SISAS

# Implementing Cisco Security Access Solutions

**Version 1.0** **Lab Guide**

Part Number: 97-3328-01

https://t.me/learningnets

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2014 Cisco Systems, I

https://t.me/learningnets

# Table of Contents


***Lab 1-1: Bootstrap Identity System*** ***L-5***

Visual Objective L-6
Required Resources L-6
Command List L-6
Job Aids L-7
Task 1: Define Local User in Cisco ISE L-11
Task 2: Define the switch as a NAD in Cisco ISE L-12
Task 3: Configure AAA Settings on Switch L-13
Task 4: Configure RADIUS Settings on Switch L-14
Task 5: Configure Switch for 802.1X Monitor Mode L-16
Task 6: Enable Windows 802.1X Supplicant on Employee-PC L-18

***Lab 2-1: Enroll Cisco ISE in PKI*** ***L-25***

Visual Objective L-26
Task 1: Task 1: Verify IE Operation Before ISE PKI Enrollment L-26
Task 2: Task 2: Verify the Supplicant Operation Before ISE PKI Enrollment L-30
Task 3: Task 3: Enroll Cisco ISE in PKI L-33
Task 4: Task 4: Explore System Behavior after ISE PKI Enrollment L-38

***Lab 2-2: Implement MAB and Internal Authentication*** ***L-41***

Visual Objective L-42
Command List L-42
Task 1: Deploy MAC Authentication Bypass L-43
Task 2: Deploy AnyConnect Supplicant L-50
Task 3: Configure CA Trust with the AnyConnect Profile Editor L-53

***Lab 2-3: Implement External Authentication*** ***L-59***

Visual Objective L-60
Task 1: Join ISE to the Active Directory L-60
Task 2: Configure Authentication Against the Active Directory L-62
Task 3: Test Authentication of Domain Users L-64
Task 4: Join the Workstation to the Active Directory L-66
Task 5: Test User and Machine Authentication Using Windows Credentials L-68

***Lab 3-1: Implement EAP-TLS*** ***L-71***

Visual Objective L-72
Task 1: Configure Employee-PC for EAP-TLS L-72
Task 2: Configure ISE for Certificate-Based Client Authentication L-76
Task 3: Test EAP-TLS L-78

***Lab 3-2: Implement Authorization*** ***L-81***

Visual Objective L-82
Command List L-82
Task 1: Enable EAP Chaining L-82
Task 2: Configure Switch for AAA Authorization and 802.1X Low-Impact Mode L-85


**https://t.me/learningnets**

Task 3: Retrieve User Groups from Active Directory L-87
Task 4: Configure Authorization for IT Users and Domain Computers L-89
Task 5: Configure Authorization for Remaining Employees L-98
Task 6: Configure Authorization for Domain Administrators L-100
Task 7: Configure Authorization for Local ISE Users L-102
Task 8: Configure Authorization for Print Servers L-104

***Lab 3-3: Implement Cisco TrustSec and MACsec L-109***

Visual Objective L-110
Command List L-110
Task 1: Prepare ISE for TrustSec communication with the HQ-SW L-111
Task 2: Configure the Switch to Act as SGA Device L-114
Task 3: Dynamically Apply SGT during 802.1X Authorization L-117
Task 4: Implement Egress Filtering on Switch L-119
Task 5: Provision a PAC for the ASA (Optional) L-126
Task 6: Implement SXP and SGFW (Optional) L-131
Task 7: Implement Downlink MACsec (Optional) L-136

***Lab 4-1: Implement WebAuth for Employees L-143***

Visual Objective L-144
Task 1: Configure Switch for Central WebAuth L-144
Task 2: Configure ISE Authentication for WebAuth L-145
Task 3: Configure ISE Authorization to Enforce Traffic Redirection L-149
Task 4: Configure ISE Authorization Rule for Employees Authenticated via WebAuth L-156

***Lab 4-2: Implement Guest Service L-161***

Visual Objective L-162
Task 1: Configure Access to the Sponsor Portal L-162
Task 2: Provision Guest User in the Sponsor Portal L-164
Task 3: Configure Authorization for Guest Users L-168

***Lab 5-1: Implement Posture Service L-173***

Visual Objective L-174
Task 1: Prepare Initial Components L-174
Task 2: Configure Client Provisioning Policy L-177
Task 3: Configure Authorization for Compliant, Noncompliant, and Unknown Status L-179
Task 4: Deploy Antivirus Installation Remediation L-189
Task 5: Deploy Automatic Antispyware Definition Remediation (Optional) L-198
Task 6: Provision Web Agent on Guest-PC (Optional) L-200

***Lab 5-2: Implement Profiler Service L-209***

Visual Objective L-210
Task 1: Observe Profiling without Probes L-210
Task 2: Deploy DHCP, RADIUS, and HTTP Probes L-213
Task 3: Configure Print Server Profiling L-217

***Lab 6-1: (Optional) Troubleshooting Prep L-225***

Task 1: Restore Broken Backup Configurations on Switch and ISE L-226


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

*Lab 6-2: (Optional) Troubleshoot Network Access Controls* *L-229*

Visual Objective L-229
Task 1: Troubleshoot 802.1X Authentication Against Local ISE Database L-230
Task 2: Guide for Troubleshooting 802.1X Authentication Against Local ISE Database L-231
Task 3: Troubleshoot 802.1X Authentication Against Active Directory L-237
Task 4: Guide For Troubleshooting 802.1X Authentication Against Active Directory L-238
Task 5: Troubleshoot EAP-TLS Authentication L-241
Task 6: Guide For Troubleshooting EAP-TLS L-243
Task 7: Troubleshoot Authorization L-247
Task 8: Guide For Troubleshooting Authorization L-248
Task 9: Troubleshoot Central WebAuth L-249
Task 10: Guide For Troubleshooting Central WebAuth L-250
Task 11: Troubleshoot Posture L-256
Task 12: Guide For Troubleshooting Posture L-256

*Lab Answer Keys* *L-259*

Lab 1-1: Bootstrap Identity System L-259
Lab 2-1: Enroll Cisco ISE in PKI L-259
Lab 2-2: Implement MAB and Internal Authentication L-259
Lab 2-3: Implement External Authentication L-260
Lab 3-1: Implement EAP-TLS L-260
Lab 3-2: Implement Authorization L-260
Lab 3-3: Implement Cisco TrustSec and MACsec L-260
Lab 4-1: Implement WebAuth for Employees L-260
Lab 4-2: Implement Guest Service L-261
Lab 5-1: Implement Posture Service L-261
Lab 5-2: Implement Profiler Service L-261
Lab 6-1: (Optional) Troubleshooting Prep L-261
Lab 6-2: (Optional) Troubleshoot Network Access Controls L-262

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 1-1: Bootstrap Identity System

## Activity Objective

In this lab exercise you will jump start the switch and the Cisco Identity Services Engine to deploy 802.1X in monitor mode. You will create a user in the local ISE database and define the switch as a NAD on the ISE. You will configure the switch with the necessary AAA, RADIUS, and 802.1X settings to enable the switch to act as a 802.1X authenticator. You will test 802.1X operations using the Windows native 802.1X supplicant on the Employee-PC.

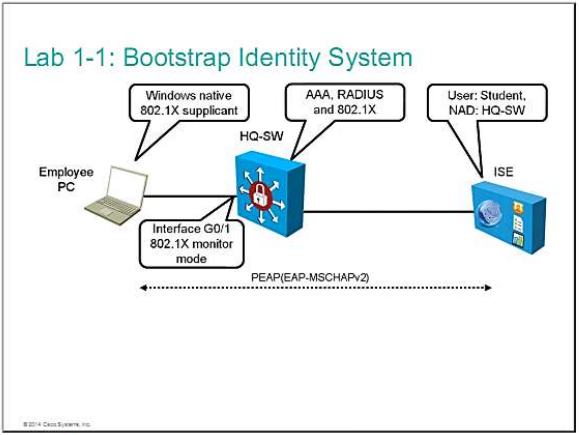
Upon completing this exercise, you will be able to:

- Define local users in ISE local user database.
- Define NADs in the ISE.
- Configure Cisco IOS switch to act as 802.1X authenticator.
- Enable Windows native 802.1X supplicant.
- Deploy PEAP.
- Verify basic 802.1X authentications against Cisco ISE.

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Required Resources

The following resources and equipment are required to complete this activity:

- Catalyst switch
- Windows 7 workstation
- Cisco ISE

# Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

## Commands

| Command | Description |
|---|---|
| **aaa accounting dot1x default start-stop group radius** | Enables accounting for 802.1X and MAB. Stop records are used for session closing and releasing license counts. |
| **aaa authentication dot1x default group radius** | Creates an IEEE 802.1X port-based authentication method list. |
| **aaa authorization auth-proxy default group radius** | Enables authentication and authorization for WebAuth transactions. |
| **aaa authorization network default group radius** | Enables VLAN and dACL assignment. |


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **aaa new-model** | Enables AAA. |
| **authentication open** | Enables preauthentication open access (low impact or monitoring modes). |
| **authentication port-control auto** | Enables port-based authentication on the interface |
| **dot1x pae authenticator** | Enables 802.1X authentication on the interface |
| **dot1x system-auth-control** | Globally enables 802.1X port-based authentication. |
| **ip device tracking** | Enable the IP device tracking table that is required to use dACLs. |
| **radius-server attribute** *6 on-for-login-auth* | Sends the service-type attribute in access requests. |
| **radius-server attribute** *6 support-multiple* | Supports multiple Service-Type values for each RADIUS profile. |
| **radius-server attribute 8 include-in-access-req** | Sends the framed-IP-address attribute in access requests. |
| **radius-server attribute 25 access-request include** | Sends the class attribute in access requests. |
| **radius-server vsa send accounting** | Enables VSAs to be sent in accounting messages. |
| **radius-server vsa send authentication** | Configures the NAD to recognize and use authentication VSAs. |

# Job Aids

These job aids are available to help you complete the lab activity.


https://t.me/learningnets

### Pod Information

The table shows the devices that are used in the lab and the operating systems that are running on the devices.

| Device | Hardware | Operating System and Filenames |
|---|---|---|
| Partner-ISR | Cisco 2901 ISR | c2900-universalk9-mz.SPA.153-1.T.bin |
| Branch-ISR | Cisco 2901 ISR | c2900-universalk9-mz.SPA.153-1.T.bin |
| HQ-ISR | Cisco 2901 ISR | c2900-universalk9-mz.SPA.153-1.T.bin |
| HQ-ASA | Cisco ASA 5515-X with Cisco IPS or Cisco ASA CX software module | asa911-4-smp-k8.bin<br>IPS-SSP_5515-K9-sys-1.1-a-7.1-4-E4.aip<br>asa911-4-smp-k8.bin<br>asacx-5500x-boot-9.1.1-14.img |
| HQ-SW | Cisco Catalyst WS-C3560X-24 | c3560e-universalk9-mz.150-2.SE2.bin |
| Internet-RTR | Cisco 2901 ISR | c2900-universalk9-mz.SPA.153-1.T.bin |
| Partner-SRV | Virtualized | Microsoft Windows Server 2008 R2 Standard |
| SP-SRV | Virtualized | Microsoft Windows Server 2008 R2 Standard |
| Branch-SRV | Virtualized | Microsoft Windows Server 2008 R2 Standard |
| DMZ-SRV | Virtualized | Linux Ubuntu |
| HQ-SRV | Virtualized | Microsoft Windows Server 2008 R2 Standard |
| Admin-PC | Virtualized | Microsoft Windows 7 |
| Guest-PC | Virtualized | Microsoft Windows 7 |
| Employee-PC | Virtualized | Microsoft Windows 7 |
| Attacker-PC | Virtualized | Linux Kali |
| HQ-ISE | Virtualized | Cisco ISE version 1.2 |
| HQ-CDA | Virtualized | Cisco CDA version 1.0.0.11 |
| HQ-ESA | Virtualized | AsyncOS version 8.0.0-550 |
| HQ-WSA | Virtualized | AsyncOS version 7.7.5-093 |

The table shows the usernames and passwords that are used to access the equipment in this lab.

| Device | Username | Password |
|---|---|---|
| HQ-ASA | **admin** | **Ci5coAdmin**<br>Enable: **cisco** |
| HQ-IPS | **cisco** | **Ci5coAdmin** |
| Partner-SRV | **administrator** | **Ci5coAdmin** |
| SP-SRV | **administrator** | **Ci5coAdmin** |
| Branch-SRV | **administrator** | **Ci5coAdmin** |
| DMZ-SRV | **administrator** | **Ci5coAdmin** |

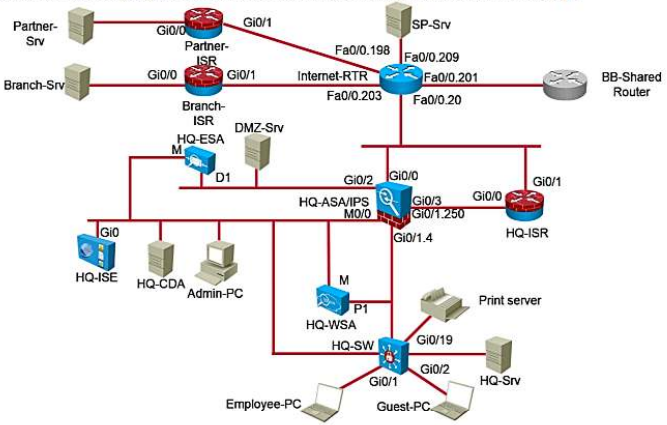

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| Device | Username | Password |
|---|---|---|
| HQ-SRV | **administrator** | **Ci5coAdmin** |
| Admin-PC | **student** | **Ci5coAdmin** |
| Guest-PC | **student** | **Ci5coAdmin** |
| Employee-PC | **student** | **Ci5coAdmin** |
| Attacker-PC | **root** | **Ci5coAdmin** |
| HQ-ISE | **admin** | **Ci5coAdmin** |
| HQ-CDA | **admin** | **Ci5coAdmin** |
| HQ-ESA | **admin** | **Ci5coAdmin** |
| HQ-WSA | **admin** | **Ci5coAdmin** |

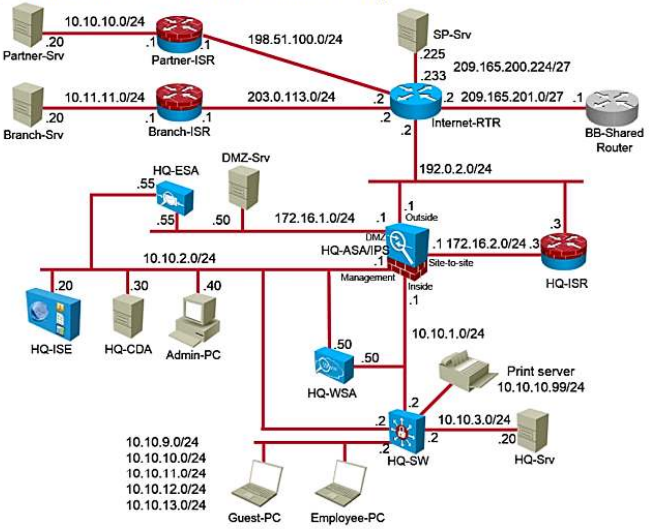

https://t.me/learningnets

### Topology and IP Addressing

The figure shows the topology and interface identifications that are used in this lab setup.




The figure shows the IP addresses that are used in this lab setup.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 1: Define Local User in Cisco ISE

In this task you will define a user named student with the password Ci5coAdmin in the local user database of Cisco ISE.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Access the ISE GUI: Connect to Admin-PC (**student/Ci5coAdmin**). Open the Internet Explorer browser and connect to **https://ise.secure-x.local**. Log in as user **admin** with the password **Ci5coAdmin**.

#### *Step 2*

Create a local user named student with the password Ci5coAdmin in Cisco ISE:

A) In the Cisco ISE GUI, choose **Administration > Identity Management > Identities** and click the **Users** folder in the Identities pane on the left side of the window.

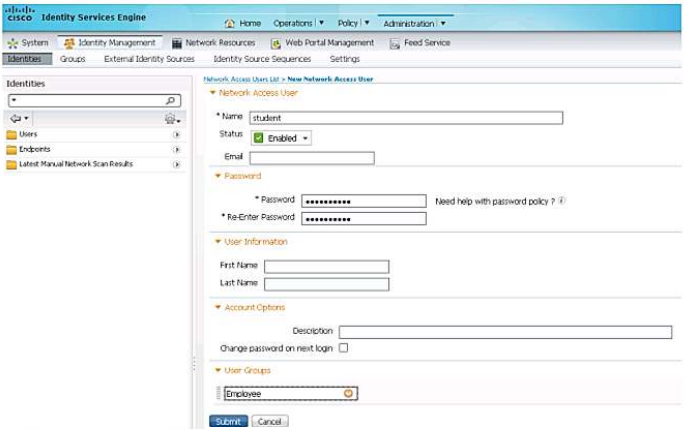
B) In the Network Access Users pane, click **Add**. The New Network Access User pane is displayed.

C) Define the user's attributes as follows:

Name: **student**

Password and Re-Enter Password: **Ci5coAdmin**

User Groups: **Employee**




D) Click **Submit** to apply the changes.

E) Verify that the user named student is now defined in the Network Access Users table and the status is Enabled.


https://t.me/learningnets

# Task 2: Define the switch as a NAD in Cisco ISE

Before a RADIUS server and a RADIUS client can communicate, they must be defined to each other. At a minimum they need to be configured with each other's IP addresses and with a shared secret that is used to secure communications between the two systems. In ISE, the RADIUS clients are NADs. ISE allows the creation and use of Network Device Groups for the purpose of organizing NADs. In this task you will define a Network Device Group for the headquarters location and you will define the HQ-SW as a NAD in that location.

### Activity Procedure

Complete the following steps:

#### *Step 1*

In the Cisco ISE GUI, configure a Network Device Group named HQ as a child to the default Network Device Group named All Locations:

A) Navigate to **Administration >Network Resources > Network Device Groups**.

B) In the Network Device Groups pane on the left, expand **Groups** and choose **All Locations**. An empty Network Device Groups table will be displayed.

C) Click **Add** above the empty table. Define a group named **HQ** and click **Submit**.

D) Verify that the location HQ is now in the Network Device Group table.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

Define the HQ-SW as a NAD in the ISE.

A) Navigate to **Administration >Network Resources >Network Devices**.

B) In the Network Devices pane on the left side of the window, choose **Network Devices** if necessary. The empty Network Devices Table should be displayed.

C) Above the Network Devices table, click **Add**.

D) Define the NAD with these attributes:

Name: **HQ-SW**

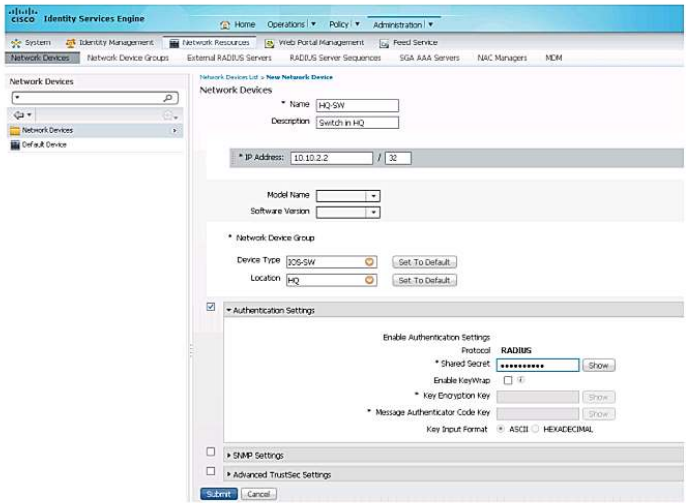
IP Address: **10.10.2.2/32**

Device Type: **IOS-SW**

Location: **HQ**

Authentication Settings: **[X] Checked**

Shared Secret: **radius-key**




# Task 3: Configure AAA Settings on Switch

In this task you will configure AAA settings on the HQ-SW.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets

### *Step 1*

Connect to the HQ-SW's console port.

### *Step 2*

Before any AAA authentication, authorization or accounting commands can be configured, AAA must be enabled globally on the switch.

```
aaa new-model
```

### *Step 3*

Enabling AAA globally changes the authentication behavior on the console and the VTY lines. Set the enable secret to **cisco** and set the default authentication method for logins to use the enable secret.

```
enable secret cisco
aaa authentication login default enable
```

### *Step 4*

On the switch, configure the global AAA settings required for proper 802.1X operation:

A) Define the default method for authentication of 802.1X access requests, specifying the group ISE-RADIUS as the AAA server group.

B) Define the default method of authorizing network access sessions, specifying the group ISE-RADIUS as the AAA server group.

C) Define the default method of accounting to be used for 802.1X sessions, specifying the group ISE-RADIUS as the AAA server group.

| | |
|---|---|
| **Note** | Expect the message %AAAA-4-SERVUNDEF: The server-group "ISE-TEST" is not defined. Please define it. You will define this server-group in the next task. |

```
aaa authentication dot1x default group ISE-RADIUS
aaa authorization network default group ISE-RADIUS
aaa accounting dot1x default start-stop group ISE-RADIUS
```

# Task 4: Configure RADIUS Settings on Switch

In this task you will configure RADIUS settings on the HQ-SW.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 1

Define the ISE appliance as a RADIUS server, include it in the AAA server group ISE-RADIUS, and set the dead criteria for RADIUS servers

A) Create a RADIUS server instance named ISE-KEY with the IP address 10.10.2.20 using UDP ports 1812 and 1813, and specify the shared key 'radius-key'.

B) Create an AAA server group named ISE-RADIUS and assign the RADIUS server named ISE-KEY to the group.

C) Set the RADIUS timeout to 10 seconds with a 3 attempt failure limit.

**Note** AAA server groups are a construct that allows different sets of servers to be specified for different AAA applications. For example, one set can be used for 802.1X AAA and another set for administrative access AAA. You are defining an AAA server group in this lab to prepare for a workaround in a later lab. The explanation will become clear when it is time to implement the workaround.

```
radius server ISE-KEY
 address ipv4 10.10.2.20 auth-port 1812 acct-port 1813
 key radius-key
!
aaa group server radius ISE-RADIUS
 server name ISE-KEY
!
radius-server dead-criteria time 10 tries 3
```

### Step 2

Configure the additional RADIUS attributes that are required by ISE:

A) Include the RADIUS Service-Type attribute in the authentication requests.

B) Include the endpoint IP address in the framed-IP-address attribute in the authentication requests.

C) Include the class attribute in RADIUS authentication requests.

```
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
```

### Step 3

Configure the switch to use RADIUS vender specific attributes:

A) Configure the switch to use VSAs in authentication requests.

B) Configure the switch to use VSAs in accounting updates.

```
radius-server vsa send authentication
radius-server vsa send accounting
```


https://t.me/learningnets

### *Step 4*

IP device tracking is required to allow the switch to learn endpoint IP addresses and populate the Framed-IP-Address field in the RADIUS authentication requests. Enable IP device tracking:

```
ip device tracking
```

### *Step 5*

Before going any further, use the **test aaa** command to verify communications between the switch and ISE (**group ISE-RADIUS**). Testing with the credentials you defined in ISE (student/Ci5coAdmin) should be successful. If it is not, you most likely have a typographical error in the RADIUS preshared key on either the switch or in ISE.

```
HQ-SW#test aaa group ISE-RADIUS student Ci5coAdmin new-code
User successfully authenticated
USER ATTRIBUTES
username              0    "student"
```

# Task 5: Configure Switch for 802.1X Monitor Mode

In this task you will enable 802.1X and configure 802.1X settings the switch interface to which the Employee-PC us connected. At this point in the deployment you will configure 802.1X monitor mode. Monitor mode allows access even when authentication fails. This allows the administrator to perform authentication audits without disrupting network availability. After authentication issues are addressed, the systems can migrate to low impact mode or closed mode. Monitor mode is implemented on a port using the **authentication open** command without the use of a pre-auth ACL on the port.

### Activity Procedure

Complete the following steps:

### *Step 1*

Enable 802.1X globally on the switch:

A) Enable 802.1X globally on the switch.

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


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Configure the interface supporting the Employee-PC (GigabitEthernet0/1) for 802.1X monitor mode:

A) Configure multiple authentication (multi-auth) mode.

B) Configure the interface of the Employee-PC for 802.1X open mode. Do not use any local access lists.

C) Enable recurring re-authentication.

D) Allow the RADIUS server to specify the re-authentication interval.

E) Enable the 802.1X authenticator role on the port.

F) Set the 802.1X timeout for supplicant retries to 10 seconds.

G) Allow 802.1X authentication to control the port's status.

```
interface GigabitEthernet0/1
 authentication host-mode multi-auth
 authentication open
 authentication periodic
 authentication timer reauthenticate server
 dot1x pae authenticator
 dot1x timeout tx-period 10
 authentication port-control auto
```

### Activity Verification

You have completed this task when you verify the 802.1X configuration on the switch using this procedure:

### *Step 1*

On the switch, view the overall 802.1X status using the **show dot1x all** command. You should see that the system authentication control is enabled and the pae type on interface GigabitEthernet 0/1 is set to authenticator.

```
HQ-SW# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
Dot1x Info for GigabitEthernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 10
```


https://t.me/learningnets

### *Step 2*

On the switch console, observe the failed access attempts through the interface GigabitEthernet 0/1. It may take 90 seconds before the messages are displayed. You should see that the authentication fails because there is no supplicant and there is no failover authentication method.

```
%DOT1X-5-FAIL: Authentication failed for client (Unknown MAC) on Interface Gi0/1
AuditSessionID 0A0A0202000000440E875158
%AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client
(Unknown MAC) on Interface Gi0/1 AuditSessionID 0A0A0202000000440E875158
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (Unknown MAC) on Interface
Gi0/1 AuditSessionID 0A0A0202000000440E875158
%AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (Unknown
MAC) on Interface Gi0/1 AuditSessionID 0A0A0202000000440E875158
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (Unknown MAC) on
Interface Gi0/1 AuditSessionID 0A0A0202000000440E875158
```

### *Step 3*

On the switch, view the status of authentication sessions on the interface using the show a**uthentication sessions interface gigabitethernet 0/1** command. You should see that the status is Authz Failed. Note that the endpoint IP address is defined because IP device tracking is enabled. The IP address that you see may differ from the sample as the address is assigned via DHCP.

```
HQ-SW#show authentication sessions interface gigabitethernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3dad
           IP Address:  10.10.9.10
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000003F065E99C7
      Acct Session ID:  0x00000006
              Handle:  0x1D000040
Runnable methods list:
       Method   State
       dot1x    Failed over
```

# Task 6: Enable Windows 802.1X Supplicant on Employee-PC

In this task you enable the Windows native 802.1X supplicant on the Employee-PC.

**Note** Having configured the access switch for 802.1X and the RADIUS communications with the ISE, you will now enable the native Windows supplicant on the Employee-PC. In this scenario you will deploy Protected EAP (PEAP), which is the default method.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Connect to the Employee-PC by using the appropriate shortcut on your springboard PC. Log in as local administrator **'student'** with password **Ci5coAdmin**. Enable the **Wired AutoConfig** service, which enables the 802.1X supplicant:

A) Click **Start** and type **services.msc**. Click **services.msc** under **Programs**. The Services console opens.

B) Scroll down and find **Wired AutoConfig**.

C) Open the properties and change the **Startup Type** to **Automatic**. Also, click **Start**, then click **OK**.

D) Close the **Services** console.


https://t.me/learningnets

***Step 2***

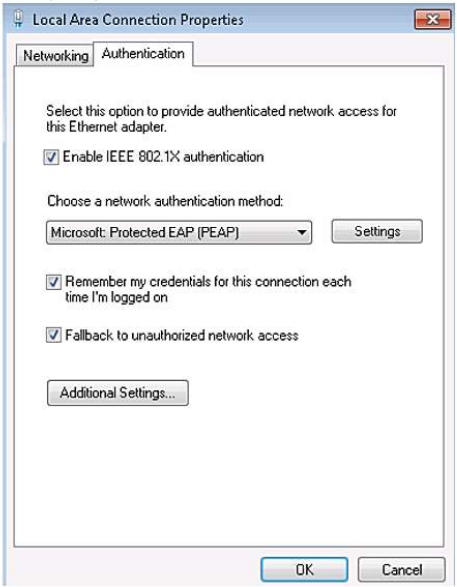
Enable the native Windows 802.1X supplicant and configure it to bypass server certificate validation:

A) Right-click the **Network** icon in the system tray. Select **Open Network and Sharing Center**.

B) Click **Change adapter settings**. This navigates you to the Network Connections list.

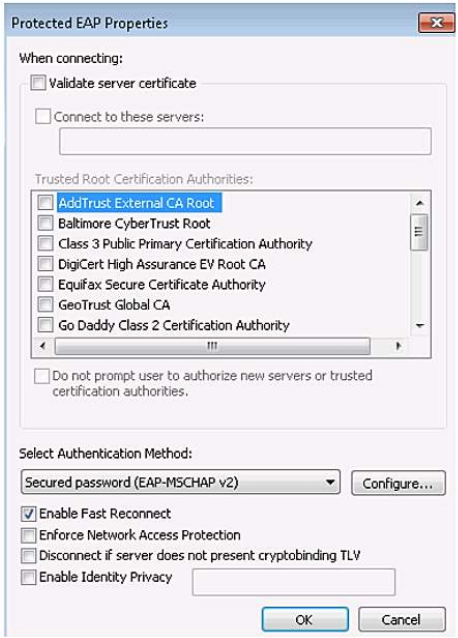
C) Double-click **Local Area Connection**. Click **Properties**, select the **Authentication** tab.

D) Check the **Enable IEEE 802.1X authentication** checkbox. Verify that the supplicant defaults to Microsoft Protected EAP (PEAP).




E) Click **Settings**. The Protected EAP Properties window opens. Clear the **Validate server certificate** checkbox. Since the ISE has not yet been enrolled into the PKI, the supplicant will not be able to validate the ISE certificate.

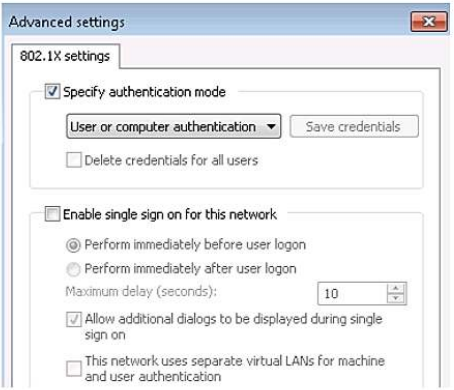

https://t.me/learningnets
© 2014 Cisco Systems, Inc.




F) Click **Configure** and verify the the Windows supplicant uses Windows credentials by default.

G) Click OK twice to close the two most recent windows.

H) On the Local Area Connection Properties window, click **Additional Settings**. Verify that the Windows supplicant defaults to user or machine authentication.




I) Click **OK** twice to close the two most recent windows and then close all remaining open windows.

### Activity Verification

It may not be obvious, but 802.1X authentication should have completed in the background. The Employee-PC has cached the login credentials (student/Ci5c0Admin), and will offer the credentials in the authentication process which will kick off as soon all of the components are configured. You have completed this task when you see a record of a successful 802.1X authentication attempt on the ISE and view status on the switch. Follow this verification procedure:

#### *Step 1*

In the Cisco ISE GUI, navigate to **Operations > Authentications**. You should see a successful access attempt of user student.

#### *Step 2*

Click the **Add or Remove Columns** button. Choose options that you want to display and click **Save**. The key information is shown below:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 3

Click the Details button in the third column. Examine the information in the Overview, Authentication Details, Other Attributes, Result, and Session Events sections.

### Step 4

On the switch, verify the authentication status on the port GigabitEthernet 0/1, where the Employee-PC is connected. This time, you should see that the authentication and authorization status of user student is reported as success. You should see the endpoint IP address because IP tracking has been enabled on the switch. The IP address in your pod may differ from the output below, because IP addresses are obtained dynamically.

```
HQ-SW# show authentication sessions interface gigabitethernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.10
            User-Name:  student
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000007816374BF0
      Acct Session ID:  0x00000068
               Handle:  0x21000079
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 2-1: Enroll Cisco ISE in PKI

## Activity Objective

In this lab exercise you will first observe that the 802.1X rejects the self-signed Cisco Identity Services Engine certificate and that the HTTPS session to the ISE is untrusted. Then you will enroll the ISE with the Public Key Infrastructure (PKI) and examine the trust established through the PKI infrastructure.

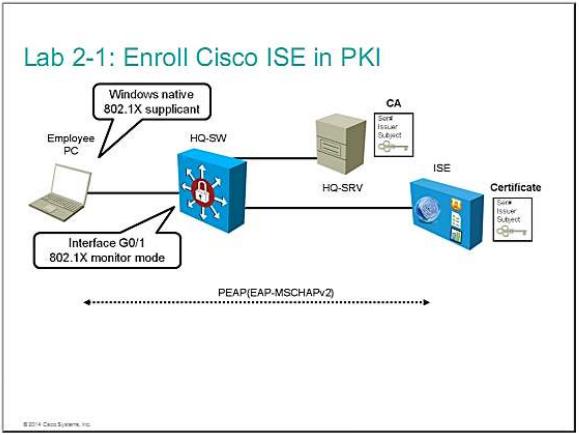
Upon completing this exercise, you will be able to:

- Enroll Cisco ISE to PKI
- Verify server-side certificate in PEAP

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Task 1: Verify IE Operation Before ISE PKI Enrollment

Upon initial setup, ISE creates a self signed certificate that it uses for both HTTPS and EAP. Systems that use PKI have a store of trusted certificate authority root certificates. Each of those root certificates documents the public key used by the CA to sign identity certificates. This allows systems to verify the validity of the identity certificates of remote peers. They use the public key of the CA to verify the signature of the remote peer's identity certificate. In this task you will explore how Internet Explorer when it is used for an administrative session to ISE and ISE is using a self-signed certificate.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Access the desktop of the **Admin-PC**. If any Internet Explorer windows are currently open, close the IE windows.

#### *Step 2*

Open **Internet Explorer** and connect to the ISE (**https://ise.secure-x.local**). Note that the URL entry field is red and a Certficate Error is indicated.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

Click on the **Certficate Error**. A description of the issue is displayed. It indicates that the certificate presented by the SSL server (Cisco ISE) was not issued by a trusted certificate authority.

https://t.me/learningnets

### *Step 4*

Click on the **View certificates** link. A certificate window opens. Note that both the Issued to: and Issued by: fields are ise.secure-x.local. This is a self signed certificate.

### *Step 5*

Close the certificate window.

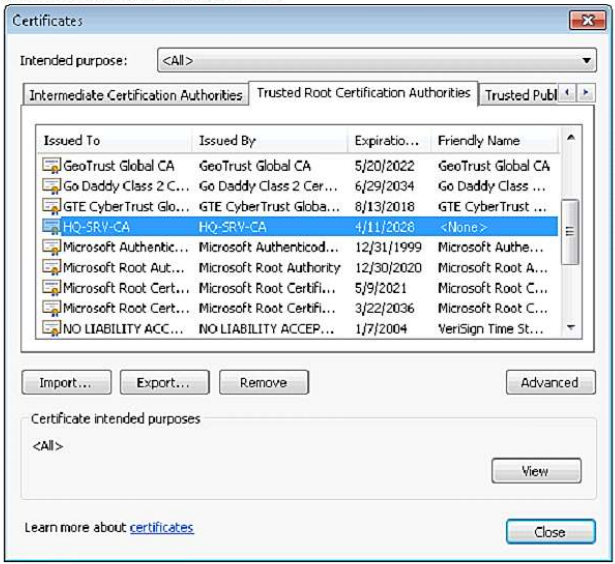
### *Step 6*

In IE, navigate to **Tools > Internet Options**. In the Internet Options window, select the **Content** tab and then click the **Certificates** button. The Certificates window will open, displaying the contents of the Windows certificate store.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 7*

In the Certificates window, select the **Trusted Root Certification Authorities** tab. Scroll down and note that there is a root certificate for the HQ-SRV-CA.




| | |
|---|---|
| **Note** | The Windows certificate store is used by both Internet Explorer and Windows' native 802.1X supplicant. Both applications will trust identity certificates that are signed by the HQ-SRV's CA. Not all applications use the Windows certificate store. Firefox is an example. Other applications may require importing trusted root certificates into their separate certificate store. |

### *Step 8*

Close the Certificates window and the Internet Options window.

# Task 2: Task 2: Verify the Supplicant Operation Before ISE PKI Enrollment

In a previous lab, you disabled the server certificate validation in the native Windows 802.1X supplicant. This was done to enable successful PEAP authentications. In this task you will return the supplicant settings to validate the server certificate, configuring the supplicant to trust certificates signed by HQ-SRV-CA. You will see that the 802.1X operations will fail. The supplicant will only pass credentials to RADIUS servers that it trusts via the public key infrastructure.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Access the desktop of the **Employee-PC** using **student** and **Ci5coAdmin** for credentials.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Configure the native supplicant to validate server certificate:

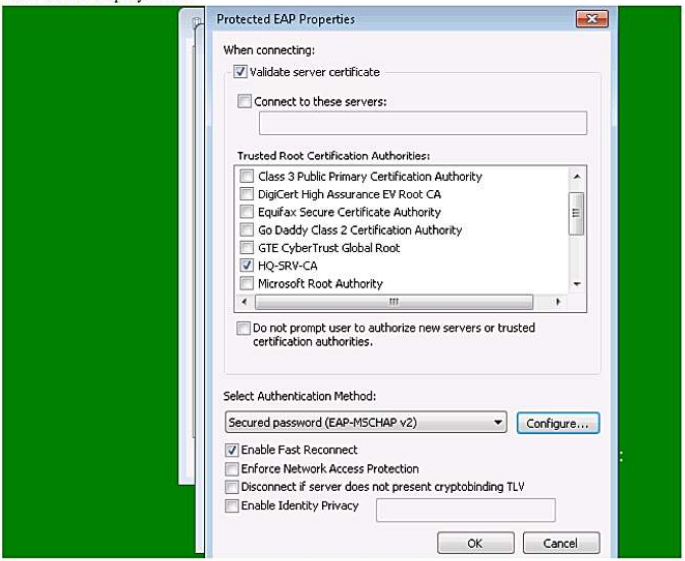
A) Right-click the **Network** icon in the system tray. Click **Open Network and Sharing Center**.

B) Click the **Change adapter settings** link on the left side of the window.

C) Click the **Local Area Connection** link and click the **Properties** button.

D) Select the **Authentication** tab and note that the authentication method is PEAP. Click the **Settings** button. The Protected EAP Properties window opens.

E) Check the **Validate server certificate** checkbox. In the Trusted Certfication Authorities list, check the **HQ-SRV-CA** checkbox. You see the HQ-SRV-CA root certificate in the list because it has been pre-installed on the Employee-PC.




F) Click **OK** twice to close the Protected EAP Properties window and the Local Area Connection Properties window. Also close the Local Area Connection Status window and the Network Connections window.

### Activity Verification

At this point, the supplicant on the Employee-PC will only trust RADIUS servers that have a certificate signed by HQ-SRV-CA. ISE is not yet enrolled with that CA. Verify that the supplicant rejects the ISE certificate. Follow these steps:


https://t.me/learningnets

### Step 1

It is possible that the the periodic reauthentication process has not yet occurred. To ensure that authentication has been attempted since the reconfiguration of the supplicant, disable and then enable interface G0/1 on the HQ-SW. Note that the 802.1X authentication process immediately begins and fails.

```
HQ-SW# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-SW(config) # int g0/1
HQ-SW(config-if)# shutdown
Nov 20 16:30:53.778: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
Nov 20 16:30:54.784: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
Nov 20 16:31:01.017: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
HQ-SW(config-if)# no shutdown
Nov 20 16:31:04.162: %AUTHMGR-5-START: Starting 'dot1x' for client (a036.9f1a.3dad)
on Interface Gi0/1 AuditSessionID 0A0A0202000000A21F4A81C2
Nov 20 16:31:04.229: %DOT1X-5-FAIL: Authentication failed for client (a036.9f1a.3dad)
on Interface Gi0/1 AuditSessionID 0A0A0202000000A21F4A81C2
Nov 20 16:31:04.229: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for
client (a036.9f1a.3dad) on Interface Gi0/1 AuditSessionID 0A0A0202000000A21F4A81C2
Nov 20 16:31:04.229: %AUTHMGR-5-FAIL: Authorization failed or unapplied for client
(a036.9f1a.3dad) on Interface Gi0/1 AuditSessionID 0A0A0202000000A21F4A81C2
Nov 20 16:31:06.100: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Nov 20 16:31:07.106: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
HQ-SW(config-if)# end
HQ-SW#
```

### Step 2

On HQ-Sw, examine the authentication status of port GigabitEthernet0/1. Again, you should see that authentication has failed.

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3dad
           IP Address:  10.10.9.21
            User-Name:  student
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000009F1F44FDF3
      Acct Session ID:  0x00000068
              Handle:  0xC70000A0
Runnable methods list:
       Method   State
       dot1x    Authc Failed
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| Note | The ISE certificate has been rejected because it is a factory-installed self-signed certificate. The clients trust only certificates that have been signed by a trusted certificate authority (CA) or explicitly installed in the trusted certificate store. |
|---|---|

| Note | In the next task you will enroll the ISE with the CA. This enrollment will cause the Employee-PC to trust the ISE certificate. |
|---|---|

# Task 3: Task 3: Enroll Cisco ISE in PKI

In this task you will enroll Cisco ISE with the CA running on the HQ server. The enrollment involves several steps. First you will copy the CA root certificate into the ISE certificate store. Then you will generate a certificate signing request (CSR) in ISE. You will then present the CSR to the CA which will then issue a certificate for the ISE. Finally you will install the CA-signed ISE certificate on the ISE.

| Note | The enrollment involves several steps. First you will copy the CA root certificate into the ISE certificate store. The ISE will generate a CSR. Then the CA will issue a certificate for the ISE in response to the CSR. Finally you will install the CA-signed ISE certificate on the ISE. |
|---|---|

### Activity Procedure

Complete the following steps:

#### *Step 1*

Download the CA root certificate from the HQ-SRV to the Admin-PC. This will allow you to load the CA root certificate onto the ISE in the next step.

A) On the **Admin-PC**, open a new tab in the Internet Explorer and navigate to **http://hq-srv.secure-x.local:5080/certsrv**. You should be prompted for credentials. Log in as **administrator** with the password **Ci5coAdmin**.

B) Click the **Download a CA Certificate, Certificate Chain, or CRL** link.

C) Select the default encoding method (**DER**), and click the **Download CA Certificate** link. Click **Save**, and save the file as **ca-cert.cer** on the C:\ disk.

D) Close the Download complete window.

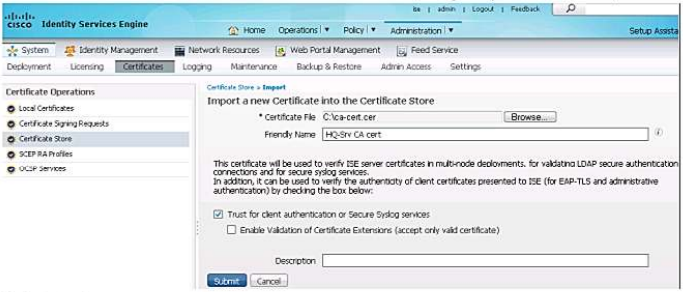
***Step 2***

Install the CA root certificate on Cisco ISE:

A) If you haven't already, log in to ISE using **admin** and **Ci5coAdmin** as the credentials.

B) In the Cisco ISE GUI, navigate to **Administration > System > Certificates > Certificate Store**. Above the Certificate Store table, click **Import** and install the CA certificate:

- Click **Browse** and select the locally saved CA root cert file (**C:\ca-cert.cer**).
- Set the **Friendly Name** to **HQ-SRV CA cert**.
- Check the **Trust for client authentication or secure Syslog services** check box.
- Do **not** click **Enable Validation of Certificate Extensions** (accept only valid certificate).




- Click **Submit**.

C) Examine the certificate: Select the **HQ-SRV CA cert** via it's check box and click **Edit.** You should see that this is the root certificate signed by the CA itself. The subject is the same as issuer (DC=local,DC=secure-x,CN=HQ-SRV-CA.)

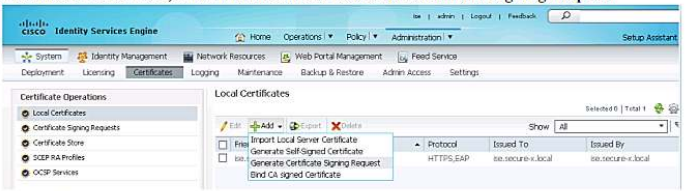

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

Generate a Certificate Signing Request on Cisco ISE:

A CSR is message given to a CA that contains the identity information including public key of the requesting system. The CA will use this data to build an identity certificate for the requesting system and then sign that certificate with the CA's own private key. You will generate a CSR in this step.

A) Using the Certificate Operations pane on the left side of the window, select **Local Certificates**. Above the Local Certificates table, click **Add** and choose **Generate Certificate Signing Request**.




B) Enter the following parameters in the Generate Certificate Signing Request form:

**Certificate Subject: CN=ise.secure-x.local**

**Key Length: 2048**

**Digest to Sign WIth: SHA-256**

C) Click **Submit**. Click **OK** on the notification window.

D) In the **Certificate Operations** pane on the left, choose **Certificate Signing Requests**.

E) Check the CSR that you just created and click **Export**. Save the file as **ise-csr.pem** on the C:\ disk.

***Step 4***

Enroll the ISE with the CA:

You now have a CSR with ISE's identity information, including ISE's public key on the Admin-PC. In this step you will provide this CSR to the HQ-SRV CA, it will generate an identity certificate and sign it with its private key. You will thenl download that certificate to the Admin-PC.

A) In the Internet Explorer browser tab for http://hq-srv.secure-x.local:5080/certsrv, click the **Home** link in the upper right corner.

B) Click the **Request a Certificate** link, click the **Advanced Certificate Request** link, and then click the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file**... link.

C) Open **WordPad** and open the **C:\ise-csr.pem** file.

| **Note** | In WordPad, you can choose **All Documents (*.*)** to display the .pem files. |
|---|---|

D) Select all of the text in the document and copy the entire contents of the CSR to the Windows clipboard. Paste it into the text box in the **Saved Requests** section of the CSR request form.

E) In the **Certificate Template** drop-down list, choose **Web Server**.

F) Click **Submit**.

G) With **DER** selected, click **Download Certificate** and save the certificate as C:**ise-cert.cer**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

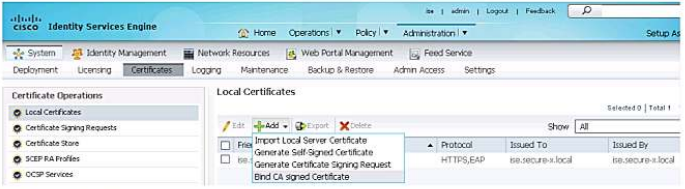
***Step 5***

Install the Cisco ISE certificate:

Now you have a signed identity certificate for ISE on the Admin-PC. You will upload this certificate and install it in ISE in this step.

A) In the Cisco ISE GUI, you should still be at **Administration > System > Certificates**. In the **Certificate Operations** pane on the left, select **Local Certificates**.

B) Above the Local Certificates table Click **Add** and then select **Bind CA Certificate** in the drop-down list.




C) Enter these options:

**Certificate File**: C:**ise-cert.cer** (You can use the Browse button to select this file)

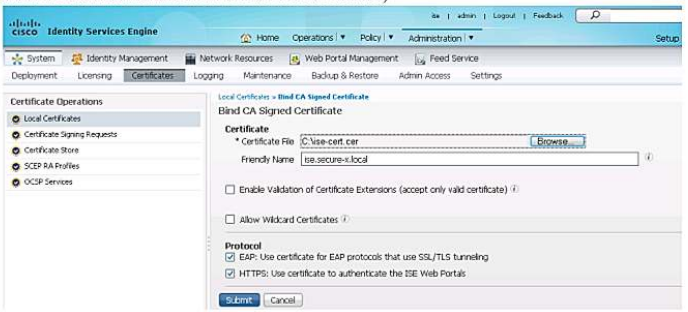
**Friendly Name**: **ise.secure-x.local**

**Enable Validation of Certificate Extensions**: [ ] <leave blank>

**Allow Wildcard Certificates**: [ ] <leave blank>

**EAP**: [X] <checked>

**HTTPS**: [X] <checked> (Checking this will cause a notification indicating that the application server will have to restart. Click **OK** on the notification)




D) Click **Submit**. You will receive a notification that the system will restart. Acknowledge the notification.

E) You are returned to an ISE login screen. Wait a couple minutes while ISE restarts. Log back in using **admin** and **Ci5coAdmin** as the credentials. Once you can successfully log in, proceed to the next task.


https://t.me/learningnets

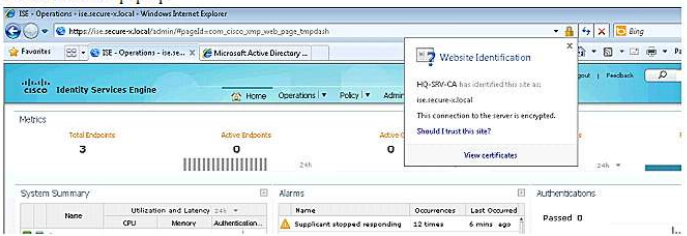
# Task 4: Task 4: Explore System Behavior after ISE PKI Enrollment

Now that ISE is using an identity certificate that was signed by the HQ-SRV CA, and both the Admin-PC and the Employee-PC have the root certificate of the HQ-SRV CA in their certificate stores, both systems should trust ISE. In this task you will verify that there are no longer SSL certificate warnings in IE and that the Employee-PC can successfully authenticate via 802.1X.

### Activity Procedure

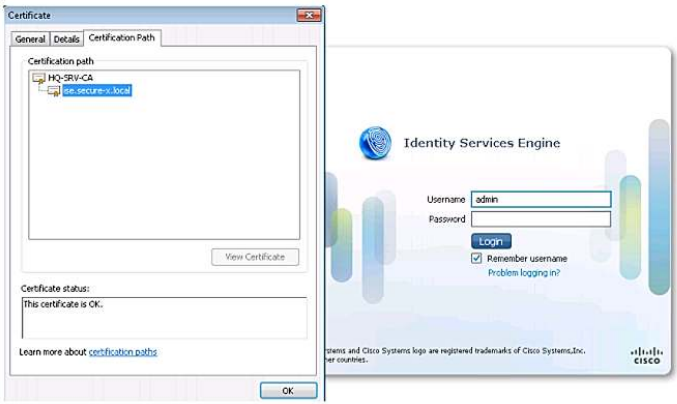
#### *Step 1*

You may not even have noticed, but the URL entry field on IE should no longer be red. Also, it should no longer indicate a certificate error. Click the HTTPS lock icon to the right of the URL entry field to view the website identification pop up.




#### *Step 2*

Click **View Certificates** and examine the three tabs: General, Details, and Certification Path. You should see that the ISE certificate has been signed by HQ-SRV-CA. Close the Certificate window when you are done.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Access the HQ-SW console. As you did before, to ensure that there are no timing issues with when the last reauthentication attempt happened, disable and then enable interface G0/1 on the HQ-SW. Note that the 802.1X authentication process immediately begins, and this time it succeeds.

