

NAC: LDAP Integration with ACS Configuration Example

Document ID: 107285

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

Configuration

- Flow Chart Diagram
- Beacon Endpoint Profiler System Configuration for MAB
- ACS Configuration for MAB and Utilization of Beacon as an External User Database
- Configure Cisco SecureGroup(s)
- ACS External User Database Configuration
- Network Access Profile Configuration
- Switch Configuration for MAC Authentication Bypass

Verify

Related Information

Introduction

This document provides a sample configuration of steps in order to configure Beacon and ACS to enable Cisco devices configured for MAB to effectively and efficiently authenticate non-802.1X capable devices in the authenticated network.

Cisco has implemented a feature called MAC Authentication Bypass (MAB) on their switches as well as requisite support in ACS in order to accommodate endpoints in the 802.1X-enabled networks that are unable to authenticate through 802.1X. This functionality ensures that endpoints that attempt connection to the 802.1X-enabled network that are not equipped with 802.1X functionality, for example, do not have a functional 802.1X supplicant, can be authenticated prior to admission, as well as have basic network usage policy enforced throughout their connection.

MAB enables the network to be configured to admit identified devices with the use of their MAC address as the primary credential when the device fails to participate in the 802.1X protocol. In order for MAB to be deployed and utilized effectively, the environment must have a means to identify the devices in the environment that are not capable of 802.1X authentication, and maintain an up-to-date database of these devices over time as moves, adds and changes occur. This list needs to be populated and maintained in the Authentication server (ACS) manually, or through some alternative means in order to ensure that the devices that authenticate on MAC is completed and valid at any point in time.

The Beacon Endpoint Profiler can automate the process of the identification of non-authenticating endpoints, those without 802.1X supplicants, and the maintainance of the validity of these endpoints in networks of varying scale on the Endpoint Profiling and Behavior Monitoring functionality. Through a standard LDAP interface, the Beacon system can serve as an External Database or Directory of the endpoints to be authenticated through MAB. When a MAB request is received from the edge infrastructure, ACS can query the Beacon system in order to determine whether or not a given endpoint should be admitted to the network based on most current information about the endpoint known by Beacon, in order to prevent the need for

manual configuration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco Switch 3750 that runs 12.2(25)SEE2
- Cisco Secure Access Control Server for Windows 4.1

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

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

MAB is an essential functionality for dynamic support of devices such as printers, IP Phones, fax machines and other non-802.1X capable devices in the environment post-802.1X deployment. Without a MAB capability, network access ports that provide connectivity to non-802.1X capable endpoints must be provisioned statically in order to not attempt 802.1X authentication or through the use of other features that provide very limited policy options. For obvious reasons, this is inherently not scalable in large enterprise environments. With MAB enabled in conjunction with 802.1X on all access ports, known non-802.1X capable endpoints can be moved anywhere in the environment and still reliably (and securely) connect to the network. Because the devices admitted to the network are being authenticated, different policies can be applied to different devices

In addition, non-802.1X capable endpoints that are not known in the environment, such as laptops that belong to visitors or contractors, can be provided restricted access to the network through MAB if desired.

As the name suggests, MAC Authentication Bypass utilizes the MAC address of the endpoint as the primary credential. With MAC Authentication Bypass enabled on an access port, if an endpoint connects and fails to respond to the 802.1X authentication challenge, the port reverts to MAB mode. The switch that attempts MAB of an endpoint makes a standard RADIUS request to ACS with the MAC of the station. It attempts to connect to the network and requests authentication of the endpoint from ACS prior to admission of the endpoint to the network.

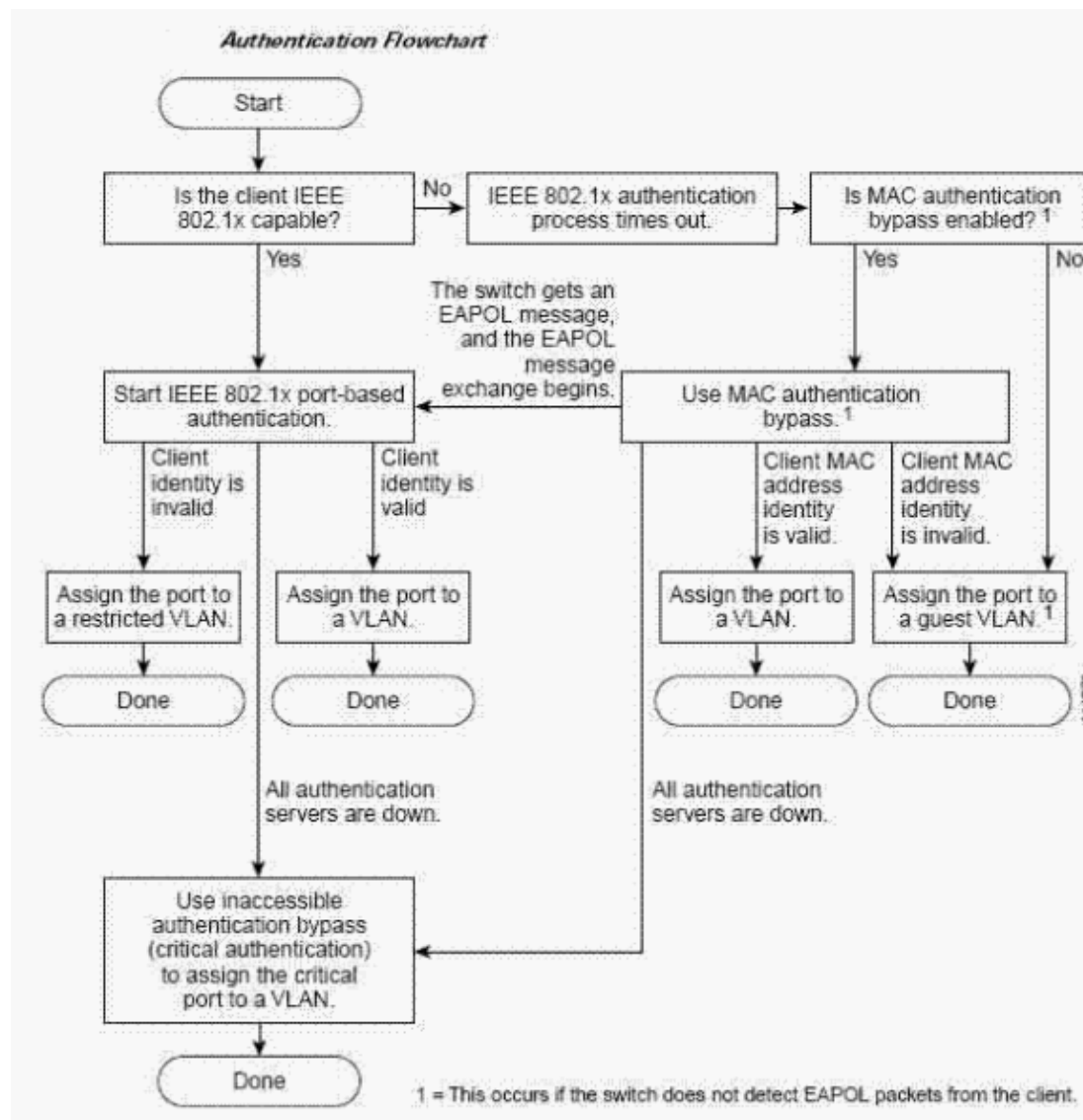
Configuration

Flow Chart Diagram

This flowchart taken from Cisco Systems documentation illustrates how MAB is utilized in conjunction with 802.1X authentication on Cisco edge infrastructure as new endpoints attempt to connect to the network.

