Policy Aware IBNS
Wired Deployment Guide

November, 2013

Contents

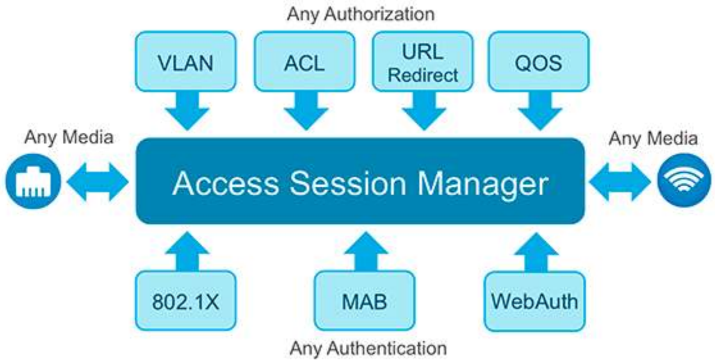
Overview

With the evolution of Bring-Your-Own-Device (BYOD) and the diverse workgroup access requirements, enterprises are compelled to adopt a secure way of granting network access. While network authentication with IEEE 802.1X is fundamental for such deployments, to cater to the ever-evolving trends, a flexible and comprehensive solution is needed. Building on to the traditional Identity based networking services, the current deployment challenges demand for an extensible framework, that can provision enhanced authentication flexibility, local authorizations, role-based access control, consistent policy driven access and has the capability to handle IPv6 end-points. This document covers how to deploy policy aware IBNS on the Cisco Catalyst 3850 running IOS-XE 3.3.0SE. However most of the use cases can be deployed on Catalyst 2K,3K and the 4K series switch platforms that support 15.2(1)E or XE3.5.0E and later.

Policy Aware IBNS

The enhanced Access session manager provides a policy and identity-based framework for flexible and scalable services to the secure access clients. This evolutionary framework enhances its predecessor, auth-manager, by provisioning for any authentication with any authorization on any media, wired or wireless. While the new policy engine is equipped with a set of enhanced capabilities, a flexible configuration option with the Cisco Common Classification Policy Language (C3PL) gives administrators more power in defining the enterprise-wide secure access policies.

Figure 1. Access Session Manager

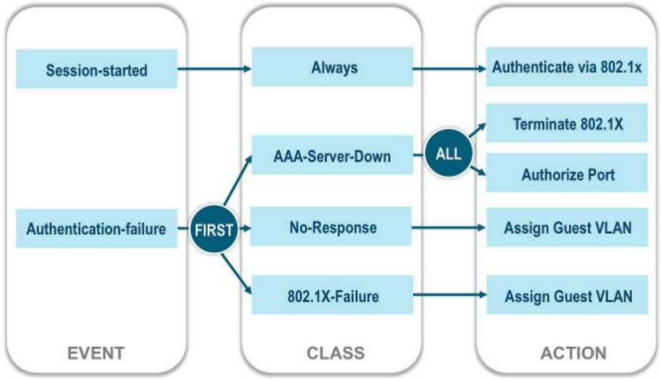


Identity Control Policy (C3PL)

The identity control polices define the actions that the Access session manager takes in response to specified conditions and end point events. A variety of system actions, conditions, and events can be combined using a consistent policy language. For various events, such as session start or session failure, administrators can specify actions in the control policy. These actions can be executed conditionally for different subscribers (endpoints) based on various match criteria. Control policies are activated on interfaces and typically control the authentication of end-point identity and the activation of services on sessions. For example, administrator can configure a control policy to authenticate specific end users, and then provide them with access to specific services.

A control policy consists of one or more control policy rules and a decision strategy that governs how the policy rules are evaluated. A control policy rule consists of a control class (a flexible condition clause), an event for which the condition is evaluated, and one or more actions. Actions are general system functions, such as “authenticate” or “activate.” Administrators define the specific actions that an event will trigger, and some events have default actions.

Figure 2. Identity Control Policy



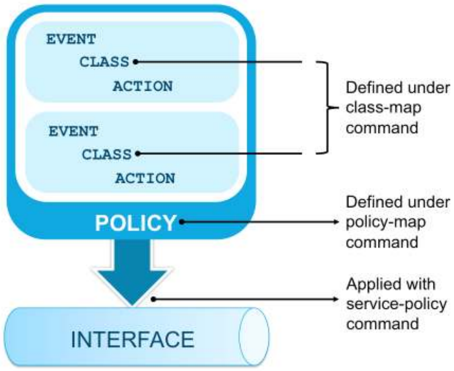
Analogy: The Identity control policy can be analogous to an email management policy on a workstation application. Where ‘Event’ could be an email arriving, ‘Class’ being classification of the emails based on pre-defined conditions (from-an-address, to-an-address), and moving the email to a specific folder, delete, mark-urgent, etc. can be one of the items defined as a ‘Action’.

Identity Control Policy Configuration Overview

Control policies express system functionality in terms of an event, a condition, and an action. There are three steps in defining a control policy:

1. **Create one or more control classes**—A control class specifies the conditions that must be met for a control policy to be activated. A control class can contain multiple conditions, each of which will evaluate as either true or false. Match directives specify whether all, any, or none of the individual conditions must evaluate true for the class to evaluate true. Or, administrators can specify the default control class that does not contain any conditions, and always evaluates true.
2. **Create a control policy**—A control policy contains one or more control policy rules. A control policy rule consists of a control class, an event that causes the class to be evaluated, and one or more actions. Actions are numbered and executed sequentially.
3. **Apply the control policy**—A control policy is activated by applying it to an interface.

Figure 3. Identity Control Policy Configuration


EVENT
CLASS
ACTION
EVENT
CLASS
ACTION
POLICY
INTERFACE
Defined under class-map command
Defined under policy-map command
Applied with service-policy command

Migrating Identity Configurations to c3pl Policy

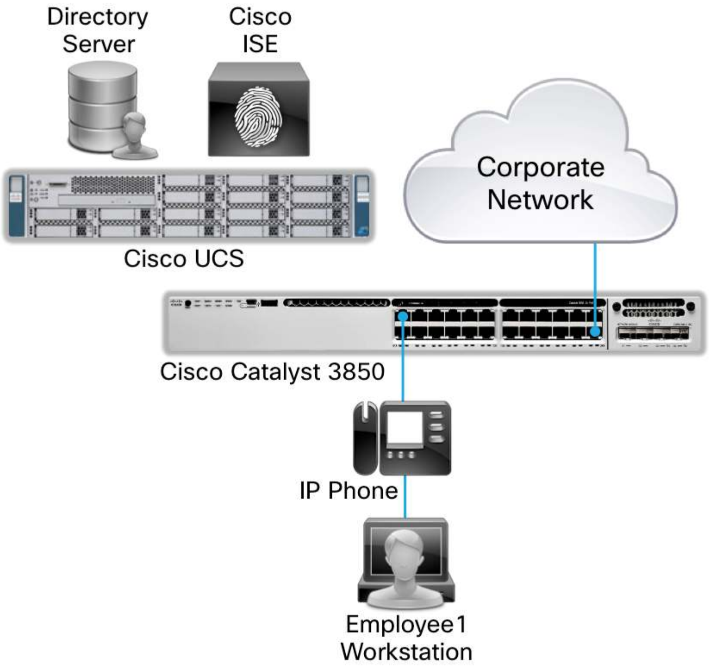
The power of the Access session manager can be leveraged with a new set of configuration commands and the C3PL policies. The new configuration method offers greater flexibility in defining enterprise wide security policies, and helps to reduce repeated configurations on a per port basis. Configuring the C3PL policy from scratch could sound challenging considering the various options the command-set is equipped with. To ease this effort, the IOS comes with a ‘conversion tool’ that migrates the legacy identity configuration commands on the port to new policy mode configurations.

The device defaults to the legacy configuration mode until the network administrator does one of the following:

Execute the ‘authentication display new-style’ command: This command switches the conventional identity configurations to C3PL display mode, temporarily converting the legacy configuration to a policy aware Identity configuration so administrators can see how it looks before making the conversion permanent. It is possible to switch back to legacy mode by using the authentication display legacy command.

Configure new identity commands: After entering the first explicit new identity command or edit the C3PL policy in the system, the configuration converts to C3PL display mode permanently and legacy commands are suppressed. The authentication display command is disabled, and the system can no longer revert to the legacy configuration mode.

Figure 4. Policy Aware IBNS Network Topology



In the topology diagram above (Figure 4), the Catalyst 3850 is configured for 802.1X port authentication. The configuration commands are of the traditional type, which are synonymously called the Auth-manager style.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa session-id common
!
dot1x system-auth-control
!
radius server ise
 address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
 automate-tester username probe-user
 key cisco
!
```

The per port configuration on the box is set for low-impact-mode. Note that the legacy commands starts with ‘authentication’ key word.

```
interface GigabitEthernet1/0/1
 description ** Access Port **
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 10
 ip access-group IPV4-PRE-AUTH-ACL in
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
```

The authentication display new-style command converts the legacy configurations in to new style. Notice the disclaimer that states that the legacy mode cannot be returned to if the system is reloaded with the configurations saved, and to configure IPv6-capable web authentication, new-style configurations is a must.

```
switch#authentication display new-style
Please note that while you can revert to legacy style configuration at any time
unless you have explicitly entered new-style configuration, the following caveats
should be carefully read and understood.
(1) If you save the config in this mode, it will be written to NVRAM in NEW-style
    config, and if you subsequently reload the router without reverting to legacy
    config and saving that, you will no longer be able to revert.
    (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become
    IPv6-capable once you have entered new-style config manually, or have
    reloaded with config saved in 'authentication display new' mode.
```

Two key changes to notice after moving on to the new-style configurations are (1) the ‘authentication’ commands will be replaced with commands starting with ‘access-session’ keyword (2) A service-policy referencing an identity control policy-map with the name POLICY_<Interface-Name> gets applied on the port.

```
interface GigabitEthernet1/0/1
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 10
  ip access-group IPV4-PRE-AUTH-ACL in
  access-session port-control auto
  mab
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber POLICY_Gi1/0/1
!
```

The policy-map unlike the QoS MQC shall have statements specific for an identity control policy.

```
policy-map type control subscriber POLICY_Gi1/0/1
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
      20 authenticate using mab priority 20
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 60
    30 class always do-until-failure
      10 terminate dot1x
      20 terminate mab
      30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
!
```

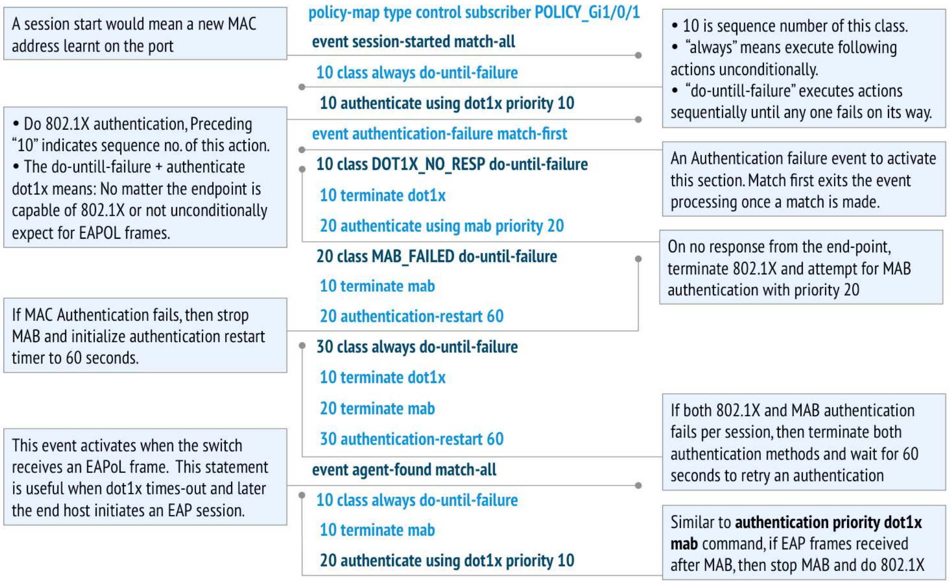
The system auto-generates class-maps that are referenced in the identity control policy.

```
class-map type control subscriber match-all DOT1X_NO_RESP
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
  match method mab
  match result-type method mab authoritative
!
```

The new-style can be reverted back to old style as long as no new-style commands (access-session, policy-map type control, class-map type control) are executed.

Tip: Use the “authentication display” exec command to switch back and forth between the command modes. This gives a fair understanding on how to build an Identity control policy.

Figure 5. Interpreting Identity Control Policy



```
policy-map type control subscriber POLICY_Gi1/0/1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  30 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
```

A session start would mean a new MAC address learnt on the port

- 10 is sequence number of this class.
- “always” means execute following actions unconditionally.
- “do-untill-failure” executes actions sequentially until any one fails on its way.

- Do 802.1X authentication, Preceding “10” indicates sequence no. of this action.
- The do-untill-failure + authenticate dot1x means: No matter the endpoint is capable of 802.1X or not unconditionally expect for EAPOL frames.

An Authentication failure event to activate this section. Match first exits the event processing once a match is made.

On no response from the end-point, terminate 802.1X and attempt for MAB authentication with priority 20

If MAC Authentication fails, then strop MAB and initialize authentication restart timer to 60 seconds.

If both 802.1X and MAB authentication fails per session, then terminate both authentication methods and wait for 60 seconds to retry an authentication

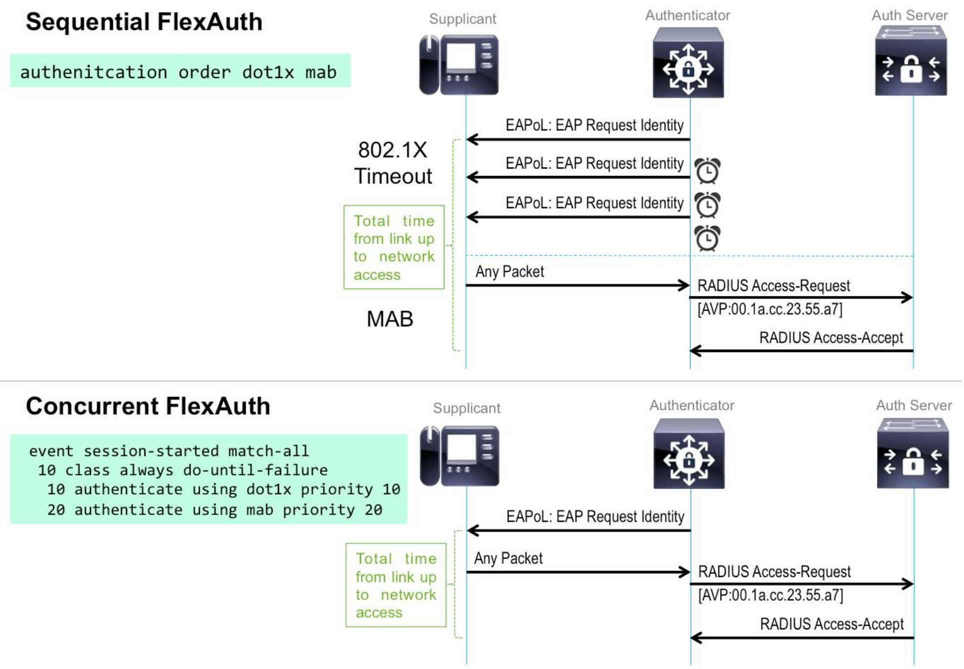
This event activates when the switch receives an EAPoL frame. This statement is useful when dot1x times-out and later the end host initiates an EAP session.

Similar to **authentication priority dot1x mab** command, if EAP frames received after MAB, then stop MAB and do 802.1X

Enhanced FlexAuth: Concurrent Authentication

Traditionally flexible authentication has been implemented in a sequential manor, where in one authentication method, for example 802.1X, is tried first and upon authentication-failure or a time-out, the next method is attempted, which in most cases is Mac Authentication Bypass (MAB). Optionally, the third authentication method could be web authentication on MAB failure. This sequence, along with the other port transitioning sequence because of power provisioning, and spanning-tree convergence, imposes a considerable delay in on-boarding the endpoints to the network. The session manager addresses this limitation in two ways: (1) The session manager can attempt multiple authentication methods concurrently (2) The authentication is triggered on reception of a First-Sign-of-Life (FSoL) packet, which could be a DHCP/CDP/ARP or any other packet that has the MAC address of the device in it.

Figure 6. Concurrent Authentication



```
authenitcation order dot1x mab
```

```
event session-started match-all
 10 class always do-until-failure
  10 authenticate using dot1x priority 10
  20 authenticate using mab priority 20
```

To configure concurrent authentication, either the system-generated policy-map has to be modified, or a new policy-map that calls for all authentication methods must be defined under “session-started” event.

Note: When either the Identity control policy is being modified, or a new one is created, the system puts up a warning message mentioning that the new commands cannot be converted back to the legacy commands. Type “yes” to continue.

```
switch(config)#policy-map type control subscriber ENT-IDENTITY-POL
This operation will permanently convert all relevant authentication commands to
their CPL control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are
strongly advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
```

All the authentication methods must be defined under “session-start” event for concurrent authentication to function.

```
policy-map type control subscriber ENT-IDENTITY-POL
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using mab priority 20
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 60
    30 class always do-until-failure
      10 terminate dot1x
      20 terminate mab
      30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
   !
```

Configuring the new identity commands will disable the legacy commands.

```
switch#authentication display ?
% Unrecognized command
switch#show authentication ?
% Unrecognized command
```

Once the new policy-map is created, it has to be applied on the interface of interest with the service-policy command.

```
switch(config)#interface gigabitEthernet 1/0/1
switch(config-if)#no service-policy type control subscriber POLICY_Gi1/0/1
switch(config-if)#service-policy type control subscriber ENT-IDENTITY-POL
```

On a port bounce, the changes can be seen. The onboarding of the endpoints happens faster because of the simultaneous authentication attempts. The syslogs and the show access-session command can be referred to, to notice the changes.

```
*Sep 3 22:47:42.591: %MAB-5-FAIL: Authentication failed for client
(7011.248d.4b7f) on Interface Gi1/0/1 AuditSessionID 050F142800000FC6006055E0
*Sep 3 22:49:18.949: %DOT1X-5-FAIL: Authentication failed for client
(8875.5651.51d9) on Interface Gi1/0/1 AuditSessionID 050F142800000FC700606468
switch#
switch#show access-session interface gigabitEthernet 1/0/1
Interface  MAC Address     Method   Domain  Status   Fg Session ID
---------------------------------------------------------------------------
Gi1/0/1    7011.248d.4b7f  dot1x    DATA    Auth     050F142800000FC6006055E0
Gi1/0/1    8875.5651.51d9  mab      VOICE   Auth     050F142800000FC700606468

Key to Session Events Status Flags:
 A–Applying Policy (multi-line status for details)
 D–Awaiting Deletion
 F–Final Removal in progress
 I–Awaiting IIF ID allocation
 P–Pushed Session (non-transient state)
 R–Removing User Profile (multi-line status for details)
 U–Applying User Profile (multi-line status for details)
 X–Unknown Blocker

Runnable methods list:
 Handle  Priority  Name
 11      5         dot1x
```

```
12      10        mab
7       15        webauth
```

Note: Since the system runs in the new-style configuration mode, the authentication commands are replaced with access-session commands.

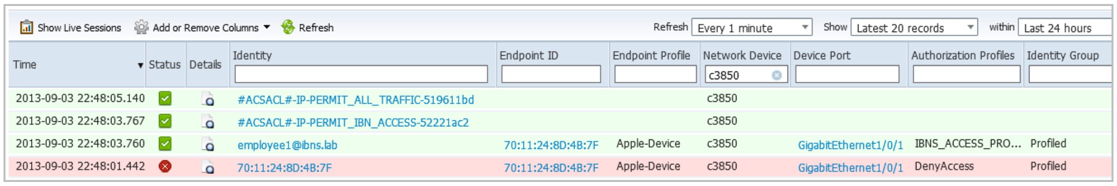
```
switch#show access-session interface gigabitEthernet 1/0/1 details
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x107E440000000DB
      MAC Address:  7011.248d.4b7f
     IPv6 Address:  2001:DB8:100:0:915:AB3:E1F4:E698
     IPv4 Address:  172.20.100.9
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
   Session timeout  N/A
Common Session ID:  050F142800000FC6006055E0
  Acct Session ID:  0x00000FD1
           Handle:  0xCD00001B
   Current Policy:  ENT-IDENTITY-POL

Server Policies:
          ACS ACL:  xACSACLx-IP-PERMIT_IBN_ACCESS-52221ac2
Method status list:
  Method   State
  dot1x    Authc Success
  mab      Stopped
----------------------------------------
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x108C780000000DC
      MAC Address:  8875.5651.51d9
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.15.2
        User-Name:  88-75-56-51-51-D9
           Status:  Authorized
           Domain:  VOICE
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  050F142800000FC700606468
  Acct Session ID:  0x00000FD3
           Handle:  0xD300001C
   Current Policy:  ENT-IDENTITY-POL

Server Policies:
       Vlan Group:  Vlan: 15
```

```
               ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd

      Method status list:
        Method    State
        dot1x     Stopped
        mab       Authc Success
```

Note: The “show ip access-list” command on the conventional catalyst switches shows the translation of the source “any” keyword to the host IP address on successful authorization. On the Catalyst 3850 and the 3650 switches, the ACL is not applied per port, it is applied per session, and the same command “show ip access-list” will not tell if the ip address of the host is translated for the “any” keyword of the dACL. At this time there isn’t any direct method for knowing these translations.

On the RADIUS server, one authentication failed (MAB for PC) and two authentication passed logs (MAB for phone and 802.1X for PC) can be observed.

OPERATIONS → AUTHENTICATIONS



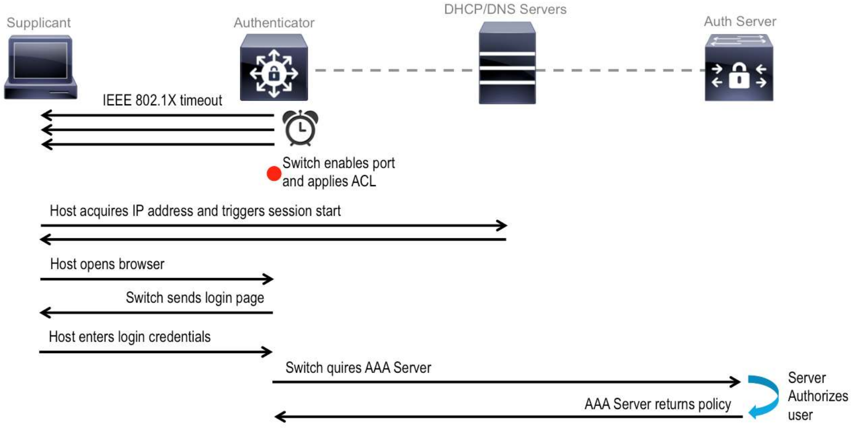
Show Live Sessions | Add or Remove Columns | Refresh | Refresh: Every 1 minute | Show: Latest 20 records | within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group
						c3850			
2013-09-03 22:48:05.140	✓		#ACSACL#-IP-PERMIT_ALL_TRAFFIC-519611bd			c3850			
2013-09-03 22:48:03.767	✓		#ACSACL#-IP-PERMIT_IBN_ACCESS-52221ac2			c3850			
2013-09-03 22:48:03.760	✓		employee1@ibns.lab	70:11:24:8D:4B:7F	Apple-Device	c3850	GigabitEthernet1/0/1	IBNS_ACCESS_PRO...	Profiled
2013-09-03 22:48:01.442	☒		70:11:24:8D:4B:7F	70:11:24:8D:4B:7F	Apple-Device	c3850	GigabitEthernet1/0/1	DenyAccess	Profiled

Enhanced FlexAuth: Local Web Authentication

Provisioning web authentication for network access is essential in cases where the corporate users have to login to network, when they have an expired certificate or may be having other problems with 802.1X logins. Also to on-board guest users, web authentication is the key. Web authentication can be done in two ways: Local Web Authentication (LWA) and Central Web Authentication (CWA). In the former, the authentication happens in two steps: http(s) between the supplicant and the authenticator, and RADIUS between the authenticator and the authentication server. In the latter case, the authentication happens over http(s) between the supplicant and a centralized web server with RADIUS Server doing authorizations (Cisco ISE RADIUS Server can be configured as centralized Web Server for CWA).

Figure 7. Local Web Authentication



WebAuth enhancements with Session manager:

- Same Session-id per MAC address (802.1X, MAB and WebAuth)
- RADIUS Change of Authorization (CoA) for WebAuth Sessions
- IPv6 local web authentication and URL redirects
- Use of custom AAA authentication and authorization method list in contrast to the default login method used in the legacy IOS*
- Modular configuration method with "parameter maps"

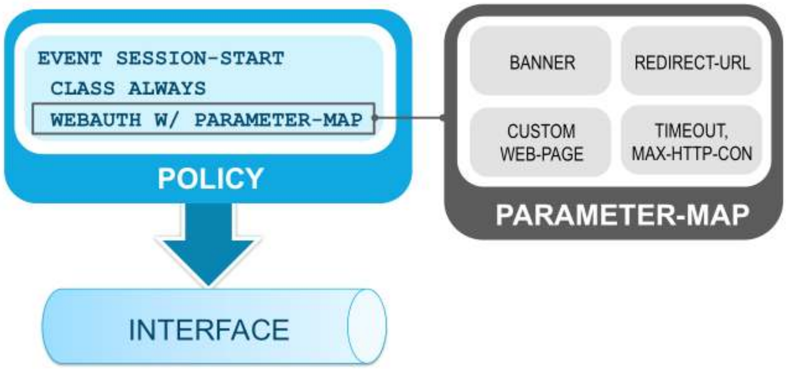
* It is important to note that the legacy implementation of WebAuth requires the use of the default login authentication group as RADIUS. As soon as it is configured, the default login group applies to all login attempts for the switch, including Virtual Teletype Terminal (VTY) and console access. Everyone attempting to use Telnet to access the switch or to access the console is required to authenticate through RADIUS. To prevent the default AAA login configuration from applying to the console and VTY sessions, define a nondefault login group and apply this to the VTYs and the console.

This section focuses on two items: (1) configuring LWA in new-style (2) common session-id for Web Authentication.

Parameter-map

A parameter map allows specification of parameters that control the behavior of actions specified under a control policy. The use of parameter-map is currently limited to web-authentications. A parameter map for web-based authentication sets parameters that can be applied to access sessions during authentication.

Figure 8. Parameter map



Some of the options that can be defined in a parameter-map are:

Banner	Can define banner text or file
Consent	Consent parameters
Custom-Page	To define custom pages: login, expired, success or failure pages
Max-http-conns	Maximum number of HTTP connections per client
Redirect	Redirect URL
Timeout	Timeout for the webauth session

Apart from the AAA and RADIUS global commands for port authentication, an aaa authentication command to cater for web authentication is necessary. In legacy IOS this command used to be “aaa authentication login default group radius”.