```
HQ-SW# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-SW(config)# int g0/1
HQ-SW(config-if)# shutdown
Nov 20 21:25:26.253: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down
Nov 20 21:25:27.260: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed
state to down
Nov 20 21:25:35.312: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
HQ-SW(config-if)# no shut
Nov 20 21:25:38.256: %AUTHMGR-5-START: Starting 'dot1x' for client (a036.9f1a.3dad)
on Interface Gi0/1 AuditSessionID 0A0A0202000000BA2058353F
Nov 20 21:25:38.475: %DOT1X-5-SUCCESS: Authentication successful for client
(a036.9f1a.3dad) on Interface Gi0/1 AuditSessionID 0A0A0202000000BA2058353F
Nov 20 21:25:38.475: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x'
for client (a036.9f1a.3dad) on Interface Gi0/1 AuditSessionID 0A0A0202000000BA2058353F
Nov 20 21:25:38.995: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(a036.9f1a.3dad) on Interface Gi0/1 AuditSessionID 0A0A0202000000BA2058353F
Nov 20 21:25:40.211: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Nov 20 21:25:41.217: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
HQ-SW(config-if) # end
```


https://t.me/learningnets

### Step 4

On the HQ-SW, examine the authentication status of port GigabitEthernet0/1. Again, you should see that authentication has succeeded.

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/1
           Interface:  GigabitEthernet0/1
         MAC Address:  a036.9f1a.3dad
          IP Address:  10.10.9.21
           User-Name:  student
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
        Vlan Policy:  N/A
     Session timeout:  N/A
       Idle timeout:  N/A
   Common Session ID:  0A0A0202000000BA2058353F
     Acct Session ID:  0x00000084
              Handle:  0x390000BB
Runnable methods list:
      Method   State
      dot1x    Authc Success
```

### Step 5

On the Admin-PC, in the Cisco ISE GUI, navigate to **Operations > Authentications**. Verify that the PEAP authentication of user student is now successful. Use the **Add** or **Remove** columns button to adjust your view. With repeated access attempts, the counter in the top-most line will increment to represent multiple occurrences of the last authentication result.

**Note** The client does not reject the ISE certificate any longer, because the ISE is using a certificate issued by the HQ-SRV-CA. The Employee-PC can validate the ISE certificate because the HQ-CA root certificate has been pre-installed on the Admin-PC in the certificate store.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 2-2: Implement MAB and Internal Authentication

## Activity Objective

In this lab exercise you will deploy MAC Authentication Bypass (MAB) and the Cisco AnyConnect 802.1X supplicant to secure the access layer in your lab infrastructure. First you configure the switch to enable MAB on the interface where a print server is connected. You create an endpoint in the ISE endpoint database and verify the MAB operation. When you install the Network Access Manager (NAM) on the Employee-PC, you will see that the default EAP-FAST authentication fails because the AnyConnect supplicant does not trust the ISE certificate. Finally you configure the NAM to trust the CA root certificate and verify successful user authentications using EAP-FAST with EAP-MSCHAPv2 as the inner protocol.

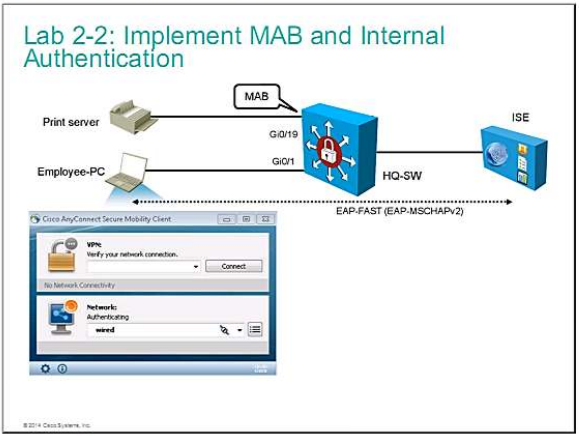
Upon completing this exercise, you will be able to:

- Deploy MAB
- Deploy the AnyConnect supplicant
- Configure Network Access Manager profile to trust CA root certificate

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

## Commands

| Command | Description |
|---|---|
| **authentication host-mode multi-auth** | Allows more data clients to independently authenticate on an authorized port. Each host, or MAC address, is authenticated individually. |
| **authentication open** | Enables preauthentication open access (low impact or monitoring modes). |
| **authentication port-control auto** | Enables port-based authentication on the interface |
| **dot1x pae authenticator** | Enables 802.1X authentication on the interface |
| **dot1x system-auth-control** | Globally enables 802.1X port-based authentication. |
| **mab** | Enables MAB. |


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 1: Deploy MAC Authentication Bypass

In this task you will implement MAB for the print server attached to switch interface GigabitEthernet 0/19. Having established an authentication infrastructure for 802.1X-based access you will now provide access to devices that do not support 802.1X, such as printer servers. In the lab topology, a print server is connected to the GigabitEthernet 0/19 interface of the access switch. You will enable MAB on the switch, and add the print server MAC address to the endpoint database on the ISE. When you enable MAB on the switch, the access attempt will be made with the client username set to the print server MAC address. If the MAC address exists in the ISE endpoint database, the authentication will succeed.

### Activity Procedure

Complete the following steps:

#### *Step 1*

On the switch, copy the 802.1X settings of interface GigabitEthernet0/1 to interface **GigabitEthernet0/19**.

```
interface GigabitEthernet0/19
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 dot1x pae authenticator
 dot1x timeout tx-period 10
```


https://t.me/learningnets

### *Step 2*

Examine the 802.1X authentication results on the switch. Since the print server does not have an 802.1X supplicant, authentication will fail. This step has you observe the status while 802.1X is running and after it times out. This only takes 90 seconds. If you missed some of the status documented here and would like to reproduce the behavior, you can disable and then re-enable the interface on the switch.

A You may have noticed a Syslog message similar to this, indicating that 802.1X authentication has started.

```
Nov 22 15:12:28.351: %AUTHMGR-5-START: Starting 'dot1x' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000000230324E3E6
```

B Use the **show authentication sessions** command to view authentication status of the interface.

```
HQ-Sw# show authentication sessions int g0/19
            Interface:  GigabitEthernet0/19
          MAC Address:  0014.bf66.fb84
           IP Address:  Unknown
               Status:  Running
               Domain:  UNKNOWN
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000230324E3E6
      Acct Session ID:  0x00000026
               Handle:  0x91000024
Runnable methods list:
       Method   State
       dot1x    Running
```

C Ninety seconds after the authentication process started, Syslog messages similar to the following indicate that authentication has timed out and failed.

```
Nov 22 15:14:01.021: %DOT1X-5-FAIL: Authentication failed for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000000230324E3E6
Nov 22 15:14:01.021: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'dot1x' for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000000230324E3E6
Nov 22 15:14:01.021: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000000230324E3E6
Nov 22 15:14:01.021: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication
methods for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000000230324E3E6
Nov 22 15:14:01.021: %AUTHMGR-5-FAIL: Authorization failed or unapplied for
client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000000230324E3E6
```

D Showing the authentication sessions again, you should see that the current status is, indeed, failed.

```
HQ-Sw# show authentication sessions int g0/19
            Interface:  GigabitEthernet0/19
          MAC Address:  0014.bf66.fb84
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
           IP Address:  Unknown
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000000230324E3E6
      Acct Session ID:  0x00000026
               Handle:  0x91000024
Runnable methods list:
       Method   State
       dot1x    Failed over
```

E Remember, though, everything is still configured for monitor mode. Failed authentication does not impact connectivity. Using the **show interface status** command, you can see that the port is connected. Attempting to **ping** the print server (10.10.10.99), you will find its IP address is reachable.

```
HQ-Sw# show interface g0/19 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/19                       connected    10         a-full  a-100
10/100/1000BaseTX
HQ-Sw#ping 10.10.10.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

### *Step 3*

In the Cisco ISE GUI, verify that there are no authentication attempts through that port in the **Operations > Authentications** page.

**Note** You do not see any authentication attempts because the print server does not respond to EAPoL frames from the switch. You can examine the Authentication result 'no-response' from 'dot1x' for client (...) on Interface Gi0/19 messages on the switch. There is no fallback to MAB, because MAB is not yet enabled on the port.

***Step 4***

Configure MAB on the print server port:

A) Enable MAB.

B) Set the authentication order to MAB > 802.1X. This will ensure that MAB and WebAuth processing is not delayed for the tx-period until 802.1X fails.

C) Set the authentication priority to 802.1X > MAB. This will ensure that 802.1X has higher priority even if MAB succeeds.

```
interface GigabitEthernet 0/19
 mab
 authentication order mab dot1x
 authentication priority dot1x mab
```

| **Note** | In a production deployment, it is recommended to configure access ports in a consistent fashion. You would normally configure 802.1X and MAB on all access ports. In this lab, MAB was intentionally not configured at first to allow you to see the behavior of the 802.1X system when there isn't a supplicant on the endpoint. |
|---|---|

| **Note** | Configuring MAB first in the authentication order makes authentication quicker for devices that do not have a supplicant But if there is a supplicant, having MAB first consumes resources with the MAB authentication attempt. In situations where an 802.1X supplicant is expected more often than not, it is better to have 802.1X before MAB in the authentication order. |
|---|---|


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 5*

Examine the MAB authentication results on the switch.

A You may have noticed Syslog messages similar to this which indicate that MAB was attempted and failed. The interface is now properly configured for MAB, but ISE does not know the MAC address of the print server yet.

```
Nov 22 18:12:52.359: %AUTHMGR-5-START: Starting 'mab' for client (0014.bf66.fb84)
on Interface Gi0/19 AuditSessionID 0A0A01020000000230324E3E6
Nov 22 18:12:52.393: %MAB-5-FAIL: Authentication failed for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A01020000000230324E3E6
Nov 22 18:12:52.393: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'mab' for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A01020000000230324E3E6
Nov 22 18:12:52.393: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A01020000000230324E3E6
Nov 22 18:12:52.393: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication
methods for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A01020000000230324E3E6
Nov 22 18:12:52.401: %AUTHMGR-5-FAIL: Authorization failed or unapplied for
client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A01020000000230324E3E6
```

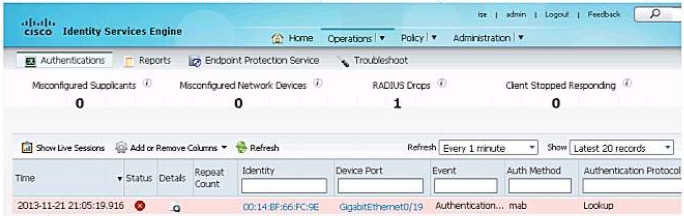
B Use the **show authentication sessions** command to view authentication status of the interface. Note that both 802.1X and MAB have failed.

```
HQ-Sw# show authentication sessions int g0/19
            Interface:  GigabitEthernet0/19
          MAC Address:  0014.bf66.fb84
           IP Address:  10.10.10.99
            User-Name:  0014bf66fb84
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000000230324E3E6
      Acct Session ID:  0x00000026
              Handle:  0x91000024
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
```


https://t.me/learningnets

### *Step 6*

From Admin-PC connect to the ISE GUI, navigate to **Operations > Authentications** and then click **Show Live Authentications**. Note the the failed authentication on port GigabitEthernet 0/19. You should see print server MAC address authentication attempts failing because the subject is not found in the identity store.




| **Note** | The MAC address in your pod may differ from the print server MAC address displayed in the lab guide. |
|---|---|

| **Note** | **Operations > Authentications** has two views that you can toggle between: Live Sessions and Live Authentications. The views are not directly identified. If the button Show Live Sessions is displayed, you are looking at a Live Authentications view. If the button Show Live Authentications is displayed, you are looking at a Live Sessions view. It may not be intuitive, but the button that is offered identifies the view that you can toggle to from the current view. The Live Sessions view only shows active authentication sessions. It does not display any information about failed authentication attempts. For that information you must use the Live Authentications view. |
|---|---|

### *Step 7*

Write down the MAC address of the print server in your pod:

_____


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 8*

Create an endpoint identity group named PrintServers on Cisco ISE. Endpoint groups improve organizational manageability of the system.

A) In the Cisco ISE GUI, choose **Administration > Identity Management > Groups > Endpoint Identity Groups** and click **Add**.

B) Create an endpoint identity group named **PrintServers** with no parent group. Click **Submit**.

### *Step 9*

Create an endpoint in the local endpoint identity store.

A) In the Cisco ISE GUI, choose **Administration > Identity Management > Identities > Endpoints** and click **Add**.

B) Create an endpoint with the print server MAC address, no static policy assignment, and static group assignment to the **PrintServers** group.

C) Click **Submit**.

### Activity Verification

You have completed this task when you verify that MAB works. Complete these steps:

### *Step 1*

On the switch, disable and re-enable the print server interface (g0/19). If logging is enabled you will see messages about successful MAB:

```
%AUTHMGR-5-START: Starting 'mab' for client (0014.bf66.fc9e) on Interface Gi0/19
AuditSessionID 0A0A02020000024444ECADD5
%MAB-5-SUCCESS: Authentication successful for client (0014.bf66.fc9e) on Interface
Gi0/19 AuditSessionID 0A0A02020000024444ECADD5
%AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0014.bf66.fc9e) on Interface Gi0/19 AuditSessionID 0A0A02020000024444ECADD5
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0014.bf66.fc9e) on Interface
Gi0/19 AuditSessionID 0A0A02020000024444ECADD5
```


https://t.me/learningnets

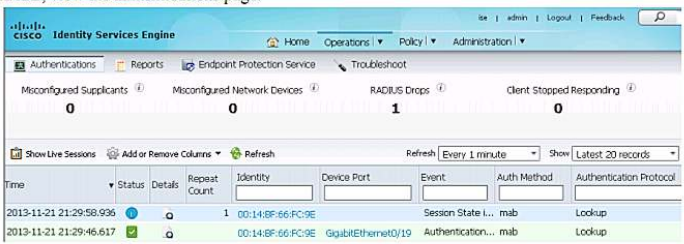
### *Step 2*

On the switch, verify the authentication status of the print server port. You should see success for a username identical to the MAC address. The MAB method resulted in authentication success and 802.1X was not run at all.

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/19
            Interface:  GigabitEthernet0/19
          MAC Address:  0014.bf66.fc9e
           IP Address:  Unknown
            User-Name:  00-14-BF-66-FC-9E
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000024444ECADD5
      Acct Session ID:  0x00000249
               Handle:  0x5D000245
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

### *Step 3*

On the ISE, view the authentications page.




# Task 2: Deploy AnyConnect Supplicant

In this task you will install the Network Access Manager and use it for the default EAP method. The default EAP method of the AnyConnect supplicant is EAP-FAST with EAP-MSCHAPv2 as the inner protocol. The AnyConnect supplicant supports both user and machine authentication by default. At the end of this task the EAP-FAST authentication will fail, because the AnyConnect supplicant is not yet configured to trust the CA root certificate. The AnyConnect supplicant uses by default the machine certificate store to verify the EAP server certificate, and the HQ-SRV-CA root certificate is not in that store.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

On the Employee-PC, disable the native Windows 802.1X supplicant:

A) Right-click the **Network** icon in the system tray. Select **Open Network and Sharing Center**.

B) Click **Change adapter settings**. This navigates you to the Network Connections list.

C) Double-click **Local Area Connection**. Click **Properties**, select the **Authentication** tab.

D) Clear the **Enable IEEE 802.1X authentication** checkbox. Click **OK** and **Close**.

E) Close any remaining open windows.

#### *Step 2*

On the Employee-PC, install the NAM:

A) Use Windows Explorer and navigate to the **D:\AnyConnect\anyconnect-win-3.1.04059-pre-deploy-k9** folder.

B) Install the AnyConnect Security Mobility Client (**anyconnect-win-3.1.04059-pre-deploy-k9.msi** installer), which is required for NAM installation. Accept the license agreement and follow the installation wizard.

C) Install the AnyConnect NAM (**anyconnect-nam-win-3.1.04059-k9.msi** installer). Accept the license agreement and follow the installation wizard.

D) After installation finishes, you will be prompted to restart the Employee-PC. Proceed with the restart.

### Activity Verification

#### *Step 1*

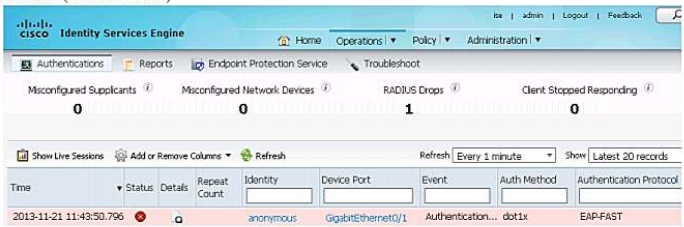
After about a minute the Employee-PC should boot and have the NAM window open. From the system tray, click on the AnyConnect icon. You should see that the supplicant is attempting to access the default network **wired**. Log on as student with password Ci5coAdmin.

| | |
|---|---|
| **Note** | If you want to reset the supplicant at any time, right-click the AnyConnect icon from the system tray and choose Network Repair. |


https://t.me/learningnets

### *Step 2*

In the Cisco ISE GUI, view the live authentications. You should see a failed access attempt from 'anonymous' on port GigabitEthernet 0/1. Anonymous is the default unprotected identity pattern of the NAM. For tunneled EAP types, the NAM differentiates between two identities: unprotected (outer tunnel) and protected (inner method.)




### *Step 3*

Click the **Details** button to examine the authentication details. You should see that the authentication failed because the supplicant rejected the EAP server certificate. By default, the NAM uses the OS certificate store to identify trusted CA root certificates. The HQ-SRV-CA root certificate is not in the machine certificate store.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 4***

Verify that the CA root certificate does not exist in the machine certificate store:

A) Access the **Employee-PC** and launch the Microsoft Management Console (**Start > mmc**).

B) Choose **File > Add/Remove Snap-in**.

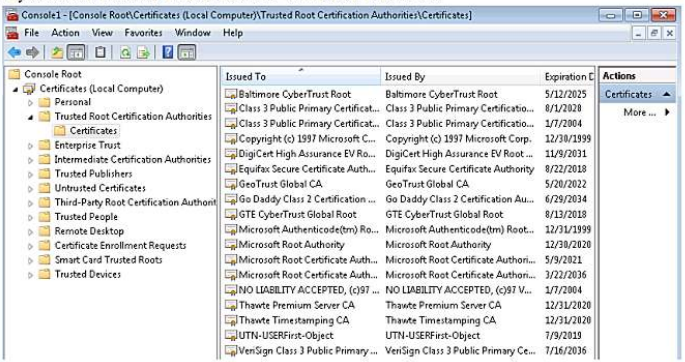
C) Choose **Certificates** from the **Available Snap-ins** list and click **Add** to move it to the **Selected Snap-ins** pane.

D) Choose **Computer account** and click **Next**.

E) Accept the **Local computer** selection and click **Finish**. Click **OK**.

F) Go to **Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**.

G) Verify that the HQ-SRV-CA root certificate is not in the list. The NAM uses this list to identify trusted PKI systems and therefore refuses the EAP connection to the ISE.




# Task 3: Configure CA Trust with the AnyConnect Profile Editor

It would be possible to install the HQ-SRV-CA root certificate into the machine Employee-PC's machine certificate store. But, we will take advantage of this opportunity to introduce the AnyConnect Profile editor. In this task you will install the Network Access Manager Profile Editor and create a profile that will enable trust in the HQ-SRV-CA root certificate. You will configure the supplicant to explicitly trust the HQ-SRV-CA certificate without using the machine certificate store. You will leave all other supplicant settings at their default values. Once the profile is saved, you will reset the supplicant and verify that it successfully performs user authentication using EAP-FAST with inner MSCHAPv2 protocol.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets

***Step 1***

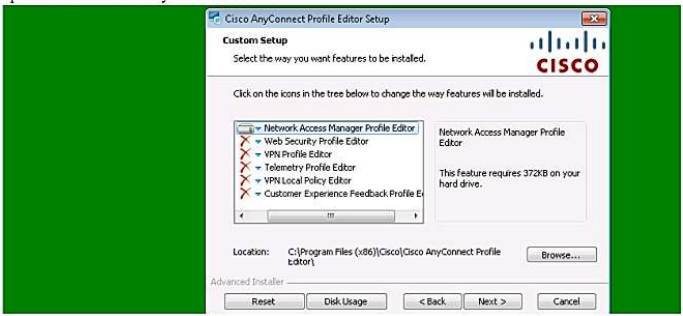
On the **Employee-PC**, install the AnyConnect Profile Editor:

A) Use Windows Explorer to view the **D:\AnyConnect** folder.

B) Run the installer (**anyconnect-profileeditor-win-3.1.04059-k9.exe**).

C) Click **Next** and choose **Custom** installation.

D) Make sure that only the default selection, the Network Profile Editor, will be installed. Click **Next** to accept the default directory. Click **Install**.





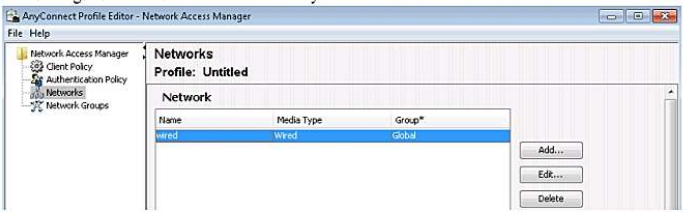
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

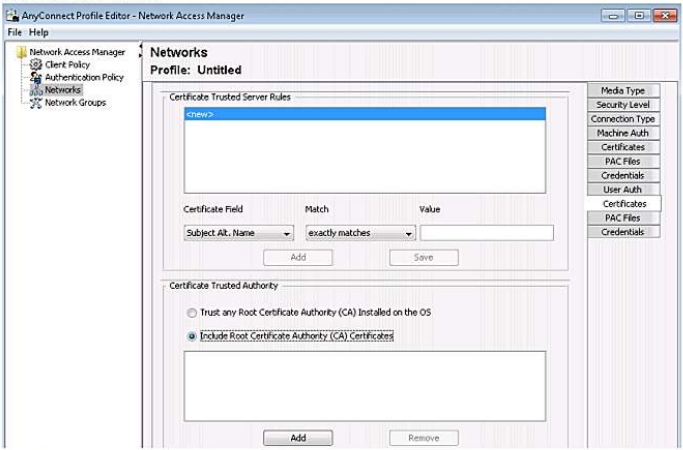
Create a profile to enable trust in the HQ-SRV-CA root certificate:

A) Launch the Network Access Manager Profile Editor (**Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Network Access Profile Editor**).

B) Go to **Network Access Manager > Networks**. In this menu you can define various networks and the 802.1X settings for each. Select the default entry '**wired**' and click **Edit**.

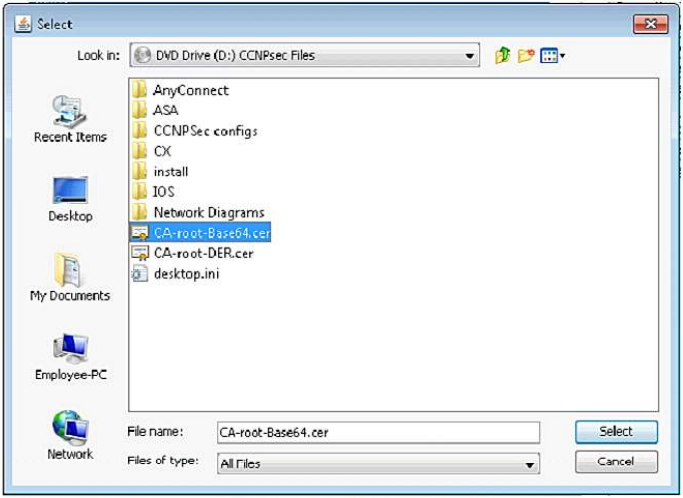



C) The profile editor provides a wizard to define all aspects of the network settings. The wizard can be navigated using the Next buttons at the bottom of each page or with the tabs on the right side of the window. We just need to edit one setting. Select the second **Certificates** tab (the one that is below the **User Auth** tab). In this section you can configure certificate trust for user authentication. In the **Certificate Trusted Authority** section, select the **Include root Certificates Authority (CA) Certificates** radio button.

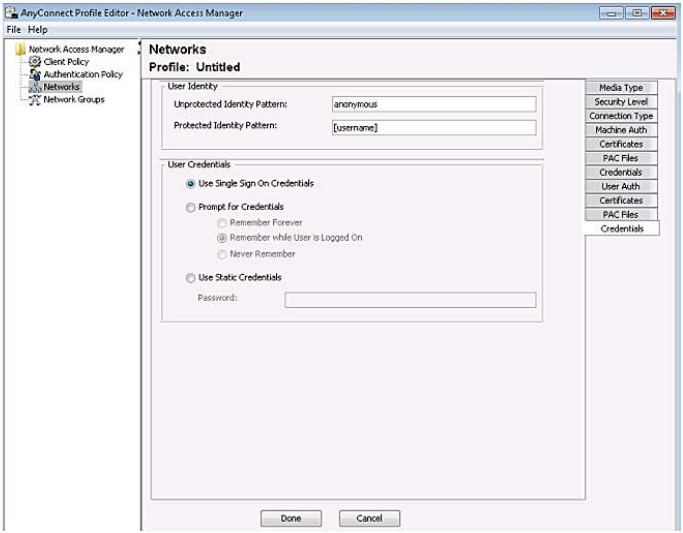



D) Click **Add** and browse to the **CA-root-Base64.cer** file on the **D:** drive. You will have to specify files of type **All Files** as the file extension is not .pem. The Base-64 format is equivalent to PEM. Microsoft certificate services uses the .cer extension by default, regardless of the certificate encoding.


https://t.me/learningnets




E) To skip to the end of the wizard, click the **Credentials** tab (the bottom tab) and click **Done**.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

F) Use **File > Save As** to save the profile. Save the profile as **configuration.xml.** You must use this naming convention without changing the path to which the file is saved. This file will be temporary. If properly named, the profile editor will immediately process the file, update the AnyConnect profile, and delete this temporary file. If it is not properly named, the file will be ignored by the profile editor.

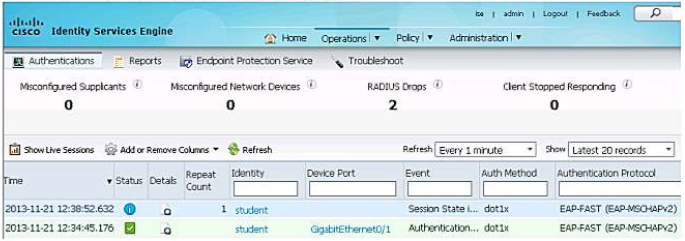
### Activity Verification

#### *Step 1*

From the system tray on the **Employee-PC**, right-click the **AnyConnect** icon and select **Network Repair** to reset the supplicant. A logon pop-up window should show. Log in as **student** with password **Ci5coAdmin**.

#### *Step 2*

In the Cisco ISE GUI, verify successful user authentication.




#### *Step 3*

Click the **Details** button on the authentication record. Amongst the authentication details you should see that the **EAP Tunnel Method** is **EAP-FAST**, and that the **EAP Authentication Method** is **EAP-MSCHAPv2**.


https://t.me/learningnets

### *Step 4*

On the switch, verify the authentication status of the access interface:

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.11
            User-Name:  student
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000023843006822
      Acct Session ID:  0x00000239
               Handle:  0xBF000239
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

### *Step 5*

Verify IP connectivity from the Employee-PC. For example, use IE to browse **http://hq-srv**. You should find that you have full network connectivity.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 2-3: Implement External Authentication

## Activity Objective

Most enterprises deploy a scalable authentication infrastructure and authenticate the clients against a centralized user repository. The most common authentication database in enterprise environments is the Active Directory. In this exercise you will integrate the Cisco Identity Services Engine with the Active Directory. First you will join the ISE to the Active Directory. Then you will configure an identity source sequence that authenticates the clients against the Active Directory, and if this method fails, falls back to the internal user database. At this stage you will test the authentication of domain users and see that they need to provide their credentials in the supplicant pop-up window. When you join the Employee-PC to the Active Directory, you will be able to verify that the user and machine authentication succeeds without the need to explicitly provide any credentials in the AnyConnect supplicant.

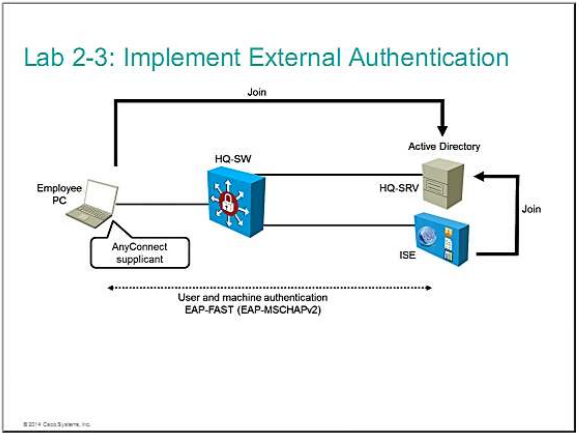
Upon completing this exercise, you will be able to:

- Join Cisco ISE to Active Directory
- Configure the ISE policy to authenticate clients against Active Directory
- Test EAP-FAST (EAP-MSCHAPv2) authentication of domain users
- Join workstation to the Active Directory domain
- Test EAP-FAST (EAP-MSCHAPv2) authentication of domain users and computers

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Join ISE to the Active Directory

In this task, you will join Cisco ISE to the Active Directory. Joining the ISE to the Active Directory will allow you to authenticate the users against the central enterprise database. Such authentication increases the manageability in larger enterprise environments.

### Activity Procedure

Complete the following steps:

#### *Step 1*

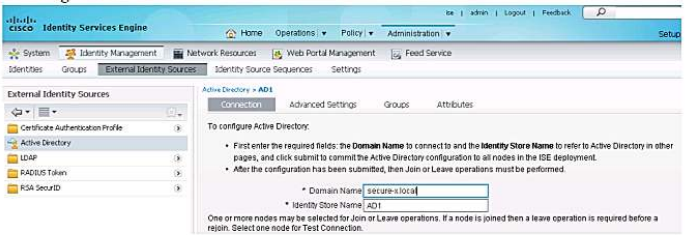
In the Cisco ISE GUI, navigate to **Administration > Identity Management > External Identity Sources** and click **Active Directory** in the left pane.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

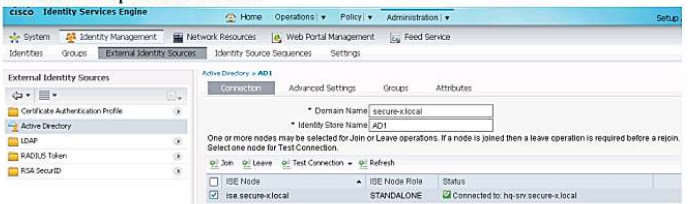
Join Cisco ISE to the Active Directory:

A) In the **Domain Name** field enter **secure-x.local**. Leave the **Identity Store Name** as **AD1** and click **Save Configuration** at the bottom.




B) Explore the two connectivity test options and then join AD:

1. Note that the current status of ise.secure-x.local is **Not Joined to Domain**.
2. Check the checkbox for the **ise.secure-x.local** node and then click select **Test Connection > Basic Test** from the toolbar. Use the credentials **administrator** and **Ci5coAdmin** and click **OK**. Accept the message about submitting the dialog. You should see **Status: SUCCESS** and **Password For User Administrator Is Correct**. Click **Close**.
3. This time select **Test Connection > Detailed Test** from the toolbar. Accept the pop-up notification. Authenticate again using **administrator** and **Ci5coAdmin** as the credentials. Examine the results. Close the test results window.
4. From the toolbar, click **Join**. Use the same credentials. After the join operation completes, close the Join Operation Status window. You should see the status for the node ise.secure-x.local is now **Connected to: hq-srv.secure-x.local**.




### Activity Verification

You have completed this task when you attain this result:


https://t.me/learningnets

### *Step 1*

Verify on the HQ server (the AD domain controller) that the ISE node is amongst the domain computers.

A Access the HQ-Srv,

B Open **Start > Administrative Tools > Active Directory Users and Computers** and navigate to the **Computers** container.

C You should see the Cisco ISE node.

### *Step 2*

Explore the computer properties of ISE in AD.

A Right click on **ise** in the computer list and select **Properties**.

B Select the **Operating System** tab. Note, from the service pack, you can see that ISE uses the Centrify plugin to tie to AD.

C Close the open windows on the HQ-Srv desktop.

# Task 2: Configure Authentication Against the Active Directory

Currently, ISE is using its internal user database for authentication of 802.1X. In this task, you will adjust the authentication policy to authenticate 802.1X access against the Active Directory database.

You will configure an identity source sequence that defines a sequence of databases that should be consulted in an attempt to authenticate a user. The authentication chain will include Active Directory and the internal user database. If the user is not found in the first database, the ISE will try the next one in the sequence.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 1***

Configure an identity source sequence named AD_Internal that lists active directory first and the internal user database second:

A) In the Cisco ISE GUI, choose **Administration > Identity Management > Identity Source Sequences**.

B) Click **Add** in the toolbar and create an entry named **AD_Internal** with these settings:

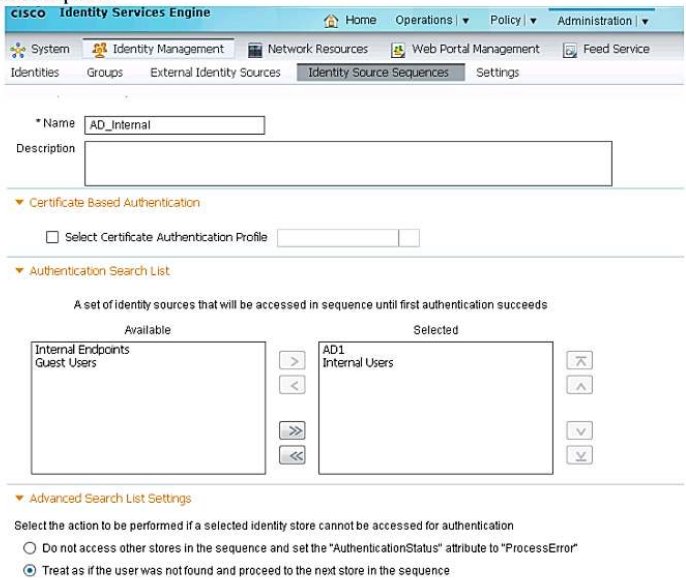
Selected in the Authentication Search List:

a) **AD1**

b) **Internal Users**

**Note** Be sure that AD1 is at the top, so the sequence will first search the AD database. It will only use the internal users database if authentication against AD fails.

Advanced Search List Settings: **Treat as if the user was not found and proceed to the next store in the sequence**.




C) **Submit** the configuration.

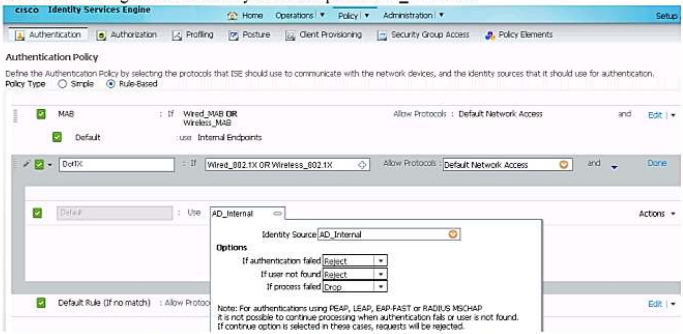
### *Step 2*

Adjust the 802.1X authentication policy, so it uses the new identity source sequence:

A) Choose **Policy > Authentication**.

B) Examine the **Dot1X** policy. Observe that the Identity Source is currently **Internal Users**.

C) Click **Edit** and change it to the identity source sequence **AD_Internal**.




D) Click **Done** to indicate that you are done with editing. Click **Save** to apply the changes.

# Task 3: Test Authentication of Domain Users

This task describes how to test the authentication of domain users.

Having joined the ISE to the Active Directory, you will now be able to authenticate as a domain user, such as it1, sales1, engineer1, or marketing1. All these domain user accounts have the same password: cisco. Because the Employee-PC is not a domain computer, you will need to explicitly authenticate the user through an authentication pop-up window of the AnyConnect supplicant.

### Activity Procedure

Complete the following steps:

### *Step 1*

On the Employee-PC, reset the NAM and authenticate as user it1 with password cisco:

A) Access the **Employe-PC**.

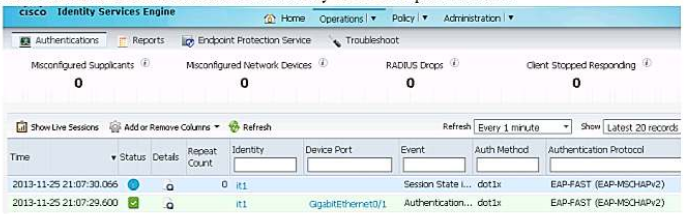
B) From the system tray, right-click the **AnyConnect** icon and select **Network Repair**. An authentication window should pop up.

C) Log in as **it1** with password **cisco**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 2

Verify the authentication in ISE. In the Cisco ISE GUI, navigate to **Operations > Authentications**. You should see a successful authentication of the identity **it1** at the top of the table.




### Step 3

Examine the authentication details: Click the **Details** link associated with the successful authentication. Note that amongst the many Authentication Details, the **Identity Store** is **AD1**. Close the report window.

### Step 4

Verify the authentication on the HQ-SW. Access the HQ-SW console and display the authentication status of the interface GigabitEthernet 0/1:

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.11
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000171F13DC4E16
      Acct Session ID:  0x00001723
               Handle:  0xFF000738
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

**Note** You may test the authentication of other domain users or administrator. The domain users are: it1, sales1, engineer1, or marketing1, all with password cisco. The domain administrator account is administrator with password Ci5coAdmin. All of these access attempts should work.


https://t.me/learningnets

| Note | An interesting optional experiment to try is to log on using the local account (**employee-pc\student** with password **Ci5coAdmin**). This ID is not defined in the Active Directory. The ISE will fall back to the internal database as the second entry in the identity source sequence. Authentication should still be successful, but if you explore the authentication details you will see that the identity store that is used is **Internal Users**. |
|---|---|

# Task 4: Join the Workstation to the Active Directory

This task describes the procedure of joining the Employee-PC to the Active Directory domain. This will enable both domain user and machine authentication. The authentication will succeed without the need to explicitly provide the client credentials in the AnyConnect supplicant pop-up window. The AnyConnect supplicant will automatically use the Windows credentials of the logged-on user and the machine credentials obtained from the domain controller during the join process.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 1***

Join the Employee-PC to the Active Directory:

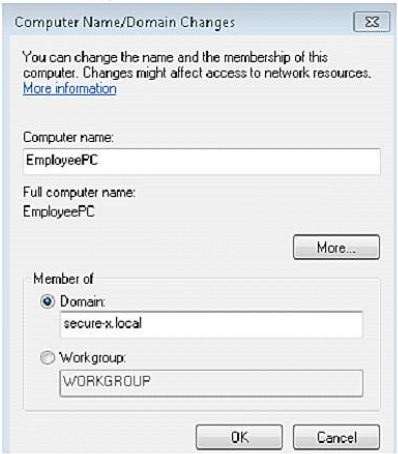
A) Access the **Employee-PC**.

B) Click **Start**, right-click **Employee-PC**, and then click **Properties**.

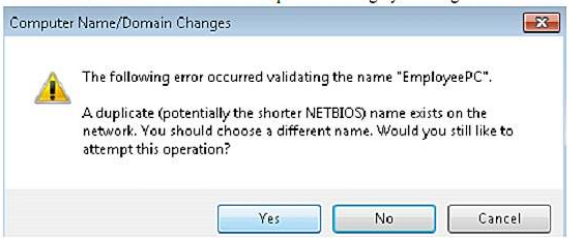
C) In the right hand pane, under **Computer Name, Domain, and Workgroup Settings**, find and click **Change Settings**.

D) Select the **Computer Name** tab and then click **Change**.

E) Under **Member of**, select **Domain**. Type **secure-x.local**, and then click **OK**.




F) You may be warned about the name conflict. Accept the warning by clicking **Yes**.




G) Authenticate as **Administrator** with the password **Ci5coAdmin** to join the domain.

H) Click **OK** on the welcome notification.

I) Once you are successfully joined to the domain, you will be prompted to restart your computer. Accept the notification and **Restart Now**.


https://t.me/learningnets

# Task 5: Test User and Machine Authentication Using Windows Credentials

Having joined the Employee-PC to the Active Directory domain you will now test domain user and machine authentication. The authentication will succeed without the need to explicitly provide the client credentials in the AnyConnect supplicant pop-up window. The AnyConnect supplicant will automatically use the Windows credentials of the logged-on user. When the user is logged off the supplicant will attempt the AD machine credentials.

### Activity Procedure

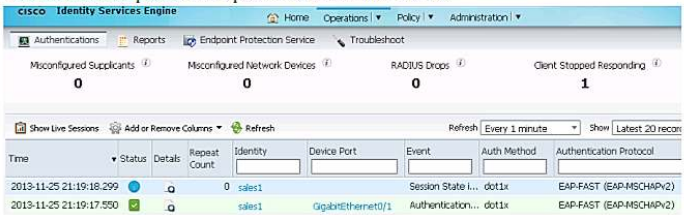
Complete the following steps:

#### *Step 1*

Log on to Employee-PC as domain user **sales1** with password **cisco**. The AnyConnect supplicant should automatically connect using the logged-on user and its Windows credentials.

#### *Step 2*

As you have done before, verify the authentication status using **Operations > Authentications** in the ISE GUI. You should see a successful EAP-FAST (EAP-MSCHAPv2) authentication of the domain user. The inner EAP-MSCHAPv2 protocol uses password-based authentication.

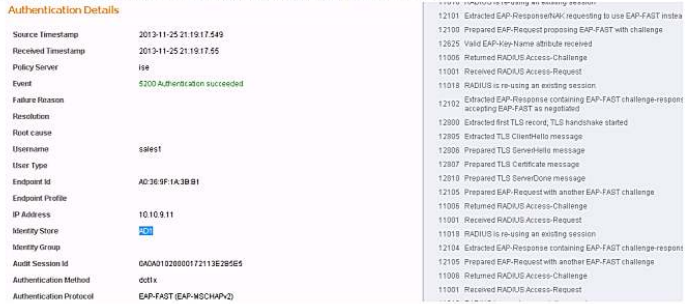




https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 3

Click the **details** button, go to the Authentication Details section of the report and examine the identity store field. You should see that the user was authenticated against the AD.




### Step 4

Log off from the Employee-PC. Verify the authentication information in the ISE GUI. You should see a successful authentication of the Employee-PC.

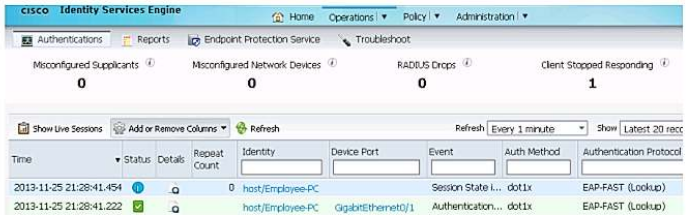
Log off from the Employee-PC.

Return to **Operations > Authentications** in the ISE GUI. You may have to use the **Refresh** button. You should see a record of a successful authentication of **host/Employee-PC**.

---

**Note** The machine authentication is successful because the Employee-PC was provisioned with machine credentials when it was enrolled with the domain controller. The AnyConnect supplicant automatically attempts machine authentication when no user is logged on.

---




### Step 5

Click the **Details** button and verify that the Employee-PC has been authenticated using the identity store AD1. Close the report window.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 3-1: Implement EAP-TLS

## Activity Objective

In this lab exercise you will deploy EAP-TLS. EAP-TLS uses certificate-based client authentication, in contrast to EAP-MSCHAPv2, which has been used in the previous exercises. EAP-MSCHAPv2 is based on password-based client authentication. EAP-MSCHAPv2 has been deployed as the inner authentication protocol, protected by an outer TLS tunnel - first with PEAP (default in native Windows supplicant), and then EAP-FAST (default in AnyConnect supplicant). EAP-TLS is an open IEEE standard that scales well and can be used in environments that don't have Active Directory. There is some management overhead to provision certificates for clients, but given the popularity of the BYOD movement, this can often be an advantage. Controlling what devices can enroll with the PKI controls exactly what devices can connect to the network. While it is beyond the scope of this lab, it is good to be aware that Cisco ISE provides many features to solve issues with BYOD solutions, including automating the provisioning of BYOD endpoints.

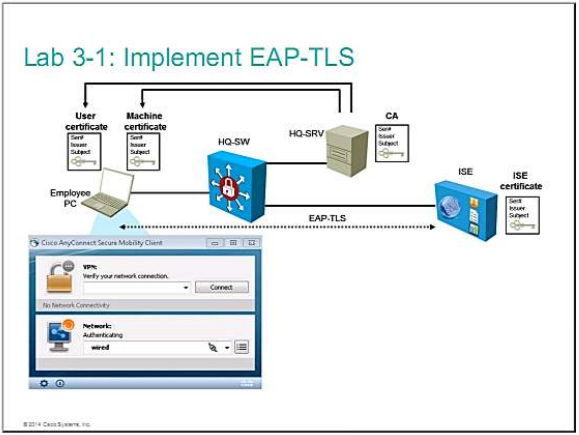
Upon completing this exercise, you will be able to:

- Install user and machine certificates on the Employee-PC
- Configure the AnyConnect supplicant for EAP-TLS
- Configure a certificate authentication profile
- Apply the certificate authentication profile to an identity source sequence
- Test EAP-TLS authentication

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Configure Employee-PC for EAP-TLS

Having used password-based user authentication in the 802.1X environment, you will now deploy certificate-based client authentication. You will first install machine and user certificates on the Employee-PC. Then you will configure the AnyConnect supplicant on the Employee-PC to use EAP-TLS.

### Activity Procedure

Complete the following steps:

#### *Step 1*

The domain administrator account has privileges to request machine certificates, so you will use this ID for this lab. Log in to the Employee-PC as the domain administrator **secure-x\administrator** with the password **Ci5coAdmin**.

| | |
|---|---|
| **Note** | You must use the domain prefix when entering the domain administrator username. Otherwise the PC will attempt to authenticate a local user. |


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

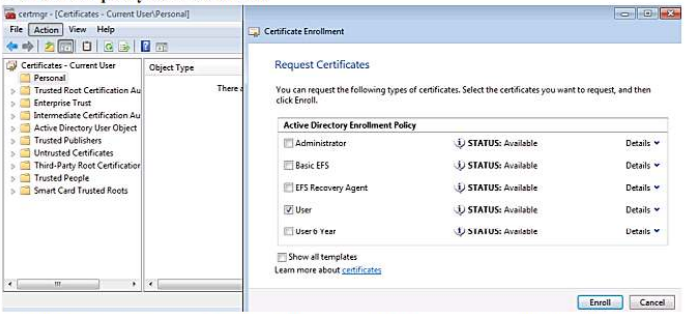
Use the Certificate Manager console to install the user certificate in the user certificate store:

A) Click **Start**, and enter **certmgr.msc** into the **Search programs and files** field, then press **<Enter>**.

B) In the **certmgr**, choose **Certificates - Current User > Personal** and observe that the user has no certificate.

C) Choose **Action > All Tasks > Request New Certificate**. Follow the wizard (**Next > Next**).

D) Choose the **User policy** and click **Enroll**.




E) Click **Finish**. Optionally you can double click on the certificate received for the **Administrator**, and examine the results. Close all open windows on the Employee-PC.

***Step 3***

Install the machine certificate in the machine certificate store using the Microsoft Management Console (MMC).

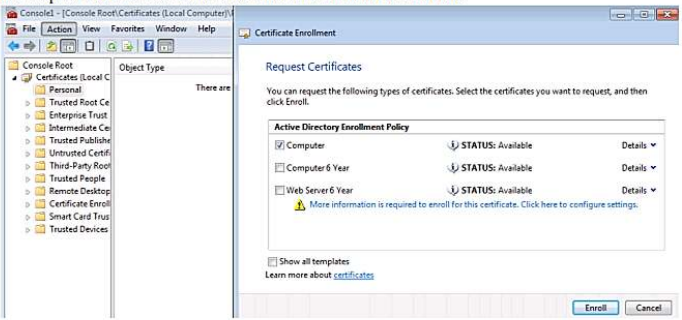
A) Launch the MMC utility: Click **Start**, and enter **mmc** into the Search programs and files field, then press **<Enter>**.

B) Add the Computer Account Certificate snap-in to the console. In the console window, click **File > Add/Remove Snap-in** and choose **Certificates** and **click Add >**. Select **Computer account** and click **Next**. Select **Local Computer** and click **Finish**. Click **OK** to close the Add or Remove Snap-ins window.

C) In the console window, navigate to **Console Root > Certificates (Local Computer) > Personal** and verify that there is no machine certificate.

D) Choose **Action > All Tasks > Request New Certificate**.

E) Follow the wizard. Click **Next** on the first window and **Next** on the second window. Select **Computer** on the Request Certificates window and then click **Enroll** and **Finish**.




F) Again you can optionally double click on the certificate to examine its details. Close all open windows when you are done. You do not need to save the settings of the console.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

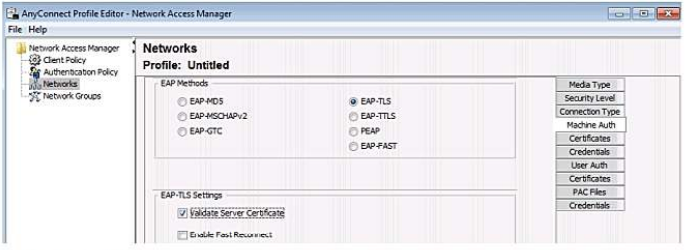
***Step 4***

Configure the AnyConnect supplicant to use EAP-TLS:

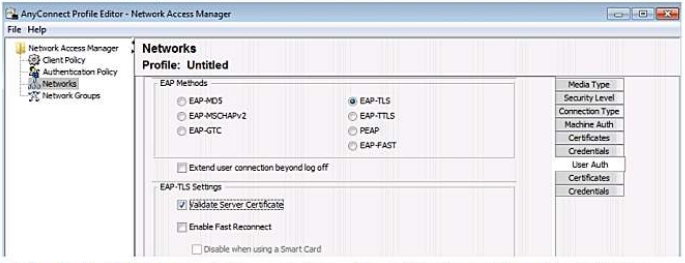
A) Open the NAM Profile Editor from the desktop via **Start > Cisco > Cisco AnyConnect Profile Editor > Network Access Manager Profile Editor**.

B) Navigate to **Network Access Manager > Networks**. Select the default entry '**wired**' and click **Edit**.

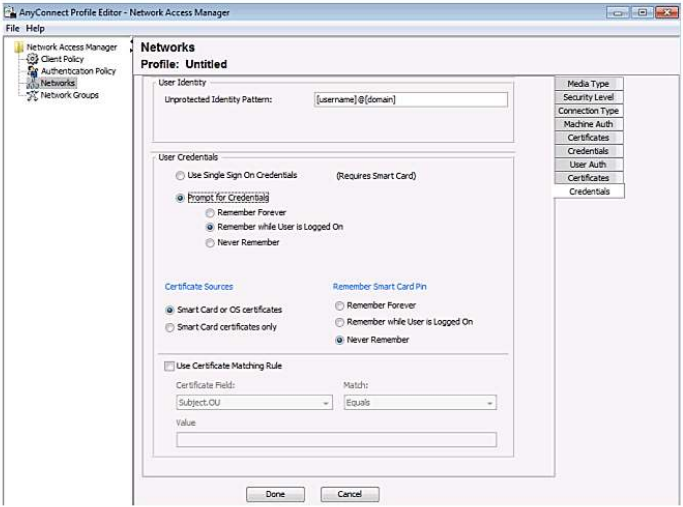
C) You only need to modify a few options that are available in the profile editing wizard. Select the **Machine Auth** tab, choose **EAP-TLS** and check the **Validate Server Certificate** checkbox.




D) Select the **User Auth** tab, choose **EAP-TLS** and check the **Validate Server Certificate** checkbox.




E) Select the **Credentials** tab at the bottom, and choose **Prompt for Credentials** option in the User Credentials section. This option enables the supplicant to use the user certificate store instead of a smart card. Leave all other settings at their default values.




F) Click **Done**. Use **File > Save As** to save the profile. Save the profile as **configuration.xml**. You must use this naming convention without changing the path to which the file is saved. This file will be temporary. If properly named, the profile editor will immediately process the file, update the AnyConnect profile, and delete this temporary file. If it is not properly named, the file will be ignored by the profile editor.

G) Close the Profile Editor window.

# Task 2: Configure ISE for Certificate-Based Client Authentication

Having obtained client certificates, you need to configure the ISE to extract the desired principal username from the certificate. This is done using the certificate authentication profiles. You will now configure a certificate authentication profile that sets the principal username to the certificate common name. Then you will apply the apply the certificate authentication profile to the identity source sequence AD_Internal, which is consulted for 802.1X access attempts. Consequently, when EAP-TLS clients present their certificates to the ISE, the ISE will extract the common name from the client certificate and display it as the username in the authentication page. The common name will also be used for other purposes, such as authorization.

### Activity Procedure

Complete the following steps:

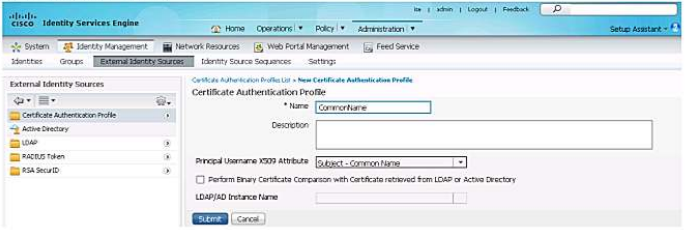

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 1*

In the Cisco ISE GUI, create a certificate authentication profile:

A) Choose **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**, then click **Add**.

B) Specify **CommonName** as the profile Name and select **Subject - Common Name** as the Principal Username X.509 Attribute.

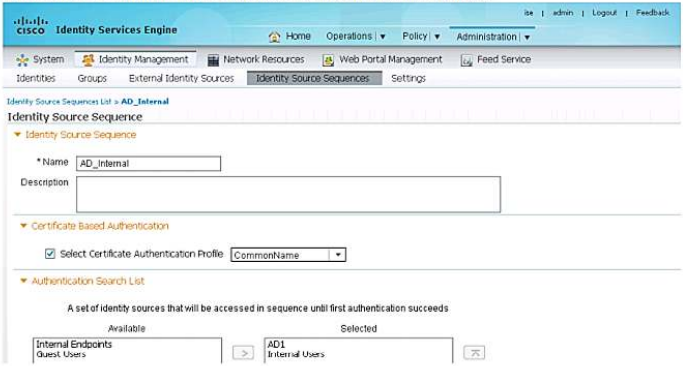



**Note** The certificate authentication profile defines which username you will see for a certificate-authenticated client.

C) **Submit** the configuration.

### *Step 2*

Adjust the identity source sequence AD_Internal: Navigate to **Administration > Identity Management > Identity Source Sequences**. Select **AD_Internal** and click **Edit**. Check **Select Certificate Authentication Profile** and select **CommonName** in the drop-down list. **Save** the changes.





https://t.me/learningnets

# Task 3: Test EAP-TLS

Having installed both user and machine certificates on the Employee-PC, you will now test that the EAP-TLS succeeds for both user and machine authentication.

### Activity Procedure

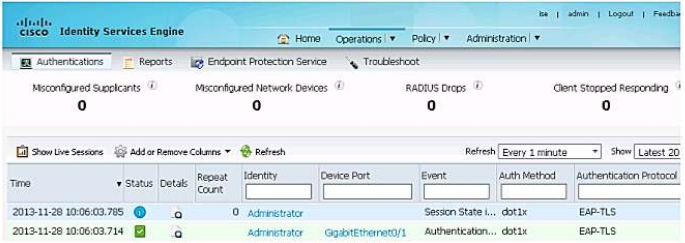
Complete the following steps:

#### *Step 1*

On the **Employee-PC**, reset the AnyConnect profile by right-clicking the **AnyConnect** icon from the system tray and choosing **Network Repair**.

#### *Step 2*

In the Cisco ISE GUI, verify a successful user authentication using EAP-TLS, which uses a user certificate for client-side authentication. The certificate common name (Administrator) appears as the client identity.




#### *Step 3*

Log off from the Employee-PC. In the Cisco ISE GUI, you should see a successful EAP-TLS authentication. The common name of the machine certificate (EMPLOYEE-PC.secure-x.local) is displayed as the identity name.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| | |
|---|---|
| **Note** | This lab was performed with the domain administrator account on the Employee-PC. Under the lab circumstances, this was the easiest way to request a machine certificate for the Employee-PC. The domain users do not have that privilege. At this point, after successful EAP-TLS implementation for the domain administrator, it is possible to implement EAP-TLS for other accounts, but the method is tricky. If you log on to the Employee-PC using one of the domain user accounts (for example it1 with the password **cisco**), there won't be a user certificate available for that user. As such, AnyConnect won't allow the network connection. Note, the connectivity restriction is not from ISE or the switch. Remember that the switch is still configured for monitor mode, so it will allow access even for failed authentications. The issue is with AnyConnect. If you have time and would like the challenge, you can certainly login as a domain user, revert the AnyConnect profile to EAP-FAST, request a user certificate for the domain user, and reconfigure AnyConnect back to EAP-TLS. The implementation of EAP-TLS was solely for demonstration. The authentication environment will switch to EAP-FASTv2 with EAP chaining in the next lab. |


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 3-2: Implement Authorization

## Activity Objective

In this lab exercise you will change the 802.1X deployment mode to low-impact and the EAP method of the Employee-PC to EAP-FAST(EAP-MSCHAPv2) with EAP chaining. You will retrieve the user groups from the Active Directory and configure the authorization on the Cisco Identity Services Engine. The authorization policy will contain conditions that check which group a user belongs to and whether they use corporate-owned endpoints. You will also configure authorization for local ISE users and for the print server that leverages MAB as the access method.

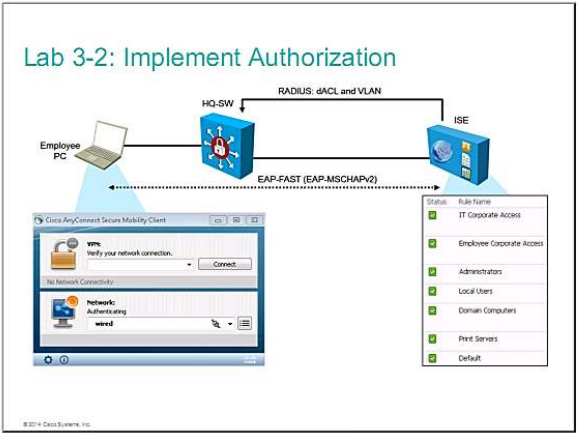
Upon completing this exercise, you will be able to:

- Enable EAP chaining
- Configure the switch for AAA authorization and 802.1X low-Impact mode
- Retrieve user groups from Active Directory
- Configure authorization for users and endpoints

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Command List

The table describes the commands that are used in this activity. The commands are listed in alphabetical order so that you can easily locate the information that you need. Refer to this list if you need configuration command assistance during the lab activity.

## Commands

| Command | Description |
|---|---|
| **aaa authorization network default group radius** | Enables VLAN and dACL assignment. |

# Task 1: Enable EAP Chaining

Most EAP methods either authenticate the user or authenticate the machine. It is common to authenticate the machine when the OS is booted but no user is logged in. When a user logs in, the authentication switches to authenticating the user. EAP chaining allows you to authenticate the user and the machine simultaneously. This is powerful when it is time to define authorization policy. You may provide different privileges when they are logged in from their corporate laptop than you would for that same user logged in from a personal laptop.

In this task you will enable EAP chaining in the Employee-PC supplicant and in the allowed protocols on the ISE. The AnyConnect supplicant supports EAP chaining by default, so you will replace the current EAP-TLS settings with the default settings.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

**Activity Procedure**

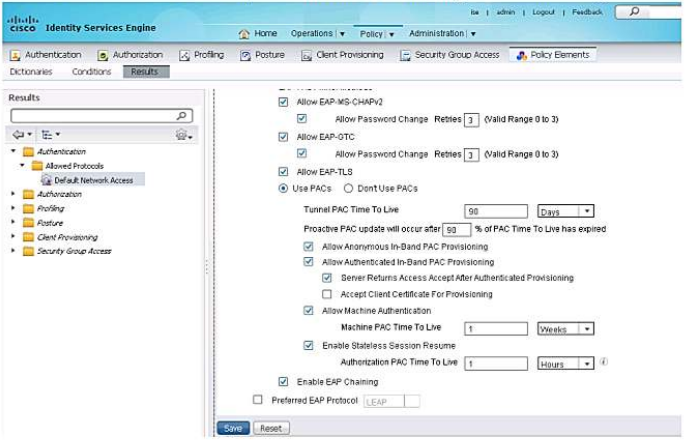
Complete the following steps:

***Step 1***

In the ISE GUI, enable EAP chaining in the default allowed protocol list.

A) Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols > Default Network Access.**

B) Scroll down to the EAP-FAST section, check **Enable EAP Chaining** and **Save** the changes.




***Step 2***

On the Employee-PC, reset the AnyConnect supplicant to its default settings. This will enable EAP-FAST (EAP-MSCHAPv2) and EAP chaining:

A) If you are not already logged in to the **Employee-PC**, log in as **secure-x\administrator** with password **Ci5coAdmin**. Otherwise stay logged on as the current user.

B) Open the Network Access Manager Profile Editor by clicking its desktop icon.

C) Go to **Network Access Manager > Networks**. Select the default entry '**wired**' and click **Edit**.

D) Select the second **Credentials** tab which is at the bottom of the available tabs. Click **Done**. Use **File > Save As** to save the profile. Save the profile as **configuration.xml** without changing the path to which the file is saved. This file name is manditory. This file is temporary. The profile editor will immediately process the file, update the AnyConnect profile, and delete this temporary file.

### Activity Verification

#### *Step 1*

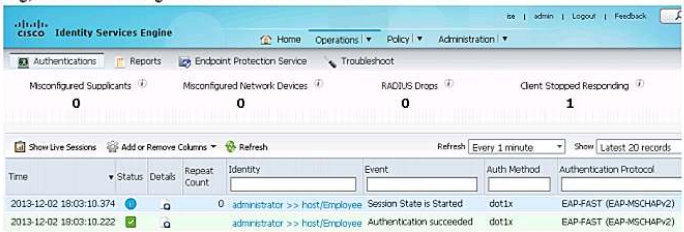
On the Employee-PC, reset 802.1X connection using the updated AnyConnect profile by right-clicking the AnyConnect icon from the system tray and choosing **Network Repair**.

#### *Step 2*

In the Cisco ISE GUI, verify a successful chained authentication of the administrator and Employee-PC. You will identify it by the >> notation between the user and endpoint identity.

#### *Step 3*

Click the **details** button and examine the details. In the Authentication Details section, you should see Username: administrator,host/Employee-PC. In the Other Attributes section, you should see Use Case: EAP Chaining, and EAPChainingResult: User and machine both succeeded.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 4*

Log off from the Employee-PC. In the Cisco ISE GUI, you should see a successful EAP authentication of Employee-PC.

### *Step 5*

Click the **details** button and examine the details. In the Authentication Details section, you should see Username: host/Employee-PC. In the Other Attributes section, you should see Use Case: EAP Chaining, and EAPChainingResult: User failed and machine succeeded.

# Task 2: Configure Switch for AAA Authorization and 802.1X Low-Impact Mode

In this task, you will enable RADIUS authorization on the switch and change the switch port configurations from monitor mode to low-impact mode. 802.1X low-impact mode can restrict the initial basic connectivity of the devices that have not yet authenticated. Like monitor mode, it is configured with the **authentication open** command, but it adds a port ACL on the access interface. The pre-authentication ACL will provide access to basic services such as DNS and DHCP, but deny general access to the network. The low-impact mode will become fully functional in the later tasks, when specific authorization profiles are applied to override the pre-authentication ACL that is configured on the port.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Configure the switch for network authorization:

