

Identity Manager Deployment Guide

June 2013

Contents

- Introduction..... 3
- What’s New in this Guide..... 4
- What’s Changed in this Guide..... 4
- Installing Identity Manager on VMware Platforms 5
- Identity Manager HTTP Redirection Process 5
- Integrating Identity Manager with System Director 8
 - Configuring System Director..... 8
 - Configuring Identity Manager 13
- Deployment Examples 15
 - Use Case 1: Providing Enterprise Security in BYOD Environments..... 15
 - Use Case 2: Providing Secure Guest Access..... 31
 - Use Case 3: Configuring Captive Portal for Wired Clients 44
 - Use Case 4: Configuring Role-Based Access Control for Personal and Corporate Devices 52
 - Use Case 5: Providing Guest Access Paid Subscription Systems for Wi-Fi Hotspots..... 57
 - Use Case 6: Basic Customization of a Guest Portal Using Default Tools 74
 - Use Case 7: Advanced Customization of Guest Portals by Importing a New Theme..... 79
- Where to Find More Information 86

Introduction

The “bring your own device” (BYOD) phenomenon is a result of more people acquiring personal mobile devices. As people expect to stay connected wherever they are, they are asking whether they can bring personal mobile devices to the workplace. As more people bring their devices to work, IT managers are dealing with new security and bandwidth issues with their networks. With the increase in mobile devices in the workplace, companies must have a strong management policy with minimal overhead on IT resources and a network able to handle the client density.

Developing a strong management policy includes automatically controlling device access and introducing security by providing interface-to-NAC solutions. Guest users at organizations are now increasingly requiring online access to perform their work. Management applications should be fast and easy enough to provide quick network access to allow guests to be more productive.

Single users with multiple devices who access your WLAN require tremendous RF resources. To provide quality service, the APs must be able to handle heavy usage from many different types of Wi-Fi client devices. Meru’s unique single-channel architecture helps maximize the available RF-spectrum consumption and can also effectively use channel layers to address high density areas as required.

Meru Identity Manager is a complete provisioning, management, and reporting system that provides temporary network access for visitors, contractors, consultants, or customers. Identity Manager works alongside wireless controllers, LAN switches, NAC systems, firewalls, and other network enforcement devices to provide secure network access.

Identity Manager allows any user with appropriate privileges to easily create temporary guest accounts and sponsor guests. Identity Manager performs full authentication of sponsors, the users who create guest accounts, and allows sponsors to provide account details to the guest by printout, email, or SMS. The entire experience, from user-account creation to guest network access, is stored for audit and reporting. Identity Manager provides vital guest network access accounting by consolidating the entire audit trail from guest account creation to guest use of the account so that reports can be generated with a central management interface.

This guide provides information about the following:

- Integrating Identity Manager with Meru controllers
- Deploying Smart Connect to provide network access:
 - Secure private network access using WPA2-Enterprise security with 802.1X authentication
 - Secure guest access using WPA2-PSK

- Providing secure access for users with wired clients
- Configuring role-based access for corporate and personal devices
- Configuring Identity Manager for paid access subscription for guest users in hotspots
- Captive Portal Customization examples in Identity Manager

You should have basic knowledge about Identity Manager concepts, such as sponsors, guests, guest portals, and Smart Connect. You should also know how to configure a Meru controller using System Director. For more information, see the *Meru Identity Manager User Guide* and the *Meru System Director Configuration Guide*.

What's New in this Guide

The following use cases were added:

- [Use Case 5: Providing Guest Access Paid Subscription Systems for Wi-Fi Hotspots](#)
- [Use Case 6: Basic Customization of a Guest Portal Using Default Tools](#)
- [Use Case 7: Advanced Customization of Guest Portals by Importing a New Theme](#)

What's Changed in this Guide

The following lists changes in this guide:

- The guide is based on System Director Release 6.0 and Identity Manager Version 13.6.
If you are using an earlier Identity Manager version, see the previous version of the [Identity Manager Deployment Guide](#), which is based on Identity Manager Version 11.12. Note that Identity Manager screen captures might differ, depending on which version of Identity Manager you are using.
- The [Identity Manager HTTP Redirection Process](#) topic was updated to reflect System Director Release 6.0 and Identity Manager Version 13.6.
- In [Use Case 1: Providing Enterprise Security in BYOD Environments](#), an Active Directory server was added to the network environment to provide authentication for corporate users.