```
aaa new-model
aaa authentication login WebAuth group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa accounting identity default start-stop group radius
aaa session-id common
!
dot1x system-auth-control
!
radius server ise
 address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
 automate-tester username probe-user
 key cisco
!
```

Note: aaa accounting dot1x default start-stop group radius, which is essential for logging 802.1X accounting changes to aaa accounting identity default start-stop group radius in new-style mode.

IP device tracking and http server configurations are fundamental for Local Web Authentication (LWA) to work.

```
ip device tracking
!
ip http server
ip http secure-server
!
```

A parameter-map must be configured with attributes that make up the web authentication profile.

```
parameter-map type webauth LWA-PROFILE
 timeout init-state sec 60
 max-http-conns 10
 banner text ^C Cisco Systems, Inc. ^C
!
```

The custom parameter-map should be referenced within the identity control policy along with webauth authentication method. The webauth authentication method can be set as the only authentication method on the port, which is less likely, in a real-time deployment. The typical sequence can be 802.1X, MAB and WebAuth or just the 802.1X and WebAuth methods. With policy-aware IBNS, all the authentications can be set for concurrent attempts too.

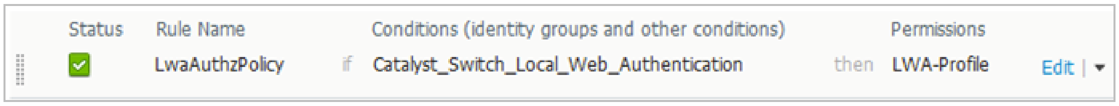
```
policy-map type control subscriber ENT-WEBAUTH-POL
 event session-started match-all
 10 class always do-until-failure
  10 authenticate using dot1x priority 10
  20 authenticate using webauth aaa authc-list WebAuth parameter-map LWA-PROFILE
priority 30
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
  20 class always do-until-failure
   10 terminate dot1x
   20 terminate webauth
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 terminate webauth
   30 authenticate using dot1x priority 10
!
```

The Identity control policy must be applied on the interface along with a pre-auth-acl to allow only limited access until an authentication.

```
interface GigabitEthernet1/0/5
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  ip access-group IPV4-PRE-AUTH-ACL in
  access-session port-control auto
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber ENT-WEBAUTH-POL
!
```

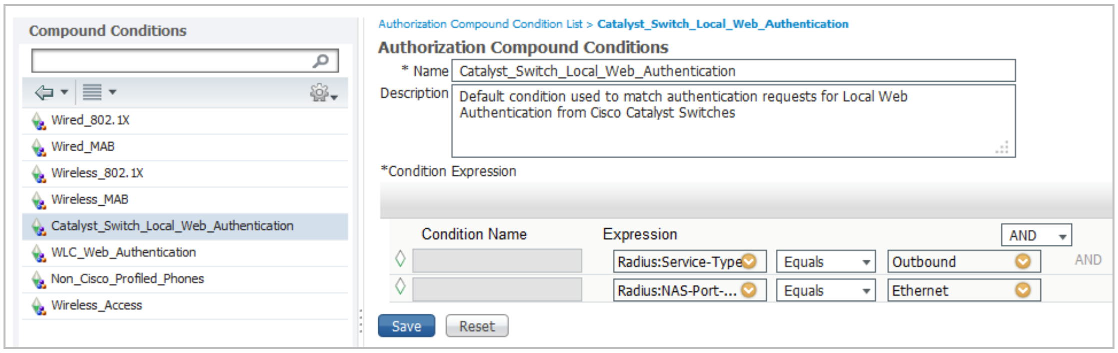
The ISE has to be configured for two items: (1) An authorization policy definition to authorize switch local web authentication sessions (2) An authorization profile, that would send down Cisco AV-Pair: "priv-lvl=15" to the switch upon successful authentication.

POLICY → AUTHORIZATION



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	LwaAuthzPolicy	if	Catalyst_Switch_Local_Web_Authentication	then	LWA-Profile	Edit | ▾

POLICY → POLICY ELEMENTS → CONDITIONS → COMPOUND CONDITIONS



Compound Conditions
Wired_802.1X
Wired_MAB
Wireless_802.1X
Wireless_MAB
Catalyst_Switch_Local_Web_Authentication
WLC_Web_Authentication
Non_Cisco_Profiled_Phones
Wireless_Access
Authorization Compound Condition List > Catalyst_Switch_Local_Web_Authentication

Authorization Compound Conditions

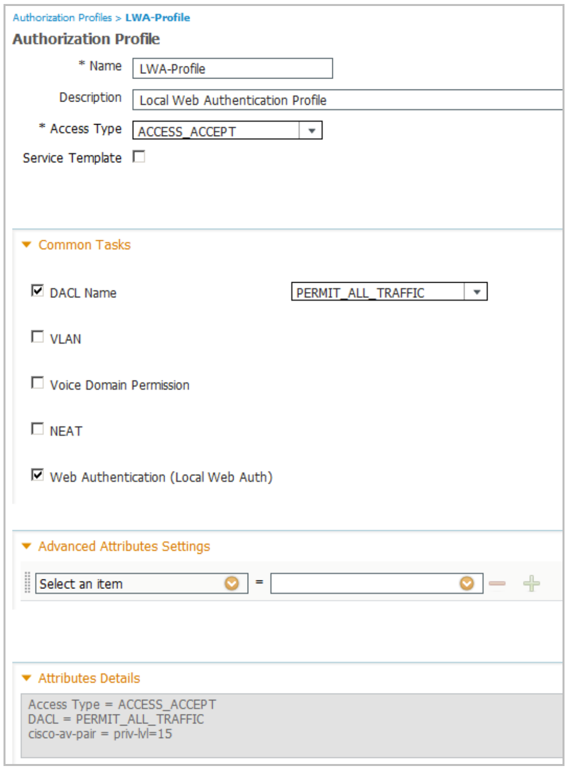
* Name: Catalyst_Switch_Local_Web_Authentication

Description: Default condition used to match authentication requests for Local Web Authentication from Cisco Catalyst Switches

*Condition Expression

Condition Name	Expression			AND
	Radius:Service-Type	Equals	Outbound	AND
	Radius:NAS-Port-...	Equals	Ethernet	

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > LWA-Profile

Authorization Profile

* Name: LWA-Profile

Description: Local Web Authentication Profile

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

□ VLAN

□ Voice Domain Permission

□ NEAT

☑ Web Authentication (Local Web Auth)

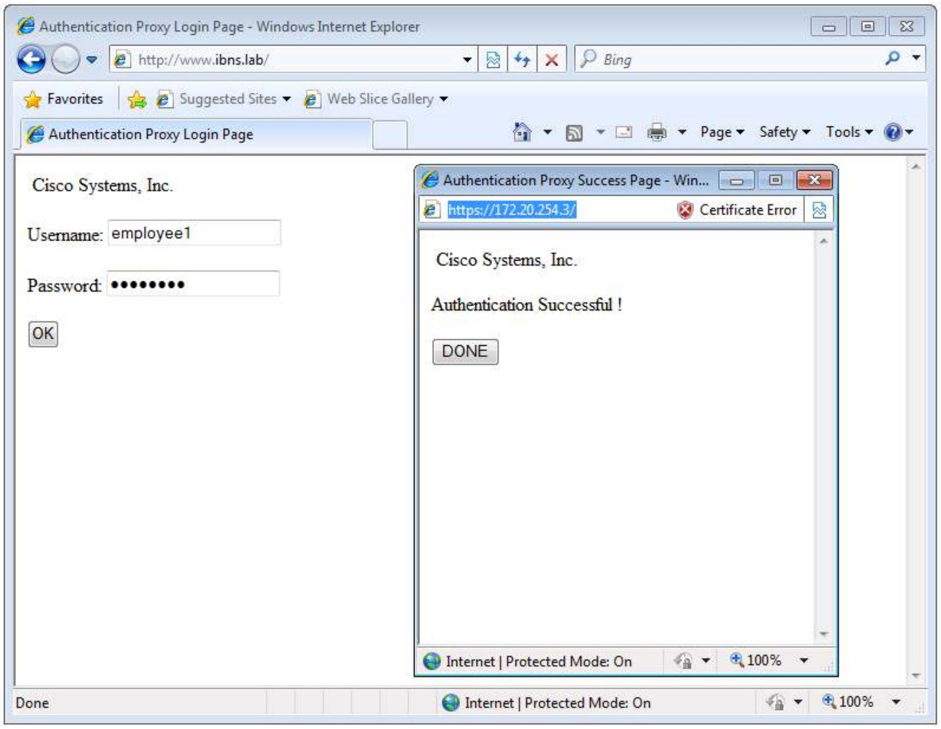
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC
cisco-av-pair = priv-lvl=15

On the client machine, the device gets the IP address, and when the end user opens up a browser and tries to access any URL, the URL gets redirected to the switch web login page. Upon providing valid credentials, the end user is authorized appropriately.



Authentication Proxy Login Page - Windows Internet Explorer

http://www.ibns.lab/

Cisco Systems, Inc.

Username: employee1

Password: ●●●●●●●●

OK

Authentication Proxy Success Page - Win...

https://172.20.254.3/ Certificate Error

Cisco Systems, Inc.

Authentication Successful !

DONE

Since the Identity control policy on the port is configured for concurrent 802.1X and local web authentication methods, the switch would fail 802.1X when there is no valid response, and would open the port for web authentication in parallel.

```
*Sep 8 03:58:26.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/5, changed state to up
*Sep 8 03:58:39.815: %DOT1X-5-FAIL: Authentication failed for client
(000c.293d.75b2) on Interface Gi1/0/5 AuditSessionID AC14FE6500000FCC0301E908

switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x10534C0000000C7
      MAC Address:  000c.293d.75b2
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.100.7
        User-Name:  employee1
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FB40018077C
  Acct Session ID:  0x00000FAE
           Handle:  0x93000009
   Current Policy:  ENT-WEBAUTH-POL

Server Policies:
          ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd

Method status list:
  Method   State
  dot1x    Stopped
  webauth  Authc Success
```

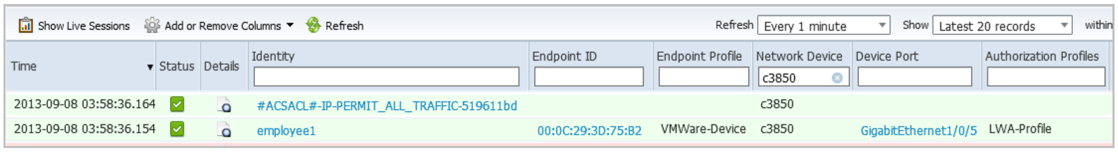
The IP Admission cache comes handy in cases of WebAuth failures. In a normal flow the ip admission cache would look like the following example below:

```
!*** Before Local Web Authentication ***
switch#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
  Client MAC 000c.293d.75b2 Client IP 0.0.0.0 IPv6 ::, State INIT, Method Webauth
```

```
!*** After Local Web Authentication ***
switch#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
  Client MAC 000c.293d.75b2 Client IP 172.20.100.7 IPv6 ::, State AUTHZ,
Method Webauth
```

The ISE live authentication can be referred to trace the authentication and authorization flow.

OPERATIONS → AUTHENTICATIONS



Refresh Every 1 minute
Show Latest 20 records

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles
						c3850		
2013-09-08 03:58:36.164	✓		#ACSACL#-IP-PERMIT_ALL_TRAFFIC-519611bd			c3850		
2013-09-08 03:58:36.154	✓		employee1	00:0C:29:3D:75:B2	VMWare-Device	c3850	GigabitEthernet1/0/5	LWA-Profile

When the same host that has a successful web authenticated session, goes through an 802.1X authentication, the end user's session on the switch is updated with newer attributes against the same session-id.

In legacy IOS, when a 802.1X authentication happens post successful local web authentication, a new auth-session is created on the port; destroying the previous one against the same MAC address.

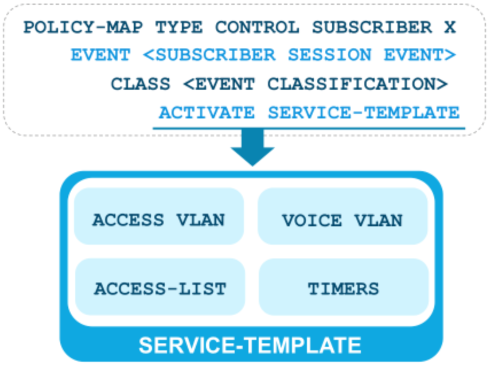
```
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x10534C0000000C7
      MAC Address:  000c.293d.75b2
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.200.4
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain   DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FB40018077C
  Acct Session ID:  0x00000FAF
           Handle:  0x93000009
   Current Policy:  ENT-WEBAUTH-POL

Server Policies:
         Template:  FinanceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd
```

```
Method status list:
  Method    State
  dot1x     Authc Success
  webauth   Stopped

switch#show ip admission cache
Authentication Proxy Cache
```

Service-Templates

A service template contains a set of service-related attributes or features, such as Access Control Lists (ACLs) and VLAN assignments, that can be activated on one or more subscriber sessions in response to session life-cycle events. Templates simplify the provisioning and maintenance of network session policies, where policies fall into distinct groups or are role-based.

Figure 9. Service Template


POLICY-MAP TYPE CONTROL SUBSCRIBER X
EVENT <SUBSCRIBER SESSION EVENT>
CLASS <EVENT CLASSIFICATION>
ACTIVATE SERVICE-TEMPLATE
ACCESS VLAN
VOICE VLAN
ACCESS-LIST
TIMERS
SERVICE-TEMPLATE

A service template is applied to sessions through its reference in a control policy, through RADIUS Change of Authorization (CoA) requests, or through a user profile or service profile. User profiles are defined per subscriber (user/device) and service profiles can apply to multiple subscribers.

Policy aware identity supports two types of service templates:

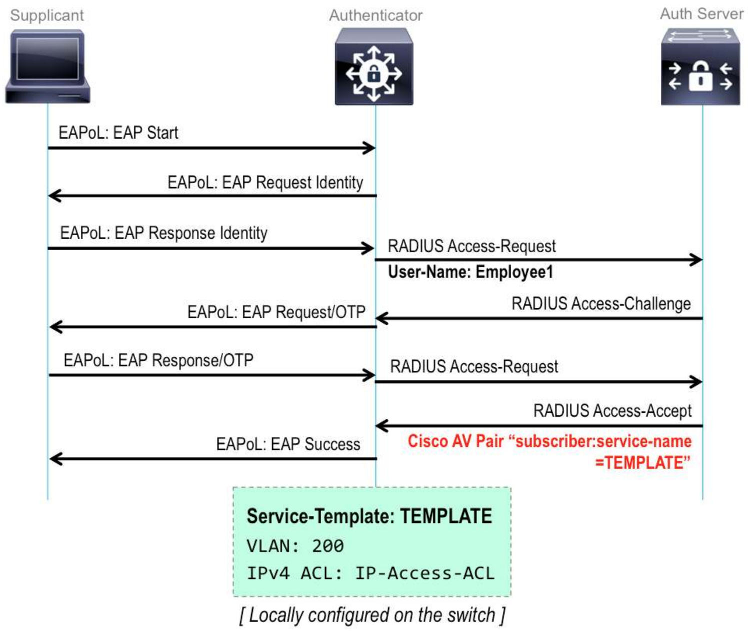
- Downloadable Service Templates—The service template is configured centrally on an external AAA server and downloaded on demand.
- Locally Configured Service Templates—The service template is configured locally on the device through the Cisco IOS Command-Line Interface (CLI).

Benefits of Service-templates:

- Service-templates offer role based authorizations
- A common authorization profile reference that contains various authorization attributes (VLAN, ACL, Filter-ID, Timer, etc.)
- Provisions for local authorizations
- Can be activated or deactivated on session events

Authorizing User Session with Local Service-template

Figure 10. Local Service Template Authorization

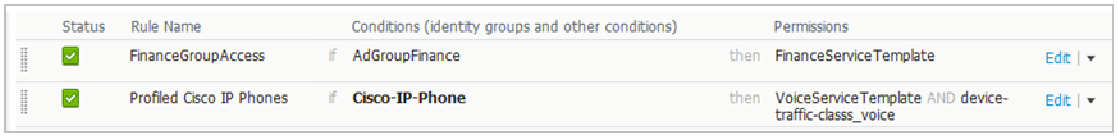


A service-template with local authorization attributes must be configured on the switch.

```
ip access-list extended Finance-ACL
 deny ip any host 172.20.254.4
 permit ip any any
!
service-template FinanceServiceTemplate
 access-group Finance-ACL
 vlan 200
!
service-template VoiceServiceTemplate
 voice vlan
 vlan 15
!
```

The authorization policy on the RADIUS server must be set to authorize the host with a service-template name. The service-template name on the switch and the authorization-profile on the server must match.

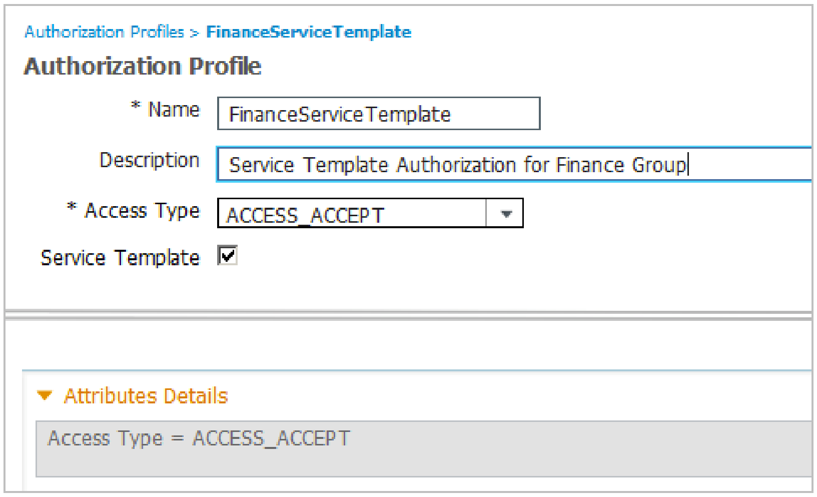
POLICY → AUTHORIZATION



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	FinanceGroupAccess	if	AdGroupFinance	then	FinanceServiceTemplate	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	VoiceServiceTemplate AND device-traffic-classs_voice	Edit | ▾

The Service Template option must be checked in ISE authorization profile.

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > FinanceServiceTemplate

Authorization Profile

* Name: FinanceServiceTemplate

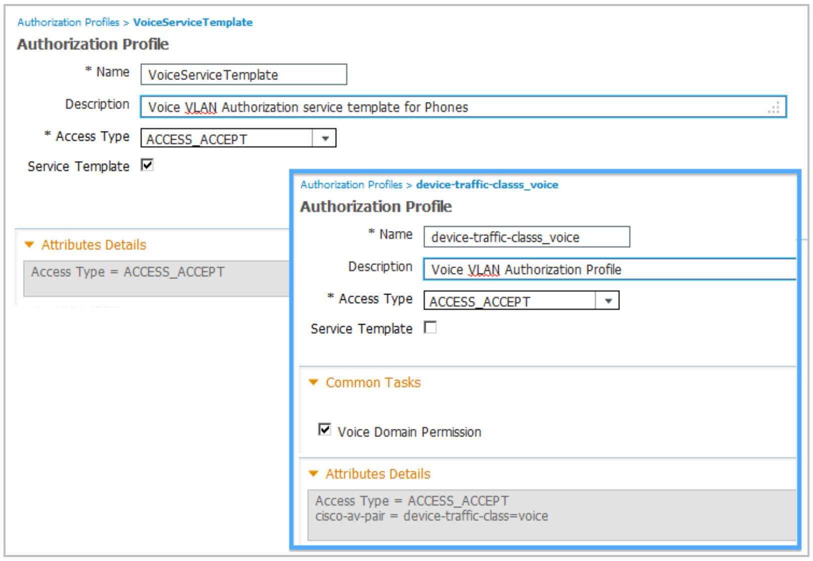
Description: Service Template Authorization for Finance Group

* Access Type: ACCESS_ACCEPT

Service Template: ☑

Attributes Details

Access Type = ACCESS_ACCEPT



Authorization Profiles > VoiceServiceTemplate

Authorization Profile

* Name: VoiceServiceTemplate

Description: Voice VLAN Authorization service template for Phones

* Access Type: ACCESS_ACCEPT

Service Template: ☑

Attributes Details

Access Type = ACCESS_ACCEPT

Authorization Profiles > device-traffic-classs_voice

Authorization Profile

* Name: device-traffic-classs_voice

Description: Voice VLAN Authorization Profile

* Access Type: ACCESS_ACCEPT

Service Template: □

Common Tasks

☑ Voice Domain Permission

Attributes Details

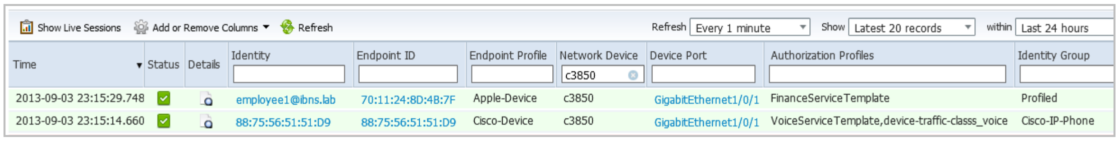
Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=voice

Upon authenticating successfully, the endpoints will be authorized with locally defined service-templates.