```
aaa authorization network default group radius
```

#### *Step 2*

On the switch create an ACL named Basic-ACL that permits only baseline traffic. This ACL will restrict the initial traffic until a specific ACL is downloaded from the ISE as part of an authorization profile.

A) DHCP (UDP/67)

B) DNS (UDP/53)

C) HTTP (TCP/80) to HQ-Srv (10.10.3.20)

**Note** The requirements of the pre-authentication ACL will differ between environments. For example, an environment which utilizes PXE may need to have TFTP permitted by the pre-authentication ACL.

```
ip access-list extended Basic-ACL
 permit udp any any eq bootps
 permit udp any any eq domain
 permit tcp any host 10.10.3.20 eq www
```

#### *Step 3*

Apply the ACL (Basic-ACL) to the interfaces GigabitEthernet 0/1 (where the Employee-PC is attached), and 0/19 (wher the print server is attached). Note that the **authentication open** command was configured previously to implement monitor mode.

```
interface GigabitEthernet 0/1
 ip access-group Basic-ACL in
interface GigabitEthernet 0/19
 ip access-group Basic-ACL in
```

### Activity Verification

From the Employee-PC, try to access the HQ-Srv (10.10.3.20) using ICMP ping and HTTP. Only HTTP should work, as permitted in the Basic-ACL.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 3: Retrieve User Groups from Active Directory

In this task you will retrieve user groups from the Active Directory. After retrieving the groups, the authorization policy on the ISE will apply authorization profiles based on the group membership. The access privileges will be granted based on user group membership.

### Activity Procedure

Complete the following steps:

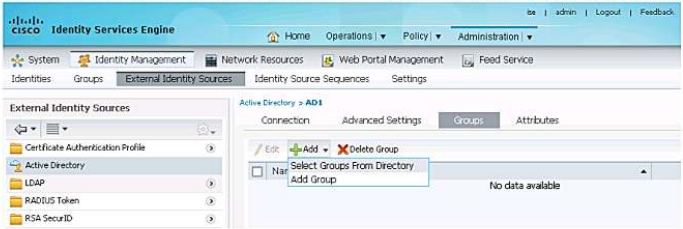

https://t.me/learningnets

***Step 1***

Retrieve groups from the Active Directory:

A) Choose **Administration > Identity Management > External Identity Sources > Active Directory**.

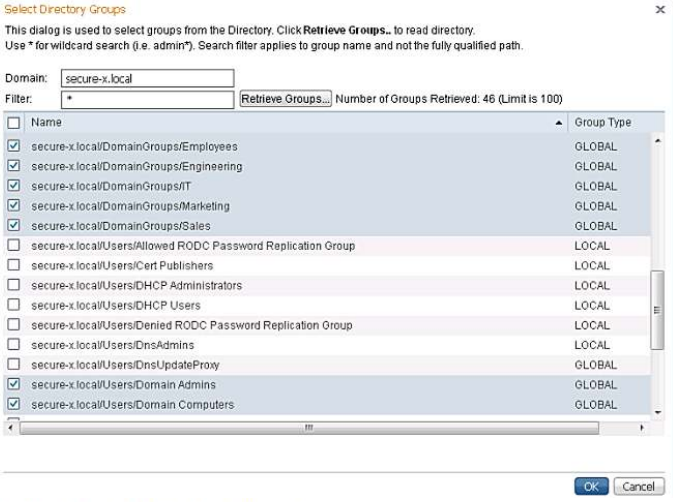
B) Choose the **Groups** tab of your Active Directory **AD1**. Choose **Add > Select Groups from Directory**.




**Note** You are retrieving groups that you will match when authorizing the clients.

C) Leave the filter as simply an *, and click **Retrieve Groups**.

D) Choose all **secure-x.local/DomainGroups (Contractors, Employees, Engineering, IT, Marketing, Sales)**, **secure-x.local/Users/Domain Admins**, and **secure-x.local/Users/Domain Computers**.




E) Click **OK**, and then click **Save Configuration**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 4: Configure Authorization for IT Users and Domain Computers

In this task you will configure authorization of users from the IT group on domain computers. EAP chaining allows you to assign appropriate privileges when the IT users connect from enterprise-owned endpoints. To achieve this goal you will assign a dACL and a VLAN to an authorization profile. The authorization profile will be referenced in the authorization policy rule. The authorization policy rule (named IT Corporate Access) will check that the EAP chaining result is 'User and machine both succeeded' and that the user belongs to the IT group in Active Directory, and will enforce the appropriate authorization profile upon the client.

### Activity Procedure

Complete the following steps:

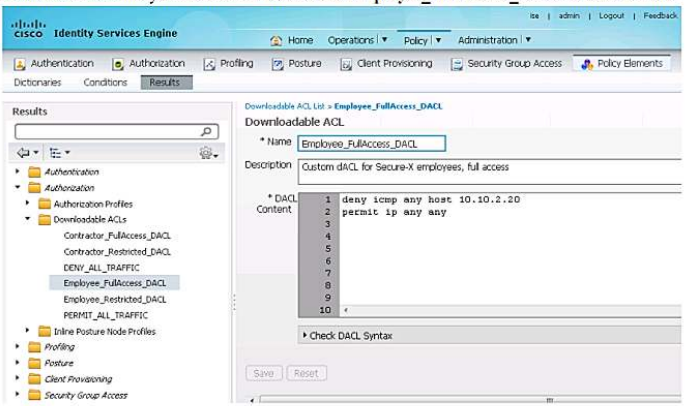
#### *Step 1*

In the ISE GUI, examine the pre-configured downloadable ACLs:

A) Go to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

B) You will see six dACLs. PERMIT_ALL_TRAFFIC and DENY_ALL_TRAFFIC have been factory installed. Contractor_FullAccess_DACL, Contractor_Restricted_DACL, Employee_FullAccess_DACL, and Employee_Restricted_DACL have been preconfigured in this lab environment to save some time.

C) Examine the dACL that you are about to use. Check **Employee_FullAccess_DACL** and click **Edit**.




**Note** This ACL was designed to demonstrate a simple authorization enforcement. It allows all traffic except for ICMP traffic destined for 10.10.2.20 (ISE's management IP address). Optionally you can investigate the other dACLs that have been preconfigured.


https://t.me/learningnets

***Step 2***

Create an authorization profile named IT_Corp which assigns VLAN 10 and the Employee_FullAccess_DACL dACL. This authorization profile will be applied to IT users when they are logged on to enterprise-owned computers.

A Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

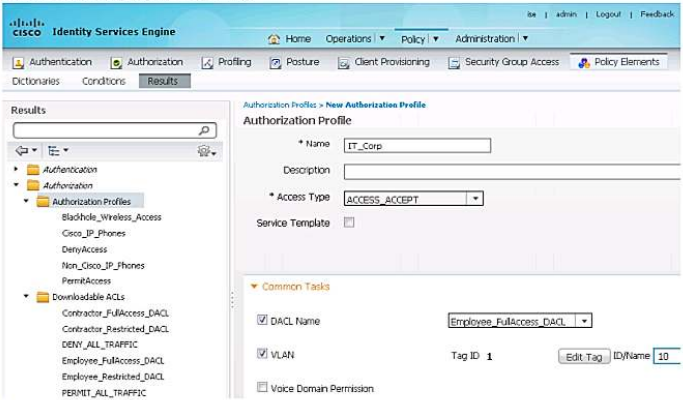
B Click **Add**.

C Define the following settings:

Name: **IT_Corp**

Select **DACL Name** and select **Employee_FullAccess_DACL**

Select **VLAN** and specify VLAN **10**

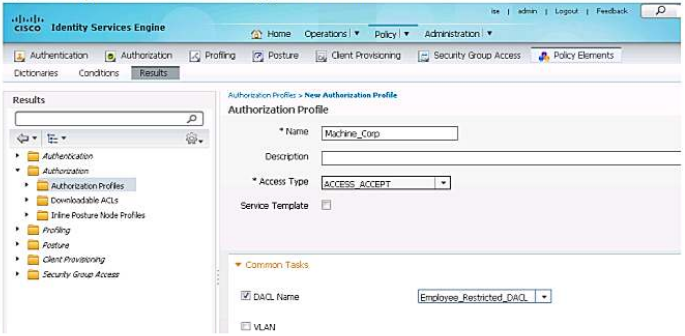



D Click **Submit**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Create another authorization profile for corporate endpoints, named **Machine_Corp**, which assigns just the dACL **Employee_Restricted_DACL**. **Submit** the configuration. This authorization profile will be applied to enterprise computers when no user is logged on to them.



***Step 4***

Configure an authorization policy rule for IT users accessing from corporate assets:

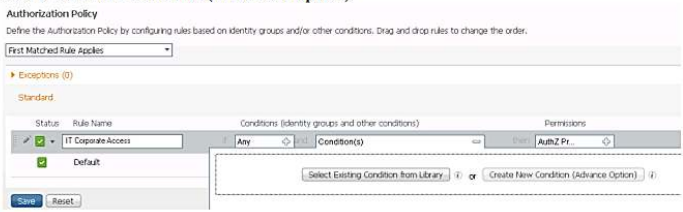
Authorization policies are used to define what authorization profiles are applied under which conditions. In this step you will add an authorization policy rule that applies the IT_Corp authorization profile that you recently defined when both the user and machine successfully authenticate with EAP chaining and that user is a member of the IT group in Active Directory.

A) Choose **Policy > Authorization**.

B) Currently there is just the default authorization rule. Insert a new rule above this by clicking the **Arrow** button to the right of the **Edit** link. Choose **Insert New Rule Above**.

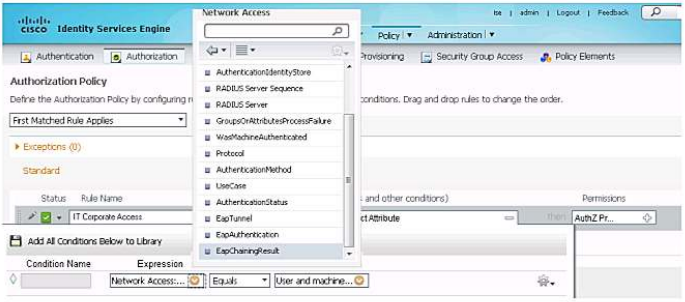
C) Name the new rule **IT Corporate Access**.

D) Begin the definition of the first condition. Click the + symbol in the **Conditions** field. (Note, this field will change names to **Select Attribute** if you expand it and the collapse it without making a selection). Choose **Create New Condition (Advanced Option)**.



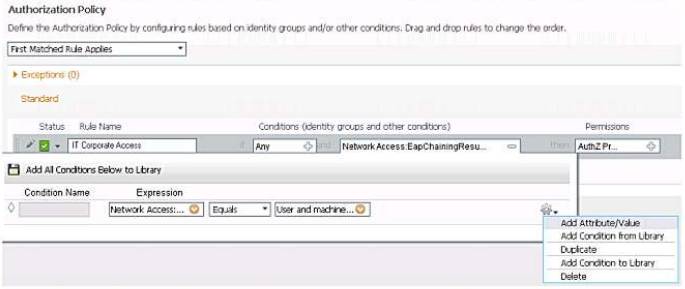

E) Configure the condition to specify that the EAP chaining result must indicate success for both the user and the machine. There are three fields to define for the condition: Attribute, Operator and Value. Use the drop down menu for the **Attribute** field and choose **Network Access > EAPChainingResult**. In the **Operator** field, choose **Equals**. In the **Value** field, choose **User and machine both succeeded**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

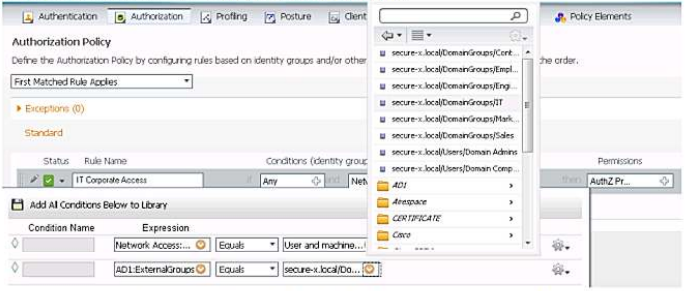



**Note** You may type any character into a field to open the respective menu and choose the desired option.

F) Click the wheel icon to the right of the just created condition. Select the **Add Attribute/Value** option. This will create another attribute/value sub-condition. Leave the default operator AND unchanged.

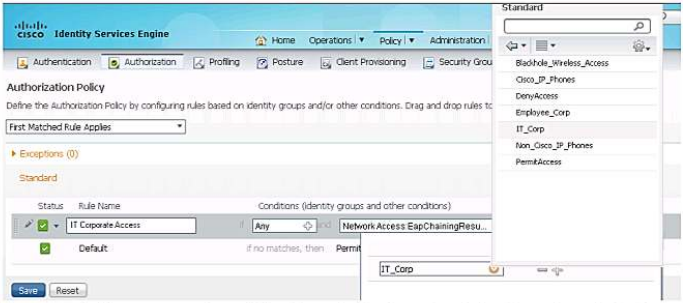



G) In the **Attribute** field, choose **AD1 > ExternalGroups**. In the **Operator** field, choose **Equals**. In the **Parameter** field, choose **secure-x.local/DomainGroups/IT**.




H) The conditions are now defined. What is left is to define the authorization profile to apply when the conditions are met. In the **Permissions** field, choose **Standard > IT_Corp**.


https://t.me/learningnets




I) Click **Done** to indicate you are done editing the authorization rule and then **Save** the authorization policy.

### *Step 5*

Use the same procedure to configure an authorization policy for domain computers:
This authorization rule will apply the Machine_Corp authorization profile when the the EAP chaining result is User failed and machine succeeded and the machine is a member of Domain Computers.

A) Place the new rule between the IT Corporate Access and the default rule. Although this order does not matter, it being suggested for better readability.

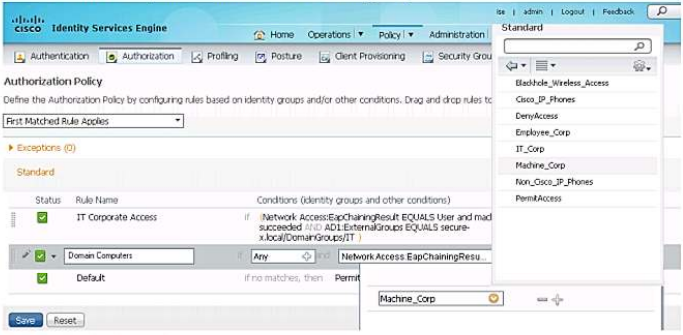
B) Rule name: **Domain computers**

C) First attribute/value: **Network Access:EAPChainingResult Equals 'User failed and machine succeeded'**

D) Operator: **AND**

E) Second attribute/value: **AD1:ExternalGroups Equals 'secure-x.local/ Users/Domain Computers'**

F) In the **Permissions** field, choose **Standard > Machine_Corp**.

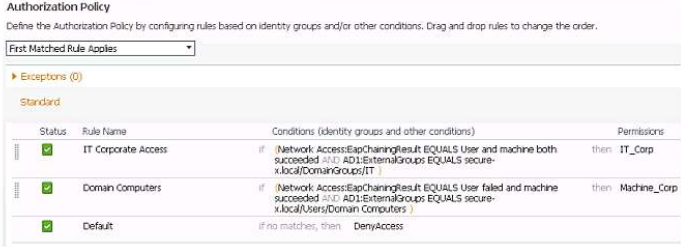



G) **Save** the authorization policy.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 6*

Change the permission in the Default rule to **Standard > Deny Access**. This implements the stronger fail-close security approach. Again, **Save** the configuration.

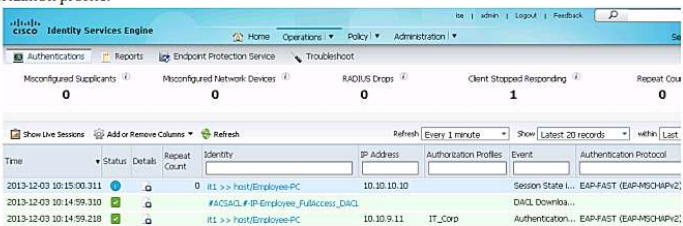



## Activity Verification

You have completed this task when you verify that the RADIUS-based authorization for IT users and domain computers succeeds:

### *Step 1*

Log on to the Employee-PC as it1 with password **cisco**. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session. Adjust the shown columns to see the applied authorization profile.



### Step 2

Verify the authentication and authorization on the switch. You should see that the authorization is successful, assigned VLAN is 10, the client pulled an IP address from the 10.10.10.0/24 subnet and a dACL has been pushed to the interface.

```
SW-podx# show authentication session interface gigabit 0/1
                    Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.10.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000174E20F2EFCB
      Acct Session ID:  0x000017a6
               Handle:  0x39000767
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

### Step 3

Verify the dACL applied to the switch port.

```
HQ-Sw# show ip access-lists interface gigabitEthernet 0/1
     deny icmp any host 10.10.2.20
     permit ip any any (7 matches)
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 4

Verify the VLAN applied to the switch port:

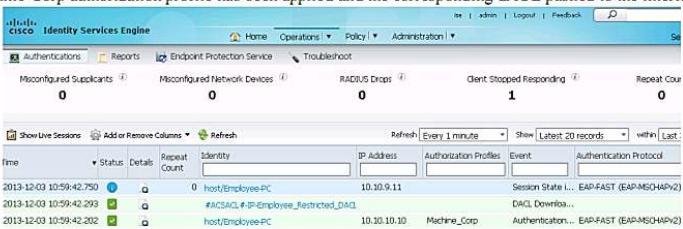
```
HQ-Sw# show interface GigabitEthernet 0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
....
```

### Step 5

On the **Employee-PC**, open a browser and verify that you can connect to cisco.com. Also, use a command prompt and attempt to ping ise.secure-x.local. This is the one type of traffic that is denied by the ACL and hence the pings should time out.

### Step 6

Restart the **Employee-PC**. Wait for it to boot to a login prompt, but do not log in yet. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session. You should see that the Machine-Corp authorization profile has been applied and the corresponding dACL pushed to the interface.



### *Step 7*

Verify the authentication and authorization on the switch. You should see that the authorization has been successful, no VLAN has been received from the ISE, so the port returned to the VLAN specified in the local configuration for the interface and the machine pulled an IP address from the 10.10.9.0/24 subnet. Also, the Employee_Restricted_DACL dACL has been pushed to the interface.

```
HQ-Sw# show authentication session interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.11
            User-Name:  host/Employee-PC
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-Employee_Restricted_DACL-52777cc3
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000174E20F2EFCB
      Acct Session ID:  0x000017C1
               Handle:  0x39000767
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

# Task 5: Configure Authorization for Remaining Employees

In this task you will configure authorization for the remaining employees who belong to various user groups in the Active Directory. The groups include Sales, Engineering, and Marketing. All employees jointly belong to a super-group called Employees. In a production environment you will typically assign different privileges for each user group. For simplicity in this exercise, you will define a single rule for all members of the Employees group when they use corporate-owned endpoints. This less specific rule will be placed after the more specific rule for members of the IT group.

### Activity Procedure

Complete the following steps:

### *Step 1*

Create an authorization profile (**Policy > Policy Elements > Results > Authorization > Authorization Profiles**), for all employees accessing from corporate endpoints, named **Employee_Corp**, which assigns the dACL **Employee_FullAccess_DACL**. **Submit** the configuration.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Configure an authorization policy rule for employees accessing from corporate assets:

A) Navigate to **Policy > Authorization** and place the new rule after the 'IT Corporate Access' rule.

> **Note** The order matters. If you placed the rule for all employees before the 'IT Corporate Access' rule, it would also match the IT users. The more specific rule for IT employees ('IT Corporate Access') would never be matched and the IT employees would never be assigned to their dedicated VLAN 10.

B) Rule name: **Employee Corporate Access**

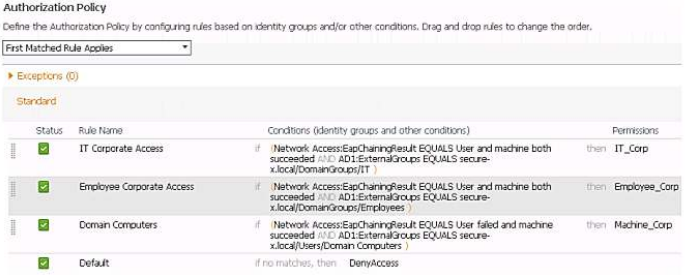
C) First attribute/value: **Network Access:EAPChainingResult equals 'User and machine both succeeded'**

D) Operator: **AND**

E) Second attribute/value: **AD1:ExternalGroups Equals 'secure-x.local/DomainGroups/Employees'**

F) Permission: **Standard > Employee_Corp**.

G) **Save** the authorization policy.

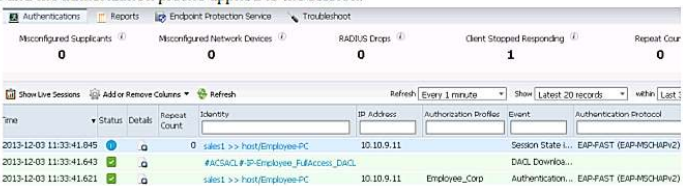



### Activity Verification

You have completed this task when you verify that the authorization succeeds for all employees:

### *Step 1*

Log on to the Employee-PC as sales1 with password cisco. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session.





https://t.me/learningnets

***Step 2***

Optionally you can verify the authentication and authorization on the switch. You should see that the authentication was successful, the interface is in the locally configured VLAN (9), and the Employee_FullAccess_DACL is in place.