Note: To implement Use Case 1 with an Active Directory server, you must use Identity Manager Version 13.2 or later.

Installing Identity Manager on VMware Platforms

You can install Identity Manager on the following VMware platforms:

- ESX 3.5
- ESX 3.5i
- ESX 4.x
- ESX 4.xi
- ESX 5.xi
- Server 1.0 or later
- Microsoft Hyper V on Windows 2008 or later
- Workstation 5.0 or later
- Fusion 2.0 or later

Note: Workstation and Fusion versions are supported only for evaluation or demonstration purposes.

For more information, see the *Meru Identity Manager User Guide*.

Identity Manager HTTP Redirection Process

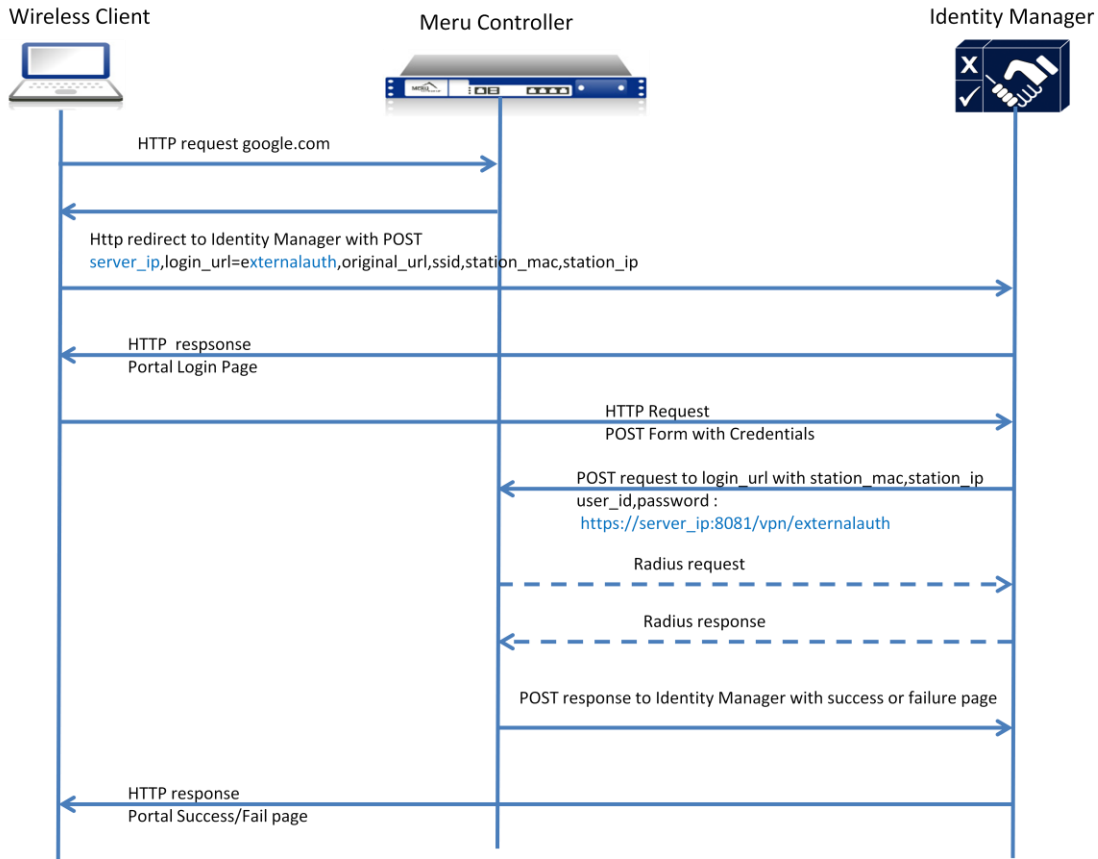
In a network environment using Identity Manager Version 13.6 and System Director Release 6.0, the HTTP redirection process depends on whether APs are connected in tunneled or bridged mode.

The following must be configured on the controller, regardless of whether the APs are in tunneled or bridged mode:

- In the security profile, the Captive Portal Authentication method must be specified as External.
- The external URL pointing to Identity Manager must be configured in the Captive Portal configuration page.
- RADIUS profiles for authentication and accounting pointing to Identity Manager must be configured in the Captive Portal configuration page.
- QoS rules to allow pre-authentication traffic to the Identity Manager IP address must be added on the controller.