```
switch#show access-session interface gigabitEthernet 1/0/1 details
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x1031580000000DE
      MAC Address:  8875.5651.51d9
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.15.2
        User-Name:  88-75-56-51-51-D9
           Status:  Authorized
           Domain:  VOICE
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  050F142800000FC9007941F4
  Acct Session ID:  0x00000FD6
           Handle:  0xD800001E
   Current Policy:  ENT-IDENTITY-POL

Server Policies:
         Template:  VoiceServiceTemplate (priority 100)
       Voice Vlan:  10
 Vlan Group: Vlan:  15

Method status list:
  Method    State
  dot1x     Stopped
  mab       Authc Success
----------------------------------------
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x1046800000000DD
      MAC Address:  7011.248d.4b7f
     IPv6 Address:  2001:DB8:10:0:1089:9857:57BF:4330, FE80::C545:C384:22BC:4722,
2001:DB8:200:0:11CD:C2DD:8D4C:CAA5
     IPv4 Address:  172.20.200.3
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  050F142800000FC800793362
  Acct Session ID:  0x00000FD7
           Handle:  0xB400001D
   Current Policy:  ENT-IDENTITY-POL
Server Policies:
         Template:  FinanceServiceTemplate (priority 100)
        Filter-ID:  Finance-ACL
       Vlan Group:  Vlan: 200

Method status list:
  Method    State
  dot1x     Authc Success
  mab       Stopped
```

The ISE logs can be referred to, to see the authorization happening with service-templates.

OPERATIONS → AUTHENTICATIONS

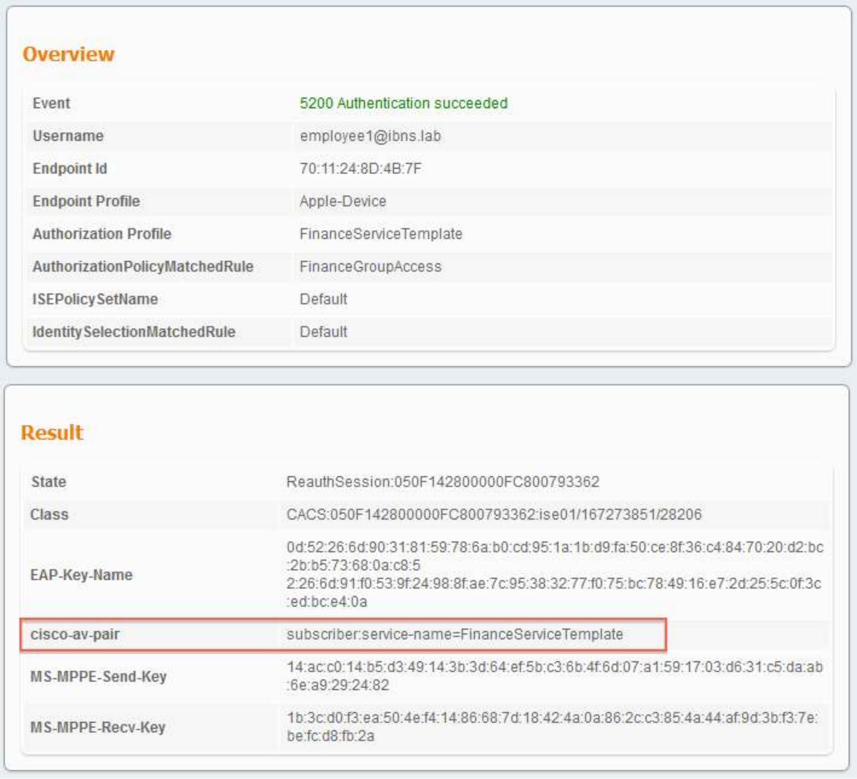


Refresh: Every 1 minute   Show: Latest 20 records   within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group
						c3850			
2013-09-03 23:15:29.748	✓		employee1@ibns.lab	70:11:24:8D:4B:7F	Apple-Device	c3850	GigabitEthernet1/0/1	FinanceServiceTemplate	Profiled
2013-09-03 23:15:14.660	✓		88:75:56:51:51:D9	88:75:56:51:51:D9	Cisco-Device	c3850	GigabitEthernet1/0/1	VoiceServiceTemplate,device-traffic-classs_voice	Cisco-IP-Phone

Clicking on the details icon at the ISE live authentications page, the detailed logs of the authentication and the authorization sequence can be read.

OPERATIONS → AUTHENTICATIONS (DETAILS)

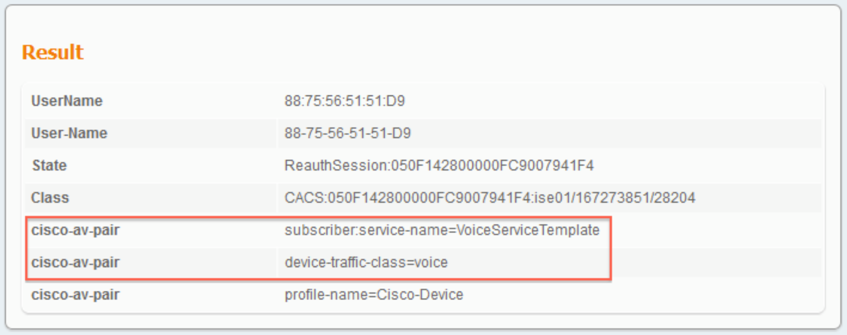


Overview

Event	5200 Authentication succeeded
Username	employee1@ibns.lab
Endpoint Id	70:11:24:8D:4B:7F
Endpoint Profile	Apple-Device
Authorization Profile	FinanceServiceTemplate
AuthorizationPolicyMatchedRule	FinanceGroupAccess
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Result

State	ReauthSession:050F142800000FC800793362
Class	CACS:050F142800000FC800793362:ise01/167273851/28206
EAP-Key-Name	0d:52:26:6d:90:31:81:59:78:6a:b0:cd:95:1a:1b:d9:fa:50:ce:8f:36:c4:84:70:20:d2:bc :2b:b5:73:68:0a:c8:5 2:26:6d:91:f0:53:9f:24:98:8f:ae:7c:95:38:32:77:f0:75:bc:78:49:16:e7:2d:25:5c:0f:3c :ed:bc:e4:0a
cisco-av-pair	subscriber:service-name=FinanceServiceTemplate
MS-MPPE-Send-Key	14:ac:c0:14:b5:d3:49:14:3b:3d:64:ef:5b:c3:6b:4f:6d:07:a1:59:17:03:d6:31:c5:da:ab :6e:a9:29:24:82
MS-MPPE-Recv-Key	1b:3c:d0:f3:ea:50:4e:f4:14:86:68:7d:18:42:4a:0a:86:2c:c3:85:4a:44:af:9d:3b:f3:7e: be:fc:d8:fb:2a



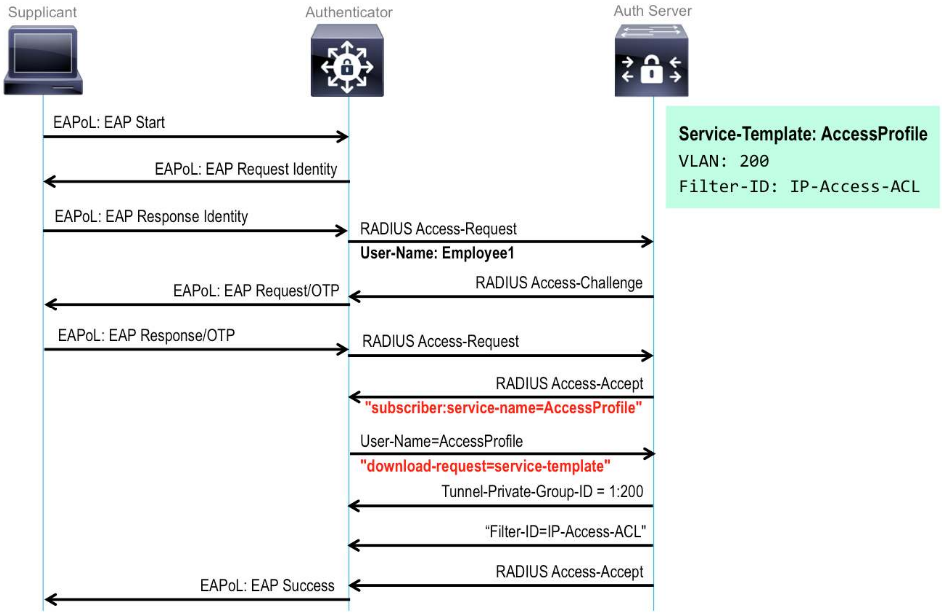
Result

UserName	88:75:56:51:51:D9
User-Name	88-75-56-51-51-D9
State	ReauthSession:050F142800000FC9007941F4
Class	CACS:050F142800000FC9007941F4:ise01/167273851/28204
cisco-av-pair	subscriber:service-name=VoiceServiceTemplate
cisco-av-pair	device-traffic-class=voice
cisco-av-pair	profile-name=Cisco-Device

Downloadable Service-templates

Similar to other authorization methods, such as ACLs or VLAN assignments, Service-templates can also be downloaded from the RADIUS servers. Downloadable service-templates function very similar to downloadable ACLs, in that the authorization flow is twofold: the initial authorization is the name of the authorization profile against an endpoint identity (device/user) and the second authorization is the specific authorizations (VLANs / ACLs) against the template name. The RADIUS server treats the service-template request as a user authentication with the service-template name as the identity.

Figure 11. Downloadable Service-template

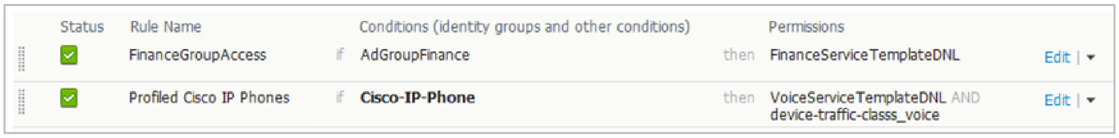


The configuration on the switch global and the interfaces doesn’t need to be modified for service-template authorizations.

```
interface GigabitEthernet1/0/1
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 10
  ip access-group IPV4-PRE-AUTH-ACL in
  access-session port-control auto
  mab
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber ENT-IDENTITY-POL
!
```

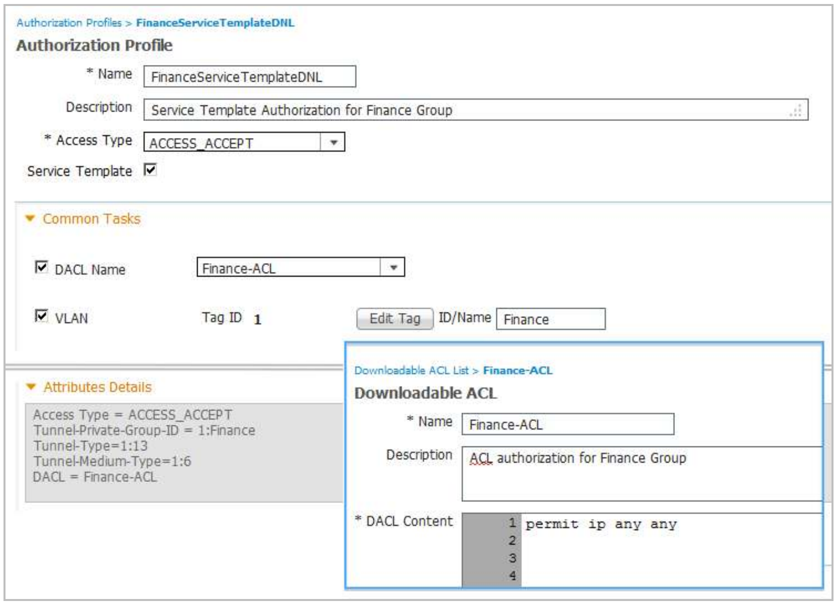
On the ISE however, the authorization profile and the authorization policy must be configured to onboard the endpoints with service-template based authorizations.

POLICY → AUTHORIZATION



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	FinanceGroupAccess	if	AdGroupFinance	then	FinanceServiceTemplateDNL	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	VoiceServiceTemplateDNL AND device-traffic-classs_voice	Edit | ▾

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > FinanceServiceTemplateDNL

Authorization Profile

* Name	FinanceServiceTemplateDNL
Description	Service Template Authorization for Finance Group
* Access Type	ACCESS_ACCEPT
Service Template	☑

Common Tasks

☑ DACL Name: Finance-ACL

☑ VLAN: Tag ID 1, ID/Name Finance

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:Finance
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = Finance-ACL
```

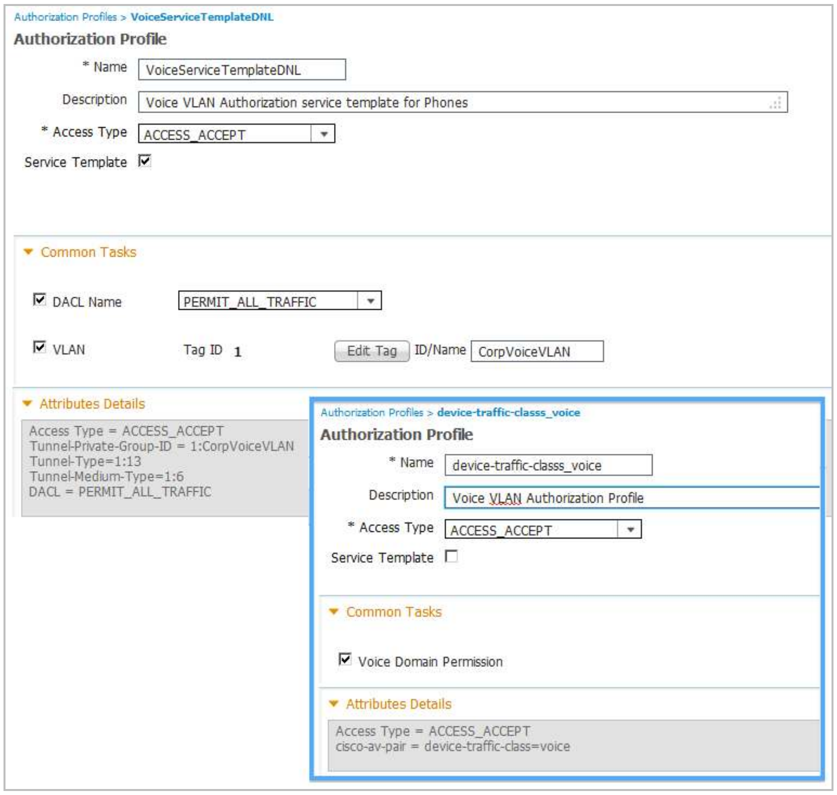
Downloadable ACL List > Finance-ACL

Downloadable ACL

* Name	Finance-ACL
Description	ACL authorization for Finance Group

* DACL Content

```
permit ip any any
```



Authorization Profiles > VoiceServiceTemplateDNL

Authorization Profile

* Name	VoiceServiceTemplateDNL
Description	Voice VLAN Authorization service template for Phones
* Access Type	ACCESS_ACCEPT
Service Template	☑

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☑ VLAN: Tag ID 1, ID/Name CorpVoiceVLAN

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:CorpVoiceVLAN
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = PERMIT_ALL_TRAFFIC
```

Authorization Profiles > device-traffic-classs_voice

Authorization Profile

* Name	device-traffic-classs_voice
Description	Voice VLAN Authorization Profile
* Access Type	ACCESS_ACCEPT
Service Template	□

Common Tasks

☑ Voice Domain Permission

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=voice
```

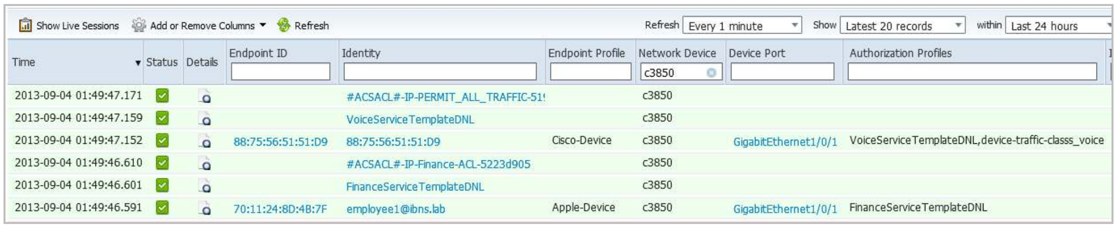
Upon successful authentication, the endpoints will be authorized with the service-template defined on the ISE.

```
switch#show access-session interface gigabitEthernet 1/0/1 details
          Interface:  GigabitEthernet1/0/1
             IIF-ID:  0x1044D80000000E1
        MAC Address:  7011.248d.4b7f
       IPv6 Address:  FE80::C545:C384:22BC:4722
       IPv4 Address:  172.20.200.3
```

```
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  050F142800000FCC0106B32C
  Acct Session ID:  0x00000FDE
           Handle:  0xAF000021
   Current Policy:  ENT-IDENTITY-POL
Server Policies:
         Template:  FinanceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-Finance-ACL-5223d905

Method status list:
  Method    State
  dot1x     Authc Success
  mab       Stopped
----------------------------------------
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x1092880000000E2
      MAC Address:  8875.5651.51d9
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.15.2
        User-Name:  88-75-56-51-51-D9
           Status:  Authorized
           Domain:  VOICE
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  050F142800000FCD0106BFA2
  Acct Session ID:  0x00000FDF
           Handle:  0xC5000022
   Current Policy:  ENT-IDENTITY-POL

Server Policies:
         Template:  VoiceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 15
          ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd
Method status list:
  Method    State
  dot1x     Running
  mab       Authc Success
```

The ISE live authentication may be referred for details on the authentication and authorization flow between the authentication-server and the supplicant.

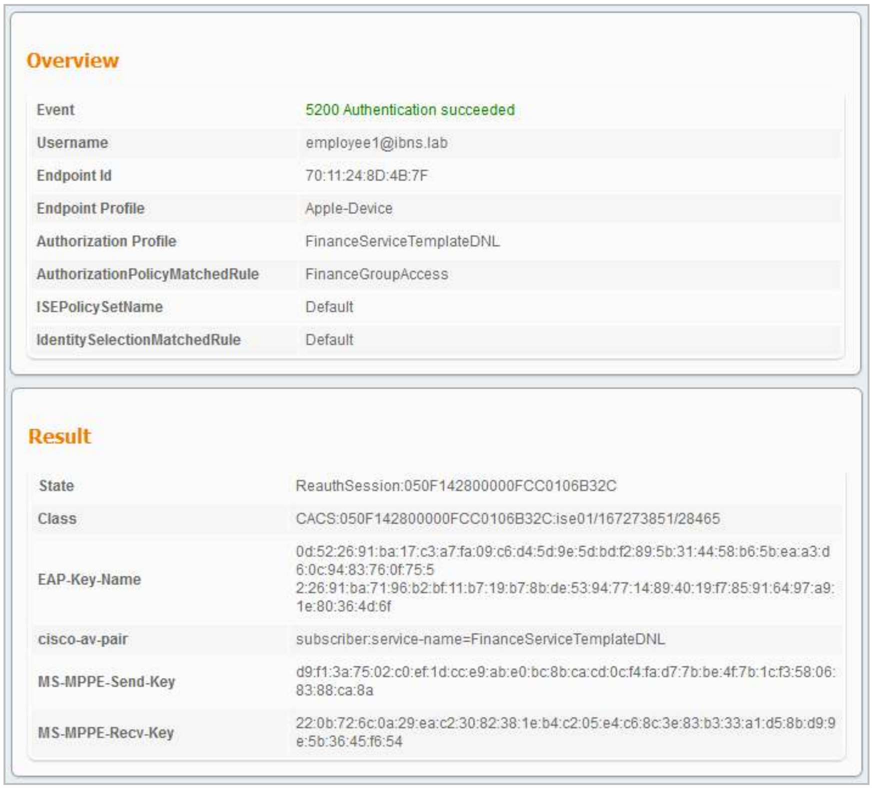
OPERATIONS → AUTHENTICATIONS



Time	Status	Details	Endpoint ID	Identity	Endpoint Profile	Network Device	Device Port	Authorization Profiles
						c3850		
2013-09-04 01:49:47.171	✓			#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51		c3850		
2013-09-04 01:49:47.159	✓			VoiceServiceTemplateDNL		c3850		
2013-09-04 01:49:47.152	✓		88:75:56:51:51:D9	88:75:56:51:51:D9	Cisco-Device	c3850	GigabitEthernet1/0/1	VoiceServiceTemplateDNL,device-traffic-classs_voice
2013-09-04 01:49:46.610	✓			#ACSACL#-IP-Finance-ACL-5223d905		c3850		
2013-09-04 01:49:46.601	✓			FinanceServiceTemplateDNL		c3850		
2013-09-04 01:49:46.591	✓		70:11:24:8D:4B:7F	employee1@ibns.lab	Apple-Device	c3850	GigabitEthernet1/0/1	FinanceServiceTemplateDNL

The ISE live authentication detailed logs would provide insight in to the authentication and authorization sequence.

