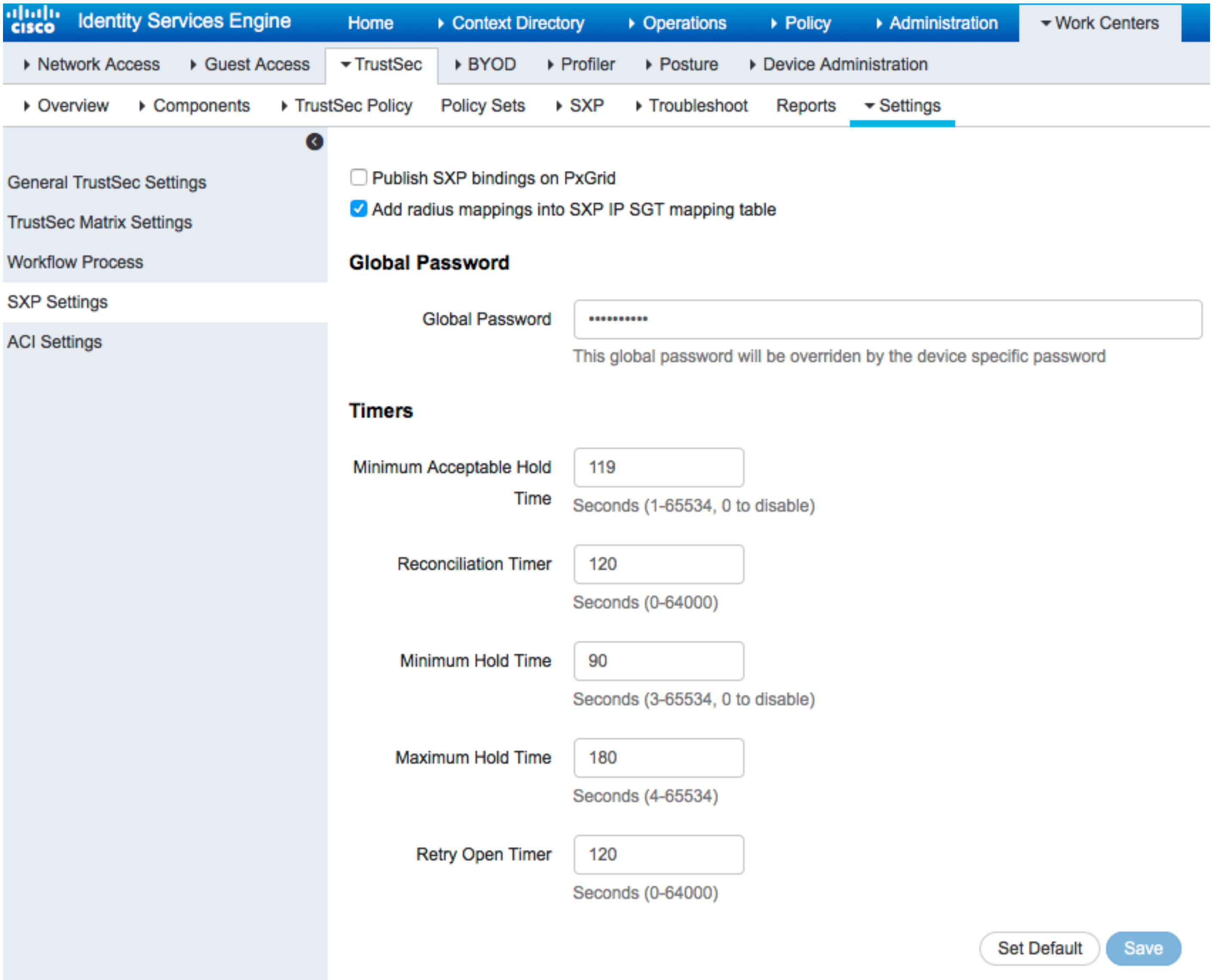
History interval is the time during which Easy Connect reads user login information that already occurred. This is required upon startup or restart of Identity Mapping to catch up with events generated while it was unavailable.

User session aging time is the amount of time the user can be logged in. Easy Connect identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables Cisco ISE to determine the time interval for which the user is logged in.

You can select either **NTLMv1** or **NTLMv2** as the communications protocol between the ISE and the Domain Controller.

Setting SXP Attributes

Before adding SXP Devices / Connections in ISE, you can set SXP attributes (like timers and default password) under Work Centers > TrustSec > Settings > SXP Settings



□ Publish SXP bindings on PxGrid

☑ Add radius mappings into SXP IP SGT mapping table

Global Password

Global Password: •••••••••••

This global password will be overriden by the device specific password

Timers

Minimum Acceptable Hold Time: 119 Seconds (1-65534, 0 to disable)

Reconciliation Timer: 120 Seconds (0-64000)

Minimum Hold Time: 90 Seconds (3-65534, 0 to disable)

Maximum Hold Time: 180 Seconds (4-65534)

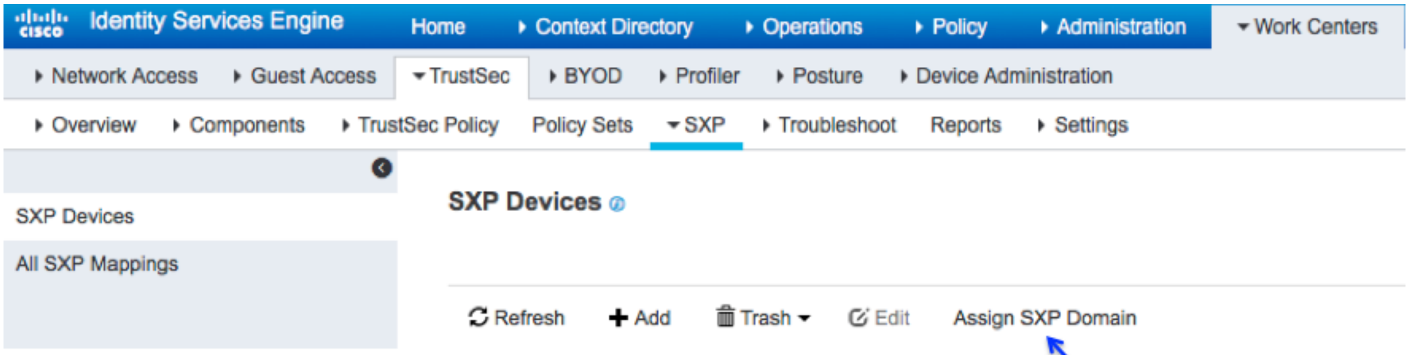
Retry Open Timer: 120 Seconds (0-64000)

Note: Ensure the tick boxes are selected appropriately for publishing SXP bindings on PxGrid and/or adding dynamic RADIUS mappings into the ISE SXP mapping table.

Adding SXP Domains

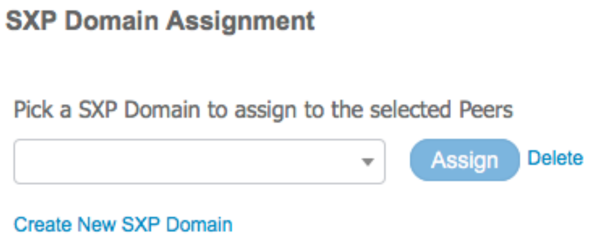
Before adding SXP Devices / Connections in ISE, there is a concept of SXP Domains that needs to be understood. An SXP Domain is a collection of SXP Devices and the administrator can decide which domain to send IP-to-SGT mappings to. This is not mandatory as a Default Domain exists and this is used by default for all SXP Devices and all IP-to-SGT mappings.

If using SXP Domains to control the distribution of mappings, add the required Domains from Work Centers > TrustSec > SXP > SXP Devices:



Click here to add SXP Domains

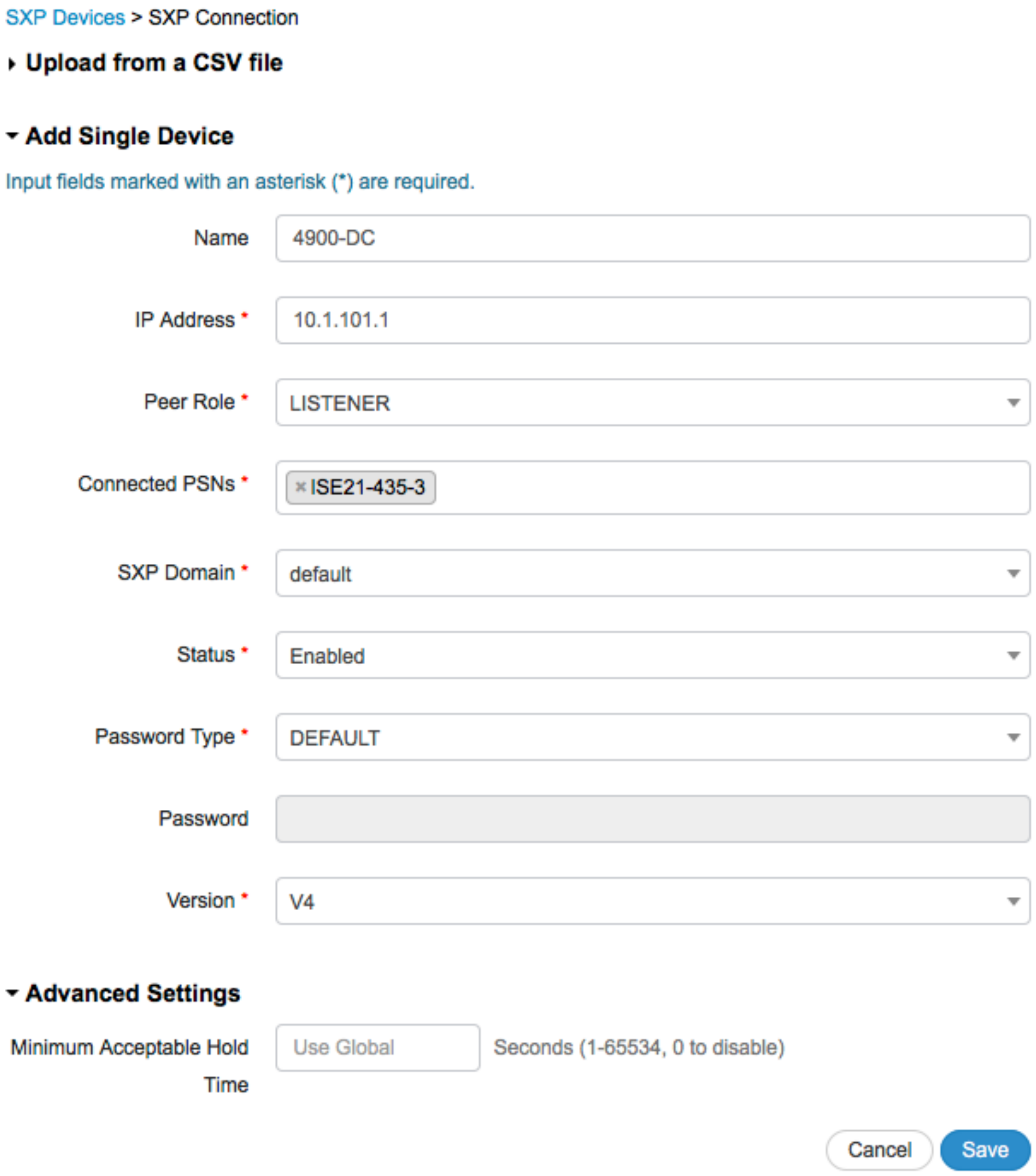
Once ‘Assign SXP Domain’ is selected, click on the ‘Create New SXP Domain’ link as shown below:



These domains are selected when adding SXP Devices and can also be assigned / modified after the Devices have been added.

Adding SXP Devices / Connections

SXP Devices / Connections can be added using Work Centers > TrustSec > SXP > SXP Devices



SXP Devices > SXP Connection

▸ Upload from a CSV file

▾ Add Single Device

Input fields marked with an asterisk (*) are required.

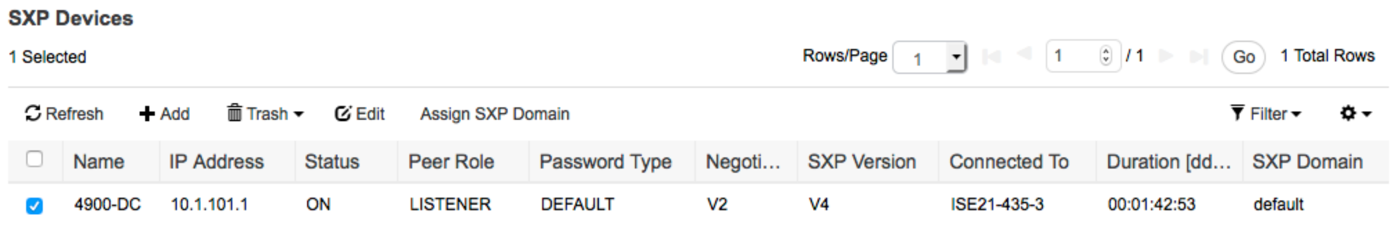
Name	4900-DC
IP Address *	10.1.101.1
Peer Role *	LISTENER
Connected PSNs *	× ISE21-435-3
SXP Domain *	default
Status *	Enabled
Password Type *	DEFAULT
Password	
Version *	V4

▾ Advanced Settings

Minimum Acceptable Hold Time: Use Global Seconds (1-65534, 0 to disable)

When the network device at the remote end of the SXP connection has been configured and communication established, the SXP status shown on ISE will be shown as 'ON'.

