# NAC: LDAP Integration with ACS 5.x and Later Configuration Example

## Document ID: 113566

## Contents



# Introduction

This document provides a sample configuration in order to configure Beacon and Cisco Secure Access Control System (ACS) 5.x and later to enable Cisco devices configured for MAC Authentication Bypass (MAB) to effectively and efficiently authenticate non−802.1X capable devices in the authenticated network.

Cisco has implemented a feature called MAB on their switches, as well as requisite support in ACS, in order to accommodate endpoints in the 802.1X−enabled networks that cannot authenticate through 802.1X. This functionality ensures that endpoints attempting to connect 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 before 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 are 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 maintenance 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, the ACS can query the Beacon system in order to determine whether or not a given endpoint should be admitted to the network based on the most current information about the endpoint known by Beacon. This prevents the need

for manual configuration.

For a similar configuration using versions earlier than ACS 5.x, refer to NAC: LDAP Integration with ACS Configuration Example.

# 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 3750 Switch that runs Cisco IOS® Software Release 12.2(25)SEE2
- Cisco Secure ACS 5.x and later

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 MAB 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 before admission of the endpoint to the network.

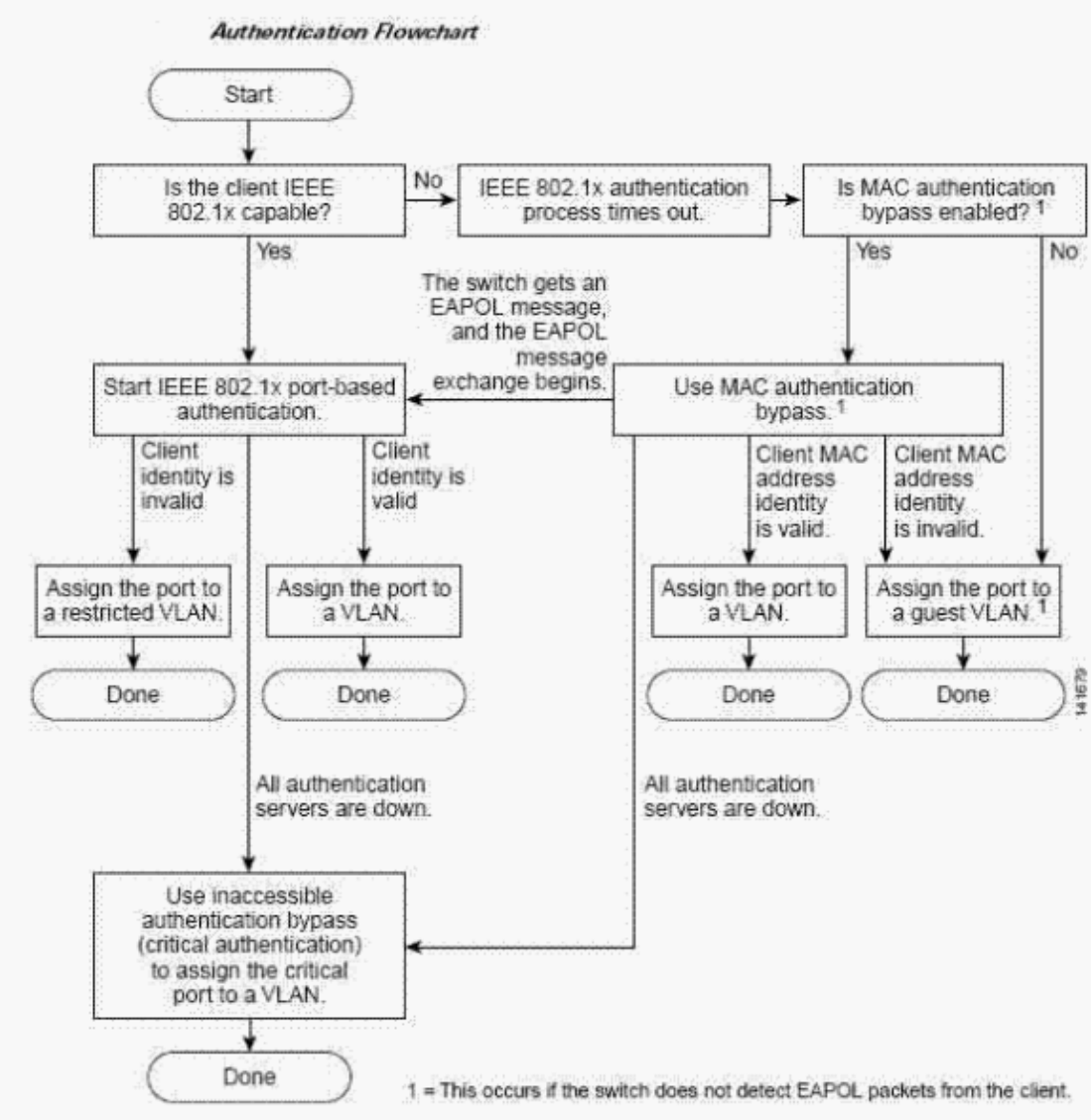
# Configuration

## Flowchart Diagram

This flowchart 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 Flowchart workflow:

**Figure 1: Authentication Flow**




The 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 the 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, the ACS can query Beacon through LDAP in order to determine if the MAC should be admitted to the network, and which group the endpoint should be mapped. This significantly automates and enhances the MAB feature, particularly in large enterprise environments.

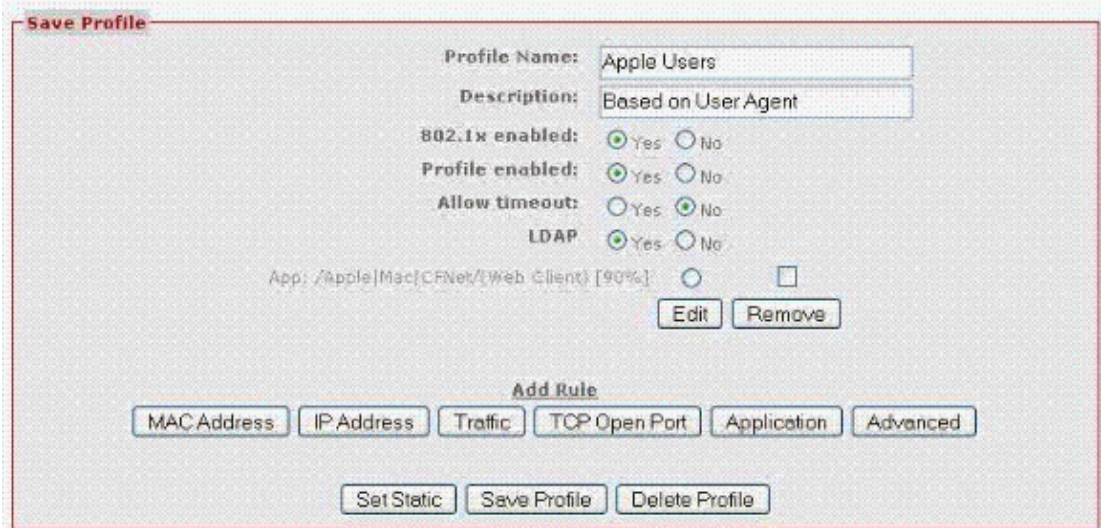
Through the Behavioral Monitoring functionality provided by Beacon, devices that are observed to behave inconsistently with the Profiles enabled for MAB are transitioned out of 4 LDAP−enabled profiles and subsequently fail the next regular re−authentication attempt.

## 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, must 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 choosing the LDAP radio button in the Endpoint Profile configuration, as shown in this example:

**Figure 2: Enable a Profile for LDAP**




When the ACS proxies MAC authentication to Beacon through LDAP, the query consists of two sub queries. Both of these 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 the ACS, and the authentication of the endpoint by Beacon fails. It depends on how the 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. This 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.

When you attempt MAB for a particular endpoint that attempts to connect to the network, the 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.

In this document, two separate profiles are created:

- BeaconKnownDevices for the endpoints discovered and Profiled by Beacon
- BeaconUnknownDevices for devices that are not currently known by Beacon

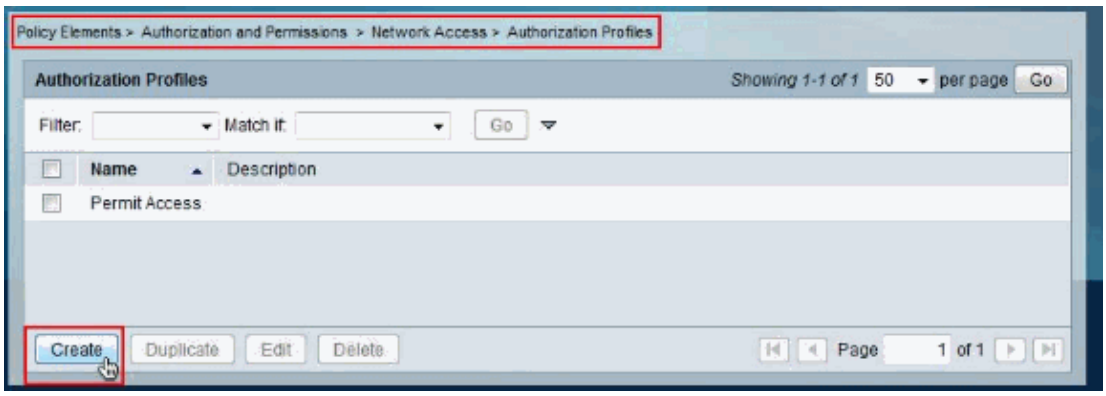
Either Beacon has not discovered the MAC, or has not currently profiled it to an LDAP−enabled profile. BeaconKnownDevices profile will put the endpoints in VLAN 10 and the BeaconUnkownDevices profile will put the endpoints in VLAN 7.

Later in this document, an LDAP connection to the Beacon Endpoint Profiler from ACS is created and groups are chosen from the Beacon Endpoint Profiler based on which endpoints will be considered as BeaconKnown devices, and will be assigned the BeaconKnownDevices profile (which will put them in VLAN 10). All the unknown devices that either Beacon has not discovered the MAC, or has not currently profiled it into an LDAP−enabled profile will be assigned the BeaconUnkownDevices profile (which will put them in VLAN 7).