OPERATIONS → AUTHENTICATIONS (DETAILS)

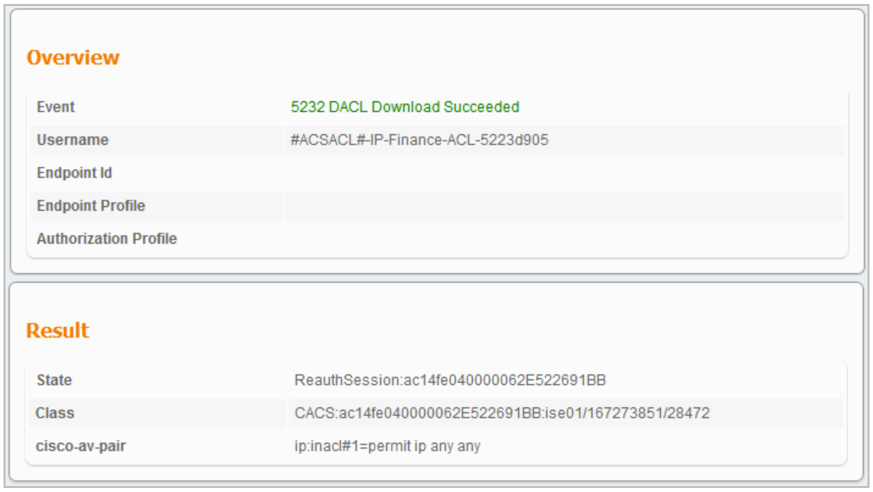


Overview

Event	5200 Authentication succeeded
Username	employee1@ibns.lab
Endpoint Id	70:11:24:8D:4B:7F
Endpoint Profile	Apple-Device
Authorization Profile	FinanceServiceTemplateDNL
AuthorizationPolicyMatchedRule	FinanceGroupAccess
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Result

State	ReauthSession:050F142800000FCC0106B32C
Class	CACS:050F142800000FCC0106B32C:ise01/167273851/28465
EAP-Key-Name	0d:52:26:91:ba:17:c3:a7:fa:09:c6:d4:5d:9e:5d:bd:f2:89:5b:31:44:58:b6:5b:ea:a3:d6:0c:94:83:76:0f:75:5 2:26:91:ba:71:96:b2:bf:11:b7:19:b7:8b:de:53:94:77:14:89:40:19:f7:85:91:64:97:a9:1e:80:36:4d:6f
cisco-av-pair	subscriber:service-name=FinanceServiceTemplateDNL
MS-MPPE-Send-Key	d9:f1:3a:75:02:c0:ef:1d:cc:e9:ab:e0:bc:8b:ca:cd:0c:f4:fa:d7:7b:be:4f:7b:1c:f3:58:06:83:88:ca:8a
MS-MPPE-Recv-Key	22:0b:72:6c:0a:29:ea:c2:30:82:38:1e:b4:c2:05:e4:c6:8c:3e:83:b3:33:a1:d5:8b:d9:9e:5b:36:45:f6:54

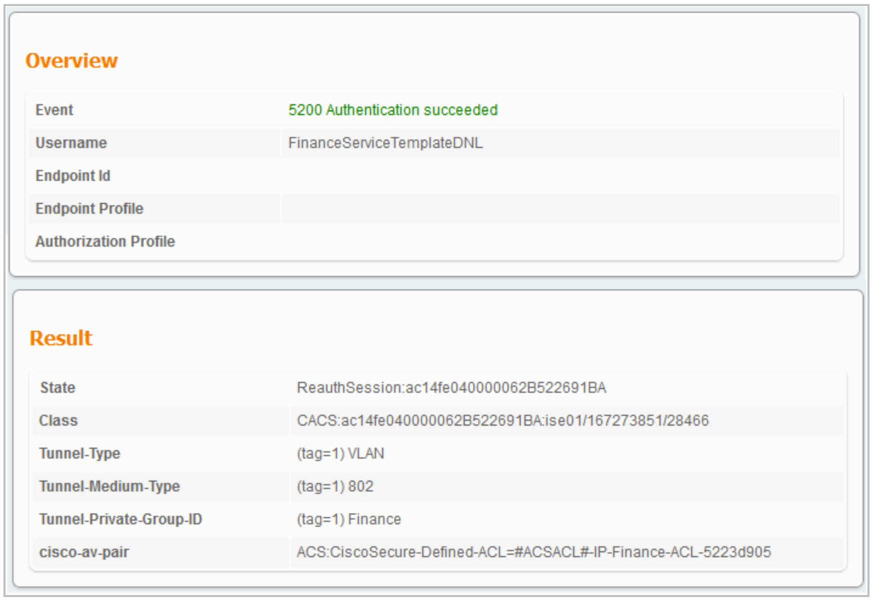


Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-Finance-ACL-5223d905
Endpoint Id	
Endpoint Profile	
Authorization Profile	

Result

State	ReauthSession:ac14fe040000062E522691BB
Class	CACS:ac14fe040000062E522691BB:ise01/167273851/28472
cisco-av-pair	ip:inacl#1=permit ip any any



Overview

Event	5200 Authentication succeeded
Username	FinanceServiceTemplateDNL
Endpoint Id	
Endpoint Profile	
Authorization Profile	

Result

State	ReauthSession:ac14fe040000062B522691BA
Class	CACS:ac14fe040000062B522691BA:ise01/167273851/28466
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) Finance
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-Finance-ACL-5223d905

Intelligent Aging

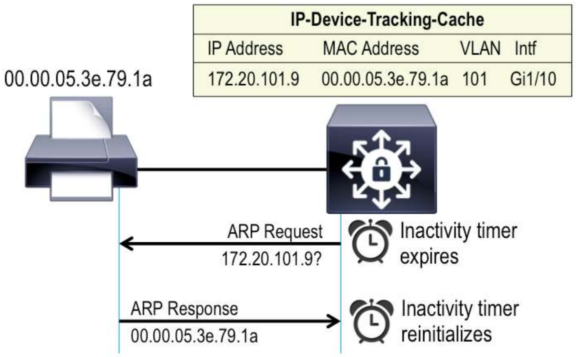
When the inactivity timer is enabled, the switch monitors the activity from authenticated endpoints. When the inactivity timer expires, the switch removes the authenticated session.

The inactivity timer for an access-session can be assigned in any of these three ways:

1. Configured on a per port basis using the "subscriber aging inactivity-timer" command
2. Define it under a service-template and activate it on a session event
3. Authorization from the RADIUS server [Idle-time-out (28), Terminate-Action (29)] along with the other attributes

The inactivity timer is an indirect mechanism the switch uses to infer that an endpoint has disconnected. An expired inactivity timer cannot guarantee that an endpoint has disconnected. Therefore, a quiet endpoint that does not send traffic for long periods of time, such as a network printer that services occasional requests but is otherwise silent, may have its session cleared, even though it is still connected. That endpoint must then send traffic before it can be authenticated again and have access to the network.

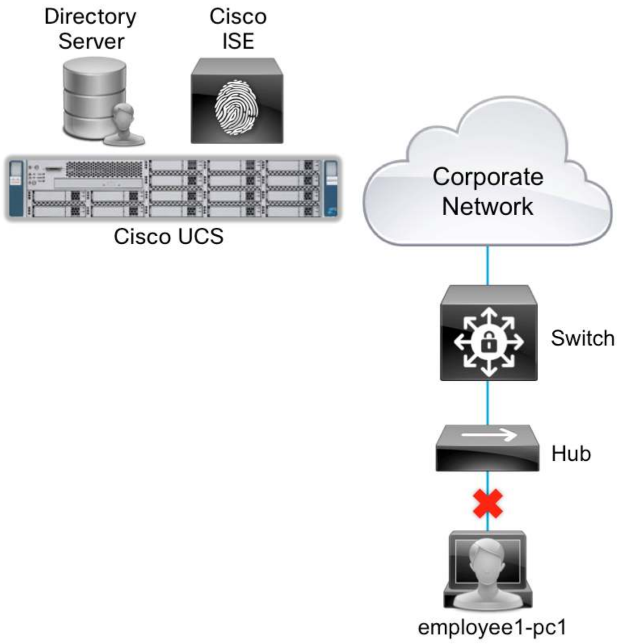
Figure 12. Intelligent Aging



IP-Device-Tracking-Cache			
IP Address	MAC Address	VLAN	Intf
172.20.101.9	00.00.05.3e.79.1a	101	Gi1/10

To counter these types of cases, an arp-probe can be enabled along with the inactivity-timer, so that the switch periodically sends ARP probes to endpoints in the IP Device Tracking table (which is initially populated by DHCP requests or ARP from the end point). As long as the endpoint is connected and responds to these probes, the inactivity timer is not triggered, and the endpoint is not inadvertently removed from the network.

Figure 13. Intelligent Aging Topology



Configuring the inactivity timer on a per-port basis:

A simple way to configure the inactivity timer is on per interface basis with the “subscriber aging inactivity-timer <1-65535> {probe}” command.

```
interface GigabitEthernet1/0/5
 description ** Access Port **
 subscriber aging inactivity-timer 30 probe
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 10
 ip access-group IPV4-PRE-AUTH-ACL in
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber ENT-IDENTITY-POL
!
```

When an access-session is setup on an interface, the timer value kicks in to monitor the session inactivity.

```
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x10236C0000000E1
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A, 2001:DB8:200:0:5C9C:B348:7CF:EE9B
     IPv4 Address:  172.20.200.4
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FCF01445222
  Acct Session ID:  0x00000FE1
           Handle:  0x31000024
   Current Policy:  ENT-IDENTITY-POL

Local Policies:
     Idle timeout:  30 sec
arp-probe-timeout:  yes

Server Policies:
         Template:  FinanceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-Finance-ACL-5223d905
Method status list:
 Method    State
 dot1x     Authc Success
```

```
  mab      Stopped
```

When the host disconnects indirectly from the port, the access-session terminates after the inactivity period.

```
switch#debug access-session events
Auth Manager events debugging is on
*Sep 1 07:39:51.390: AUTH-EVENT: Raising ext evt Inactivity Timeout (7) on
session 0x31000024, client iaf (5), hdl 0x00000000, attr_list 0x00000000
*Sep 1 07:39:51.391: AUTH-EVENT: Handling client event DELETE (17) for PRE,
handle 0x31000024
...

<output truncated>
switch#show access-session interface gigabitEthernet 1/0/5
No sessions match supplied criteria.

Runnable methods list:
  Handle  Priority  Name
  11      5         dot1x
  12      10        mab
  7       15        webauth
```

Defining The Inactivity Timer with Service-template

If it is required to monitor session activity across the switch access-ports, then the timer and probe can be defined under a service-template and be applied on the interfaces via an identity control policy.

```
service-template IA-TIMER
  inactivity-timer 60 probe
!
policy-map type control subscriber ENT-IDENTITY-POL
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using mab priority 20
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 60
    30 class always do-until-failure
      10 terminate dot1x
      20 terminate mab
      30 authentication-restart 60
  event agent-found match-all
    10 class always do-until-failure
      10 terminate mab
      20 authenticate using dot1x priority 10
  event authentication-success match-all
    10 class always do-until-failure
    10 activate service-template IA-TIMER
  event inactivity-timeout match-all
   10 class always do-until-failure
    10 unauthorize
```

Note: If the inactivity timer is configured both on the port and the service-template being applied on the port, then the time defined under the interface takes precedence (254).

```
interface GigabitEthernet1/0/5
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 10
  ip access-group IPV4-PRE-AUTH-ACL in
  access-session port-control auto
  mab
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber ENT-IDENTITY-POL
!
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x1066F00000000E2
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A, 2001:DB8:200:0:5C9C:B348:7CF:EE9B,
2001:DB8:200:0:7522:2AD2:B276:B2ED, 2001:DB8:200:0:C45B:AEF4:307F:8D7A
     IPv4 Address:  172.20.200.4
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FD001509DD4
  Acct Session ID:  0x00000FE3
           Handle:  0x92000025
   Current Policy:  ENT-IDENTITY-POL

Local Policies:
         Template:  IA-TIMER (priority 150)
     Idle timeout:  60 sec
arp-probe-timeout:  yes

Server Policies:
         Template:  FinanceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-Finance-ACL-5223d905
```

```
Method status list:
  Method    State
  dot1x     Authc Success
  mab       Stopped

switch#show debugging

Auth Manager:
  Auth Manager events debugging is on

*Sep 1 07:53:42.200: AUTH-EVENT: Raising ext evt Inactivity Timeout (7) on
session 0x92000025, client iaf (5), hdl 0x00000000, attr_list 0x00000000
*Sep 1 07:53:42.201: AUTH-EVENT: [000c.293d.75b2, Gi1/0/5] Handling external PRE
event Inactivity Timeout for context 0x92000025.
...
<output trunckated>

switch#show access-session interface gigabitEthernet 1/0/5
No sessions match supplied criteria.

Runnable methods list:
  Handle   Priority  Name
  11       5         dot1x
  12       10        mab
  7        15        webauth
```

Setting The Inactivity Timer on The RADIUS Server

The inactivity timer and terminate action can be set on the RADIUS server using the RADIUS attributes 28 (Idle-Timeout) and attribute 29 (Termination-Action). These attributes can be sent to the switch along with other authorization attributes.

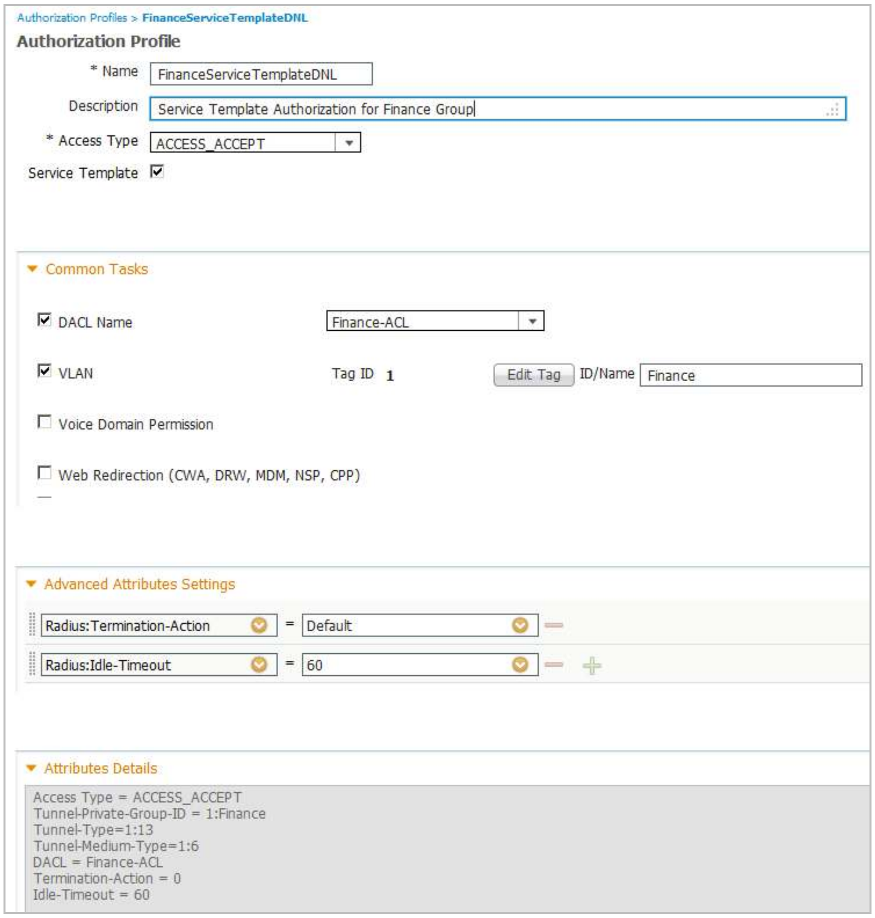
The identity control policy need not contain the inactivity timer configuration (on port or service-template) for this method to work.

```
policy-map type control subscriber ENT-IDENTITY-POL
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using mab priority 20
  event authentication-failure match-first
    10 class DOT1X_NO_RESP do-until-failure
      10 terminate dot1x
    20 class MAB_FAILED do-until-failure
      10 terminate mab
      20 authentication-restart 60
    30 class always do-until-failure
      10 terminate dot1x
      20 terminate mab
      30 authentication-restart 60
```

```
event agent-found match-all
  10 class always do-until-failure
    10 terminate mab
    20 authenticate using dot1x priority 10
```

On the ISE, under Authorization Profiles, configure two additional RADIUS attributes to handle the endpoint inactivity.

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > FinanceServiceTemplateDNL

Authorization Profile

* Name: FinanceServiceTemplateDNL

Description: Service Template Authorization for Finance Group

* Access Type: ACCESS_ACCEPT

Service Template ☑

Common Tasks

☑ DACL Name: Finance-ACL

☑ VLAN: Tag ID 1 | Edit Tag | ID/Name: Finance

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Advanced Attributes Settings

Radius:Termination-Action = Default

Radius:Idle-Timeout = 60

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:Finance
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = Finance-ACL
Termination-Action = 0
Idle-Timeout = 60
```

The “show access-session interface” command would show the aging time as defined on the RADIUS server.

```
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x10460C0000000E4
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A,
2001:DB8:200:0:C45B:AEF4:307F:8D7A, 2001:DB8:200:0:6197:9744:6852:9E6E
     IPv4 Address:  172.20.200.4
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FD2015F6F12
  Acct Session ID:  0x00000FE7
           Handle:  0x7F000027
   Current Policy:  ENT-IDENTITY-POL
Server Policies:
         Template:  FinanceServiceTemplateDNL (priority 100)
     Idle timeout:  60 sec
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-Finance-ACL-5223d905

Method status list:
  Method   State
  dot1x    Authc Success
  mab      Stopped
```

When the endpoint goes inactive, the access-session is terminated.

```
switch#show debugging

Auth Manager:
  Auth Manager events debugging is on

*Sep 1 08:06:12.001: AUTH-EVENT: [000c.293d.75b2, Gi1/0/5] Handling external PRE
event Inactivity Timeout for context 0x7F000027.
*Sep 1 08:06:12.001: AUTH-EVENT: [000c.293d.75b2, Gi1/0/5] Queued 0x7F000027 for
deletion
...
<output trunckated>

switch#show access-session interface gigabitEthernet 1/0/5
No sessions match supplied criteria.

Runnable methods list:
  Handle  Priority  Name
  11      5         dot1x
```

```
12        10         mab
7         15         webauth
```

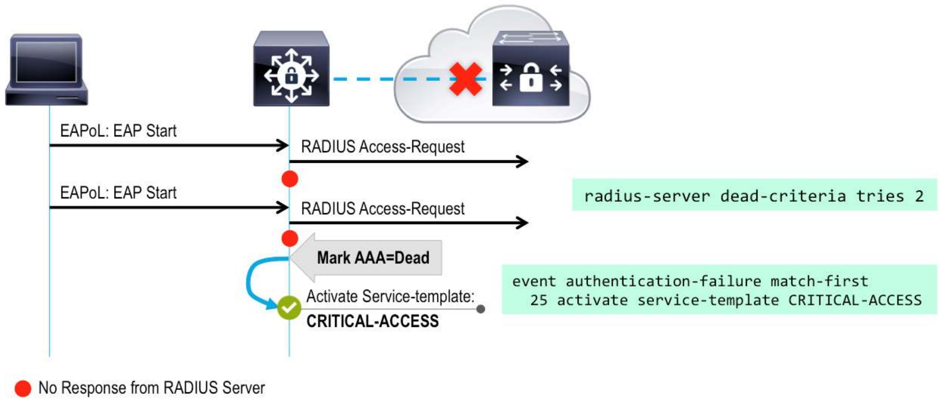
Critical ACL on AAA Failure

Connectivity to the policy server is fundamental for secure network access. The AAA/RADIUS server infrastructure could become unavailable due to various failures, or can be unreachable because of network connectivity issues. This could lead to a situation where the network authenticators (switches or Wireless Controllers) cannot authorize the end users. The Critical Auth-VLAN authorization is a remedy that on-boards the endpoints for limited access on to the network during a AAA server failure.

A common practice for port authentication is to authorize the user with VLAN and an ACL enforcement. This type of access permission allows for both network segmentation and access control at the enterprise edge. The ACL authorization infrastructure however mandates for a pre-auth-acl to be applied on the port prior to an access session. This check mates the critical authorization scenario, where the end users can be put to an critical VLAN, but the port ACL would block the end user’s traffic at the ingress of the access network. There is a need to have a comprehensive solution, that not only authorizes the end users with appropriate VLAN assignment when the AAA infrastructure fails, but also authorizes the critical session with an ACL enforcement, thereby unblocking the port for limited access.

The service-template and the identity control policy offers options to cater to such requirements. It is now known that a service-template can contain ip access-control-list and VLAN definitions that can be activated during session events. Let’s explore further on how to leverage this flexibility in addressing one of the common deployment needs that most enterprise networks have today.

Figure 14. Critical ACL



```
radius-server dead-criteria tries 2
```

```
event authentication-failure match-first
  25 activate service-template CRITICAL-ACCESS
```

A typical policy to address the critical authentication requirement must satisfy three requirements:

1. The system must be configured for AAA server status determination (DEAD/ALIVE).
4. Critical authorization options must be configured for activation during AAA server failure.
5. On a AAA server connectivity resumption, the system flow for reinitializing the critical-auth sessions must be setup.

The following global commands sets the system to mark the RADIUS server dead on two failed communication attempts, and keeps the Dead status for three minutes, before the system marks the server as “Up” and attempts to communicate with it.

```
radius-server dead-criteria tries 2
radius-server deadtime 3
!
```

A service-template referencing an IP ACL has to be configured for use with in an Identity control policy to activate during a AAA failure.

```
ip access-list extended ACL-CRITICAL-V4
 deny tcp any host 172.20.254.4
! deny access to some protected resources during the critical condition
 permit ip any any
!
service-template CRITICAL-ACCESS
 description *Fallback Policy on AAA Fail*
 access-group ACL-CRITICAL-V4
!
service-template CRITICAL_AUTH_VLAN
 vlan 100
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
!
```

Configure an Identity control policy to activate a local service-template on an authentication failure event, matching AAA server failure event-classification.

```
policy-map type control subscriber ENT-IDENTITY-POL
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using mab priority 20
 event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   25 activate service-template CRITICAL-ACCESS
   30 authorize
   40 pause reauthentication
  20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  30 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
  40 class MAB_FAILED do-until-failure
   10 terminate mab
   20 authentication-restart 60
  50 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  60 class always do-until-failure
   10 terminate dot1x
   20 terminate mab
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
  20 authenticate using dot1x priority 10
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template IA-TIMER
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 unauthorize
!
```

Tip: The best way to create an Identity control policy catering to the critical-auth requirement is to leverage the migration tool (authentication display Exec command). Have all the “authentication event server” commands in the legacy mode and then covert them to the new-style. The system generates a descriptive policy, that can be modified for critical ACL flow.

If an identity control policy is created based on the conversion the migration command does, then most of the class-maps will be system-generated.

```
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match result-type aaa-timeout
 match authorization-status authorized
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
```

```
  match result-type method dot1x authoritative
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
  match activated-service-template CRITICAL_AUTH_VLAN
  match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
  match activated-service-template CRITICAL_AUTH_VLAN
  match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!

interface GigabitEthernet1/0/1
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  switchport voice vlan 10
  ip access-group IPV4-PRE-AUTH-ACL in
  shutdown
  access-session port-control auto
  mab
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber ENT-IDENTITY-POL
!
```

When the endpoints try to onboard the network during the time that the AAA server is down, the critical authentication activates, authorizing the critical-ACL, remediating the pre-auth-acl port block issue.

```
switch#show aaa servers
RADIUS: id 1, priority 1, host 172.20.254.4, auth-port 1812, acct-port 1813
  State: current DEAD, duration 191s, previous duration 5224s
<output truncated>

switch#show access-session interface gigabitEthernet 1/0/1

Interface  MAC Address    Method  Domain   Status   Fg Session ID
-----------------------------------------------------------------------------
Gi1/0/1    7011.248d.4b7e dot1x   UNKNOWN  Auth     AC14FE6500000FB300625CE6
Gi1/0/1    8875.5651.51d9 mab     UNKNOWN  Auth     AC14FE6500000FB400627172
<output truncated>
```

IP Telephony and Critical ACL: When the AAA server does not respond, the port goes into critical authentication mode. When traffic coming from the host is tagged with the voice VLAN, the connected device (the phone) is put in the configured voice VLAN for the port. The IP phones learn the voice VLAN identification through CDP (for Cisco devices) or through LLDP or DHCP. The critical ACL that is applied on the port will be subjected to both DATA and VOICE access. The critical ACL must ensure that the phone has access to the voice infrastructure.