On ISE, navigate to Work Centers > TrustSec > SXP > SXP Devices:



SXP Devices

1 Selected

☐	Name	IP Address	Status	Peer Role	Password Type	Negoti...	SXP Version	Connected To	Duration [dd...	SXP Domain
☑	4900-DC	10.1.101.1	ON	LISTENER	DEFAULT	V2	V4	ISE21-435-3	00:01:42:53	default

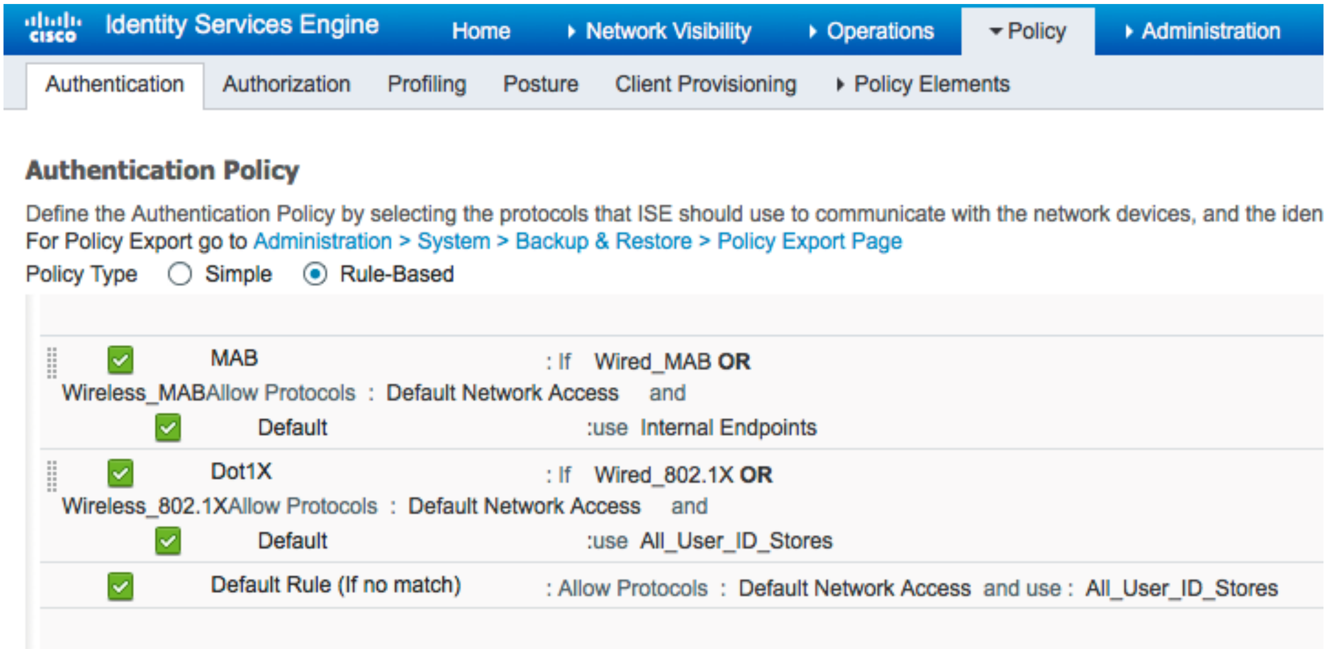
ISE Authentication

With Easy Connect, actual client authentication is accomplished directly against AD.

However, the MAB RADIUS Access-Requests are still routed through the ISE authentication process and therefore entries to handle this must be present in the ISE authentication table.

Using Policy Sets in ISE is not a prerequisite so using the single Default policy table is sufficient; Policy Sets can be used if required.

To configure or display the Authentication Policy without using Policy Sets, navigate to Policy > Authentication:



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the iden
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and
☑ Default :use Internal Endpoints

☑ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access and
☑ Default :use All_User_ID_Stores

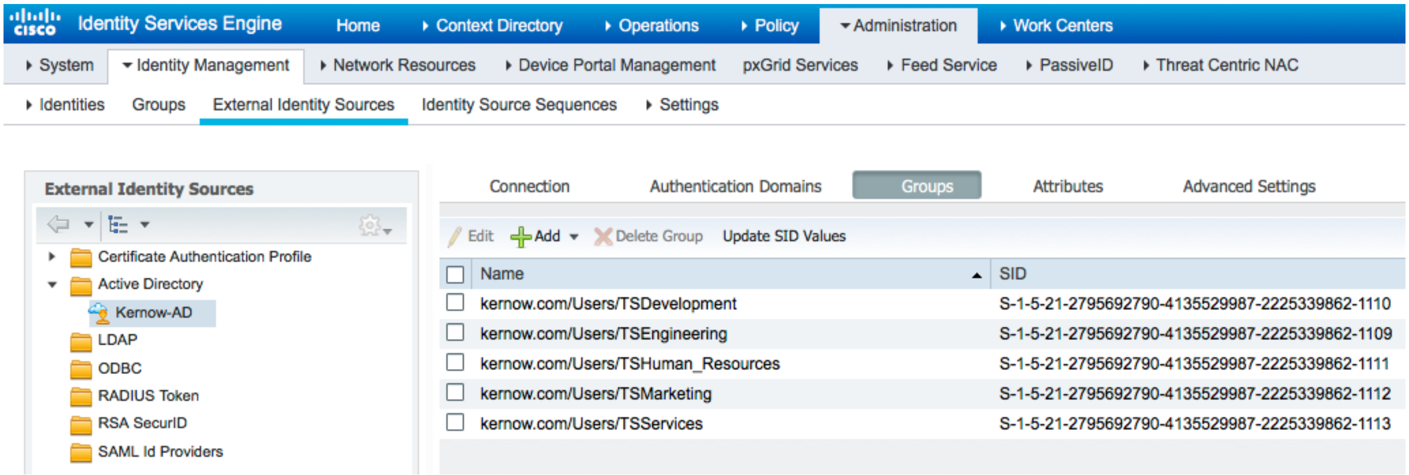
☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : All_User_ID_Stores

The default authentication entry in ISE for MAB is adequate for use with Easy Connect; this can be modified, or other rules added, if required.

ISE Authorization and Components

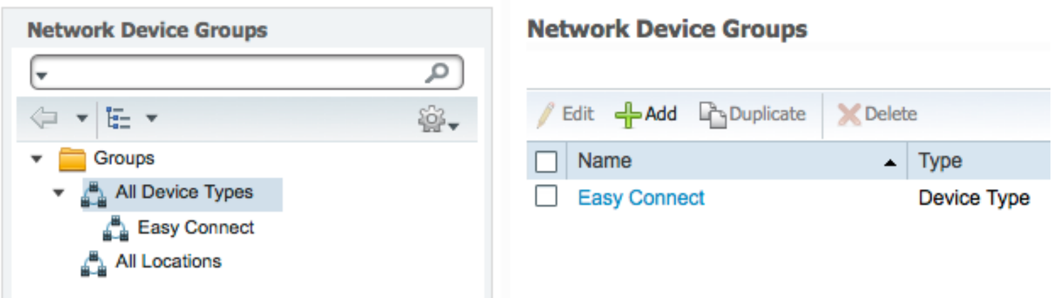
Authorization is a term used to define what access an entity is granted. To determine what access to assign, conditions are used such as being a member of a certain AD group or the request being sourced from a particular Network Device Group (NDG) for example. Once conditions are met, results within permission lists are used to grant the appropriate access.

In order to use AD groups in the ISE authorization policy conditions, the groups first need to be imported into ISE. Using Administration > Identity Management > External Identity Sources > Active Directory > "AD Server Name" > Groups, the required AD groups can be imported into ISE:



☐	Name	SID
☐	kernow.com/Users/TSDevelopment	S-1-5-21-2795692790-4135529987-2225339862-1110
☐	kernow.com/Users/TSEngineering	S-1-5-21-2795692790-4135529987-2225339862-1109
☐	kernow.com/Users/TSHuman_Resources	S-1-5-21-2795692790-4135529987-2225339862-1111
☐	kernow.com/Users/TSMarketing	S-1-5-21-2795692790-4135529987-2225339862-1112
☐	kernow.com/Users/TSServices	S-1-5-21-2795692790-4135529987-2225339862-1113

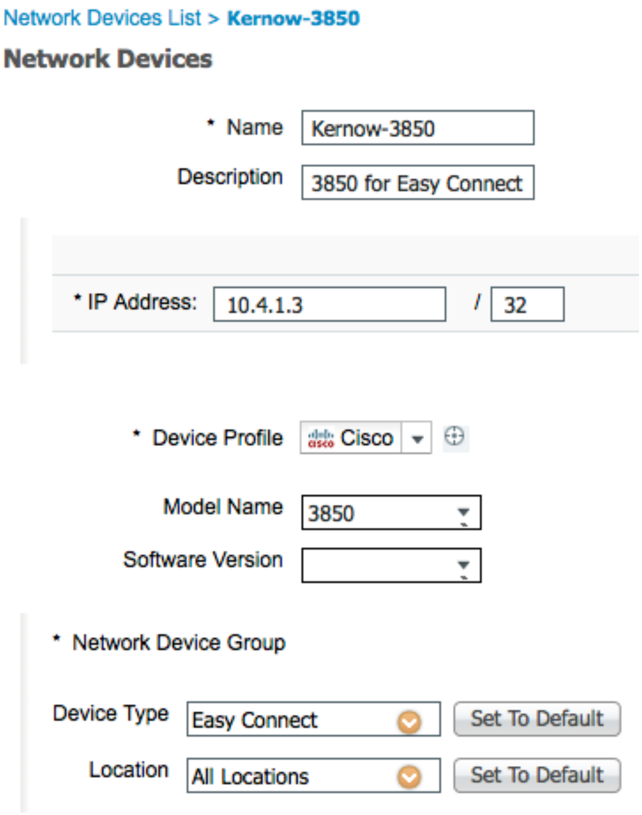
A Network Device Group can be added in ISE using Administration > Network Resources > Network Device Groups. In this example, a Network Device Group called 'Easy Connect' has been added:



☐	Name	Type
☐	Easy Connect	Device Type

This NDG is assigned to an access device. The NDG can then used as a condition in the Authorization Policy to be used when an authentication request originates from that access device.

In this example, the NDG is provisioned into the Device Type field of a 3850 that will be handling the Easy Connect sessions:



Network Devices List > **Kernow-3850**

Network Devices

* Name	Kernow-3850
Description	3850 for Easy Connect
* IP Address:	10.4.1.3 / 32
* Device Profile	Cisco
Model Name	3850
Software Version	