This document uses this Flow Chart work flow:

Figure 1: Authentication Flow



ACS can be configured to utilize either its own internal database or an external LDAP server in order to authenticate MAC address user requests. The Beacon Endpoint Profiler system is fully LDAP-enabled by default and can be utilized by ACS in order to authenticate MAC address user requests through the standard LDAP functionality. Because Beacon automates both the discovery as well as Profiling of all endpoints on the network, ACS can query Beacon through LDAP in order to determine if the MAC should be admitted to the network, and into which group the endpoint should be mapped. This significantly automates and enhances the MAC Authentication Bypass feature, particularly in large enterprise environments.

Through the Behavioral Monitoring functionality provided by Beacon, devices that are observed to behave inconsistently with the Profiles enabled for MAB are transitioned out of 4 LDAP-enabled profiles and subsequently fail the next regular re-authentication attempt.

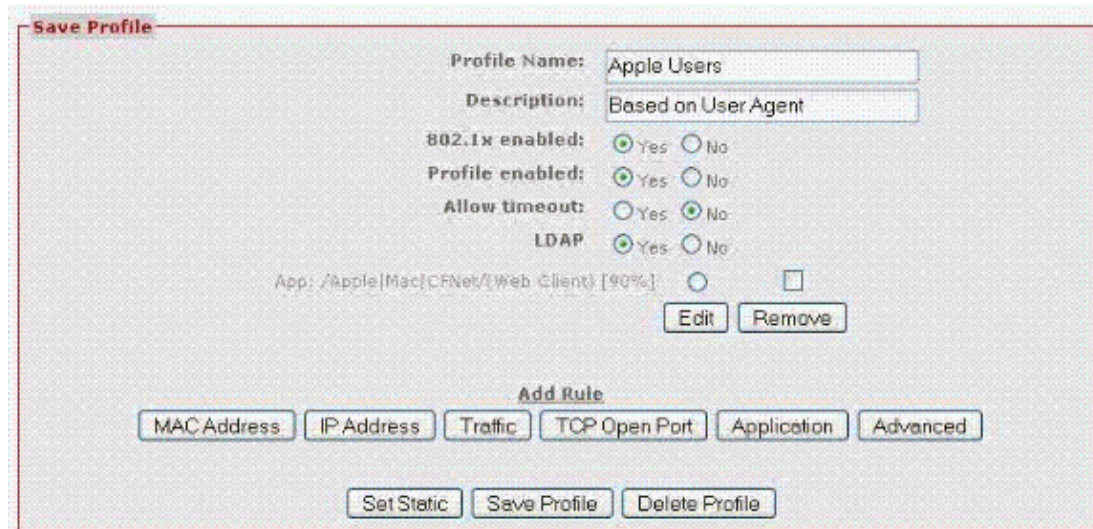
Beacon Endpoint Profiler System Configuration for MAB

Configuration of the Beacon system for integration with ACS for the purposes of MAB support is straightforward as the LDAP functionality is enabled by default. The primary configuration task is to identify the Profiles that contain endpoints that are desired to be authenticated through MAB in the environment, and

then enable those Profiles for LDAP. Typically, the Beacon Profiles, which contain devices owned by the organization, should be provided network access when seen on a port yet are known to be unable to authenticate through 802.1X. Typically these are Profiles that contain printers, IP Phones or manageable UPSs as common examples.

If printers profiled by Beacon were placed in a profile named *Printers*, and IP Phones in a profile named *IP Phones*, for example, then these profiles need to be enabled for LDAP such that the endpoints placed in those Profiles result in successful authentication as known IP Phone and Printers in the environment through MAB. If you enable a profile for LDAP, this requires that the LDAP radio button in the Endpoint Profile configuration be selected, as shown in this example:

Figure 2: Enable a Profile for LDAP



When ACS proxies MAC authentication to Beacon through LDAP, the query consists of two sub queries, both of which must return a valid, non-null result. The first query to Beacon is whether or not the MAC is known to Beacon, for example, if it has been discovered and added to the Beacon database. If the endpoint has yet to be discovered by Beacon, the endpoint is considered to be unknown. The second query is not necessary in the case of endpoints that Beacon has not discovered and are not in its database. If the endpoint has been discovered and is in the Beacon database, the next query is to determine the current Profile of the endpoint. If an endpoint has yet to be profiled or is currently in a profile not 5 enabled for LDAP, the unknown result is returned to ACS, and the authentication of the endpoint by Beacon fails. It depends on how ACS is configured that this can result in the device with the denial of access to the network altogether, or be given a Policy that is appropriate for unknown or guest devices.

Only in the case where the MAC is an endpoint that Beacon has discovered and placed in an LDAP-enabled Profile, the response is that the endpoint is known and Profiled by Beacon be returned to ACS. Most importantly, for these endpoints Beacon provides the current Profile name, which enables ACS to map known endpoints to Cisco SecureAccess Groups. This enables a granular Policy determination made, as granular as a separate Policy for each Beacon LDAP-enabled Profile, if desired.

ACS Configuration for MAB and Utilization of Beacon as an External User Database

Configuration of ACS for MAB and the utilization of Beacon as an External User Database requires three distinct steps. The order illustrated in this document follows a workflow that is efficient when it performs the MAB configuration in its entirety, and can vary for systems that have been in operation with other authentication modes already configured.

Configure Cisco SecureGroup(s)

When you attempt MAB for a particular endpoint that attempts to connect to the network, ACS queries Beacon on LDAP in order to determine if Beacon has discovered the MAC, and what Profile Beacon has currently placed the MAC address in as described earlier in the document.

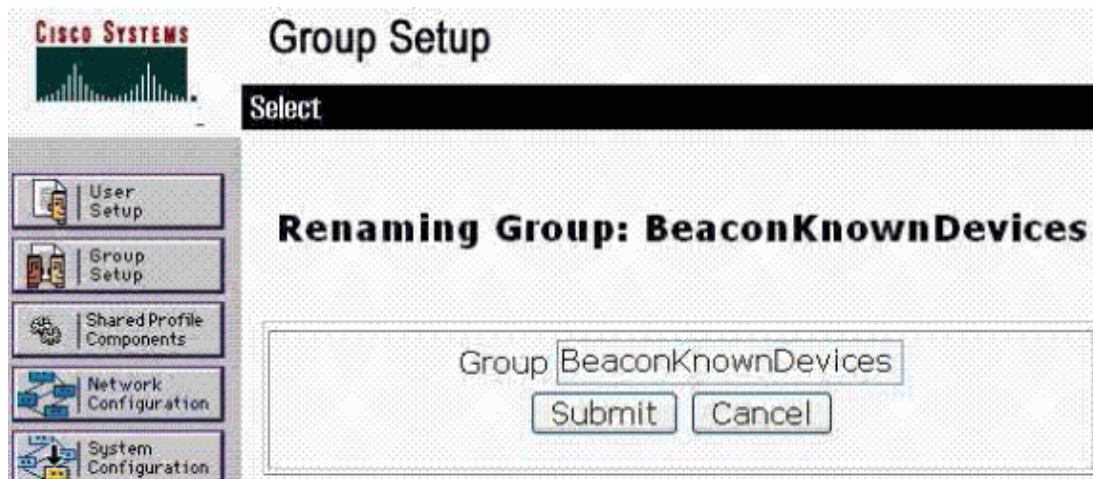
The Cisco SecureGroup mechanism with ACS can be used to both authenticate and apply policy to endpoints that have been discovered and Profiled by Beacon through MAB, as well as authentication failures those devices not known or not currently Profiled by Beacon.