```
switch#show access-session interface gigabitEthernet 1/0/1 details
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x1012900000000C5
```

```
      MAC Address:  7011.248d.4b7e
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.100.11
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  UNKNOWN
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FB300625CE6
  Acct Session ID:  0x00000FB3
           Handle:  0x7D000008
   Current Policy:  ENT-IDENTITY-POL

Local Policies:
         Template:  CRITICAL_AUTH_VLAN (priority 150)
       Vlan Group:  Vlan: 100
         Template:  DEFAULT_CRITICAL_VOICE_TEMPLATE (priority 150)
       Voice Vlan:  10
         Template:  CRITICAL-ACCESS (priority 150)
        Filter-ID:  ACL-CRITICAL-V4

Method status list:
  Method    State
  dot1x     Authc Failed
  mab       Stopped
----------------------------------------
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x10936C0000000C6
      MAC Address:  8875.5651.51d9
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.10.2
        User-Name:  8875565151d9
           Status:  Authorized
           Domain:  UNKNOWN
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FB400627172
  Acct Session ID:  0x00000FB4
           Handle:  0x12000009
   Current Policy:  ENT-IDENTITY-POL
Local Policies:
         Template:  CRITICAL_AUTH_VLAN (priority 150)
       Vlan Group:  Vlan: 100
         Template:  DEFAULT_CRITICAL_VOICE_TEMPLATE (priority 150)
       Voice Vlan:  10
```

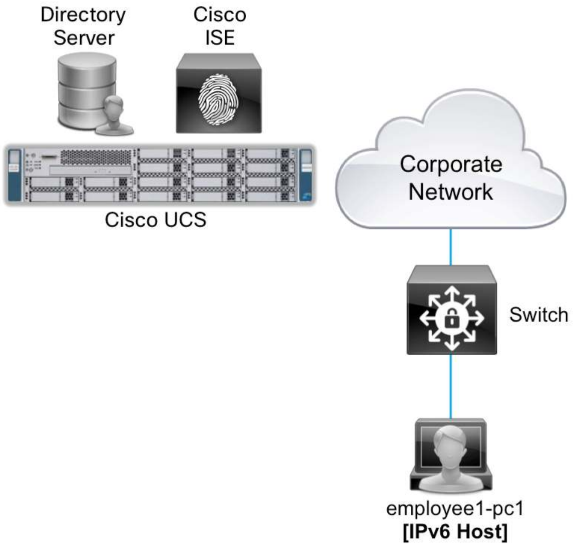
```
           Template:  CRITICAL-ACCESS (priority 150)
          Filter-ID:  ACL-CRITICAL-V4

  Method status list:
    Method    State
    dot1x     Running
    mab       Authc Failed
```

IPv6 Identity

Authenticating IPv6 endpoints and authorizing them to VLAN assignments in closed-mode is possible with current IOS software(s). Policy aware IBNS extends this capability to perform ACL based authorizations (in low-impact mode) and web authentications. Apart from that, the critical ACL for IPv6 access can be configured to be consistent with IPv4 configurations. The IOS provisions for defining an IPv6 only RADIUS server. Even with Cisco ISE, which as of today doesn't support IPv6, has a lot of functionalities that can still be run using the local service-template activations. This section focuses on IPv6 identity deployments with service-template authorizations.

Low Impact Mode in an IPv6 Network

Figure 15. IPv6 Identity topology



To setup low-impact mode (authorizing endpoints with pre-auth and post-auth ACLs) for IPv6 hosts, the following three items are necessary:

1. An IPv6 Pre-Auth ACL on the access port
2. An IPv6 Post-Auth ACL for authorizing successful access sessions
3. Appropriate RADIUS server configurations

Since Cisco ISE doesn't support IPv6 capabilities today, local Service-templates for this requirement can be leveraged.

Note: Service-template authorization with IPv6 ACLs is currently supported on the Catalyst 3850 and 3650 only.

A IPv6 Pre-Auth ACL, that allows for only DHCP and DNS protocols and blocks everything else, has to be configured for hosts access before a successful authentication takes place on the network.

```
ipv6 access-list IPV6-PRE-AUTH-ACL
  remark Allow DHCP
  permit udp any eq bootpc any eq bootps
  remark Allow DNS
  permit udp any any eq domain
  remark Deny all else
  deny ipv6 any any
!
ip access-list extended IPV4-PRE-AUTH-ACL
  remark Allow DHCP
  permit udp any eq bootpc any eq bootps
  remark Allow DNS
  permit udp any any eq domain
  remark Deny all else
  deny ip any any
```

A local service-template that contains a VLAN number and a IPv4 and IPv6 access-control-list can be configured for authorizing authenticated clients.

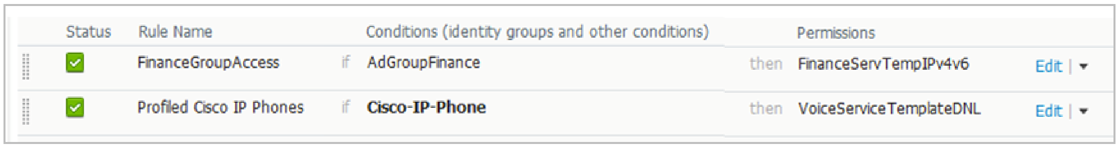
```
ipv6 access-list ACCESS_IPV6
  permit ipv6 any any
!
ip access-list extended ACCESS_IPV4
  permit ip any any
!
service-template FinanceServTempIPv4v6
  access-group ACCESS_IPV4
  access-group ACCESS_IPV6
  vlan 200
!
```

The following commands are essential for IPv6 context in identity. These commands perform the equivalent of DHCP snooping and IP device tracking features for IPv6.

```
vlan configuration 15-250
  ipv6 nd suppress
  ipv6 snooping
!
ipv6 snooping policy snoop-v6
  trusted-port
!
interface GigabitEthernet1/0/24
  description ** Uplink Port to Dist Switch **
  switchport trunk allowed vlan 10,15,100,150,151,200,254
  switchport mode trunk
  ipv6 snooping attach-policy snoop-v6
  ip dhcp snooping trust
!
ipv6 neighbor tracking
ipv6 neighbor binding
!
```

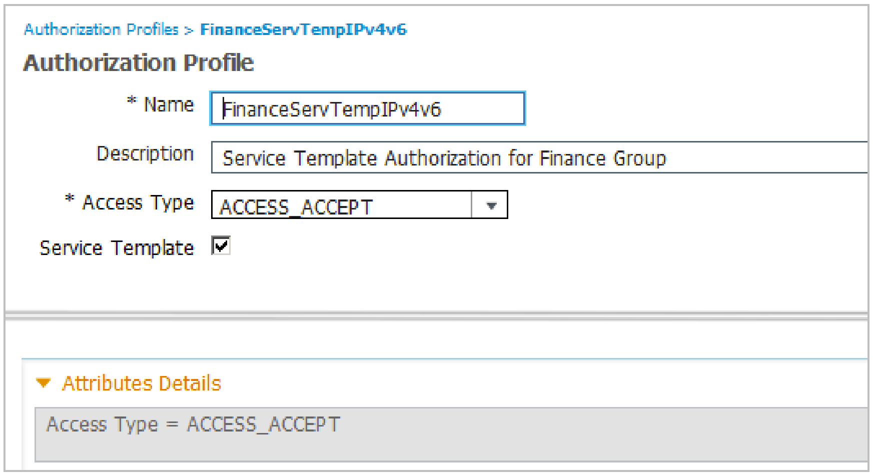
On the ISE, configure the Authorization profile to push down a service-template name with ACCESS-ACCEPT for a successful network authentication.

POLICY → AUTHORIZATION



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	FinanceGroupAccess	if	AdGroupFinance	then	FinanceServTempIPv4v6	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	VoiceServiceTemplateDNL	Edit | ▾

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > **FinanceServTempIPv4v6**

Authorization Profile

* Name	FinanceServTempIPv4v6
Description	Service Template Authorization for Finance Group
* Access Type	ACCESS_ACCEPT ▾
Service Template	☑

▾ Attributes Details

Access Type = ACCESS_ACCEPT

The service-template “FinanceServTempIPv4v6” on the switch gets activated when the end user’s session goes through a successful network authentication.

```
switch#show access-session interface gigabitEthernet 1/0/5 details
```

```
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x100BF80000000D6
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A,
2001:DB8:200:0:BDAE:84F3:C2B3:E5F7, 2001:DB8:200:0:2931:E6C3:E417:1912,
2001:DB8:200:0:28D8:1903:965:95D7
     IPv4 Address:  172.20.200.4
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FC4007E7CE6
  Acct Session ID:  0x00000FCB
           Handle:  0xD6000019
   Current Policy:  ENT-IDENTITY-POL

Local Policies:
         Template:  IA-TIMER (priority 150)
     Idle timeout:  60 sec
arp-probe-timeout:  yes

Server Policies:
         Template:  FinanceServTempIPv4v6 (priority 100)
        Filter-ID:  ACCESS_IPV6
        Filter-ID:  ACCESS_IPV4
       Vlan Group:  Vlan: 200

Method status list:
  Method   State
  dot1x    Authc Success
  mab      Stopped
```

The identity control policy doesn't require any changes to address the IPv6 ACL based authorizations, however if parity for critical access (authorization when the AAA server is down) needs to be maintained, make minute changes to the policy and service-template(s).

```
policy-map type control subscriber ENT-IDENTITY-POL
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using mab priority 20
  event authentication-failure match-first
    10 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
      10 activate service-template CRITICAL_AUTH_VLAN
      20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
      25 activate service-template CRITICAL-ACCESS
      30 authorize
```

```
   40 pause reauthentication
 20 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
  10 pause reauthentication
  20 authorize
 30 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authentication-restart 60
 40 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 50 class DOT1X_FAILED do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 60 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 10
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template IA-TIMER
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 unauthorize
!

ip access-list extended ACL-CRITICAL-V4
 deny tcp any host 172.20.254.4
 permit ip any any
!
ipv6 access-list ACL-CRITICAL-V6
 deny ipv6 any host 2001:DB8:254::4
 permit ipv6 any any
!
service-template CRITICAL-ACCESS
 description *Fallback Policy on AAA Fail*
 access-group ACL-CRITICAL-V4
 access-group ACL-CRITICAL-V6
!
```

When an IPv6 client tries to on-board the network while the AAA server is down, then the local service-template CRITICAL-ACCESS activates authorizing limited access until the server becomes reachable again.

```
*Sep 2 01:46:07.891: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.254.4:1812,1813
is not responding.
*Sep 2 01:46:28.071: %RADIUS-3-ALLDEADSERVER: Group radius: No active radius
servers found. Id 203.
switch#show aaa servers
RADIUS: id 1, priority 1, host 172.20.254.4, auth-port 1812, acct-port 1813
  State: current DEAD, duration 65s, previous duration 8615s
...
<output truncated>

switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x106D940000000D7
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A, 2001:DB8:200:0:28D8:1903:965:95D7,
2001:DB8:100:0:C45B:AEF4:307F:8D7A, 2001:DB8:100:0:B9EB:34CB:214D:6C29
     IPv4 Address:  172.20.100.3
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  UNKNOWN
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FC50088195E
  Acct Session ID:  0x00000FCD
           Handle:  0x0600001A
   Current Policy:  ENT-IDENTITY-POL

Local Policies:
         Template:  CRITICAL_AUTH_VLAN (priority 150)
       Vlan Group:  Vlan: 100
         Template:  DEFAULT_CRITICAL_VOICE_TEMPLATE (priority 150)
       Voice Vlan:  10
         Template:   CRITICAL-ACCESS (priority 150)
        Filter-ID:  ACL-CRITICAL-V6
        Filter-ID:  ACL-CRITICAL-V4
Method status list:
  Method    State
  dot1x     Authc Failed
  mab       Stopped
```

Web Authentication in an IPv6 Network

The policy aware IBNS framework extends the web authentication capability to IPv6 clients. To facilitate consistency between the IPv4 and IPv6 web authentication, the following options are available on the switch:

1. Common configuration for IPv4 and IPv6 RADIUS servers

2. Use of parameter-map for the web authentication profile
3. Use of IPv6 redirect URLs for central web authentication

Though the system supports defining a RADIUS server with an IPv6 address, due to limitations with the Cisco ISE, this document covers configurations with the current set of capabilities on the ISE and Cisco IOS device.

The switch can authenticate IPv6 endpoints while interfacing with the RADIUS server on an IPv4 address.

```
radius server ise
 address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
 automate-tester username probe-user
 key cisco
!
```

Note: Since the Cisco ISE does not support IPv6 today, the RADIUS server configuration on the switch is setup for IPv4 in this guide. However, if a RADIUS server in use allows to configure: (1) an IPv6 address on one of its interfaces and (2) a pre-shared key for secure RADIUS communications over IPv6, then “address ipv6” under the “radius server” command on the switch can be used to define the IPv6 RADIUS server.

To control access prior to authentication, an IPv6 pre-auth-acl is necessary to be configured on the system allowing for DHCP and DNS traffic only.

```
ipv6 access-list IPV6-PRE-AUTH-ACL
 remark Allow DHCP
 permit udp any eq bootpc any eq bootps
 remark Allow DNS
 permit udp any any eq domain
 remark Deny all else
 deny ipv6 any any
!
```

The identity control policy for both IPv4 and IPv6 local web authentication is similar.

```
policy-map type control subscriber ENT-WEBAUTH-POL
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
   20 authenticate using webauth aaa authc-list WebAuth parameter-map LWA-PROFILE priority 30
 event authentication-failure match-first
  10 class DOT1X_NO_RESP do-until-failure
   10 terminate dot1x
  20 class always do-until-failure
   10 terminate dot1x
   20 terminate webauth
   30 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 terminate webauth
   30 authenticate using dot1x priority 10
```

```
!
parameter-map type webauth LWA-PROFILE
   timeout init-state sec 60
   max-http-conns 2
   banner text ^C Cisco Systems, Inc. ^C
!
```

Client facing interface configuration is very similar to IPv4 access in that an IPv6 Pre Auth ACL has to be applied for limited access prior to authentication(s).

```
interface GigabitEthernet1/0/5
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  access-session port-control auto
  ipv6 traffic-filter IPV6-PRE-AUTH-ACL in
  dot1x pae authenticator
  spanning-tree portfast
  service-policy type control subscriber ENT-WEBAUTH-POL
!
```

For the Access session manager to be IPv6 aware, IPv6 snooping and device tracking must be configured with the following commands.

```
vlan configuration 15-250
  ipv6 nd suppress
  ipv6 snooping
!
ipv6 snooping policy snoop-v6
  trusted-port
!
interface GigabitEthernet1/0/24
  description ** Uplink Port to Dist Switch **
  switchport trunk allowed vlan 10,15,100,150,151,200,254
  switchport mode trunk
  ipv6 snooping attach-policy snoop-v6
  ip dhcp snooping trust
!
ipv6 neighbor tracking
ipv6 neighbor binding
!
```

Details on IPv6 device tracking can be found here: http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6-dev-track.pdf.

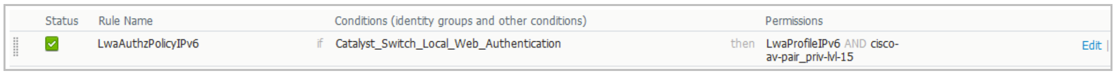
To permit the IPv6 clients for authorized resources, a local authorization profile in terms of a service-template, can be leveraged.

```
ipv6 access-list PERMIT-ANY-V6
  permit ipv6 any any
!
```

```
service-template LwaProfileIPv6
  access-group PERMIT-ANY-V6
!
```

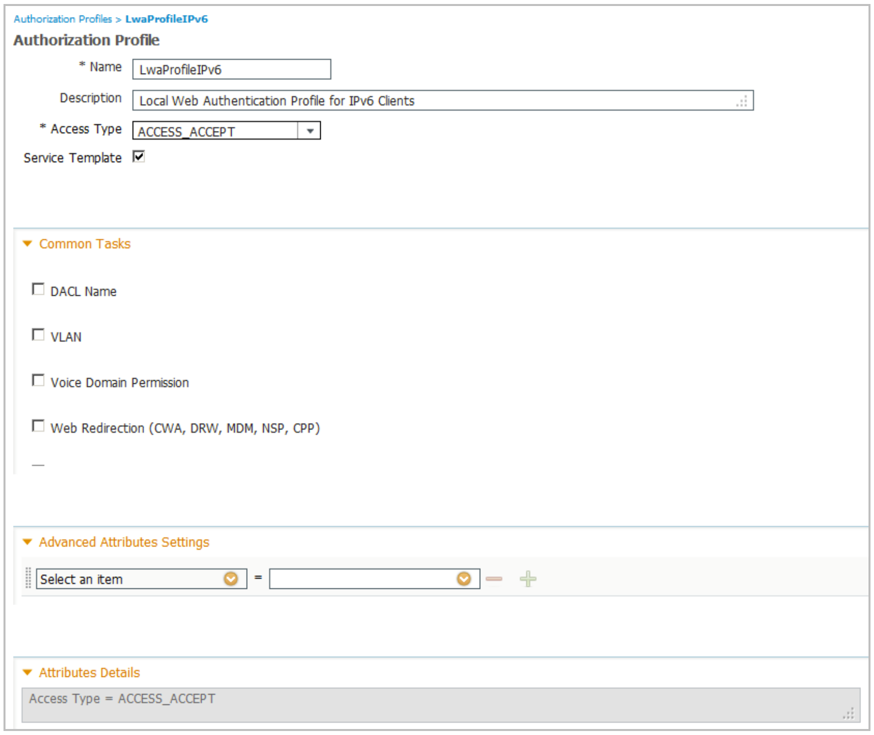
The ISE authorization policy must be configured for condition matching on local web authentication attempt and permissions granting a reference to the local service-template and importantly RADIUS Cisco AV Pair Privlvl=15

OPERATIONS → AUTHENTICATIONS



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	LwaAuthzPolicyIPv6	if	Catalyst_Switch_Local_Web_Authentication	then	LwaProfileIPv6 AND cisco-av-pair_priv-lvl-15	Edit

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > **LwaProfileIPv6**

Authorization Profile

* Name: LwaProfileIPv6

Description: Local Web Authentication Profile for IPv6 Clients

* Access Type: ACCESS_ACCEPT

Service Template ☑

Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

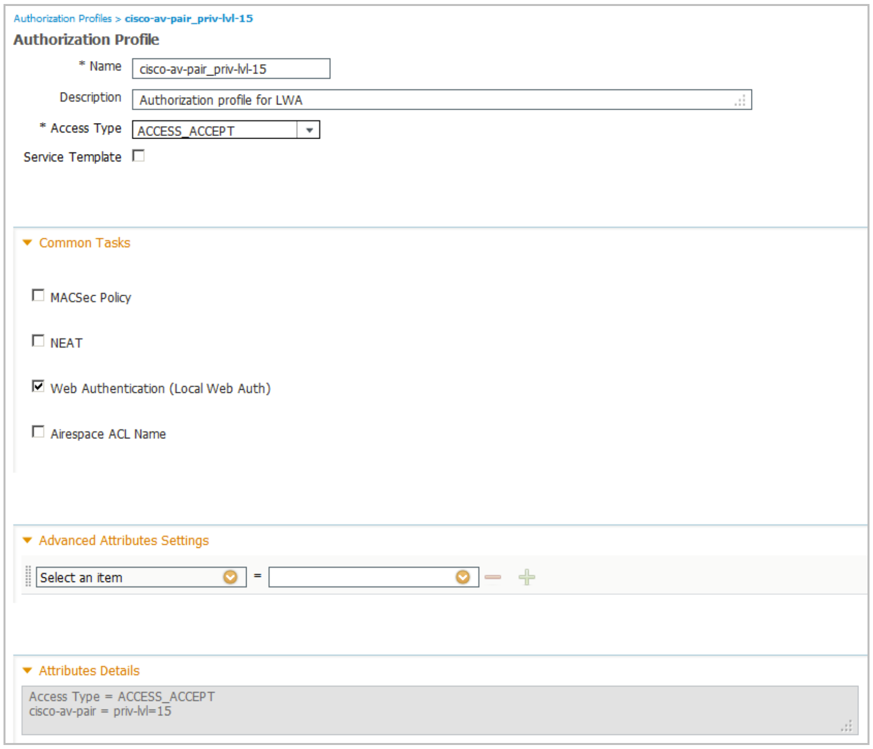
□ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT



Authorization Profiles > cisco-av-pair_priv-lvl-15

Authorization Profile

* Name: cisco-av-pair_priv-lvl-15

Description: Authorization profile for LWA

* Access Type: ACCESS_ACCEPT

Service Template: □

Common Tasks

□ MACSec Policy

□ NEAT

☑ Web Authentication (Local Web Auth)

□ Airespace ACL Name

Advanced Attributes Settings

Select an item =

Attributes Details

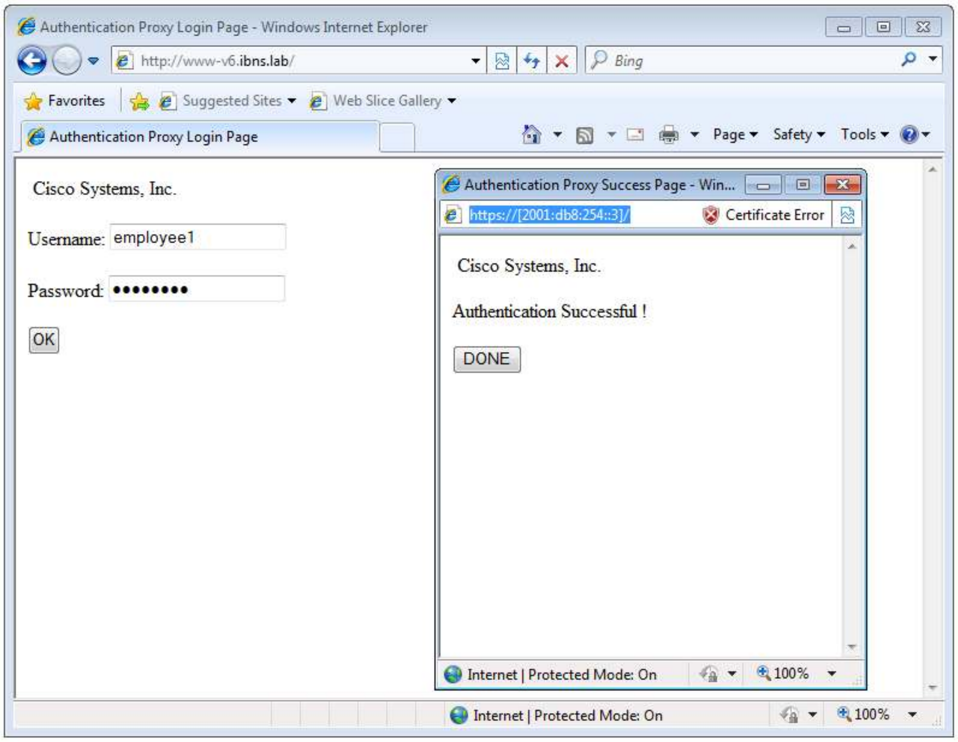
Access Type = ACCESS_ACCEPT
cisco-av-pair = priv-lvl=15

Upon successful authentication, the IPv6 clients will be authorized with the local service-template for access.