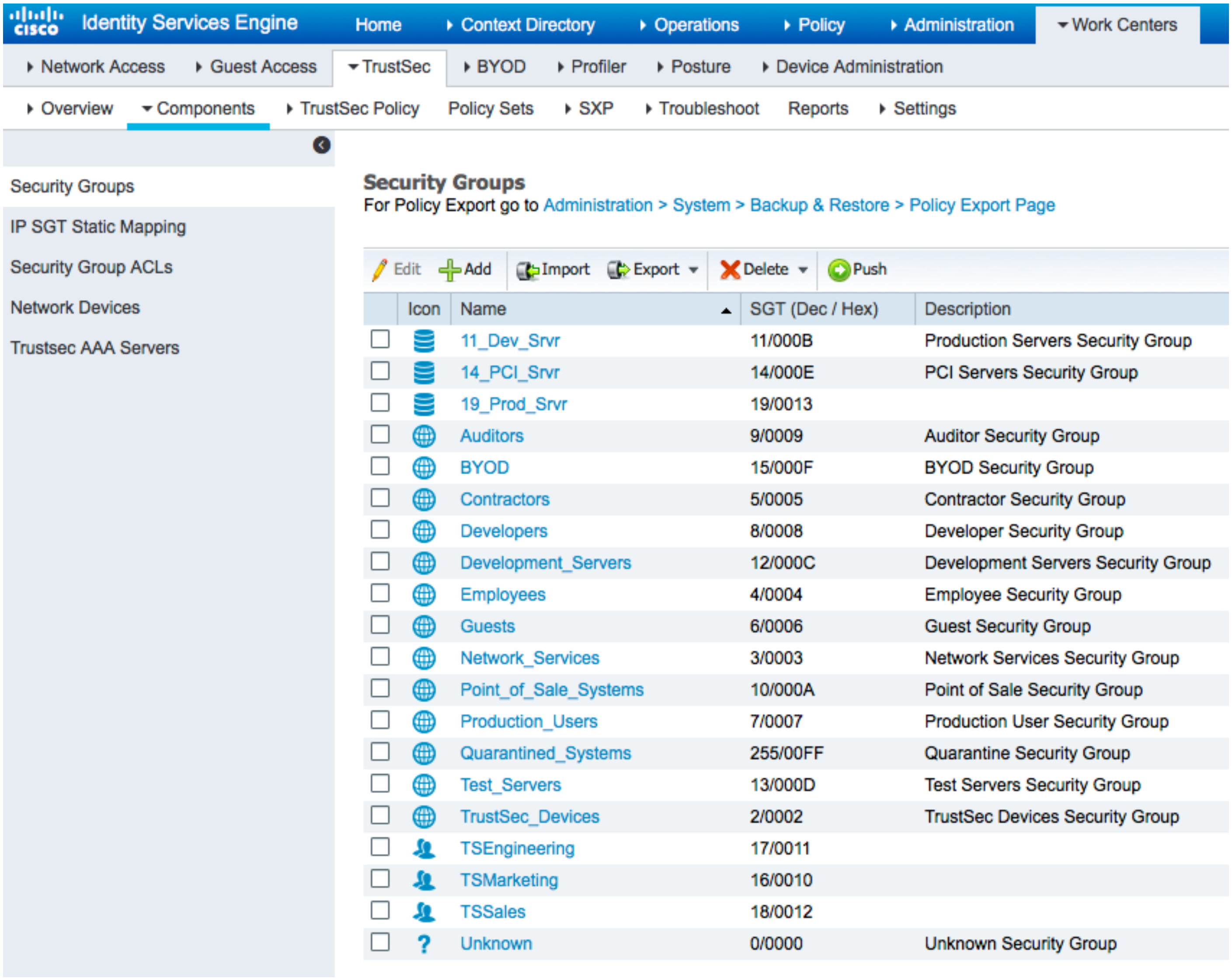
* Network Device Group

Device Type	Easy Connect	Set To Default
Location	All Locations	Set To Default

For ISE authorization permissions, TrustSec Security Groups are used to classify endpoints/users and therefore define the resources those endpoints/users can access.

In order to assign Security Groups in authorization profile permissions, the Security Groups first have to be added into ISE. In ISE 2.1, a number of default Security Groups exist so these can be used or new Security Groups can be added.

In the example below, two new Security Groups that have been added are called TSMarketing and TSEngineeering. These are added in ISE under Work Centers > TrustSec > Components> Security Groups. The Security Group Tag (SGT) assigned to those groups is 16 and 17 respectively in this example:



Security Groups

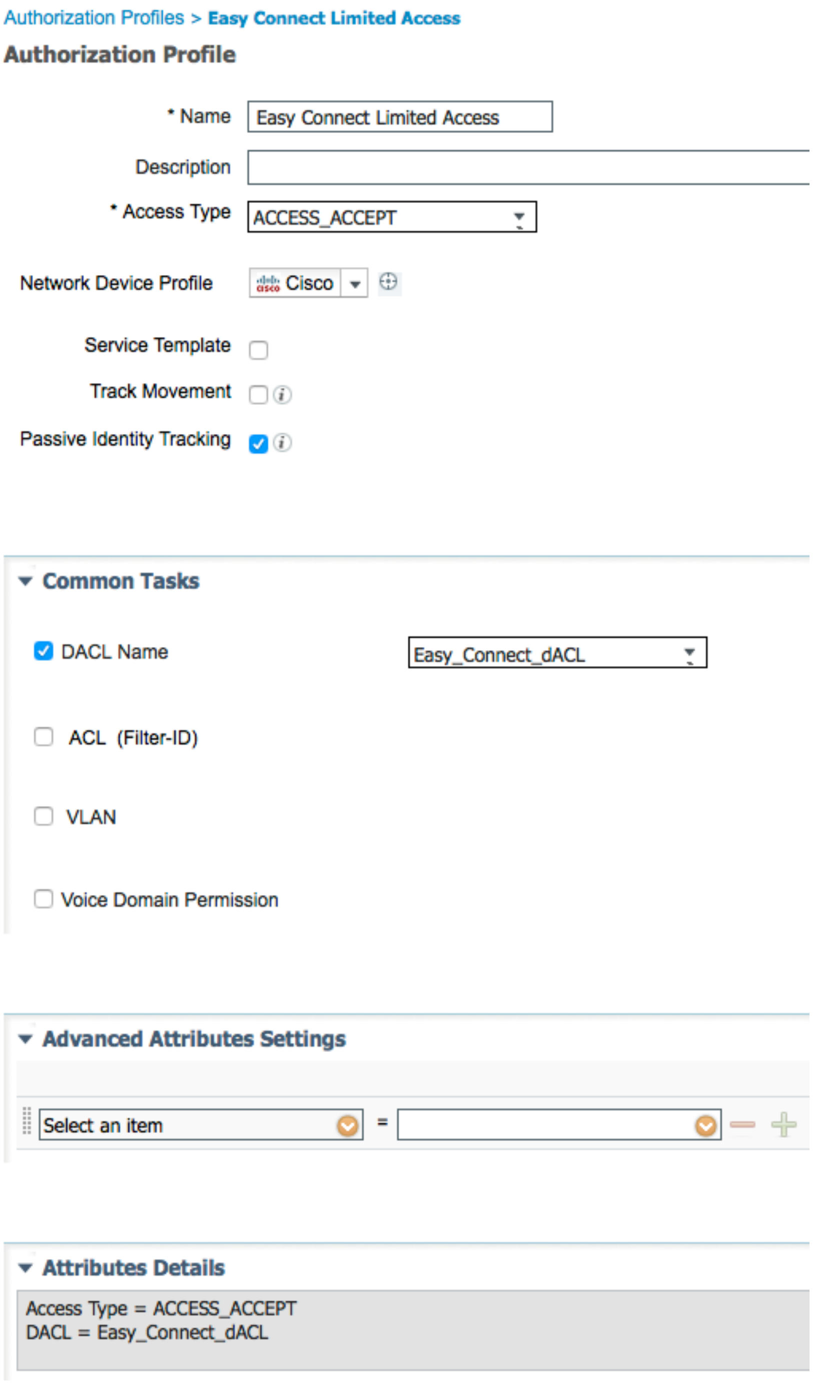
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Icon	Name	SGT (Dec / Hex)	Description
□		11_Dev_Srvr	11/000B	Production Servers Security Group
□		14_PCI_Srvr	14/000E	PCI Servers Security Group
□		19_Prod_Srvr	19/0013	
□		Auditors	9/0009	Auditor Security Group
□		BYOD	15/000F	BYOD Security Group
□		Contractors	5/0005	Contractor Security Group
□		Developers	8/0008	Developer Security Group
□		Development_Servers	12/000C	Development Servers Security Group
□		Employees	4/0004	Employee Security Group
□		Guests	6/0006	Guest Security Group
□		Network_Services	3/0003	Network Services Security Group
□		Point_of_Sale_Systems	10/000A	Point of Sale Security Group
□		Production_Users	7/0007	Production User Security Group
□		Quarantined_Systems	255/00FF	Quarantine Security Group
□		Test_Servers	13/000D	Test Servers Security Group
□		TrustSec_Devices	2/0002	TrustSec Devices Security Group
□		TSEngineering	17/0011	
□		TSMarketing	16/0010	
□		TSSales	18/0012	
□	?	Unknown	0/0000	Unknown Security Group

As well as assigning Security Group Tags (SGTs) in ISE authorization permissions, other results can be defined. You can apply limited access or full access for example. These assignments are set under Authorization Profiles in ISE.

Adding and configuring the authorization profiles can be accomplished by navigating to Policy > Policy Elements > Results > Authorization > Authorization Profiles.

In the following example, the 'Easy Connect Limited Access' entry is defined for when ISE has yet to determine the username of a session. In order to provide a limited service, the authorization profile may well include a limiting downloadable ACL as shown below, but access to AD must be given. This initial authorization profile must have 'Passive Identity Tracking' enabled so the session is tracked for PassiveID operation:



Authorization Profiles > **Easy Connect Limited Access**

Authorization Profile

* Name: Easy Connect Limited Access

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking ☑

Common Tasks

☑ DACL Name: Easy_Connect_dACL

□ ACL (Filter-ID)

□ VLAN

□ Voice Domain Permission

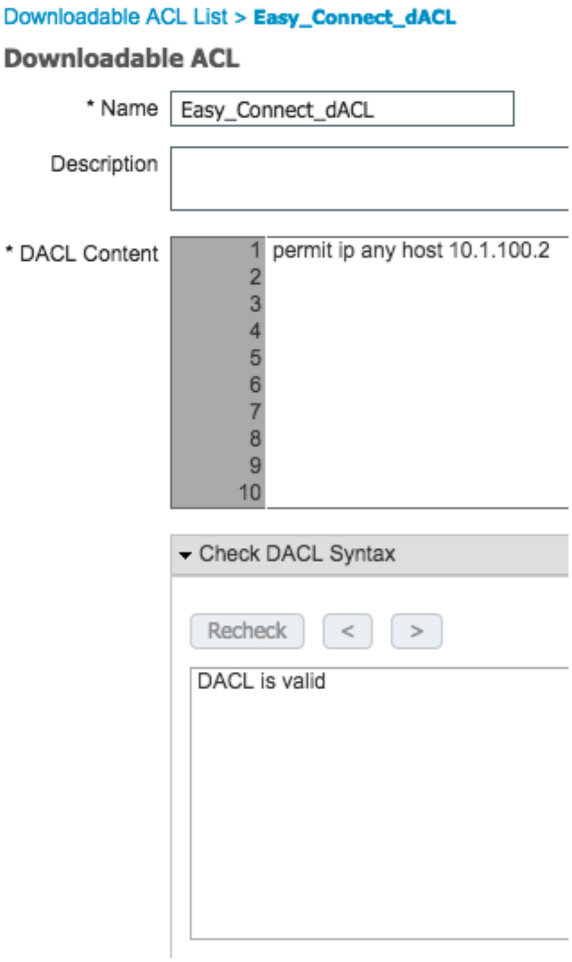
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = Easy_Connect_dACL
```

The dACL named 'Easy_Connect_dACL' was previously defined under Policy > Policy Elements > Results > Authorization > Downloadable ACLs. We are using this to only permit access to Active Directory (10.1.100.2) in the limited access phase:



* Name: Easy_Connect_dACL

Description:

* DACL Content:

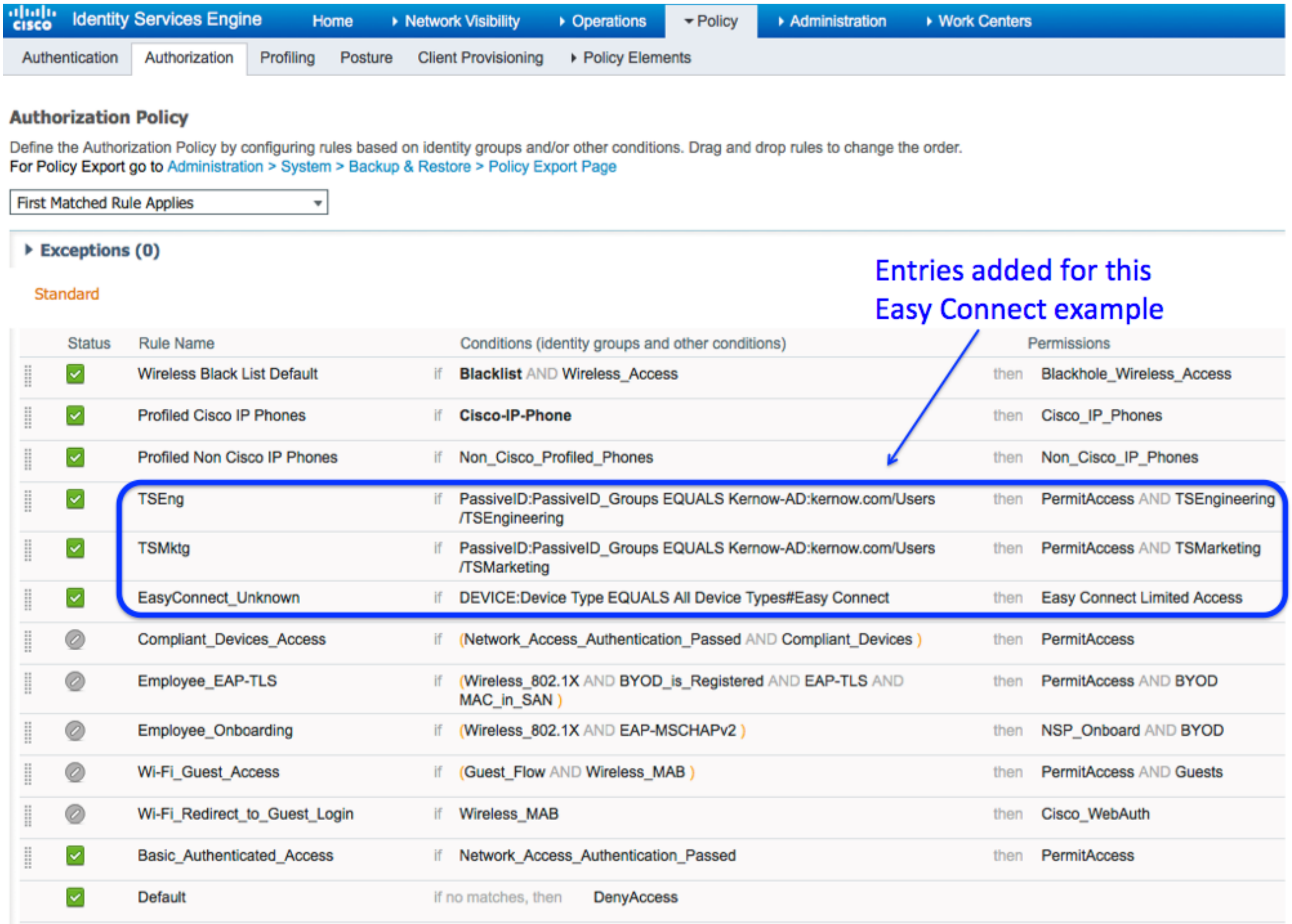
```
permit ip any host 10.1.100.2
```

DACL is valid

The default 'PermitAccess' Authorization Profile entry is used when the user is known and full access is to be granted.

Note: The Passive Identity Tracking selection is only required in the authorization profile for the initial MAB rule i.e. the Limited Access profile, not for the Full Access profile.

Now that the components of authorization have been defined, we can build the Authorization Policy. This is accomplished by navigating to Policy > Authorization in a system without Policy Sets defined.



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

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	TSEng	if	PassiveID:PassiveID_Groups EQUALS Kernow-AD:kernow.com/Users /TSEngineering	then	PermitAccess AND TSEngineering
✓	TSMktg	if	PassiveID:PassiveID_Groups EQUALS Kernow-AD:kernow.com/Users /TSMarketing	then	PermitAccess AND TSMarketing
✓	EasyConnect_Unknown	if	DEVICE:Device Type EQUALS All Device Types#Easy Connect	then	Easy Connect Limited Access
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD
⊘	Wi-Fi_Guest_Access	if	(Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
✓	Default	if no matches, then	DenyAccess		

When the initial MAB request is received by ISE, the username is not known. After the authentication process, ISE steps through the authorization table entries and in this example, the EasyConnect_Unknown rule is matched due to the configured conditions, assigning 'Easy Connect Limited Access' to the session. No SGT is assigned in this example in this limited access state but a SGT can be allocated if required.

The condition used to match this rule in this example is Device Type being 'Easy Connect' which was added previously as a Network Device Group (NDG). Any number of conditions can be used to select your Easy Connect sessions depending on the requirements.

Once ISE has retrieved the WMI message from AD (PassiveID) with the username of the user for this session, a RADIUS CoA (Authorize-Only) instigates a second MAB request from the NAD. This time, when ISE steps through the authorization table entries, the TSEng entry will be matched if the PassiveID user belongs to the AD group called TSEngineering or the TSMktg entry will be matched if the PassiveID user belongs to the AD group called TSMarketing. Full access will then be granted through the allocation of the PermitAccess Authorization profile along with the assignment of the appropriate Security Group Tag (SGT) of TSEngineering or TSMarketing.

Access Switch Configuration

The access switch to be used in this solution does not need to be TrustSec aware but it does require the ability to support RADIUS, MAB and AAA Accounting.

An example switch configuration is shown here:

```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client <ISE IP Address> server-key x
!
aaa session-id common
!
ip device tracking
!
dot1x system-auth-control
!
interface GigabitEthernet1/0/1
 description Connected to Easy Connect Client
 switchport access vlan <VLAN ID>
 switchport mode access
 authentication host-mode multi-auth
 authentication open
 authentication order mab
 authentication priority mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
radius-server vsa send accounting
radius-server vsa send authentication
!
radius server ISE
 address ipv4 <ISE IP Address> auth-port 1812 acct-port 1813
 key x
```

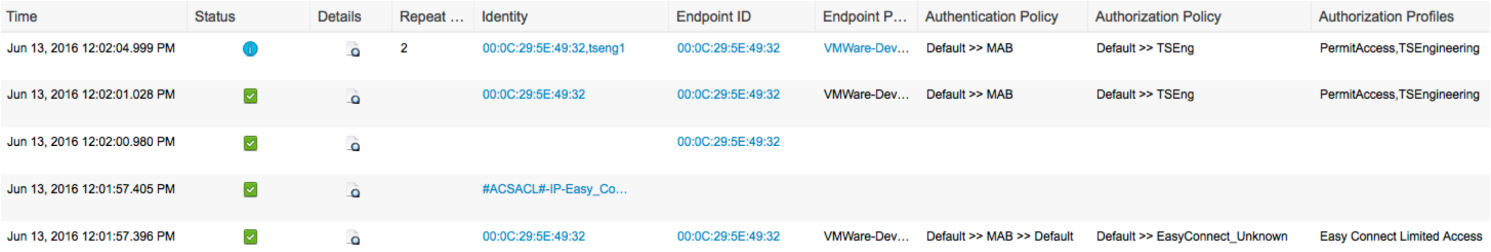
If used in an 802.1X backup scenario, the interface configuration may look similar to the following:

```
interface FastEthernetX
 description Connected to Easy Connect Client
 switchport access vlan <VLAN ID>
 switchport mode access
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
 spanning-tree bpduguard enable
```

Authenticate User and Investigate ISE Livelog

An authentication request can now be tested. Connect a Windows endpoint (without a dot1x supplicant) to the switch access port configured above and log into the windows domain. Alternatively, connect a dot1x client and test the backup to MAB.

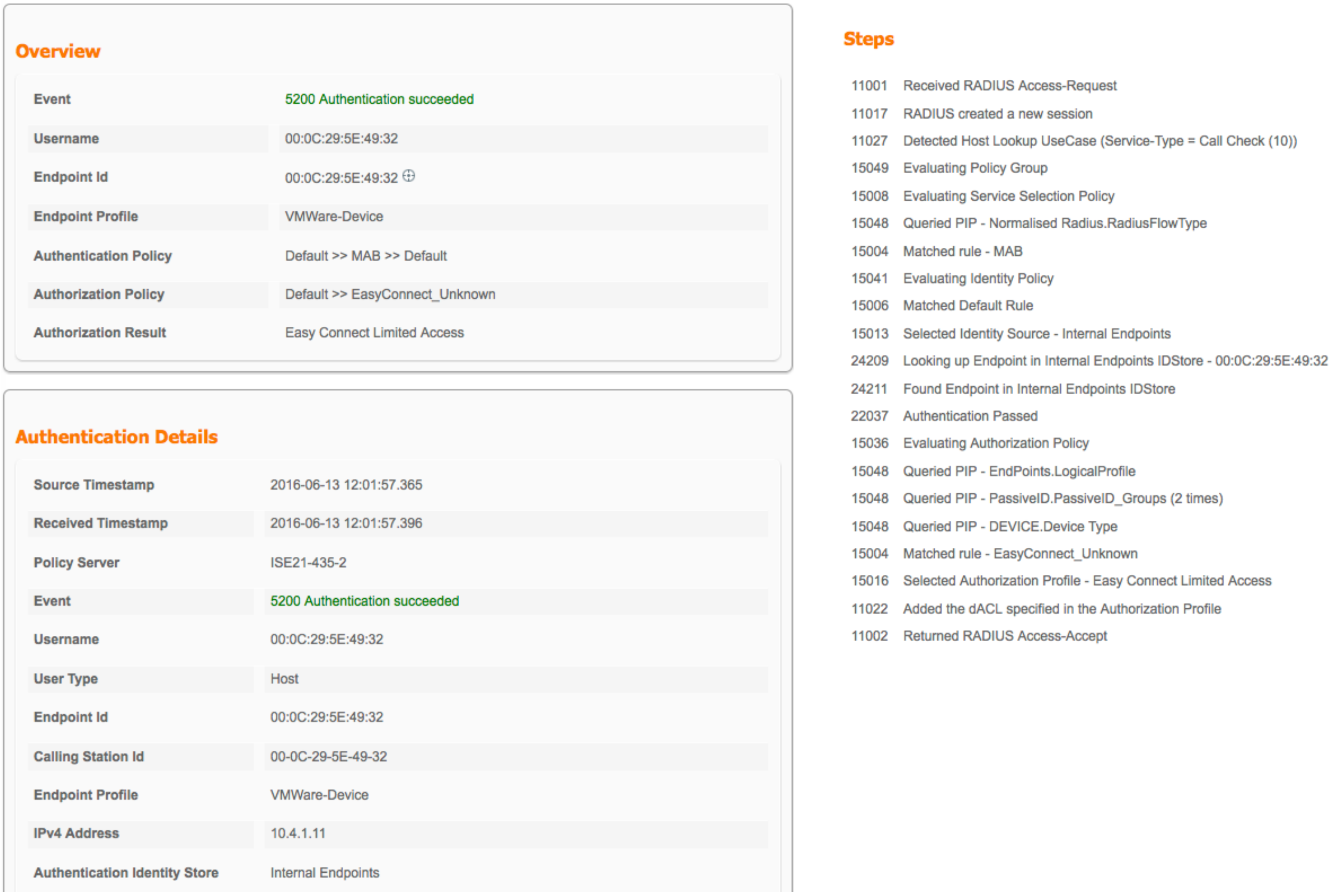
ISE shows the Livelog by navigating to Operations > RADIUS > Livelogs:



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles
Jun 13, 2016 12:02:04.999 PM	ⓘ	🔍	2	00:0C:29:5E:49:32,tseng1	00:0C:29:5E:49:32	VMWare-Dev...	Default >> MAB	Default >> TSEng	PermitAccess,TSEngineering
Jun 13, 2016 12:02:01.028 PM	✓	🔍		00:0C:29:5E:49:32	00:0C:29:5E:49:32	VMWare-Dev...	Default >> MAB	Default >> TSEng	PermitAccess,TSEngineering
Jun 13, 2016 12:02:00.980 PM	✓	🔍			00:0C:29:5E:49:32				
Jun 13, 2016 12:01:57.405 PM	✓	🔍		#ACSACL#-IP-Easy_Co...					
Jun 13, 2016 12:01:57.396 PM	✓	🔍		00:0C:29:5E:49:32	00:0C:29:5E:49:32	VMWare-Dev...	Default >> MAB >> Default	Default >> EasyConnect_Unknown	Easy Connect Limited Access

Working from bottom to top in the livelog entries above, the first entry is logged when the MAB RADIUS-Request is received by ISE. It can be seen above that the Authorization Policy hit is the 'EasyConnect_Unknown' policy, as the user is not known at this stage. The Authorization Profile allocated is 'Easy Connect Limited Access' as previously defined.

Details of that Livelog entry:



Overview

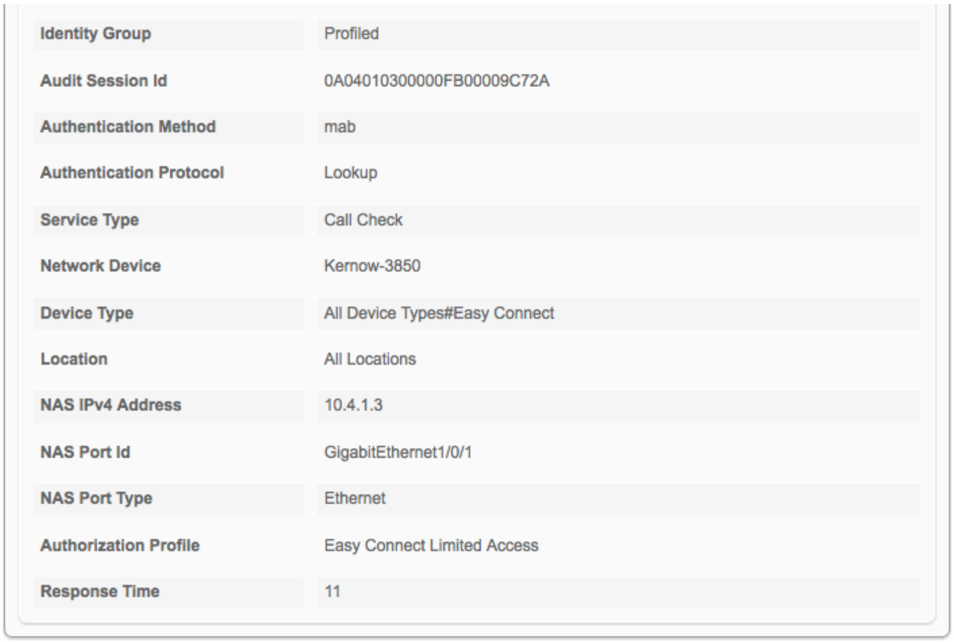
Event	5200 Authentication succeeded
Username	00:0C:29:5E:49:32
Endpoint Id	00:0C:29:5E:49:32 ⊕
Endpoint Profile	VMWare-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> EasyConnect_Unknown
Authorization Result	Easy Connect Limited Access

Authentication Details

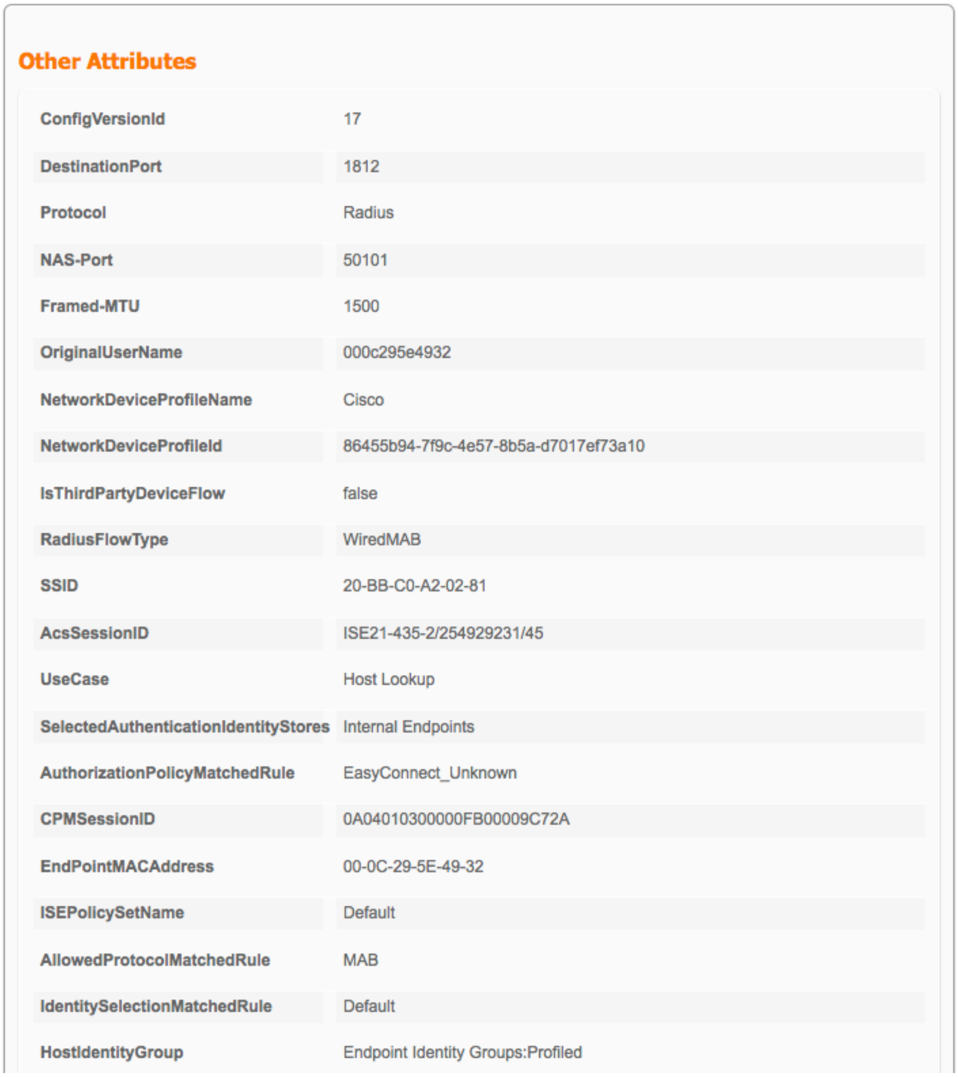
Source Timestamp	2016-06-13 12:01:57.365
Received Timestamp	2016-06-13 12:01:57.396
Policy Server	ISE21-435-2
Event	5200 Authentication succeeded
Username	00:0C:29:5E:49:32
User Type	Host
Endpoint Id	00:0C:29:5E:49:32
Calling Station Id	00-0C-29-5E-49-32
Endpoint Profile	VMWare-Device
IPv4 Address	10.4.1.11
Authentication Identity Store	Internal Endpoints

Steps