For example, a Group can be added to the ACS configuration for endpoints discovered and Profiled by Beacon and called *BeaconKnownDevices*, and another group *BeaconUnknownDevices* added for devices that are not currently known by Beacon. Either Beacon has not discovered the MAC, or has not currently profiled it into an LDAP-enabled profile. As shown later in this document, the Groups enable the application of policy to endpoints as they attempt to join the network.

Note that in the example outlined in this document, only two groups, BeaconKnown and BeaconUnknown are configured. But it is possible to create multiple SecureGroups for endpoints discovered and profiled by Beacon, as many as one for each LDAP-enabled profile in Beacon, each with different policy parameters such as VLAN assignment. In addition, the BeaconUnknown device group can be configured to deny all access to endpoints that have yet to be discovered or placed in a Profile enabled for LDAP by 6 Beacon. This is accomplished if you choose the Group Disabled checkbox in the parameters of the BeaconUnknownDevices group configuration window.

Group creation on ACS is initiated from the Group Setup button in the ACS user interface. Choose one of the available Groups, and then choose the **Rename Group** button in order to change the Group Name to KnownBeaconDevices as shown in this example. Click **Submit** in order to save the change.

Figure 3: Edit CiscoSecure Group



Choose **Edit Settings** in order to edit the settings of the Group. Edit the parameters of the BeaconKnownDevices group as desired. For the purposes of the example in this document, the group parameters that are changed include only the IETF Radius Attributes, found at the bottom of the page.

Specifically you designate that devices authenticated to this group, the MAC addresses that Beacon has Profiled to the Profiles selected for MAB and enabled for LDAP, have policy parameters returned to the authenticating switch that enables admission of the endpoints to the network on the proper VLAN. In order to do this, RADIUS attributes 064 Tunnel-Type, 065 Tunnel-Medium-Type, and 081 Tunnel-Private-Group-ID are set to result in endpoints being placed on the desired VLAN, as shown in Figure 4.

Ensure that the checkboxes next to each RADIUS attribute is checked.

Figure 4: Group VLAN Attributes

The screenshot shows the Cisco Systems Group Setup interface. The 'Jump To' dropdown is set to 'Access Restrictions'. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main configuration area includes the following RADIUS attributes:

- [062] Port-Limit: Value 0
- [063] Login-LAT-Port: Value [empty]
- [064] Tunnel-Type:
 - Tag 1: Value VLAN
 - Tag 2: Value [empty]
- [065] Tunnel-Medium-Type:
 - Tag 1: Value 802
 - Tag 2: Value [empty]
- [081] Tunnel-Private-Group-ID:
 - Tag 1: Value 10
 - Tag 2: Value [empty]

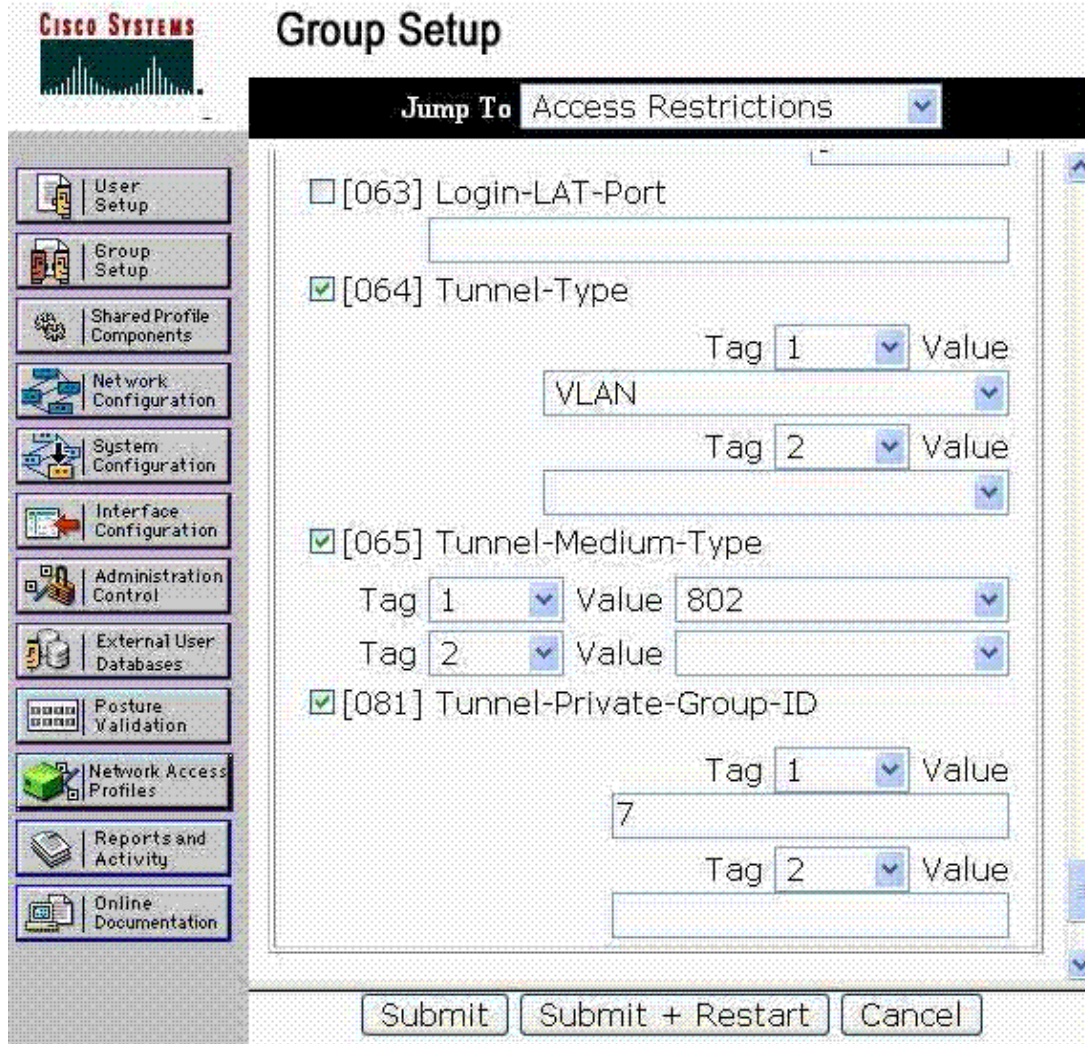
Buttons at the bottom: Submit, Submit + Restart, Cancel.