```
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x10241400000014F
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A,
2001:DB8:100:0:CC62:7933:DA8E:232A, 2001:DB8:100:0:C45B:AEF4:307F:8D7A
     IPv4 Address:  Unknown
        User-Name:  employee1
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FC4062D37B8
  Acct Session ID:  0x00000FC4
           Handle:  0x5E00000C
Current Policy: ENT-WEBAUTH-POL

Server Policies:
         Template:  LwaProfileIPv6 (priority 100)
        Filter-ID:  PERMIT-ANY-V6
```

```
Method status list:
  Method     State
  dot1x      Stopped
  webauth    Authc Success
```

The users must open the browser on the host and type in a url that can be DNS resolved. Upon doing so, the switch will redirect to the web authentication page, where the end user can type in his credentials and gain authorized access.



Authentication Proxy Login Page - Windows Internet Explorer
http://www-v6.ibns.lab/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Authentication Proxy Login Page
Page
Safety
Tools
Authentication Proxy Success Page - Win...
https://[2001:db8:254::3]/
Certificate Error
Internet | Protected Mode: On
100%
Internet | Protected Mode: On
100%

Cisco Systems, Inc.

Username: employee1

Password: ••••••••

OK

Cisco Systems, Inc.

Authentication Successful !

DONE

IPv6 device tracking is essential for local web authentication to work. It is possible to glance through the device tracking table with the following command:

```
switch#show ipv6 neighbors binding interface gigabitEthernet 1/0/5
portDB has 3 entries for interface Gi1/0/5, 3 dynamic
Codes: L—Local, S—Static, ND—Neighbor Discovery, DH—DHCP, PKT—Other Packet, API—
API created
Preflevel flags (prlvl):
0001:MAC and LLA match   0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk  0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated   0080:Cert authenticated    0100:Statically assigned

IPv6 address                          Link-Layer addr  Interface vlan prlvl  age
state      Time left
ND FE80::C45B:AEF4:307F:8D7A          000C.293D.75B2   Gi1/0/5   100  0005   3mn
REACHABLE  111 s try 0
ND 2001:DB8:100:0:CC62:7933:DA8E:232A 000C.293D.75B2   Gi1/0/5   100  0005   173s
REACHABLE  138 s try 0
ND 2001:DB8:100:0:C45B:AEF4:307F:8D7A 000C.293D.75B2   Gi1/0/5   100  0005   3mn
```

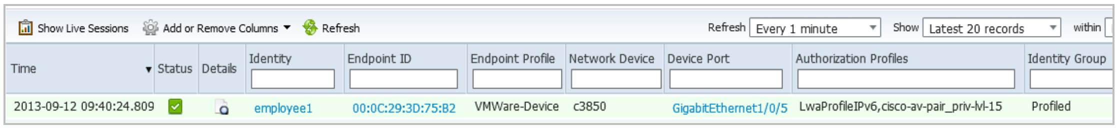
```
    REACHABLE  105 s try 0
```

The “show ip admission cache” is a handy command that can be used to debug issues related to web authentication. The following logs are the output of this command prior and post IPv6 local web authentication on the access port Gi 1/0/5:

```
!Prior to IPv6 LWA
switch#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
  Client MAC 000c.293d.75b2 Client IP 0.0.0.0 IPv6 ::, State INIT, Method Webauth

! After IPv6 LWA
switch#show ip admission cache
Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 0
  Client MAC 000c.293d.75b2 Client IP 0.0.0.0 IPv6 
2001:DB8:100:0:C45B:AEF4:307F:8D7A, State AUTHZ, Method Webauth
```

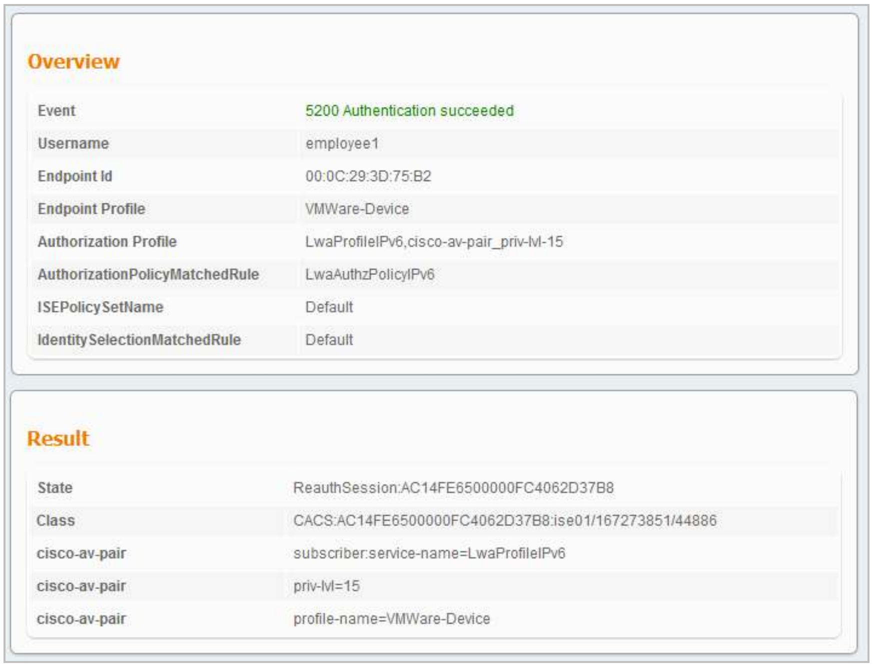
The ISE live authentication logs can be referred to, to track the IPv6 Local web authentication and authorization flows.

OPERATIONS → AUTHENTICATIONS



Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group
2013-09-12 09:40:24.809	✓		employee1	00:0C:29:3D:75:B2	VMWare-Device	c3850	GigabitEthernet1/0/5	LwaProfileIPv6,cisco-av-pair_priv-lvl-15	Profiled

OPERATIONS → AUTHENTICATIONS (DETAILS)



Overview

Event	5200 Authentication succeeded
Username	employee1
Endpoint Id	00:0C:29:3D:75:B2
Endpoint Profile	VMWare-Device
Authorization Profile	LwaProfileIPv6,cisco-av-pair_priv-lvl-15
AuthorizationPolicyMatchedRule	LwaAuthzPolicyIPv6
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Result

State	ReauthSession:AC14FE6500000FC4062D37B8
Class	CACS:AC14FE6500000FC4062D37B8:ise01/167273851/44886
cisco-av-pair	subscriber:service-name=LwaProfileIPv6
cisco-av-pair	priv-lvl=15
cisco-av-pair	profile-name=VMWare-Device

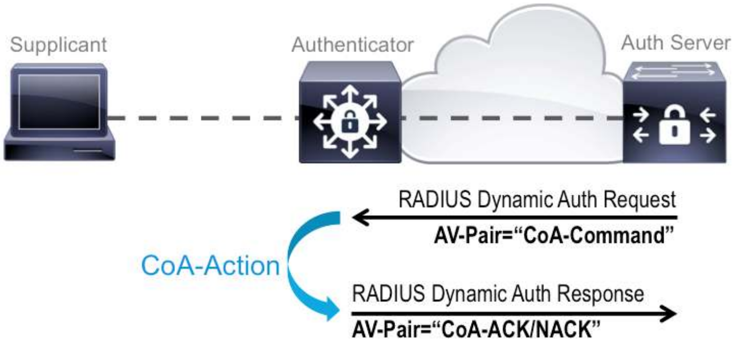
Note: For IPv6 central web authentication, the following configuration on the switch should be enough:

```
parameter-map type webauth IPv6-CWA
redirect portal ipv6 2001:DB8:254::4
!
policy-map type control subscriber ENT-CENTRAL-WEBAUTH
  event session-started match-all
    10 class always do-until-failure
      10 authenticate using dot1x priority 10
      20 authenticate using webauth aaa authc-list WebAuth parameter-map IPv6-CWA
priority 30
!
```

RADIUS Change of Authorization (COA)

Policy aware IBNS supports RADIUS Change of Authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.

Figure 16. RADIUS Change of Authorization



Session Identification

For disconnect and CoA requests targeted at a particular session, the device locates the session based on one or more of the following attributes:

Acct-Session-Id (IETF attribute #44)

Audit-Session-Id (Cisco VSA)

Calling-Station-Id (IETF attribute #31, which contains the host MAC address)

IPv6 Attributes, which can be one of the following:

- Framed-IPv6-Prefix (IETF attribute #97) and Framed-Interface-Id (IETF attribute #96), which together create a full IPv6 address per RFC 3162
- Framed-IPv6-Address
- Plain IP Address (IETF attribute #8)

If more than one session identification attribute is included in the message, all of the attributes must match the session, or the device returns a Disconnect-NAK or CoA-NAK with the error code "Invalid Attribute Value."

For CoA requests targeted at a particular enforcement policy, the device returns a CoA-NAK with the error code “Invalid Attribute Value” if any of the above session identification attributes are included in the message.

Table 1. RADIUS CoA Commands Supported on Policy Aware IBNS

CoA Command	Cisco VSA	Purpose
Activate Service	Cisco:Avpair=“subscriber:command=activate-service” Cisco:Avpair=“subscriber:service-name=<service-name>” Cisco:Avpair=“subscriber:precedence=<precedence-number>” Cisco:Avpair=“subscriber:activation-mode=replace-all”	The CoA activate service command can be used to activate a service template on a session.
Deactivate service	Cisco:Avpair=“subscriber:command=deactivate-service” Cisco:Avpair=“subscriber:service-name=<service-name>”	The CoA deactivate service command can be used to deactivate a service template on a session.
Bounce host port	Cisco:Avpair=“subscriber:command=bounce-host-port”	The CoA bounce host port command terminates a session and bounces the port (initiates a link down event followed by a link up event).
Disable host port	Cisco:Avpair=“subscriber:command=disable-host-port”	The CoA disable host port command administratively shuts down the authentication port that is hosting a session, which terminates the session.
Session query	Cisco:Avpair=“subscriber:command=session-query”	The CoA session query command requests service information about a subscriber session.
Session reauthenticate	Cisco:Avpair=“subscriber:command=reauthenticate” Cisco:Avpair=“subscriber:reauthenticate-type=last” or Cisco:Avpair=“subscriber:reauthenticate-type=rerun”	This CoA initiates session authentication.
Session terminate	This is a standard disconnect request and does not require a VSA.	A CoA Disconnect-Request command terminates a session without disabling the host port.

Note: Cisco ISE 1.2 supports all the CoA command types except for the “Activate-Service” and “Deactivate-Service” commands.

Per-Session CoA for Session Query

Cisco Identity Services Engine 1.2 supports the session query CoA command that can be used to gather information about an access-session running on an authenticator. This command is useful in collecting the session specific data from a centralized policy server.

Apart from the AAA and RADIUS commands, for CoA to work, the switch must be configured to accept CoA commands from authorized server(s).

```
aaa new-model
aaa session-id common
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
  client 172.20.254.4 server-key cisco
  server-key cisco
!
radius server ise
  address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
  automate-tester username probe-user
  key cisco
!
```

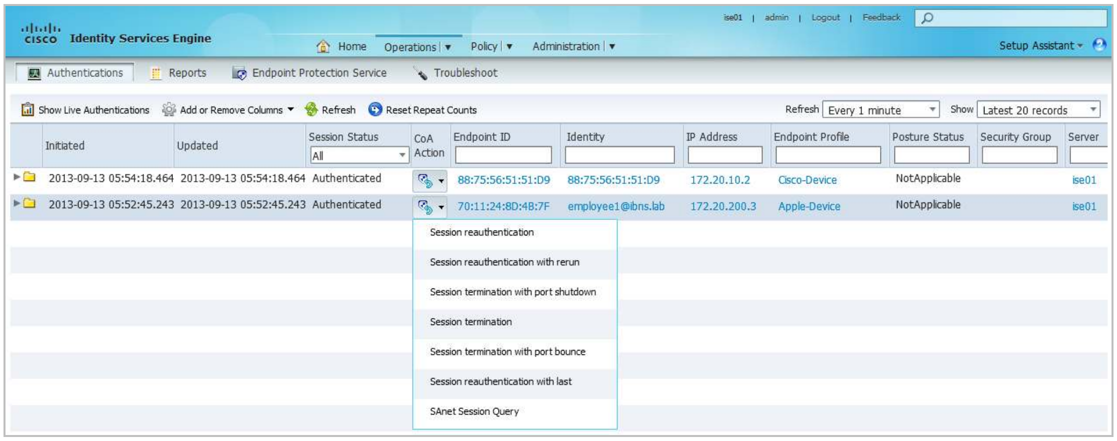
To trigger a CoA, the session context is essential and there are various attributes of a session that can be used to uniquely identify a session running on a switch.

```
switch#show access-session interface gigabitEthernet 1/0/1 details
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x10059C000000152
      MAC Address:  7011.248d.4b7f
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.200.3
        User-Name:  employee1@ibns.lab
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FCC0A83BF62
  Acct Session ID:  0x00000FCF
           Handle:  0xDE00000F
   Current Policy:  POLICY_Gi1/0/1

Server Policies:
          Template  FinanceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 200
          ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd
Method status list:
  Method    State
  dot1x     Authc Success
----------------------------------------
        Interface:  GigabitEthernet1/0/1
           IIF-ID:  0x10395C000000153
      MAC Address:  8875.5651.51d9
     IPv6 Address:  Unknown
     IPv4 Address:  172.20.15.2
        User-Name:  88-75-56-51-51-D9
           Status:  Authorized
           Domain:  VOICE
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FCD0A83CCE6
  Acct Session ID:  0x00000FD0
           Handle:  0x4C000010
   Current Policy:  POLICY_Gi1/0/1

Server Policies:
```

```
         Template:  VoiceServiceTemplateDNL (priority 100)
       Vlan Group:  Vlan: 15
          ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd

Method status list:
  Method    State
  dot1x     Stopped
  mab       Authc Success
```

To query a session from ISE, click on “**SAnet Session Query**” under:

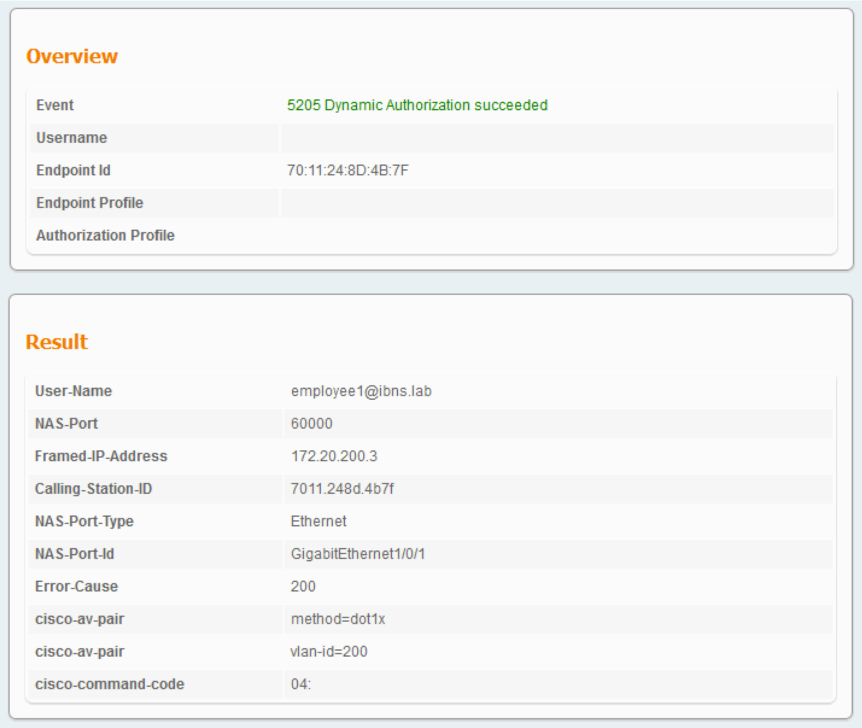
OPERATIONS → AUTHENTICATIONS → “SHOW LIVE AUTHENTICATIONS”



Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Security Group	Server
2013-09-13 05:54:18.464	2013-09-13 05:54:18.464	Authenticated		88:75:56:51:51:D9	88:75:56:51:51:D9	172.20.10.2	Cisco-Device	NotApplicable		ise01
2013-09-13 05:52:45.243	2013-09-13 05:52:45.243	Authenticated		70:11:24:8D:4B:7F	employee1@ibns.lab	172.20.200.3	Apple-Device	NotApplicable		ise01

On the ISE, details about the queried session attributes can be found under:

OPERATIONS → AUTHENTICATIONS (DETAILS)



Overview

Event	5205 Dynamic Authorization succeeded
Username	
Endpoint Id	70:11:24:8D:4B:7F
Endpoint Profile	
Authorization Profile	

Result

User-Name	employee1@ibns.lab
NAS-Port	60000
Framed-IP-Address	172.20.200.3
Calling-Station-ID	7011.248d.4b7f
NAS-Port-Type	Ethernet
NAS-Port-Id	GigabitEthernet1/0/1
Error-Cause	200
cisco-av-pair	method=dot1x
cisco-av-pair	vlan-id=200
cisco-command-code	04:

On the Switch RADIUS, debugging can be enabled to validate CoA in action.

```
switch#show debugging

Radius protocol debugging is on
Radius packet protocol (authentication) debugging is on

switch#
*Sep 13 06:10:07.506: RADIUS: COA received from id 8 172.20.254.4:59599, CoA
Request, len 158
*Sep 13 06:10:07.507: RADIUS/ENCODE(00000000):Orig. component type = Invalid
*Sep 13 06:10:07.507: RADIUS(00000000): sending
*Sep 13 06:10:07.507: RADIUS(00000000): Send CoA Ack Response to
172.20.254.4:59599 id 8, len 217
*Sep 13 06:10:07.507: RADIUS: authenticator 26 83 79 8C 60 CA 00 42–2D F7 C3 74
AF 4A BC 92
*Sep 13 06:10:07.507: RADIUS: Framed-IP-Address [8] 6 172.20.200.3
*Sep 13 06:10:07.507: RADIUS: Vendor, Cisco [26] 20
*Sep 13 06:10:07.507: RADIUS: Cisco AVpair [1] 14 "method=dot1x"
*Sep 13 06:10:07.507: RADIUS: Vendor, Cisco [26] 49
*Sep 13 06:10:07.507: RADIUS: Cisco AVpair [1] 43 "audit-session-
id=AC14FE6500000FCC0A83BF62"
*Sep 13 06:10:07.508: RADIUS: User-Name [1] 20 "employee1@ibns.lab"
*Sep 13 06:10:07.508: RADIUS: Vendor, Cisco [26] 19
*Sep 13 06:10:07.508: RADIUS: Cisco AVpair [1] 13 "vlan-id=200"
```

```
*Sep 13 06:10:07.508: RADIUS: NAS-Port [5] 6 60000
*Sep 13 06:10:07.508: RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/1"
*Sep 13 06:10:07.508: RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
*Sep 13 06:10:07.508: RADIUS: Vendor, Cisco [26] 9
*Sep 13 06:10:07.508: RADIUS: ssg-command-code [252] 3
*Sep 13 06:10:07.508: RADIUS: 04
*Sep 13 06:10:07.508: RADIUS: Calling-Station-Id [31] 16 "7011.248d.4b7f"
*Sep 13 06:10:07.508: RADIUS: Dynamic-Author-Error[101] 6 Success [200]
*Sep 13 06:10:07.508: RADIUS: Message-Authenticato[80] 18
*Sep 13 06:10:07.508: RADIUS: 0B 77 48 92 9B 67 5E D7 AB 1B 06 2B 50 43 88 EE [
wHg^+PC]
```

CoA for Local Web Authentication

The Access session manager can now facilitate Change-of-Authorization for web authentication sessions. All the CoA commands that can be executed for any authentication session is also applicable for web authentication. This topic explains how to trigger a CoA from ISE to Admin shutdown the access-port for a web-Auth session.

The switch requires minimal configuration to accept CoA messages from authorized RADIUS servers.

```
aaa server radius dynamic-author
 client 172.20.254.4 server-key cisco
 server-key cisco
!
```

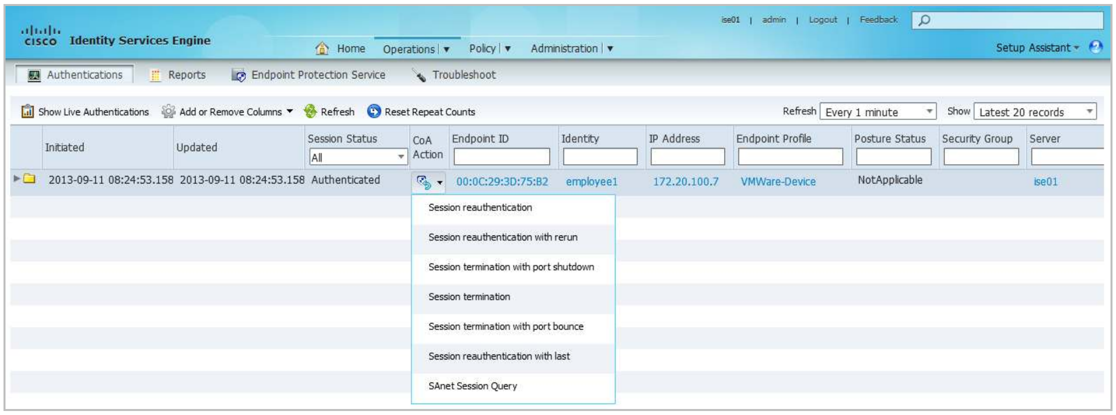
A session is identified with various attributes as explained under the CoA section; Acct-Session-Id (IETF attribute #44), Audit-Session-Id (Cisco VSA), Calling-Station-Id (IETF attribute #31, which contains the host MAC address), IPv6 Attributes and Plain IP address (IETF attribute #8).

```
switch#show access-session interface gigabitEthernet 1/0/5 details
        Interface:  GigabitEthernet1/0/5
           IIF-ID:  0x1008B000000014A
      MAC Address:  000c.293d.75b2
     IPv6 Address:  FE80::C45B:AEF4:307F:8D7A,
2001:DB8:100:0:CC62:7933:DA8E:232A, 2001:DB8:100:0:C45B:AEF4:307F:8D7A
     IPv4 Address:  172.20.100.7
        User-Name:  employee1
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FB600C19ED6
  Acct Session ID:  0x00000FB1
           Handle:  0xC9000007
   Current Policy:  ENT-WEBAUTH-POL

Server Policies:
          ACS ACL:   xACSACLx-IP-PERMIT_ALL_TRAFFIC-519611bd

Method status list:
```

```
Method   State
dot1x    Stopped
webauth  Authc Success
```

To trigger a CoA from ISE, go to:

OPERATIONS → AUTHENTICATIONS → "SHOW LIVE AUTHENTICATIONS"



Identity Services Engine
ise01 | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Assistant
Authentications
Reports
Endpoint Protection Service
Troubleshoot
Show Live Authentications
Add or Remove Columns
Refresh
Reset Repeat Counts
Session reauthentication
Session reauthentication with rerun
Session termination with port shutdown
Session termination
Session termination with port bounce
Session reauthentication with last
SAnet Session Query

Refresh: Every 1 minute
Show: Latest 20 records

Initiated	Updated	Session Status	CoA Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	Security Group	Server
		All								
2013-09-11 08:24:53.158	2013-09-11 08:24:53.158	Authenticated		00:0C:29:3D:75:B2	employee1	172.20.100.7	VMWare-Device	NotApplicable		ise01

The "debug radius authentication" command can be executed on the switch to debug CoA in action.