***Step 3***

Restart the Employee-PC. Do not log back on before the next task.

# Task 6: Configure Authorization for Domain Administrators

In this task you will configure authorization for the domain administrators. In this scenario, you will assign the same authorization profile independently of whether the administrators use enterprise-owned or personal assets. This practice may not be recommended in production but it demonstrates another way of defining conditions. For simplicity, the administrators will get the same authorization profile as the employees.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Configure an authorization policy rule for domain administrators. This rule will not evaluate the type of their endpoints

A) Place the new rule after the 'Employee Corporate Access' rule.

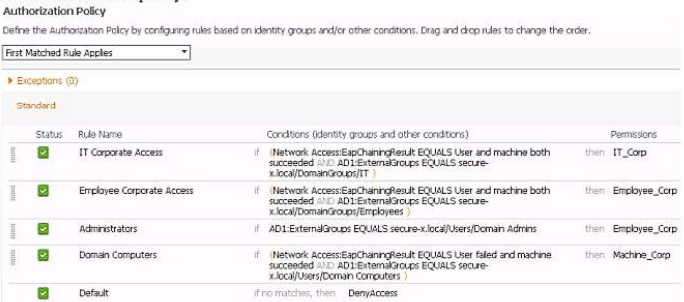
| **Note** | The order does not matter, but it is recommended that uncommon lookups are placed after the more frequent ones. |
|---|---|

B) Rule name: **Administrators**

C) Attribute/value: **AD1:ExternalGroups Equals 'secure-x.local/Users/Domain Admins'**

D) Permission: **Employee_Corp**.

E) **Save** the authorization policy.

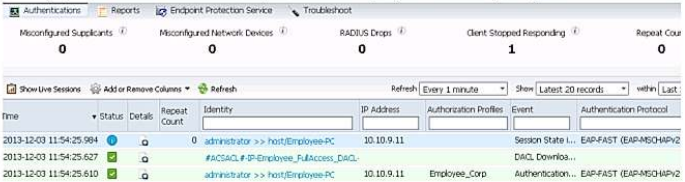



### Activity Verification

You have completed this task when you verify that the authorization works correctly:

#### *Step 1*

Log on to the Employee-PC as **secure-x\administrator** with password **Ci5coAdmin**. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session. If a previous user is still showing up in the authorization results, restart the Employee-PC and log in again.





https://t.me/learningnets

***Step 2***

Restart the Employee-PC. Do not log back on until instructed to do so in the next task.

# Task 7: Configure Authorization for Local ISE Users

In this task you will configure authorization for the local users in the ISE database. For simplicity, the local users will be assigned the same authorization profile as employees independently of the type of endpoints (corporate or personal).


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

**Activity Procedure**

Complete the following steps:

***Step 1***

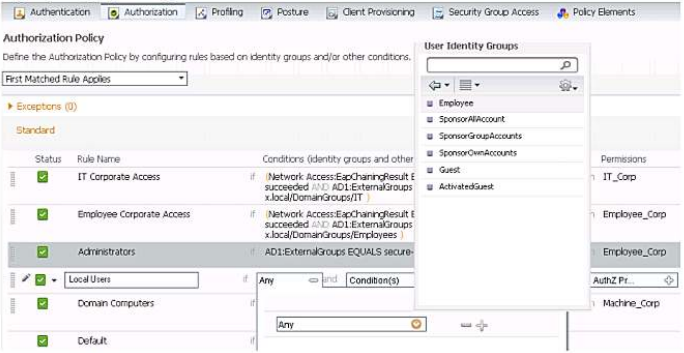
Configure an authorization policy rule for the local users. This rule will not evaluate the type of their endpoints.

A) Place the new rule after the **Administrators** rule.

| **Note** | The order does not matter. It is recommended for easier verification. |
|---|---|

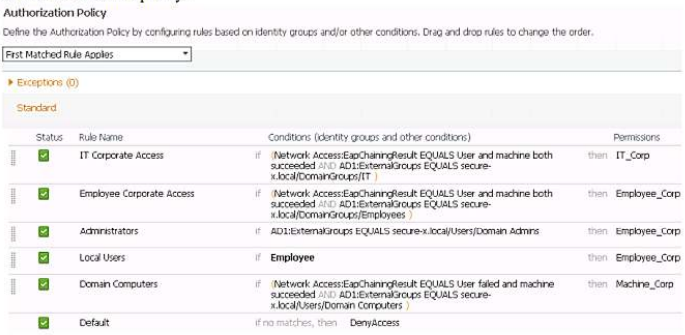
B) Rule name: **Local Users**

C) Note, the configuration process is different than the previous policies. To reference the internal databases, use the first box that is currently set to "Any". Click the + (plus) sign in the first condition field. Select **User Identity Groups > Employee**. The local user student was assigned to the default local group Employee in a previous exercise.




D) Permission: **Employee_Corp**.

E) **Save** the authorization policy.





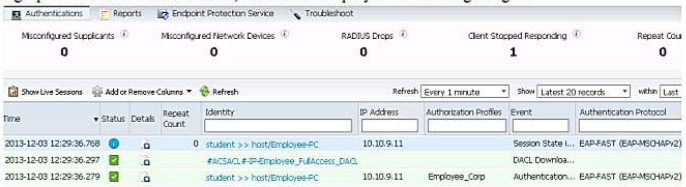
https://t.me/learningnets

### Activity Verification

You have completed this task when you verify that the authorization succeeds for local user accounts:

#### *Step 1*

Log on to the Employee-PC as employee-pc\student with password **Ci5coAdmin**. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session. If a previous user is still showing up in the authorization results, restart the Employee-PC and log in again.




#### *Step 2*

Restart the **Employee-PC**. Do not log back on until instructed to do so in the next task.

## Task 8: Configure Authorization for Print Servers

In this task you will configure authorization for the print server. In a previous exercise the print server attached to GigabitEthernet0/19 has been defined as an endpoint in the ISE endpoint database and assigned to the endpoint identity group 'PrintServers'. You will start this task by exploring the current behavior for the print server's switch port. You will then grant the authorization profile 'Machine_Corp' to the members of the 'PrintServers' group. For simplicity you will be reusing the same authorization profile that is applied to enterprise computers. In a production environment it would be common to develop a unique authorization profile for print servers.

### Activity Procedure

Complete the following steps:

#### *Step 1*

From the Admin-PC or the switch console ping the print server at **10.10.10.99**. The ping should fail.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Investigate the behavior of the print server's switch port (g0/19) on the switch:

A Enter configuration mode and disable and then re-enable interface g0/19 on the switch. Observe the Syslog messages which indicate authentication failure. Leave configuration mode.

```
HQ-Sw#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-Sw(config)#int g0/19
HQ-Sw(config-if)#shutdown
Dec  5 13:48:56.383: %LINK-5-CHANGED: Interface GigabitEthernet0/19, changed
state to administratively down
Dec  5 13:48:57.389: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/19, changed state to down
Dec  5 13:49:08.680: %LINK-3-UPDOWN: Interface GigabitEthernet0/19, changed state
to down
HQ-Sw(config-if)#no shutdown
Dec  5 13:49:11.724: %LINK-3-UPDOWN: Interface GigabitEthernet0/19, changed state
to up
Dec  5 13:49:12.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/19, changed state to up
Dec  5 13:49:26.077: %AUTHMGR-5-START: Starting 'mab' for client (0014.bf66.fb84)
on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:26.127: %MAB-5-FAIL: Authentication failed for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:26.127: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'mab' for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000005BC45CC4C27
Dec  5 13:49:26.135: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:26.135: %AUTHMGR-5-START: Starting 'dot1x' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:49.446: %SYS-5-CONFIG_I: Configured from console by console
Dec  5 13:49:57.020: %DOT1X-5-FAIL: Authentication failed for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:57.020: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'dot1x' for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000005BC45CC4C27
Dec  5 13:49:57.020: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
(0014.bf66.fb84) on Interface Gi0/19 AuditSessionID 0A0A0102000005BC45CC4C27
Dec  5 13:49:57.020: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication
methods for client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000005BC45CC4C27
Dec  5 13:49:57.020: %AUTHMGR-5-FAIL: Authorization failed or unapplied for
client (0014.bf66.fb84) on Interface Gi0/19 AuditSessionID
0A0A0102000005BC45CC4C27
HQ-Sw(config-if)#end
```

B Display the authentication session status for interface g0/19. Note the MAC address, which was previously defined in ISE to support MAB is known, but MAB is now failing.

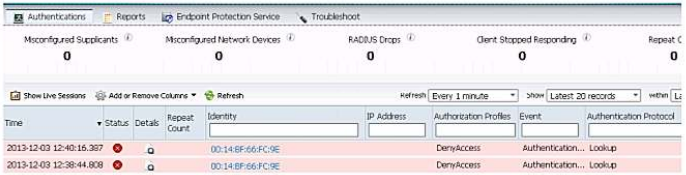
```
HQ-Sw#show authentication sessions int g0/19
            Interface:  GigabitEthernet0/19
          MAC Address:  0014.bf66.fb84
           IP Address:  10.10.10.99
            User-Name:  0014bf66fb84
               Status:  Authz Failed
```


https://t.me/learningnets

```
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
        Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000005BC45CC4C27
      Acct Session ID:  0x000005FD
               Handle:  0xD40005BD
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
```

### *Step 3*

Return to the ISE GUI and view the Live Authentications. You will find authentication failures for the print server.

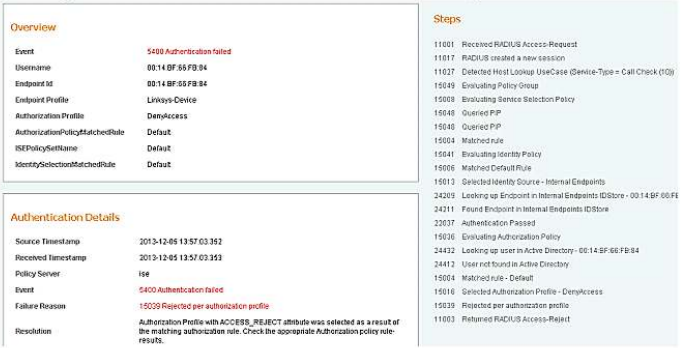




https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 4*

What has changed? Click the **Details** link for the failed authentication to get a closer look.




There are several things to note:

The event is **Authentication failed**

The Failure Reason is **Rejected per authorization profile**

The authorization profile is **DenyAccess**

The AuthorizationPolicyMatchedRule is **Default**

In the authorization policy, the rule default is at the bottom of the rule table. Remember, earlier in this lab you changed the authorization profile referenced by the default rule from PermitAccess to DenyAccess. Because the print server didn't match any specific policies, it now falls through to this default and access is denied.

Understand, MAB was actually successful, just as it was prior to the start of this lab. For a very detailed audit trail, look at the Steps that are documented on the right side of the details window. About two thirds of the way down the steps list you can see that the endpoint was found in the internal endpoint store and that authentication passed. After that you see the authorization steps which ultimately resulted in a RADIUS Access-Reject message to be sent back to the switch.

### *Step 5*

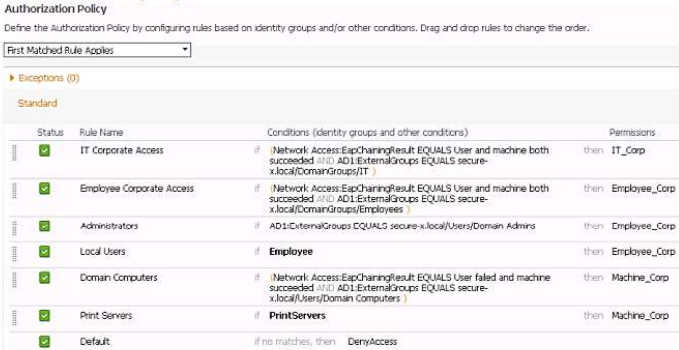
Configure an authorization policy rule for the print servers. Place the new rule before the Default rule.

A) Rule name: **Print Servers**

B) Click the + (plus) sign in the first condition window. Select **Endpoint Identity Groups > PrintServers**.

C) Permission: **Machine_Corp**.

D) **Save** the authorization policy.

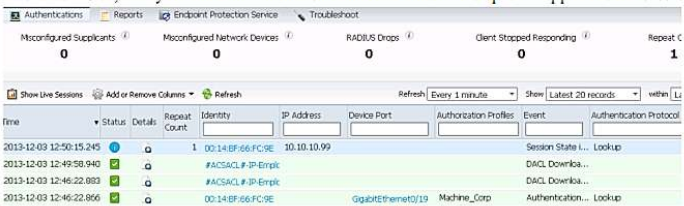



## Activity Verification

You have completed this task when you verify that the authorization works correctly:

### *Step 1*

In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session.




### *Step 2*

From the Admin-PC or the switch console, ping the print server again (**10.10.10.99**). The ping should now succeed.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 3-3: Implement Cisco TrustSec and MACsec

## Activity Objective

In this lab exercise, you will implement and verify several aspects of a TrustSec solution. The exercise is not intended to demonstrate a full TrustSec solution, but instead provide some awareness of and experience with major TrustSec components. The lab results will include dynamic SGT assignment for IT Staff members during 802.1X authorization, static SGT assignment of the Server VLAN, and enforcement by SGACLs controlling traffic between IT Staff and the Server VLAN. There are also optional tasks which demonstrate transporting tag mappings from the HQ-SW to the ASA, implementing SGFW policy on the ASA and the configuration of downlink MACsec to protect traffic on links connecting to IT Staff.

The procedure you will use in the lab is as follows: You will add the switch as a TrustSec device to the TrustSec domain. Once the switch obtains the Protected Access Credential (PAC) from the ISE, it will be able to download the TrustSec data. You will configure three security groups on the ISE: for the NADs, for the IT users, and for the servers. You will use the security group tags (SGT) and egress filtering on the switch to block FTP connections from the IT users to the servers. Optionally you will extend the TrustSec functionality to the ASA. You will provision a PAC on the ASA, configure a SGT Exchange Protocol (SXP) connection between the switch and the ASA, and deploy egress filtering on the ASA. This setup will effectively block FTP traffic to the DMZ server, which is attached to the ASA. The last optional task is to configure the HQ-SW, ISE and the AnyConnect supplicant to support MACsec protection on the links to which IT Staff members are connected.

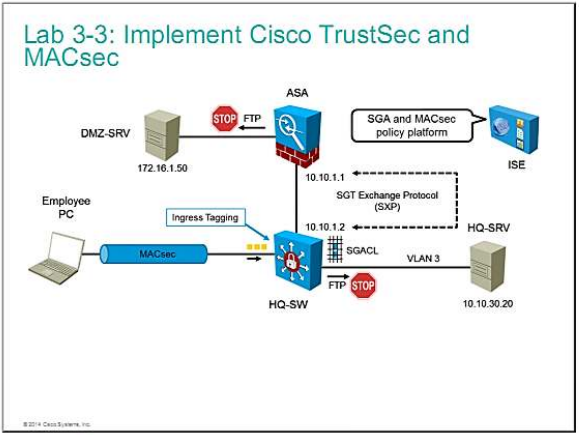
Upon completing this exercise, you will be able to:

- Define Seed Device in Cisco ISE
- Configure the switch to act as a SGA device
- Apply SGT at ingress
- Deploy egress filtering on the switch
- Provision PAC on ASA
- Deploy egress filtering on the ASA
- Implement downlink MACsec

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Command List

The table describes the commands that are used in this activity. Refer to this list if you need configuration command assistance during the lab activity.

## Commands

| Command | Description |
|---|---|
| **pac key radius-key** | Set the secret for Protected Access Credential (PAC) provisioning. Configured in the RADIUS server configuration mode. |
| **aaa authorization network** | Enable authorization |
| **cts authorization list** | Configure the authorization method for Cisco TrustSec (CTS) |
| **cts credentials** | Configure CTS credentials |
| **cts role-based enforcement** | Enable CTS role-based enforcement globally on the switch |
| **cts role-based enforcement vlan-list** | Enable CTS role-based enforcement for a specific egress VLAN |
| **cts role-based sgt-map vlan-list** *<vlan-id>* **sgt** *<sgt-value>* | Map an egress VLAN to a SGT value |
| **cts role-based sgt-map** *<ip-address>* **sgt** *<sgt-value>* | Map an egress IP address to a SGT value |
| **cts sxp enable** | Enable SGT Exchange Protocol (SXP) |
| **cts sxp connection peer** | Configure a SXP connection |


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| Command | Description |
|---|---|
| **show cts pac** | Display CTS PAC |
| **show cts environment-data** | Display CTS environment data |
| **show cts rbacl** | Display CTS SGACLs |
| **show cts role-based counters** | Display SGACL statistics |
| **show cts sxp connections** | Display SXP sessions |
| **authentication host-mode single-host** | Sets interface 802.1X host mode to single-host |
| **macsec** | Enables MACsec on an interface |
| **mka default-policy** | Enables the default MACsec Key Agreement (MKA) policy on an interface |
| **authentication linksec policy** | Configures the liksec policy |

# Task 1: Prepare ISE for TrustSec communication with the HQ-SW

In this task you will define the HQ-SW as a TrustSec-aware NAD in the ISE. You will configure a security group dedicated to the NADs, which will allocate a SGT to them. Being a member of the security group, the switch will be able to download the TrustSec data and join the TrustSec domain.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Configure the SGA AAA Server:

The SGA AAA servers defines a list of RADIUS servers that will be used by the TrustSec capable network access devices (NADs) to obtain Cisco TrustSec (CTS) environment data and policy. This list can be populated multiple servers in a distributed ISE deployment. The NADs use their configured RADIUS servers for initial CTS authorization, and will then use the servers on this list for ongoing CTS operations.

A) In the ISE GUI navigate to **Administration > Network Resources > SGA AAA Servers**.

B) Verify that there is an entry named ise-1 with the IP address 10.10.2.20.

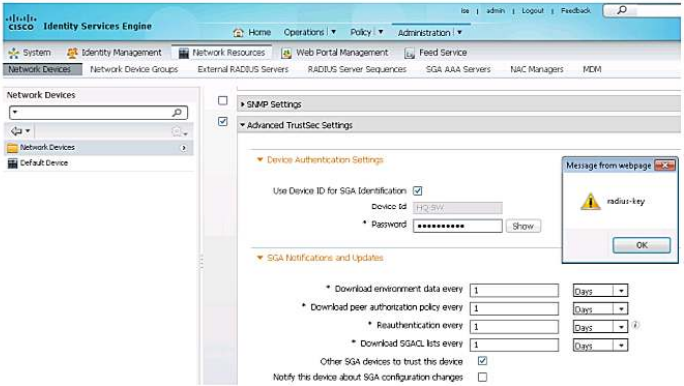
***Step 2***

Configure SGA settings for the HQ-SW in ISE:

Additional settings must be configured in ISE for devices that will participate in CTS. The NADs will also have to have corresponding settings in their configurations.

A) Go to to **Administration > Network Resources > Network Devices**. Select the **HQ-SW**.

B) Check the **Advanced TrustSec Settings** checkbox. Keep the **Use Device ID for SGA Identification** checkbox checked. Enter the RADIUS secret **radius-key** and leave all other settings at their default values.




**Note** The update timers kept by the CTS devices are controlled by ISE. You didn't change the values. ISE defaults each of the timers to 1 day.

C) Click **Save**.

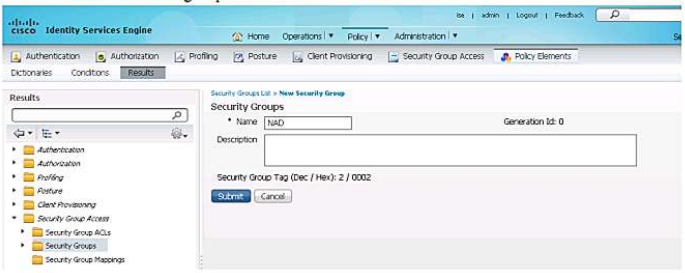

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Create a new security group to associate with the network access devices:

A) Go to to **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

B) Click **Add** to create a device group. Name it **NAD**. Click **Submit**.



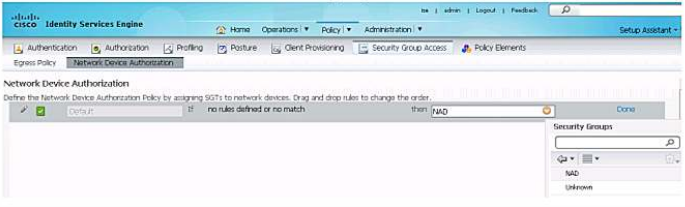

**Note** While you choose the name, ISE specifies the numeric value for the tag. If you follow the lab directions closely, the tag numbers will match what is shown in the screen shots. Make a note if you find that the NAD SGT has a numeric value other than 2.

### *Step 4*

Define an authorization policy that assigns the NAD security group to all devices that pass CTS authentication:

A) Go to to **Policy > Security Group Access > Network Device Authorization**.

B) Edit the default rule and set the result to the **NAD** group. **Save** the changes.




**Note** The **Push** button appears in many of the TrustSec oriented areas of ISE. The function of the button is to send updated CTS policies to devices that are currently active. This function is currently supported only on select high-end platforms. For the Catalyst 3000 family, policy updates will occur automatically based on a locally kept timer or immediately when initiated from the CLI of a device.


https://t.me/learningnets

# Task 2: Configure the Switch to Act as SGA Device

In this task, you will configure the HQ-SW as a member of the CTS domain. Requirements include the setting of the PAC secret and the CTS credentials. Once configuration is complete, the switch will automatically authenticate and retrieve the CTS environment data and CTS policy.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Define ISE as a RADIUS server named ISE-PAC, using ports 1812 and 1813 for authentication and accounting. Also specify **radius-key** as the PAC key for this server. Then add this server to the AAA server group named ISE-PAC

```
radius server ISE-PAC
 address ipv4 10.10.2.20 auth-port 1812 acct-port 1813
 pac key radius-key
!
aaa group server radius ISE-CTS
 server name ISE-PAC
```

#### *Step 2*

Configure the switch for Cisco TrustSec (CTS) network authorization:

A) Create a network authorization list named **cts-author-list** that uses the **ISE-CTS** group. A

```
aaa authorization network cts-author-list group ISE-CTS
```

| **Note** | Although ISE is the only RADIUS server in the lab topology, you defined two AAA server groups and added ISE to each of the groups. You used different authentication and authorization ports to allow the switch to accept this duplication. The reason for this effort is a work around to an issue on Catalyst 3000 platform and ISE with the version used in this lab. When a switch is provisioned with a PAC, ISE expects all RADIUS messages, including accounting messages, to be authenticated using the PAC. The switch, however, will continue to use the RADIUS key to authenticate accounting messages, leading to dropped accounting requests. This effort is not required on other switch platforms. |
|---|---|

B) Enable CTS authorization using the **cts-author-list** method list.

```
cts authorization list cts-author-list
```

#### *Step 3*

Configure CTS credentials. Set the device ID to **HQ-SW** and password to **radius-key**. On the Catalyst 3000 series, this setting is performed in privileged mode, not configuration mode.

```
cts credentials id HQ-SW password radius-key
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Verification

#### *Step 1*

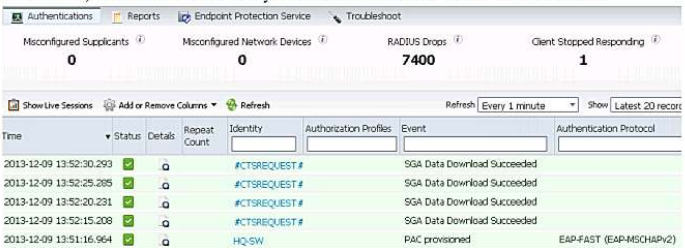
Verify the PAC provisioning and data download process:

A) View the authentications in the ISE GUI. After about two minutes you should see a notification about a PAC provisioned event:

B) On the switch, view the PAC received from the ISE:

```
HQ-Sw# show cts pacs
  AID: D7BFE8E16837FDFED5698FE295398B0F
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: D7BFE8E16837FDFED5698FE295398B0F
    I-ID: HQ-SW
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 05:51:16 PT Mar 9 2014
  PAC-Opaque:
<output omitted>
```

C) In the ISE GUI, after about two minutes you will see notifications of CTS data download.




D) Examine the details. You should see a RADIUS request from 'CTSREQUEST' with Cisco AV pair cts-pac-opaque.


https://t.me/learningnets

E) Examine the downloaded CTS environmental data on the switch:

```
HQ-Sw# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00:NAD
Server List Info:
Installed list: CTSServerList1-0004, 1 server(s):
 *Server: 10.10.2.20, port 1812, A-ID D7BFE8E16837FDFED5698FE295398B0F
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime =
20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:NAD
Environment Data Lifetime = 86400 secs
Last update time = 10:19:50 PT Tue Dec 10 2013
Env-data expires in   0:23:59:13 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:13 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

**Note** There are several things to note in the output. The update was successful. The SGT applied to the local device is indeed number 2 with the name NAD. The CTS server list was downloaded from ISE. The update timer settings were also downloaded from ISE and the timers will expire and data will be refreshed in just under one day.

**Note** If you want to repeat the process, you may have to clear the CTS settings. You can use the commands clear cts credentials, clear cts environmental-data, and clear cts pac all.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 3: Dynamically Apply SGT during 802.1X Authorization

A very important feature of Cisco TrustSec is the ability to have ISE utilize all of the contectual data it has available to dynamically classify endpoints and assign the appropriate SGT as part of 802.1X authorization. In this task you will configure a SGT for the IT users and configure the ISE authorization policy to set the SGT as a result in their authorization policy rule. For the sake of time, you will only define SGT policy for the IT user group.

### Activity Procedure

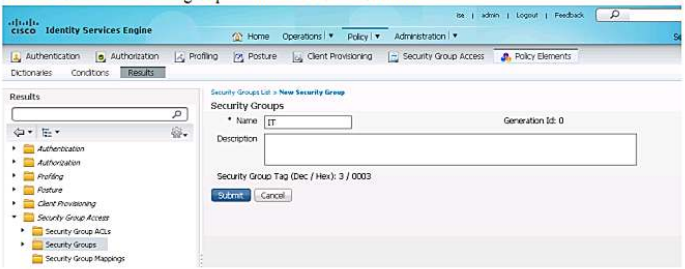
Complete the following steps:

#### *Step 1*

Create a new security group for the IT users.

A) Go to to **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

B) Click **Add** to create a device group. Name it **IT**. Click **Submit**.




**Note** Again, if you are following the specifications of this lab, it is expected that the tag number for the IT group will be 3. If you have deviated from the lab directions you may find that the numeric tag value is different. If you do, make a note of the tag value that you see.

### *Step 2*

Apply the IT security group to the appropriate authorization policy rule:

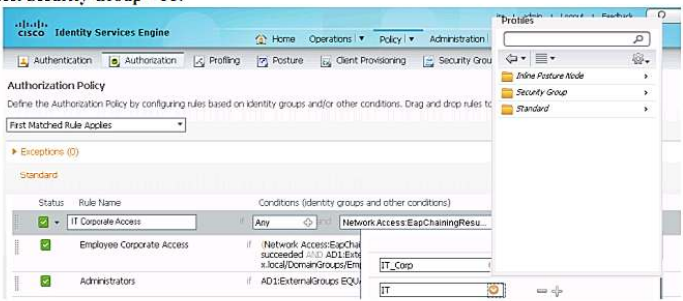
Currently there is an authorization rule for the IT users named IT Corporate Access. Currently the authorization rule assigns a dACL. In this step, you will add the SGT assignment as a second result to the authorization rule.

A) Go to to **Policy > Authorization.**

B) Edit the rule for IT users (**IT Corporate Access**). Click the + (plus) sign in the Permissions window.

C) Click the + (plus) sign near the existing authorization profile to add a new result.

D) Select **Security Group > IT**.



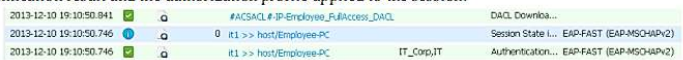

E) Click **Done** on the updated authorization rule and then click **Save** at the bottom of the rule table.

## Activity Verification

The dynamic classification of IT users with the IT security group tag is now configured on ISE. To verify this is working correctly you will log on to the Employee-PC as the user it1 and verify the results on ISE and the switch.

### *Step 1*

Restart the **Employee-PC**, then, log on as **it1** with password **cisco**. In the Cisco ISE GUI, verify the authentication result and the authorization profile applied to the session.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

Verify the authentication and authorization on the switch. You should see that the appropriate SGT is being applied to incoming traffic:

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
           Interface:  GigabitEthernet0/1
         MAC Address:  a036.9f1a.3bb1
          IP Address:  10.10.10.10
           User-Name:  it1
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
                 SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A0A01020000023000AF1FD
     Acct Session ID:  0x0000004b
              Handle:  0xA6000024
Runnable methods list:
      Method   State
      dot1x    Authc Success
```

# Task 4: Implement Egress Filtering on Switch

In this task you will configure CTS enforcement using a security group ACL (SGACL). To accomplish this, you will configure both ISE and the HQ-SW appropriately. In ISE, you will define a new security group for the Servers, configure an SGACL that blocks FTP traffic while permitting everything else and apply this SGACL to traffic sourced from the IT users security group and destined to the Servers security group. On the switch, you will statically assign the Servers security group to VLAN 3 and enable CTS enforcement, both globally and on VLAN 3.

### Activity Procedure

Complete the following steps:

### *Step 1*

Observe the behavior prior to implementing the SGACL policy:

Before configuring the SGACL policy, verify that FTP is currently allowed from IT users to the HQ-Srv. On the Employee-PC, open a command prompt and FTP to the HQ-SRV. Authenticate as **anonymous** with any password of your choosing. The connection should be successful. Use the **bye** command to terminate the session.

```
C:\Users\it1>ftp hq-srv
Connected to hq-srv.secure-x.local.
220--
220--
220-HQ-Srv
220--
220--
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
User (hq-srv.secure-x.local:(none)): anonymous
331 Password required for anonymous
Password: password
230 Logged on
ftp> bye
221 Goodbye
```

### *Step 2*

Create a new security group for the for the corporate servers.

A) Navigate to **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

B) Click **Add** to create a security group. Name it **Servers**. Click **Submit**.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Configure a security group ACL that blocks FTP.

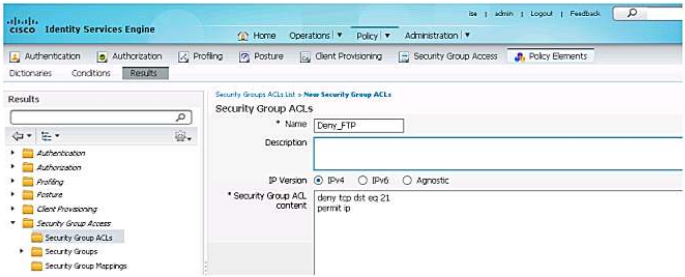
A) Go to to **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**.

B) Click **Add** to create an SGACL. Name it **Deny_FTP**. Deny FTP and permit all other IPv4 traffic. Click **Submit**.

---

**Note** The syntax for SGACLs is different from dACLs. Neither source or destination IP addresses are specified in an SGACL. SGACLs are applied to the intersection of tags in the SGT matrix. It is the intersection in the matrix that specifies the source and destination in the form of security group tags.

---

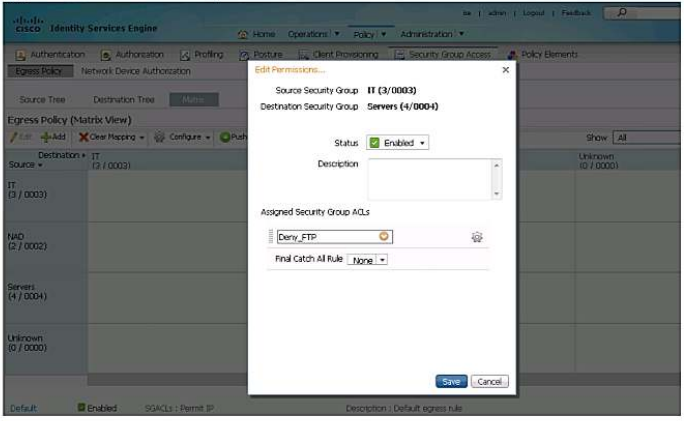


***Step 4***

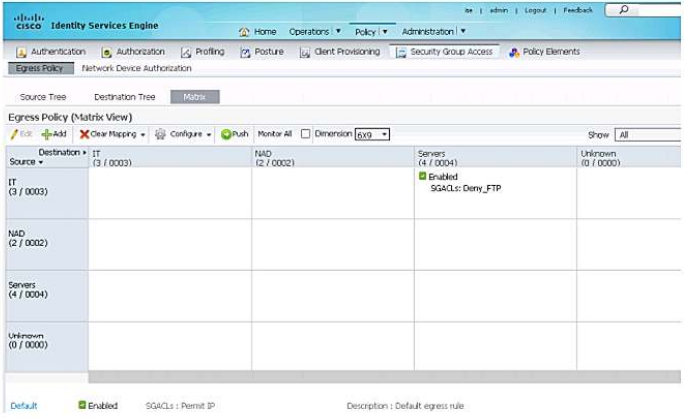
Apply the SGACL (**Deny_FTP**) to traffic from security group **IT** to security group **Servers**:

A) Go to to **Policy > Security Group Access > Egress Policy**. Select the **Matrix** tab.

B) The matrix specifies source group tags in the by row and the destination group tag by column. Select the cell that is the intersection of the **IT row** and the **Servers column**. Double-click the cell. Select the **Deny_FTP** SGACL from the drop-down box.




C) Click **Save**.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 5*

On the switch, enable the appropriate CTS role-based access enforcement:

A) Enable the role-based access enforcement globally on the switch.

```
cts role-based enforcement
```

B) Enable the role-based access enforcement for the egress VLAN, where the HQ-SRV is attached (VLAN 3).

```
cts role-based enforcement vlan-list 3
```

### *Step 6*

On the switch, statically map VLAN 3 to the Servers SGT:

The HQ-SRV is on VLAN 3. In a production environment it is common to put servers together on a single VLAN. In such cases, it is efficient to assign an SGT to a whole VLAN. Alternatives are to apply SGTs to individual ports or to IP addresses.

The example command assumes that you closely followed the instructions of this lab, leading to the assignment of 4 as the numeric tag value for the Server security group. If the Server group was assigned a different numeric value in ISE, you will need to modify this command.

```
cts role-based sgt-map vlan-list 3 sgt 4
```

### Activity Verification

You have completed this task when you verify that the CTS-based authorization for IT users and domain computers succeeds:

### *Step 1*

Remember that CTS policy changes made on ISE are downloaded periodically by the CTS devices, based on their update timers. These timers are set to 24 hours by default. On the switch, manually initiate a refresh of the CTS environment data.

```
HQ-Sw#cts refresh environment-data
Environment data download in progress
```


https://t.me/learningnets

### Step 2

View the downloaded data. You will see that the switch has downloaded the security group definitions from ISE, and the timers have reset to download again in 24 hours:

```
HQ-Sw#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00:NAD
Server List Info:
Installed list: CTSServerList1-0004, 1 server(s):
 *Server: 10.10.2.20, port 1812, A-ID D7BFE8E16837FDFED5698FE295398B0F
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime =
20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:NAD
    3-00:IT
    4-00:Servers
Environment Data Lifetime = 86400 secs
Last update time = 11:45:28 PT Tue Dec 10 2013
Env-data expires in   0:23:59:25 (dd:hr:mm:sec)
Env-data refreshes in 0:23:59:25 (dd:hr:mm:sec)
Cache data applied          = NONE
State Machine is running
```

### Step 3

On the switch, examine the downloaded role-based ACLs. You will see two ACLs. The Deny_FTP ACL that you defined on ISE and another prepared by default that permits all IP traffic.

```
HQ-Sw# show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
  name    = Deny_FTP-30
  IP protocol version = IPV4
  refcnt = 2
  flag    = 0x41000000
  stale   = FALSE
  RBACL ACEs:
    deny tcp dst eq 21
    permit ip
  name    = Permit IP-00
  IP protocol version = IPV4
  refcnt = 2
  flag    = 0x41000000
  stale   = FALSE
  RBACL ACEs:
    permit ip
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| Note | The term SGACL (Security Group ACL) and RBACL (Role Based ACL) are synonymous. SGACL is the more common term, but the Catalyst switch platform CLI uses RBACL. |
|---|---|

### Step 4

On the switch, examine the role-based permissions. You should see that the role-based ACL has been applied to traffic from the **IT** group to the **Servers** group.

```
HQ-Sw# show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 3:IT to group 4:Servers:
        Deny_FTP-30
```

### Step 5

On the switch, examine the dACL applied to interface GigabitEthernet0/1.

```
HQ-Sw#show ip access-lists interface gigabitEthernet0/1
     deny icmp host 10.10.10.10 host 10.10.2.20
     permit ip host 10.10.10.10 any (26 matches)
```

| Note | Static ACL policy, dACL policy and SGACL policy can all coexist. The dACL that is assigned to IT users was defined in an earlier exercise. It permits everything except access to ISE's IP address. In general, dACL policy is applied ingress on the interface where the endpoint connects and SGACL policy is applied egress on the interface leading towards the destination security group. |
|---|---|

### Step 6

On the Employee-PC, attempt to FTP to the HQ-Srv. This access should be denied by the SGACL. As you did before, use a command prompt window to FTP to the HQ-Srv. This time, no password is required, as the connection is not allowed. You can use Ctrl-C if you don't want to wait for the connection to time out, or use the **bye** command at the ftp> prompt if you did wait.

```
C:\Users\it1>ftp hq-srv
ftp> bye
```


https://t.me/learningnets

### *Step 7*

On the Employee-PC, attempt to ping 10.10.2.20. This attempt should be blocked by the dACL that is applied to the inteface.

```
C:\Users\it1>ping 10.10.2.20
Pinging 10.10.2.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.2.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

### *Step 8*

Verify that other connections succeed from the Employee-PC. Ping the HQ-Srv and browse it via HTTP. Optionally you can verify other connections. For example, you should be able to ping, browse and FTP to the DMZ server (ftp.secure-x.public) and to the SP-Srv (sp-srv.sp.public).

### *Step 9*

On the switch, examine the traffic statistics. You will see permitted and dropped packet counters for traffic from the IT group to the Servers group and for the default traffic.

```
HQ-Sw# show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted
*       *       0               0               1617            23932
3       4       0               29              0               341
```

# Task 5: Provision a PAC for the ASA (Optional)

In this task, you will configure CTS communication between ISE and the ASA. In ISE you will define the ASA as a NAD and provision a PAC file for the ASA. On the ASA you will define ISE as a RADIUS server and import the provisioned PAC file. You will then verify that the ASA can obtain the CTS environment data from ISE.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 1*

In the ISE GUI, define the ASA as a NAD. Navigate to **Administration > Network Resources > Network Devices** and create a NAD with these settings:

A) Name: **ASA**

B) IP address: **10.10.1.1**

C) Device type: **ASA**

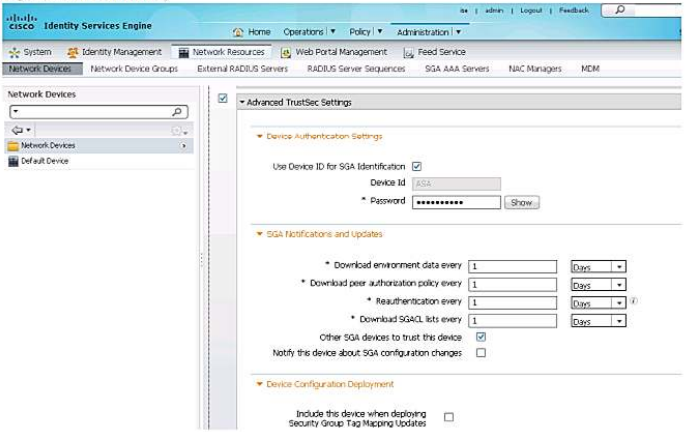
D) Location: **HQ**

E) Check: **Authentication Settings**

F) RADIUS shared secret: **radius-key**

G) Check: **Advanced TrustSec Settings**

H) SGA password: **radius-key**




I) Leave all other settings at their default values and click **Submit**.

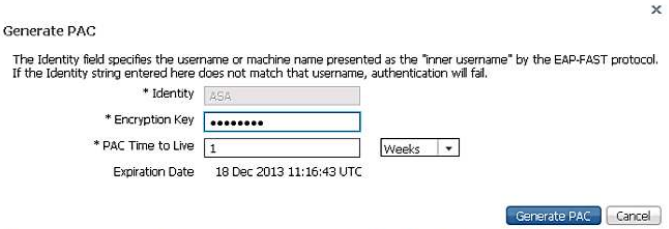

https://t.me/learningnets

### *Step 2*

In the ISE GUI, generate the PAC for the ASA:

A) In **Administration > Network Resources > Network Devices**, select the **ASA** and click **Generate PAC**.

B) Enter **cisco123** as the encryption key and click **Generate PAC**.




C) You should see a pop-up and have the option to save the PAC. **Save** it under the default name **ASA.pac** on disk **C:**. Retry the operation if it fails at first.

### *Step 3*

On Admin-PC launch the **ASDM** using the Cisco ASDM-IDM Launcher shortcut on the desktop. Connect to **10.10.2.1** and authenticate as **admin** with password **Ci5coAdmin**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 4***

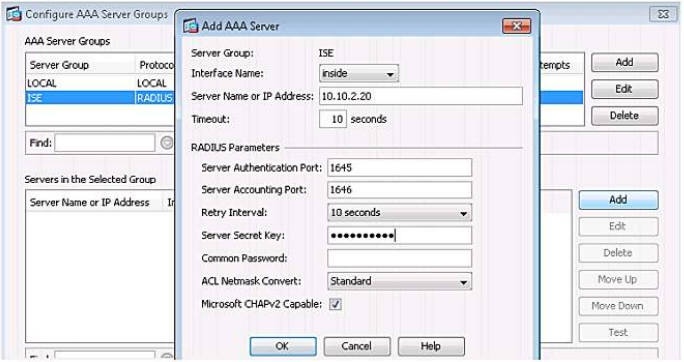
In the ASDM, provision the PAC:

A) Navigate to **Configuration > Firewall > Identity by TrustSec**.

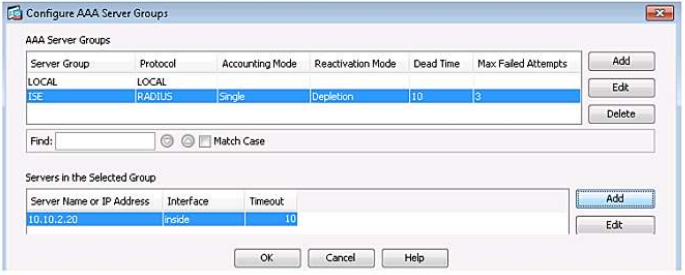
B) Click **Manage** in the Server Group Setup section.

C) In the upper AAA Server Groups pane, click **Add** to create server group. Name it **ISE** and click **OK**. The Configure AAA Server Groups window opens.

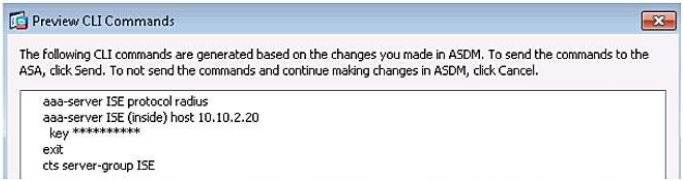
D) WIth the ISE RADIUS server group highlighted, in the lower Servers in the Selected Group pane, click **Add** to define a server. Choose the **inside** interface, set the IP address to **10.10.2.20**, and the secret to **radius-key**.



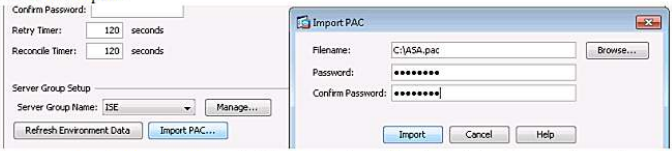

E) Click **OK** to close the Add AAA Server window.



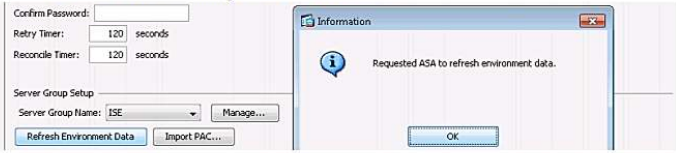

F) Click **OK** to close the Configure AAA Server Groups window, then click **Apply** and **Send** the configuration.




G) Click **Import PAC** at the bottom of the Identity by TrustSec screen. Browse to the PAC file, enter encryption password (**cisco123**) and **Import** the PAC. Click **OK** on the notification that indicates the success of the import.




H) Click **Refresh Environment Data** and click **OK** on the notification window. Do not leave this ASDM window. You will continue to configure SXP in the next task.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Verification

#### *Step 1*

Verify the PAC and environment data on the ASA:

A) Connect to the ASA CLI by clicking the appropriate shortcut on your student PC. Enter a blank password if prompted for credentials.

B) View the CTS PAC:

```
HQ-ASA# show cts pac
  PAC-Info:
    Valid until: Dec 18 2013 11:20:41
    AID:         d7bfe8e16837fdfed5698fe295398b0f
    I-ID:        ASA
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
<output omitted>
```

C) Vie the CTS environment data:

```
HQ-ASA# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          11:44:11 GMT Dec 11 2013
Env-data expires in:       0:23:52:45 (dd:hr:mm:sec)
Env-data refreshes in:     0:23:42:45 (dd:hr:mm:sec)
```

# Task 6: Implement SXP and SGFW (Optional)

The ASA is not capable of inline tagging. That is, it can't read SGTs or impose SGTs in the ethernet header of frames. For it to learn IP to tag mappings, the SGT Exchange Protocol (SXP) is used. In this task, you will configure an SXP connection between the HQ-SW and the ASA. The HQ-SW will act as the speaker and the ASA as the listener. Through this SXP connection, the HQ-SW will convey IP to tag mappings to the ASA. You will configure a static mapping of the DMZ server address to the Server security group on the HQ-SW, and observe that the mapping is received by the ASA. Finally, you will use the Security Group Firewall (SGFW) feature on the ASA to block FTP traffic from the IT security group to the Server security group. This will effectively block FTP from the user it1 to the DMZ-Srv.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets

### *Step 1*

Configure the SXP connection on the ASA:

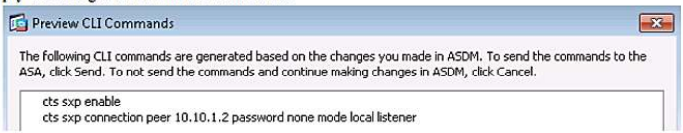
A) Verify that, in ASDM you are still at **Configuration > Firewall > Identity by TrustSec**.

B) Check **Enable the SGT Exchange Protocol**.

C) Click **Add** to the right of the (currently empty) Connection Peers list to define a new SXP connection.

D) Set the following in the Add Connection Peer window: IP address: **10.10.1.2**, Password: **none**, Mode: **Local** and Role: **Listener**. Click **OK** to close the window.

E) **Apply** the changes and **Send** the commands.




### *Step 2*

Configure the SXP connection on the switch:

A) Access the console of the HQ-SW.

B) Enable SXP.