In the example shown, endpoints authenticated successfully by Beacon and subsequently assigned to the ACS BeaconKnownDevices group are placed on VLAN 10, the authorized VLAN in the example network configuration, during the connection to the network and successfully authenticated on MAB by ACS with the use of Beacon as an External User Database.

Similarly the BeaconUnknownDevices group is created for devices that are not currently known by Beacon as shown. Again, if these devices should get no access to the network, simply check the **Group Disabled** checkbox at the top of the form. Endpoints that have not been discovered by Beacon or are not currently Profiled by Beacon into an LDAP-enabled Profile fail MAB and are not admitted to the network.

This figure shows the alternative than the use of the Group Disabled checkbox. In this case, endpoints that cannot be authenticated by Beacon are assigned to a group that is enabled, but has a different policy than that for endpoints that are known. Refer to Figure 5.

Figure 5: VLAN Parameters for BeaconUnknownDevices



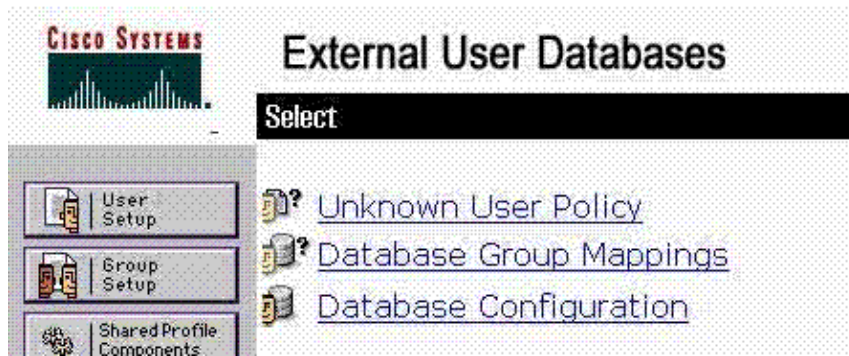
Note that for unknown devices in this example, they are admitted to the network but are relegated to a Guest or Restricted VLAN, VLAN 7. In the example network, VLAN 7 is the Guest VLAN, which allows endpoints only Internet access, and prohibits access to internal resources.

When ACS requests authentication from Beacon of a MAC of an endpoint that has yet to be discovered or Profiled by Beacon, ACS places the MAC in this group and returns the result to the authenticating switch enabled for MAB.

ACS External User Database Configuration

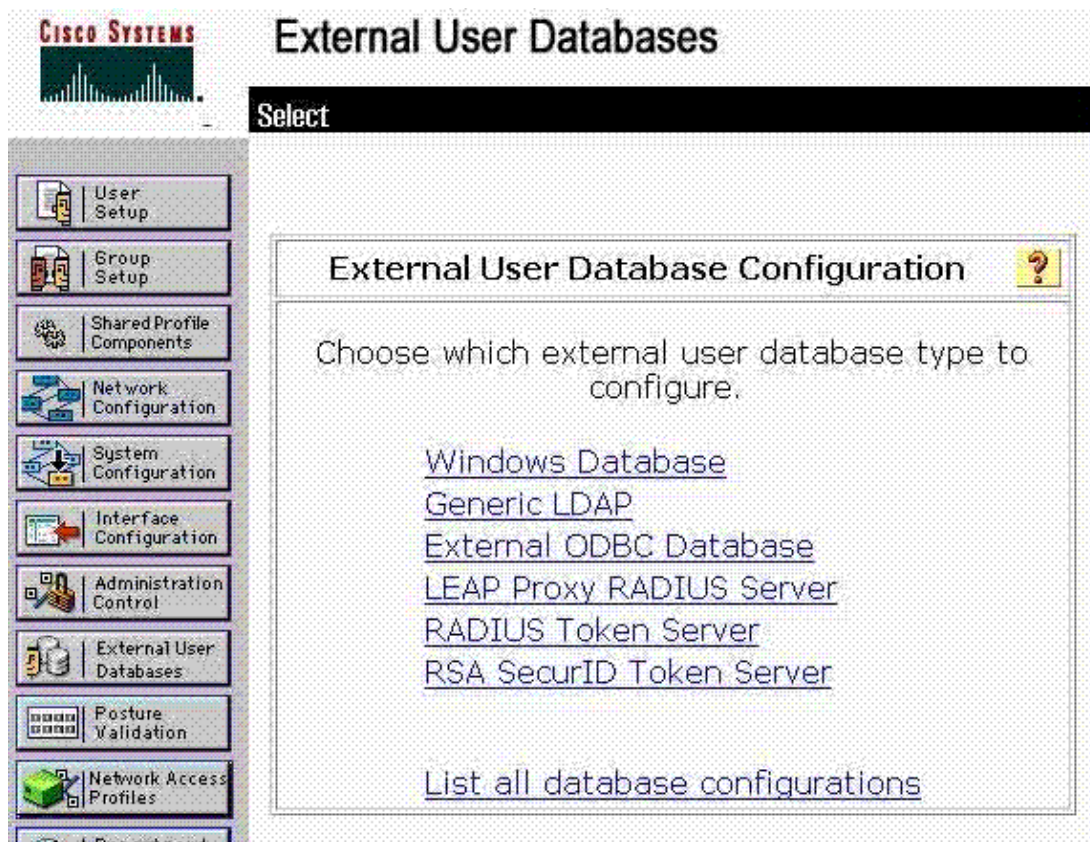
ACS must be configured to proxy MAB requests from access switches to Beacon via LDAP. This requires that the ACS configuration includes the Beacon system as a Generic LDAP External User Database. The steps outlined in this section illustrate how to add the 9 Beacon Endpoint Profiler system as an external user database to be queried by ACS when it receives MAB requests. Choose **External User Database** on the global navigation pane in order to bring up the External User Database window illustrated in Figure 6.