```
switch#show debugging

Radius protocol debugging is on
Radius packet protocol (authentication) debugging is on

*Sep 11 08:29:07.851: RADIUS: COA received from id 15 172.20.254.4:53698, CoA
Request, len 168

<output truncated>
*Sep 11 08:29:07.867: RADIUS: Dynamic-Author-Error[101] 6 Success [200]

<output truncated>
*Sep 11 08:29:09.848: %LINK-5-CHANGED: Interface GigabitEthernet1/0/5, changed
state to administratively down
*Sep 11 08:29:10.849: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/5, changed state to down

switch#show interfaces gigabitEthernet 1/0/5 status

Port      Name                Status    Vlan    Duplex  Speed   Type
Gi1/0/5   ** Connected to Wo  disabled  100     auto    auto    10/100/1000BaseTX
```

Per MAC VLAN Assignment

Multi-Auth: Per MAC Address VLAN Assignment

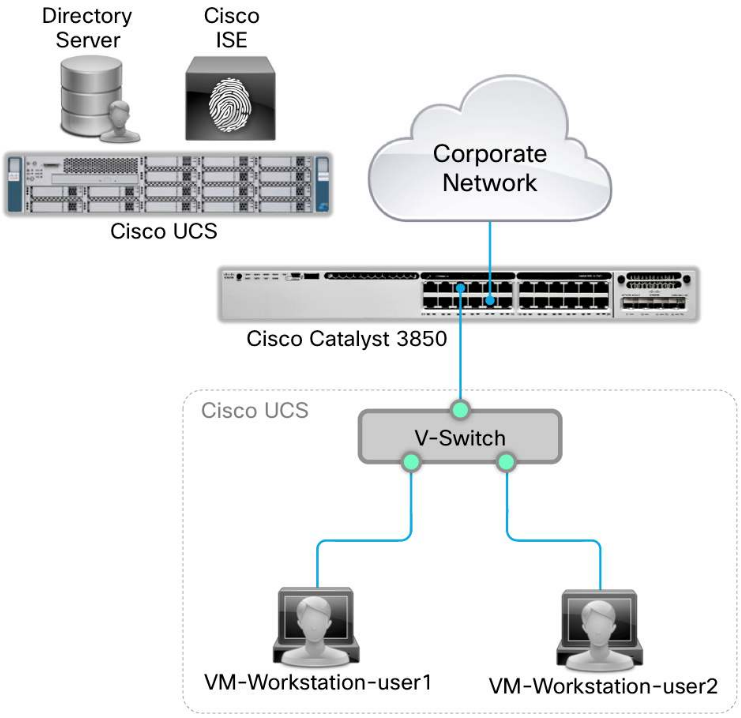
Several identity deployments require the edge switches to be able to authorize multiple hosts or MAC-Addresses on a single switch-port to different VLANs. Typical use cases are: an extended LAN segment spanning through an Ethernet hub, workgroup access from host OS and virtual machines in bridged-mode, data center virtualization and many more.

In the legacy switches, the multiple authentication (multi-auth) host mode allows for more than one host on an access-port to be authenticated and authorized, but with a caveat of only "one" VLAN authorization per port, where either all the hosts are authorized to a common access VLAN, or no VLAN authorizations falling back to the VLAN configuration on the port. At most times, trunk switch-ports serve this purpose, however not many Network Interface Cards (NICs) can support either 802.1Q or ISL trunking natively.

The 3850 and 3650 platforms possess the capability to assign VLANs per MAC address, in contrast to the per port VLAN assignment only capability of the legacy switches. With this capability, without the need for a tagging capable network adapter, the end hosts can be placed in different VLANs even though they connect to a common switch access port.

Note: The Per MAC Address VLAN assignment feature is currently supported on the Catalyst 3850 and 3650 only.

Figure 17. Multi-Auth—Per MAC Address VLAN Assignment



For 802.1X authentication and RADIUS authorizations, global configurations are necessary.

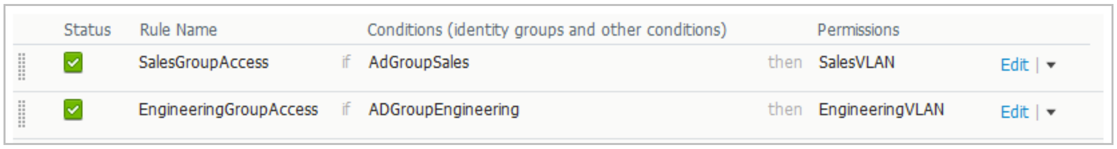
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization exec default local
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
aaa session-id common
!
dot1x system-auth-control
!
radius server ise
  address ipv4 172.20.254.4 auth-port 1812 acct-port 1813
  automate-tester username probe-user
  key cisco
!
```

Authorizing hosts with different VLANs on the same access-port can be done both in legacy and new-style mode. To setup a Per-MAC VLAN assignment, a minimalistic configuration similar to the one below should suffice (remember “multi-auth” host mode is a must to authenticate and authorize the hosts in respective VLANs):

```
interface GigabitEthernet1/0/2
  description ** Access Port **
  switchport access vlan 100
  switchport mode access
  authentication host-mode multi-auth
  authentication port-control auto
  dot1x pae authenticator
  spanning-tree portfast
!
```

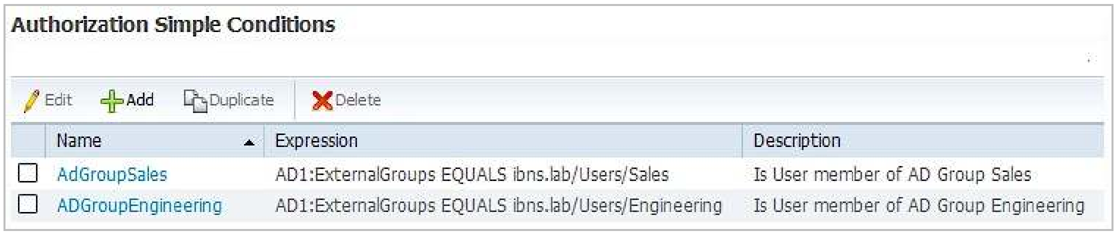
On the Identity Services Engine, configure authorization policies to assign VLANs on authentication. This configuration is similar to a legacy VLAN assignment authorization profile, where hosts are expected on different access ports.

POLICY → AUTHORIZATION



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	SalesGroupAccess	if	AdGroupSales	then	SalesVLAN	Edit | ▾
✓	EngineeringGroupAccess	if	ADGroupEngineering	then	EngineeringVLAN	Edit | ▾

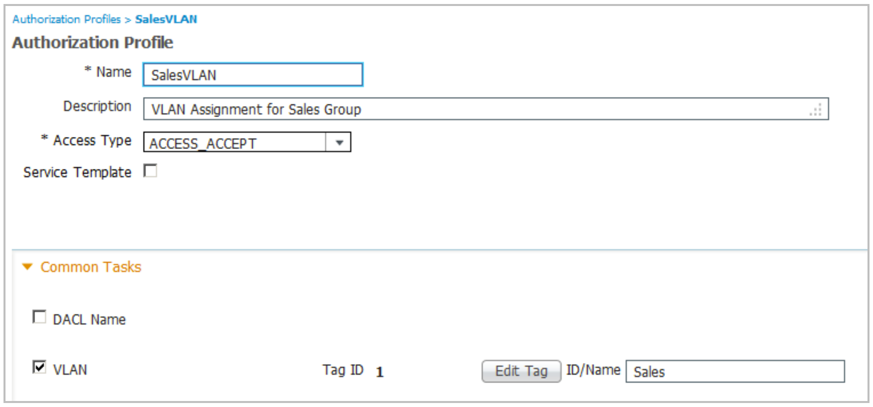
POLICY → POLICY ELEMENTS → CONDITIONS → SIMPLE CONDITIONS



Authorization Simple Conditions

	Name ▲	Expression	Description
□	AdGroupSales	AD1:ExternalGroups EQUALS ibns.lab/Users/Sales	Is User member of AD Group Sales
□	ADGroupEngineering	AD1:ExternalGroups EQUALS ibns.lab/Users/Engineering	Is User member of AD Group Engineering

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > SalesVLAN

Authorization Profile

* Name: SalesVLAN

Description: VLAN Assignment for Sales Group

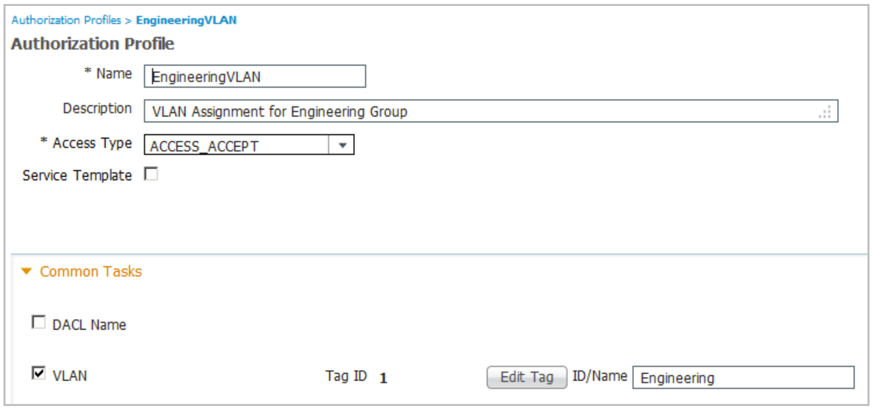
* Access Type: ACCESS_ACCEPT

Service Template □

▾ Common Tasks

□ DACL Name

☑ VLAN Tag ID 1 ID/Name Sales



Authorization Profiles > EngineeringVLAN

Authorization Profile

* Name: EngineeringVLAN

Description: VLAN Assignment for Engineering Group

* Access Type: ACCESS_ACCEPT

Service Template □

▾ Common Tasks

□ DACL Name

☑ VLAN Tag ID 1 ID/Name Engineering

RADIUS Attribute Details	
Sales VLAN	**Engineering VLAN**

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:Sales
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
	Access Type = ACCESS_ACCEPT
	Tunnel-Private-Group-ID = 1:Engineering
	Tunnel-Type=1:13
	Tunnel-Medium-Type=1:6

The VLANs have to be configured in the switch network. If the ISE authorization profile is defined for a VLAN number, then a matching VLAN number must be configured on the switch, otherwise on ISE, if a VLAN name is defined, then any VLAN number matching the VLAN name must be configured on the switch.

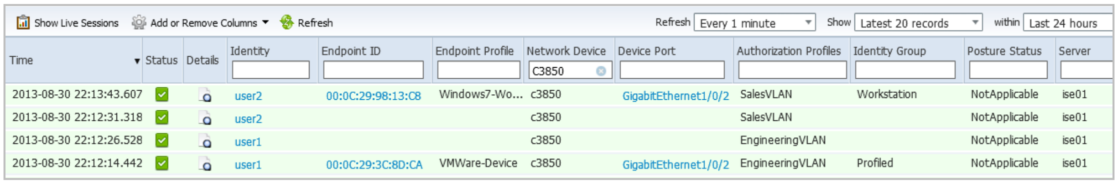
```
C3850#show vlan brief

VLAN   Name                    Status        Ports
----   -------------------     ------------  ---------------------------
1      default                 active        Gi1/0/1, Gi1/0/3, Gi1/0/4
                                             Gi1/0/5, Gi1/0/6, Gi1/0/7
                                             Gi1/0/8, Gi1/0/9, Gi1/0/11
                                             Gi1/0/12, Gi1/0/13, Gi1/0/14
                                             Gi1/0/15, Gi1/0/16, Gi1/0/17
                                             Gi1/0/18, Gi1/0/19, Gi1/0/20
                                             Gi1/0/21, Gi1/0/22, Gi1/0/23
                                             Gi1/0/24,
10     VoiceVLAN             active
100    DefaultAccess         active        Gi1/0/2
150    Engineering           active
151    Sales                 active
254    Management            active
1002   fddi-default          act/unsup
1003   token-ring-default    act/unsup
```

Upon successful port authentication, the hosts are authorized with their respective VLANs.

```
C3850#show authentication sessions interface gigabitEthernet 1/0/2 details
        Interface:  GigabitEthernet1/0/2
           IIF-ID:  0x1055340000000D1
      MAC Address:  000c.2998.13c8
     IPv6 Address:  FE80::7D2E:FC23:9230:B590,
2001:DB8:151:0:7D2E:FC23:9230:B590, 2001:DB8:151:0:BD78:5F90:F296:EB58
     IPv4 Address:  172.20.151.2
        User-Name:  user2
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FBF24B78B16
  Acct Session ID:  0x00000FBF
           Handle:  0x58000014
   Current Policy:  POLICY_Gi1/0/2

       Vlan Group:  Vlan: 151
Method status list:
  Method    State
  dot1x     Authc Success
----------------------------------------
        Interface:  GigabitEthernet1/0/2
           IIF-ID:  0x1053840000000D0
      MAC Address:  000c.293c.8dca
     IPv6 Address:  FE80::5824:E766:EEAA:4513,
2001:DB8:150:0:5824:E766:EEAA:4513, 2001:DB8:150:0:499F:A2F3:3906:E405
     IPv4 Address:  172.20.150.2
        User-Name:  user1
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FBE24B78B16
  Acct Session ID:  0x00000FC0
           Handle:  0x61000013
```

```
    Current Policy:  POLICY_Gi1/0/2

Server Policies:
       Vlan Group:  Vlan: 150
Method status list:
  Method    State
  dot1x     Authc Success

C3850#show vlan brief | include Engineering|Sales
150 Engineering         active Gi1/0/2
151 Sales               active Gi1/0/2

C3850#show mac address-table |  include 1/0/2
150 000c.293c.8dca             STATIC Gi1/0/2
151 000c.2998.13c8             STATIC Gi1/0/2
```

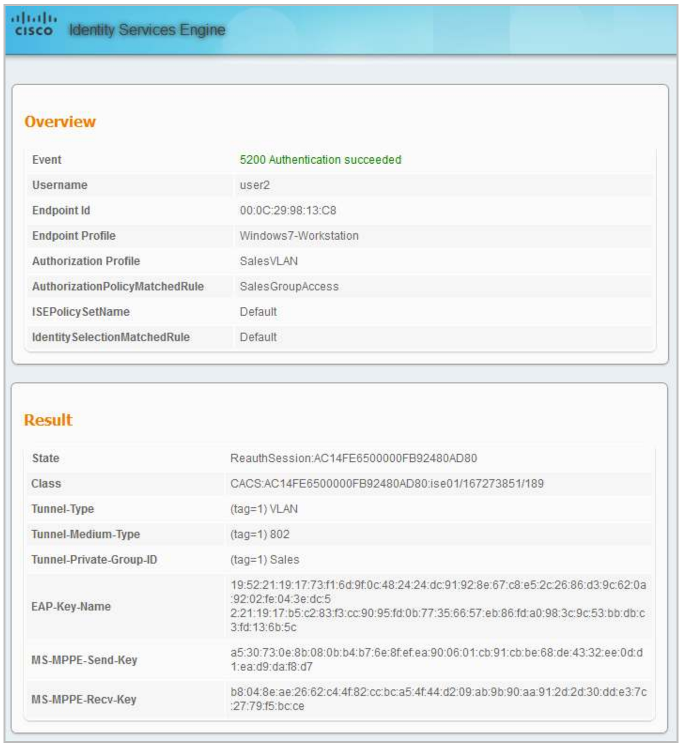
On the AAA server logs, the authentication and authorization may be validated. The “Live Authentications” section in ISE provides the authentication and authorization details of the access sessions:



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

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server
						C3850					
2013-08-30 22:13:43.607	✓		user2	00:0C:29:98:13:C8	Windows7-Wo...	c3850	GigabitEthernet1/0/2	SalesVLAN	Workstation	NotApplicable	ise01
2013-08-30 22:12:31.318	✓		user2			c3850		SalesVLAN		NotApplicable	ise01
2013-08-30 22:12:26.528	✓		user1			c3850		EngineeringVLAN		NotApplicable	ise01
2013-08-30 22:12:14.442	✓		user1	00:0C:29:3C:8D:CA	VMWare-Device	c3850	GigabitEthernet1/0/2	EngineeringVLAN	Profiled	NotApplicable	ise01

OPERATIONS → AUTHENTICATIONS (DETAILS)



Overview

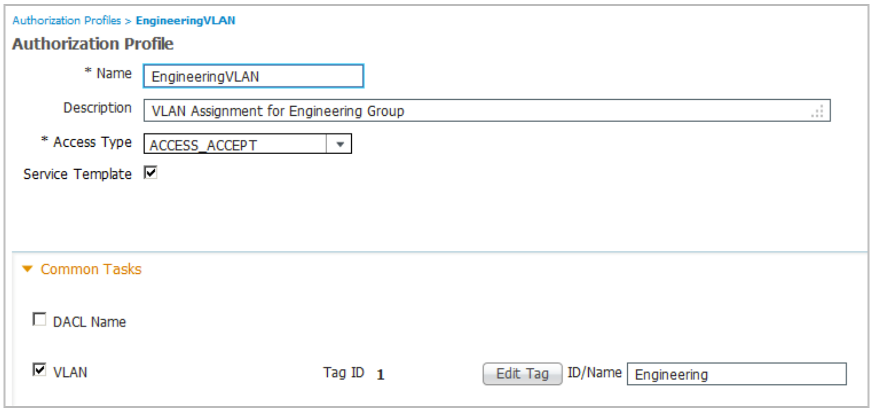
Event	5200 Authentication succeeded
Username	user2
Endpoint Id	00:0C:29:98:13:C8
Endpoint Profile	Windows7-Workstation
Authorization Profile	SalesVLAN
AuthorizationPolicyMatchedRule	SalesGroupAccess
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Result

State	ReauthSession:AC14FE6500000FB92480AD80
Class	CACS:AC14FE6500000FB92480AD80:ise01/167273851/189
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) Sales
EAP-Key-Name	19:52:21:19:17:73:f1:6d:9f:0c:48:24:24:dc:91:92:8e:67:c8:e5:2c:26:86:d3:9c:62:0a:92:02:fe:04:3e:dc:5 2:21:19:17:b5:c2:83:f3:cc:90:95:fd:0b:77:35:66:57:eb:86:fd:a0:98:3c:9c:53:bb:db:c3:fd:13:6b:5c
MS-MPPE-Send-Key	a5:30:73:0e:8b:08:0b:b4:b7:6e:8f:ef:ea:90:06:01:cb:91:cb:be:68:de:43:32:ee:0d:d1:ea:d9:da:f8:d7
MS-MPPE-Recv-Key	b8:04:8e:ae:26:62:c4:4f:82:cc:bc:a5:4f:44:d2:09:ab:9b:90:aa:91:2d:2d:30:dd:e3:7c:27:79:f5:bc:ce

The end users can also be authorized with Service-templates. All that is needed is to check the service-template option under the ISE authorization profiles.

POLICY → POLICY ELEMENTS → RESULTS → AUTHORIZATION → AUTHORIZATION PROFILES



Authorization Profiles > **EngineeringVLAN**

Authorization Profile

* Name: EngineeringVLAN

Description: VLAN Assignment for Engineering Group

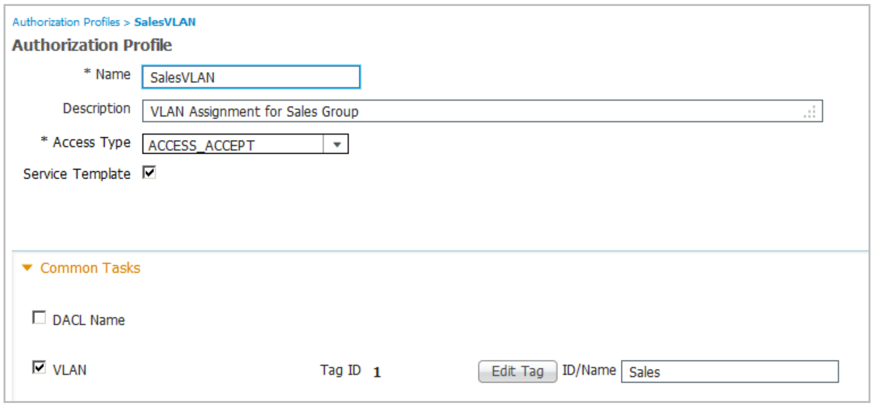
* Access Type: ACCESS_ACCEPT

Service Template ☑

Common Tasks

☐ DACL Name

☑ VLAN Tag ID 1 ID/Name: Engineering



Authorization Profiles > **SalesVLAN**

Authorization Profile

* Name: SalesVLAN

Description: VLAN Assignment for Sales Group

* Access Type: ACCESS_ACCEPT

Service Template ☑

Common Tasks

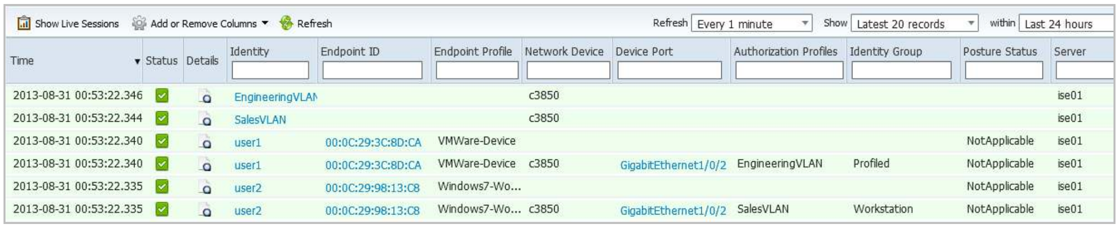
☐ DACL Name

☑ VLAN Tag ID 1 ID/Name: Sales

```
C3850#show authentication sessions interface gigabitEthernet 1/0/2 details
        Interface:  GigabitEthernet1/0/2
           IIF-ID:  0x106EAC0000000D4
      MAC Address:  000c.2998.13c8
     IPv6 Address:  FE80::7D2E:FC23:9230:B590,
2001:DB8:151:0:7D2E:FC23:9230:B590, 2001:DB8:151:0:BD78:5F90:F296:EB58
     IPv4 Address:  172.20.151.2
        User-Name:  user2
           Status:  Authorized
           Domain:  DATA
   Oper host mode:  multi-auth
 Oper control dir:  both
  Session timeout:  N/A
Common Session ID:  AC14FE6500000FC22514342E
  Acct Session ID:  0x00000FC7
           Handle:  0xDC000017
   Current Policy:  POLICY_Gi1/0/2

Server Policies:
         Template:  SalesVLAN (priority 100)
```