```
cts sxp enable
```

C) Configure the SXP session with the ASA (10.10.1.1) with no password and local role set to Speaker.

```
cts sxp connection peer 10.10.1.1 password none mode local speaker
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Verify the SXP connection:

A) On the switch:

```
HQ-Sw# show cts sxp connections
 SXP              : Enabled
 Highest Version Supported: 3
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP           : 10.10.1.1
Source IP         : 10.10.1.2
Conn status       : On
Conn version      : 2
Local mode        : SXP Speaker
Connection inst#  : 1
TCP conn fd       : 1
TCP conn password: none
Duration since last state change: 0:00:07:41 (dd:hr:mm:sec)
Total num of SXP Connections = 1
```

B) On the ASA:

```
HQ-ASA# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Not Set
Default local  IP  : Not Set
Reconcile period   : 120 secs
Retry open period  : 120 secs
Retry open timer   : Not Running
Total number of SXP connections: 1
Total number of SXP connections shown: 1
----------------------------------------------------------
Peer IP            : 10.10.1.2
Source IP          : 10.10.1.1
Conn status        : On
Conn version       : 2
Local mode         : Listener
Ins number         : 1
TCP conn password  : None
Reconciliation timer   : Not Running
Delete hold down timer : Not Running
Duration since last state change: 0:00:09:31 (dd:hr:mm:sec)
```

### *Step 4*

Access the console of the HQ-SW and map the DMZ server IP address(172.16.1.50) to SGT 4, which has been assigned to the Servers group. If the Servers security group has received a different numeric value when you defined it in ISE, you will have to modify the value shown in the sample command.

```
cts role-based sgt-map 172.16.1.50 sgt 4
```


https://t.me/learningnets

### *Step 5*

Access the console of the ASA and examine the SGT mapping table:

A) Using **show cts sgt-map**, without any arguments, you should see all of the SGT mappings that the ASA is aware of, including the DMZ server. The show cts sgt-map command also offers several arguments to focus on particular security groups or particular IP addresses and to control the detail of the output.

```
HQ-ASA# show cts sgt-map
Active IP-SGT Bindings Information
IP Address          SGT   Source
============================================================
10.10.1.2             2   SXP
10.10.2.2             2   SXP
<output omitted>
172.16.1.50           4   SXP
IP-SGT Active Bindings Summary
============================================
<output omitted>
```

B) You can also use the **show cts sxp** command to provide details on the mappings and where they were learned from. Execute this command, but focus on **sgt-map sgt 4**.

```
HQ-ASA# show cts sxp sgt-map sgt 4
Total number of IP-SGT mappings : 11
Total number of IP-SGT mappings shown: 2
SGT         : 4
IPv4        : 10.10.3.20
Peer IP     : 10.10.1.2
Ins Num     : 1
Status      : Active
SGT         : 4
IPv4        : 172.16.1.50
Peer IP     : 10.10.1.2
Ins Num     : 1
Status      : Active
```

### *Step 6*

Before configuring an SGFW ACL on the ASA in the next step, verify that you currently can connect via FTP to the DMZ server (**ftp.secure-x.public or 172.15.1.50**). Use a command prompt window on to the **Employee-PC** (where you are logged in as **it1**. The FTP connection from the Employee-PC should succeed. When challenged for credentials, use **anonymous** with any password you like. Use the **bye** command to terminate the session.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 7***

Configure an ACL using SGFW properties on the ASA:

The ACL will be applied to the inside interface. The ACL will have two lines. The first will deny FTP traffic that is sourced from the IT security group and destined to the Servers security group. The second will permit all other traffic.

A) In ASDM, navigate to **Configuration > Firewall > Access Rules**.

B) Currently the inside interface only has the implicit incoming rule. Select the **inside** interface and the select **Add > Add Add Access Rule**.

C) In the Add Access Rule window, define the rule as follows:

Action: **Permit**

Source Criteria Security Group: **IT** (expand the ellipses (**...**) to select the security group)

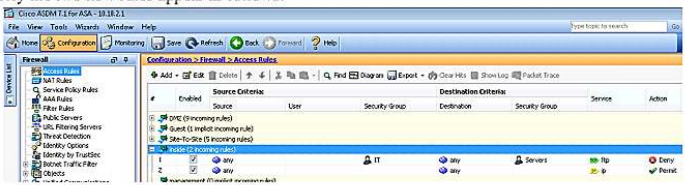
Destination Criteria Security Group: **Servers** (expand the ellipses (**...**) to select the security group)

Destination Criteria Service: **tcp/ftp**

Accept the default values for the other fields and click **OK**.

D) With the new access rule highlighted in the Access Rules table, select **Add > Add Access Rule** a second time. The default values shown in the Add Access Rule windows permits all IP traffic. Accept the default values and click **OK**.

E) Verify the two new rules appear as follows:




F) **Apply** the changes and **Send** the commands.


https://t.me/learningnets

### *Step 8*

Verify the SGFW filtering on the ASA:

A) On the Employee-PC, use a command prompt window and attempt to FTP **ftp.secure-x.public** (or **172.16.1.50** if you prefer). The connection attempt will fail. You will not be challenged for credentials. Use the **bye** command to terminate the FTP client.

B) Currently the policy that is in place on the HQ-SW and the ASA will prevent it1 from the Employee-PC to reach the ISE server in any fashion and it will prevent FTP to the HQ-Srv and the DMZ-Srv. Other connectivity should be allowed. For example, try to ping the DMZ-Srv and try to FTP to ftp.sp.public. Both of these should succeed.

C) On the ASA, examine the hits of the access-list. ASDM sets the name for the access list to **inside_access_in**. Use the command **show access-list** inside_access_in to display the access list entries along with their hit counters. You should hits on the line that references SGTs, corresponding to the FTP attempts you just made.

```
access-list inside_access_in; 2 elements; name hash: 0x433a1af1
access-list inside_access_in line 1 extended deny tcp security-group tag
3(name="IT") any security-group tag 4(name="Servers") any eq ftp (hitcnt=6)
0x1beba637
access-list inside_access_in line 2 extended permit ip any any (hitcnt=85)
0xa925365e
```

# Task 7: Implement Downlink MACsec (Optional)

In this task, you will configure the switch port for downlink MACsec, adjust the authorization profile for the IT users on the ISE, and enable MACsec protection in the AnyConnect supplicant. You will set the protection status to 'should secure'.

### Activity Procedure

Complete the following steps:

### *Step 1*

Enable MACsec on GigabitEthernet0/1 where Employee-PC is connected:

A) Change the 802.1X host mode to single. Multi-host is not supported with MACsec.

```
authentication host-mode single-host
```

B) Enable MAC security.

```
macsec
```

C) Enable the default MACsec Key Agreement (MKA) policy.

```
mka default-policy
```

D) Set the link security policy to 'should-secure'. It is the default setting.

```
authentication linksec policy should-secure
```

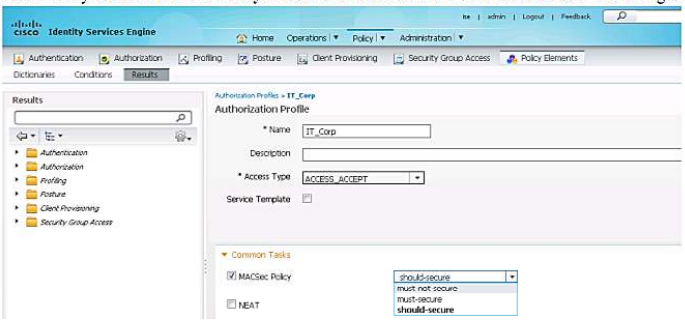

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

On the ISE, set the MACsec policy in the authorization profile for IT users:

A) In ISE, navigate to **Policy > Policy Elements > Results, Authorization > Authorization Profiles**.

B) Select the authorization profile for IT users (**IT_Corp**). Under Common Tasks, scroll down to find MACsec Policy. Check **MACsec Policy** and select **should-secure** from the menu. **Save** the changes.



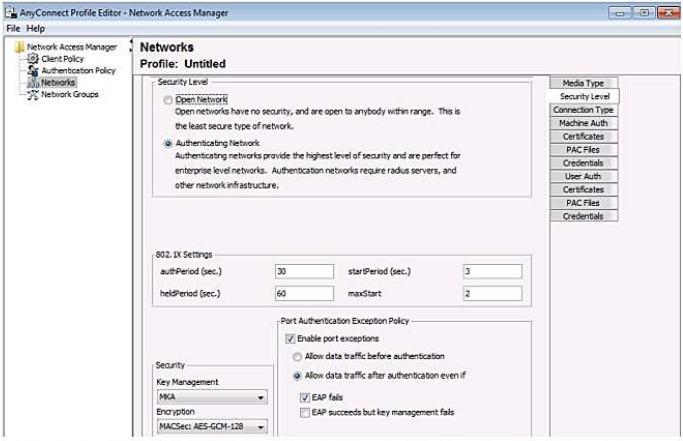
***Step 3***

On the Employee-PC, enable the AnyConnect supplicant for MACsec:

A) Open the Network Access Manager Profile Editor via **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Network Access Manager Profile Editor**.

B) Go to **Network Access Manager > Networks**. Select the default entry '**wired**' and click **Edit**.

C) Select the **Security Level** tab, which is the second tab from the top. In the Security section, set the key management to MKA and encryption to MACsec: AES-GCM-128.




D) Select the **Credentials** tab at the bottom of the tabs list and click **Done**. Use **File > Save As** to save the profile. Save the profile as **configuration.xml** without changing the path to which the file is saved.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Verification

#### *Step 1*

On the switch, view the authentication status of the access port. The security status should be still unsecured.

```
HQ-Sw#show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.10.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  10
              ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
                  SGT:  0003-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000004D0BCE6BD6
      Acct Session ID:  0x00000078
               Handle:  0x5B00004E
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

#### *Step 2*

On the Employee-PC, reset 802.1X connection using the updated AnyConnect profile by right-clicking the AnyConnect icon from the system tray and choosing **Network Repair**. Wait until you see the AnyConnect notification that indicates that you are connected to Wired. This can take a minute.

#### *Step 3*

On the Employee-PC, verify that you have network connectivity by using a browser to view **http://hq-srv**.


https://t.me/learningnets

***Step 4***

On the switch examine the MACsec-related information.

A) View the authentication status of the access port. The security status should be secured.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.10.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  10
              ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
                  SGT:  0003-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000004D0BCE6BD6
      Acct Session ID:  0x00000078
               Handle:  0x5B00004E
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

B) Examine the MACsec information for the interface:

```
HQ-Sw# show macsec interface gigabitEthernet 0/1
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 Transmit Secure Channels
  SCI : ACF2C55BFC010002
   Elapsed time : 14:41:38
   Current AN: 0   Previous AN: -
   SC Statistics
    Auth-only (0 / 0)
    Encrypt (88101 / 0)
 Receive Secure Channels
  SCI : A0369F1A3BB10000
   Elapsed time : 14:41:38
   Current AN: 0   Previous AN: -
   SC Statistics
    Notvalid pkts 0       Invalid pkts 0
    Valid pkts 8438          Late pkts 10
    Uncheck pkts 0        Delay pkts 0
  Port Statistics
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Ingress untag pkts  0          Ingress notag pkts 89549
Ingress badtag pkts 0          Ingress unknownSCI pkts 0
Ingress noSCI pkts 0           Unused pkts 0
Notusing pkts 0                Decrypt bytes 1681652
Ingress miss pkts 89549
```

C) View the current MACsec Key Agreement (MKA) sessions. You should see the details for the session established with the Employee-PC.

```
HQ-Sw# show mka sessions
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0
=============================================================================
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status   CKN
=============================================================================
Gi0/1     a036.9f1a.3bb1/0000 *DEFAULT POLICY* 0A0A01020000004D0BCE6BD6
2         acf2.c55b.fc01/0002 YES     Secured  C8F4EA15380FC0815B229E7BE4AC6D7B
```

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 4-1: Implement WebAuth for Employees

## Activity Objective

In this activity, you will configure and deploy Central WebAuth for enterprise employees. Central WebAuth can provide access to users from devices which do not have an 802.1X supplicant. The configuration procedure involves the configuring appropriate settings on the switch and in the Cisco ISE GUI. You will configure the MAB authentication policy to continue if the user is not found in the local user database. You will modify the guest portal identity store sentence and the authorization policy to enable WebAuth for employees.

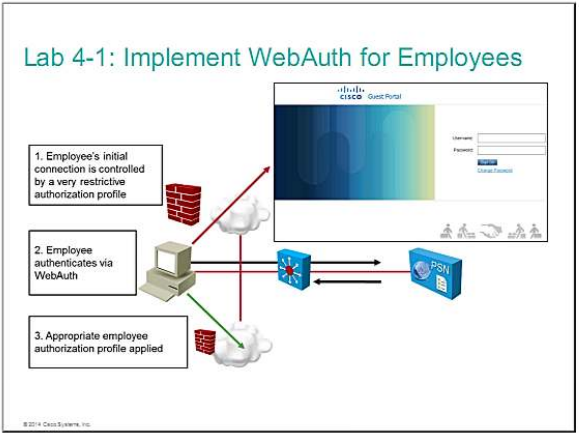
You will be able to meet these objectives:

- Implement Central WebAuth on a switch
- Configure ISE authentication for WebAuth
- Configure ISE authorization for WebAuth

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Configure Switch for Central WebAuth

In this task, you will prepare the HQ-Sw to support Central Web Authentication. You will enable CoA on the switch, configure an ACL to specify traffic for redirection to the web authentication portal, enable the HTTP and HTTPS services on the switch, and configure interface G0/2 (where the Guest-PC attaches) for dynamic authentication and authorization.

### Activity Procedure

Complete the following steps:

#### *Step 1*

On the switch, enable the Change of Authorization (CoA) feature, specifying that it is a client to ISE. CoA will allow ISE to send an updated authorization policy to the switch when ISE recognizes a change in status. In this case, the initial policy will be to implement redirection of web traffic to ISE's Web Authentication portal. After a user successfully authenticates to ISE, ISE can use CoA to send the appropriate, user-specific profile to the switch. Use the same key that is used for RADIUS peering (**radius-key**).

```
aaa server radius dynamic-author
 client 10.10.2.20 server-key 0 radius-key
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 2

Configure an ACL that will be used to classify the traffic that will be redirected to WebAuth. This ACL should permit all HTTP (TCP/80) and HTTPS traffic (TCP/443). All web traffic should be redirected to the Web Authentication portal. The ACL will be referenced by an authorization profile configured later on the ISE.

```
ip access-list extended ACL-WEBAUTH-REDIRECT
 permit tcp any any eq 80
 permit tcp any any eq 443
```

### Step 3

Generate an RSA key pair with modulus 2048, and enable HTTP and HTTPS service. The RSA key pair is needed to support HTTPS connections. The switch must run the HTTP and HTTPS services to be able to redirect users to Central WebAuth running on the Cisco ISE.

```
crypto key generate rsa modulus 2048
!
ip http server
ip http secure-server
```

### Step 4

This lab exercise will use the Guest-PC to demonstrate the functioning of WebAuth. The Guest-PC is connected to interface G0/2 on the HQ-Sw. Copy the relevant configuration of G0/19 (where the Print Server is connected) to interface G0/2. Do not copy the description or access VLAN commands. They are already correct on interface G0/2 (description Guest-PC and access VLAN 11).

```
interface GigabitEthernet0/2
 ip access-group Basic-ACL in
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
```

# Task 2: Configure ISE Authentication for WebAuth

In this task, you will configure the MAB authentication policy to continue if the user is not found in the local user database. You will also tune the default guest portal settings: disable the self-provisioning flow and allow authentication against the Active Directory.


https://t.me/learningnets

**Activity Procedure**

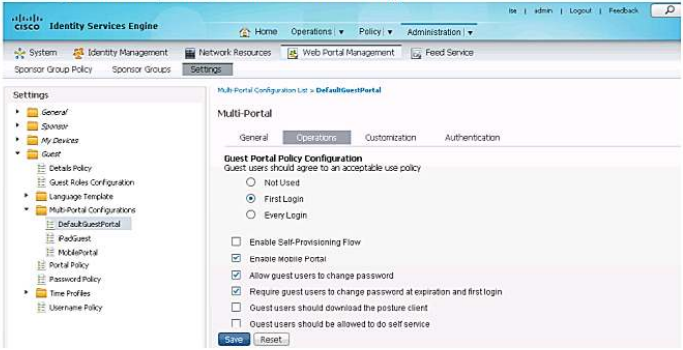
Complete the following steps:

***Step 1***

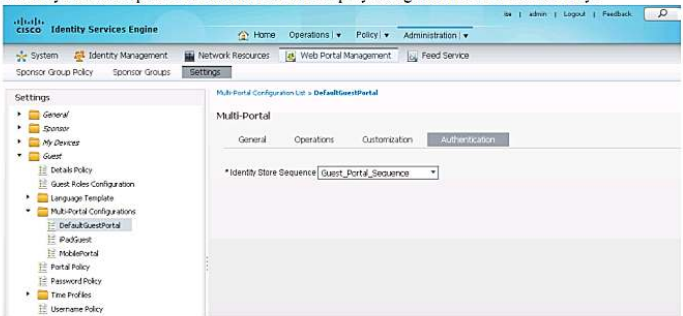
Examine and tune the default guest portal settings:

A) Go to **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations > Default Guest Portal**.

B) Click the **Operation** tab. Disable **Enable Self-Provisioning Flow** and click **Save**.




C) Click the **Authentication** tab. Examine which identity store sequence is used by default. You should see that the Guest_Portal_Sequence is the default selection. When web traffic is later redirected to WebAuth, this source sequence defines the user databases to consult. In the next step you will modify this identity source sequence to authenticate the employees against the Active Directory.





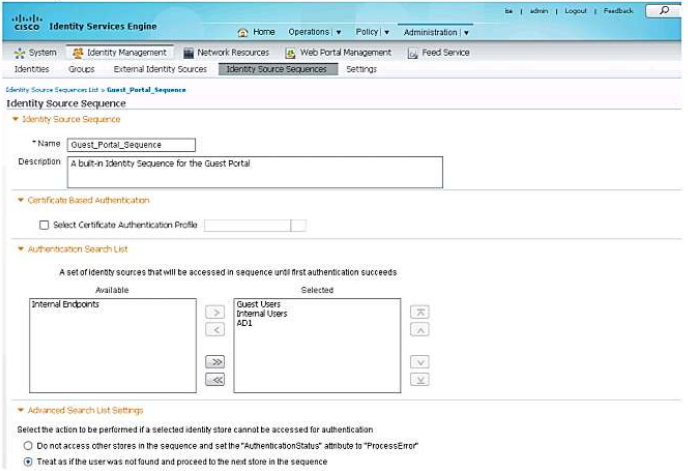
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

Modify the identity store sequence Guest_Portal_Sequence to enable authentication against the Active Directory if the user is not found locally.

A) Navigate to **Administration > Identity Management > Identity Source Sequences** menu.

B) Select **Guest_Portal_Sequence** and click **Edit**. Select AD1 and move to the right pane. It should be placed last, after Internal Users.



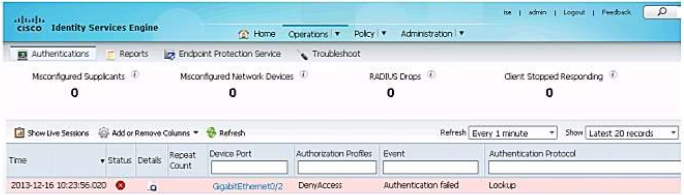

C) **Save** the changes.


https://t.me/learningnets

***Step 3***

In the previous task, you configured 802.1X and MAB on interface G0/2. There has been some authentication activity since it was configured. Examine the failed access attempts through the Gigabitethernet0/2 interface:

A) Go to **Operations > Authentications** and view the access attempts.




B) Click the details button and examine the failure reason. Examine the steps that are listed on the right side of the details report. You should see steps that are similar to what is shown below. MAB fails when the Guest-PC MAC address is not found in the internal endpoints database. After MAB failure, the Continue option is implemented. This leads to looking for the Guest-PC MAC address in Active Directory. This also fails, and the authorization profile named DenyAccess is applied. The DenyAccess profile leads to a RADIUS Access-Reject. In the next tasks you will configure the ISE authorization policy to support WebAuth.

```
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
15048 Queried PIP
15004 Matched rule
15041 Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Source -
24209 Looking up Endpoint in Internal Endpoints IDStore - A0:36:9F:1A:3D:AE
24217 The host is not found in the internal endpoints identity store
22056 Subject not found in the applicable identity store(s)
22058 The advanced option that is configured for an unknown user is used
22060 The 'Continue' advanced option is configured in case of a failed
authentication request
15036 Evaluating Authorization Policy
24432 Looking up user in Active Directory - A0:36:9F:1A:3D:AE
24412 User not found in Active Directory
15004 Matched rule - Default
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 3: Configure ISE Authorization to Enforce Traffic Redirection

You will start this task by creating a new dACL which will control access prior to web authentication. You will you will create an authorization profile, named WEBAUTH, that references the dACL and enforces traffic redirection to the WebAuth portal. Authorization profiles need to be referenced by authorization policy rules. You will configure an authorization rule that pushes the WEBAUTH authorization profile after a MAB failure. This state is recognized with the condition NetworkAccess:Use Case=Host Lookup. You will finish by verifying the behavior from the Guest-PC. As you configured in the previous step, when MAB fails, the process continues. The result is passed to the authorization process which will match the authorization rule for web authentication. The NAD is instructed to implement redirection of HTTP and HTTPS traffic to the ISE web authentication portal.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Create a new dACL named Pre-WebAuth which permits basic networking services and communications with the policy service features in ISE.

A In ISE, navigate to **Policy > Policy Elements > Results, Authorization > Downloadable ACLs**.

B Click **Add**.

C Enter **Pre-WebAuth** in the Name field.

D Define the ACL entries as follows:

```
permit udp any any eq bootps
permit udp any any eq domain
permit icmp any any echo
permit icmp any any echo-reply
permit tcp any any eq www
permit tcp any any eq 443
permit tcp any host 10.10.2.20 eq 8443
permit tcp any host 10.10.2.20 eq 8905
permit tcp any host 10.10.2.20 eq 8909
permit udp any host 10.10.2.20 eq 8905 8906
permit udp any host 10.10.2.20 eq 8909
```

**Note** This ACL is more complex than it needs to be at the moment, but it demonstrates what is commonly put in the ACL. The first two lines permit DHCP and DNS. ICMP echo and echo reply are allowed for troubleshooting. HTTP and HTTPS are required to allow the traffic that would be redirected. Port 8443 is used by the ISE guest portal. 8905 and 8906 are used by the NAC Agent Swiss protocol (used for profiling). 8909 is used for client provisioning activity.

E Expand the **Check DACL Syntax** option. If it does not report that the DACL syntax is valid, recheck your work.

F Click **Submit**.


https://t.me/learningnets

***Step 2***

Create a new authorization profile (**Policy > Policy Elements > Results, Authorization > Authorization Profiles > Add**). Configure these attributes:

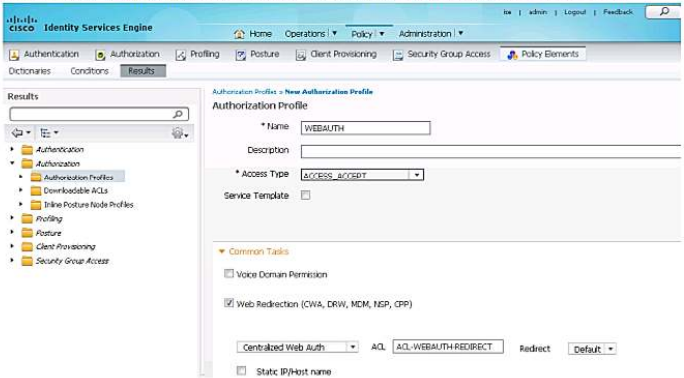
A) **Name: WEBAUTH**

B) **Access Type: ACCESS_ACCEPT**

C) **dACL: Pre-WebAuth**

| **Note** | This ACL controls traffic allowed prior to successful authentication of the user by WebAuth. |
|---|---|

D) **Web Redirection: Centralized, ACL: ACL-WEBAUTH-REDIRECT, Redirect: Default**




| **Note** | This ACL does not block traffic. It specifies which of the allowed traffic is redirected to the web authentication portal. |
|---|---|

| **Note** | Make sure that the redirect ACL name matches exactly the ACL configured on the switch. |
|---|---|

E) Click **Submit**.

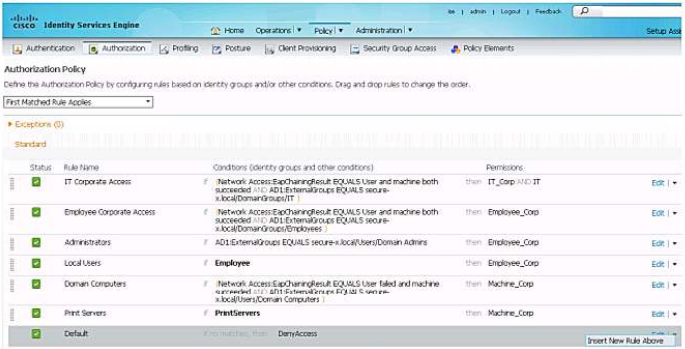
| **Note** | The goal is to push this authorization profile to the authenticating interface on the NAD when the endpoint doesn't have a supplicant (hence, 802.1X fails) and the endpoint MAC address is not in ISE's internal endpoint database (hence MAB fails). In the previous task, you configured the MAB authentication rule to continue when the user (MAC address) was not found. In the next step, you will configure an authorization policy rule that will apply this authorization profile under those circumstances. With this authorization profile pushed to the NAD, when the user on the endpoint opens a browser and generates some web traffic, the traffic will be redirected to WebAuth. |
|---|---|


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

In the authorization policy (**Policy > Authorization**), add an additional rule (**WebAuth**) before the last rule (**Default**). It will use be used to enforce traffic redirection to WebAuth.

A) Click the drop down menu arrow near the **Edit** link of the **Default** rule and choose **Insert New Rule Above.**




B) Change the name from Standard Rule 1 to **WebAuth**. In the **Conditions** field, select **Create New Condition (Advanced Option).**

C) Define the Expression as follows: Attribute: **Network Access:Authentication Status**, Operator: **Equals**, Value: **UnknownUser**.

D) In the **Permissions** field, choose **Standard > WEBAUTH**.

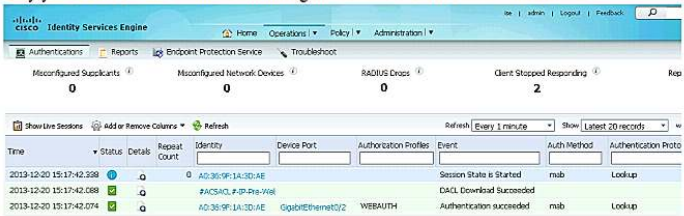
E) Click **Save**.


https://t.me/learningnets

## Activity Verification

### *Step 1*

View the access attempts in Cisco ISE. In the **Operations > Authentications** menu you will see a successful authentication of the Guest-PC MAC address. The authentication method is MAB, the authentication protocol is **Lookup**, and the authorization profile is **WEBAUTH**. After the event of applying this policy you should see the event documenting the download of the **Pre-WebAuth** dACL.




### *Step 2*

Click the details link for event where the WEBAUTH authorization profile is applied. Examine the steps documented on the right hand side of the details report. The steps should be similar to what is shown below.

```
   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
   15048 Queried PIP
   15004 Matched rule
   15041 Evaluating Identity Policy
   15006 Matched Default Rule
   15013 Selected Identity Source -
   24209 Looking up Endpoint in Internal Endpoints IDStore - A0:36:9F:1A:3D:AE
   24217 The host is not found in the internal endpoints identity store
   22056 Subject not found in the applicable identity store(s)
   22058 The advanced option that is configured for an unknown user is used
   22060 The 'Continue' advanced option is configured in case of a failed
authentication request
   15036 Evaluating Authorization Policy
   24432 Looking up user in Active Directory - A0:36:9F:1A:3D:AE
   24412 User not found in Active Directory
   15048 Queried PIP
   15004 Matched rule - WebAuth
   15016 Selected Authorization Profile - WEBAUTH
   11022 Added the dACL specified in the Authorization Profile
   11002 Returned RADIUS Access-Accept
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Examine the authentication and authorization of the client on the switch. You should see that the ISE sent to the switch the Pre-WebAuth dACL, the name of URL Redirect ACL and the redirect URL. The redirect URL includes the common session ID, visible in the output.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  A0-36-9F-1A-3B-B2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Pre-WebAuth-517998c3
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A0102000000A423990BA6&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000A423990BA6
      Acct Session ID:  0x000000DC
               Handle:  0x0D0000A5
Runnable methods list:
       Method   State

       mab      Authc Success
       dot1x    Not run
```


https://t.me/learningnets

***Step 4***

The Web Authentication policy is in place on interface G0/2. The Guest-PC which is connected to this interface. Submit a connection request from Internet Explorer on the Guest-PC.

Connect to the **Guest-PC.** If needed, log in as **student** with the password **Ci5coAdmin**.

Open Internet Explorer and connect to the HQ server (**http://hq-srv**). You should be redirected to the guest portal.

| | |
|---|---|
| **Note** | The specification of any valid HTTP URL would suffice. In fact, with most browsers today, entering any string into the URL entry field leads to a search engine query for that string. In such cases, the search engine query would still be intercepted and a connection to the web authentication portal would result. |

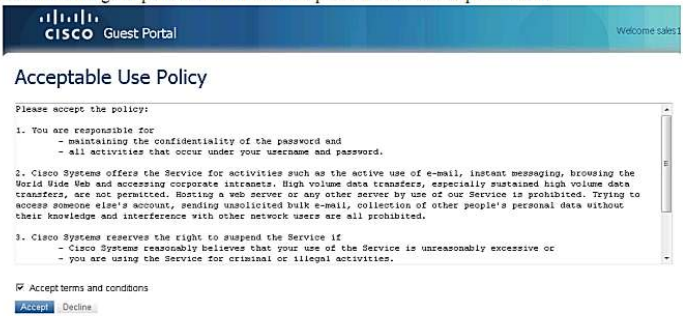
Before authenticating, examine the redirection URL. Note that the URL ends with the session ID.

| | |
|---|---|
| **Note** | The common session ID is what keeps ISE and the switch in sync with operations. The session ID embedded in the URL is identical to the common session ID that was documented on the switch. Because it is carried in the URL, the ISE web portal can identify that the user is trying to authenticate for this particular session ID amongst any other WebAuth sessions that may be running in parallel. |


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 5

Authenticate to the guest portal as **sales1** with the password **cisco**. Accept the AUP.




### Step 6

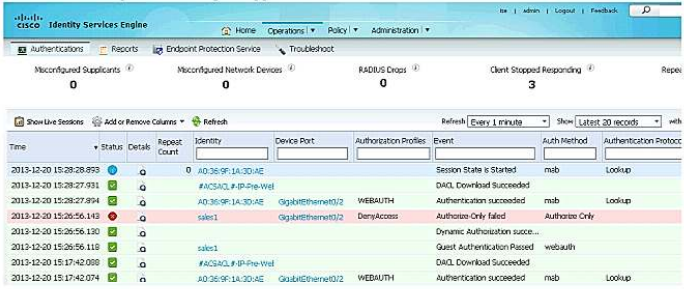
You should be notified of a success and instructed to retry the original request.

### Step 7

Attempt to connect to HQ-SRV again. This will take you to the guest portal again, because you have not yet configured an authorization rule for employees authenticated via WebAuth. This will be completed in the next task.

***Step 8***

Before configuring an authorization rule for employees authenticated via WebAuth, examine the status of ISE's live authentications at **Operations > Authentications**. You should see that after the application of the WEBAUTH profile that the user sales1 did indeed pass Guest Authentication. But then authorization failed. There were no authorization policies that matched the guest authenticated user, so the default rule applied. Then the WEBAUTH profile was again applied.




# Task 4: Configure ISE Authorization Rule for Employees Authenticated via WebAuth

In this task, you will add an authorization policy rule for employees that authenticate via WebAuth. This rule will need to be placed above the current WebAuth rule. The rule will require that the user is in the Employees group in AD. It will also specify the condition Network Access:Use Case equals 'guest flow'. This condition is met when a user has successfully authenticated via WebAuth, and the switch port is set again for a new MAB.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 1***

Add a new rule, named Employee WebAuth, to the authorization policy to define the access privileges for employees authenticating via WebAuth.

A) In ISE, navigate to **Policy > Authorization**.

B) Place the rule directly after the Employee Corporate Access rule for best readability. The rule could be placed anywhere before the WebAuth rule. Click the arrow near the **Edit** button of the **Employee Corporate Access** rule and choose **Insert New Rule Below.**

C) Change the name from Standard Rule 1 to **Employee via WebAuth**.

D) In the **Conditions** field, select **Create New Condition (Advanced Option)**.

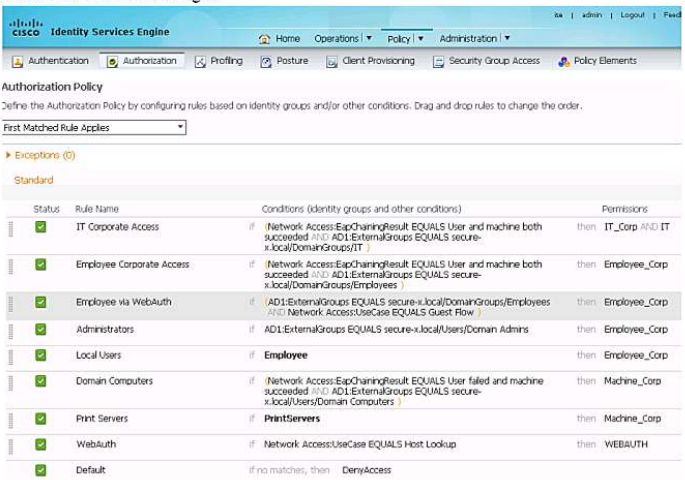
E) Set the expression to Attribute: **AD1 > External Groups**, Operator: **Equals**, Value: **secure-x.local/Users/Employees**.

F) Click the wheel icon to add a second condition and choose **Add Attribute/Value**. You will combine the second condition using the **AND** operator.

G) Define the second expression as: Attribute: **Network Access > Use Case**, Operator: **Equals** Value: **Guest Flow**.

H) In the Permissions field of the new authorization rule, choose **Standard > Employee_Corp**.

I) Click **Done** and **Save** the changes.



### Activity Verification

#### *Step 1*

Complete the authentication process as follows.

From the **Guest-PC**, attempt a new HTTP connection to **HQ-Srv**.

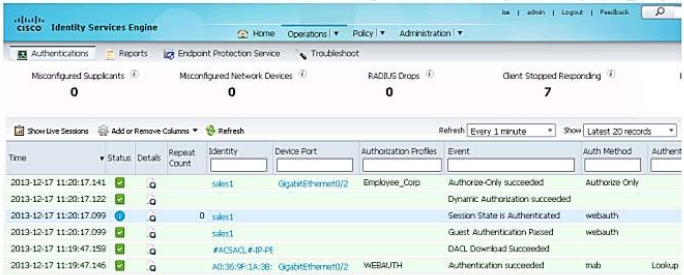
Login as **sales1** with the password **cisco**.

Accept the AUP.

When the portal indicates that you have signed on successfully, attempt to browse the **HQ-Srv** again. This time it should be successful.

#### *Step 2*

Return to ISE and view the authentication information in **Operations > Authentications**. The sequence of event should now end with a successful authorization using the authorization profile Employee_Corp.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

On the switch, verify the authentication status of interface G0/2. You should see a successful authorization of the employee sales1 with an appropriate dACL, and the same common session ID that was in the WebAuth redirect URL.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  sales1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000AB2436A0BA
      Acct Session ID:  0x000000a6
               Handle:  0xDD0000AC
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 4-2: Implement Guest Service

## Activity Objective

In this activity, you will configure and deploy central WebAuth for guests. The configuration procedure involves the appropriate settings on the administration portal, the sponsor portal, and the guest portal. You will use the sponsor portal and the guest portal to implement the entire life cycle of guest users.

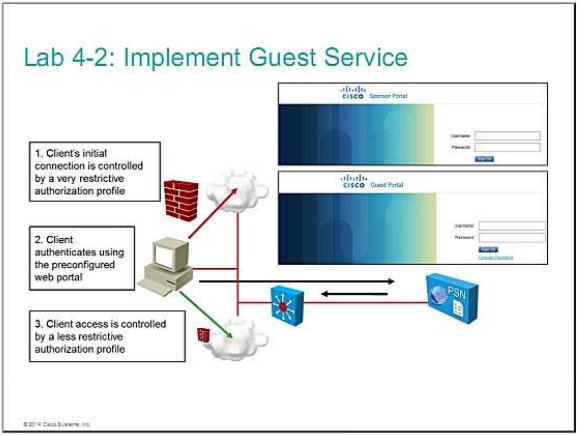
You will be able to meet these objectives:

- Enable guest access using the sponsor portal
- Implement authorization for guest roles

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Configure Access to the Sponsor Portal

In this task, you will configure the Sponsor_Portal_Sequence identity source sequence to authenticate the sponsors against the Active Directory. You will also define two sponsor group policy rules. The first rule will assign domain administrators to the sponsor group privilege SponsorAllAccounts. The second rule will assign domain employees to the sponsor group privilege SponsorGroupGrpAccounts. This will give full sponsor privileges to the domain administrators and group sponsor privileges to the domain employees.

### Activity Procedure

Complete the following steps:

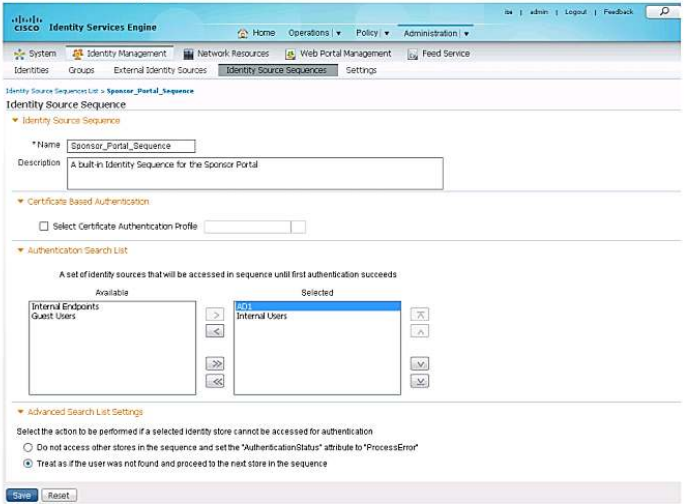
#### *Step 1*

In the Cisco ISE GUI, go to **Administration > Web Portal Management > Settings, Sponsor > Authentication Source**. Observe that the default identity source sequence is called **Sponsor_Portal_Sequence**. You will modify this sequence in the next step.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

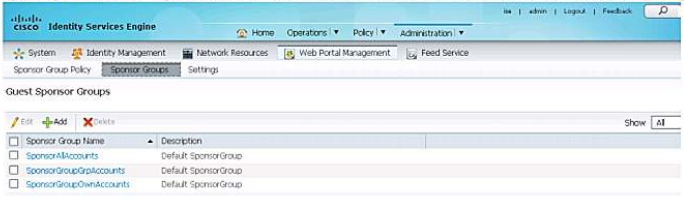
### *Step 2*

Go to **Administration > Identity Management > Identity Source Sequences**, select the **Sponsor_Portal_Sequence**, add the **AD1** database to the selected sources, and move it to the first position in the list. **Save** the changes.




### *Step 3*

Go to **Administration > Web Portal Management > Sponsor Groups**. View the default sponsor groups on the Cisco Identity Services Engine. Observe that there are three default groups: SponsorAllAccounts, SponsorGroupGrpAccounts, and SponsorGroupOwnAccounts. This alphabetic order reflects also the privilege scope - from the highest to the lowest. Click each of them and examine their individual settings.





https://t.me/learningnets

***Step 4***

Assign **Domain Admins** to the first sponsor group and the **Domain Employees** to the second sponsor group.

A) Go to **Administration > Web Portal Management > Sponsor Group Policy**.

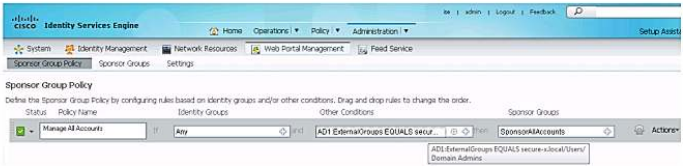
B) There is one policy rule in the table. Modify that rule as follows:

   A Change the Policy Name to **Manage All Accounts**.

   B Set the Identity Groups field to **Any**.

   C In Other Conditions field, choose the **Create New Condition (Advanced Option)**, and then define set the expression to **AD1:ExternalGroups Equals secure-x.local/Users/Domain Admins**.

   D Leave the value of the Sponsor Group field at the default: **SponsorAllAccounts**.



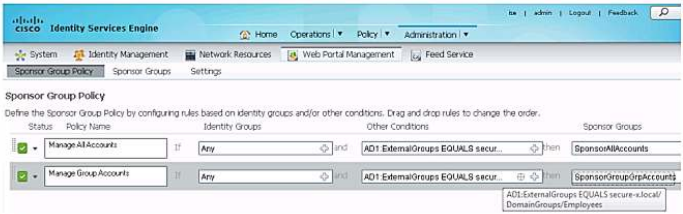

C) Click Actions button on the right and add a new policy below this one. Define the new rule as follows:

   A Name the new rule **Manage Group Accounts**.

   B Set the Identity Groups field to **Any**.

   C In the Other Condition field, choose the **Create New Condition (Advanced Option)**, and then set the expression to **AD1:ExternalGroups Equals secure-x.local/DomainGroups/Employees**.

   D Set the Sponsor Group field to **SponsorGroupGrpAccounts**.




D) Click **Save**.

# Task 2: Provision Guest User in the Sponsor Portal

In this task, you will provision a guest user.

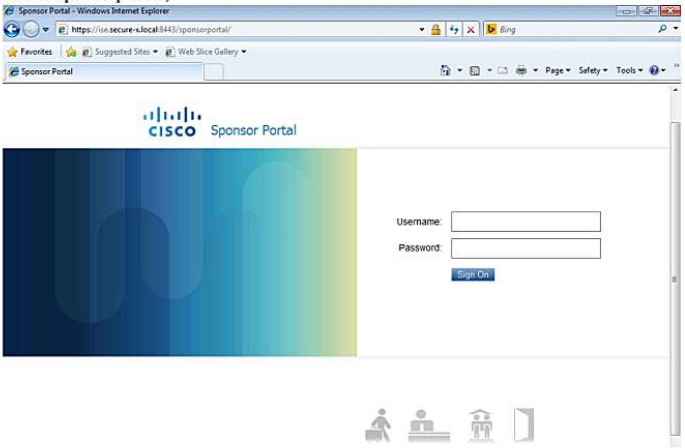

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

**Activity Procedure**

Complete the following steps:

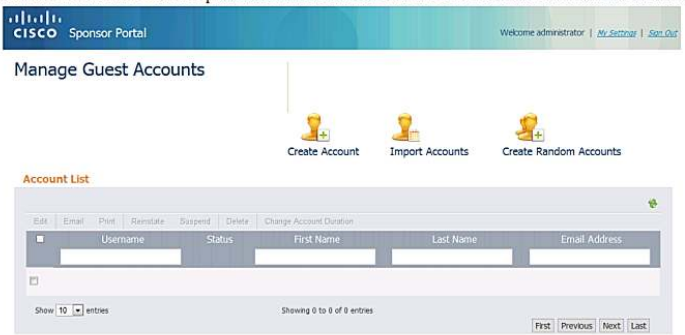
***Step 1***

On the Employee-PC, open the Internet Explorer and connect to the sponsor portal (**https://ise.secure-x.local:8443/sponsorportal/**)




***Step 2***

Log on as **administrator** with the password **Ci5coAdmin**. This is an AD domain administrator account.



### *Step 3*

Define a new guest user account as follows:

A Click **Create Account** to define a single guest user account.

B Specify the first name and last name of your choosing. Observe the default account properties. They are fine to leave as they are. Click **Submit**.

C Review the account details. Write down the username and password in the space provided below. You will test this account later in the lab.

| | |
|---|---|
| Username | |
| Password | |

D Click **View Guest Accounts**. Note that the status of the account is "Awaiting Initial Login."

### *Step 4*

Optionally, log off the portal and log back on as a domain employee (for example, **it1**/**cisco**). Examine the differences in the sponsor portals between full sponsor privileges and group sponsor privileges.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Verification

#### *Step 1*

On the switch, shut down and re-enable the GigabitEthernet 0/2 interface. This is the interface which is connected to the Guest-PC. Wait about 30 seconds, until the authorization profile is applied to the switch port. Verify the port authentication and authorization status.