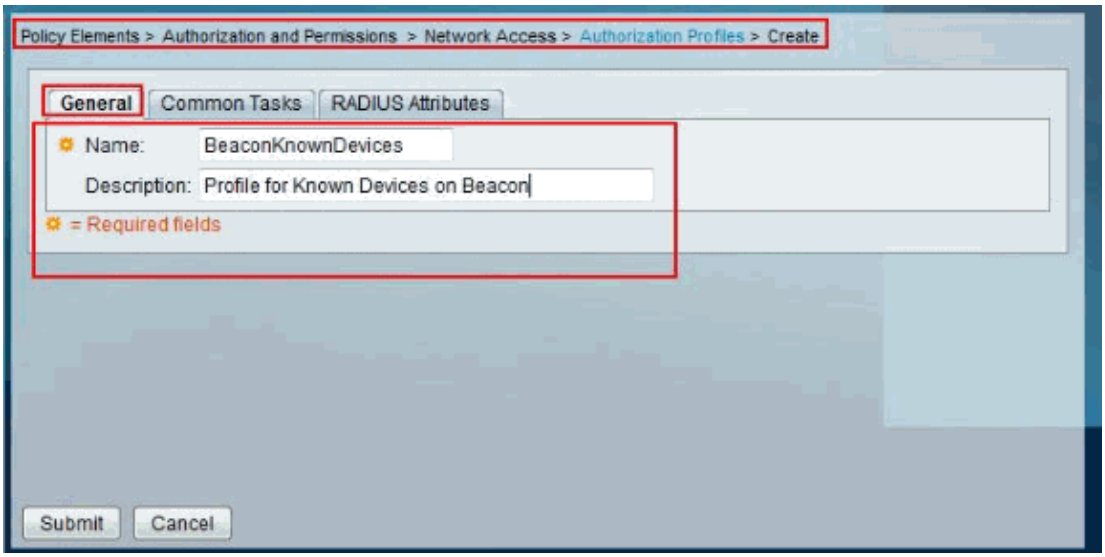
## Create an Authorization Profile

Complete these steps in order to create an Authorization Profile:

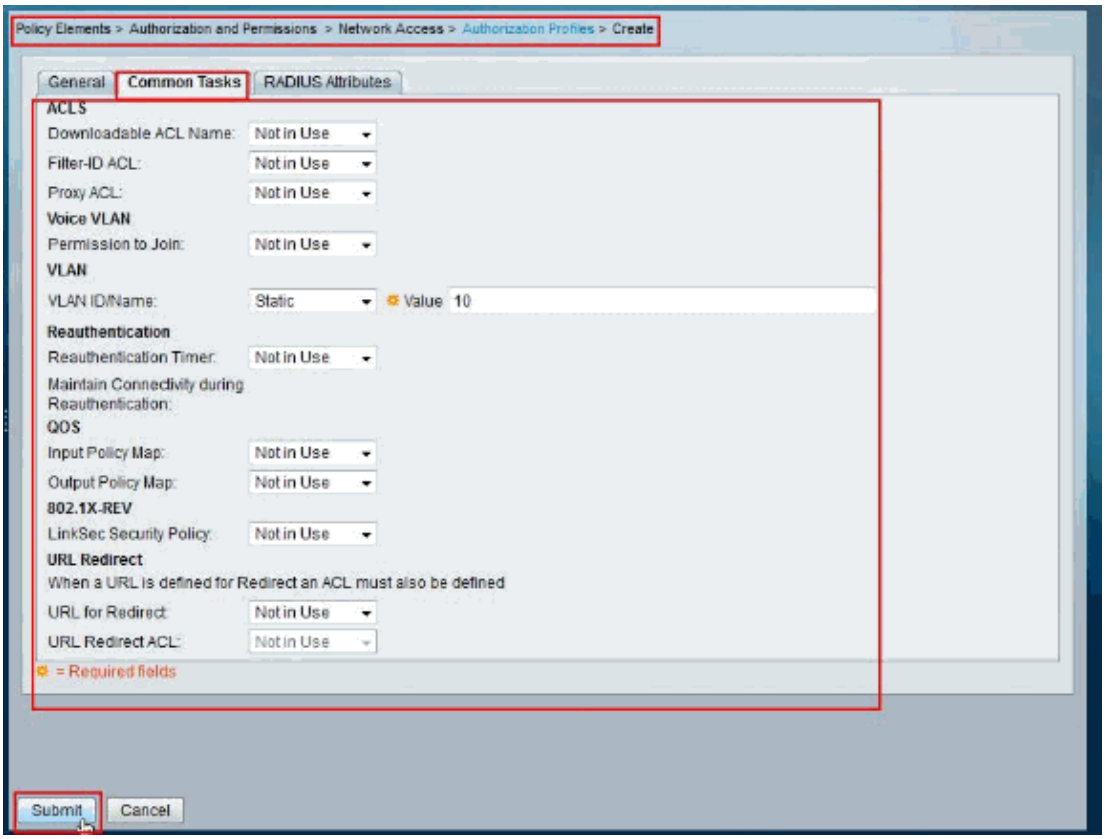
1. Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create** to create a new Authorization Profile.



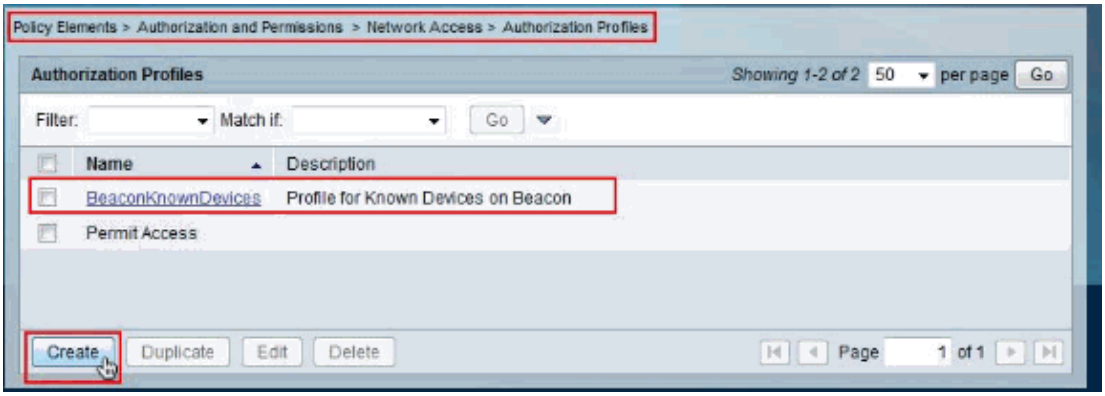

2. Provide the **Name** of the new Authorization Profile.



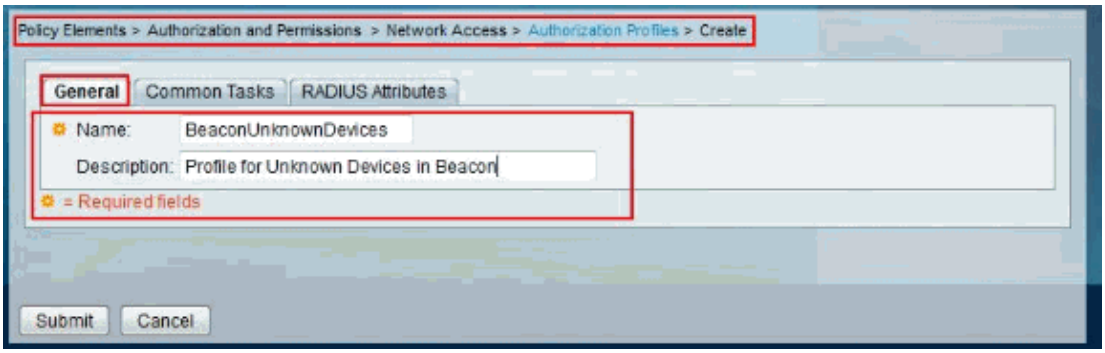

3. In the **Common Tasks** tab set the **VLAN to Static** with the **Value** as **10**. Then, click **Submit**.



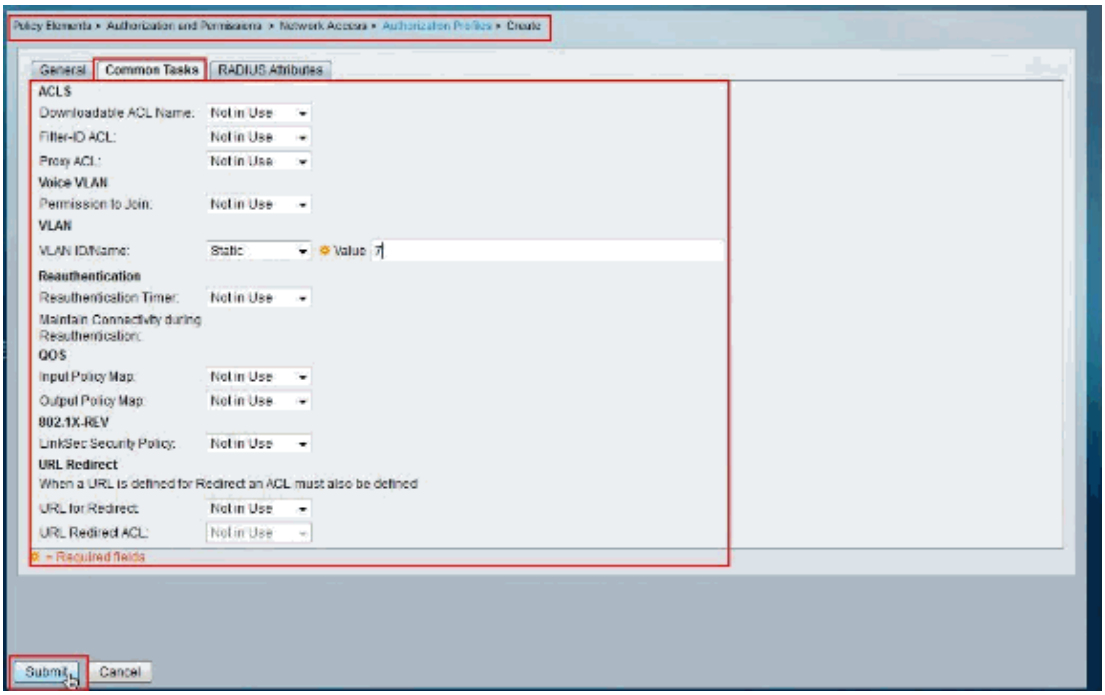

4. Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles** and click **Create** to create a new Authorization Profile.




