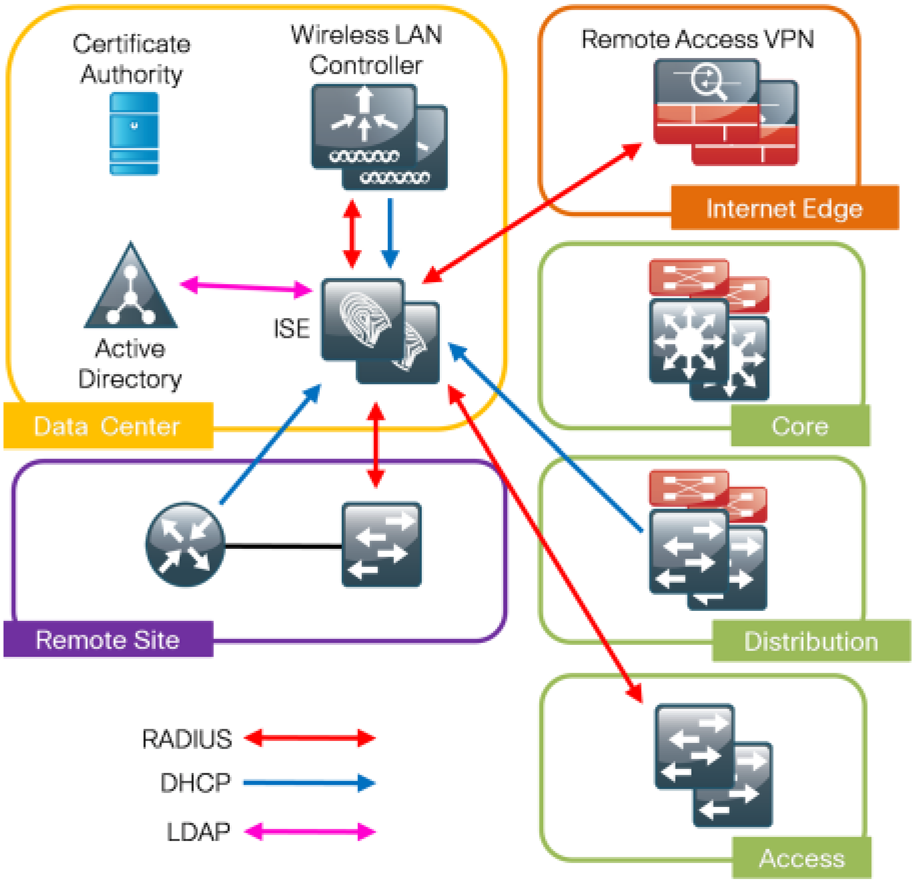
Windows Integrated 802.1x AAA Using Sx300/500 Switch and ISE and AD

Jie Yuan jieyuan@cisco.com

Jiang Albert jialbert@cisco.com

Introduction



Sx300/500 series switches can team together with Cisco ISE (Identity Service Engine) and Windows AD server to provide integrated 802.1x AAA (authentication/authorization/accounting) using Windows domain username/password for end user device.

Authentication

Users login to device using Windows domain username/password and Windows 802.1x client automatically use Windows username/password to authenticate user.

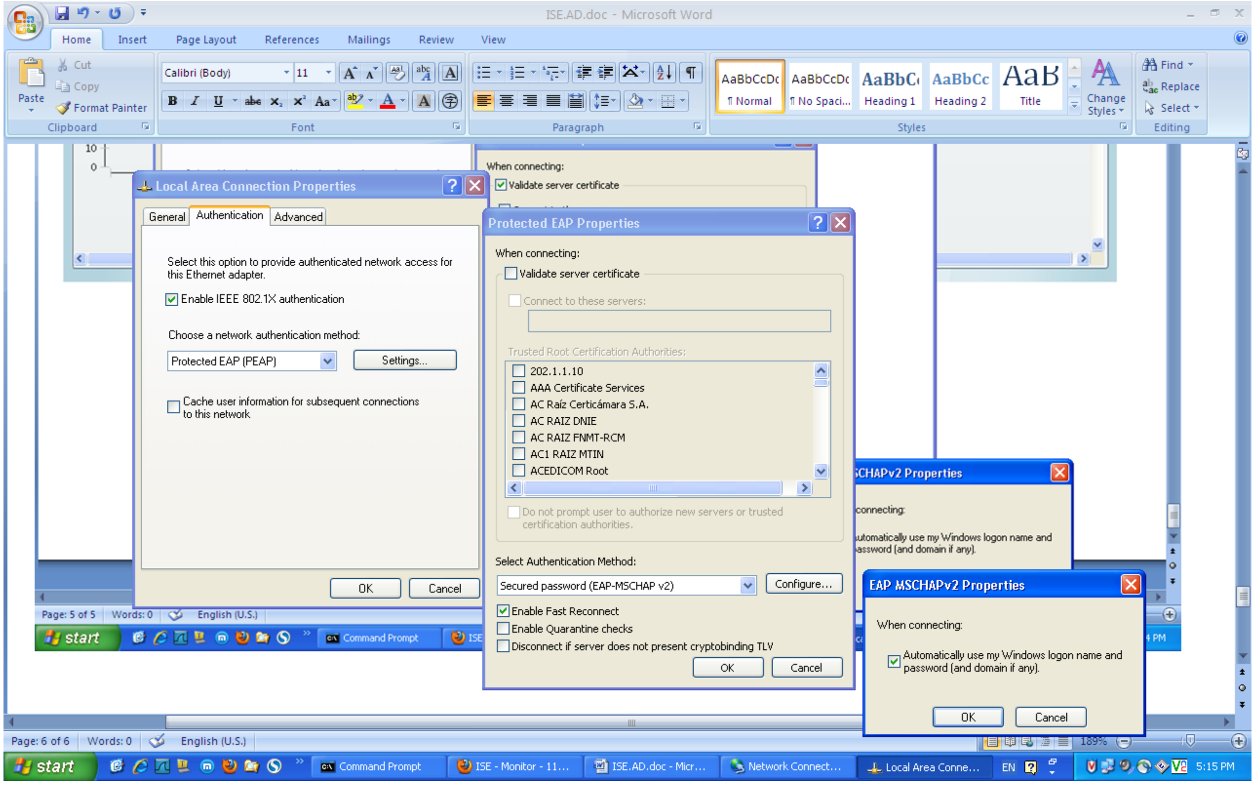
Authorization

User access port is in an un-authorized VLAN (VLAN 999 e.g.) before authentication. After user is authenticated, access port is assigned to authorized VLAN (VLAN 10 e.g.).

Accounting

Every user session duration is logged in AAA server via Radius message.

Windows 802.1x Client Configuration



Local Area Connection Properties

General | Authentication | Advanced

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Protected EAP (PEAP) — Settings...