[Figure 1](#) shows the Identity Manager HTTP redirection for stations in tunneled mode.

Figure 1: Identity Manager Redirection in Tunneld Mode



The controller redirects any HTTP/HTTPS traffic from unauthenticated stations for the Identity Manager-configured ESS profile to the external Identity Manager URL. The controller redirects with a POST request to the Identity Manager URL, along with following parameters:

- server_ip: Controller IP address, which Identity Manager uses for authentication.
- login_url: URL that Identity Manager uses when contacting the controller for authentication. It creates a complete URL as follows:
`https://server_ip:8081/vpn/login_url`
- original_url: Original URL requested by the station.
- ssid: SSID of the station that is currently connected.
- station_mac: MAC address of the station.
- station_ip: IP address of the station.

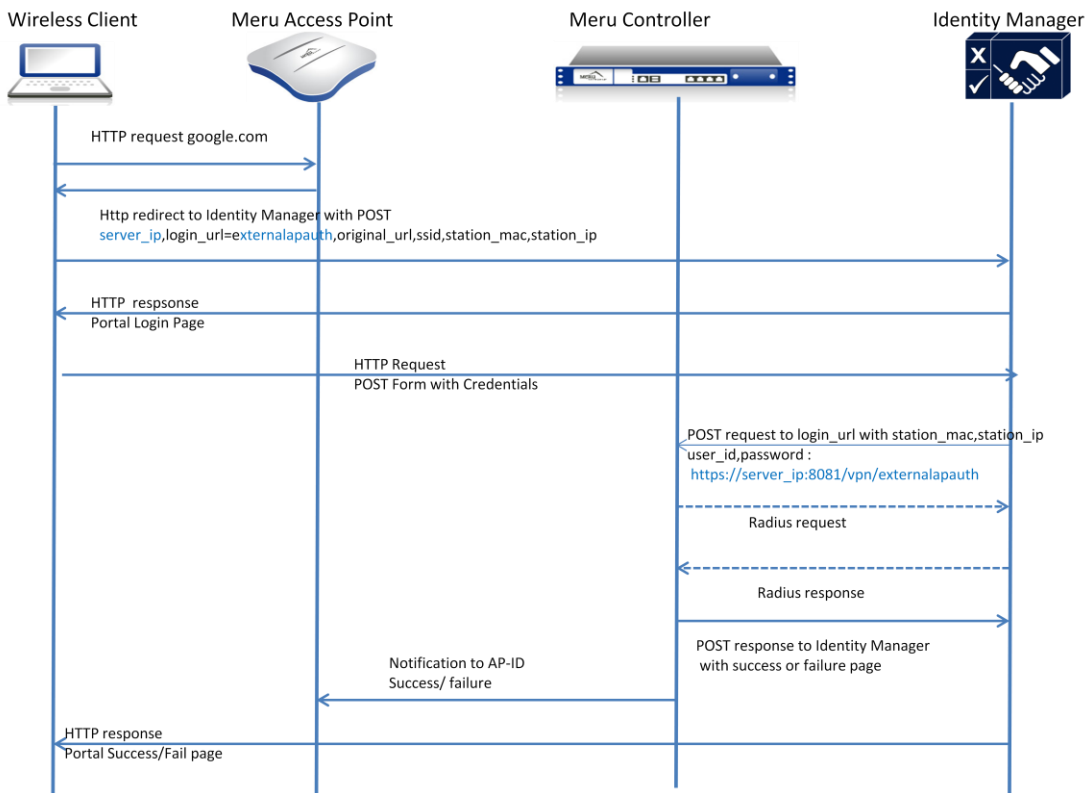
After receiving the redirect POST request from a client, Identity Manager serves the login pages to stations. After the station provides login credentials, Identity Manager will POST the login credentials, along with station_mac and station_ip to the login_url.

Identity Manager ignores any HTTPS certificate-related errors when contacting the controller for authentication based on HTTPS POST. After receiving the authentication request from Identity Manager with HTTPS POST, the controller authenticates the credentials based on station_mac and station_ip.

Authentication results are sent back to Identity Manager as a POST response as Success/Failure HTML pages. Based on the HTTPS response, Identity Manager serves its own success/failure pages to the client. If the client authentication is successful, Identity Manager redirects the station to original_url, and the controller allows all traffic from that client.