5. Provide the **Name** of the new Authorization Profile.



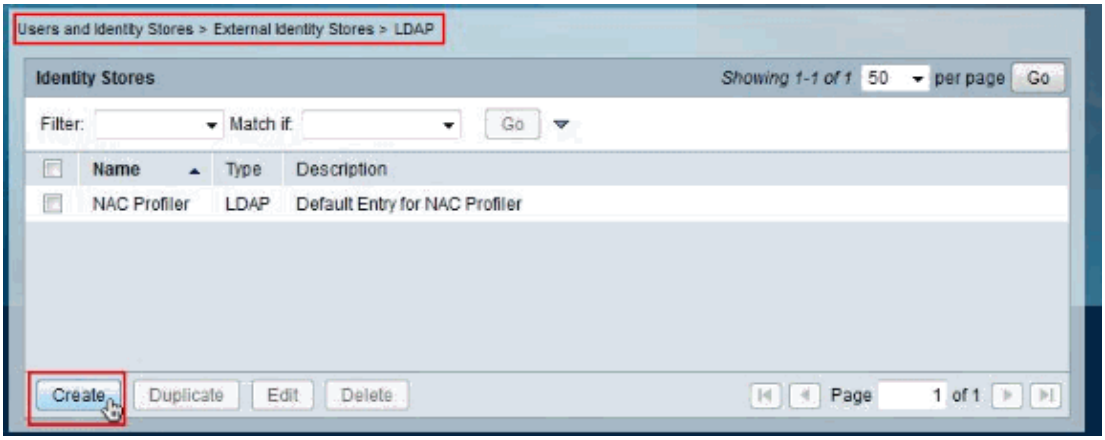

6. In the **Common Tasks** tab set the **VLAN** to **Static** with the **Value** as **7**. Then, click **Submit**.



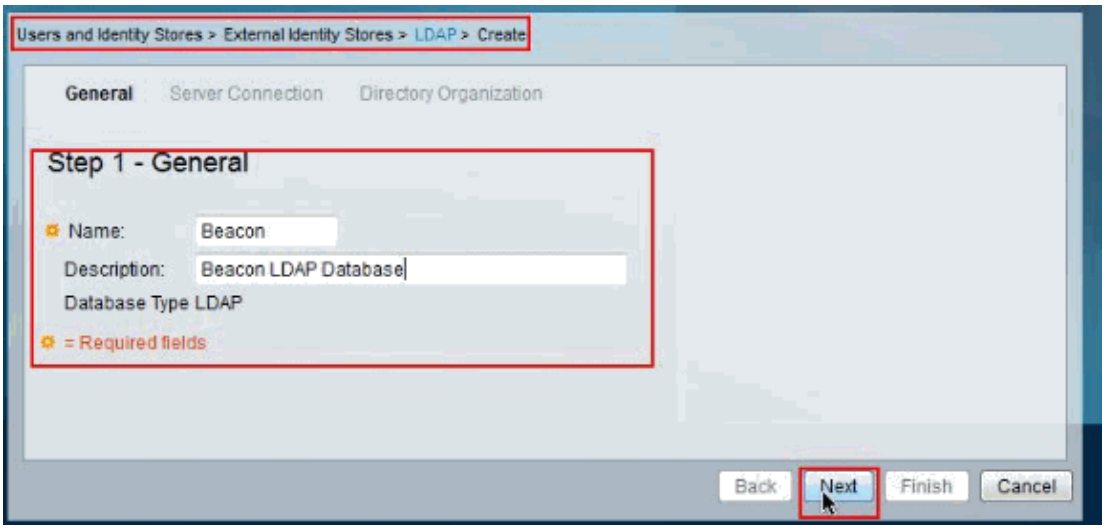

## Create an LDAP Database Connection

Complete the steps in order to create an LDAP database connection:

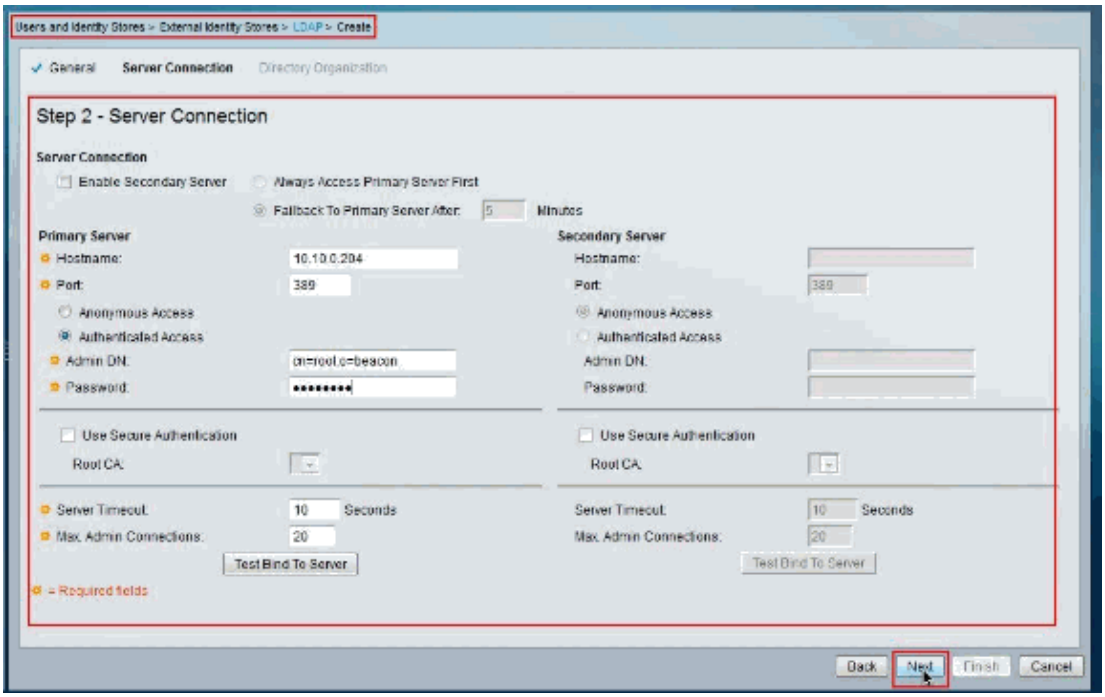
1. Choose **Users and Identity Stores > External Identity Stores > LDAP** and click **Create** to create a new LDAP database connection.



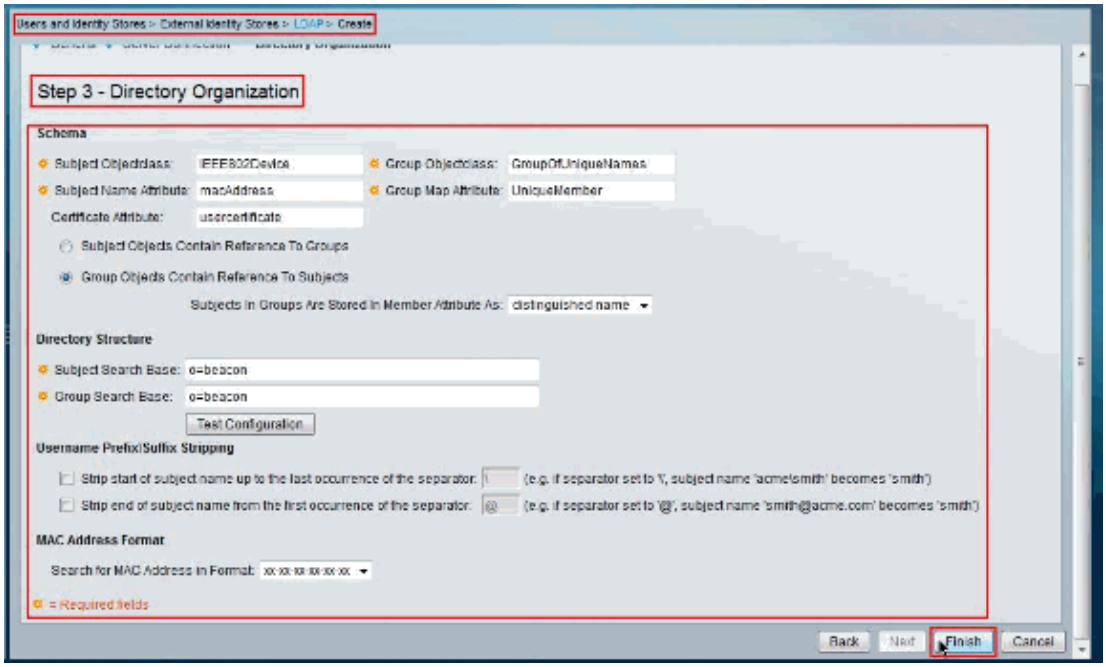

2. Provide a **Name** for the new **LDAP database connection** and click **Next**.



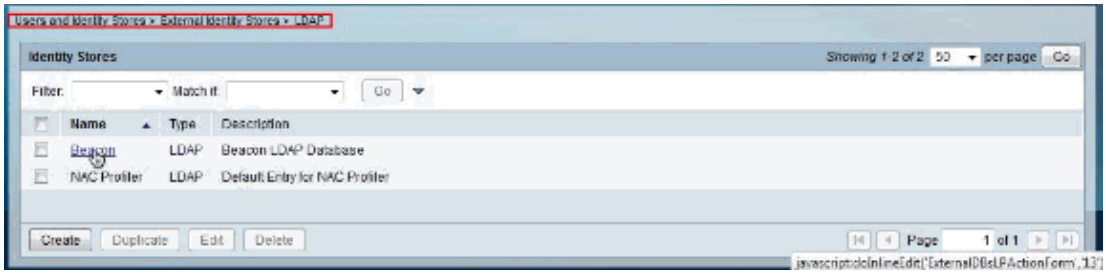

3. In the **Server Connection** tab enter the **Hostname/IP Address** of the **BEACON LDAP Sever, port, Admin DN, Password** (GBSbeacon in this example). Then, click **Next**.