☐ Cache user information for subsequent connections to this network

OK | Cancel

Protected EAP Properties

When connecting:

☐ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

☐ 202.1.1.10
☐ AAA Certificate Services
☐ AC Raíz Certicámara S.A.
☐ AC RAIZ DNIE
☐ AC RAIZ FNMT-RCM
☐ AC1 RAIZ MTIN
☐ ACEDICOM Root

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2) — Configure...

☑ Enable Fast Reconnect
☐ Enable Quarantine checks
☐ Disconnect if server does not present cryptobinding TLV

OK | Cancel

EAP MSCHAPv2 Properties

When connecting:

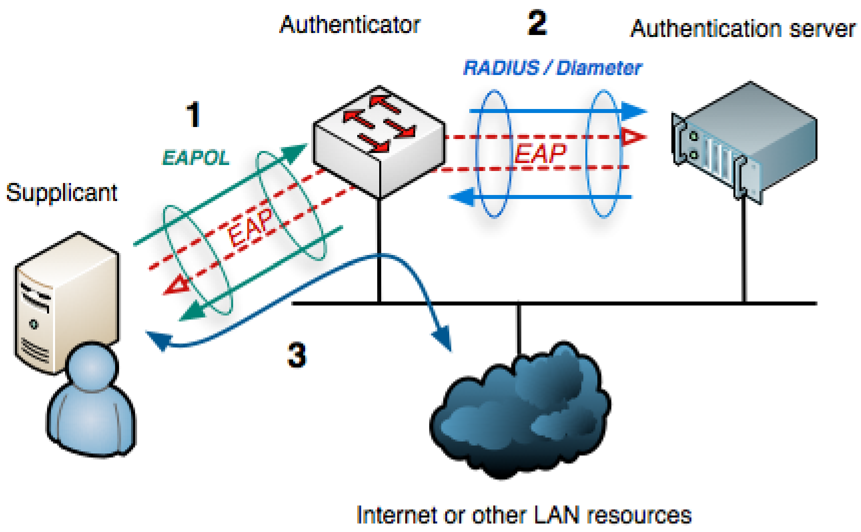
☑ Automatically use my Windows logon name and password (and domain if any).

OK | Cancel

Sx300/500 Switch Configuration

[Enable 802.1x]

```
dot1x system-auth-control
```



Supplicant is user, authenticator is switch, and authentication server is Radius server (ISE server).

[Radius Server and password]

```
encrypted radius-server host 111.111.111.188 key cisco
```

[802.1x authentication via Radius Server]

```
aaa authentication dot1x default radius
```

[802.1x accounting]

```
aaa accounting dot1x
```

If accounting is enabled, switch will send “start” messages to Radius server when user login, and “stop” message when user log off. “Stop” message also includes session time of supplicant.

If a new supplicant replaces an old supplicant (even if port is still in authorized state), switch sends a “stop” message for old supplicant and “start” for new supplicant.

In multiple session mode (explained later), switch sends “start/stop” message for each supplicant.

In multiple host mode, switch sends “start/stop” message only for authenticated supplicant.

If port is force-authorized, switch does not send “start/stop” message.

Switch does not send “start/stop” message for guest VLAN and unauthenticated VLAN.

[Interface]

interface fastethernet1/2/3

[Enable 802.1x for port]

dot1x port-control [auto|force-authorized|force-unauthorized] [time-range *time-range-name]*

auto: enable 802.1x

force-authorized: put port into authorized state without authentication.

Force-unauthorized: put port into un-authorized state ignoring any user authentication.

Default is force-authorized, use “auto” to enable 802.1x authentication.

[802.1x host mode]

dot1x host-mode [multi-sessions| multi-host | single-host]

Multi-session: each host (source MAC) must be authenticated to grant network access.

Multi-host: one host authenticated for all hosts to access network.

Single-host: only one host can be authenticated to access network.

Port-security cannot be enabled on port with single-host or multiple session mode.

[802.1x reauthentication]

Either in global configuration mode

dot1x re-authenticate [interface-id]

If interface-id is omitted, apply to all ports.

Or in interface configuration mode

dot1x reauthentication

These commands enable periodic 802.1x re-authentication, the interval is configured via

```
dot1x timeout reauth-period seconds
```

default 3600s

[Authorization dynamic VLAN assignment]

```
dot1x radius-attributes vlan [reject | vlan-id]
```

After authentication, Radius server will pass authorized VLAN via TLV to switch. Switch will dynamically assign this VLAN to user access port.

Reject: if Radius server does not provide VLAN information, supplicant is rejected.

Vlan-id: if Radius server does not provide VLAN information, supplicant is accepted and the configured vlan is assigned to the port.

[Guest VLAN]

If the guest vlan is defined and enabled for port, the port is in guest vlan when the port is unauthorized and leaves it when the port becomes authorized. To be able to join or leave guest vlan, the port should not be a static member of the guest VLAN.

```
interface vlan 300
        dot1x guest-vlan
interface gi1/0
        dot1x guest-vlan enable
```

[MAC authentication]

Authenticate user by MAC, switch uses supplicant MAC as username/password to authentication user. Radius server should recognized user by MAC as name and password.

Guest vlan must be enabled when MAC authentication is enabled.

Static MAC cannot be authorized. Do not change an authenticated MAC to static MAC.

Do not delete authenticated MAC.

Reauthentication must be enabled.

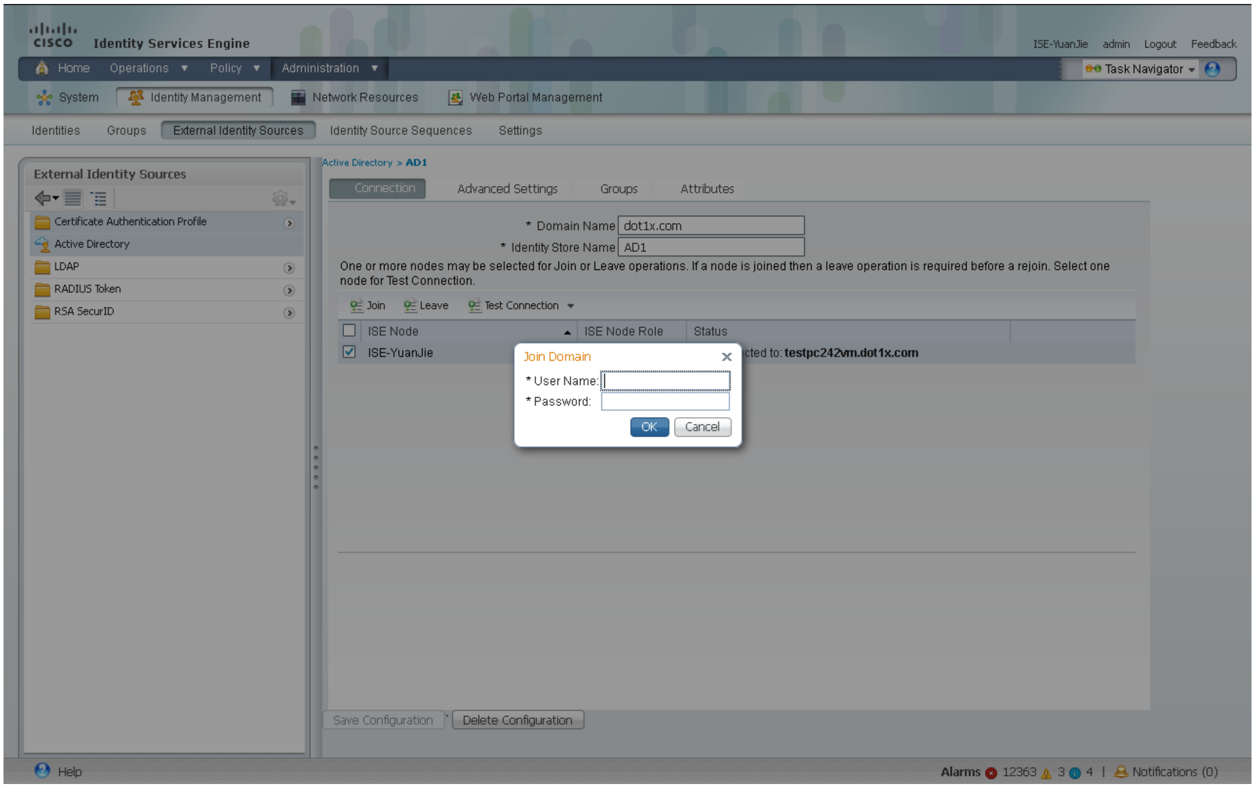
```
Interface gi1/0
        do1x mac-authentication [mac-only| mac-and-802.1x]
```