[Figure 2](#) shows the Identity Manager HTTP redirection process for stations connected in bridged mode.

Figure 2: Identity Manager Redirection in Bridged Mode



APs redirect any HTTP/HTTPS traffic from unauthenticated stations for an Identity Manager-configured ESS profile to external Identity Manager URL. The AP redirects with a POST request to the Identity Manager URL, along with following parameters:

- **server_ip:** Controller IP address, which Identity Manager uses for authentication purposes.
- **login_url:** URL that Identity Manager uses when contacting the controller for authentication. It creates a complete URL as follows:
`https://server_ip:8081/vpn/login_url`
- **original_url:** Original URL requested by the station.

- ssid: SSID of the station that is currently connected.
- station_mac: MAC address of the station.
- station_ip: IP address of the station.
- apid: AP ID where station is connected.

After receiving the redirect POST request from a client, Identity Manager serves the login pages to stations. After the station provides login credentials, Identity Manager will POST the login credentials, along with station_mac, station_ip and apid to the login_url.

Identity Manager ignores any HTTPS certificate-related errors while contacting controller for authentication based on HTTPS POST. After receiving authentication request from Identity Manager via HTTPS POST, the controller authenticates the credentials based on the station MAC address and IP address.

Authentication results are sent back to Identity Manager as a POST response as Success/Failure HTML pages. If authentication is successful, the controller updates the AP (based on apid) about the station's authentication state.

Based on HTTPS response, Identity Manager serves its own success/failure pages to the client. If the client authentication is successful, Identity Manager redirects the station to original_url, and the AP allows all traffic from that client.

Integrating Identity Manager with System Director

You can configure Identity Manager to work seamlessly with System Director. This guide is based on System Director Release 6.0 and Identity Manager Version 13.6.

Configuring System Director

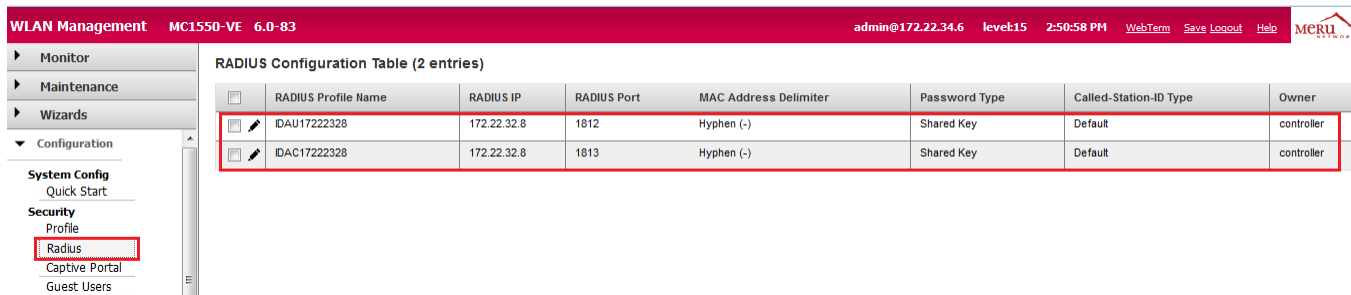
Before configuring Identity Manager, you must perform the following configuration tasks on the controller:

- [Creating RADIUS Profiles](#)
- [Mapping the RADIUS Profile to the Captive Portal and Configuring the External Captive Portal URL](#)
- [Configuring QoS Rules](#)
- [Creating a Security Profile](#)
- [Creating an ESS Profile](#)
- [Verifying Firewall Filters](#)

Creating RADIUS Profiles

For authentication and accounting of guest users, you must create RADIUS profiles on the controller, referencing the IP address of Identity Manager on ports 1812 and 1813 or 1645 and 1646. As shown in [Figure 3](#), RADIUS profiles that reference ports 1812 and 1813 are created.