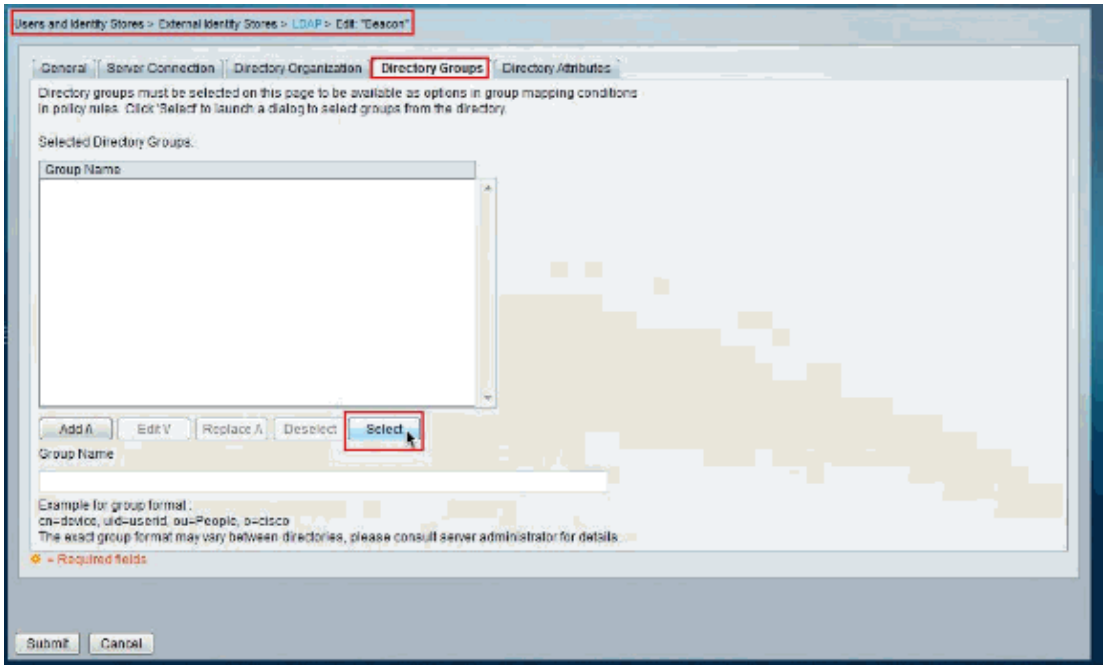

4. In the **Directory Organization** tab enter the required information. Then, click **Finish**.



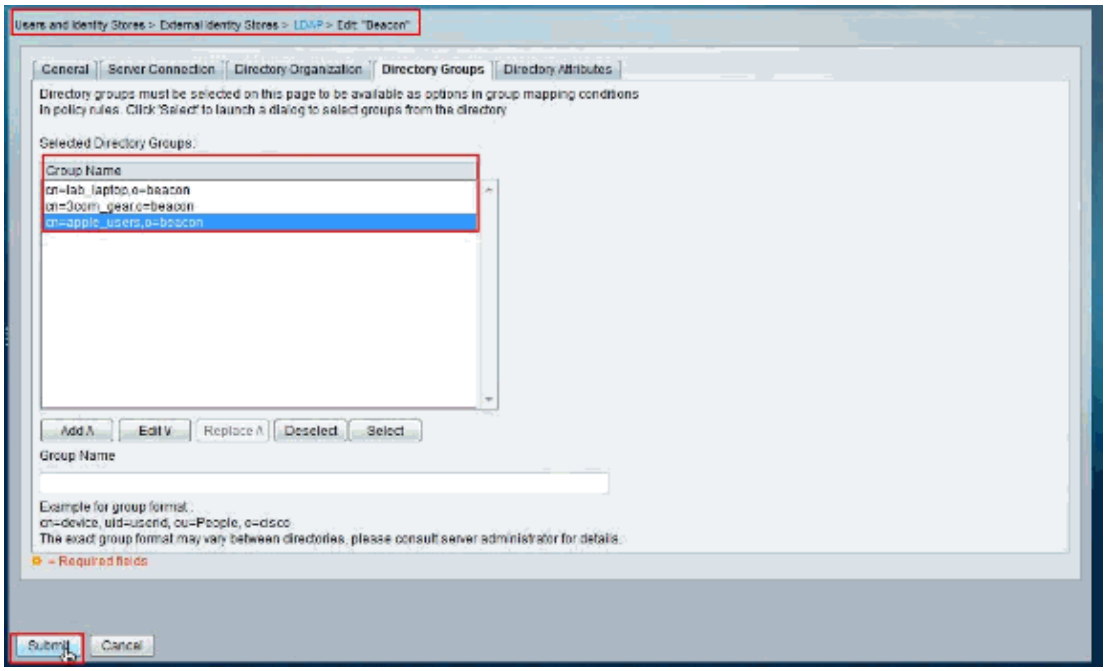

5. Click the newly created **LDAP Connection** (Beacon in this example).




6. Choose the **Directory Groups** tab and click **Select**. connection.



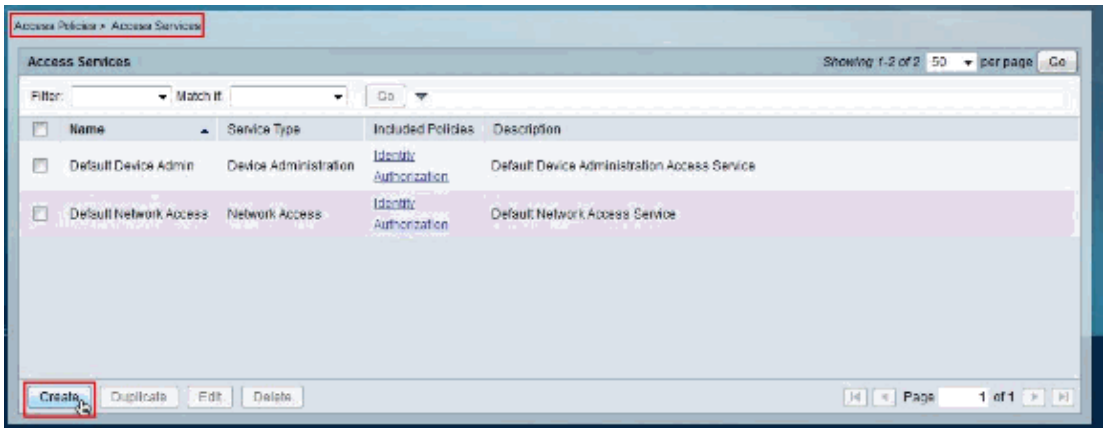

7. Select all the groups in the next screen that you want to map to **BeaconKnownDevices**.
8. In this example these groups, namely lab_laptop, 3com_gear and apple_users, are chosen. Then, click **Submit**.



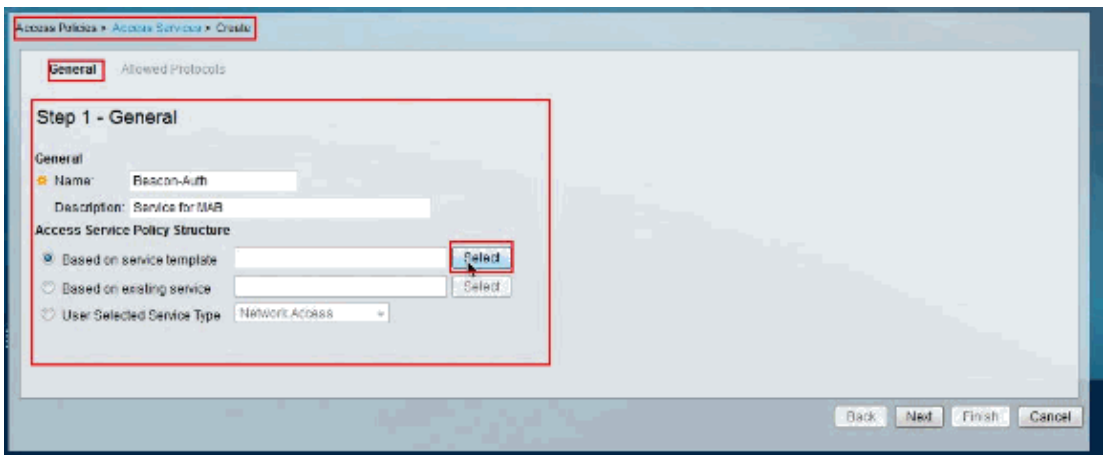

## Configure Access Services

Complete these steps in order to configure the Access Services:

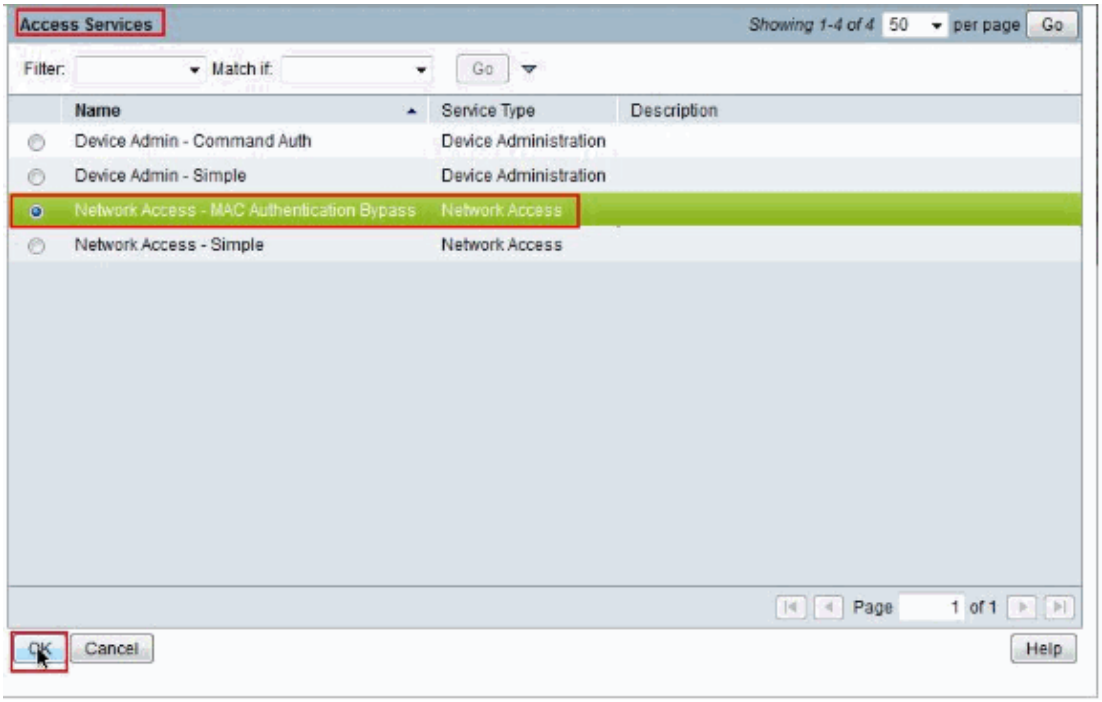
1. Choose **Access Policies > Access Services** and click **Create** to create a new Access Service.