```
11001  Received RADIUS Access-Request
11017  RADIUS created a new session
11027  Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049  Evaluating Policy Group
15008  Evaluating Service Selection Policy
15048  Queried PIP - Normalised Radius.RadiusFlowType
15004  Matched rule - MAB
15041  Evaluating Identity Policy
15006  Matched Default Rule
15013  Selected Identity Source - Internal Endpoints
24209  Looking up Endpoint in Internal Endpoints IDStore - 00:0C:29:5E:49:32
24211  Found Endpoint in Internal Endpoints IDStore
22037  Authentication Passed
15036  Evaluating Authorization Policy
15048  Queried PIP - EndPoints.LogicalProfile
15048  Queried PIP - PassiveID.PassiveID_Groups (2 times)
15048  Queried PIP - DEVICE.Device Type
15004  Matched rule - EasyConnect_Unknown
15016  Selected Authorization Profile - Easy Connect Limited Access
11022  Added the dACL specified in the Authorization Profile
11002  Returned RADIUS Access-Accept
```

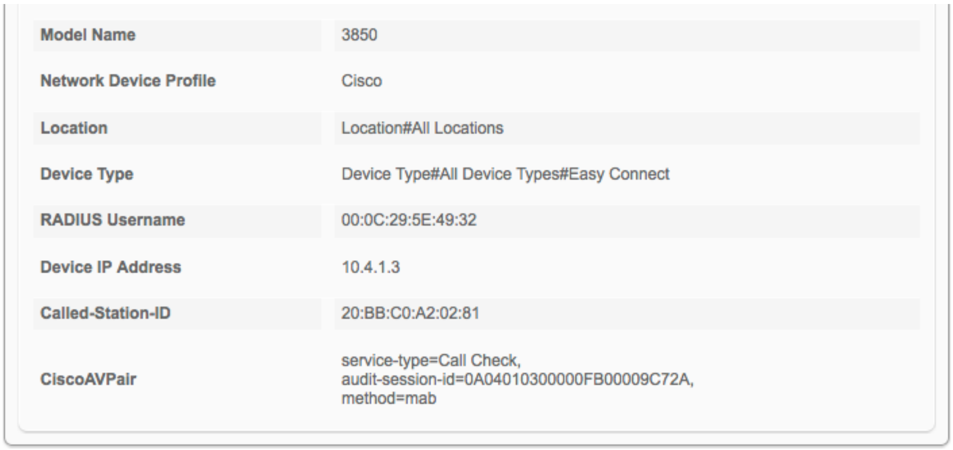


Identity Group	Profiled
Audit Session Id	0A04010300000FB00009C72A
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	Kernow-3850
Device Type	All Device Types#Easy Connect
Location	All Locations
NAS IPv4 Address	10.4.1.3
NAS Port Id	GigabitEthernet1/0/1
NAS Port Type	Ethernet
Authorization Profile	Easy Connect Limited Access
Response Time	11



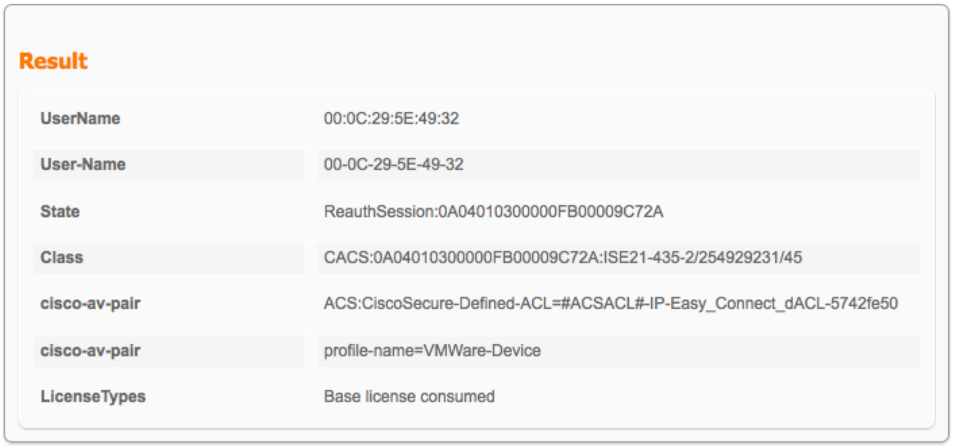
Other Attributes

ConfigVersionId	17
DestinationPort	1812
Protocol	Radius
NAS-Port	50101
Framed-MTU	1500
OriginalUserName	000c295e4932
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	86455b94-7f9c-4e57-8b5a-d7017ef73a10
IsThirdPartyDeviceFlow	false
RadiusFlowType	WiredMAB
SSID	20-BB-C0-A2-02-81
AcsSessionID	ISE21-435-2/254929231/45
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
AuthorizationPolicyMatchedRule	EasyConnect_Unknown
CPMSessionID	0A04010300000FB00009C72A
EndPointMACAddress	00-0C-29-5E-49-32
ISEPolicySetName	Default
AllowedProtocolMatchedRule	MAB
IdentitySelectionMatchedRule	Default
HostIdentityGroup	Endpoint Identity Groups:Profiled



Model Name	3850
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#Easy Connect
RADIUS Username	00:0C:29:5E:49:32
Device IP Address	10.4.1.3
Called-Station-ID	20:BB:C0:A2:02:81

CiscoAVPair	service-type=Call Check,
	audit-session-id=0A04010300000FB00009C72A,
	method=mab

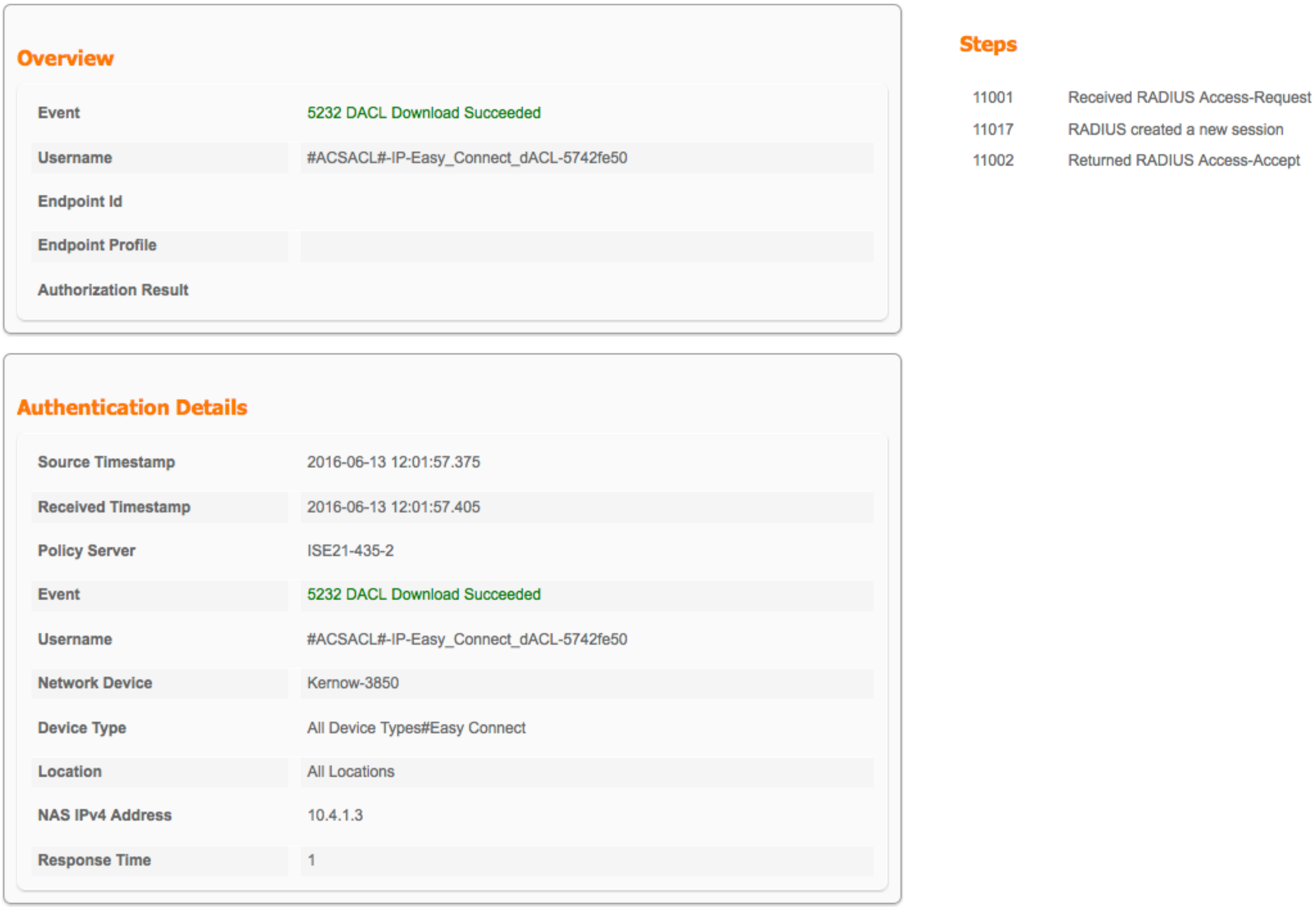


Result

UserName	00:0C:29:5E:49:32
User-Name	00-0C-29-5E-49-32
State	ReauthSession:0A04010300000FB00009C72A
Class	CACS:0A04010300000FB00009C72A:ISE21-435-2/254929231/45
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-Easy_Connect_dACL-5742fe50
cisco-av-pair	profile-name=VMWare-Device
LicenseTypes	Base license consumed

The second entry from the bottom is the downloadable ACL (dACL) sent from ISE to the NAD. This provides the limited access as defined in the Easy Connect Limited Access Authorization Profile.

Details of that Livelog entry:



Overview

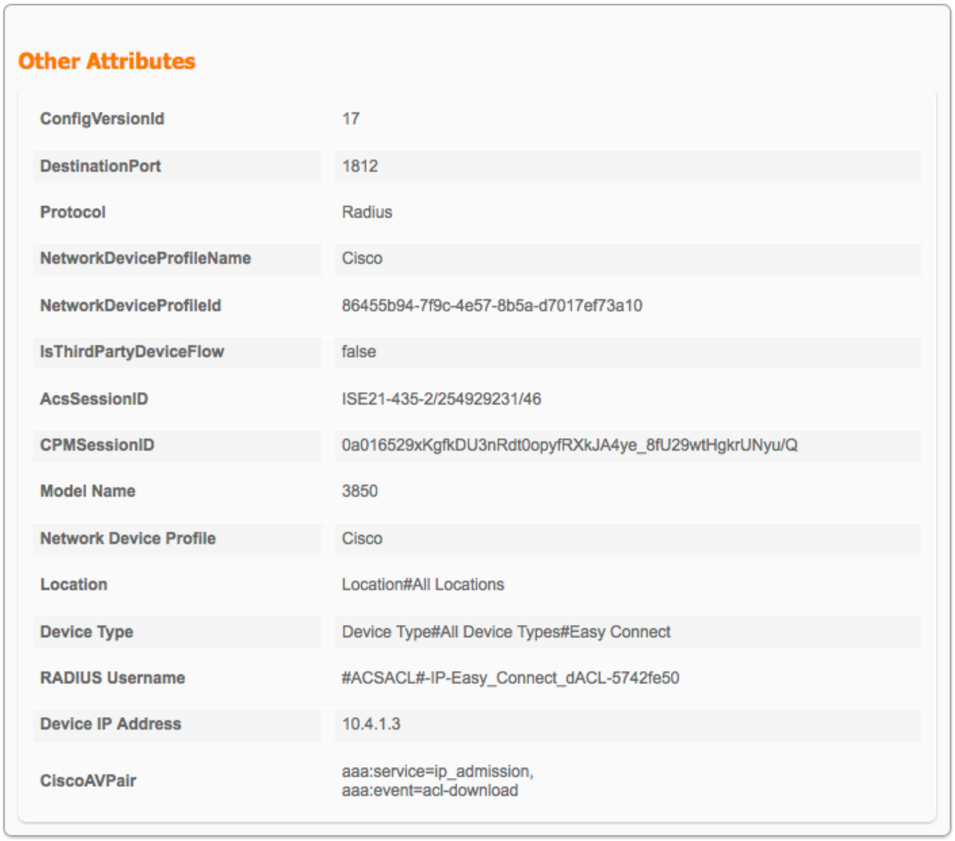
Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-Easy_Connect_dACL-5742fe50
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	2016-06-13 12:01:57.375
Received Timestamp	2016-06-13 12:01:57.405
Policy Server	ISE21-435-2
Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-Easy_Connect_dACL-5742fe50
Network Device	Kernow-3850
Device Type	All Device Types#Easy Connect
Location	All Locations
NAS IPv4 Address	10.4.1.3
Response Time	1

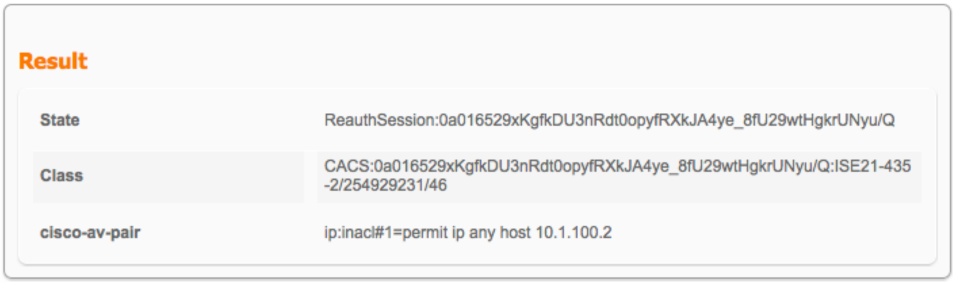
Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11002	Returned RADIUS Access-Accept



Other Attributes

ConfigVersionId	17
DestinationPort	1812
Protocol	Radius
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	86455b94-7f9c-4e57-8b5a-d7017ef73a10
IsThirdPartyDeviceFlow	false
AcsSessionID	ISE21-435-2/254929231/46