```
HQ-Sw#show authentication sessions interface g0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  A0-36-9F-1A-3B-B2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-Pre-WebAuth-52b309e2
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
        URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A0102000000C7299C9DE0&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000C7299C9DE0
      Acct Session ID:  0x00000106
              Handle:  0xD60000C8
Runnable methods list:

       Method   State
       mab      Authc Success
       dot1x    Not run
```

#### *Step 2*

On the Guest-PC, in the Internet Explorer, connect to **http://hq-srv.secure-x.local**. You should be redirected to the WebAuth portal.

### *Step 3*

Test the new guest account:

A Log on using the credentials assigned to the new guest account.

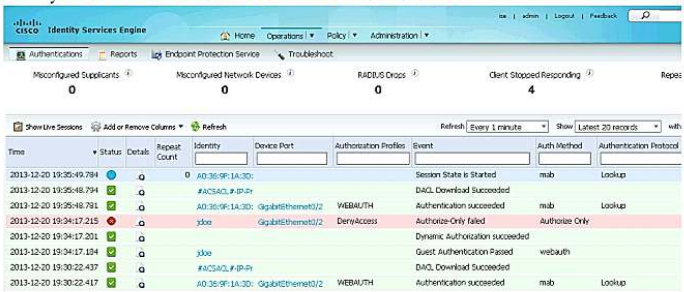
B Accept the AUP.

C You must change the password on first login. Change the password according to the password policy (default policy is at least one numeral 0-9 and at least one alphabetic character a-Z).

**Note** The password policy is one of many things that can be customized. It is defined at **Administration > Web Portal Management > Settings, Guest > Password Policy**.

### *Step 4*

In the Cisco ISE GUI, verify the authentication. The events should include, from bottom to top, the application of the WEBAUTH authorization profile, the download of the Pre-WebAuth dACL, the authentication of the guest account, and the application of the DenyAccess authorization profile via the Default Policy authorization policy rule. As shown in the figure, after 90 seconds the WEBAUTH policy is automatically reinstated. You do not have to wait for that status to continue.




### *Step 5*

Try to connect to www.cisco.com. This attempt will fail and you will be redirected to the guest portal again.

# Task 3: Configure Authorization for Guest Users

Having provisioned a guest user account, you need to define the appropriate authorization policy rule for the guest users. You will define a new authorization profile and then reference the profile in a new authorization policy rule. The policy rule will apply to authenticated guest accounts.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Define a new authorization profile for guest access.

In the ISE GUI, navigate to **Policy > Policy Elements > Results, Authorization > Authorization Profiles**.

Click Add to create a new profile.

Name the profile **Guest_Profile** and assign the access type **ACCESS_ACCEPT** and the dACL **Contractor_FullAccess_DACL**.

| | |
|---|---|
| **Note** | The dACL Contractor_FullAccess_DACL denies ICMP to the ISE host and to the HQ-Srv and it blocks HTTP to the HQ-Srv. It permits all other connections. |

Click **Submit**.

#### *Step 2*

In the authorization policy , add an additional rule (**Guests**) before the **WEBAUTH** rule. It should define the access privileges for the **Guest** and **ActivatedGuest** roles.

A) Navigate to **Policy > Authorization**.

B) Select the current **WebAuth** rule, and using the drop down arrow icon on the right, select **Insert New Rule Above**.

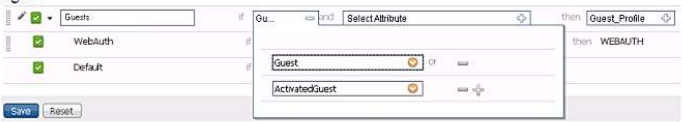
C) Change the name of the rule from Standard Rule 1 to **Guests**.

D) In the **Identity Group** field (currently set to Any), choose **User Identity Groups > Guest**

E) Click the + sign and add the **User Identity Groups > ActivatedGuest** selection. The two entries are automatically combined using the or operator, which you cannot change.

| | |
|---|---|
| **Note** | Guest and ActivatedGuest are the two guest roles that are available and defined by the guest sponsor when the account is created. The default is Guest. The difference is that users with the Guest role must authenticate via the web portal. ActivatedGuests can also authenticate via the web portal but have the option to authenticate via an 802.1X supplicant as well. |

F) Do not define any other conditions. Set the permission to **Standard > Guest_Profile** and **Save** the changes.




### Activity Verification

#### *Step 1*

From the Guest-PC try to browse to the HQ-SRV again. You will be redirected to the guest portal. Log in as the guest user.


https://t.me/learningnets

### *Step 2*

In the Cisco ISE GUI, examine the live authentication sessions. This time the event sequence should include the assignment of the authorization profile named Guest_Profile. The Contractor_FullAccess_dACL downloaded in response to the profile assignment.

### *Step 3*

Test connectivity from the Guest-PC. Browsing the HQ-SRV will fail as it is blocked by the dACL. But you can browse other sites, such as www.secure-x.public (DMZ-SRV), www.sp.public (the SP-Srv) or www.cisco.com


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 4*

On the switch, view the authentication status of interface G0/2 and view the downloaded ACL.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  kzygis
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Contractor_FullAccess_DACL-52777d60
      Session timeout:  24900s (server), Remaining: 24525s
       Timeout action:  Terminate
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000CB29D59B66
      Acct Session ID:  0x0000010B
               Handle:  0x2D0000CC
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
HQ-Sw# show ip access-lists interface gigabitEthernet 0/2
     deny icmp host 10.10.11.10 host 10.10.2.20
     deny icmp host 10.10.11.10 host 10.10.3.20
     deny tcp host 10.10.11.10 host 10.10.3.20 eq www
     permit ip host 10.10.11.10 any
```


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 5-1: Implement Posture Service

## Activity Objective

In this activity, you will configure client provisioning and posture assessment policies. After the initial preparation of the components you will deploy the Network Admission Control (NAC) agent on the Employee-PC. This functionality is implemented using two Cisco Identity Services Engine policies: the client provisioning policy and the authorization policy. The client provisioning policy defines the NAC agents to be provisioned on endpoints meeting certain criteria. The authorization policy is responsible for redirecting endpoints with unknown posture status to the client provisioning portal and applying appropriate authorization profiles to compliant and noncompliant endpoints. After a NAC agent is provisioned on the Employee-PC, you will deploy some of the automatic remediations available on the ISE: antivirus installation and antispyware definition. You will use policy elements that ISE provides by default which do not discriminate between Anti-Virus (AV) products or Anti-Spyware (AS) products. ClamWin (antivirus) and Windows Defender (antispyware) software will be used for demonstration. You will test the automatic remediations on the Employee-PC. You will deploy the NAC web agent on the Guest-PC. The NAC web agent does not support automatic remediation. So when it determines that the Guest-PC is non-compliant, you will manually install and update the AV/AS software. You will then verify successful posture compliance.

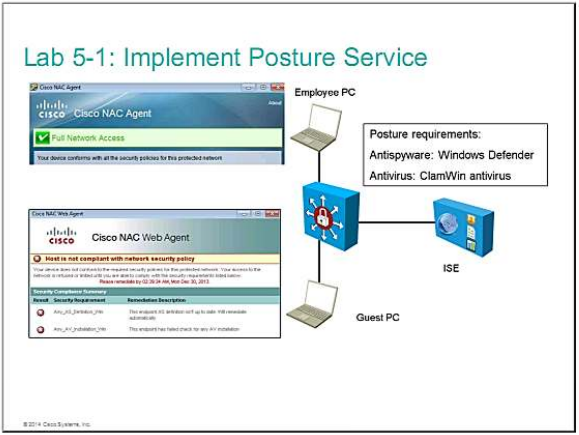
You will be able to meet these objectives:

- Configure client provisioning policy
- Configure authorization policy rules for compliant, noncompliant, and unknown endpoint status
- Configure posture assessment policy

https://t.me/learningnets

# Visual Objective

The figure illustrates what you will accomplish in this activity.




# Task 1: Prepare Initial Components

In this task, you will perform initial preparation. You will configure a redirect ACL on the switch. This ACL will be later referenced by an authorization profile. You will assign administrative privileges to domain users on Employee-PC. The administrative privileges will allow them to install the NAC agent on the Employee-PC. You will also update the posture software elements on the ISE, a process that can take up to 20 minutes and will be therefore started at the beginning of the exercise.

### Activity Procedure

Complete the following steps:

#### *Step 1*

On the switch, configure the redirection ACL for client posture provisioning. Remember, redirection ACLs do not specify whether traffic is permitted or not. They specify wether traffic requires redirection or not. This ACL will permit traffic to be redirected for client provisioning and deny other traffic. This ACL will be later referenced by name in an ISE authorization profile.

```
ip access-list extended CPP-REDIRECT-ACL
 deny udp any any eq bootps
 deny udp any any eq domain
 deny ip any host 10.10.2.20
 permit tcp any host 10.10.3.20
 deny tcp any any eq 80
 deny tcp any any eq 443
 permit ip any any
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

| | |
|---|---|
| **Note** | Line by line this ACL specifies the following: It denies (does not redirect) DHCP and DNS. It also denies (does not redirect) any traffic from the client to ISE. It permits (redirects) HTTP traffic to HQ-srv. It denies (does not redirect) HTTP/HTTPS traffic which are used for antivirus and antispyware remediation downloads. When the IP addresses of the vendor AS/AV remediation downloads are not predictable, a broad deny statement is required. This is the case in this lab environment because the ClamWin antivirus uses a signature definition database mirrored among a large number of servers. Lastly, the ACL permits (redirects) all other traffic. |

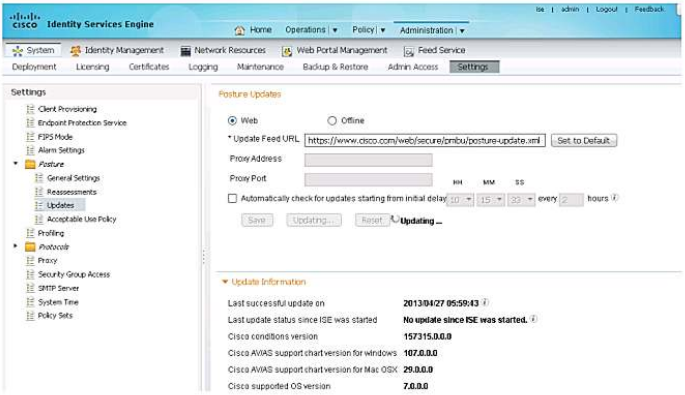
### *Step 2*

In ISE GUI, examine the posture update settings:

A) Go to **Administration > System > Settings, Posture > Updates**. Examine the default settings.

| | |
|---|---|
| **Note** | ISE has automated rulesets covering more than 350 partner applications. In a production environment, it is optimal to keep this data up to date. Note that from this location you can initiate a manual update. You can also schedule automatic checks for updates. |

| | |
|---|---|
| **Note** | In the lab environment we are using AV and AS products that ISE 1.2 supports out of the box. An update can take as long as 20 minutes. There is no need to perform an update for successful completion of the lab. The intention is simply to make you aware of the update issue. |





https://t.me/learningnets

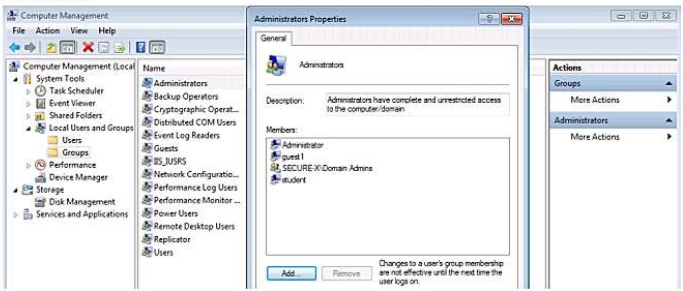
***Step 3***

There are several options NAC agent deployment. This lab exercise will have the NAC agent automatically provisioned on systems taht do not already have it installed. For this to function, the users must have privileges to complete the install. On the Employee-PC, add the domain users from the Employees group to the local administrators group. This will enable the domain users to install the persistent NAC agent.

A) Restart the Employee-PC, and log on as the domain administrator (**secure-x\administrator**) with password **Ci5coAdmin**.

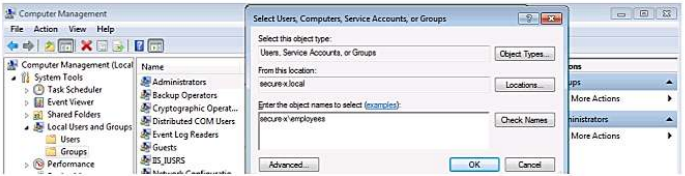
B) Choose **Start**, right-click **Computer** and select **Manage**.

C) Navigate to **Computer Management (Local) > Local Users and Groups > Groups** and double-click **Administrators**.




D) Click **Add**, enter **secure-x\employees**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.




E) Click **Check Names** to verify that the object name was syntactically acceptable. The name should change to Employees without any error messages.

F) Click **OK** twice, close the Computer Management window, and restart the Employee-PC.

# Task 2: Configure Client Provisioning Policy

In this task, you will first download the agent resources to the Cisco ISE and configure the client provisioning policy (CPP). The CPP specifies which software packages will be provisioned by the ISE on the clients. You will assign a persistent NAC agent for Windows computers that connect via 802.1X and a NAC web agent for Windows computers that authenticate via WebAuth.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets

***Step 1***

In the Cisco ISE GUI, download the latest NAC Agent for Windows and the latest NAC Web Agent from Cisco.com:

A) Navigate to **Administration > System > Settings, Client Provisioning**. Examine the default values:

**Enable Provisioning:** Enable

**Enable Automatic Download:** Disable

**Update Feed URL:** https://www.cisco.com/web/secure/pmbu/provisioning-update.xml

**Native Supplicant Provisioning Policy Unavailable:** Apply Defined Authorization Policy

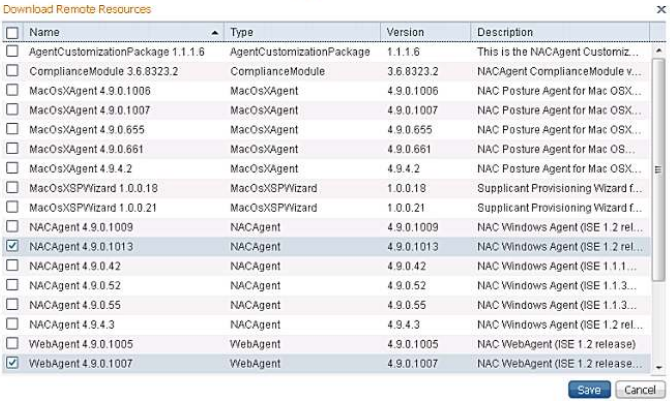
B) Navigate to **Policy > Policy Elements > Results, Client Provisioning > Resources**.

C) Choose **Add > Agent Resources from Cisco site**. After a short while a list of downloadable resources should appear.

D) Choose the following two resources and click **Save**:

The latest NACAgent (NAC Windows Agent version for ISE release 1.2, version 4.9.0.1013 or a newer). This NAC agent will be provisioned on the Employee-PC for IT employees.

The latest WebAgent (NAC WebAgent (NAC WebAgent for ISE release 1.2, 4.9.0.1007 or a newer). This Web agent will be optionally provisioned on the Guest-PC for employees.




E) Wait for the download to complete. Verify that the resources have been successfully downloaded and appear in the Resources table:

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 2***

Configure the client provisioning policy to provision the NAC agent on computers that connect and authenticate via wired 802.1X:

A) Go to **Policy > Client Provisioning**. Currently there are no rules in the table. A blank entry is waiting to be defined. Completet the remaining sub-steps to define the rule.

B) Name the rule **Win7 Wired**.

C) Choose **Windows 7 (All)** in the **Operating System** field **(Windows All > Windows 7 All)**.

D) Expand the **Conditions** field and select **Create New Condition (Advanced Option)**. Define the expression as follows: Attribute: **RADIUS:Service-Type** Operator: **Equals** Value: **Framed**.

E) Add another expression to the condition by clicking the wheel icon on the right and choosing **Add Attribute/Value**.

F) Define the second expression as: Attibute: **RADIUS:NAS-Port-Type** Operator: **Equals** Value: **Ethernet**.

G) Verify that the two conditions are combined using the **AND** operator.

H) Expand the Result field and select the available **NAC Agent** in the Agent subfield.

I) **Save** the client provisioning policy.

# Task 3: Configure Authorization for Compliant, Noncompliant, and Unknown Status

Having defined the appropriate NAC agents that should be provisioned on the clients, you will now configure authorization rules for the various posture conditions. The rule for when the endpoint status is unknown (because there isn't a NAC agent) will redirect the client to the CPP. The rule for when the endpoint status is compliant will set a permissive authorization policy. The rule for a noncompliant endpoint will specify a restrictive policy. Before you can configure these policies, the supporting components must be created, including dACLs and authorization profiles. You will configure the supporting components and the authorization rules during this task.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets

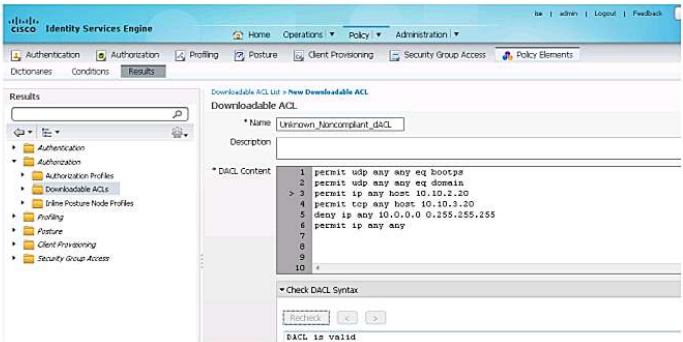
***Step 1***

In the Cisco ISE GUI, configure a dACL for restricting traffic in unknown and noncompliant states.

A) Navigate to **Policy > Policy Elements > Results, Authorization > Downloadable ACLs**. Click **Add**.

B) Configure a dACL named **Unknown_Noncompliant_dACL** that permits DHCP and DNS services, communication with ISE, TCP to HQ-Srv, denies packets to internal systems, and allows Internet connectivity for remediation purposes.

```
permit udp any any eq bootps
permit udp any any eq domain
permit ip any host 10.10.2.20
permit tcp any host 10.10.3.20
deny ip any 10.0.0.0 0.255.255.255
permit ip any any
```




C) **Check** the syntax and **Submit** the dACL.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Configure an authorization profile that redirects traffic to client provisioning. This profile will allow the clients to download the appropriate NAC agent from the CPP portal.

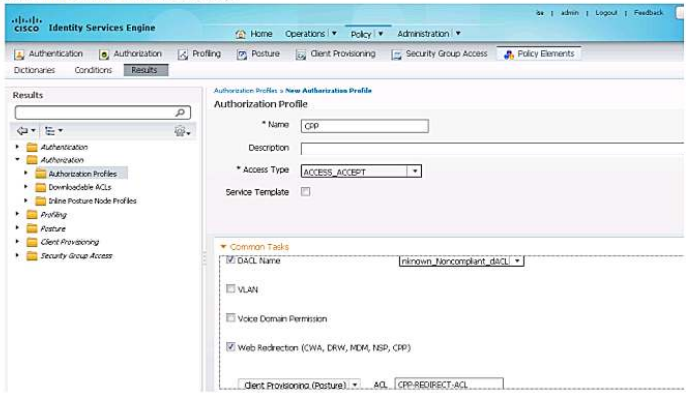
A) Navigate to **Policy > Policy Elements > Results, Authorization > Authorization Profiles**.

B) Click **Add** and create a profile with these attributes:

Name: **CPP**

dACL**: Unknown_Noncompliant_dACL**

Web Redirection to the **Client Provisioning (Posture)** portal and specifying the switch ACL **CPP-REDIRECT-ACL** (make sure that you specify the ACL name exactly as you configured on the switch earlier in this exercise).




Click **Submit** to save the authorization profile.

### *Step 3*

**Add** another authorization profile named **Noncompliant** that pushes the dACL **Unknown_Noncompliant_dACL**. This profile will be used to restrict the traffic from endpoints with an unknown or noncompliant posture status. **Submit** the profile.


https://t.me/learningnets

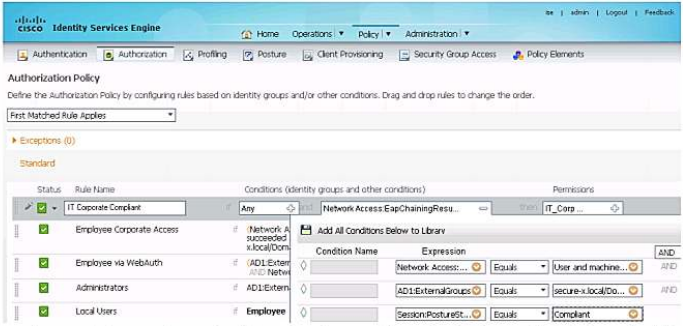
***Step 4***

Configure authorization policy rules to differentiate between unknown, compliant and noncompliant states of IT employee endpoints and to assign the appropriate authorization profile:

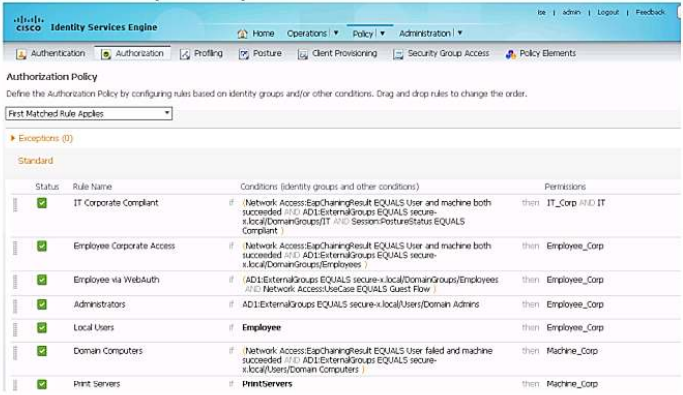
A) Go to **Policy > Authorization**.

B) **Edit** the first authorization rule, **IT Corporate Access**, and rename it to **IT Corporate Compliant.**

C) Click the Other conditions field and add a third expression: Attribute: **Session:Posture Status** Operator: **Equals** Value: **Compliant.** This rule will be matched for compliant endpoints.




D) Leave the permissions unchanged and **Save** the changes. The authorization profile IT_Corp should be applied if the IT user endpoint is compliant.




E) Duplicate the first rule (**IT Corporate Compliant**) placing the duplicate below the first rule (**Edit > Duplicate Below**). Edit the duplicate rule to redirect IT user endpoints with unknown posture status to the client provisioning portal. Change the name, compliance status and the authorization profile as follows:


https://t.me/learningnets
2014 Cisco Systems, Inc.

Change the Name: **IT Corporate Unknown**

Change the value of the value field of the Posture Status expression from Compliant to **Unknown**.

Change the Permissions settings: Select **Standard > CPP** as the first permission and remove the second permission associated with security group tags.

Click the **Done** link.

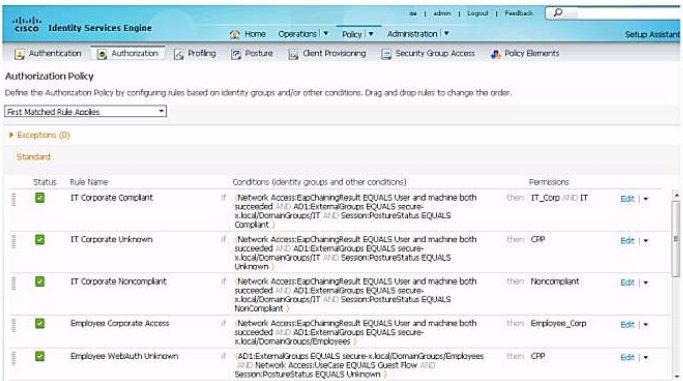
F) Repeat this process, duplicating the second rule below and modify the duplicate rule to restrict IT user endpoints with noncompliant posture status. Change the name, compliance status and the authorization profile:

Name: **IT Corporate Noncompliant**

Third expression of the condition: Attribute: **Session:Posture Status** Operator: **Equals** Value: **Noncompliant**

Permissions: Authorization profile **Standard > Noncompliant.**

Click the **Done** link.




G) **Save** the changes.

### Activity Verification

You have completed this task when you verify that the NAC agent is provisioned on the Employee-PC:

#### *Step 1*

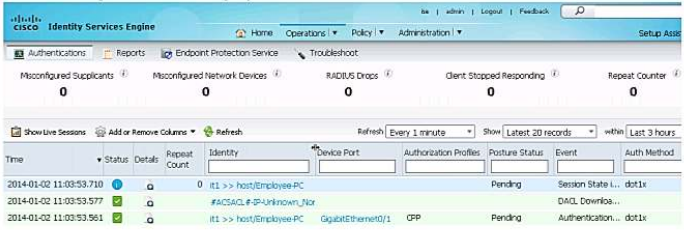
In the Cisco ISE GUI, go to **Operations > Authentications**. Click **Add or Remove Columns**. Enable the **Posture Status** column and save the changes.

#### *Step 2*

On the Employee-PC, log in as **it1** with the password **cisco**.

### Step 3

Since the NAC agent is not yet deployed on the Employee-PC, ISE cannot verify posture status. Before going any further with the Employee-PC, verify what has happened on ISE and the switch. In the Cisco ISE GUI, return to **Operations > Authentications**. The authentication of the user **it1** should be successful. The applied authorization profile should be CPP. The posture status should be pending. The dACL IP-Unknown-Noncompliant has been deployed.




### Step 4

On the switch, check the authentication status of the port. Verify several things of interest: The Unknown_Noncompliant_dACL is deployed. The CPP-REDIRECT-ACL is deployed for redirection. The redirection URL is specified, connecting to ISE on port 8443 with the common session ID and the action=cpp.

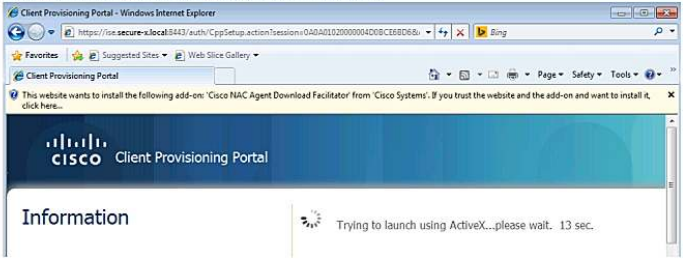
```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Unknown_Noncompliant_dACL-52bd5866
     URL Redirect ACL:  CPP-REDIRECT-ACL
         URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A01020000004D0BCE6BD6&action=cpp
       Session timeout:  N/A
          Idle timeout:  N/A
    Common Session ID:  0A0A01020000004D0BCE6BD6
      Acct Session ID:  0x000001C5
              Handle:  0x5B00004E

Runnable methods list:
       Method   State
       dot1x    Authc Success
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

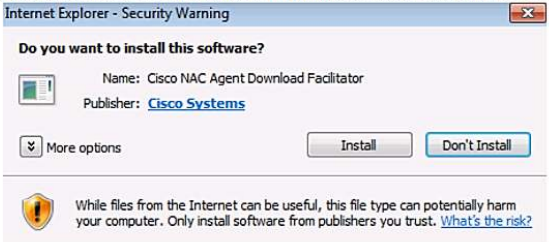
### Step 5

Now, continue with the **Employee-PC**. From the Employee-PC, use Internet Explorer to browse **http://hq-srv**. You will be redirected to the client provisioning portal.




### Step 6

The CPP portal attempts to use Active-X and if that times out it will attempt to use Java. While the ActiveX timer is counting, you will be prompted with an Active-X warning. Click the notification and **accept** the subsequent notifications until you have the option to **Install** the download facilitator Active-X control.





https://t.me/learningnets

***Step 7***

In the portal window, click the **Click to install agent** button to start the NAC agent install.

***Step 8***

Follow the wizard (**Next > Accept the License Agreement > Setup Type 'Complete' > Install > Finish**).

***Step 9***

Wait for the installation to complete.

***Step 10***

Open the NAC agent window by expanding the Windows system tray and clicking the NAC agent icon.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 11*

Note that the NAC agent reports full compliance. This is because, by default, there are no posture policy rules in ISE. You will define posture policy rules in the next task.

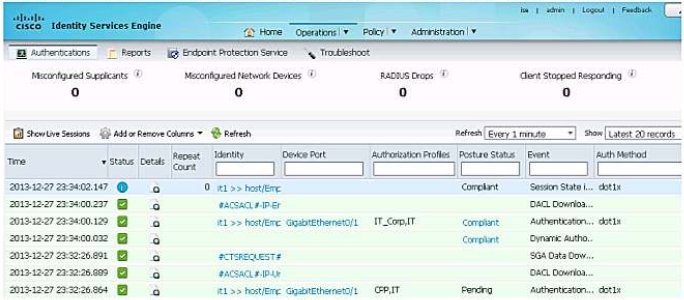
### *Step 12*

Right-click the NAC agent icon and choose **Properties**. You should see a list of antivirus and antispyware products detected by the agent. Note that Windows Defender is installed, but ClamAV is not. Windows Defender is considered Anti-Spyware (AS) and not Anti-Virus (AV).

https://t.me/learningnets

### Step 13

Return to the ISE GUI. You should still be at **Operations > Authentications**. Verify that the authentication has been successful, the posture status is compliant, and a dACL has been pushed to the NAC.




### Step 14

On the switch, verify the authentication and authorization status. You should see that, when the endpoint is identified as compliant, the full access employee ACL has been applied to the session.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.10.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
                 SGT:  0003-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A01020000018B5F29A051
      Acct Session ID:  0x000001E9
              Handle:  0x5100018C
Runnable methods list:
       Method   State
       dot1x    Authc Success
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Task 4: Deploy Antivirus Installation Remediation

In this task, you will deploy the automatic remediation of antivirus software installation and observe its behavior. Cisco ISE comes with simple default posture policy elements. You will utilize these simple elements to configure a posture policy rule that checks for any AV installation on Windows endpoints. Under these conditions, you will observe that the ISE reports a noncompliant status for the Employee-PC. You will then configure a remediation rule that will trigger the ClamWin antivirus installation to remediate the antivirus software status on the Employee-PC.

### Activity Procedure

Complete the following steps:

#### *Step 1*

In the ISE GUI, examine the default posture requirements and conditions. You will find entries for Anti-Virus (AV) and Anti-Spyware (AS) on Windows. In production environments, these elements are usually tightened to match the standard AV and AS products deployed in the organization. For the sake of time, you will use these policy elements as they are to build the posture policy.

A) Navigate to **Policy > Policy Elements > Results, Posture > Requirements**. The posture requirement **Any_AV_Installation_Win** for **Windows** is met when **ANY_av_win_inst** is met. If it is not met, the remediation is **Message Text Only**.

B) Go to **Policy > Policy Elements > Results > Conditions, Posture > AV Compound Condition**. Examine the condition **ANY_av_win_def**. It checks for any AV installation.

#### *Step 2*

Create a posture policy rule that checks the AV installation on Windows endpoints. Navigate to **Policy > Posture** and define the first rule as follows:

A) Name: **AV Installation Win**

B) OS: **Windows All**

C) Requirement: **Any_AV_Installation_Win**

D) **Save** the changes.

### Step 3

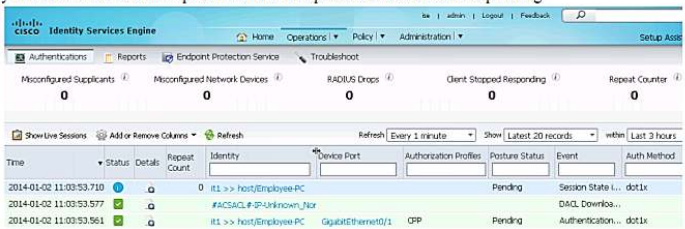
On the switch, perform a **shutdown** and a **no shutdown** to toggle the interface **Gigabitethernet0/1**. This will initiate a new authentication session. After a minute, on the Employee-PC, a NAC agent window should appear with information indicating temporary network access.

### Step 4

In the NAC agent window click the **Show Details** button to examine the reason for the noncompliant status. You will see that the Any_AV_Installation_Win requirement is not met.

### Step 5

Verify the authentication attempt on the ISE. The posture status should be pending.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 6*

Verify the authentication and authorization status on the switch:

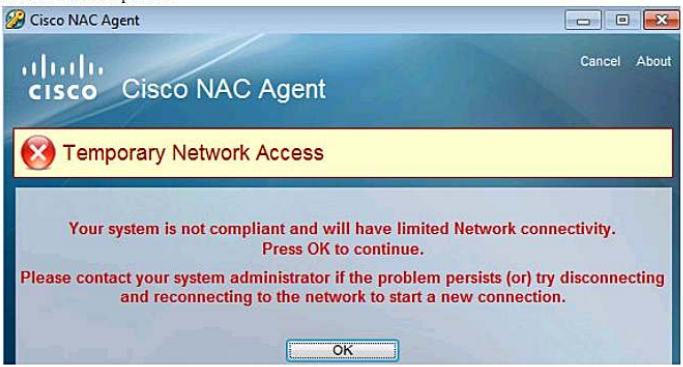
```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Unknown_Noncompliant_dACL-52bd5866
                  SGT:  0003-0
      Session timeout:  N/A
        Idle timeout:  N/A
    Common Session ID:  0A0A0102000001A1640F1A7E
      Acct Session ID:  0x00000202
               Handle:  0x690001A2
Runnable methods list:
       Method   State
       dot1x    Authc Success
```

### *Step 7*

After the remediation timer expires (4 minutes), view the authentications in the ISE GUI. You should see that the endpoint status is noncompliant.

***Step 8***

A message should be displayed in NAC Agent window on the Employee-PC indicating temporary network access due to non-compliance.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

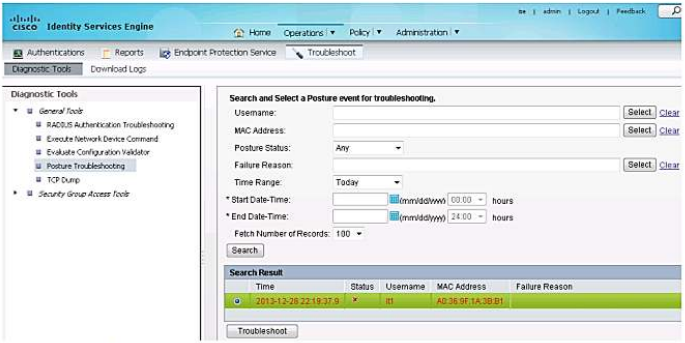
***Step 9***

Use the Cisco ISE posture troubleshooting tool:

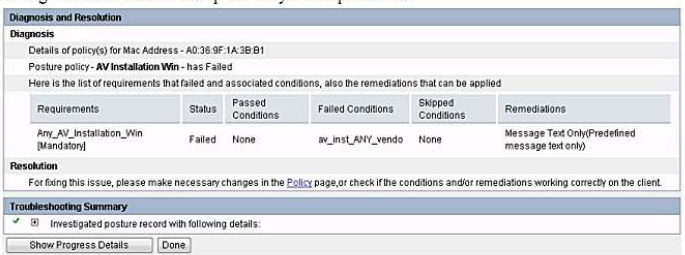
A) Go to **Operations > Troubleshoot > Diagnostic Tools, General Tools > Posture Troubleshooting**.

B) Normally you would fill in some filter details to narrow your posture event search here, but there are just a couple events presently. Simply click **Search**, choose the failed attempt, and click **Troubleshoot**.

| **Note** | The database operations for the troubleshooting reports can take time to produce as the lab implementation has minimal resources available to the ISE VM. |
|---|---|




C) Click **Show Result Summary**. Examine the displayed information. You may see output similar to the following. Proceed to the next step even if your output differs.



***Step 10***

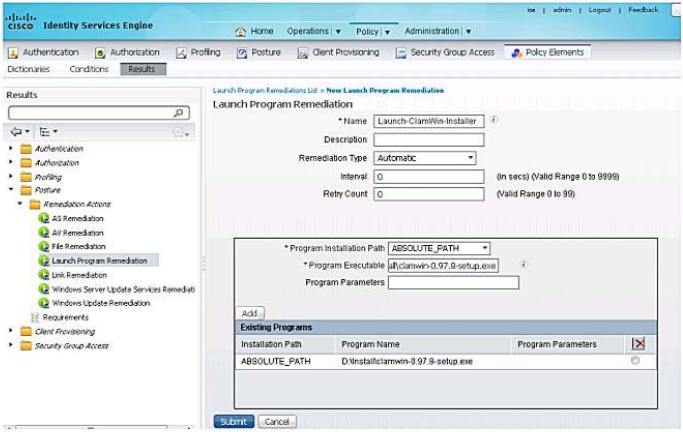
Create an automatic Launch Program Remediation that installs ClamWin antivirus. The installable file is on the D: CD-ROM drive on each of the lab VMs.

A) In the ISE GUI, go to **Policy > Policy Elements > Results, Posture > Remediation Actions > Launch Program Remediation**.

B) Click **Add**.

C) Assign the name **Launch-ClamWin-Installer**, leaving all the other main fields at their default value.

D) Populate the Existing Programs table by entering the Program Executable value: **D:\Install \clamwin-0.97.8-setup.exe** and clicking **Add**.




E) **Submit** the launch program remediation.

F) Make sure that the the antivirus installer (**D:\install\clamwin-0.97.8-setup.exe**) is available on the Employee-PC. If it is not available, contact the instructor.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

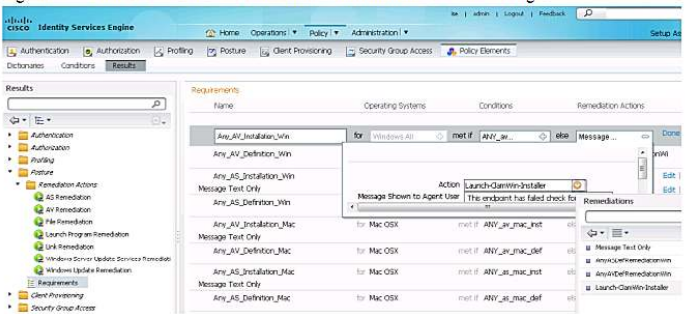
### Step 11

Change the remediation action in the requirement **Any_AV_Installation_Win** to install the ClamWin antivirus:

A) Go to **Policy > Policy Elements > Results, Posture > Requirements**.

B) **Edit** the **Any_AV_Installation_Win** requirement.

C) Change the remediation action to **Launch-ClamWin-Installer**. **Save** the changes.




### Step 12

Using the switch CLI, toggle the GigabitEthernet0/1 interface. After about 20 seconds, when the ISE applies the authorization to the port, the NAC agent on the Employee-PC should automatically launch the ClamWin installer.

### *Step 13*

Follow the installation wizard using default options: accept license agreement, install for anyone who uses the computer, use the default installation path, enable the integration options with Microsoft Outlook Express and Internet Explorer, click **Next**, select **Download Virus Database Files**, click **Install**, and then **Finish**. The installation and the download of the definition files will take up to 5 minutes. The NAC agent window will report compliance even before the definition file is updated.

**Note** If you want to roll back the ClamWin installation at any time, you can go to **Control Panel > Programs and Features**, uninstall ClamWin, shut down, and re-open the switch port to re-install ClamWin antivirus.

## Activity Verification

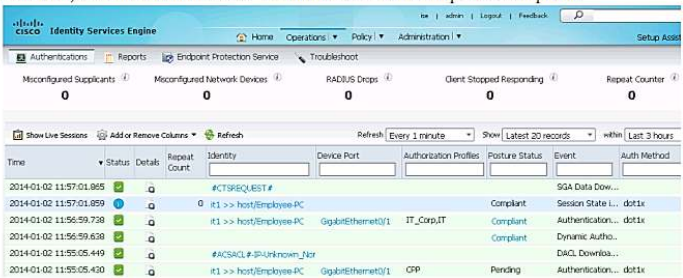
### *Step 1*

Close the NAC agent window. From the system tray, right-click the NAC agent icon and select **Properties**. The NAC agent should report finding CLAMWin AV software and Windows Defender AS software.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 2

In the ISE GUI, view the authentications. You should see that the endpoint is compliant.