Figure 6: External DB Configuration Main Screen



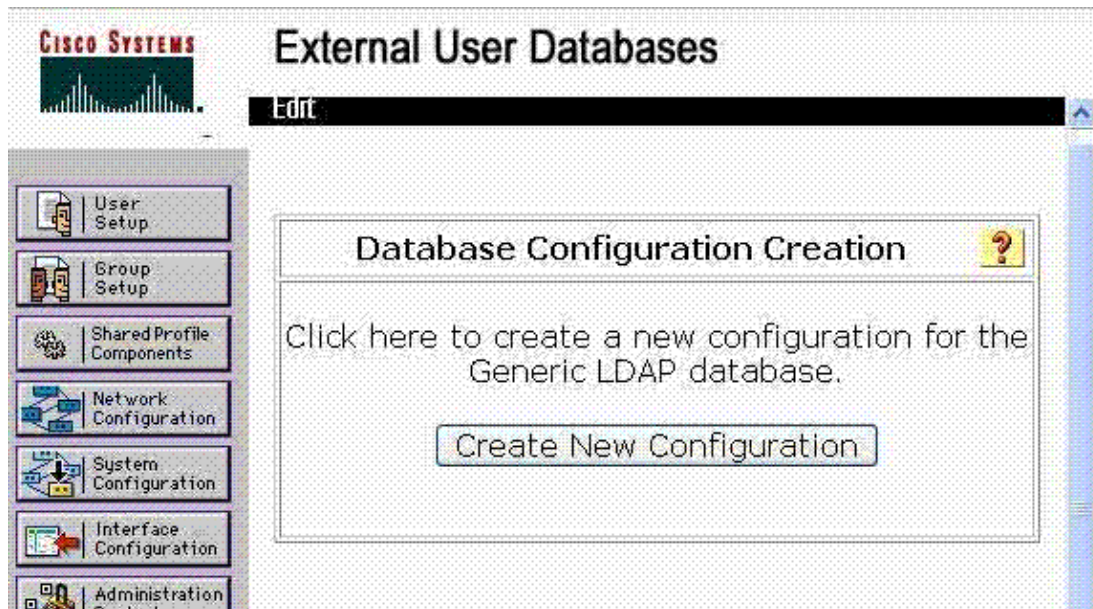
The first task in the configuration of Beacon as an External User Database is to add the Beacon system as a Generic LDAP external user data base. Choose **Database Configuration** in order for the window illustrated in Figure 7 appear.

Figure 7: ACS External User Database Configuration



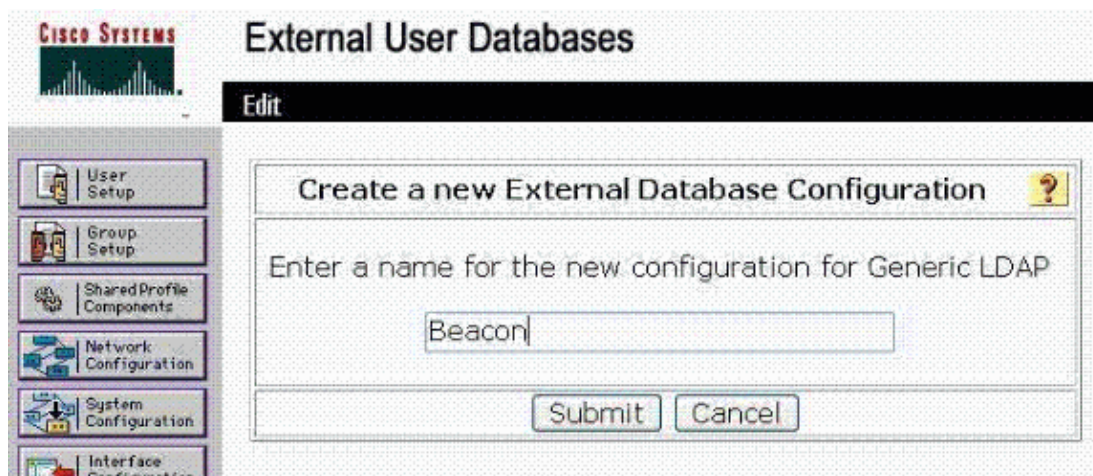
Choose **Generic LDAP** in order to open the form used to add the Beacon Endpoint Profiler system as external user DB in the ACS configuration. This window appears to enable the creation of a new External User Database Configuration of the type Generic LDAP.

Figure 8: Database Configuration Creation



Choose the **Create New Configuration** button in order to create the Generic LDAP database for Beacon. This window appears and allows the new External Database to be named.

Figure 9: Name Beacon External User Database



Enter a name for the Beacon Generic LDAP external database that allows it to be easily differentiated from other external databases in the configuration. Choose **Submit** in order to move onto entry of the required LDAP parameters that enable communication between 11 ACS and Beacon for the purpose of the authentication of MAC addresses with the use of Beacon database information.

Figure 10 illustrates the Common LDAP Configuration parameters that must be entered for the Beacon Generic LDAP external user database that is added to the ACS configuration. Note that these parameters provide ACS with the information it requires in order to query Beacon through LDAP. These parameters should be entered exactly as shown in this figure in order to facilitate communication between ACS and the Beacon Endpoint Profiler.

Figure 10: Common LDAP Configuration for Beacon

CISCO SYSTEMS External User Databases

Common LDAP Configuration

User Directory Subtree	o=beacon
Group Directory Subtree	o=beacon
UserObjectType	macAddress
UserObjectClass	IEEE802Device
GroupObjectType	cn
GroupObjectClass	GroupOfUniqueNames
Group Attribute Name	UniqueMember
Server Timeout	30 seconds
On Timeout Use Secondary	<input type="checkbox"/>
Failback Retry Delay	0 minutes
Max. Admin Connections	40

Note: Use the password **GBSbeacon** for the LDAP bind password. The password is entered at bottom of form shown in Figure 11.

Figure 11: Beacon Server Parameters

Primary LDAP Server

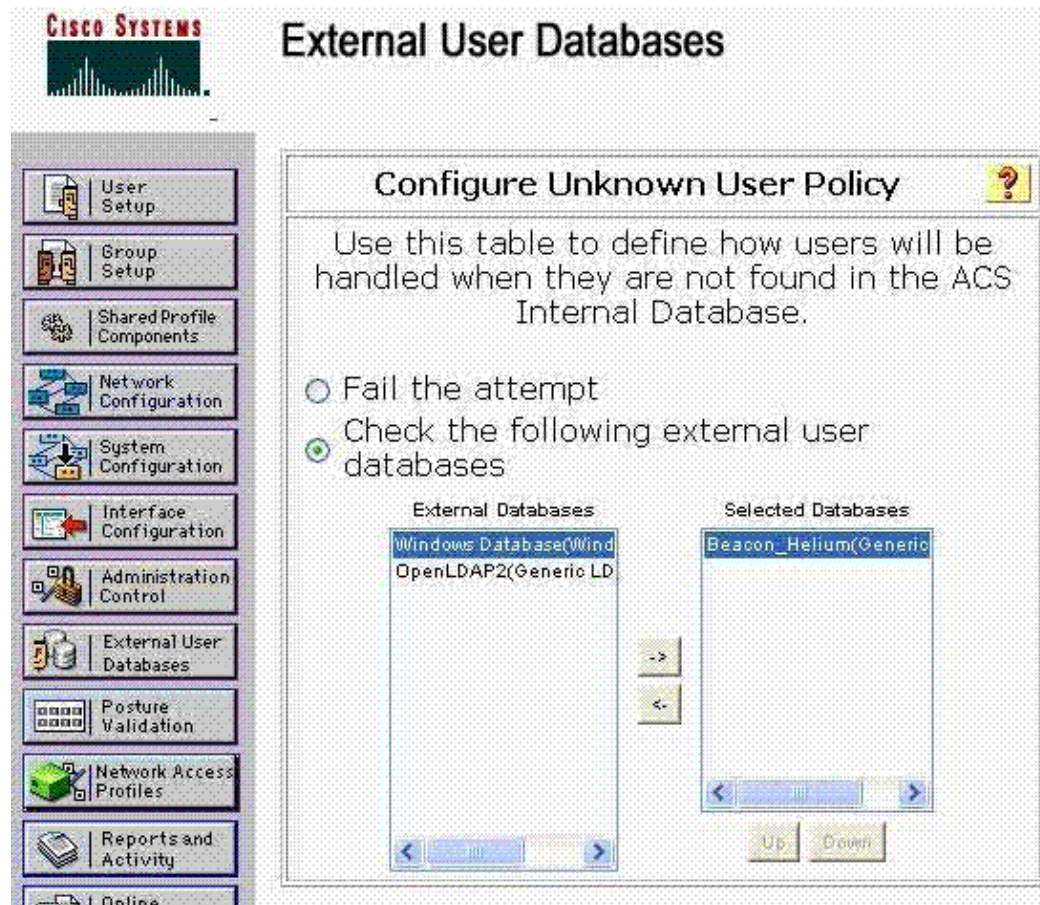
Hostname	10.10.0.204
Port	389 Default is 389
LDAP Version	<input checked="" type="checkbox"/> Use LDAP V3
Security	<input type="checkbox"/> Use Secure Authentication
<input type="radio"/> Trusted Root CA <input checked="" type="radio"/> Certificate DB Path	--- none selected --- [Empty field]
Admin DN	cn=root,o=beacon
Password	*****