mac-only: ignore 802.1x

mac-and-802.1x: both mac and 802.1x

ISE Configuration

Connect to Windows AD as external identity source using domain administrator



* Domain Name: dot1x.com

* Identity Store Name: AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

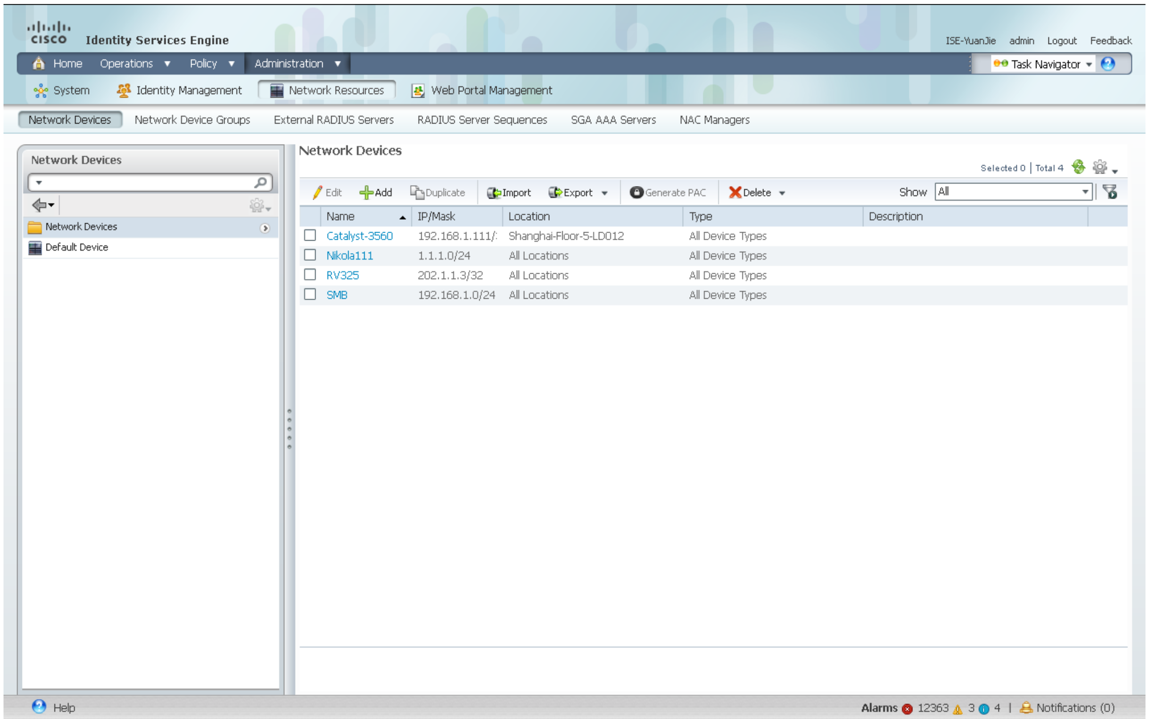
□	ISE Node	ISE Node Role	Status
☑	ISE-YuanJie		cted to: **testpc242vm.dot1x.com**

Join Domain

* User Name:

* Password:

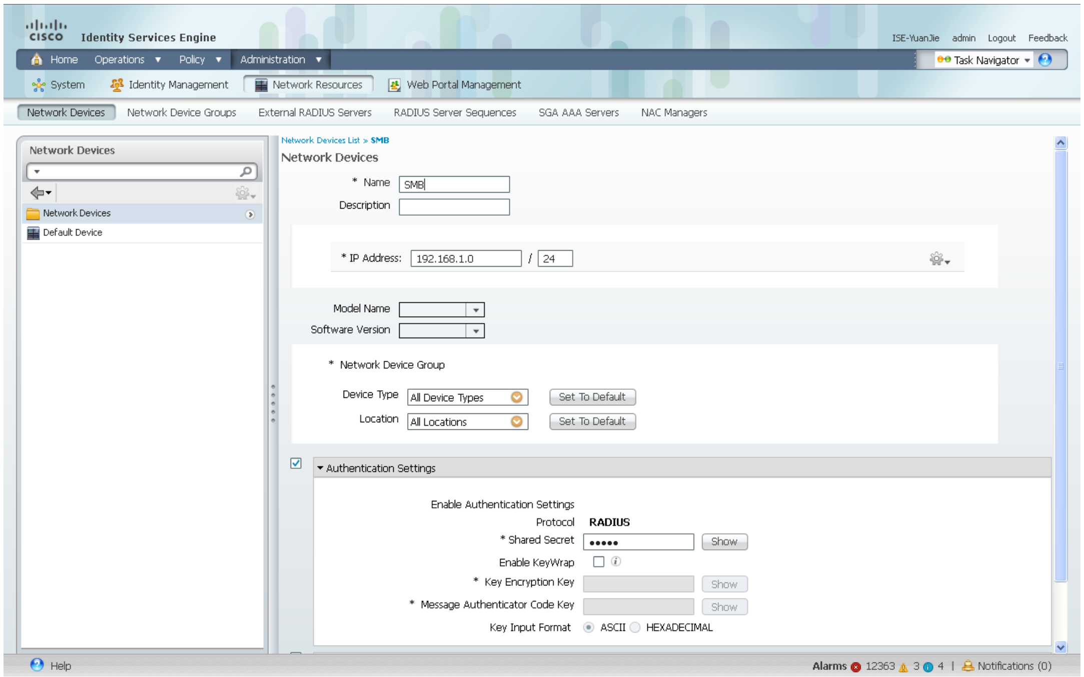
Radius connection with Switch:


Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Web Portal Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices
Network Devices
Default Device
Edit Add Duplicate Import Export ▾ Generate PAC Delete ▾
Show All
Help
Alarms 12363 3 4 | Notifications (0)

Network Devices

Selected 0 | Total 4

	Name	IP/Mask	Location	Type	Description
□	Catalyst-3560	192.168.1.111/:	Shanghai-Floor-5-LD012	All Device Types	
□	Nikola111	1.1.1.0/24	All Locations	All Device Types	
□	RV325	202.1.1.3/32	All Locations	All Device Types	
□	SMB	192.168.1.0/24	All Locations	All Device Types	


Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Web Portal Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices
Network Devices
Default Device
Set To Default
Set To Default
Show
Show
Show
Help
Alarms 12363 3 4 | Notifications (0)

Network Devices List > SMB

Network Devices

* Name SMB

Description

* IP Address: 192.168.1.0 / 24

Model Name

Software Version

* Network Device Group

Device Type All Device Types

Location All Locations

☑ Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret •••••

Enable KeyWrap □

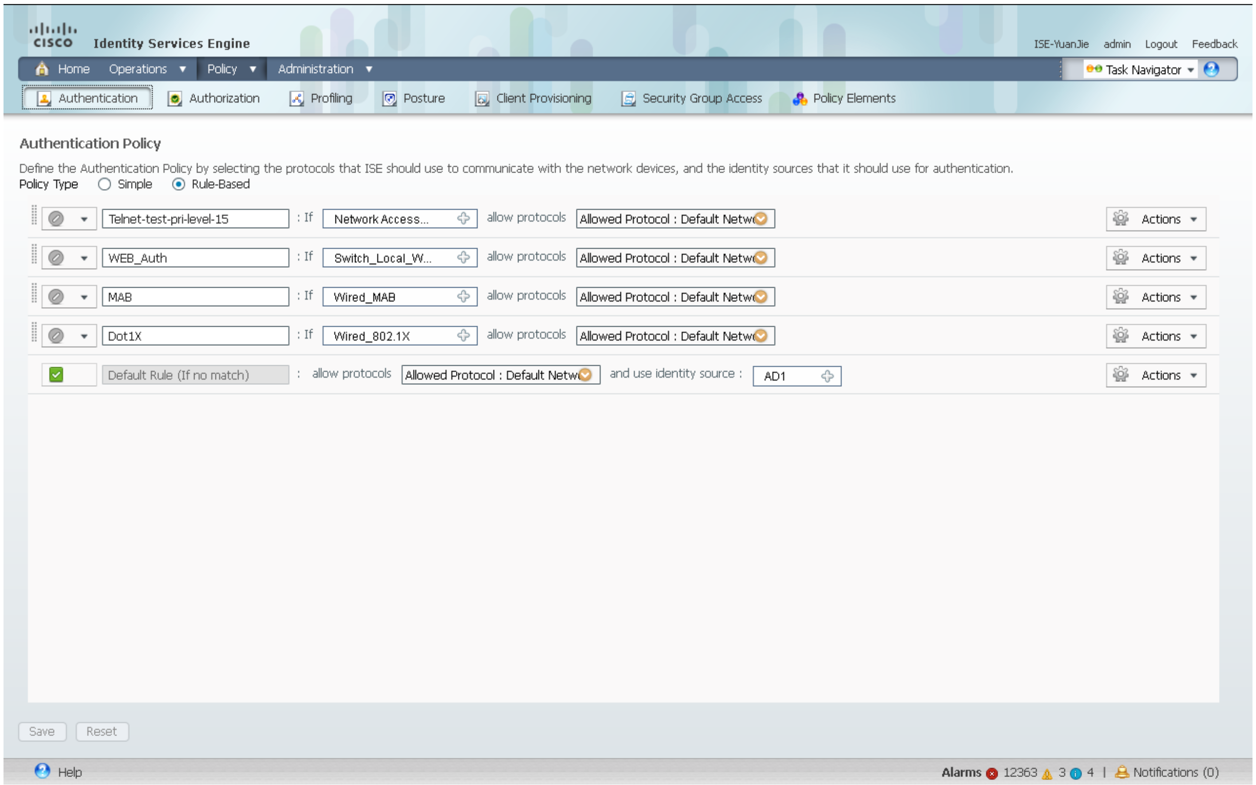
* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

Authentication

Policy: default network connection using Windows AD as external identity source



Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator ▼
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements

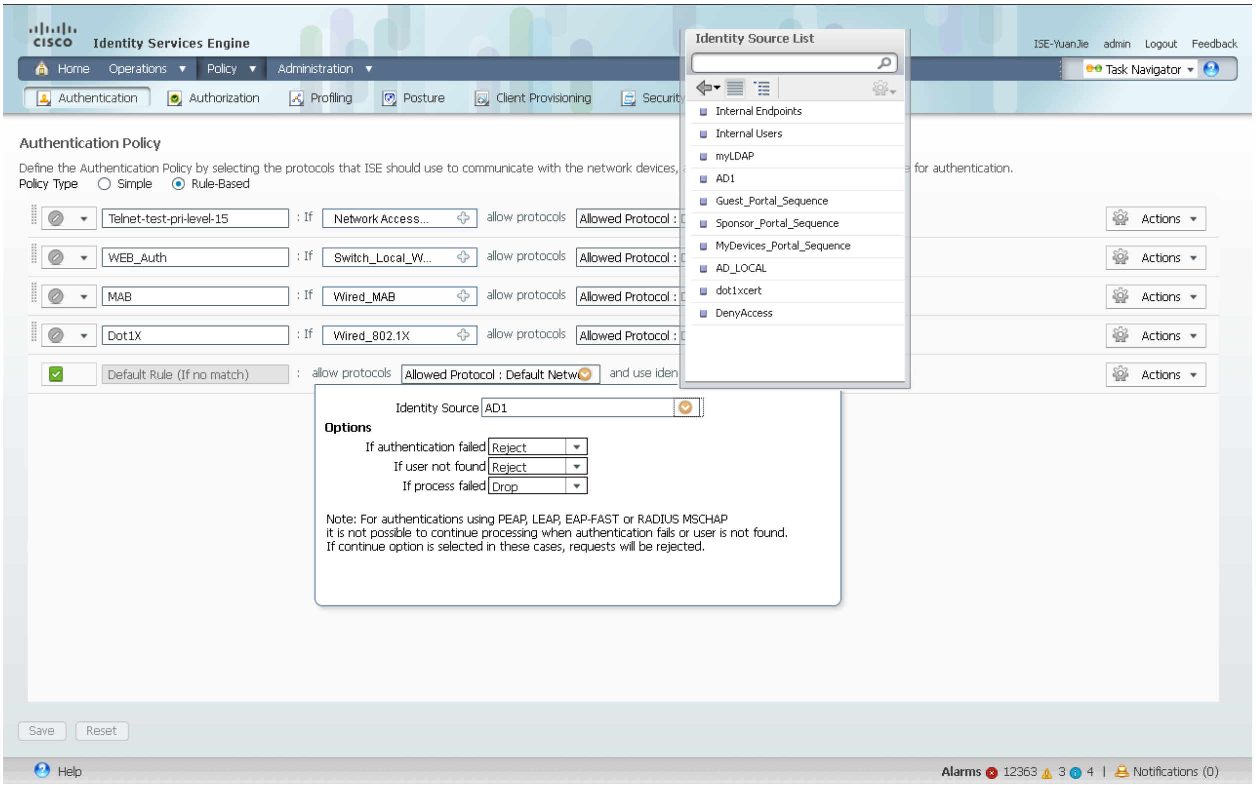
Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