Figure 3: RADIUS Profiles



<input type="checkbox"/>	RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Called-Station-ID Type	Owner
<input type="checkbox"/>	IDAU17222328	172.22.32.8	1812	Hyphen (-)	Shared Key	Default	controller
<input type="checkbox"/>	IDAC17222328	172.22.32.8	1813	Hyphen (-)	Shared Key	Default	controller

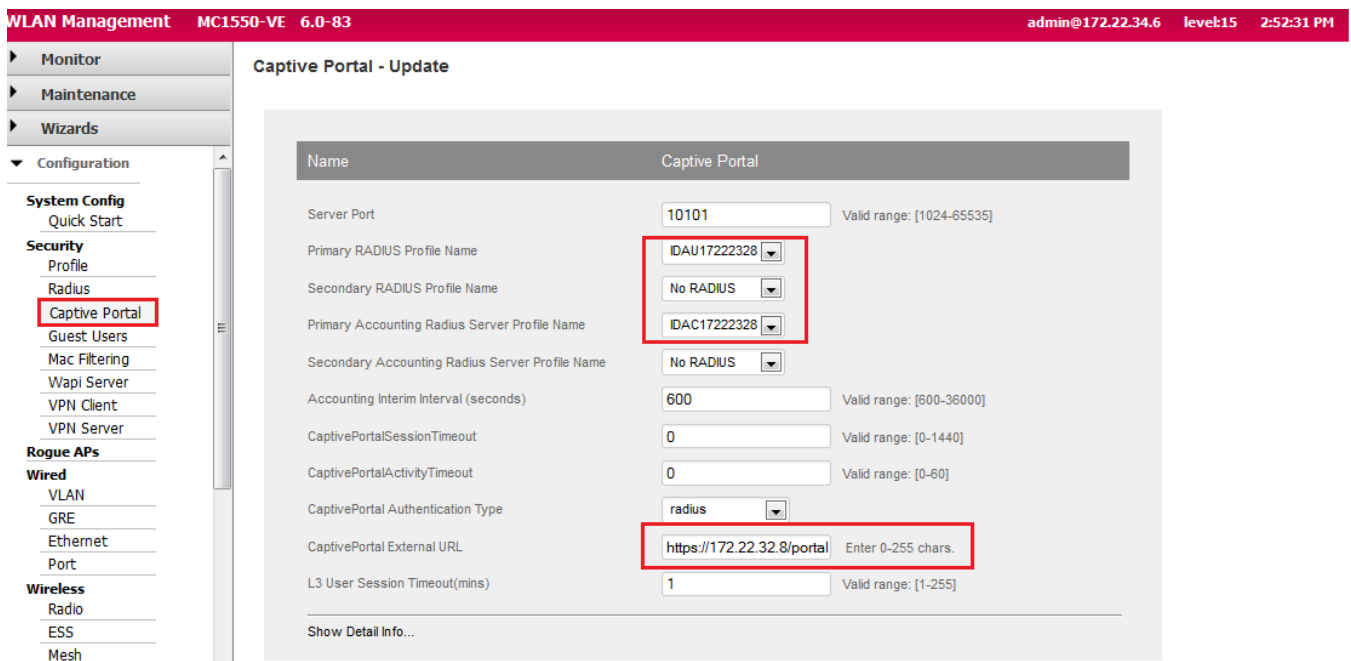
Mapping the RADIUS Profile to the Captive Portal and Configuring the External Captive Portal URL

As shown in [Figure 4](#), you must map RADIUS profiles to the Captive Portal for authentication and accounting. The Captive Portal External URL must be specified in the following format:

```
https://Identity_Manager_address/portal/controller_address?MeruInitialRedirect
```

The IP address or DNS name can be used as the Identity Manager and controller address.

Figure 4: Captive Portal - Update Page



Captive Portal - Update

Name: Captive Portal

Server Port: 10101 (Valid range: [1024-65535])

Primary RADIUS Profile Name: IDAU17222328

Secondary RADIUS Profile Name: No RADIUS

Primary Accounting Radius Server Profile Name: IDAC17222328

Secondary Accounting Radius Server Profile Name: No RADIUS

Accounting Interim Interval (seconds): 600 (Valid range: [600-36000])

CaptivePortalSessionTimeout: 0 (Valid range: [0-1440])

CaptivePortalActivityTimeout: 0 (Valid range: [0-60])

CaptivePortal Authentication Type: radius

CaptivePortal External URL: https://172.22.32.8/portal (Enter 0-255 chars.)

L3 User Session Timeout(mins): 1 (Valid range: [1-255])

Show Detail Info...

Configuring QoS Rules

To allow pre-authentication traffic to Identity Manager, you must create QoS rules using System Director. As shown in [Figure 5](#), allow traffic on port 443 to and from the Identity Manager IP address with the same firewall Filter-ID (string) mapped to each rule.