The second configuration task associated with the configuration of Beacon as an External User Database is the configuration of the Unknown User Policy. The Unknown User Policy directs ACS to query the Beacon database whenever it receives an authentication request for a user, which is a MAC address in the case of MAB, that it does not have information for in its own database.

Note that in a typical ACS deployment, there can be existing external user databases configured and can already be configured to query those databases when unknown user credentials are submitted. The Beacon external user database must be added to the list in order to query it when switches request MAB of individual MAC addresses.

These figures outline the workflow for configuration of the Unknown User Policy, and the addition of Beacon as an External User Database to be queried. To, choose the **Unknown User Policy** link on the main External User Database page as illustrated in Figure 6 in order to begin the workflow.

Figure 12: Configure Unknown User Policy



Choose the Beacon Generic LDAP database added to the ACS configuration in the last step from list of External Databases to the left (Beacon_Helium) in example. Use -> in order to move to Selected Databases. Make sure you choose the **Check the following external user databases** radio button. This ensures that when switches submit MAC addresses for authentication to ACS, ACS queries Beacon in order to determine if the endpoint is known and it has current Profile, if any.

The final configuration task to add Beacon as an external user database is the completion of Database Group Mappings. Essentially this mapping ties together the CiscoSecure groups created, for example, BeaconKnownDevices and BeaconUnknownDevices, to successful and unsuccessful LDAP queries made to Beacon so that each MAB attempted by the switches results in the assignment of the endpoint to a CiscoSecure group by ACS. This enables ACS to respond to the switch whether or not the endpoint should be admitted to the network, and if admitted, what the policy such as VLAN attributes it should be.

Choose **Database Group Mappings** on the main External User Databases page as shown in Figure 6 in order to configure the mappings.

Figure 13: Database Group Mappings

External User Databases

Select

Unknown User Group Mappings

Choose the External User Database for which you want to configure the group mappings.

Name	Type
Windows Database	Windows Database
Beacon_Helium	Generic LDAP

When you choose the Beacon external user database created earlier in this section with the selection of the link, [Beacon_Helium](#) in the previous example, this displays the window illustrated in Figure 14. Note that all the Beacon Profiles enabled for LDAP within the Beacon system configuration as described in the first section of these configuration instructions are populated in the DS Groups that are available for selection to create mappings within ACS. If the Beacon Profile names enabled for LDAP are not shown in the ACS interface, this is indicative of a problem with the ACS LDAP configuration. Refer to the instructions on the configuration Beacon as an External User Database outlined earlier in this section, in particular the LDAP parameters.

Note that this is the interface that allows mapping of individual LDAP-enabled Profiles in Beacon with the CiscoSecure groups configured within ACS. The interface allows for the mapping of each individual Beacon LDAP-enabled Profile to a single CiscoSecure group. In this example, only a single group was created for known devices in LDAP-enabled Beacon Profiles: `BeaconKnownDevices`. But, multiple groups, each with its own policy parameters can be created in order to handle successful authentications differently dependent upon the current Beacon Profile of the device.

For example, a CiscoSecure group can be created for `BeaconKnownIPPhones`, which returned the VLAN attributes that assign endpoints in the IP Phone Profile in Beacon to the Phone VLAN when you join the network and authenticate through MAB.

Figure 14: Profile-to-Group Mapping

External User Databases

Create new group mapping for LDAP Users

Define LDAP group set

DS Groups

Lab Laptop
3Com Gear

Add to selected

Remove from selected

Selected

Apple Users

Up

Down

CiscoSecure group:

BeaconKnownDevices

Submit

Cancel

Choose one DS group (Beacon Profile with LDAP enabled), and assign endpoints in that Profile to the desired CiscoSecure group from drop-down menu. In the previous example, MAC addresses currently in the Apple Users Profile in Beacon are authenticated through MAB, placed in the BeaconKnownDevices that results in a successful authentication and placement in the User VLAN when you join the network.

Selecting submit brings up the listing of current Group Mappings on ACS when authenticating unknown users to the Beacon external user database.

Figure 15: List Group Mappings

External User Databases

Edit

Group Mappings for LDAP Users

LDAP groups	CiscoSecure group
Lab Laptop, *	BeaconKnownDevices
3Com Gear, Apple Users, Lab Laptop, *	BeaconKnownDevices
All other combinations	BeaconUnknownDevices

Note that the mappings explicitly made with the procedure previously described are listed in this view. Any DS Groups (Beacon LDAP-enabled Profiles) not explicitly mapped to a group, which includes endpoints that Beacon has not yet discovered or placed in an LDAP-enabled Profile fall in the All other combinations collector. Essentially this allows endpoints that Beacon cannot provide information about into a CiscoSecure group, for example, BeaconUnknownDevices. As previously outlined, this group can be disabled altogether which results in MAB failure, or as in the previous example, it can be designed in order to provide only limited connectivity to endpoints not known by Beacon.