Telnet-test-pri-level-15	: If	Network Access...	allow protocols	Allowed Protocol : Default Netw	Actions ▼
WEB_Auth	: If	Switch_Local_W...	allow protocols	Allowed Protocol : Default Netw	Actions ▼
MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netw	Actions ▼
Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : Default Netw	Actions ▼
Default Rule (If no match)	:	allow protocols Allowed Protocol : Default Netw	and use identity source :	AD1	Actions ▼

Save Reset
Help
Alarms 12363 3 4 | Notifications (0)



Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator ▼
Authentication Authorization Profiling Posture Client Provisioning Securit

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, for authentication.

Policy Type ○ Simple ● Rule-Based

Telnet-test-pri-level-15	: If	Network Access...	allow protocols	Allowed Protocol :	Actions ▼
WEB_Auth	: If	Switch_Local_W...	allow protocols	Allowed Protocol :	Actions ▼
MAB	: If	Wired_MAB	allow protocols	Allowed Protocol :	Actions ▼
Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol :	Actions ▼
Default Rule (If no match)	:	allow protocols Allowed Protocol : Default Netw	and use iden		Actions ▼

Identity Source List

- Internal Endpoints
- Internal Users
- myLDAP
- AD1
- Guest_Portal_Sequence
- Sponsor_Portal_Sequence
- MyDevices_Portal_Sequence
- AD_LOCAL
- dot1xcert
- DenyAccess

Identity Source AD1

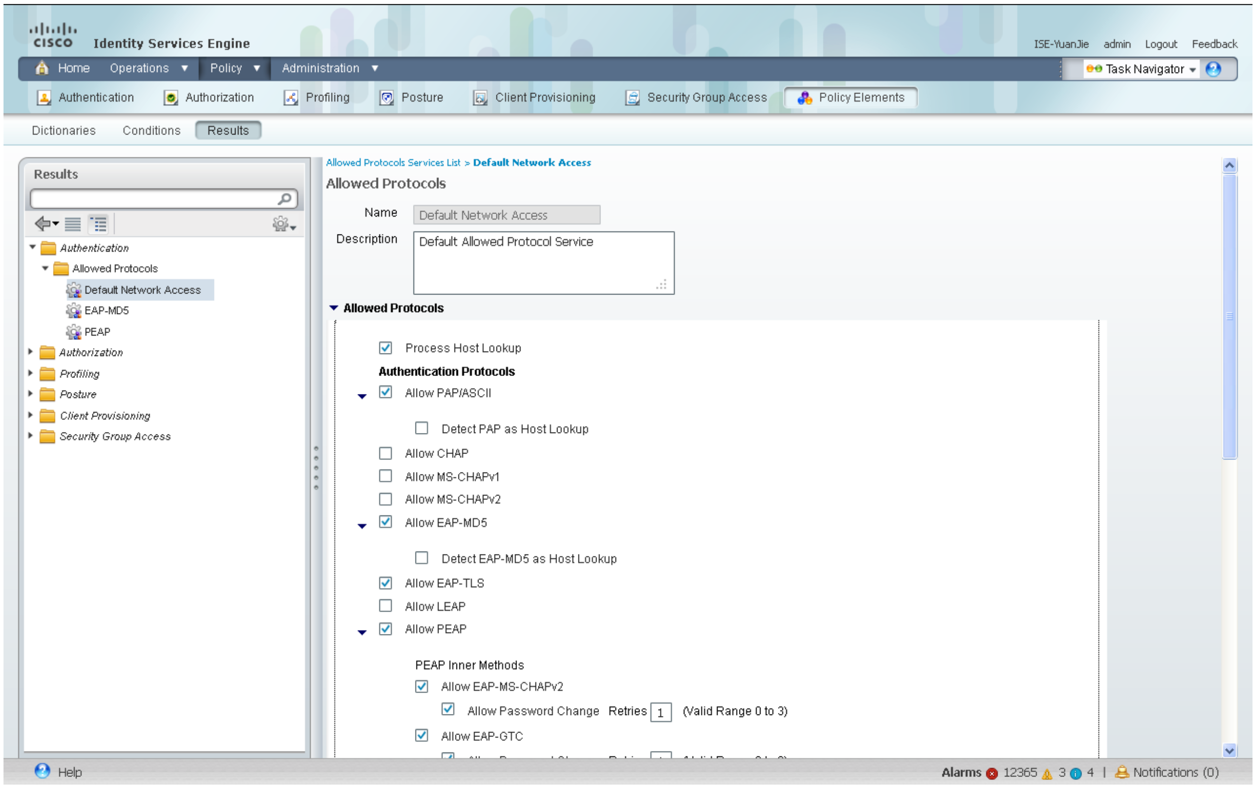
Options

If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP
it is not possible to continue processing when authentication fails or user is not found.
If continue option is selected in these cases, requests will be rejected.


Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Allowed Protocols
Default Network Access
EAP-MD5
PEAP
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Help
Alarms 12365 3 4 | Notifications (0)