CPMSessionID	0a016529xKgfkDU3nRdt0opyfRXkJA4ye_8fU29wtHgkrUNyu/Q
Model Name	3850
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#Easy Connect
RADIUS Username	#ACSACL#-IP-Easy_Connect_dACL-5742fe50
Device IP Address	10.4.1.3
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl-download

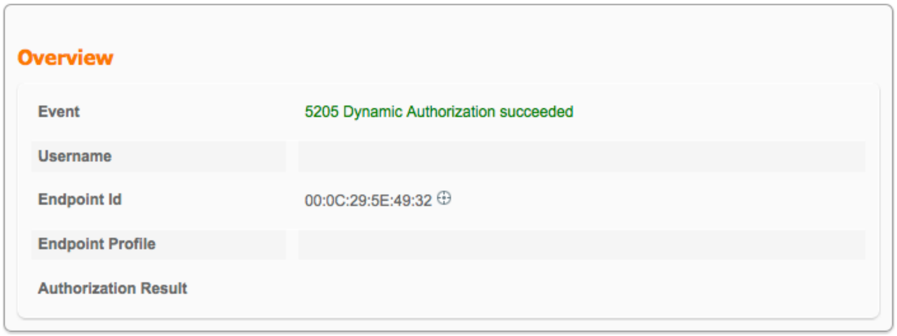


Result

State	ReauthSession:0a016529xKgfkDU3nRdt0opyfRXkJA4ye_8fU29wtHgkrUNyu/Q
Class	CACS:0a016529xKgfkDU3nRdt0opyfRXkJA4ye_8fU29wtHgkrUNyu/Q:ISE21-435-2/254929231/46
cisco-av-pair	ip:inacl#1=permit ip any host 10.1.100.2

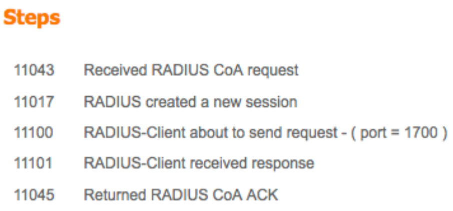
The third entry from the bottom is a RADIUS Change of Authorization (CoA) message back down to the access switch to cause a re-authentication of the session. This is the result of ISE detecting a WMI message (PassiveID) from AD containing the same IP Address plus the username of the user. ISE binds this user information with the information already gleaned from the previous MAB request, updates the session database and sends the CoA (Authorize-Only).

Details of that Livelog entry:



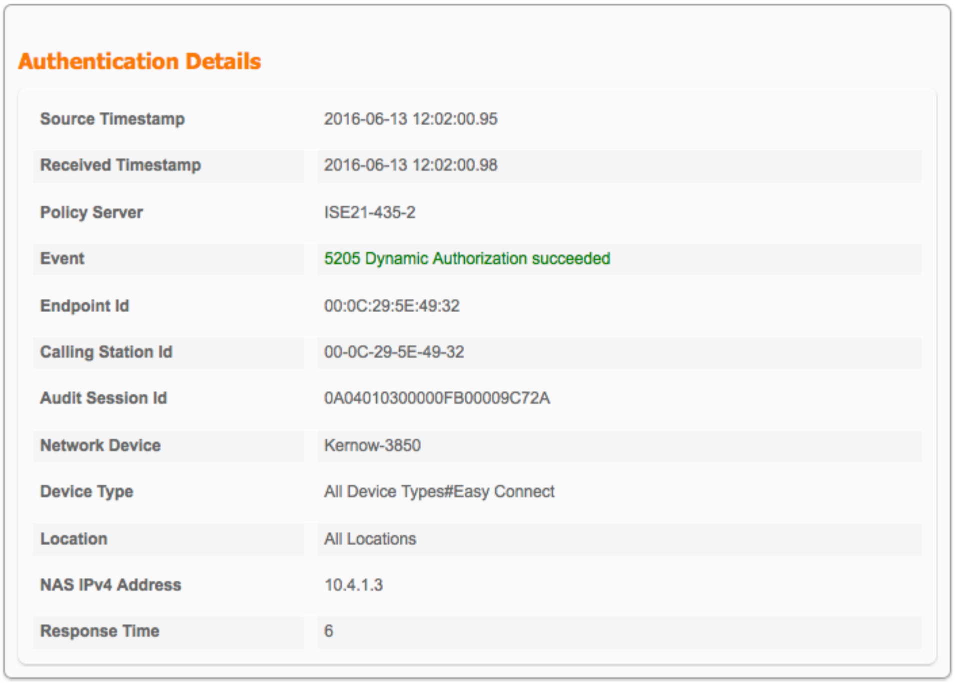
Overview

Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	00:0C:29:5E:49:32
Endpoint Profile	
Authorization Result	



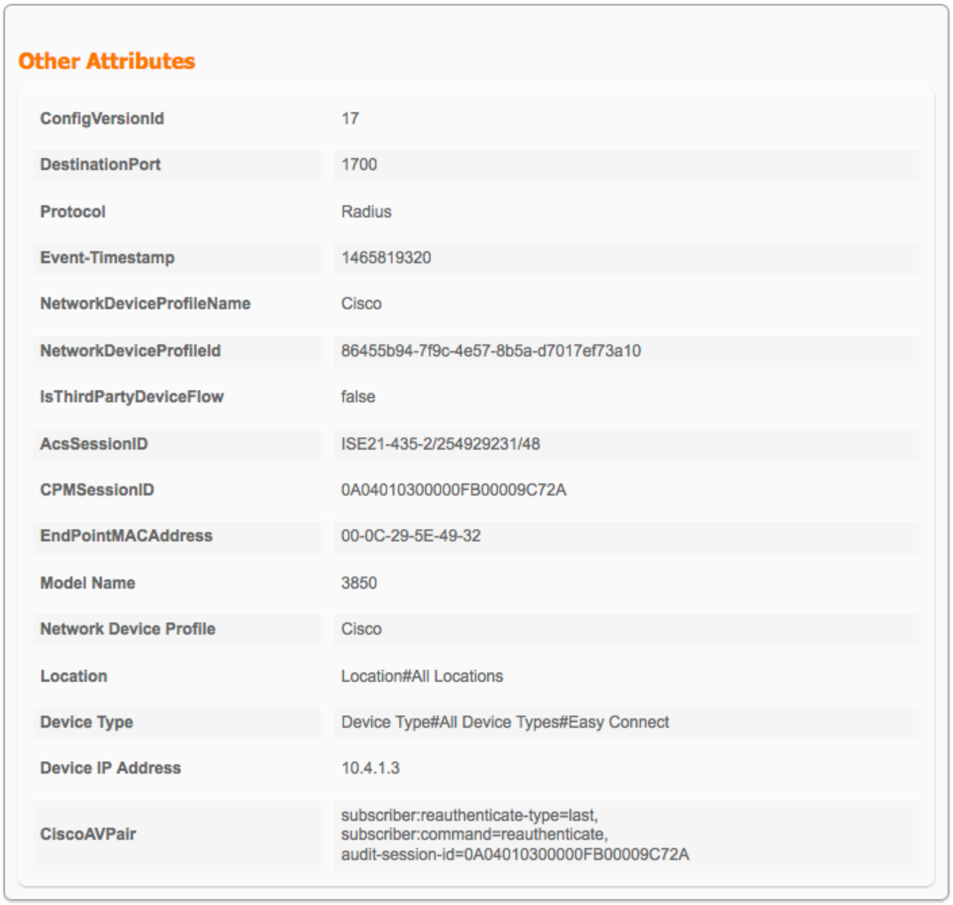
Steps

11043	Received RADIUS CoA request
11017	RADIUS created a new session
11100	RADIUS-Client about to send request - (port = 1700)
11101	RADIUS-Client received response
11045	Returned RADIUS CoA ACK



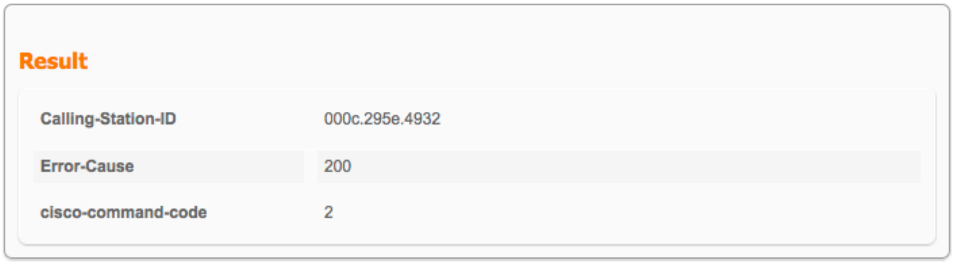
Authentication Details

Source Timestamp	2016-06-13 12:02:00.95
Received Timestamp	2016-06-13 12:02:00.98
Policy Server	ISE21-435-2
Event	5205 Dynamic Authorization succeeded
Endpoint Id	00:0C:29:5E:49:32
Calling Station Id	00-0C-29-5E-49-32
Audit Session Id	0A04010300000FB00009C72A
Network Device	Kernow-3850
Device Type	All Device Types#Easy Connect
Location	All Locations
NAS IPv4 Address	10.4.1.3
Response Time	6



Other Attributes

ConfigVersionId	17
DestinationPort	1700
Protocol	Radius
Event-Timestamp	1465819320
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	86455b94-7f9c-4e57-8b5a-d7017ef73a10
IsThirdPartyDeviceFlow	false
AcsSessionID	ISE21-435-2/254929231/48
CPMSessionID	0A04010300000FB00009C72A
EndPointMACAddress	00-0C-29-5E-49-32
Model Name	3850
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#Easy Connect
Device IP Address	10.4.1.3
CiscoAVPair	subscriber:reauthenticate-type=last, subscriber:command=reauthenticate, audit-session-id=0A04010300000FB00009C72A

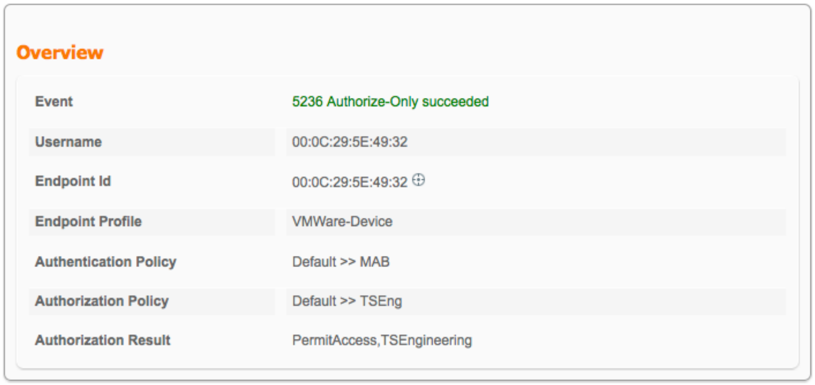


Result

Calling-Station-ID	000c.295e.4932
Error-Cause	200
cisco-command-code	2

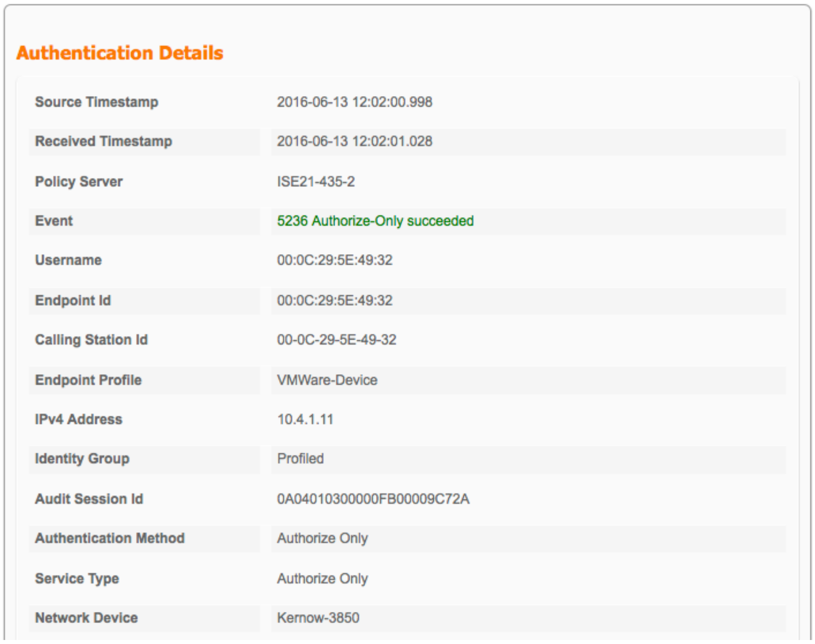
The fourth and fifth entries from the bottom (the fifth showing the session summary) are the result of this re-authentication. A second MAB RADIUS-Request is received by ISE and this time, the user is known. This allows a different authorization rule to be hit. It can be seen the username (PassiveID) is tseng1 and as this is a member of AD group TSEngineering, the TSEng authorization rule is hit assigning the 'PermitAccess' authorization profile and TSEngineering security group tag.

Details of that Livelog entry:



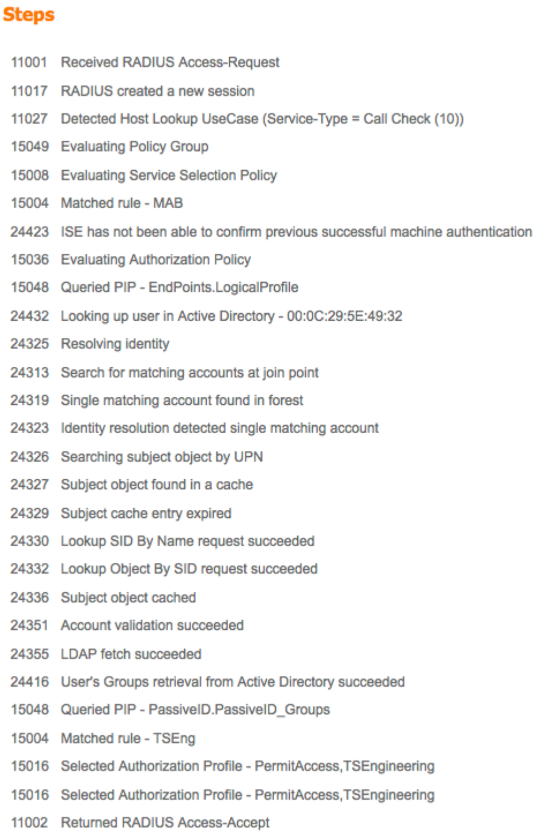
Overview

Event	5236 Authorize-Only succeeded
Username	00:0C:29:5E:49:32
Endpoint Id	00:0C:29:5E:49:32 ⊕
Endpoint Profile	VMWare-Device
Authentication Policy	Default >> MAB
Authorization Policy	Default >> TSEng
Authorization Result	PermitAccess,TSEngineering



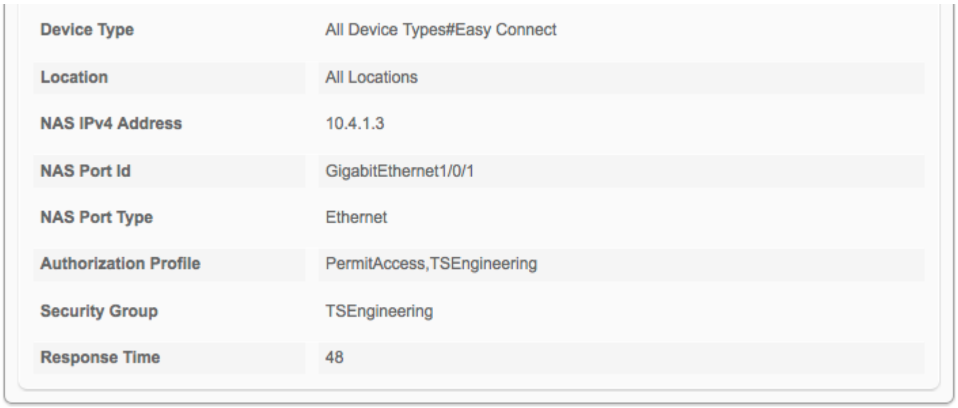
Authentication Details

Source Timestamp	2016-06-13 12:02:00.998
Received Timestamp	2016-06-13 12:02:01.028
Policy Server	ISE21-435-2
Event	5236 Authorize-Only succeeded
Username	00:0C:29:5E:49:32