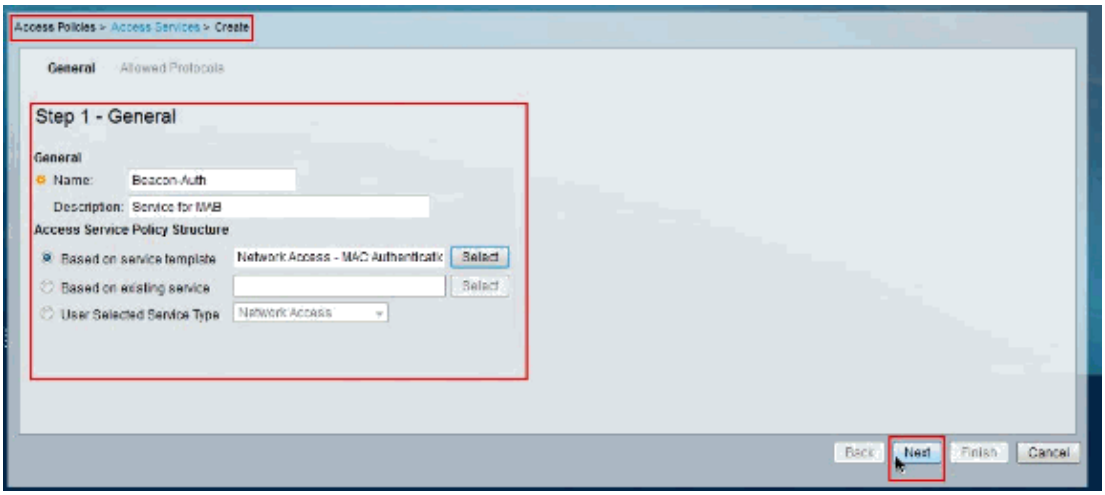

2. In the **General** tab provide the **Name** of the new service, then click **Select** next to **Based on Service template**.



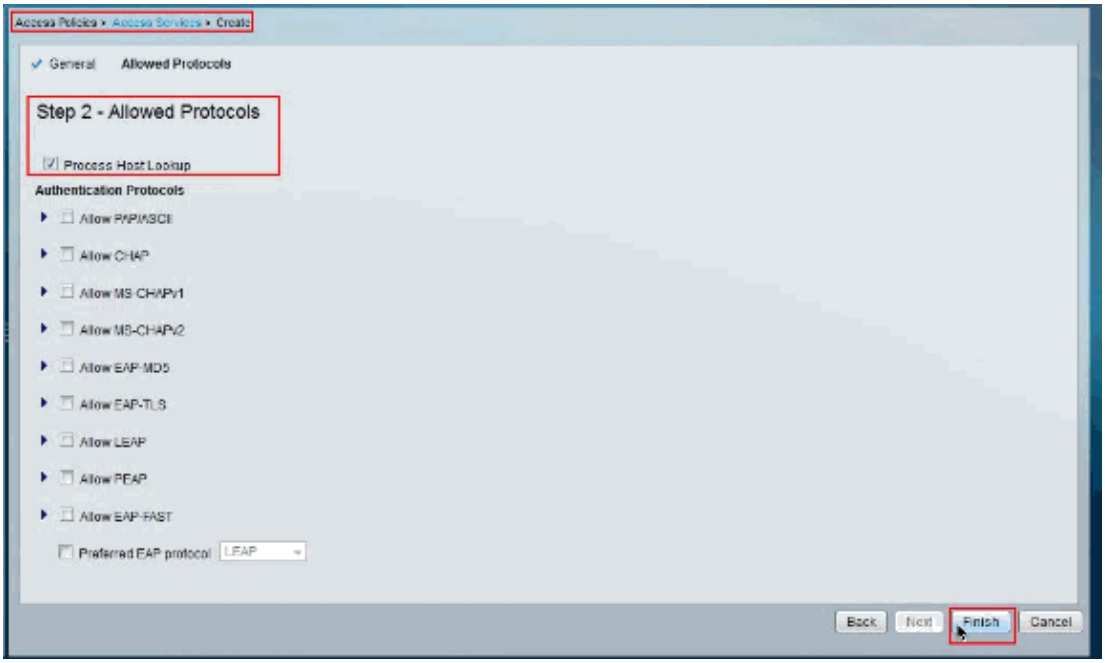
3. Choose **Network Access − MAC Authentication Bypass** and click **OK**.