Allowed Protocols Services List > **Default Network Access**

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

☐ Detect PAP as Host Lookup

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☑ Allow EAP-MD5

☐ Detect EAP-MD5 as Host Lookup

☑ Allow EAP-TLS

☐ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

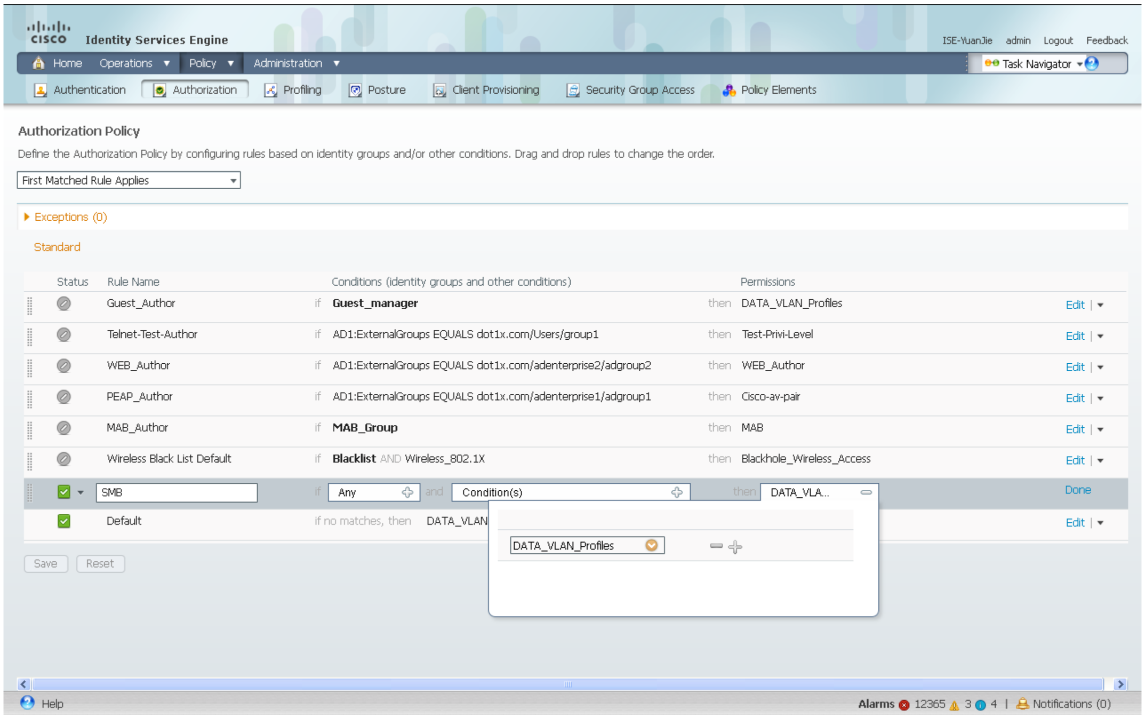
☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-GTC

Authorization

policy: assign user VLAN after authentication


Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Save Reset
Help
Alarms 12365 3 4 | Notifications (0)

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.

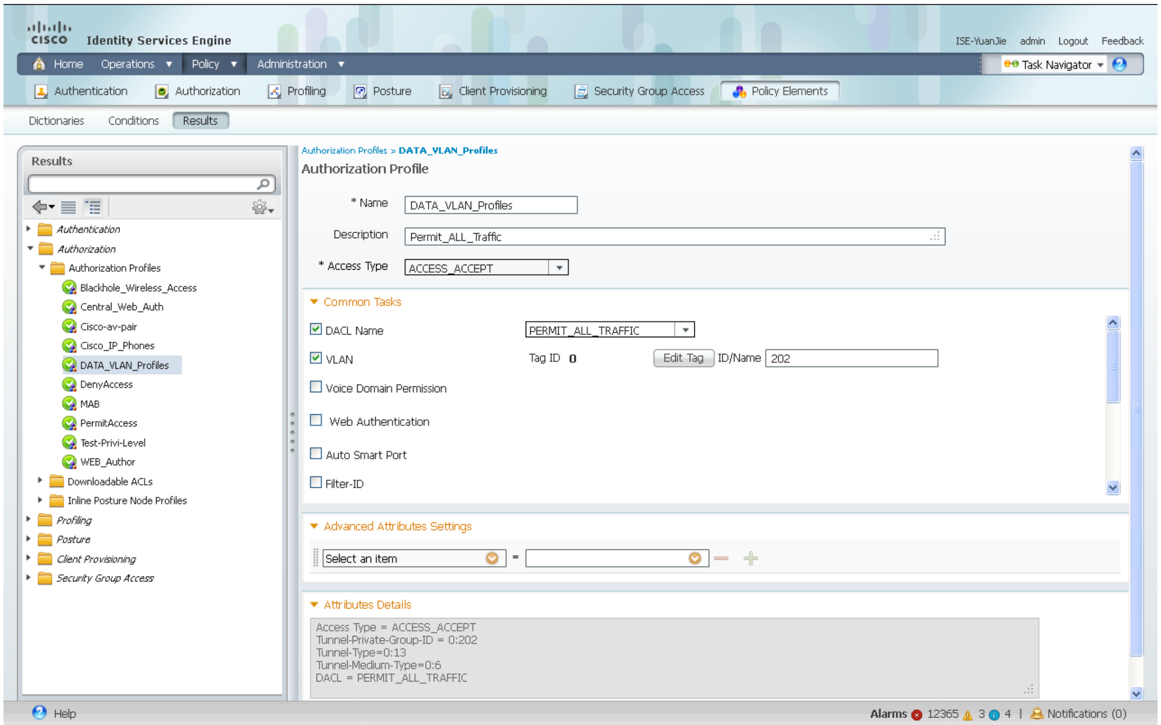
First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Guest_Author	if	**Guest_manager**	then	DATA_VLAN_Profiles	Edit |
	Telnet-Test-Author	if	AD1:ExternalGroups EQUALS dot1x.com/Users/group1	then	Test-Privi-Level	Edit |
	WEB_Author	if	AD1:ExternalGroups EQUALS dot1x.com/adenterprise2/adgroup2	then	WEB_Author	Edit |
	PEAP_Author	if	AD1:ExternalGroups EQUALS dot1x.com/adenterprise1/adgroup1	then	Cisco-av-pair	Edit |
	MAB_Author	if	**MAB_Group**	then	MAB	Edit |
	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit |
☑	SMB	if	Any and Condition(s)	then	DATA_VLA...	Done
☑	Default		if no matches, then		DATA_VLAN	Edit |

DATA_VLAN_Profiles


Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Blackhole_Wireless_Access
Central_Web_Auth
Cisco-av-pair
Cisco_IP_Phones
DATA_VLAN_Profiles
DenyAccess
MAB
PermitAccess
Test-Privi-Level
WEB_Author
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Help
Alarms 12365 3 4 | Notifications (0)