All other combinations can be assigned a CiscoSecure Group (BeaconUnknownDevices) if you click on the **All other combinations** link in order to get this window:

Figure 16: Assigning a Group to All other combinations

External User Databases

Edit

Edit group mapping for LDAP Users

LDAP Groups:
All other combinations

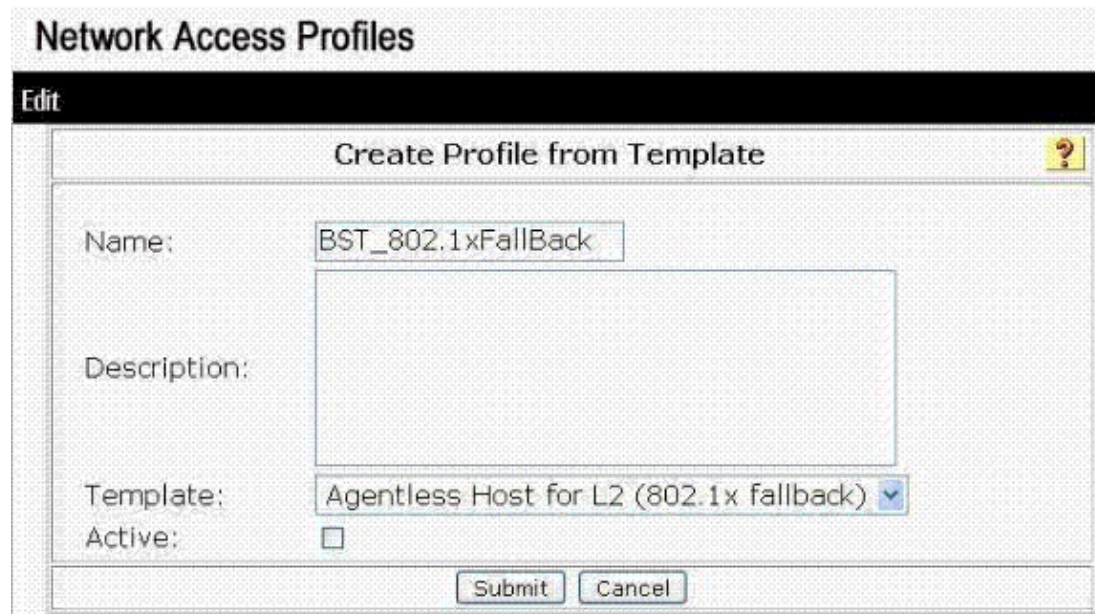
CiscoSecure group:
 

Network Access Profile Configuration

The last required step in ACS configuration for MAB to use the Beacon Endpoint Profiler system as a proxy is the configuration of a Network Access Profile for 802.1X fallback. Complete these steps outlined in order to configure the required Network Access Profile to complete the ACS Configuration such that MAB is configured and operates according to the configuration completed previously.

The Network Access Profile to be added is a Template Profile. Choose the **Network Access Profiles** from the global navigation page. Then choose **Add Template Profile** in order to bring up this form illustrated.

Figure 17: Add a Template Network Access Profile



The screenshot shows a web interface titled "Network Access Profiles" with an "Edit" tab. A modal window titled "Create Profile from Template" is open. It contains the following fields:

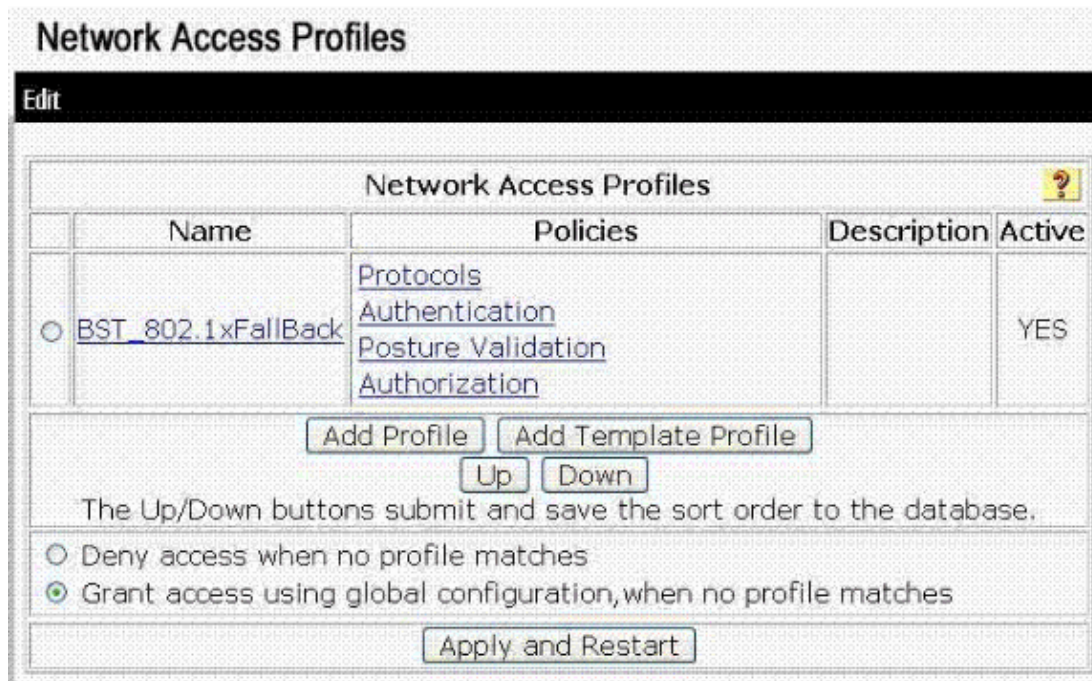
- Name:** A text input field containing "BST_802.1xFallBack".
- Description:** A large empty text area.
- Template:** A dropdown menu with "Agentless Host for L2 (802.1x fallback)" selected.
- Active:** An unchecked checkbox.

At the bottom of the modal are "Submit" and "Cancel" buttons.

Name the Network Access Profile in order to enable to distinguish it from others, and add a description if desired. The template for this profile is selected from the drop-down list. Ensure that **Agentless Host for L2 (802.1x Fallback)** is selected, and check the **Active** checkbox. Click the **Submit** button when finished in order to save the Network Access Profile.

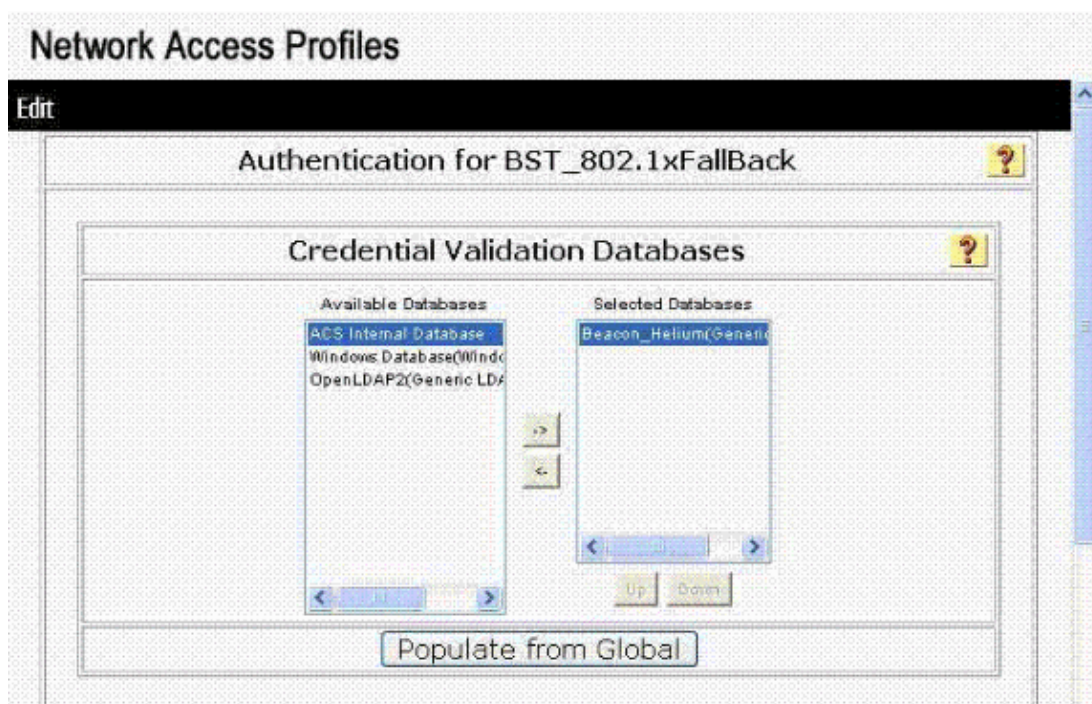
When you click submit, this form is presented that allows you to edit the parameters for the Profile just created as shown.