### Step 3

On the switch, check the authorization status. You should see that the employee full access dACL has been applied.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
           Interface:  GigabitEthernet0/1
         MAC Address:  a036.9f1a.3bb1
          IP Address:  10.10.10.10
            User-Name:  it1
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Secured
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
        Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
                 SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  0A0A0102000001BE6B4101F3
     Acct Session ID:  0x00000225
              Handle:  0x800001BF
Runnable methods list:
      Method   State
      dot1x    Authc Success
HQ-Sw# show ip access-lists interface gigabitEthernet 0/1
     deny icmp host 10.10.10.10 host 10.10.2.20
     permit ip host 10.10.10.10 any (14 matches)
```

# Task 5: Deploy Automatic Antispyware Definition Remediation (Optional)

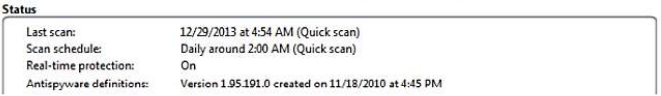
Currently, you have ISE configured to verify AV installation on Windows clients. With respect to AV and AS, ISE can verify installation, or it can go a step further and verify that the AV or AS definition files are up to date. In this optional task, you will deploy automatic remediation of antispyware (Windows Defender) definition files. You will first verify the definition file dates of the antispyware software (Windows Defender) on the Employee-PC. You will then enable the default remediation of antispyware definition files and verify the resulting behavior.

### Activity Procedure

Complete the following steps:

#### *Step 1*

On the Employee-PC, click **Start**, enter **defender** into the **Search** files field, and select **Windows Defender**. Examine the antispyware definitions. Note that they are are old.




#### *Step 2*

In the ISE GUI, examine the policy elements associated with remediation of antispyware definition files on Windows clients. These policy elements are available by default to use in posture policies:

A) Go to **Policy > Policy Elements > Results > Posture > Requirements** and examine the **Any_AS_Definition_Win** requirement. You should see that its Remediation Action is set to **AnyASDefRemediationWin**.

B) Go to **Policy > Policy Elements > Results > Posture > Remediation Actions > AS Remediation** and examine the **AnyASDefRemediationWin** remediation. You should see that it is automatic for any AS vendor type.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 3*

Navigate to **Policy > Posture**. You should see the rule that you previously created for AV installation on Windows clients. Use the down arrow icon at the end of that rule and choose to Insert new policy. Define the fields of the new policy as follows:

A) Name: **AS Definition Win**

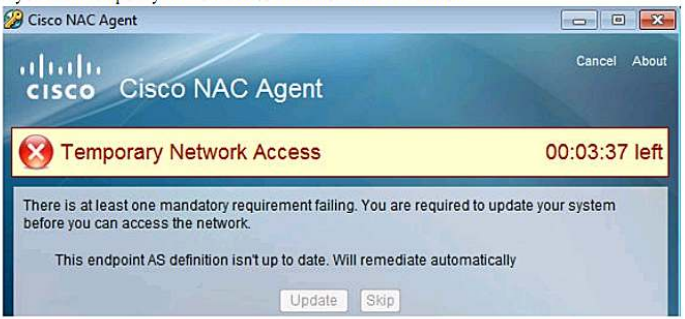
B) OS: **Windows All**

C) Requirement: **Any_AS_Definition_Win**

D) **Save** the changes.

### *Step 4*

On the switch, toggle the GigabitEthernet0/1 interface. On the Employee-PC, the NAC agent window will inform you about temporary network access and automatic remediation.



***Step 5***

After about 3 minutes the NAC agent will declare the endpoint as compliant:

**Activity Verification**

***Step 1***

On the Employee-PC, click **Start**, enter **defender** in the **Search** field, and select **Windows Defender**. Verify that the Windows Defender definitions have been updated.

| | |
|---|---|
| **Note** | If you need to roll back the installation of the Windows Defender update, choose **Start > All Programs > Accessories**, right-click the **Command Prompt** and choose **Run as Administrator** to start an elevated command prompt. In the command prompt, run the **"C:\Program Files\Windows Defender \MpCmdRun.exe" -RemoveDefinitions** command. |

***Step 2***

Check the authentication results in the Cisco ISE GUI. You should see that the endpoint is compliant.

# Task 6: Provision Web Agent on Guest-PC (Optional)

In this optional task, you will use client provisioning to deploy the NAC web agent when employees authenticate via WebAuth. The Guest-PC will be used for demonstration. In this task you will configure the required client provisioning policy and authorization policy rules and you will verify the results.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Configure the ISE to provision the web agent on Windows endpoints that connect via WebAuth:

A) Navigate to **Policy > Client Provisioning**.

B) Add a client provisioning policy rule for WebAuth access with these attributes:

**Name: Win7 WebAuth**

**Operating System: Windows 7 (All)**

**Other condition [Create New Condition (Advanced Option)]: Network Access:Use Case Equals Guest Flow**

**Result:** specify **Web Agent** in the Agent field.

C) **Save** the client provisioning policy.

#### *Step 2*

Configure the authorization policy for the compliant endpoint state when employees authenticate via WebAuth. Do this by modifying the current authorization policy for employees authenticated with WebAuth:

A) Navigate to **Policy > Authorization**.

B) **Edit** the authorization rule named **Employee via WebAuth.**

C) Rename it to **Employee WebAuth Compliant.**

D) Expand the Other conditions field and add a third expression: **Session:PostureStatus Equals Compliant.**

E) The permissions setting is good the way it is. Do not change it.


https://t.me/learningnets

### *Step 3*

Configure the authorization policy for the unknown endpoint state when employees authenticate via WebAuth. Start with a copy of the compliant policy:

A) Duplicate the Employee WebAuth Compliant rule using the **Duplicate Below** option. Change the name, the compliance check and the authorization profile:

Name: **Employee WebAuth Unknown**

Third [advanced option] condition**: Session:PostureStatus Equals Unknown**

Authorization profile (result): **Standard > CPP**

### *Step 4*

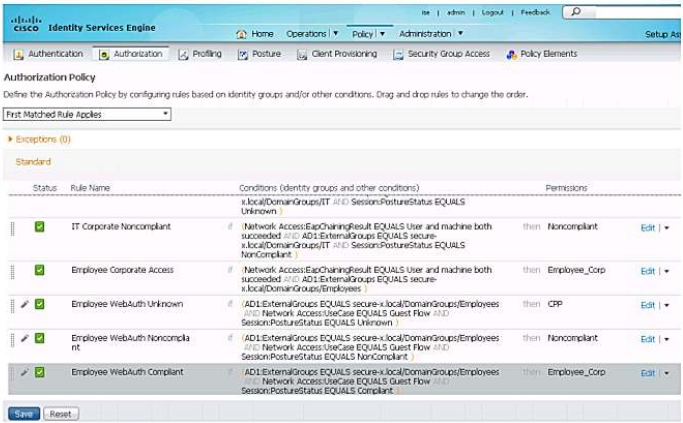
Configure the authorization policy for the noncompliant endpoint state when employees authenticate via WebAuth. Again, take advantage of rule duplication and editing:

A) Duplicate the Employee WebAuth Unknown rule using the **Duplicate Below** option. Change the name, the compliance check and the authorization profile:

Name: **Employee WebAuth Noncompliant**

Third [advanced option] condition: **Session:PostureStatus Equals Noncompliant**

Authorization profile (result): **Noncompliant**




B) **Save** the three policy changes.

### Activity Verification

You have completed this task when the web agent is provisioned on the Guest-PC and employees can gain normal network access via WebAuth on the Guest-PC.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 1

From the Guest-PC, authenticate to ISE using WebAuth:

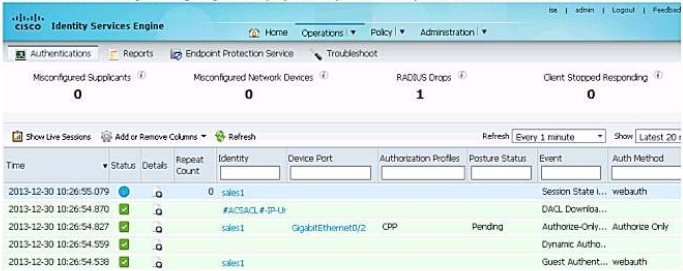
From the **Guest-PC** browse to HQ-Srv (**http://hq-srv**). You will be redirected to WebAuth.

Log in as **sales1** with password **cisco**. Accept the AUP.

Reconnect to the HQ-Srv. You should be redirected to the client provisioning portal. Do not install the agent yet.

### Step 2

In the Cisco ISE GUI, go to **Operations > Authentications** and verify the authentication attempt. The authentication of the user **sales1** should be successful. The applied authorization profile should be CPP. The posture status should be pending. Optionally, you may also verify the authentication status on the switch.

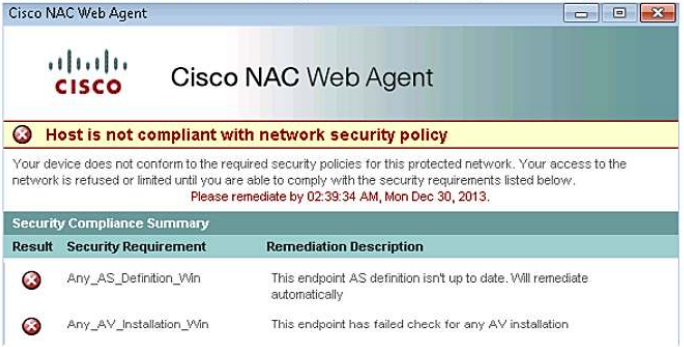




https://t.me/learningnets

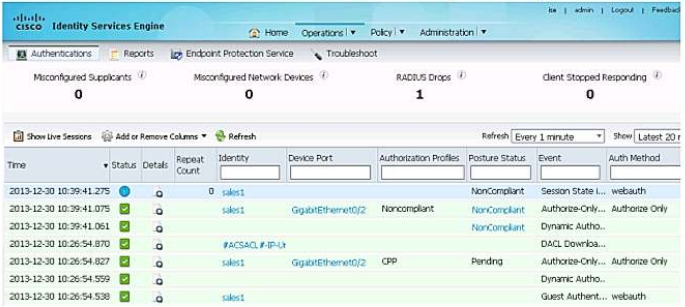
### Step 3

Return to the Guest-PC. Click the **Click to install agent** button. Accept any pop-ups and certificate warnings, and follow the installation wizard. Currently the Guest-PC does not have an AV product installed and its AS definitions are out of date. The web agent will classify the endpoint as noncompliant.




### Step 4

Note the Time Remaining countdown timer displayed in the NAC Web Agent window. This is a window of time for the user to remediate their system. To see what happens when remediation fails, wait for the timer to expire and then access the Cisco ISE GUI. Navigate to **Operations > Authentications** and examine the results. You should see that the Authorization Profile named Noncompliant is assigned.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 5*

On the Guest-PC, update the Windows Defender definition file. Manual action is required because the Web agent cannot automate this remediation.

A) Click **Start**, enter **defender** into the Search files field, and select **Windows Defender**.

B) Click **Check for Updates Now**.

C) Wait for the update to complete.

### *Step 6*

On the Guest-PC, install ClamWin AV. The Web agent cannot automate this remediation.

A) Use Windows Explorer to browse the **D:\install** directory and launch the **clamwin-0.97.8-setup.exe** installer.

B) Follow the installation wizard using default options: Accept license agreement, install for anyone who uses the computer, use the default installation path, enable the integration options with Microsoft Outlook Express and Internet Explorer, click **Next**, select **Download Virus Database Files**, click **Install**...

C) Wait for the install to complete and then click **Finish**.

### *Step 7*

On the switch, toggle the interface **GigabitEthernet0/2**. Wait until the authorization profile is applied to the port. Use the **show authentication sessions** command to verify that WebAuth redirect dACL is in place and the redirection URL specifies action=cwa.

### *Step 8*

On the Guest-PC, first verify that any NAC Web Agent windows from previous steps are closed. Then, use IE to reconnect via HTTP to HQ-SRV. You should be redirected to WebAuth. Sign in as **sales1** with password **cisco** and accept the AUP.


https://t.me/learningnets

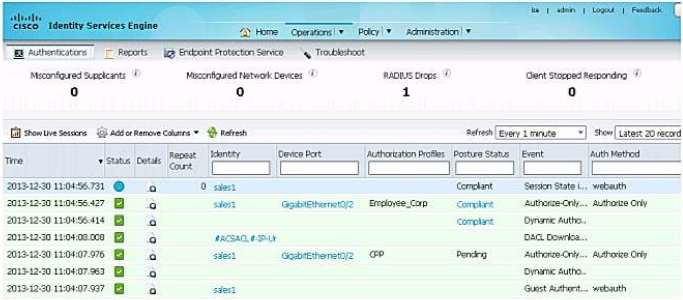
***Step 9***

Reconnect to HQ-Srv (http://hq-srv). You will be redirected to the client provisioning portal. Install the agent. At this point, the Guest-PC should be compliant. When the agent loads and checks the endpoint posture, you will be successfully logged on to the network. You will now be able to successfully browse the HQ-Srv.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 10*

View the authentication results in the ISE GUI and on the switch. You should see that the client endpoint is compliant and the appropriate authorization profile has been applied to the session.




```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  sales1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000001C16BF40F88
      Acct Session ID:  0x0000022B
               Handle:  0x4A0001C2
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 5-2: Implement Profiler Service

## Activity Objective

In this activity, you will examine the default profiling capabilities of the Cisco Identity Services Engine and fine-tune the system to increase the profiling granularity of the Linksys print servers. In the first task you will verify the results of probeless profiling. The NAC agents installed on the Employee-PC and Guest-PC report the endpoint OS information to the ISE. In the second task you will disable the probeless profiling and examine the profiling results with three most common probes enabled on the ISE: DHCP, RADIUS, and HTTP. In the third task you will configure the profiler service to granularly classify the print server that is attached to the access switch. You will also configure an appropriate authorization policy rule to enable print server connectivity.

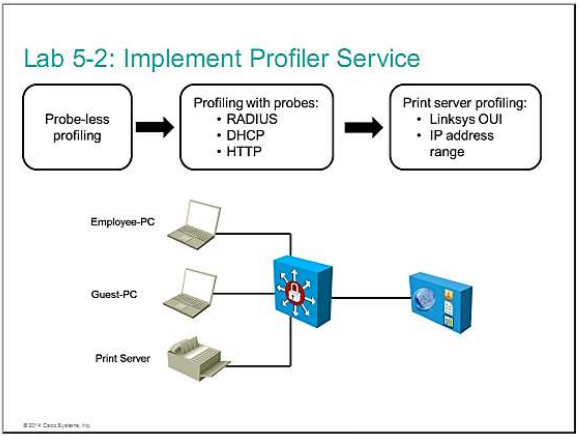
You will be able to meet these objectives:

- Test probeless profiling.
- Test the operation of the RADIUS, DHCP, and HTTP probes.
- Configure profiling conditions and policy rules to enable granular print server profiling.

https://t.me/learningnets

## Visual Objective

The figure illustrates what you will accomplish in this activity.




## Task 1: Observe Profiling without Probes

The profiler service analyzes known data about endpoints along with profile policies to classify the endpoints. The majority of this data is obtained from profiler probes that are enabled on ISE nodes. But there are other sources of data and the profiler service will make use of whatever data is available. In this task, you will observe the profiling results while all probes are disabled. You will see that the NAC agent is a source of data and that sometimes manual configuration can be the source of other data.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Verify that there are currently profiling results, despite the fact that probes have yet to be enabled.

A) First, verify that all of the probes are disabled by default. In the ISE GUI, go to **Administration > System > Deployment**. Select the node named **ise** and choose the **Profiling Configuration** tab. Note that none of the probes are checked.

B) Now, verify that some endpoints have already been profiled. Naviagate to **Administration > Identity Management > Identities, Endpoints**. You will find three endpoints, one classified as a Linksys-Device, and two as Windows7-Workstation. Why have these devices been profiled despite the disabled probes?

| | |
|---|---|
| **Note** | The Windows7-Workstations have been profiled using data collected during their connection to the client provisioning portal associated with the NAC agent installs. |

| | |
|---|---|
| **Note** | The print server was manually defined as an endpoint by MAC address in an earlier lab. This was done to enable MAB. The MAC address is enough information for the profiling as Linksys-Device. You will examine the Linksys-Device profiling policy later in this lab. |

#### *Step 2*

Observe the profiling of the Employee-PC:

A) Delete all endpoints discovered by the ISE (**Administration > Identity Management > Identities, Endpoints**).

B) On the Employee-PC, uninstall the NAC agent (**Start > Control Panel > Programs and Features**, choose the **Cisco NAC agent** and click **Uninstall**). Restart the Employee-PC (**Start > Shutdown > Restart**.)

C) Log on as **it1** with password **cisco**. At this point the NAC agent is not yet installed. In ISE, under **Administration > Identity Management > Identities, Endpoints**, verify that the endpoints list remains empty.

D) Install the NAC agent: On the Employee-PC, open a browser and connect to **http://hq-srv**. You will be redirected to the client provisioning portal. Install the NAC agent, following the wizard using the default settings.

E) After the install, observe the NAC agent. It will open automatically, but may open below the browser window. It should start by reporting temporary network access, but after the posture assessment is complete it should report that Full Network Access is granted.

F) On the ISE, navigate to **Administration > Identity Management > Identities, Endpoints** and verify that the Employee-PC has now been discovered and profiled. The MAC address is the unique identifier for this endpoint, and it is profiled as a Windows7-Workstation.


https://t.me/learningnets

***Step 3***

Examine the logic used to profile the Employee-PC:

A) From the Endpoint Identities table, click the **Windows7-Workstation** link to examine all of the attributes associated with this endpoint. There is a fair amount of detail. Amongst the attributes, notice:

EndPointPolicy: Windows7-Workstation

EndPointSource: CP

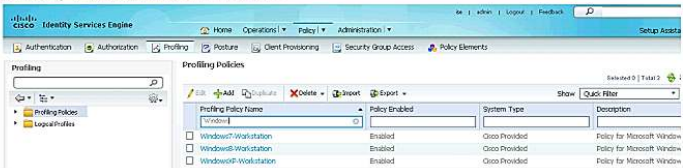
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

---

**Note** Of course, the assigned end point policy is Windows7-Workstation. Note the data source that is identified is CP. Data was obtained from the client provisioning process. Also note the User-Agent field. This is the value of the User-Agent field presented by Internet Explorer to ISE's client provisioning portal. You will see this is what the profiling logic was based on.

---

B) Examine the Windows7-Workstation Profiler Policy: Navigate to **Policy > Profiling**. To limit the number of profiling policies listed in the table, select **Quick Filter** in the Show field, and then type **Windows** in the Profiling Policy Name field of the filter. You should see three policies - one each for WIndows 7, Windows 8 and Windows XP.



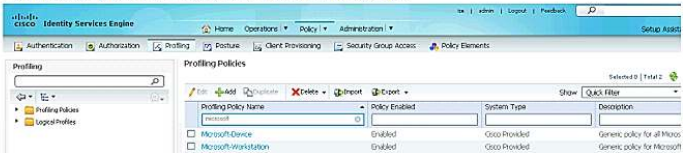

C) Click the **Windows7-Workstation** link. Note two things: 1) The Parent Policy is Microsoft-Workstation. 1) The profiler condition specified in the rules is Windows7-WorkstationRule1Check1.

---

**Note** Windows7-Workstation is a child to the Microsoft-Workstation profiling policy. The parent policy must match for the rules of a child policy to be evaluated. To understand the logic that was used you must explore the conditions associated with the Microsoft-Workstation profiling policy as well as the Windows7-WorkstationRule1Check1 condition referenced here.

---

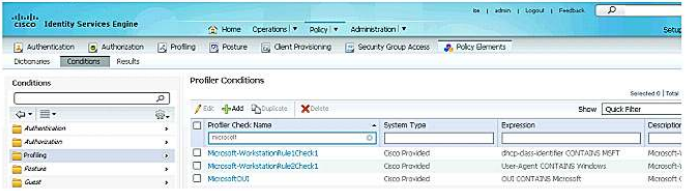
D) Examine the Microsoft-Workstation Profiler Policy: Navigate to **Policy > Profiling**. To limit the number of profiling policies listed in the table, select **Quick Filter** in the Show field, and then type **Microsoft** in the Profiling Policy Name field of the filter. With this filter, you should see two policies - one for Microsoft-Device and one for Microsoft-Workstation.




E) Click the **Microsoft-Workstation** link. Note that there are two profiler conditions specified: Microsoft-WorkstationRule1Check1 and Microsoft-WorkstationRule2Check1.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

F) Examine the conditions referenced by the Microsoft-Workstation profiler rule: Navigate to **Policy > Policy Elements > Conditions** and select the **Profiler** folder. Use the Quick Filter to look for conditions that start with the string **Microsoft**. From the table you can see the attribute operator value specifications of the condition's expression. Rule1 looks for MSFT in the dhcp-class-identifier. Rule 2 looks for Windows in the User-Agent field. Rule 2 is what allowed the parent policy Microsoft-Workstation to match. In the next task you will see an example where Rule 1 leads to the Microsoft-Workstation profile.




G) Examine the conditions referenced by the Windows7-Workstation profiler rule: Change the string in the Quick Filter from Microsoft to **Windows**. There should be a condition for Windows 7, Windows 8 and Windows XP. From the table you can see the attribute operator value specifications of the condition's expression. The Window 7 rule looks for Windows NT 6.1 in the User-Agent field.

# Task 2: Deploy DHCP, RADIUS, and HTTP Probes

In this task, you will examine the use of three commonly deployed probes and the resulting profiling of the Guest-PC.

**Activity Procedure**

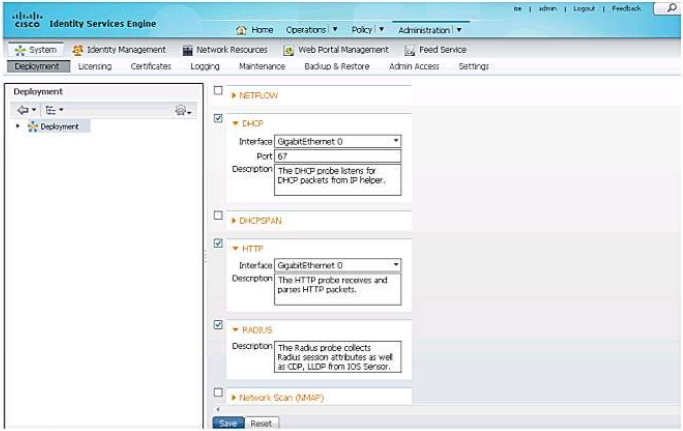
Complete the following steps:

***Step 1***

Enable the DHCP, RADIUS, and HTTP probes:

A) In the ISE GUI, navigate to **Administration > System > Deployment**.

B) Click the **ise** node and choose the **Profiling Configuration** tab. Enable three probes: **DHCP**, **HTTP**, and **RADIUS** using their default values.




C) **Save** the changes.

***Step 2***

On the switch, forward the DHCP requests from PC VLANs 9, 10, and 11 to the ISE (10.10.2.2). The helper-address configuration is needed for the DHCP probe to profile the endpoints.

```
interface Vlan9
 ip helper-address 10.10.2.20
!
interface Vlan10
 ip helper-address 10.10.2.20
!
interface Vlan11
 ip helper-address 10.10.2.20
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

Examine the profiling of the Guest-PC:

A) Restart the Guest-PC. This will cause a port transition on the switch and a new authentication session with ISE. The Guest-PC is configured to autologin with the local student ID. There is no supplicant, so the WEBAUTH authorization profile is applied.

B) After the reboot, verify that the Guest-PC has been profiled as Microsoft-Workstation: In the ISE GUI, navigate to **Administration > Identity Management > Identities, Endpoints**. Verify that after the DHCP exchange the profile is Microsoft-Workstation.

C) Click the **Microsoft-Workstation** link to examine the attributes that are available to the profiler. There are many. Amongst the attributes you should see that the Guest-PC's MAC address and IP address. The name and IP address of the switch and the port ID on the switch are also known. Of special importance, scroll to the bottom of the attribute list (the list is in alphabetical order, with lower case coming after upper case). Look for the dhcp-class-identifier. It should be set to MSFT 5.0. You may recall from the previous task, the Microsoft-WorkstationRule1Check1 profiler condition looks for MSFT in the dhcp-class-identifier.

D) On the Guest-PC, go through the WebAuth and Posture processes: Open a browser and attempt an HTTP connection to HQ-Srv, you will be redirected to the guest portal. At the guest portal, login as **sales1** with the password **cisco** and accept the AUP. You will be redirected to the guest portal. Attempt to browse the HQ-Srv again, this time you are redirected to the client provisioning portal. Click the **Click to install agent** button. Wait for the posture process to complete. The web agent should report that you are successfully logged on to the network.

E) On the ISE, verify that the Guest-PC has been identified using the Windows7-Workstation profile: In the ISE GUI, return to **Administration > Identity Management > Identities, Endpoints**. Verify that the profile is now Windows7-Workstation.


https://t.me/learningnets

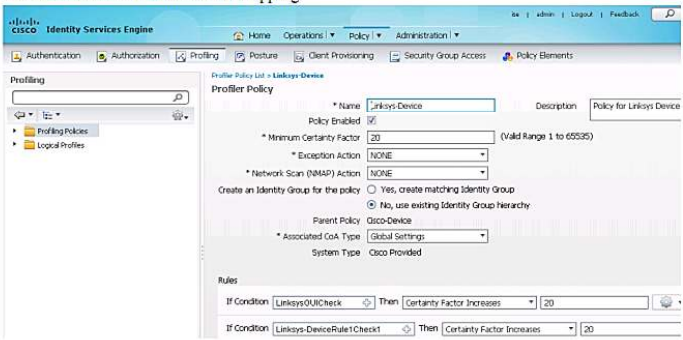
***Step 4***

Examine the profiling of the print server:

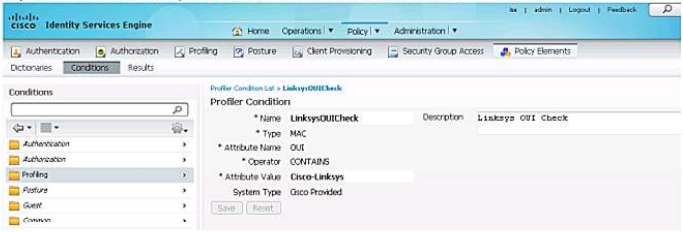
A) On the switch, toggle the interface **GigabitEthernet0/19** with a **shutdown** and a **no shutdown**. This is the port where the print server is attached.

B) In ISE, under **Administration > Identity Management > Identities, Endpoints**, verify that the print server is profiled using the Linksys-Device profile. Optionally follow the Linksys-Device link to examine all of the attributes that are currently defined for the endpoint.

C) Examine the policy that profiled the print server as a Linksys-Device. Go to **Policy > Profiling**. Use the **Quick Filter** option to display only policies that start with the string **Linksys**. Examine the Linksys-Device policy. You should see that matching the Linksys Organizational Unique Identifier (OUI) condition is sufficient to match the Linksys-Device profile because it raises certainty factor (20) to the minimum required value (20). ISE obtained the MAC address using the RADIUS probe and it has a table of OUI values for vendor mapping.

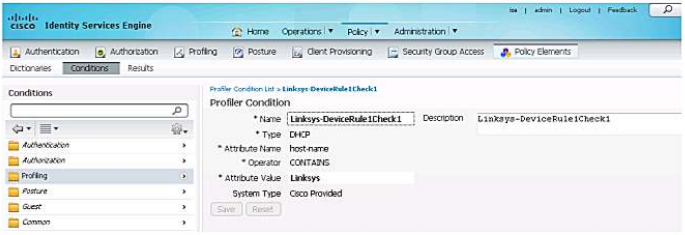



D) Examine the LinksysOUI check definition: Go to **Policy > Policy Elements > Conditions > Profiling**. Click the filter button to select the Quick Filter option. Search for conditions that start with the string Linksys. Examine the **LinksysOUICheck** condition. It matches the vendor OUI.




E) Examine the **Linksys-Device1Rule1Check1** condition. It matches the host-name attribute in DHCP request. This condition is not useful in this environment because the print server has a static IP address.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.




# Task 3: Configure Print Server Profiling

Having tested the default discovery capabilities of the ISE probes, you will fine-tune the profiler service to classify the Linksys print servers in a more granular fashion. So far the print server has been discovered as Linksys device. You will configure a child profiling policy to discover it as a Linksys print server. The criteria for classifying a device as a print server will be based on the IP address. In this scenario, the print servers have static IP addresses between 10.10.10.91 to 10.10.10.99.

### Activity Procedure

Complete the following steps:

#### *Step 1*

A) From the switch, ping the print server (10.10.10.99) to generate an IP device tracking entry. In a scenario with static device addressing, this task could be performed by a tool or an administrator.

B) When the ping succeeds, check the IP device tracking entry. The MAC address in your pod will differ from this output.

```
HQ-Sw# show ip device tracking interface GigabitEthernet 0/19
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
------------------------------------------------------------------------
  IP Address      MAC Address   Vlan  Interface                STATE
------------------------------------------------------------------------
10.10.10.99      0014.bf66.fc9e  10   GigabitEthernet0/19      ACTIVE
<output omitted>
```


https://t.me/learningnets

***Step 2***

Create a profiling condition (PrintServer-above-min-IP), which checks if the device IP address is higher than the lower range boundary:

A) In the ISE GUI, go to **Policy > Policy Elements > Conditions, Profiling**.

B) Click **Add** and create a condition with these parameters:

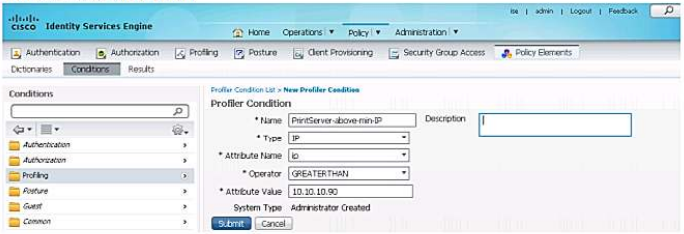
Name: **PrintServer-above-min-IP**

Type: **IP**

Attribute name: **ip**

Operator: **GREATERTHAN**

Attribute value: **10.10.10.90**




C) Click **Submit**.

| **Note** | In the next step you will check if the device IP address starts with "10.10.10.". The endpoint IP addresses are evaluated as strings, not as numbers. You can match the range 10.10.10.91-10.10.10.99 by checking if the endpoint address is higher than "10.10.10.90" and starts with "10.10.10." |
|---|---|


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

Create a profiling condition (PrintServer-network-prefix), which checks if the device IP address string starts with "10.10.10."

A) Click **Add** and create the second condition with these parameters:

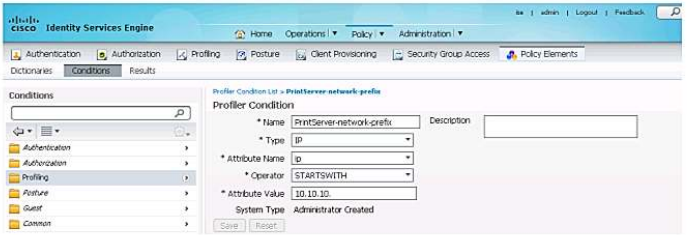
Name: **PrintServer-network-prefix**

Type: **IP**

Attribute name: **ip**

Operator: **STARTSWITH**

Attribute value: **10.10.10.**




B) Click **Submit**.

***Step 4***

Create a profiling policy, which uses the two new conditions to check if a Linksys device has an IP address in the print server range:

A) In the ISE GUI, go to **Policy > Profiling**.

B) Select the **Linksys-Device** policy and **Duplicate** it.

C) Modify the cloned policy:

Name: **Linksys-PrintServer**

Minimum certainty factor: **60**. This value will be a sum of the certainty factor 40 when Linksys OUI is discovered, 10 when the IP address is above the lower IP threshold, and 10 when it starts with 10.10.10.

Select the **Yes, create matching identity group** radio button

Parent policy: **Linksys-Device**

Raise the certainty factor of the first condition (LinksysOUICheck) to **40**.

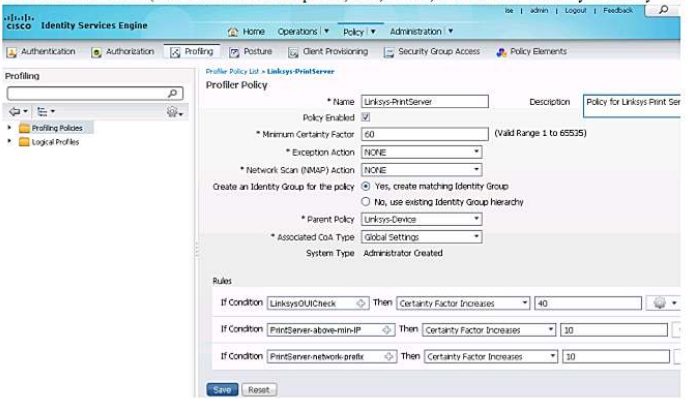
Change the second condition to PrintServer-above-min-IP and, if met, increase the certainty factor by 10.

---

**Note** When selecting a condition, a filter field is available to quickly find a particular condition. Simply type **"Print"** into the filter field to find the PrintServer-above-min-IP condition.

---

Add a third condition (PrintServer-network-prefix) and, if met, increase the certainty factor by 10.

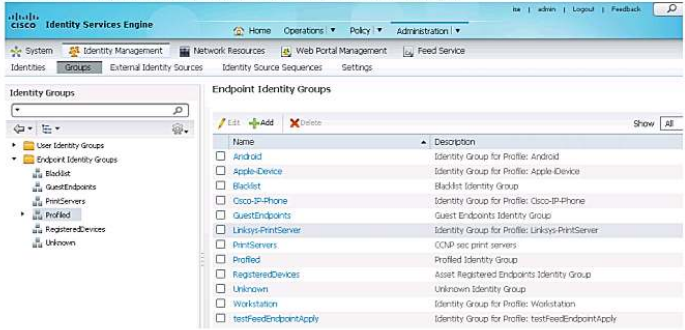



D) Click **Submit**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 5

Go to **Administration > Identity Management > Groups, Endpoint Identity Groups** and verify that the Linksys-PrintServer group has been created under the Profiled groups.

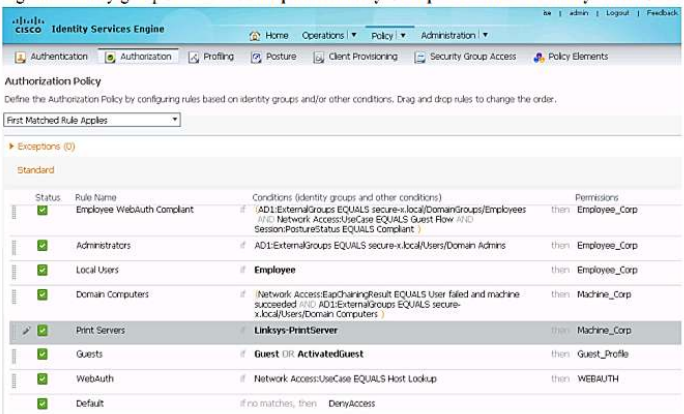



### Step 6

The current authorization policy uses the manually configured identity group named PrintServers. Change the authorization policy to use the new dynamic print server profiling:

A) Go to **Policy > Authorization** and find the **Print Servers** rule. It matches the static endpoint identity group PrintServers, which you defined by specifying the device MAC address.

B) Change the identity group selection to **Endpoint Identity Groups > Profiled > Linksys-PrintServer**.

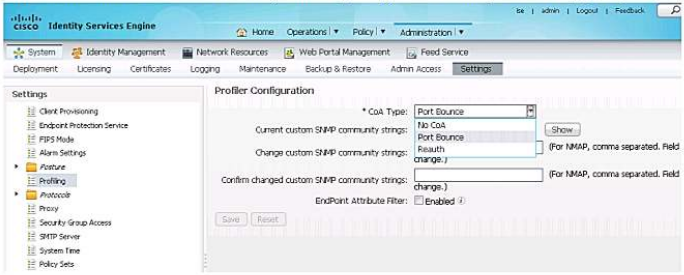



C) Leave the remaining settings unchanged and click **Save**.


https://t.me/learningnets

### *Step 7*

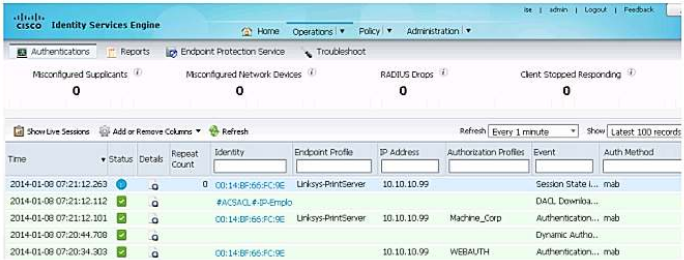
Go to **Administration > System > Settings > Profiling** and set the profiling CoA behavior to **Port bounce** and then **Save** the change. The ISE will instruct the switch to bounce the access interface when sending the CoA information after the device has been dynamically assigned to the endpoint identity group.




## Activity Verification

### *Step 1*

On the switch, toggle the print server port (**GigabitEthernet 0/19**) with a **shutdown** followed by a **no shutdown**. View the access attempt in the ISE authentications page. Make sure that the Endpoint Profile column is displayed. You should see a successful authentication, profiling, and authorization of the endpoint.

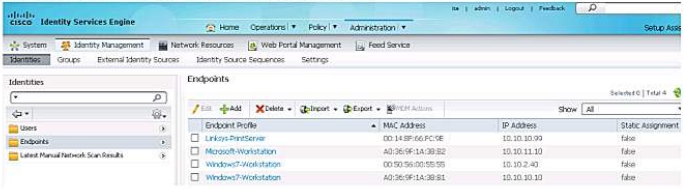




https://t.me/learningnets
© 2014 Cisco Systems, Inc.

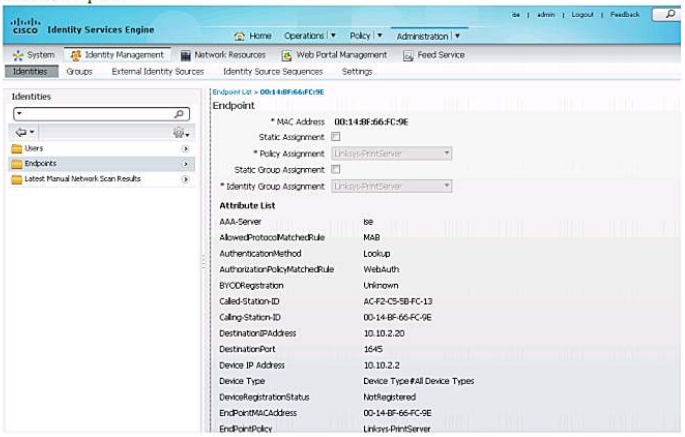
### Step 2

Go to **Administration > Identity Management > Identities > Endpoints** and verify that the print server has been discovered using the Linksys-PrintServer profile.




### Step 3

Click the **endpoint** to examine its details. You should see that the Linksys-PrintServer policy has been used to profile this endpoint.




### Step 4

From the Admin-PC, ping the print server IP address (10.10.10.99) to verify that the session authorization is effective. If not, the Basic-ACL applied to the interface would block the ICMP packets.

### Step 5

When you finish the profiling verification, start the next exercise (Troubleshooting Prep) to load the ISE configuration for the troubleshooting lab.


https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 6-1: (Optional) Troubleshooting Prep

## Activity Objective

The sole purpose of this activity is to load configurations on the switch and on the Cisco Identity Services Engine to prepare for the following lab. In the next lab, which is also optional, you will troubleshoot the network access introduced into switch configuration and into ISE's configuration.

https://t.me/learningnets

# Task 1: Restore Broken Backup Configurations on Switch and ISE

### Restore Procedure

Complete the following steps:

#### *Step 1*

On the HQ-Srv, copy the ISE and switch backup files to the FTP root directory:

A) Connect to the **HQ-Srv**.

B) Use Windows Explorer to browse the contents of the CD-ROM under **D:/ISE**.

C) Use ctrl-clicks to select the two files **ise-broken.tar.gpg** and **switch-broken.txt**. With both files selected, right-click and select **Copy**.

D) In Windows Explorer, navigate to **C:\xampp\FileZillaFTP\ftproot**. Right-click and select **Paste**.

#### *Step 2*

Load the configuration on the switch:

A) Download the switch backup file to the switch:

```
HQ-Sw# copy ftp startup-config
Address or name of remote host []? 10.10.3.20
Source filename []? switch-broken.txt
Destination filename [startup-config]? <Enter>
Accessing ftp://10.10.3.20/switch-broken.txt...
Loading switch-broken.txt !
[OK - 6793/4096 bytes]
```

B) Reload the switch without saving the current configuration:

```
HQ-Sw# reload
Proceed with reload? [confirm] <Enter>
```

C) Wait for the switch to fully reboot. The won't be connectivity between the Admin-PC and the the ISE VM until the switch has booted. The process takes about 3 minutes.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 3

In the ISE GUI, define the HQ-Srv as an FTP repository: Navigate to **Administration > System > Maintenance > Repository** and click **Add**. Define the repository as follows:

A) Name: **hq**

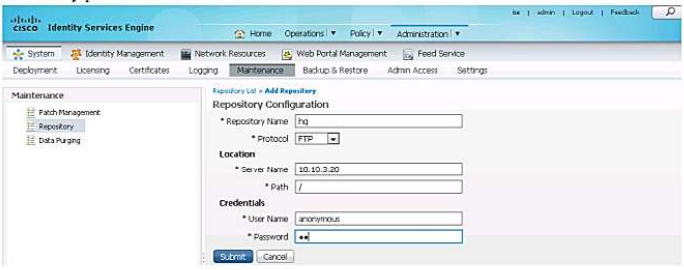
B) Protocol: **FTP**

C) Server name: **10.10.3.20**

D) Path: /

E) Username: **anonymous**

F) Password: any password




### Step 4

Restore the ISE configuration backup using the ISE CLI:

A) From the Admin-PC use PuTTY to connect to ISE via SSH. PuTTY has a device entry for the ISE. Log in as **admin** with password **Ci5coAdmin**.

B) In the CLI enter the command: **restore ise-broken.tar.gpg repository hq encryption-key plain Ci5coAdmin**

| **Note** | The configuration backup has been protected using the encryption key Ci5coAdmin. |
|---|---|

C) Initial progress indicators will give the appearnce of a rather quick restore, but then they will slow down. The entire restore operation will take approximately 60 minutes. Continue to the next steps while the restore proceeds.

### Step 5

Use the Windows Control Panel to Uninstall the NAC agent on the Employee-PC. When done, restart the Employee-PC.


https://t.me/learningnets

### *Step 6*

The Guest-PC has the non-persistant web agent. Simply restart the Guest-PC.

### *Step 7*

This completes the actions required in this preparatory lab. Verify that the ISE restore has completed before attempting the Troubleshooting lab.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 6-2: (Optional) Troubleshoot Network Access Controls

## Activity Objective

In this optional lab exercise, you will troubleshoot the network access control in an IEEE 802.1X environment with a Cisco Identity Services Engine standalone deployment. The Cisco Identity Services Engine is integrated with the Active Directory running on the HQ-Srv. The network has been preconfigured to support various EAP authentication methods and Central WebAuth. The ISE performs the posture and profiler service. You have been asked in to troubleshoot the environment. Its various parts have been set up by different engineers and some of the configuration is inconsistent.

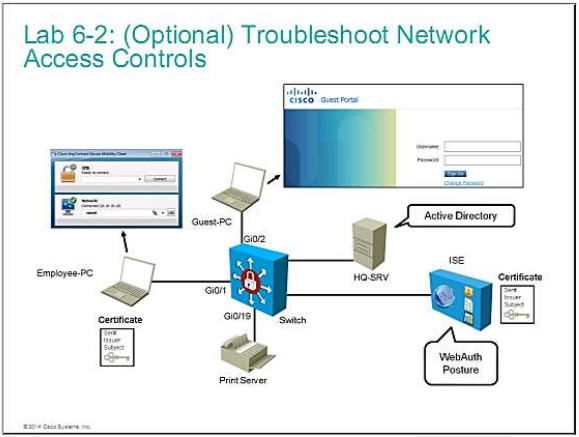
When you complete this exercise, you will be able to:

- Troubleshoot 802.1X authentication
- Troubleshoot authorization
- Troubleshoot Central WebAuth
- Troubleshoot posture

## Visual Objective

The figure illustrates what you will accomplish in this activity.

https://t.me/learningnets




# Task 1: Troubleshoot 802.1X Authentication Against Local ISE Database

In this task, you will review brief descriptions of the trouble tickets. Your goal is to try to troubleshoot the problems on your own. If you need help, the next task provides guidelines to systematically troubleshoot the given problems. Also, the last section, the Answer Key, shows the solution where applicable.

### Activity Procedure

Complete the following steps:

#### *Step 1*

**Understand the organization of this lab:**

This lab is broken up into pairs of tasks.

The odd numbered task of the pair describes a trouble ticket or set of trouble tickets.

The even numbered task of the pair provides guidance on determining the root cause or causes.

The even numbered task of the pair also specifies where to take corrective actions. For further guidance on the corrective actions, there are entries in the Answer Key, indexed by the task and step numbers.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

**Lab Task Overview:** Troubleshoot the problem reported by the local user **student,** who attempted network access from the **Employee-PC**. The password for the user **student** is **Ci5coAdmin**. The user should be able to connect to http://cisco.com.

**Background information:** The Employee-PC is connected to switch port GigabitEthernet 0/1. The switch acts as AAA client of Cisco ISE. The RADIUS shared key is radius-key. The user **student** exists in the local user database on Cisco ISE. The default authentication method is EAP-FAST.

**Troubleshooting best practice:** The primary tools that are used in this step should be **debug** and **show** commands.

Log into the Employee-PC as the local user **employee-pc\student** with password **Ci5coAdmin**. Once you are logged in, try to browse to www.cisco.com. This attempt will fail. Use the **ipconfig** windows command to verify the assigned IP address on the Employee-PC. If the 802.1x authentication is successful, you will see a DHCP-assigned IP address in the 10.10.9.x subnet.

**Tip:** When you log in as a local user to the Employee-PC, enter **employee-pc\student** as the username to differentiate it from the domain login.

# Task 2: Guide for Troubleshooting 802.1X Authentication Against Local ISE Database

This section contains guidelines on how to resolve the 802.1X issues. Use it for verification of a systematic troubleshooting approach.

### Activity Procedure

### *Step 1*

To troubleshoot 802.X authentication of user student from the Employee-PC, you may first check the ISE authentications:

A) If you examine the authentication attempts in the ISE GUI (**Operations > Authentications**), you will not see any access attempts via switchport GigabitEthernet 0/1, where the Employee-PC is attached.

Complete the following steps:


https://t.me/learningnets

***Step 2***

Troubleshoot the operation on the switch:

A) Use the **debug radius authentication** command then **shut** and **no shut** the **GigabitEthernet0/1** interface, you will not see any RADIUS communication regarding the GigabitEthernet0/1 port.

B) Use the **debug dot1x events** then **shut** and **no shut** the **GigabitEthernet0/1** interface, you should see the following messages indicating a new client being detected, but then the dot1x process stopped.