Authorization Profiles > **DATA_VLAN_Profiles**

Authorization Profile

* Name DATA_VLAN_Profiles

Description Permit_ALL_Traffic

* Access Type ACCESS_ACCEPT

Common Tasks

☑ DACL Name PERMIT_ALL_TRAFFIC

☑ VLAN Tag ID 0 Edit Tag ID/Name 202

☐ Voice Domain Permission

☐ Web Authentication

☐ Auto Smart Port

☐ Filter-ID

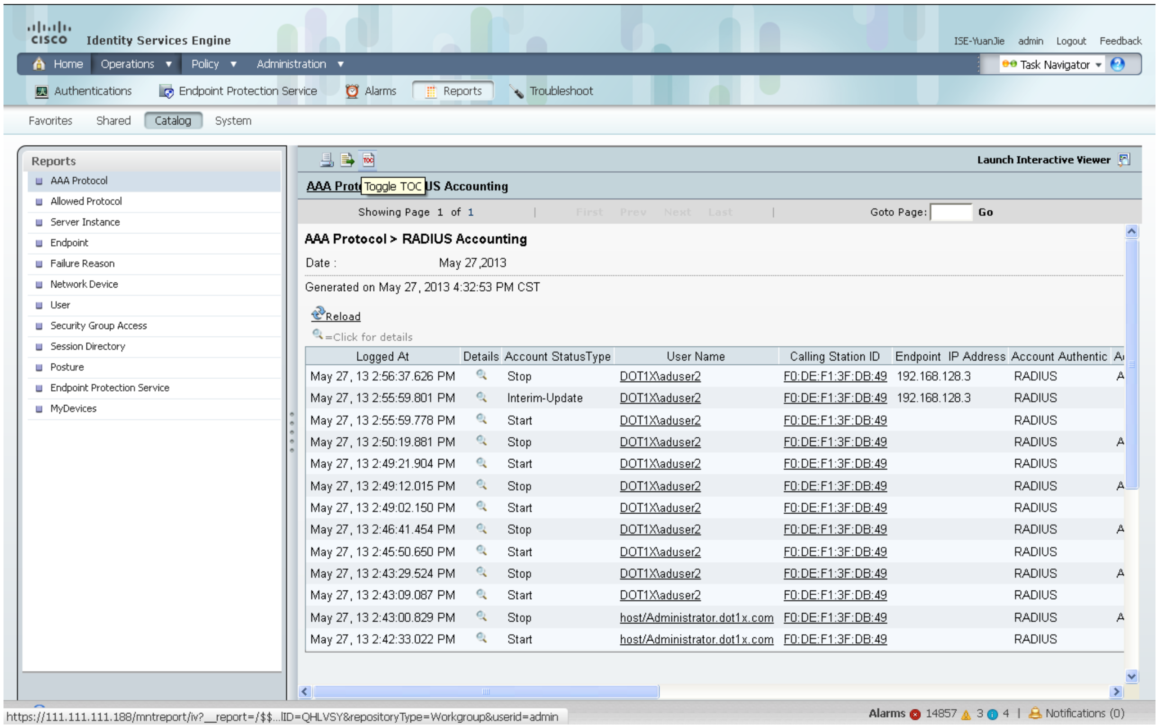
Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 0:202
Tunnel-Type=0:13
Tunnel-Medium-Type=0:6
DACL = PERMIT_ALL_TRAFFIC
```

Accounting



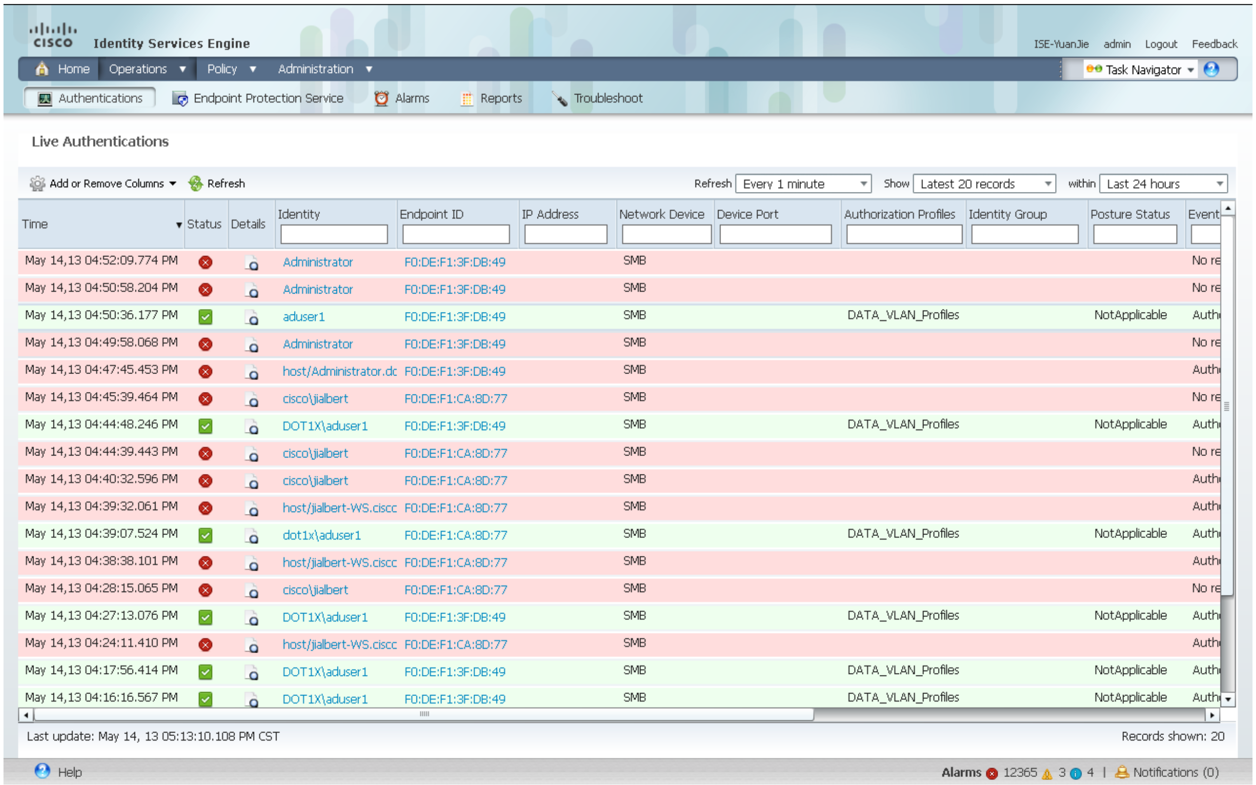
AAA Protocol > RADIUS Accounting

Date : May 27,2013

Generated on May 27, 2013 4:32:53 PM CST

Logged At	Details	Account StatusType	User Name	Calling Station ID	Endpoint IP Address	Account Authentic	A
May 27, 13 2:56:37.626 PM	🔍	Stop	DOT1X\aduser2	F0:DE:F1:3F:DB:49	192.168.128.3	RADIUS	A
May 27, 13 2:55:59.801 PM	🔍	Interim-Update	DOT1X\aduser2	F0:DE:F1:3F:DB:49	192.168.128.3	RADIUS	
May 27, 13 2:55:59.778 PM	🔍	Start	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	
May 27, 13 2:50:19.881 PM	🔍	Stop	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	A
May 27, 13 2:49:21.904 PM	🔍	Start	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	
May 27, 13 2:49:12.015 PM	🔍	Stop	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	A
May 27, 13 2:49:02.150 PM	🔍	Start	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	
May 27, 13 2:46:41.454 PM	🔍	Stop	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	A
May 27, 13 2:45:50.650 PM	🔍	Start	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	
May 27, 13 2:43:29.524 PM	🔍	Stop	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	A
May 27, 13 2:43:09.087 PM	🔍	Start	DOT1X\aduser2	F0:DE:F1:3F:DB:49		RADIUS	
May 27, 13 2:43:00.829 PM	🔍	Stop	host/Administrator.dot1x.com	F0:DE:F1:3F:DB:49		RADIUS	A
May 27, 13 2:42:33.022 PM	🔍	Start	host/Administrator.dot1x.com	F0:DE:F1:3F:DB:49		RADIUS	

Status Report



cisco Identity Services Engine
ISE-YuanJie admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
Authentications Endpoint Protection Service Alarms Reports Troubleshoot

Live Authentications

Add or Remove Columns ▾ Refresh

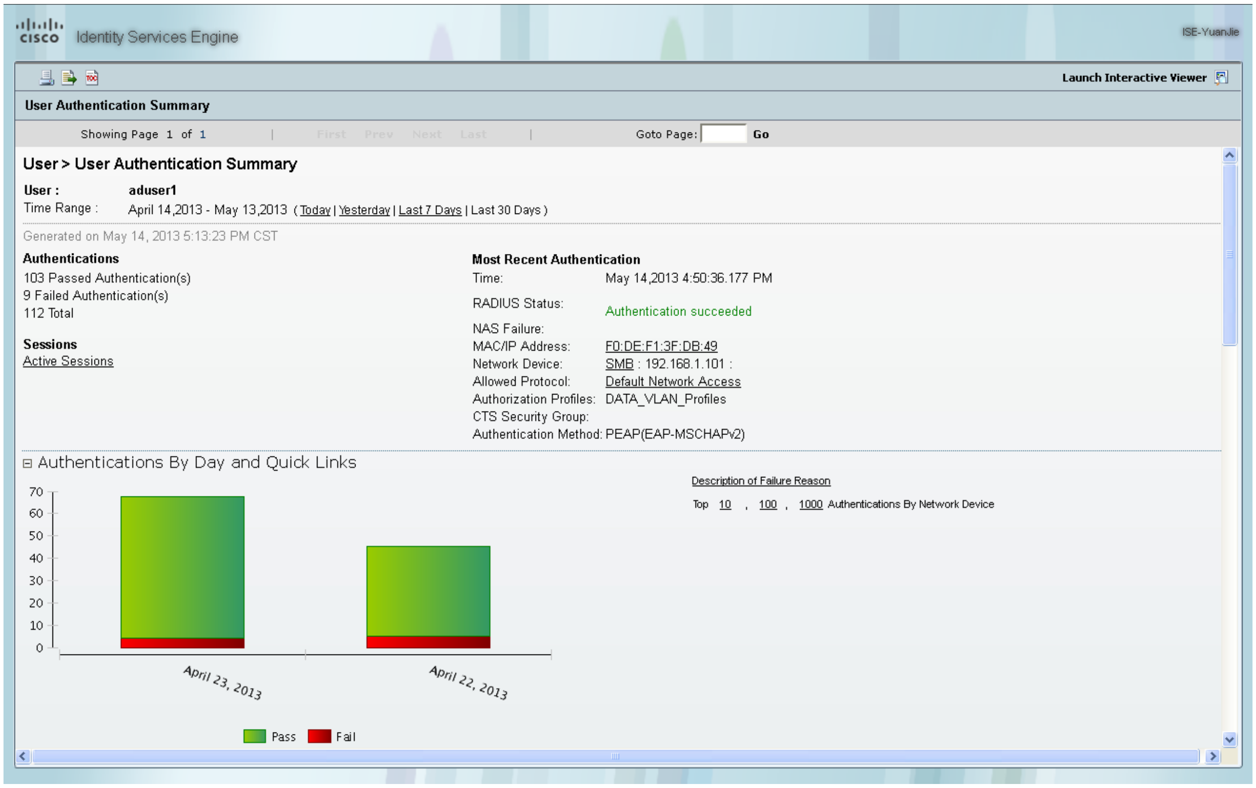
Refresh: Every 1 minute Show: Latest 20 records within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
May 14,13 04:52:09.774 PM	☒		Administrator	F0:DE:F1:3F:DB:49		SMB					No re