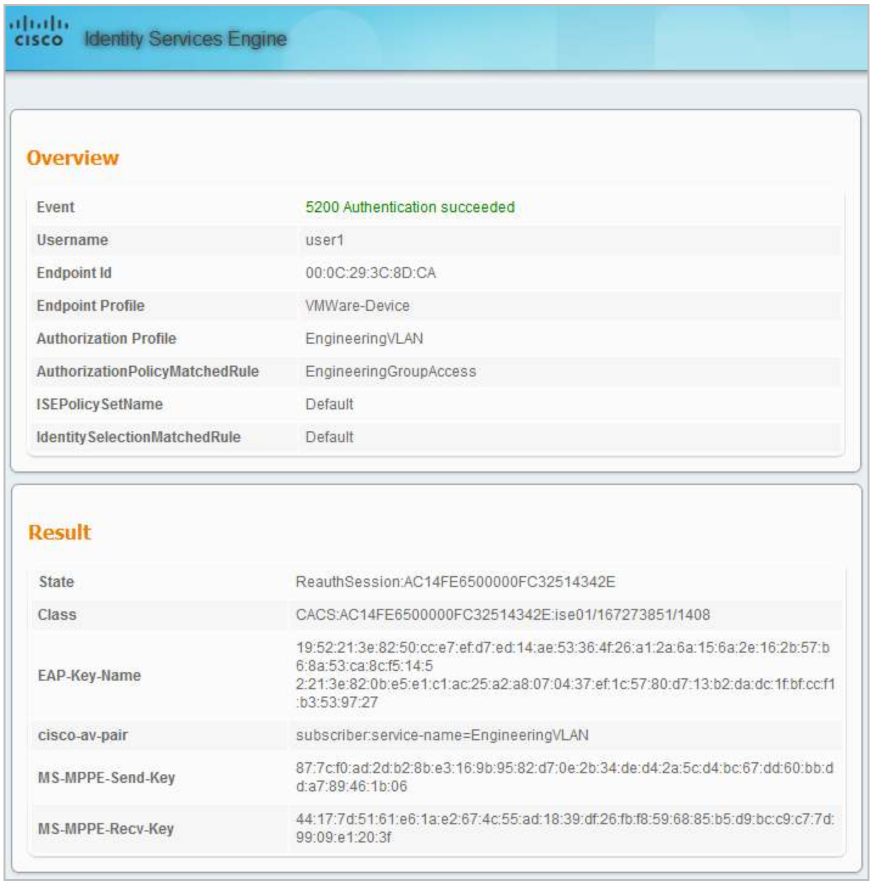
```
           Vlan Group:  Vlan: 151
   Method status list:
         Method    State
         dot1x     Authc Success
----------------------------------------
            Interface:  GigabitEthernet1/0/2
               IIF-ID:  0x104A3C0000000D5
          MAC Address:  000c.293c.8dca
         IPv6 Address:  FE80::5824:E766:EEAA:4513,
2001:DB8:150:0:5824:E766:EEAA:4513, 2001:DB8:150:0:499F:A2F3:3906:E405
         IPv4 Address:  172.20.150.2
            User-Name:  user1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC14FE6500000FC32514342E
      Acct Session ID:  0x00000FC8
               Handle:  0xD5000018
       Current Policy:  POLICY_Gi1/0/2

Server Policies:
             Template:  EngineeringVLAN (priority 100)
           Vlan Group:  Vlan: 150

Method status list:
      Method    State
      dot1x     Authc Success
```

OPERATIONS → AUTHENTICATIONS



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

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Server
2013-08-31 00:53:22.346	✓		EngineeringVLAN			c3850					ise01
2013-08-31 00:53:22.344	✓		SalesVLAN			c3850					ise01
2013-08-31 00:53:22.340	✓		user1	00:0C:29:3C:8D:CA	VMWare-Device					NotApplicable	ise01
2013-08-31 00:53:22.340	✓		user1	00:0C:29:3C:8D:CA	VMWare-Device	c3850	GigabitEthernet1/0/2	EngineeringVLAN	Profiled	NotApplicable	ise01
2013-08-31 00:53:22.335	✓		user2	00:0C:29:98:13:C8	Windows7-Wo...					NotApplicable	ise01
2013-08-31 00:53:22.335	✓		user2	00:0C:29:98:13:C8	Windows7-Wo...	c3850	GigabitEthernet1/0/2	SalesVLAN	Workstation	NotApplicable	ise01



Overview

Event	5200 Authentication succeeded
Username	user1
Endpoint Id	00:0C:29:3C:8D:CA
Endpoint Profile	VMWare-Device
Authorization Profile	EngineeringVLAN
AuthorizationPolicyMatchedRule	EngineeringGroupAccess
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Result

State	ReauthSession:AC14FE6500000FC32514342E
Class	CACS:AC14FE6500000FC32514342E:ise01/167273851/1408
EAP-Key-Name	19:52:21:3e:82:50:cc:e7:ef:d7:ed:14:ae:53:36:4f:26:a1:2a:6a:15:6a:2e:16:2b:57:b6:8a:53:ca:8c:f5:14:52:21:3e:82:0b:e5:e1:c1:ac:25:a2:a8:07:04:37:ef:1c:57:80:d7:13:b2:da:dc:1f:bf:cc:f1:b3:53:97:27
cisco-av-pair	subscriber:service-name=EngineeringVLAN
MS-MPPE-Send-Key	87:7c:f0:ad:2d:b2:8b:e3:16:9b:95:82:d7:0e:2b:34:de:d4:2a:5c:d4:bc:67:dd:60:bb:dd:a7:89:46:1b:06
MS-MPPE-Recv-Key	44:17:7d:51:61:e6:1a:e2:67:4c:55:ad:18:39:df:26:fb:f8:59:68:85:b5:d9:bc:c9:c7:7d:99:09:e1:20:3f

Appendix

The New radius server <name> Command

Conventionally the RADIUS server configuration on the switches has been done with the “radius-server host” global configuration command. On the newer switch software versions, a newer command “radius server <name>” can be used for the same purpose. This newer command offers modularity and maintains consistency between IPv4 and IPv6 RADIUS server configurations.

When upgrading the system to newer software, with the “radius-server host” command in the configuration or if it is attempted to configure the “radius-server host” command on the newer images, the following error message will appear:

```
switch(config)#radius-server host 10.1.1.1
  Warning: The CLI will be deprecated soon
  'radius-server host 10.1.1.1'
  Please move to 'radius server <name>' CLI.
```

The following table gives the correlation between the legacy and new configuration options:

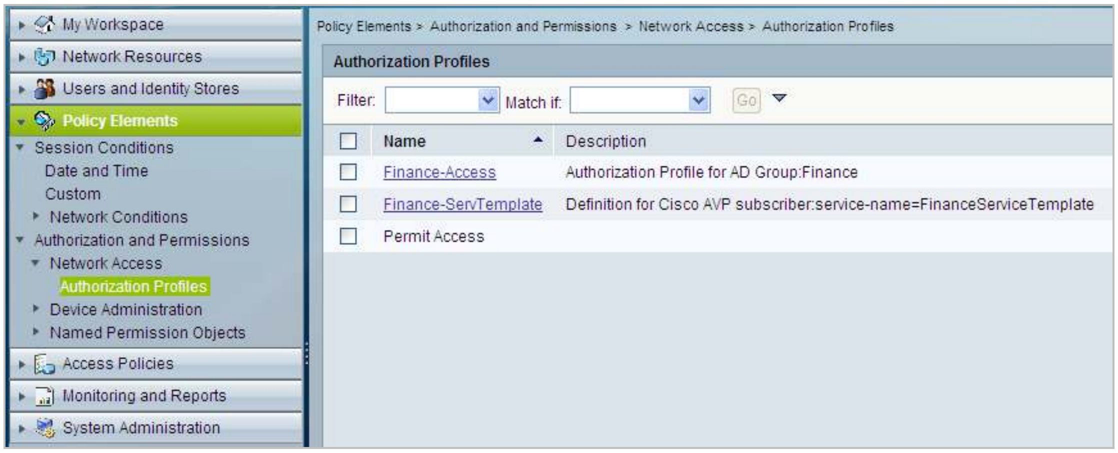
Legacy configuration	radius-server host 10.1.1.1 auth-port 1812 acct-port 1812 key cisco radius-server host 10.1.1.1 test username probe-user
New configuration	radius server ise-server address ipv4 10.1.1.1 auth-port 1812 acct-port 1812 key cisco automate-tester username probe-user

Note: Only the radius-server host command is set to be deprecated, but the rest of the radius-server parse trees shall continue to remain. The radius server <name> command has to be used in place of the radius-server host command.

Configuring Service-template on the Cisco Secure ACS5.X

The Cisco Secure ACS 5.X can be setup for Service-template authorizations. Refer the following guidelines for configurations.

Define two Authorizations Profiles, one for authorizing 802.1X authentication and the other for downloading service-template contents:

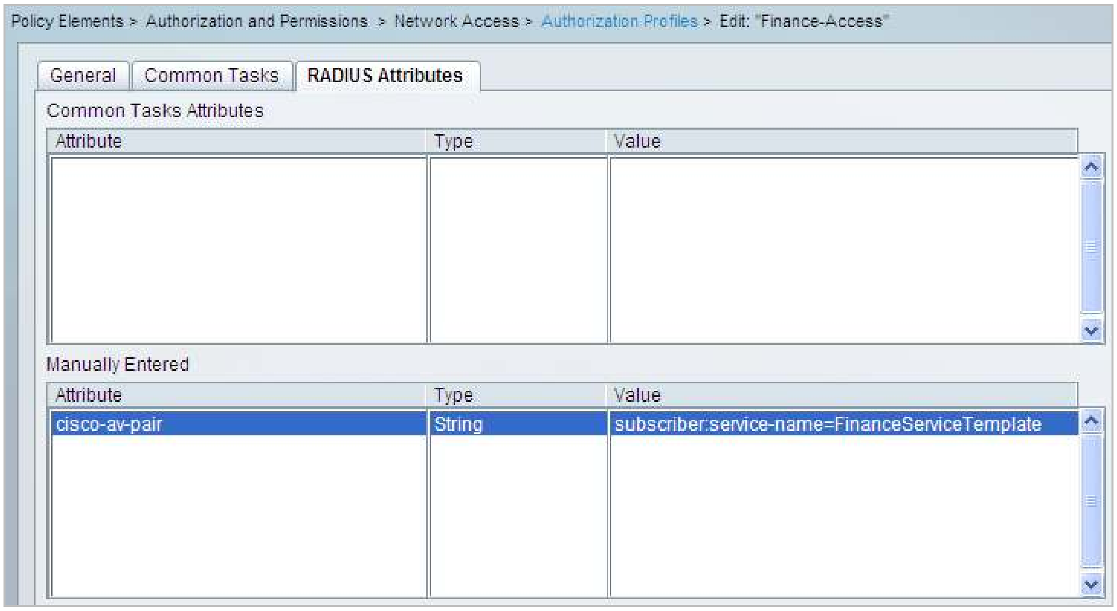


Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles

Authorization Profiles

☐	Name	Description
☐	Finance-Access	Authorization Profile for AD Group:Finance
☐	Finance-ServTemplate	Definition for Cisco AVP subscriber:service-name=FinanceServiceTemplate
☐	Permit Access	

Authorization profile “Finance-Access” definition



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Finance-Access"

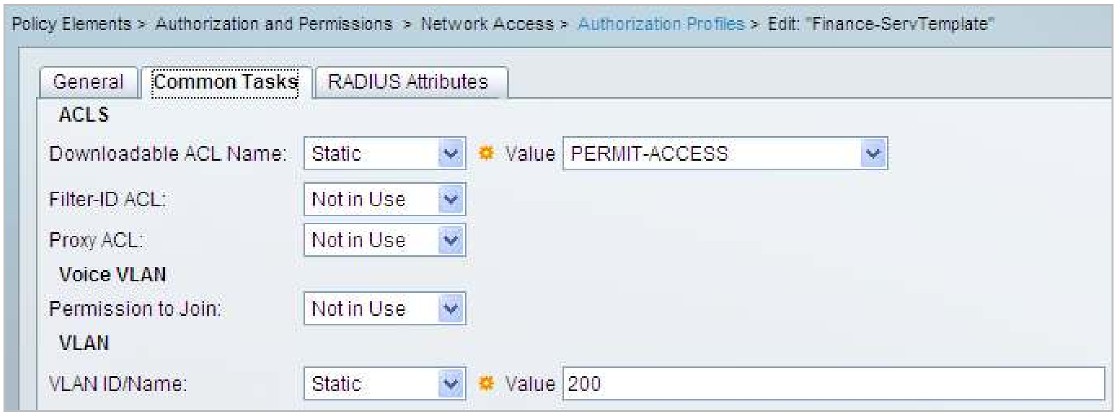
Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
cisco-av-pair	String	subscriber:service-name=FinanceServiceTemplate

Authorization profile “Finance-ServTemplate” definition



Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Finance-ServTemplate"

ACLS

Downloadable ACL Name: Static ✱ Value PERMIT-ACCESS

Filter-ID ACL: Not in Use

Proxy ACL: Not in Use

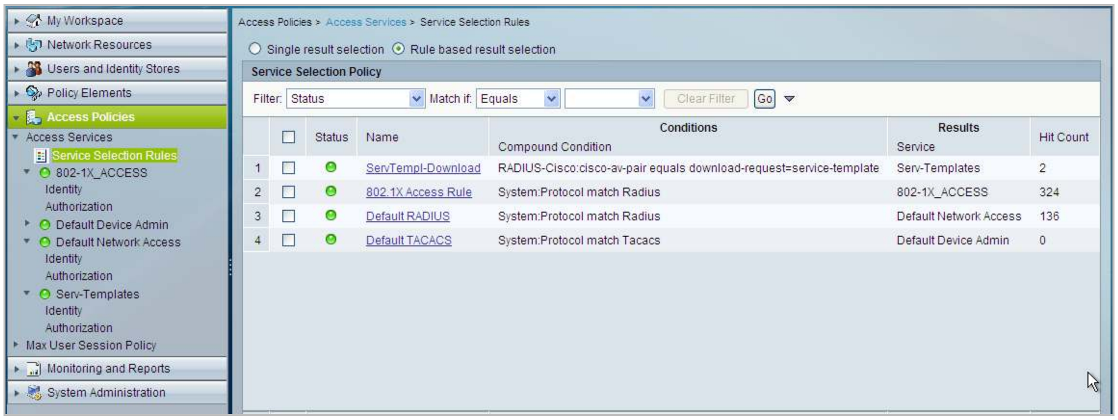
Voice VLAN

Permission to Join: Not in Use

VLAN

VLAN ID/Name: Static ✱ Value 200

Define two Access profiles, one for RADIUS authorization and other to cater to a service-template download request.



Access Policies > Access Services > Service Selection Rules

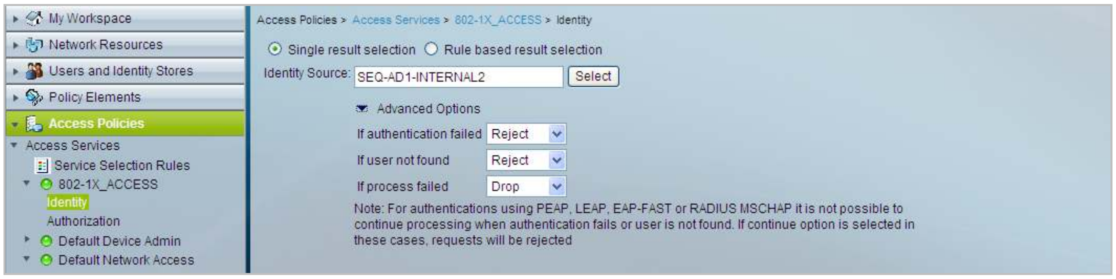
○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Clear Filter Go

	□	Status	Name	Conditions	Results	Hit Count
				Compound Condition	Service	
1	□	●	ServTempl-Download	RADIUS-Cisco:cisco-av-pair equals download-request=service-template	Serv-Templates	2
2	□	●	802.1X Access Rule	System:Protocol match Radius	802-1X_ACCESS	324
3	□	●	Default RADIUS	System:Protocol match Radius	Default Network Access	136
4	□	●	Default TACACS	System:Protocol match Tacacs	Default Device Admin	0

The RADIUS authorization access profile can optionally be set to lookup AD/LDAP for user authentication or internal user/host database lookup alone. Define authorization to respond with authorization profile set for 802.1X authentication.



Access Policies > Access Services > 802-1X_ACCESS > Identity

● Single result selection ○ Rule based result selection

Identity Source: SEQ-AD1-INTERNAL2 Select

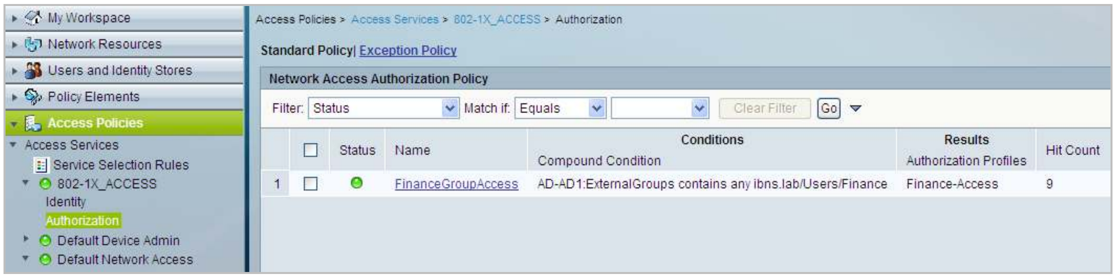
Advanced Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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



Access Policies > Access Services > 802-1X_ACCESS > Authorization

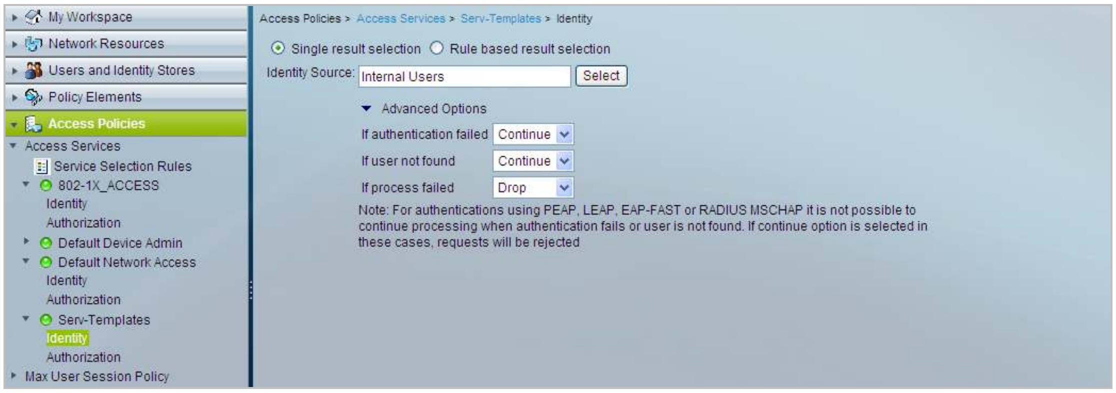
Standard Policy| Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Clear Filter Go

	□	Status	Name	Conditions	Results	Hit Count
				Compound Condition	Authorization Profiles	
1	□	●	FinanceGroupAccess	AD-AD1:ExternalGroups contains any ibns.lab/Users/Finance	Finance-Access	9

The NAS (switch) uses the service-template name as user-id during a service-template download. Setup an Access profile to authorize such requests. It's advisable not to create user account (with service-template name) since creating a user account for service-template mandates for a password definition too. It's better to define the access profile "identity" with "Continue" for authentication fail and user not found conditions.



Access Policies > Access Services > Serv-Templates > Identity

● Single result selection ○ Rule based result selection

Identity Source: Internal Users

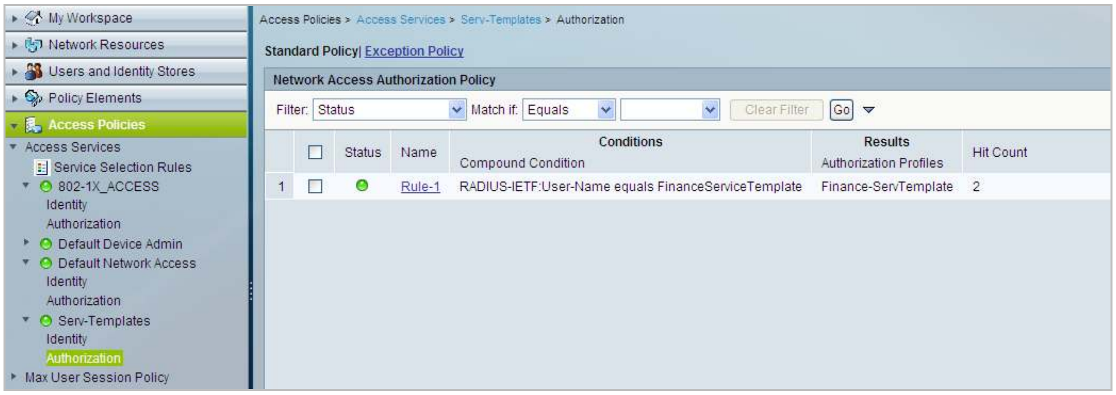
Advanced Options

If authentication failed: Continue

If user not found: Continue

If process failed: Drop

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



Access Policies > Access Services > Serv-Templates > Authorization

Standard Policy| Exception Policy

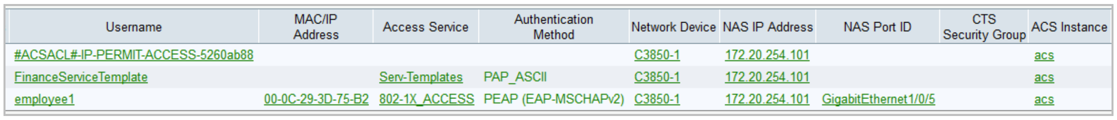
Network Access Authorization Policy

Filter: Status Match if: Equals

	☐	Status	Name	Conditions Compound Condition	Results Authorization Profiles	Hit Count
1	☐	●	Rule-1	RADIUS-IETF:User-Name equals FinanceServiceTemplate	Finance-ServTemplate	2

```
switch #show authentication sessions interface gigabitEthernet 1/0/5 details
            Interface:  GigabitEthernet1/0/5
               IIF-ID:  0x1025F40000000D1
          MAC Address:  000c.293d.75b2
         IPv6 Address:  2001:DB8:200:0:98CE:1111:4B48:67F7
         IPv4 Address:  172.20.200.2
            User-Name:  employee1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC14FE6500000FBF76C6E352
      Acct Session ID:  0x00000FBF
               Handle:  0xFB000013
       Current Policy:  POLICY_Gi1/0/5


Server Policies:
             Template:  FinanceServiceTemplate (priority 100)
           Vlan Group:  Vlan: 200
              ACS ACL:  xACSACLx-IP-PERMIT-ACCESS-5260ab88

    Method status list:
      Method    State
      dot1x     Authc Success
```

ACS monitoring logs:



Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
#ACSACL#-IP-PERMIT-ACCESS-5260ab88				C3850-1	172.20.254.101			acs
FinanceServiceTemplate		Serv-Templates	PAP_ASCII	C3850-1	172.20.254.101			acs
employee1	00-0C-29-3D-75-B2	802-1X_ACCESS	PEAP (EAP-MSCHAPv2)	C3850-1	172.20.254.101	GigabitEthernet1/0/5		acs

Platform Support Matrix

Platform	Policy Aware IBNS (New-Style)	Critical Voice VLAN	Per MAC VLANs	IPv6 Capability (Service-template w IPv6 ACL, WebAuth)	Minimum Software version
Catalyst 2960-S, 2960-SF, 2960-C, 2960-Plus and 3560-C	Yes	Yes	No	No	15.2(1)E
Catalyst 3560-X and 3750-X	Yes	Yes	No	No	15.2(1)E
Catalyst 3650 and 3850	Yes	Yes	Yes	Yes	3.3.0SE
Catalyst 4948E, 4948E-F, 4500/4500E Sup6E/Sup6-LE	Yes	Yes	No	No	15.2(1)E
Catalyst 4500X, 4500E Sup7E/Sup7-LE	Yes	Yes	No	No	3.5.0E
Catalyst 6500/E Sup720/Sup2T, Catalyst 4500E Sup8E	No	Yes*	No	No	—

* Legacy mode

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.**

Printed in USA C11-729965-00 11/13