Endpoint Id	00:0C:29:5E:49:32
Calling Station Id	00-0C-29-5E-49-32
Endpoint Profile	VMWare-Device
IPv4 Address	10.4.1.11
Identity Group	Profiled
Audit Session Id	0A04010300000FB00009C72A
Authentication Method	Authorize Only
Service Type	Authorize Only
Network Device	Kernow-3850

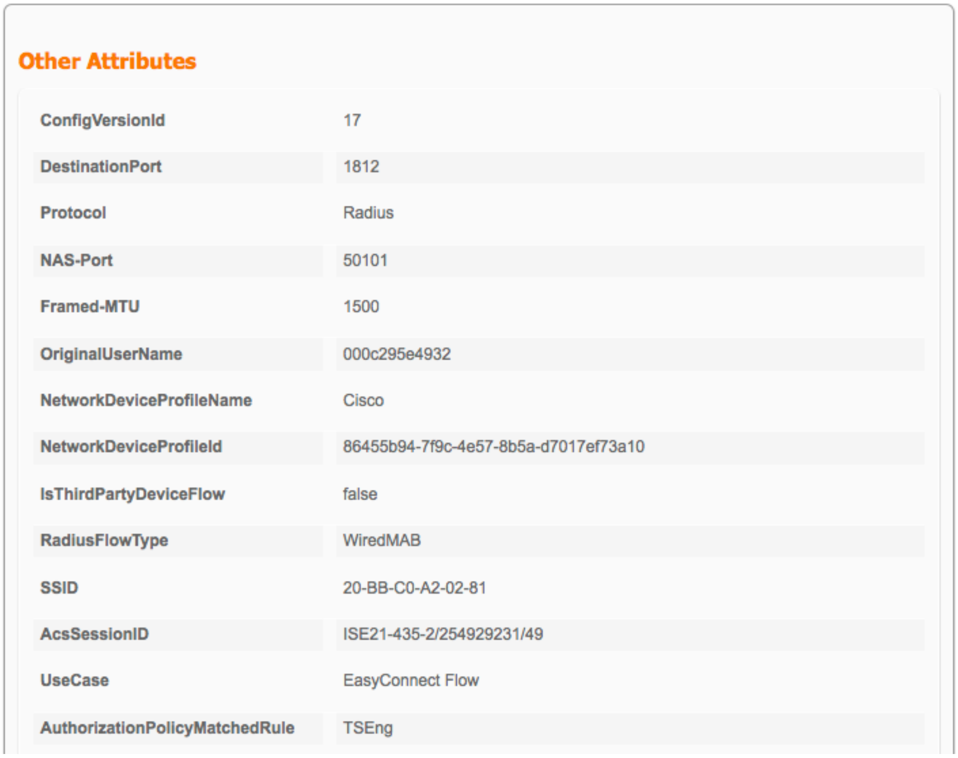


Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15004	Matched rule - MAB
24423	ISE has not been able to confirm previous successful machine authentication
15036	Evaluating Authorization Policy
15048	Queried PIP - EndPoints.LogicalProfile
24432	Looking up user in Active Directory - 00:0C:29:5E:49:32
24325	Resolving identity
24313	Search for matching accounts at join point
24319	Single matching account found in forest
24323	Identity resolution detected single matching account
24326	Searching subject object by UPN
24327	Subject object found in a cache
24329	Subject cache entry expired
24330	Lookup SID By Name request succeeded
24332	Lookup Object By SID request succeeded
24336	Subject object cached
24351	Account validation succeeded
24355	LDAP fetch succeeded
24416	User's Groups retrieval from Active Directory succeeded
15048	Queried PIP - PassiveID.PassiveID_Groups
15004	Matched rule - TSEng
15016	Selected Authorization Profile - PermitAccess,TSEngineering
15016	Selected Authorization Profile - PermitAccess,TSEngineering
11002	Returned RADIUS Access-Accept

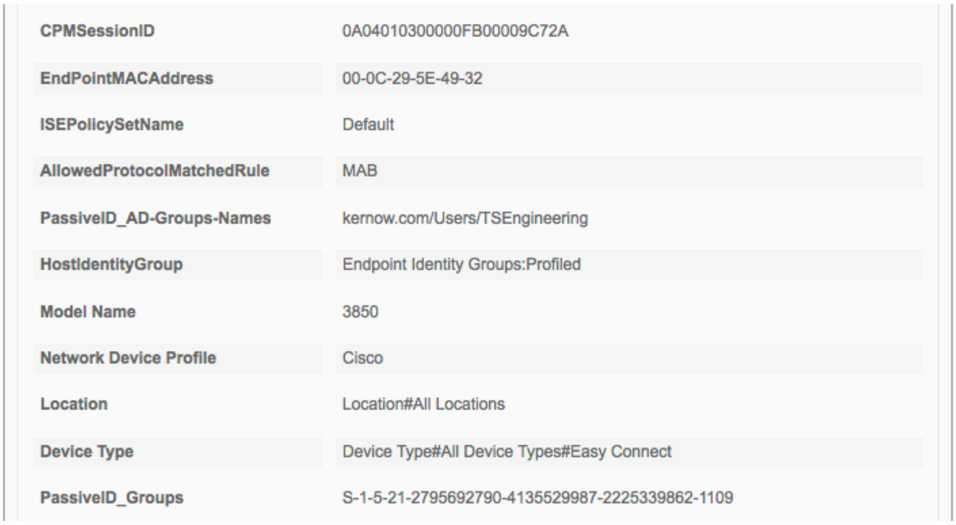


Device Type	All Device Types#Easy Connect
Location	All Locations
NAS IPv4 Address	10.4.1.3
NAS Port Id	GigabitEthernet1/0/1
NAS Port Type	Ethernet
Authorization Profile	PermitAccess,TSEngineering
Security Group	TSEngineering
Response Time	48

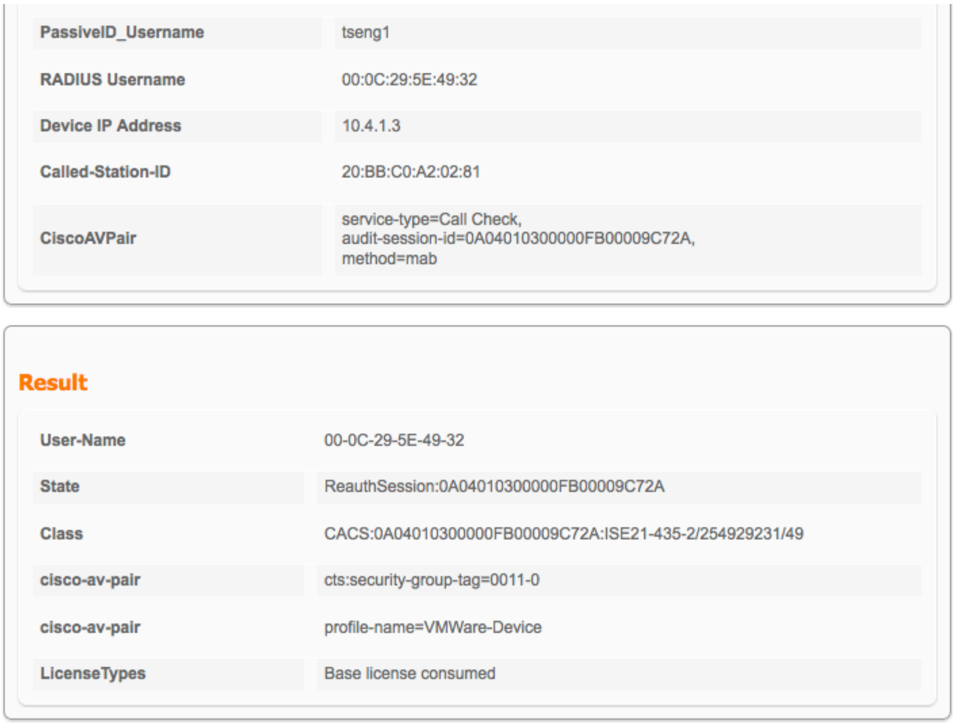


Other Attributes

ConfigVersionId	17
DestinationPort	1812
Protocol	Radius
NAS-Port	50101
Framed-MTU	1500
OriginalUserName	000c295e4932
NetworkDeviceProfileName	Cisco
NetworkDeviceProfileId	86455b94-7f9c-4e57-8b5a-d7017ef73a10
IsThirdPartyDeviceFlow	false
RadiusFlowType	WiredMAB
SSID	20-BB-C0-A2-02-81
AcsSessionID	ISE21-435-2/254929231/49
UseCase	EasyConnect Flow
AuthorizationPolicyMatchedRule	TSEng



CPMSessionID	0A04010300000FB00009C72A
EndPointMACAddress	00-0C-29-5E-49-32
ISEPolicySetName	Default
AllowedProtocolMatchedRule	MAB
PassiveID_AD-Groups-Names	kernow.com/Users/TSEngineering
HostIdentityGroup	Endpoint Identity Groups:Profiled
Model Name	3850
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types#Easy Connect
PassiveID_Groups	S-1-5-21-2795692790-4135529987-2225339862-1109



PassiveID_Username	tseng1
RADIUS Username	00:0C:29:5E:49:32
Device IP Address	10.4.1.3
Called-Station-ID	20:BB:C0:A2:02:81

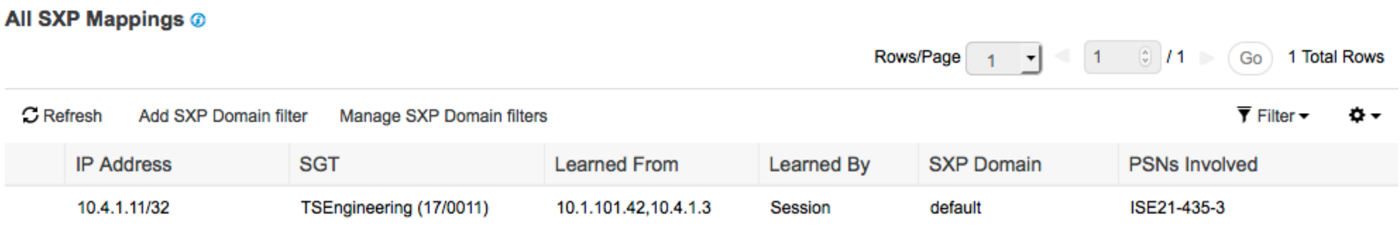
CiscoAVPair	service-type=Call Check,
	audit-session-id=0A04010300000FB00009C72A,
	method=mab

Result

User-Name	00-0C-29-5E-49-32
State	ReauthSession:0A04010300000FB00009C72A
Class	CACS:0A04010300000FB00009C72A:ISE21-435-2/254929231/49
cisco-av-pair	cts:security-group-tag=0011-0
cisco-av-pair	profile-name=VMWare-Device
LicenseTypes	Base license consumed

IP-to-SGT Mappings and SXP Forwarding

Once full authentication/authorization has completed and a SGT assigned, ISE stores that SGT along with the IP address into the SXP Mappings table. Use Work Centers > TrustSec > SXP > All SXP Mappings to check the table:



All SXP Mappings

Rows/Page 1 | 1 /1 | Go | 1 Total Rows

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
10.4.1.11/32	TSEngineering (17/0011)	10.1.101.42,10.4.1.3	Session	default	ISE21-435-3

If there are SXP connections up and operational with ISE as a Speaker and network devices as Listeners, then once in the SXP Mappings table, the IP-to-SGT mapping will be forwarded to those network devices. Check the network devices for those mappings:

```
Prompt-3850#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address            SGT     Source
============================================
10.4.1.11             17      SXP

IP-SGT Active Bindings Summary
============================================
Total number of SXP      bindings = 1
Total number of active   bindings = 1
```

Once the IP-to-SGT mappings are resident on the network devices, TrustSec role-based enforcement can be utilized for traffic sourced from or destined to the IP address of the Easy Connect client/user.

Debugging PassiveID and SXP in ISE

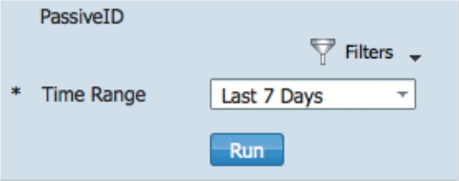
There are individual log files for both PassiveID and SXP within ISE.

In ISE, navigate to Operations > Troubleshoot > Download Logs and select the ISE node. Select the ‘Debug Logs’ tab. For PassiveID logs, scroll down to the Debug Log Type ‘PassiveID’ and for SXP, scroll down to the Debug Log Type ‘sxp’.

Reports

PassiveID reports can be displayed by navigating to Operations > Reports > ISE Reports > Endpoints and Users > PassiveID.

Set the time range and/or Filters and run the report:

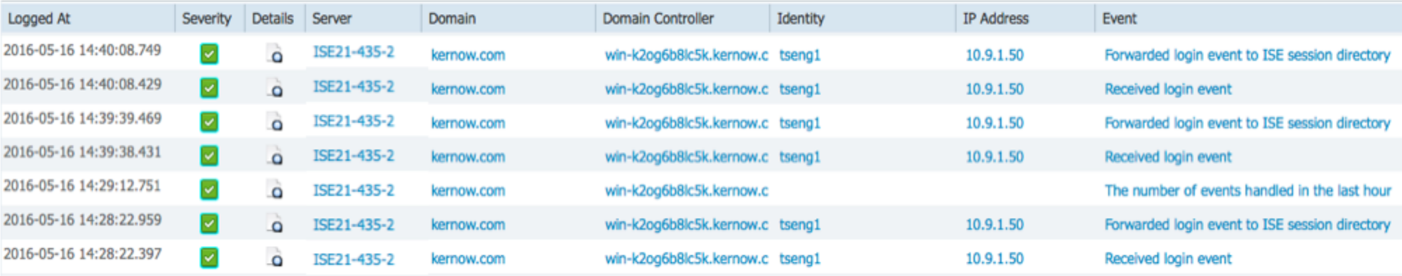


PassiveID

Filters

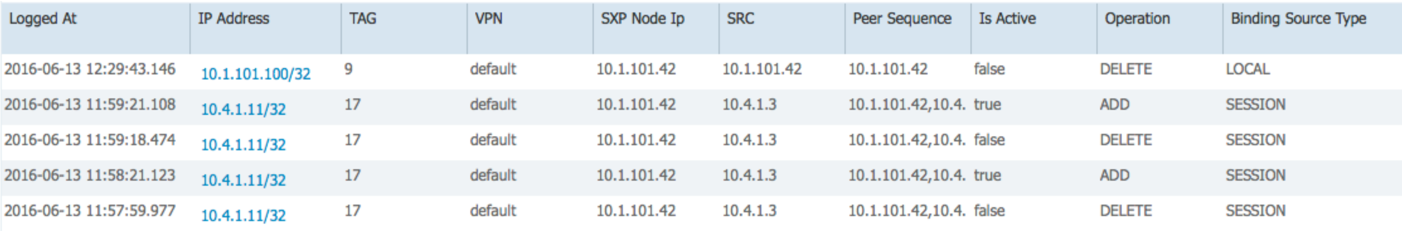
* Time Range: Last 7 Days

An extract of an example report is shown here:



Logged At	Severity	Details	Server	Domain	Domain Controller	Identity	IP Address	Event
2016-05-16 14:40:08.749	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Forwarded login event to ISE session directory
2016-05-16 14:40:08.429	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Received login event
2016-05-16 14:39:39.469	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Forwarded login event to ISE session directory
2016-05-16 14:39:38.431	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Received login event
2016-05-16 14:29:12.751	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c			The number of events handled in the last hour
2016-05-16 14:28:22.959	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Forwarded login event to ISE session directory
2016-05-16 14:28:22.397	✓	🔍	ISE21-435-2	kernow.com	win-k2og6b8lc5k.kernow.c	tseng1	10.9.1.50	Received login event

There are also a number of TrustSec reports that can be displayed under Operations > Reports > ISE Reports > TrustSec. Below is an example of the SXP Binding report:



Logged At	IP Address	TAG	VPN	SXP Node Ip	SRC	Peer Sequence	Is Active	Operation	Binding Source Type
2016-06-13 12:29:43.146	10.1.101.100/32	9	default	10.1.101.42	10.1.101.42	10.1.101.42	false	DELETE	LOCAL
2016-06-13 11:59:21.108	10.4.1.11/32	17	default	10.1.101.42	10.4.1.3	10.1.101.42,10.4.	true	ADD	SESSION
2016-06-13 11:59:18.474	10.4.1.11/32	17	default	10.1.101.42	10.4.1.3	10.1.101.42,10.4.	false	DELETE	SESSION
2016-06-13 11:58:21.123	10.4.1.11/32	17	default	10.1.101.42	10.4.1.3	10.1.101.42,10.4.	true	ADD	SESSION
2016-06-13 11:57:59.977	10.4.1.11/32	17	default	10.1.101.42	10.4.1.3	10.1.101.42,10.4.	false	DELETE	SESSION