Figure 18: Edit NAP for MAB



The Authentication policy for the newly configured Profile must be configured in order to utilize the Beacon system as a Credential Validation Database. Choose the Authentication link in the Policies column for the newly-created Network Access Profile (802.1x FallBack in the example). These forms are presented.

Figure 19: Select Database for MAB



First, choose the Beacon external user database from the Available databases table and use the → button in order to add it to Selected Databases. Scroll down to the Authenticate MAC section of the form, and choose **LDAP Server** radio button. Choose the **Beacon** database from the drop-down list. Lastly, choose the **BeaconUnknownDevice** group for the default action as shown in the next figure.

Figure 20: Designate Beacon LDAP Server

Authenticate MAC with:

<input checked="" type="radio"/> LDAP Server:	Beacon_Helium(Generic LDAP) ▾						
<input type="radio"/> Internal ACS DB	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 50%;">MAC Addresses</th> <th style="width: 50%;">User Group</th> </tr> <tr> <td colspan="2" style="text-align: center;">No MAC Group Mappings</td> </tr> <tr> <td style="text-align: center;">Add</td> <td style="text-align: center;">Delete</td> </tr> </table>	MAC Addresses	User Group	No MAC Group Mappings		Add	Delete
MAC Addresses	User Group						
No MAC Group Mappings							
Add	Delete						

Default Action	
If Agentless request was not assigned a user-group:	5: BeaconUnknownDevices ▾

This step completes the required ACS configuration for MAC Authentication Bypass with Beacon as an External User Database. Restart the ACS service in order to ensure all configuration changes are committed to the running configuration.

The system should be ready to test MAB, if the switches are configured correctly. An endpoint currently in an LDAP-enabled Beacon Profile can be disconnected from the network and readmitted with the Policy parameters specified for the BeaconKnownDevices group.

Switch Configuration for MAC Authentication Bypass

This switch configuration provides an example configuration for 802.1X authentication with MAC Authentication Bypass enabled, and dynamic VLAN reassignment required in order to apply RADIUS attributes returned from ACS.

Switch
<pre> switch#show running-config ! version 12.2 no service pad service timestamps debug uptime service timestamps log datetime service password-encryption service sequence-numbers ! ! aaa new-model aaa authentication login default line aaa authentication enable default enable aaa authentication dot1x default group radius aaa authorization network default group radius aaa accounting dot1x default start-stop group radius ! aaa session-id common switch 1 provision ws-c3750g-24ts ip subnet-zero ip routing no ip domain-lookup </pre>

```
!  
!  
!  
!  
!  
!  
dot1x system-auth-control  
no file verify auto  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
interface Port-channel1  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,7,9,10  
!  
interface Port-channel2  
description LAG/trunk to einstein  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,10  
switchport mode trunk  
!  
interface Port-channel3  
description "LAG to Edison"  
switchport access vlan 5  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,11  
switchport mode trunk  
!  
interface GigabitEthernet1/0/1  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,7,9,10  
channel-group 1 mode passive  
!  
interface GigabitEthernet1/0/2  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,7,9,10  
channel-group 1 mode passive  
!  
interface GigabitEthernet1/0/3  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,7,9,10  
channel-group 1 mode passive  
!  
interface GigabitEthernet1/0/4  
switchport access vlan 7  
switchport mode access  
!  
interface GigabitEthernet1/0/5  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/6  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,7,9  
switchport mode trunk  
switchport nonegotiate  
!  
interface GigabitEthernet1/0/7  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,10  
switchport mode trunk  
channel-group 2 mode active
```

```
!  
interface GigabitEthernet1/0/8  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,10  
switchport mode trunk  
channel-group 2 mode active  
!  
interface GigabitEthernet1/0/9  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/10  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/11  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/12  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/13  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/14  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/15  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/16  
switchport access vlan 5  
switchport mode access  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/17  
switchport access vlan 5  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,11  
switchport mode trunk  
channel-group 3 mode active  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/18  
switchport access vlan 5  
switchport trunk encapsulation dot1q  
switchport trunk allowed vlan 5,9,11  
switchport mode trunk  
channel-group 3 mode active  
spanning-tree portfast  
!  
interface GigabitEthernet1/0/19  
switchport mode access  
dot1x mac-auth-bypass
```

```
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 10
dot1x timeout reauth-period 60
dot1x timeout tx-period 10
dot1x timeout supp-timeout 10
dot1x max-req 1
dot1x reauthentication
dot1x auth-fail max-attempts 1
spanning-tree portfast
!
interface GigabitEthernet1/0/20
switchport mode access
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 10
dot1x timeout reauth-period 60
dot1x timeout tx-period 10
dot1x timeout supp-timeout 10
dot1x max-req 1
dot1x reauthentication
dot1x auth-fail max-attempts 1
spanning-tree portfast
!
interface GigabitEthernet1/0/21
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/22
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/23
switchport access vlan 10
spanning-tree portfast
!
interface GigabitEthernet1/0/24
switchport access vlan 10
spanning-tree portfast
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
no ip address
shutdown
!
interface Vlan5
ip address 10.1.1.10 255.255.255.0
!
interface Vlan9
ip address 10.9.0.1 255.255.0.0
!
interface Vlan10
ip address 10.10.0.1 255.255.0.0
ip helper-address 10.1.1.1
ip helper-address 10.10.0.204
!
```

```
interface Vlan11
ip address 10.11.0.1 255.255.0.0
ip helper-address 10.1.1.1
ip helper-address 10.10.0.204
!
ip default-gateway 10.1.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.30.0.0 255.255.0.0 10.10.0.2
ip route 10.40.0.0 255.255.0.0 10.10.0.2
ip http server
ip http secure-server
!
!
snmp-server community public RW
snmp-server host 10.1.1.191 public
radius-server host 10.10.0.100 auth-port 1645 acct-port 1646 key 7
05090A1A245F5E1B0C0612
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
password 7 02020D550C240E351F1B
line vty 0 4
password 7 00001A0803790A125C74
line vty 5 15
password 7 00001A0803790A125C74
!
end
```

Verify

There is currently no verification procedure available for this configuration.

Related Information

- [Cisco NAC Appliance \(Clean Access\)](#)
 - [Cisco Secure Access Control Server for Windows](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 04, 2008

Document ID: 107285