May 14,13 04:50:58.204 PM	☒		Administrator	F0:DE:F1:3F:DB:49		SMB					No re
May 14,13 04:50:36.177 PM	☑		aduser1	F0:DE:F1:3F:DB:49		SMB		DATA_VLAN_Profiles		NotApplicable	Auth
May 14,13 04:49:58.068 PM	☒		Administrator	F0:DE:F1:3F:DB:49		SMB					No re
May 14,13 04:47:45.453 PM	☒		host/Administrator.dc	F0:DE:F1:3F:DB:49		SMB					Auth
May 14,13 04:45:39.464 PM	☒		cisco\jialbert	F0:DE:F1:CA:8D:77		SMB					No re
May 14,13 04:44:48.246 PM	☑		DOT1X\aduser1	F0:DE:F1:3F:DB:49		SMB		DATA_VLAN_Profiles		NotApplicable	Auth
May 14,13 04:44:39.443 PM	☒		cisco\jialbert	F0:DE:F1:CA:8D:77		SMB					No re
May 14,13 04:40:32.596 PM	☒		cisco\jialbert	F0:DE:F1:CA:8D:77		SMB					Auth
May 14,13 04:39:32.061 PM	☒		host/jialbert-WS.ciscc	F0:DE:F1:CA:8D:77		SMB					Auth
May 14,13 04:39:07.524 PM	☑		dot1x\aduser1	F0:DE:F1:CA:8D:77		SMB		DATA_VLAN_Profiles		NotApplicable	Auth
May 14,13 04:38:38.101 PM	☒		host/jialbert-WS.ciscc	F0:DE:F1:CA:8D:77		SMB					Auth
May 14,13 04:28:15.065 PM	☒		cisco\jialbert	F0:DE:F1:CA:8D:77		SMB					No re
May 14,13 04:27:13.076 PM	☑		DOT1X\aduser1	F0:DE:F1:3F:DB:49		SMB		DATA_VLAN_Profiles		NotApplicable	Auth
May 14,13 04:24:11.410 PM	☒		host/jialbert-WS.ciscc	F0:DE:F1:CA:8D:77		SMB					Auth
May 14,13 04:17:56.414 PM	☑		DOT1X\aduser1	F0:DE:F1:3F:DB:49		SMB		DATA_VLAN_Profiles		NotApplicable	Auth
May 14,13 04:16:16.567 PM	☑		DOT1X\aduser1	F0:DE:F1:3F:DB:49		SMB		DATA_VLAN_Profiles		NotApplicable	Auth

Last update: May 14, 13 05:13:10.108 PM CST

Records shown: 20

Help
Alarms 12365 3 4 | Notifications (0)



cisco Identity Services Engine
ISE-YuanJie
Launch Interactive Viewer

User Authentication Summary

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

User > User Authentication Summary

User : **aduser1**
Time Range : April 14,2013 - May 13,2013 (Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on May 14, 2013 5:13:23 PM CST

Authentications
103 Passed Authentication(s)
9 Failed Authentication(s)
112 Total

Sessions
Active Sessions

Most Recent Authentication

Time:	May 14,2013 4:50:36.177 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
MAC/IP Address:	F0:DE:F1:3F:DB:49
Network Device:	SMB : 192.168.1.101 :
Allowed Protocol:	Default Network Access
Authorization Profiles:	DATA_VLAN_Profiles
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

⊟ Authentications By Day and Quick Links

Description of Failure Reason

Top 10 , 100 , 1000 Authentications By Network Device