Figure 5: QoS and Firewall Rules Page

ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	QoS Protocol	Action	QoS Rule Logging	QoS Rule Logging Frequency
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0	6		0	0	H.323	CAPTURE	Off	60
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720	6		0	0	H.323	CAPTURE	Off	60
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	17		0	0	SIP	CAPTURE	Off	60
5	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	6		0	0	SIP	CAPTURE	Off	60
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0	17		0	0	other	FORWARD	Off	60
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200	17		0	0	other	FORWARD	Off	60
20	172.22.32.8	255.255.255.255	443	0.0.0.0	0.0.0.0	0	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
21	0.0.0.0	0.0.0.0	0	172.22.32.8	255.255.255.255	443	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
30	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	1	corp	0	0	none	DROP	Off	60
31	0.0.0.0	0.0.0.0	80	0.0.0.0	0.0.0.0	0	0	pers	0	0	none	DROP	Off	60

Creating a Security Profile

As shown in [Figure 6](#), you create a security profile named Corp_Guest_Portal, with Web-Auth enabled and the Captive Portal method of authentication specified as external. The firewall Filter ID that was created in [Configuring QoS Rules](#) must be mapped to the security profile.

Figure 6: Creating a Security Profile

Profile Name	Corp_Guest_Portal		
L2 Modes Allowed	<input checked="" type="checkbox"/> Clear	<input type="checkbox"/> 802.1x	<input type="checkbox"/> Static WEP keys
	<input type="checkbox"/> WPA	<input type="checkbox"/> WPA PSK	<input type="checkbox"/> WPA2
	<input type="checkbox"/> WPA2 PSK	<input type="checkbox"/> MIXED	<input type="checkbox"/> MIXED_PSK
	<input type="checkbox"/> WAI	<input type="checkbox"/> WAI PSK	
Data Encrypt	<input type="checkbox"/> WEP64	<input type="checkbox"/> WEP128	<input type="checkbox"/> TKIP
	<input type="checkbox"/> CCMP-AES	<input type="checkbox"/> CCMP/TKIP	<input type="checkbox"/> WPI-SMS4
	<input type="checkbox"/> Clear		
Primary RADIUS Profile Name	No RADIUS		
Secondary RADIUS Profile Name	No RADIUS		
WEP Key (Alphanumeric/Hexadecimal)			
Static WEP Key Index	1	Valid range: [1-4]	
Re-Key Period (seconds)	0	Valid range: [0-65535]	
BKSA Caching Period (seconds)	0	Valid range: [0-65535]	
Captive Portal	WebAuth		
Captive Portal Authentication Method	external		
802.1X Network Initiation	Off		
Tunnel Termination	<input type="checkbox"/> PEAP	<input type="checkbox"/> TTLS	
Shared Key Authentication	Off		
Pre-shared Key (Alphanumeric/Hexadecimal)			
Group Keying Interval (seconds)	0	Valid range: [0-65535]	
PMK Caching	Off		
Key Rotation	Disabled		
Backend Auth Server Timeout	30	Valid range: [1-65535]	
Reauthentication	Off		
MAC Filtering	Off		
Firewall Capability	none		
Firewall Filter ID			
	Enter 0-16 chars.		
Security Logging	Off		
Passthrough Firewall Filter ID	IDMPREAUTH		
	Enter 0-16 chars.		

Creating an ESS Profile

You must create an ESS profile named Corp_Guest_portal for guest access. As shown in [Figure 7](#), map the security profile to the ESS profile.

Figure 7: ESS Profile - Update Page

The screenshot displays the 'ESS Profile - Update' configuration page in the WLAN Management interface. The page is titled 'WLAN Management MC1550-VE 6.0-83' and 'admin@172.22.34.6'. The left sidebar shows navigation options like Monitor, Maintenance, and Wizards. The main content area is titled 'ESS Profile - Update' and has tabs for 'ESS Profile', 'ESS-AP Table', 'Security Profiles', and 'Hotspot Profiles'. The 'ESS Profile' tab is active, showing fields for SSID Number (4), ESS Profile (Corp_Guest_portal), and SSID (Corp Guest Portal). Below these are settings for Enable/Disable (Enable), Security Profile (Corp_Guest_Portal), Primary RADIUS Accounting Server (No RADIUS), Secondary RADIUS Accounting Server (No RADIUS), Accounting Interim Interval (seconds) (3600), and Beacon Interval (msec) (100).