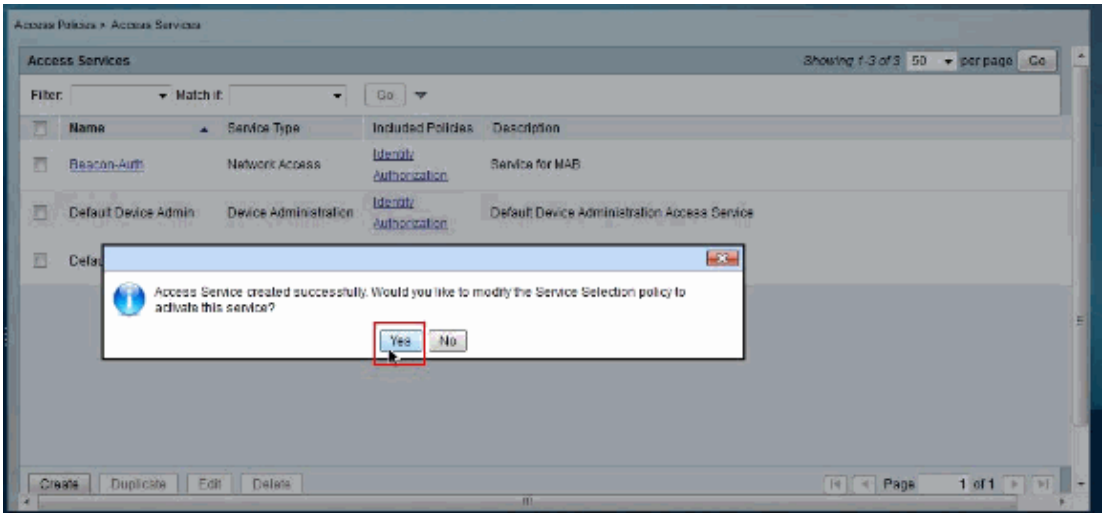

4. Click **Next**.



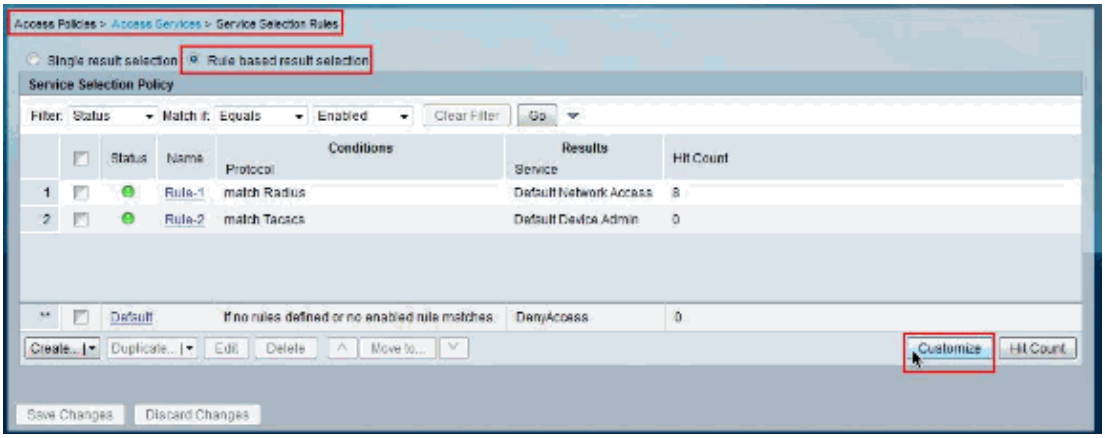

5. Click **Finish**.



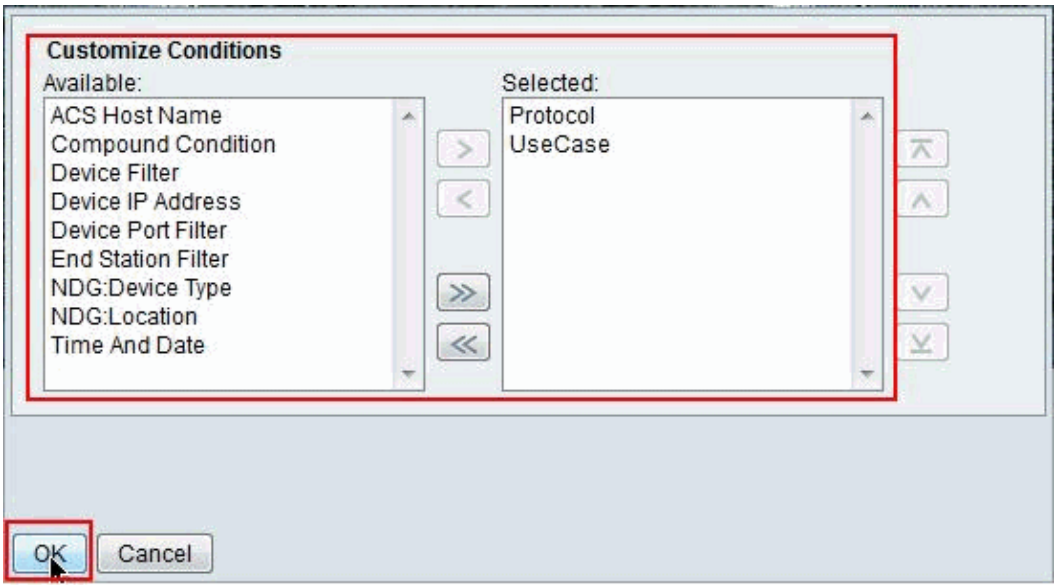

6. Click **Yes**.



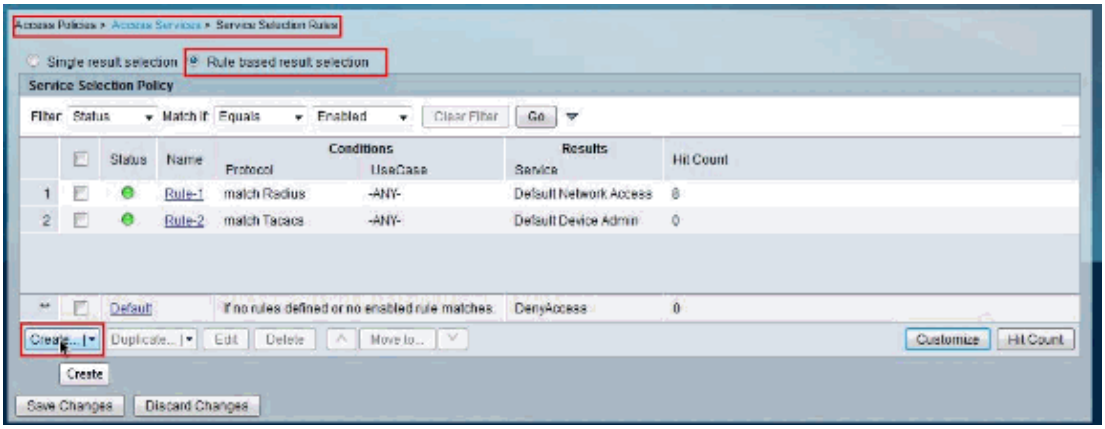

7. Click **Customize**.



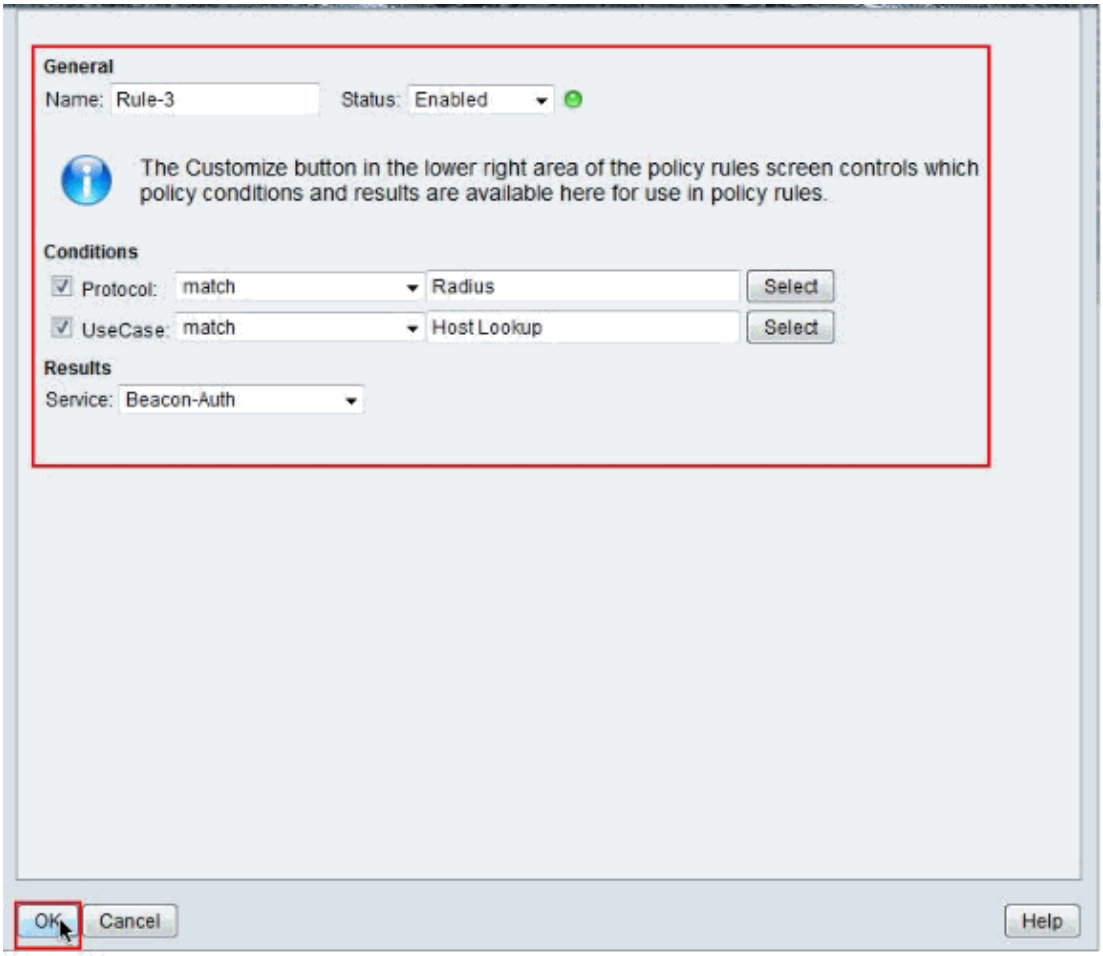

8. Move **UseCase** from **Available** to **Selected** and click **OK**.



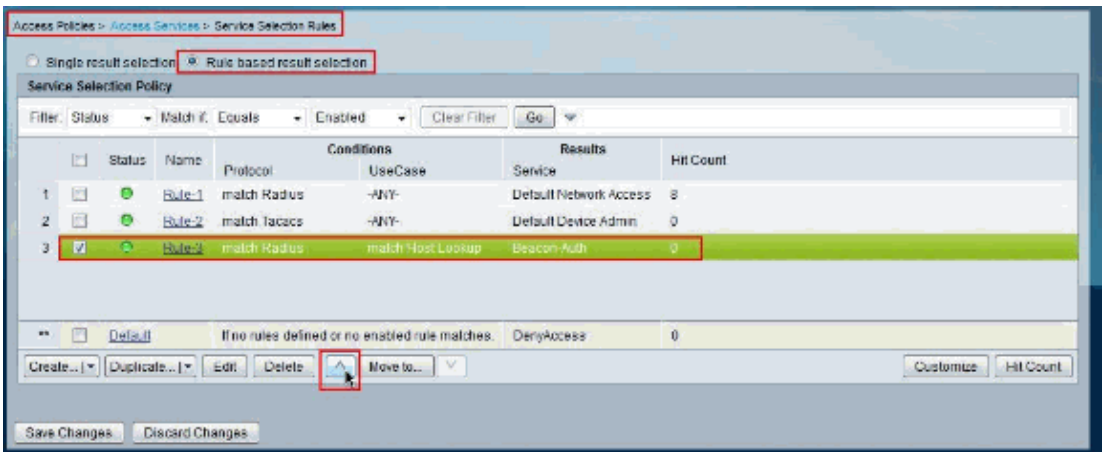

9. Click **Create** to create a new **Service Selection Rule**.



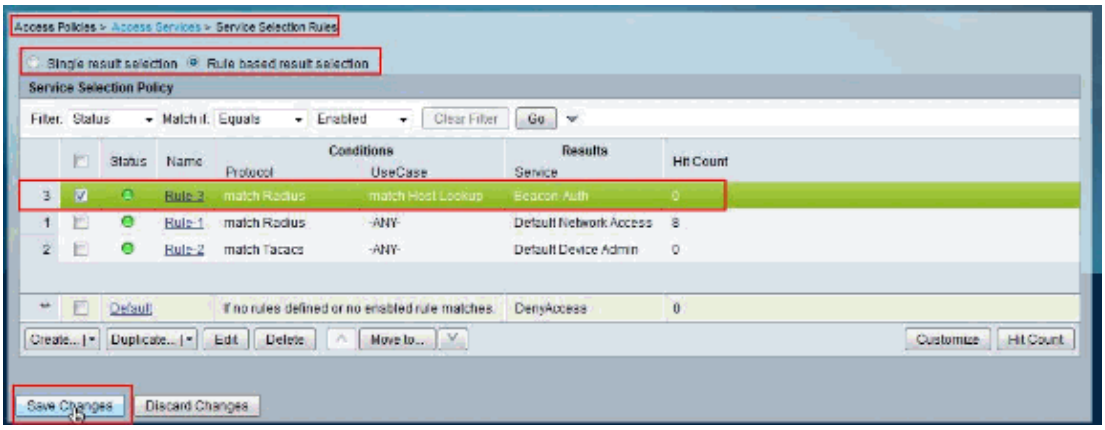

10. Select **Protocol** and use **Radius** as the value. Similarly, select **UseCase** and use **Host Lookup** as value. Choose **Beacon−Auth** as the service and click **OK**.