```
dot1x-ev(Gi0/1): Role determination not required
dot1x-ev:Enqueued the eapol packet to the global authenticator queue
EAPOL pak dump rx
EAPOL Version: 0x1 type: 0x1 length: 0x0000
dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 0,TYPE= 0,LEN= 0
dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr = 0180.c200.0003, pae-
ether-type = 888e.0101.0000
dot1x-ev(Gi0/1): New client detected, issuing Start Request to AuthMgr
```

C) This indicates that 802.1X is enabled globally on the switch, but some switch settings may be missing. Do not correct the switch configuration now, continue to the next step to use the ISE validator tool.

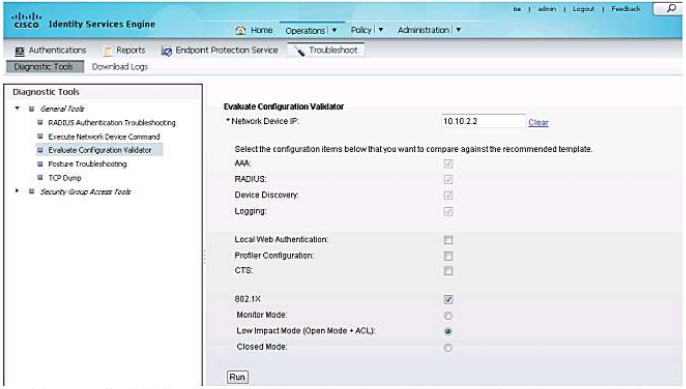

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

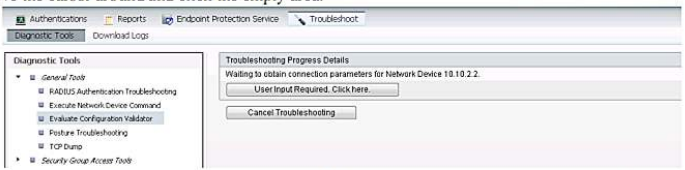
Use the Evaluate Configuration Validator on the ISE to fix the switch configuration:

A) In ISE GUI, go to **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator.**

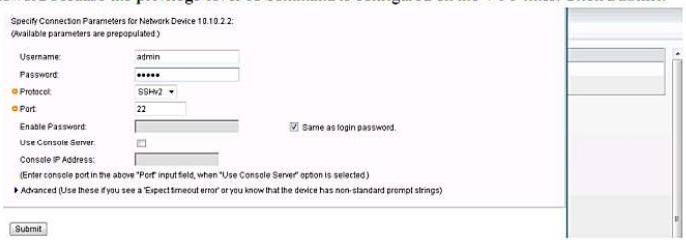
B) Enter the switch IP address (**10.10.2.2**). Uncheck **WebAuth, Profiler Configuration** and **CTS**. Select low-impact mode and click **Run**.



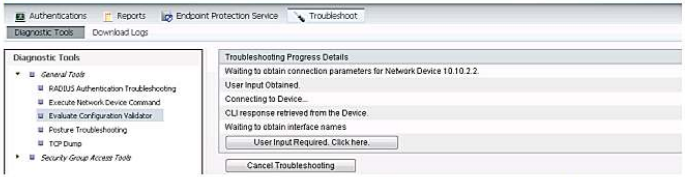

C) After a few seconds click the button **User Input Required. Click here.** If you do not see the button, move the cursor around and click the empty area.




D) Enter username **admin** with password **cisco**. Use SSHv2. You do not need to provide an enable password because the **privilege-level 15** command is configured on the VTY lines. Click **Submit**.



E) Click the button **User Input Required. Click here**. Move the cursor around if you do not see the button.

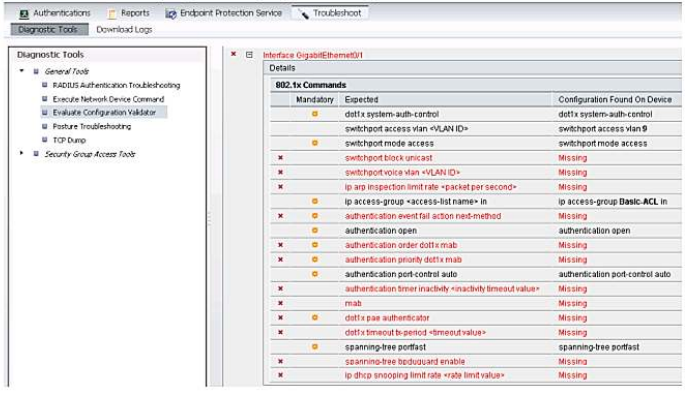



F) Select the first two Gigabit Ethernet interfaces for analysis. Scroll down and click **Submit**.

G) Click the **Show Results Summary** button, move the cursor if the button does not show. Examine the results. You will see information about many missing commands, but most of them are false alarms. Much of the verification is for recommendations or for situational requirements. An example of a false alarm is the RADIUS configuration (global) section which reports that the **radius-server host** command is missing. But this is because the configuration validator looks for the older syntax commands where the switch uses the newer syntax:

```
radius server ISE-RADIUS
 address ipv4 10.10.2.20 auth-port 1812 acct-port 1813
 key radius-key
```

H) Examine the GigabitEthernet 0/1 configuration section. The **dot1x pae authenticator** command is missing and it is definitely required for proper 802.1X operation.




**Note** You may enable **MAB** but it will not be used on GigabitEthernet 0/1.

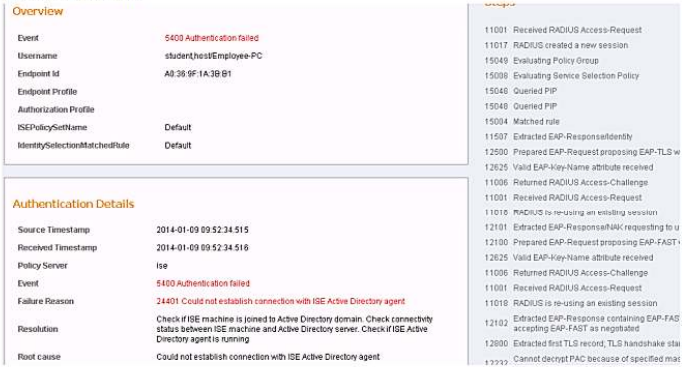

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

I) Check the configuration results on GigabitEthernet0/2. They should be the same as on GigabitEthernet 0/1.

J) **Address the configuration issues on GigabitEthernet interfaces 0/1 and 0/2**. Consult the **Answer Key** if you need more direction.

### *Step 4*

In ISE GUI, go to **Operations > Authentications**. You should see a failed authentication attempt of student on the Employee-PC. Click the **Details** button and examine the reason. The authentication failed because the connection with an AD agent could not be established. This information is a little misleading because student is a local account.

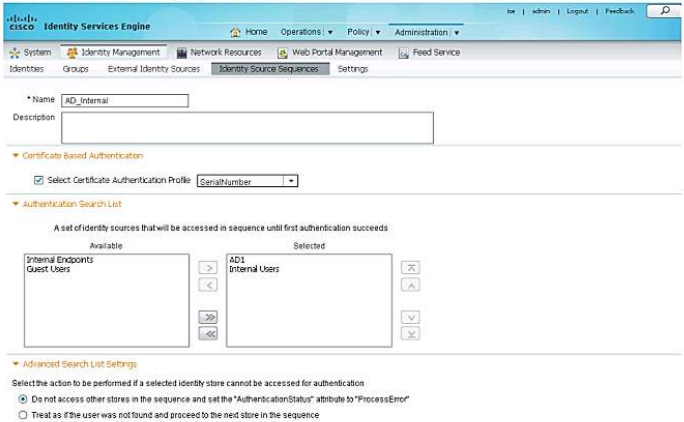



### *Step 5*

Examine the ISE authentication policy (**Policy > Authentication**). You will see that 802.1X attempts are authenticated against the identity source sequence AD_Internal.

### Step 6

Examine the identity source sequence (**Administration > Identity Management > Identity Source Sequences**). You will find that if the first store cannot be accessed, other stores will not be tried. **Fix the problem** (see the **Answer Key** if you need more direction).

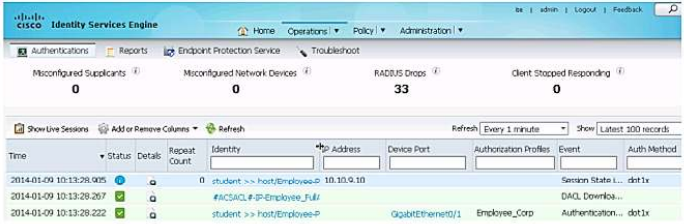



### Step 7

On the Employee-PC enter user credentials (**student/Ci5coAdmin**) in the AnyConnect supplicant pop-up window.

### Step 8

In ISE GUI, go to **Operations > Authentications**. You should see a successful authentication on port GigabitEthernet 0/1.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 9*

Verify the authentication status of the interface GigabitEthernet 0/1 on the switch.

```
HQ-Sw# show authentication sessions interface GigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.10
            User-Name:  student
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Employee_FullAccess_DACL-52777cd1
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A010200000059008A4790
      Acct Session ID:  0x00000066
               Handle:  0x2300005A
Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run
```

### *Step 10*

Verify that the Employee-PC can browse cisco.com. Restart the Employee-PC.

# Task 3: Troubleshoot 802.1X Authentication Against Active Directory

This section includes brief descriptions of the trouble tickets. Try to troubleshoot the problems on your own. The next section contains guidelines to systematically troubleshoot the given problems. The last section (Answer Key) shows the solution, where applicable.


https://t.me/learningnets

### Activity Procedure

Complete the following steps:

#### *Step 1*

Troubleshoot the problem reported by AD domain user **sales1** who attempts network access from the Employee-PC. The password for the user **sales1** is **cisco**. The user should be able to connect to http://cisco.com.

Background information: User **sales1** is an Active Directory user. The Active Directory secure-x.local is running on the HQ-Srv (10.10.3.20). The AD administrator account is **administrator** with password **Ci5coAdmin**. The ISE offloads user authentication to the Active Directory.

Follow the next task to systematically troubleshoot this problem.

#### *Step 2*

Troubleshoot the problem with Employee-PC machine authentication. When no user is logged in to Employee-PC, the Employee-PC should be authenticated and be allowed network access.

Background information: Employee-PC has been joined to the Active Directory. As a result of the join, it has obtained credentials to be authenticated against the Active Directory.

Follow the next set task to systematically troubleshoot this problem.

## Task 4: Guide For Troubleshooting 802.1X Authentication Against Active Directory

This section contains guidelines on how to resolve the issues with authentication against AD. Use it for verification of a systematic troubleshooting approach.

Complete the following steps:

#### *Step 1*

To troubleshoot 802.X authentication of the **sales1** domain user from the Employee-PC, you may first check the ISE authentications:

A) Log on to the Employee-PC and log on as **sales1** with password **cisco**.

B) Examine the authentication attempts on the ISE (**Operations > Authentications**). You should see a failed attempt.

C) Click the **Details** button and scroll down to examine the reason. You should see a problem with the authentication against the AD.

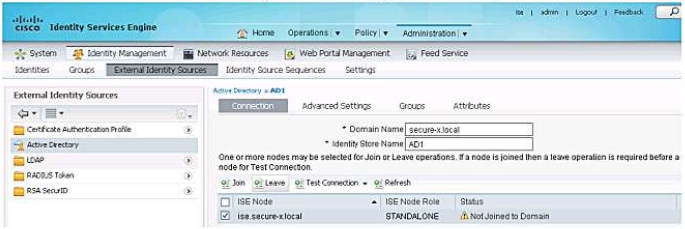

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 2*

Join and connect the ISE to the AD server:

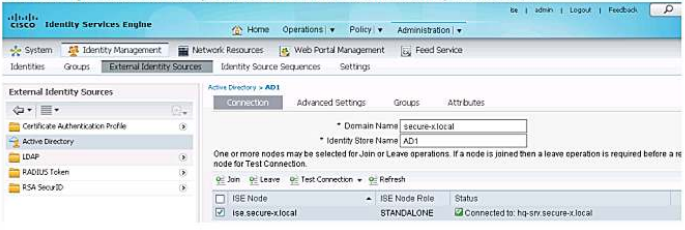
A) Go to **Administration > Identity Management > External Identity Sources > Active Directory**.

B) You should see that the ISE status is not joined to domain, select the node and click the **Join** button:




C) Enter administrator credentials: **administrator/Ci5coAdmin**

D) Confirm the operation and verify that the ISE becomes successfully connected:




| **Note** | If the ISE does not join due to large time skew, delete and re-apply the NTP server (**10.10.3.20**) in the **Administration > System > Settings > System Time** menu. |
|---|---|

### *Step 3*

Restart the Employee-PC. Wait for the logon screen to be presented on the Employee-PC and then access the ISE GUI. On the ISE you should see failed machine authentication attempts through the switch port GigabitEthernet 0/1.

### *Step 4*

Examine the details. You should see that the machine authentication against the AD has been disabled in the ISE. **Fix this issue**. If you need more direction, you can consult the **Answer Key**.

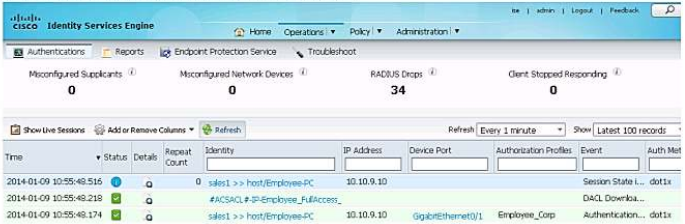
### *Step 5*

Retest machine authentication by shutting down and re-enabling the switch port GigabitEthernet 0/1. The machine authentication will now succeed.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### *Step 6*

Log in to the Employee-PC as **sales1**. Verify the successful authentication. Restart the Employee-PC. Do not log back on until instructed to do so in the next task.




# Task 5: Troubleshoot EAP-TLS Authentication

This section includes brief descriptions of the trouble tickets. Try to troubleshoot the issues on your own. The next section contains guidelines to systematically troubleshoot the problems. The last section (Answer Key) shows the solution, where applicable.

### Activity Procedure

Complete the following steps:

### *Step 1*

Log on to the Employee-PC as **secure-x\administrator** with password **Ci5coAdmin**.

### *Step 2*

Use the Certificate Manager console to verify that user certificate exists in the user certificate store:

A) Click **Start**, and enter **certmgr.msc** into the **Search programs and files** field, then press **<Enter>**.

B) Choose **Certificates - Current User > Personal** and verify the administrator certificate.

**Note** You have installed the administrator and machine certificates on the Employee-PC in a previous exercise. If you don't have them, load them again using the certmgr.msc and mmc utilities.


https://t.me/learningnets

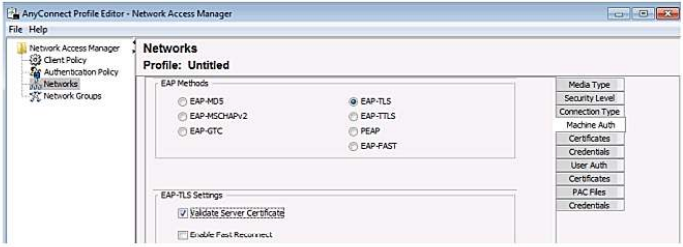
***Step 3***

Configure the AnyConnect supplicant to use EAP-TLS:

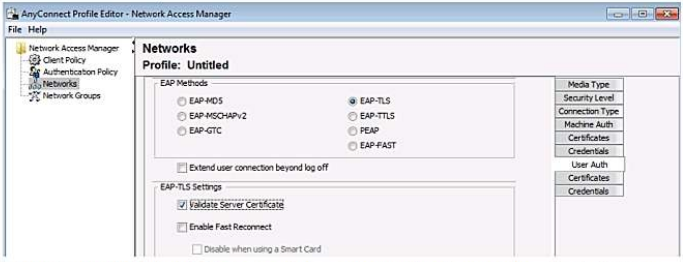
A) Open the NAM Profile Editor from the desktop via **Start > Cisco > Cisco AnyConnect Profile Editor > Network Access Manager Profile Editor**.

B) Navigate to **Network Access Manager > Networks**. Select the default entry '**wired**' and click **Edit**.

C) You only need to modify a few options that are available in the profile editing wizard. Select the **Machine Auth** tab, choose **EAP-TLS** and check the **Validate Server Certificate** checkbox.

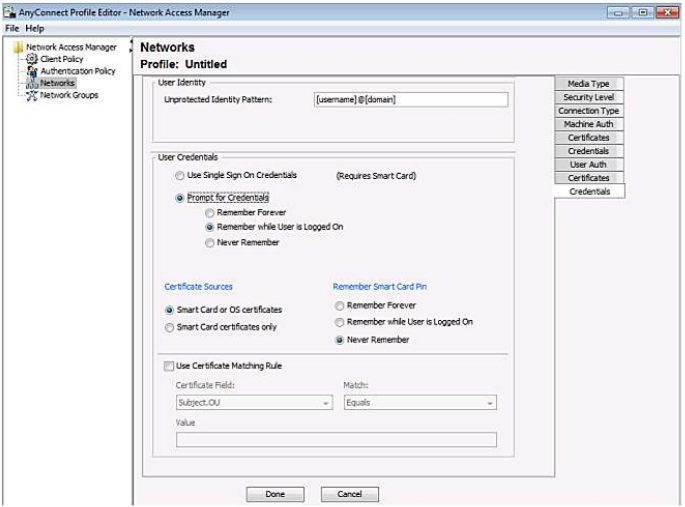



D) Select the **User Auth** tab, choose **EAP-TLS** and check the **Validate Server Certificate** checkbox.




E) Select the **Credentials** tab at the bottom, and choose **Prompt for Credentials** option in the User Credentials section. This option enables the supplicant to use the user certificate store instead of a smart card. Leave all other settings at their default values.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.




F) Click **Done**. Use **File > Save As** to save the profile. Save the profile as **configuration.xml**. If properly named, the profile editor will immediately process the file, update the AnyConnect profile, and delete this temporary file.

G) Close the Network Access Manager Profile Editor.

H) From the system tray, right-click the AnyConnect icon and select **Network Repair**.

***Step 4***

Troubleshoot the problem with EAP-TLS authentication of the domain administrator.

# Task 6: Guide For Troubleshooting EAP-TLS

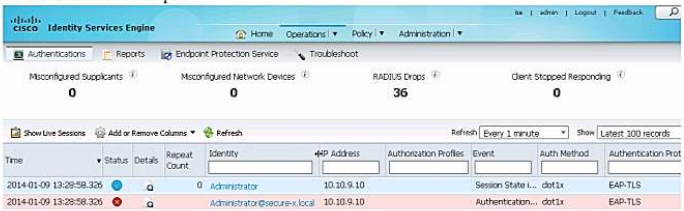
This section contains guidelines on how to resolve the issues with EAP-TLS authentication. Use it for verification of a systematic troubleshooting approach.

Complete the following steps:

### *Step 1*

Examine the authentication on the Cisco ISE:

A) View authentication attempts.




B) Examine the details. The authentication has failed because of an unknown CA in the certificate authentication chain.

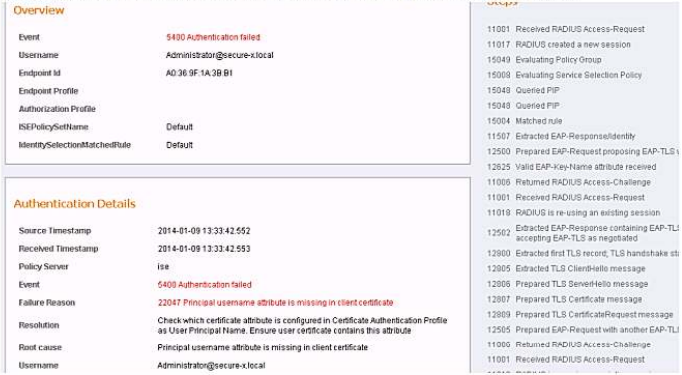
### *Step 2*

**Fix the problem with the unknown CA in the client certificate chain.** For more guidance, you can consult the **Answer Key**.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 3***

Toggle the switch port and examine the authentications on the Cisco ISE. The authentications will still fail. Examine the details. The principal username attribute is missing in the client certificate.

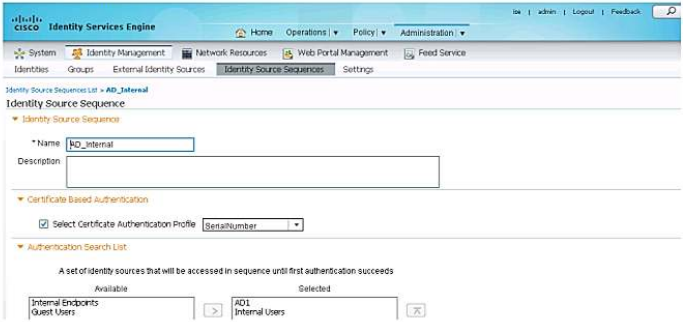


***Step 4***

Resolve the problem with the lack of principal username in the client certificate:

A) Go to **Policy > Authentication**. Examine the identity source sequence used for 802.1X authentication. It is AD_Internal.

B) Go to **Administration > Identity Management > Identity Source Sequences**. Examine the configuration of the sequence AD_Internal. You should find that it uses the Certificate Authentication Profile "SerialNumber".




**Note** Certificate authentication profiles define the which certificate field is used as the user principal name.

C) Go to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**. Examine the existing profiles. You should find that the profile "CommonName" uses the common name as the principal user ID. This will work in this environment.

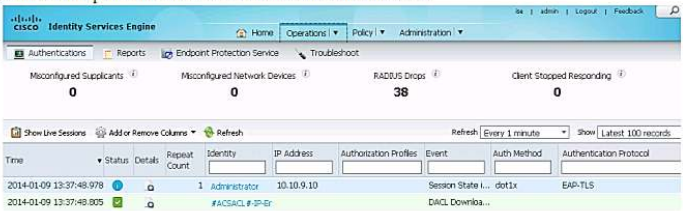
**Note** You can investigate the user and machine certificates on the Employee-PC using the certmgr.msc and Microsoft Management Console (MMC) utilities to verify that the Common Name is set correctly.

D) **Fix the problem**. Consult the **Answer Key** if you need more help.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 5

Toggle the switch port. The EAP-TLS authentication should work:




### Step 6

On the Employee-PC, reset the AnyConnect supplicant to its default settings. This will enable EAP-FAST (EAP-MSCHAPv2) and EAP chaining:

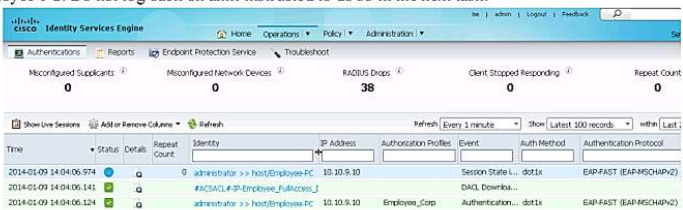
A) Open the Network Access Manager Profile Editor by clicking its desktop icon.

B) Use **File > Save As** to save the profile with default settings as **configuration.xml** without changing the path to which the file is saved.

C) From the system tray, right-click the **AnyConnect** icon and and select **Network Repair** or restart the Employee-PC if the administrator authentication does not work.

### Step 7

Verify that the administrator is successfully authenticated via EAP-FAST (EAP-MSCHAPv2). Restart the Employee-PC. Do not log back on until instructed to do so in the next task.




# Task 7: Troubleshoot Authorization

This section includes brief descriptions of the trouble tickets. Try to troubleshoot the issues on your own. The next section contains guidelines to systematically troubleshoot the problems. The last section (Answer Key) shows the solution, where applicable.


https://t.me/learningnets

### Activity Procedure

Complete the following steps:

| Note | For the rest of the trouble tickets the 802.1X supplicant on Employee-PC should use EAP-MSCHAPv2. |
|---|---|

#### *Step 1*

Troubleshoot the network connectivity problem of the domain user **marketing1**. The user password is **cisco**. The user should be able to browse cisco.com when logged on to the Employee-PC.

Follow the next task to systematically troubleshoot this problem.

#### *Step 2*

Troubleshoot the network connectivity problem of the domain user **marketing1**. The user password is **cisco**. The user should be able to browse www.cisco.com when logged on to the Employee-PC.

Follow the next task to systematically troubleshoot this problem.

## Task 8: Guide For Troubleshooting Authorization

This section contains guidelines on how to resolve the authorization issues. Use it for verification of a systematic troubleshooting approach.

### Activity Procedure

Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 1***

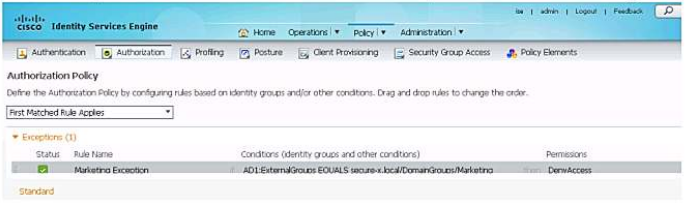
Troubleshoot the authorization of user marketing1, who cannot connect to any network resources, despite successful authentication:

A) Log on as **marketing1** to the Employee-PC. View the authentications on Cisco ISE. You should see that the authentication failed.

B) Examine the details. You should see that the reason for the authentication failure is that the client has been rejected per authorization profile. In this case the failure is caused by the authorization and not authentication failure.

C) In the ISE GUI, go to **Policy > Authorization** and examine the authorization policy. You will see that the only rule that applies the DenyAccess authorization profile is the Default rule. The access of the marketing1 user should be, however, defined by the Employee Corporate Access rule.

D) Expand the exception rules. You should see that there is an exception rule. Examine its configuration.




**Note** Exceptions rules are used to define exemptions from the authorization policy rules.

E) **Fix the problem and test the resolution.** Consult the **Answer Key** if you need more guidance.

# Task 9: Troubleshoot Central WebAuth

This section includes brief descriptions of the trouble tickets. Try to troubleshoot the issues on your own. The next section contains guidelines to systematically troubleshoot the problems. The last section (Answer Key) shows the solution, where applicable.


https://t.me/learningnets

### Activity Procedure

Complete the following steps:

#### *Step 1*

Troubleshoot the central WebAuth functionality to enable access from the Guest-PC.

Background information: the Guest-PC does not have a 802.1X supplicant. WebAuth should enable access of domain users and guests. When a user logs on to the Guest-PC and attempts a connection to the Internet, they should be redirected to the WebAuth. Your task is to troubleshoot the web authentication of domain users. When the domain users can authenticate against the guest portal, the guest access should also work. You do not need to test the guest access.

Follow the next task to systematically troubleshoot this problem.

# Task 10: Guide For Troubleshooting Central WebAuth

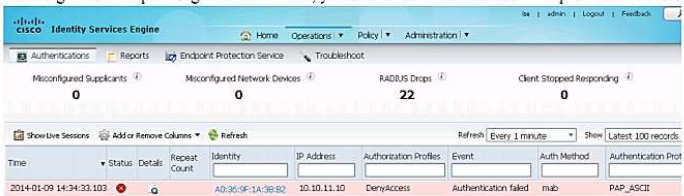
This section contains guidelines on how to resolve the central web authentication issues. Use it for verification of a systematic troubleshooting approach.

### Activity Procedure

Complete the following steps:

#### *Step 1*

After enabling the switchport GigabitEthernet 0/2, you should see failed access attempts in the ISE GUI.

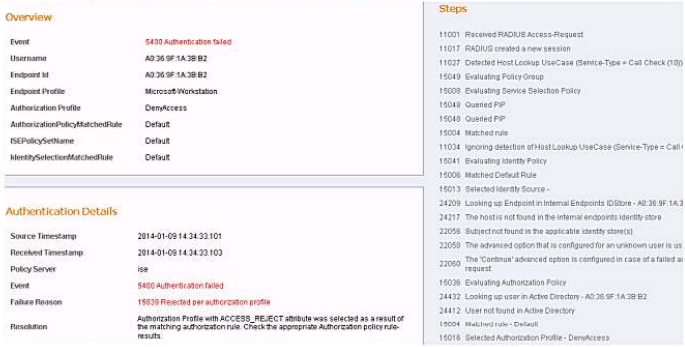




https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 2

Examine the details. You should see that the endpoint MAC address has not been found in the local endpoint database, and the 'Continue' advanced option is configured in case of a failed authentication request. Ultimately an authorization rule has been matched that denies all access.




**Note** Central WebAuth requires an authorization rule that redirects traffic for WebAuth. In the next step you will analyze the ISE authorization policy, why the WebAuth authorization rule is not matched.

### Step 3

Examine the ISE authorization policy (Policy Authorization). You will see the WebAuth that should apply the WEBAUTH profile. The only condition for the WebAuth rule is "Network Access Use Case Equals Host Lookup".

### Step 4

Re-examine the authentication details to see if the failed access attempt shows use case "Host Lookup". Look at the Steps section on the right. You should see "Detected Host Lookup Use Case" in the third line.

**Note** The current problem boils down to the fact that, despite the detected Host Lookup Use Case, the WebAuth authorization rule is not matched.

### Step 5

View the ISE authentication policy (**Policy > Authentication**). Examine the MAB authentication rule that allowed the Guest-PC to pass the authentication using the Advanced option to continue if the user not found. It specifies that the access attempts will be authenticated using the allowed protocol list **Default Network Access**.


https://t.me/learningnets

### *Step 6*

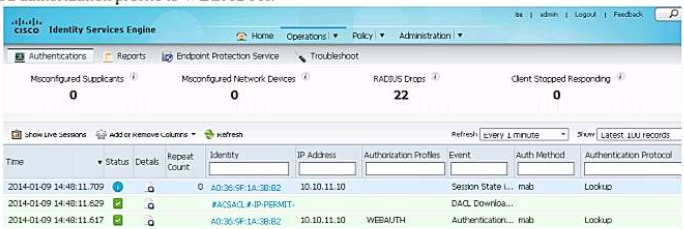
Go to **Policy > Policy Elements > Results > Authentication > Allowed Protocols** to examine the allowed protocol list **Default Network Access**.

### *Step 7*

**Resolve the problem.** See the **Answer Key** if you need further assistance.

### *Step 8*

Toggle the switchport GigabitEthernet 0/2. After a while you should see a successful authentication. The applied authorization profile is WEBAUTH.





https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 9

Despite successful authentication, when you attempt to connect to cisco.com from the Guest-PC, you are not redirected to WebAuth. Verify the authentication/authorization status of the switchport.

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.11.10
            User-Name:  A0-36-9F-1A-3B-B2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT-ALL-52cd4457
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A0102000000D601887B24&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000000D601887B24
      Acct Session ID:  0x000000F4
              Handle:  0x160000D7
Runnable methods list:

       Method   State
       mab      Authc Success
       dot1x    Not run
```

### Step 10

Verify if the switch configuration meets the requirements for WebAuth using the Evaluate Configuration Validator tool:

A) In the ISE GUI, go to **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator**. Enter the switch IP address (**10.10.2.2**) and select Web Authentication. Click **Run**.

B) Log in as admin with password **cisco**. Examine the results.

| Note | Among the missing commands reported as mandatory, the **ip admission name, aaa authorization auth-proxy default group radius** and **fallback profile** commands are not required in this environment. |
|---|---|

C) **Resolve the problem on the switch**. The **Answer Key** can provide further guidance.

### Step 11

Examine if the WebAuth redirection succeeds. It will not work.


https://t.me/learningnets

***Hint:*** *Check if the dACL permits access to the service defined by the URL redirect.*

### *Step 12*

Examine if the Guest-PC can access the URL redirect service. You may try to access the redirect URL from a web browser. Alternatively, check the dACL applied to the port. You should see that IP traffic to 10.10.2.20 is denied. If you resolve ise.secure-x.local specified in the redirect URL, you will get the ISE address 10.10.2.20.

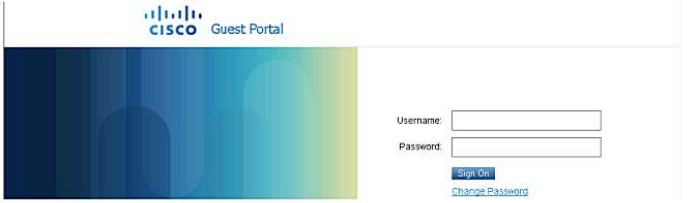
```
HQ-Sw# show ip access-lists interface gigabit 0/2
     deny tcp host 10.10.11.10 host 10.10.2.20
     permit ip host 10.10.11.10 any
```

### *Step 13*

**Fix the dACL problem on the ISE**. The correct dACL should deny ICMP traffic to the ISE and permit all other IP traffic. Further guidance is available in the **Answer Key**.

### *Step 14*

Shut down and re-enable the switchport GigabitEthernet0/2. Wait about a minute until the authorization profile is applied to the port. Attempt to connect to cisco.com. When redirected to WebAuth, log in as **it1** with password **cisco**. The login will fail.



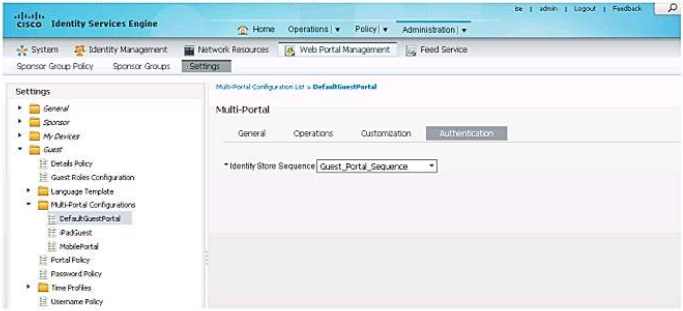

### *Step 15*

Examine the authentications on the ISE. You will not see any login attempts. The guest portal seems not to "forward" the request to the ISE authentication service.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

### Step 16

Identify the identity source sequence used by the guest portal (**Administration > Web Portal Management > Settings > Guest > Multi-portal Configurations > DefaultGuestPortal**). Under the Authentication tab you will that Guest_Portal_Sequence is used.




### Step 17

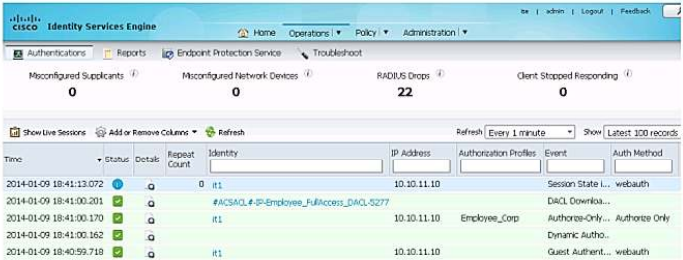
Examine the identity source sequence Guest_Portal_Sequence (**Administration > Identity Management > Identity Source Sequences**).

### Step 18

**Resolve the problem associated with the identity source sequence**. The **Answer Key** is available for further assistance.

### Step 19

Toggle the interface GigabitEthernet 0/2 on the switch. On the Guest-PC, go to cisco.com and log in to the guest portal as it1 with password cisco. Accept the AUP. Go to cisco.com again. The connection should succeed.





https://t.me/learningnets

# Task 11: Troubleshoot Posture

This section includes brief descriptions of the trouble tickets. Try to troubleshoot the issues on your own. The next section contains guidelines to systematically troubleshoot the problems. The last section (Answer Key) shows the solution, where applicable.

### Activity Procedure

Complete the following steps:

#### *Step 1*

Troubleshoot the posturing of the Employee-PC, when the employee it1 logs on.

Background information: The ISE has been configured to check the security posture of endpoints used by the IT employees. The posture service should trigger when the user it1 with password cisco logs on to the Employee-PC. The rules demand that Antivirus (AV) and Antispyware (AS) software is installed on the endpoints and is up-to-date. In this scenario, Windows Defender is used as AS software, and ClamWin Antivirus as AV software.

# Task 12: Guide For Troubleshooting Posture

This section contains guidelines on how to resolve the posture service. Use it for verification of a systematic troubleshooting approach. The solution, where applicable, is shown in the Answer Key.

### Activity Procedure

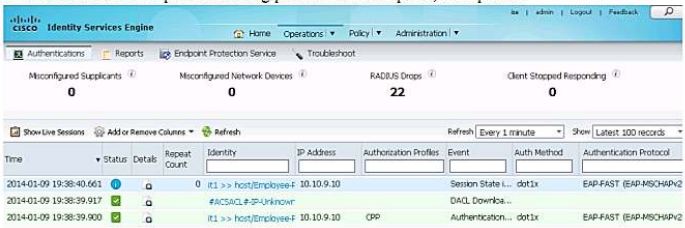
Complete the following steps:


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

***Step 1***

Troubleshoot the NAC agent provisioning on the Employee-PC:

A) After logging on to the Employee-PC as **it1** with password **cisco**, view the access attempts on the ISE. You will see that the CPP profile is being pushed to the endpoint, as expected:

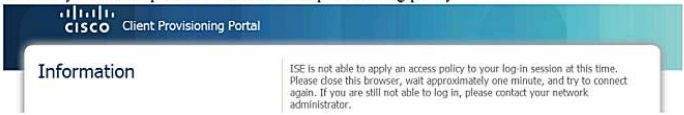



B) On the switch, examine the authentication/authorization status of the switchport GigabitEthernet 0/1, where the Employee-PC is connected:

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.10
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Unknown_Noncompliant_dACL-52bd5866
     URL Redirect ACL:  CPP-REDIRECT-ACL
         URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A0102000001E0026350A8&action=cpp
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0102000001E0026350A8
      Acct Session ID:  0x00000204
              Handle:  0x5B0001E1
Runnable methods list:

       Method   State
       dot1x    Authc Success
       mab      Not run
```

C) On the Employee-PC, open a browser and connect via HTTP to HQ-Srv. After a while you will be redirected to the client provisioning portal but the ISE will not be able to apply an access policy. This situation may indicate a problem with the client provisioning policy.





https://t.me/learningnets

D) Examine the client provisioning policy (**Policy > Client Provisioning Policy**). Edit the 'Win7 Wired' rule to investigate the conditions. You should see that RADIUS: NAS-Port-Type attribute is checked against the value Virtual.

E) **Fix this rule**. Further guidance is available in the **Answer Key**.

### *Step 2*

Refresh the browser window on the Employee-PC. The client provisioning portal will offer you the option to install the NAC agent. Install it by following the installation wizard and selecting the default options.

### *Step 3*

After the installation, the NAC will declare the endpoint as compliant. Verify it in the ISE authentications page.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab Answer Keys

## Lab 1-1: Bootstrap Identity System

### Task 1: Define Local User in Cisco ISE

***Step 1***

There are no solutions for this lab.

## Lab 2-1: Enroll Cisco ISE in PKI

### Task 1: Task 1: Verify IE Operation Before ISE PKI Enrollment

***Step 1***

There are no solutions for this lab.

## Lab 2-2: Implement MAB and Internal Authentication

### Task 1: Deploy MAC Authentication Bypass

***Step 1***

There are no solutions for this lab.

**https://t.me/learningnets**

# Lab 2-3: Implement External Authentication

## Task 1: Join ISE to the Active Directory

***Step 1***

There are no solutions for this lab.

# Lab 3-1: Implement EAP-TLS

## Task 1: Configure Employee-PC for EAP-TLS

***Step 1***

There are no solutions for this lab.

# Lab 3-2: Implement Authorization

## Task 1: Enable EAP Chaining

***Step 1***

There are no solutions for this lab.

# Lab 3-3: Implement Cisco TrustSec and MACsec

## Task 1: Prepare ISE for TrustSec communication with the HQ-SW

***Step 1***

There are no solutions for this lab.

# Lab 4-1: Implement WebAuth for Employees

## Task 1: Configure Switch for Central WebAuth

***Step 1***

There are no solutions for this lab.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

# Lab 4-2: Implement Guest Service

## Task 1: Configure Access to the Sponsor Portal

***Step 1***

There are no solutions for this lab.

# Lab 5-1: Implement Posture Service

## Task 1: Prepare Initial Components

***Step 1***

There are no solutions for this lab.

# Lab 5-2: Implement Profiler Service

## Task 1: Observe Profiling without Probes

***Step 1***

There are no solutions for this lab.

# Lab 6-1: (Optional) Troubleshooting Prep

## Task 1: Restore Broken Backup Configurations on Switch and ISE

***Step 1***

There are no solutions for this lab.


https://t.me/learningnets

# Lab 6-2: (Optional) Troubleshoot Network Access Controls

## Task 2: Guide for Troubleshooting 802.1X Authentication Against Local ISE Database

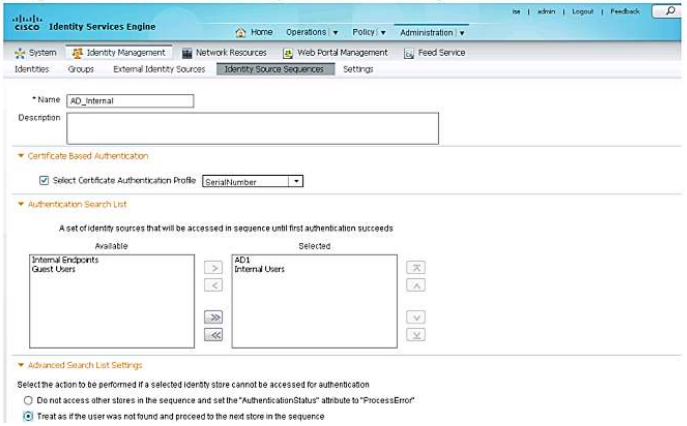
### *Step 3*

As a result of the troubleshooting with the Evaluate Configuration Validator, you should enter these commands on the switch:

```
interface GigabitEthernet 0/1
 dot1x pae authenticator
 mab
!
interface GigabitEthernet 0/2
 dot1x pae authenticator
 mab
```

### *Step 6*

After examining the identity source sequence (AD_Internal), select the option "Treat as if the user was not found and proceed to the next store in the sequence." Save the changes.



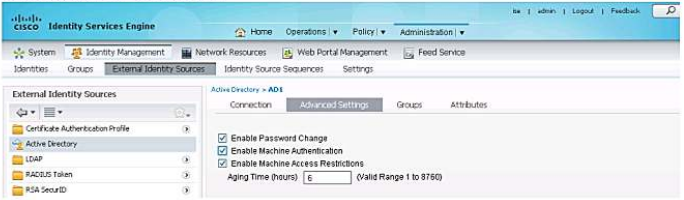


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

## Task 4: Guide For Troubleshooting 802.1X Authentication Against Active Directory

### *Step 4*

To enable machine authentication against the AD, go to **Administration > Identity Management > External Identity Sources**. Choose **Active Directory**, click the **Advanced Settings** tab, enable machine authentication, and save the changes.



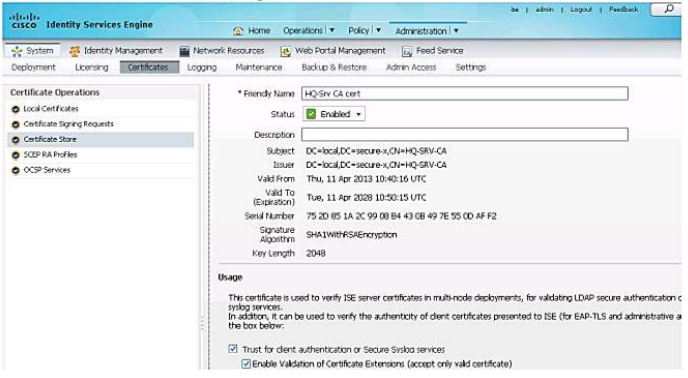

## Task 6: Guide For Troubleshooting EAP-TLS

### *Step 2*

To fix the problem with the unknown CA in the client certificate chain:

A) Go to **Administration > Certificates > Certificate Store**. Click the HQ-Srv CA cert and click **Edit**.

B) Check the **Trust for client authentication or Secure Syslog services** checkbox. Enable the validation of certificate extensions. Save the settings.

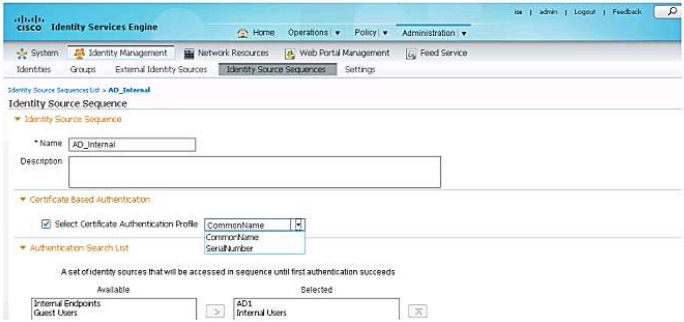




https://t.me/learningnets

### *Step 4*

To fix the problem with the principal username in the certificate, go to **Administration > Identity Management > Identity Source Sequences**. Edit the sequence AD_Internal. Set the Certificate Authentication Profile to "CommonName" and save the settings.




## Task 8: Guide For Troubleshooting Authorization

### *Step 1*

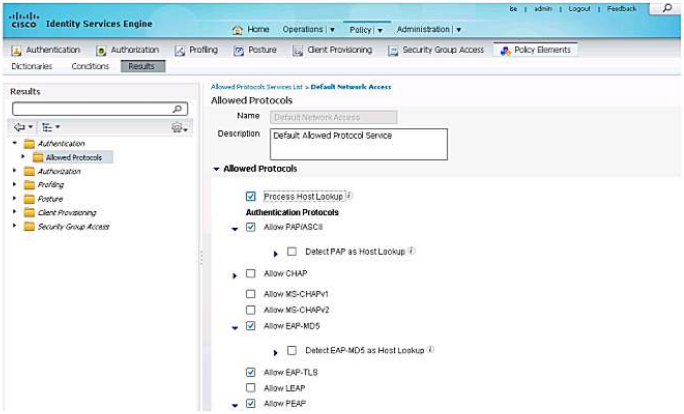
To resolve the authorization problem of the Marketing group, delete or disable the exception rule, save the policy, shut down and re-enable the switch interface. After a while verify that the network connectivity has been re-established for the user marketing1 on the Employee-PC.

## Task 10: Guide For Troubleshooting Central WebAuth

### *Step 7*

To resolve the problem of the disallowed Process Host Lookup, go to **Policy > Policy Elements > Results > Authentication > Allowed Protocols** , edit the **Default Network Access** configuration. The Process Host Lookup will be disabled. Allow it and save the configuration.


https://t.me/learningnets
© 2014 Cisco Systems, Inc.



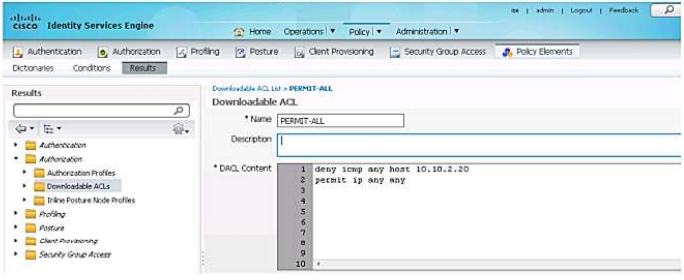

### *Step 10*

As a result of the Evaluate Configuration Validator, enter these commands on the switch:

```
ip http server
ip http secure-server
```

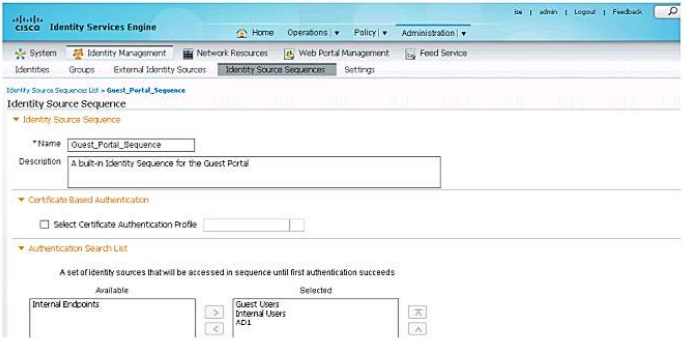
### *Step 13*

To identify the incorrect dACL on the ISE, go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Examine the WEBAUTH profile. You should see that the dACL is PERMIT-ALL. To fix the dACL on the ISE, go to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**. Edit the dACL PERMIT-ALL. Change 'tcp' in the first statement to 'icmp' and save the changes.



### *Step 18*

After examining the Guest_Portal_Sequence in the **Administration > Identity Management > Identity Source Sequences** menu, you will have discovered that the identity source AD1 is never looked up. Add the AD1 identity source to the list and save the change.




## Task 12: Guide For Troubleshooting Posture

### *Step 1*

To fix the CPP rule 'Win7 Wired', go to **Policy > Client Provisioning Policy**, and edit the NAS-Port-Type attribute condition in the Other conditions column. Change 'Radius:NAS-Port-Type Equals Virtual' to 'Radius:NAS-Port-Type Equals Ethernet'. Save the configuration.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.