Verifying Firewall Filters

To verify whether the firewall filters you created are filtering traffic correctly, use a client to connect to your guest network, and use a Web browser to access Identity Manager. After you enter the IP address of Identity Manager in a Web browser, if the browser is redirected to the Identity Manager Login page, the firewall filters are working correctly.

If the browser is not redirected to Identity Manager, check the following:

- On the controller, verify that the QoS rules are configured correctly:
 - Make sure that the appropriate Match check boxes have been selected in the QoS rules.
 - The filter IDs specified in the security profile match the filter IDs in the QoS rules.
- If the QoS rules are configured correctly, temporarily enable security logging in the security profile and check the logs. After you have finished troubleshooting, disable security logging in the security profile.

If you are using a DNS server in your network and have the Identity Manager IP address mapped to a server name (for example, idm), you can enter `https://idm` rather than the IP address in the Web browser.

Configuring Identity Manager

In Identity Manager, you must add controllers as RADIUS clients for captive portal authentication. An example of adding a controller as a RADIUS client is shown in [Figure 8](#).

Figure 8: RADIUS Client Tab

The screenshot shows the 'RADIUS Clients' configuration page. The left sidebar contains a navigation menu with items like Home, Network Access Policy, Policy Settings, Sponsor Portal, Guest Portals, Smart Connect, and Devices. Under 'Devices', 'RADIUS Clients' is selected. The main content area has tabs for Client, Attributes, SNMP, MAC Authentication, RadSec Authentication, and Automatic Setup. The 'Client' tab is active, showing fields for Name (Example Controller), Device IP Address / Prefix Length (10.10.10.10), Secret (masked), Confirm (empty), Type (Meru SD 6.0 & Later), and Description. Below these is the 'Change-of-Authorization' section with 'Use COA' checked and 'Port' set to 3799. 'Save' and 'Cancel' buttons are at the bottom.

Captive Portal and RADIUS-specific configuration that needs to be configured on the controller can be automatically pushed from Identity Manager, as shown in [Figure 9](#).

Figure 9: RADIUS Client Automatic Setup

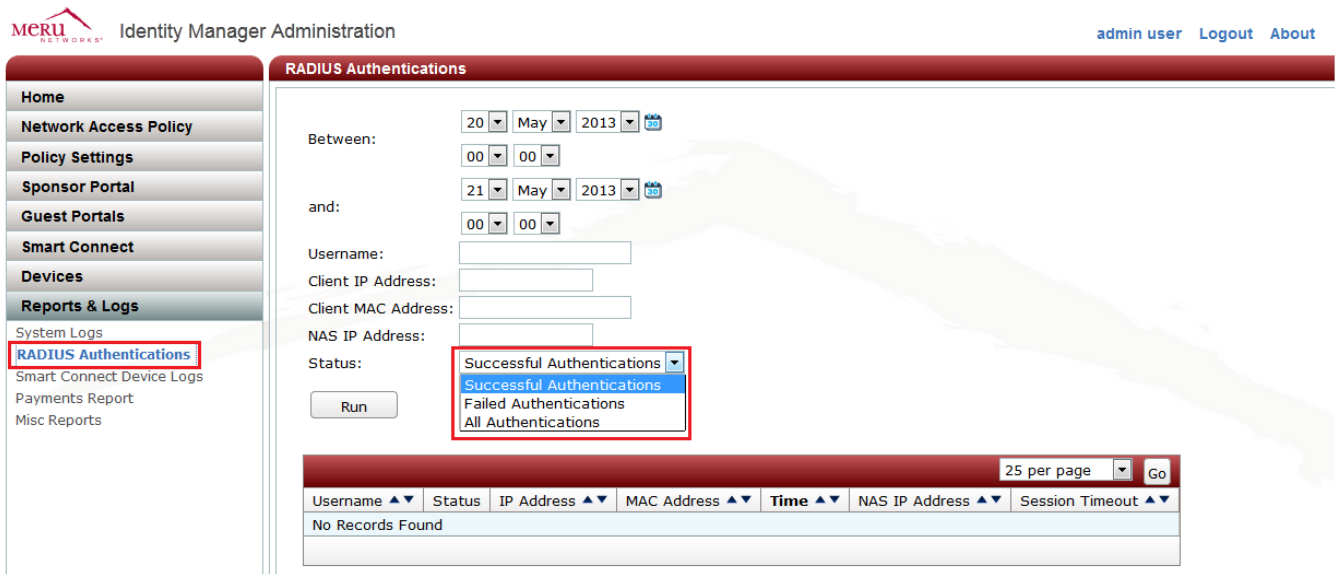
The screenshot shows the 'Automatic Setup' tab for a RADIUS client. The left sidebar is the same as in Figure 8, with 'RADIUS Clients' selected. The main content area has tabs for Client, Attributes, SNMP, MAC Authentication, RadSec Authentication, and Automatic Setup. The 'Automatic Setup' tab is active, showing fields for Identity Manager Address (172.22.32.8), Device IP Address (10.10.10.10), Admin user name (admin), and Admin Password (masked). There are checkboxes for 'Configure RADIUS profiles', 'Set Captive Portal RADIUS profiles', 'Set Captive Portal External URL', and 'Configure QoS Rules', all of which are checked. A 'Write changes to startup-config' checkbox is unchecked. A 'Setup Controller' button is at the bottom.