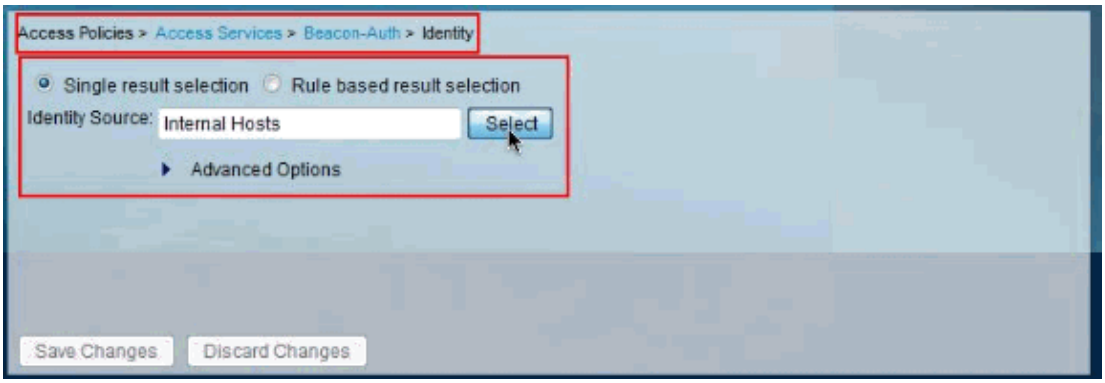

11. Move the newly created rule to the top.



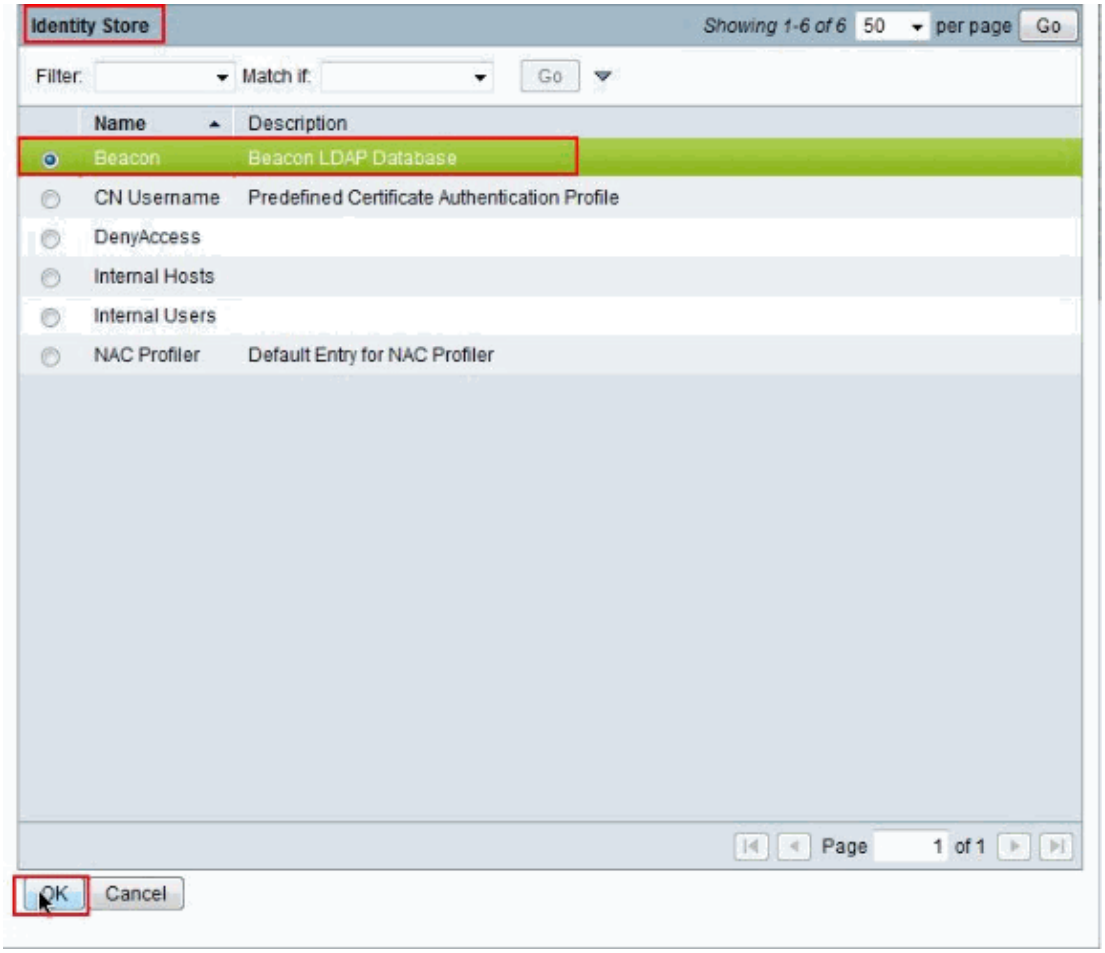

12. Click **Save Changes**.



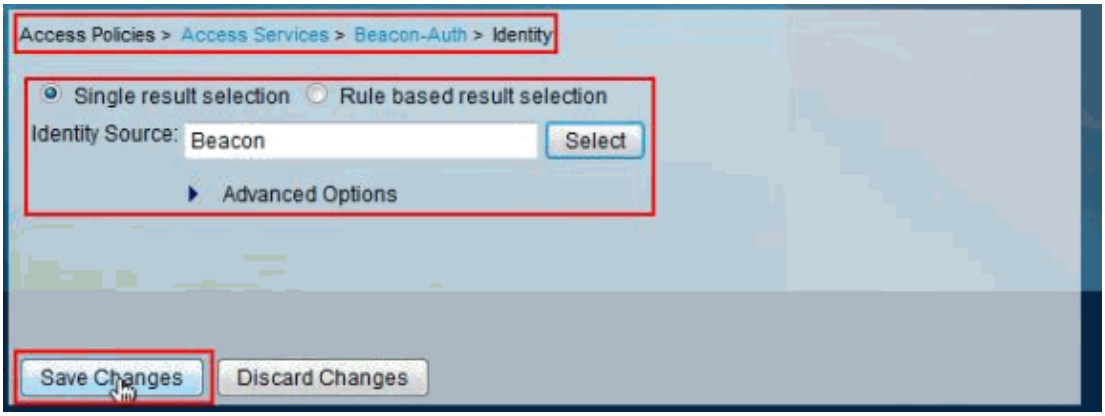

13. Choose **Access Policies > Access Services > Beacon−Auth > Identity** and click **Select** next to **Identity Source**.



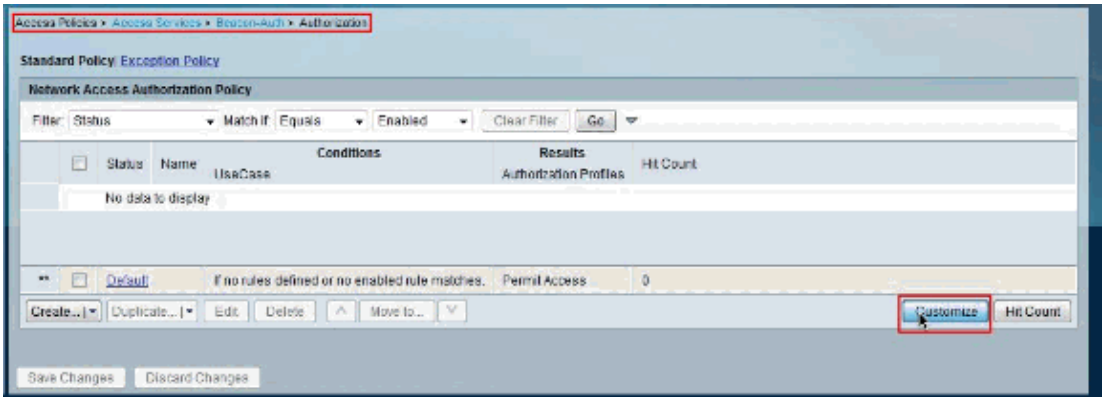

14. Choose **Beacon** and click **OK**.



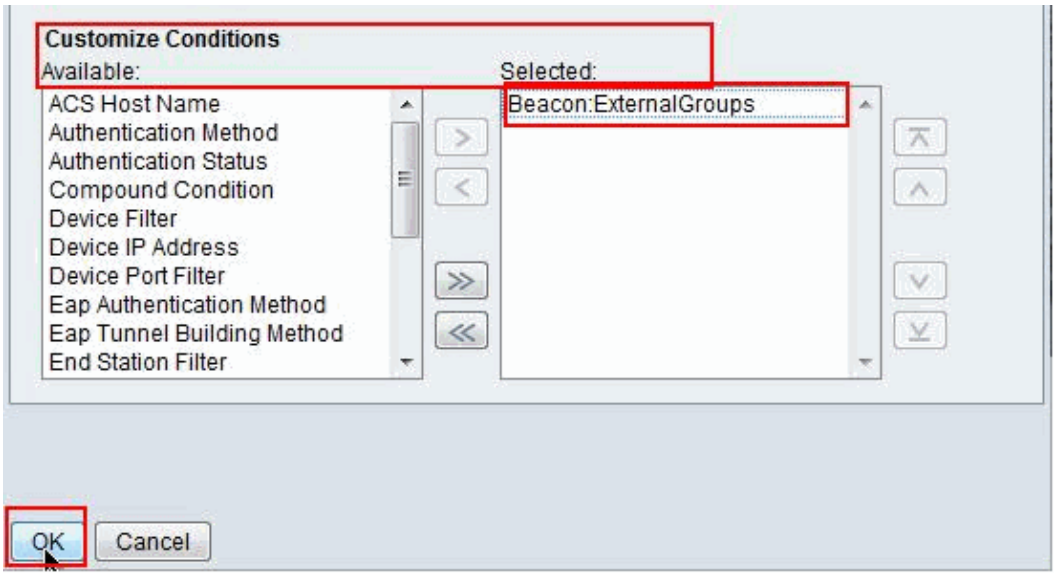
15. Click **Save Changes**.



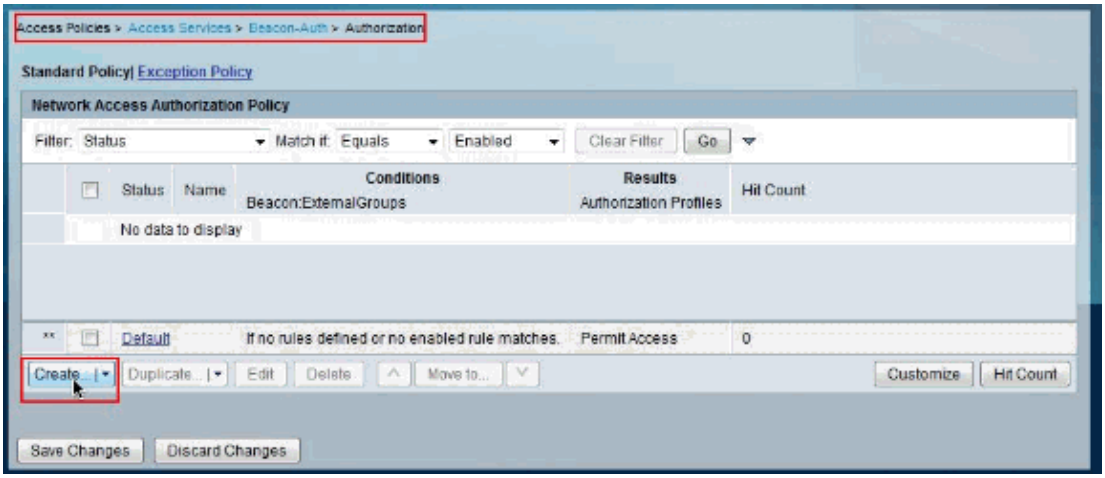

16. Choose **Access Policies > Access Services > Beacon−Auth > Authorization** and click **Customize**.



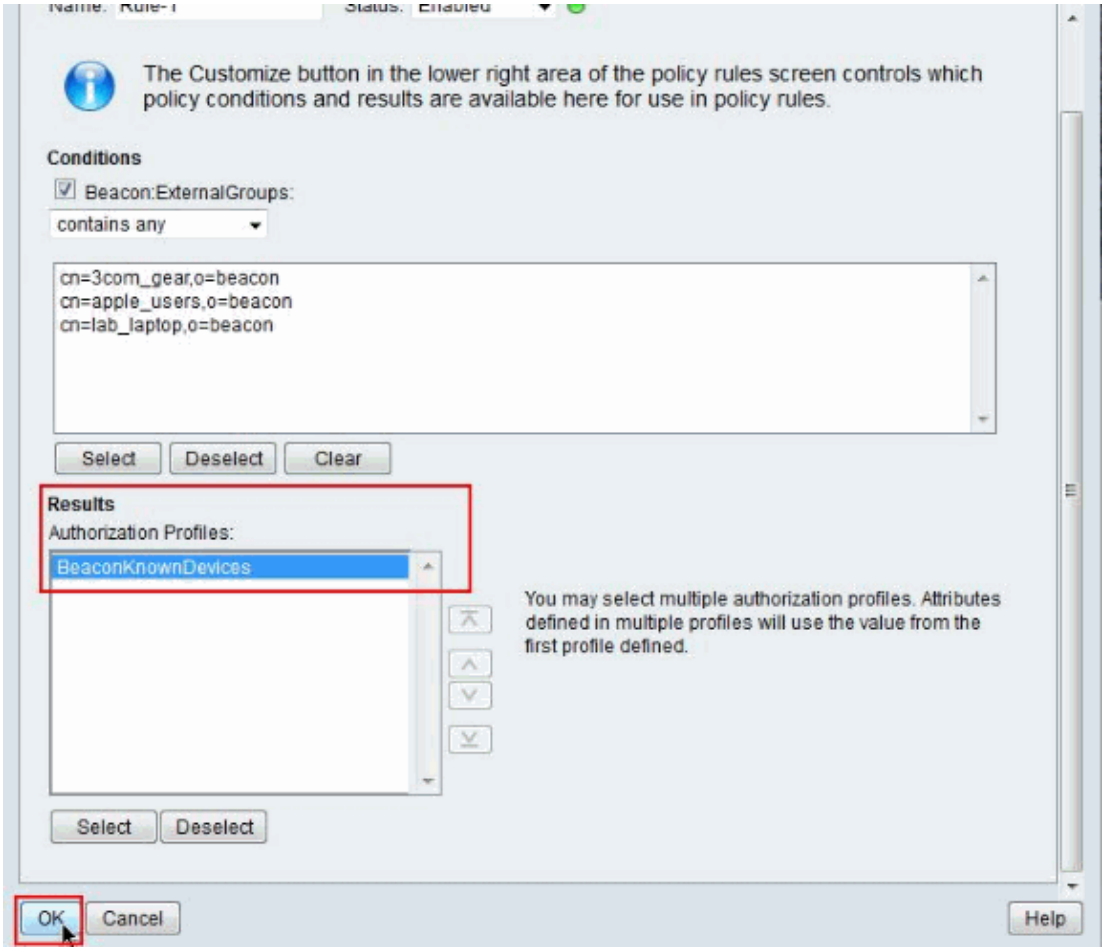

17. Move **Beacon:ExternalGroups** from **Available** to **Selected** and click **OK**.



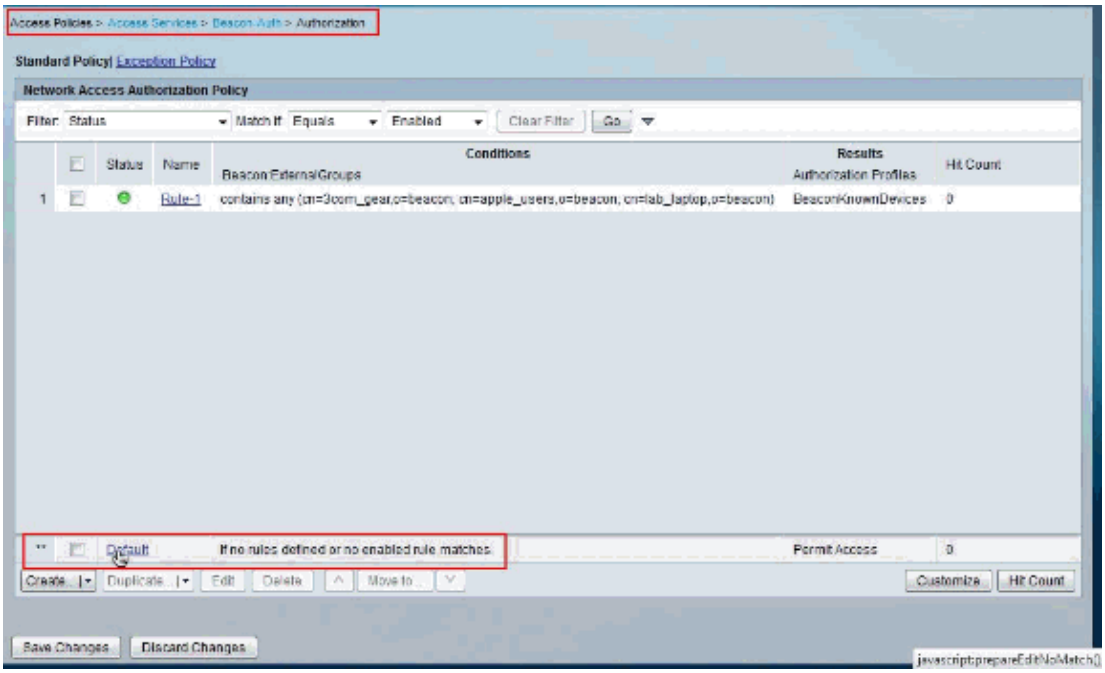

18. Click **Create** to create a new **Rule**.



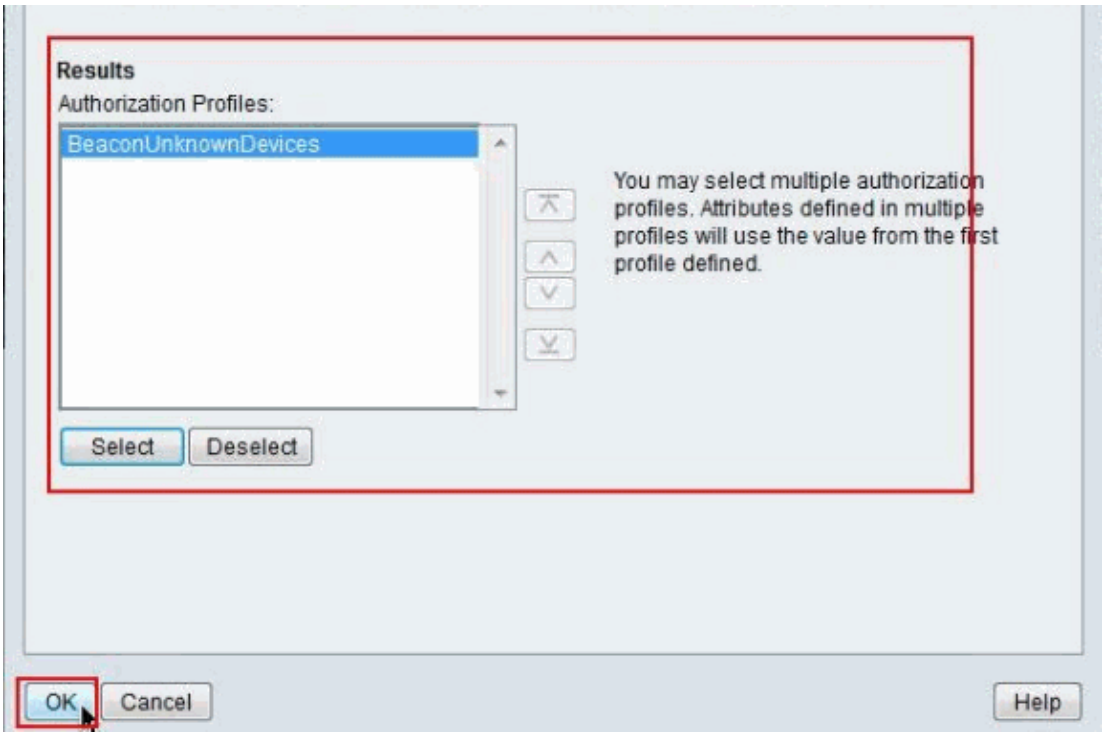

19. Choose 3com_users, apple_users and lab_laptop as the conditions and the Authorization Profile **BeaconKnownDevices** as **Result**. Then, click **OK**.



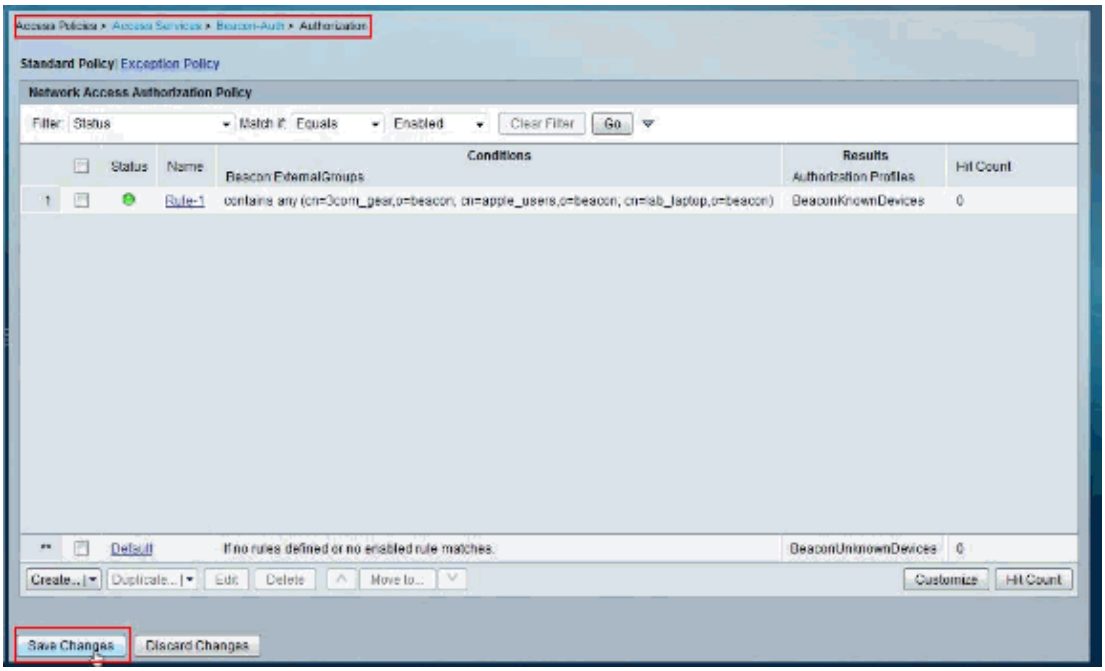

20. Click **Default**.




21. Choose 3com_users, apple_users and lab_laptop as the conditions and the Authorization Profile **BeaconUnKnownDevices** as Result. Then, click **OK**.




22. Click **Save Changes**.




This completes the procedure.

## Switch Configuration for MAC Authentication Bypass

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

| Switch |
| --- |

```
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
!
!
!
!
!
!
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 System**
- **Technical Support & Documentation − Cisco Systems**



Updated: Jun 01, 2012 Document ID: 113566