Verifying Authentication for the Captive Portal

To verify authentication for the Captive Portal, use a client to connect to the guest network. Open a Web browser window, and try to access any Web site. After being redirected to a login page, provide a user's credentials to see if authentication is successful. There are several ways in Identity Manager to verify if the authentication is successful or not.

To review successful and failed authentications, select **Reports & Logs > RADIUS Authentications**, as shown in [Figure 10](#).

Figure 10: RADIUS Authentications Page



For advanced troubleshooting, change the log settings to log errors, notices, informational and debug messages for RADIUS User Authentication logs:

1. In the Identity Manager Administration Interface, select **Server > System Logs**.
2. Click the **Log Settings** tab.
3. In the Admin Authentication and RADIUS User Authentication lists, select **Errors, Notices and Info**.
4. Click **Save**.

After changing the logging levels, select **Devices > RADIUS Clients**, and click the **Restart RADIUS in Debug** button.

After attempting authentication again, review the RADIUS log:

1. In the Identity Manager Administration Interface, select **Server > System Logs**, and click the **Support Logs** tab.
2. For the RADIUS log, click the **View** link.
On the Windows platform, the log is easier to read if you open it in WordPad.
3. Look for the following messages in the RADIUS log:
 - Incorrect shared secret messages
 - Messages stating that a guest account was not found or is in a restricted period.

If there are no messages about RADIUS authentication in the RADIUS log, verify that the RADIUS configuration on the controller is correct (correct RADIUS server IP address and port). Also see if there is a firewall between the controller and Identity Manager. Make sure that ports 1812 and 1813 (1645 and 1646) are open for RADIUS.

Deployment Examples

This guide presents seven use cases, which illustrate how you can use Identity Manager to manage guest access to your wired or wireless networks. You can also use Identity Manager to manage network access for your employees' personal and corporate devices. You can use Identity Manager Version 11.12 or later for all use cases, except for Use Case 1, which requires Identity Manager Version 13.2 or later.

- [Use Case 1: Providing Enterprise Security in BYOD Environments](#)
- [Use Case 2: Providing Secure Guest Access](#)
- [Use Case 3: Configuring Captive Portal for Wired Clients](#)
- [Use Case 4: Configuring Role-Based Access Control for Personal and Corporate Devices](#)
- [Use Case 5: Providing Guest Access Paid Subscription Systems for Wi-Fi Hotspots](#)
- [Use Case 6: Basic Customization of a Guest Portal Using Default Tools](#)
- [Use Case 7: Advanced Customization of Guest Portals by Importing a New Theme](#)

Use Case 1 and Use Case 2 use the same network environment. The other use cases use different network scenarios with different IP addresses.

Use Case 1: Providing Enterprise Security in BYOD Environments

As enterprises increasingly become “bring your own device” environments, you must be prepared to provide secure access to your wireless network. The challenge in allowing employees or students to bring their own devices is ensuring that they meet industry best practices and corporate policies for security. How do you configure hundreds or thousands of devices for 802.1X authentication and strong encryption without configuring each device individually?

In this use case, you use Smart Connect to configure tablets, smartphones, and other devices to use WPA2-Enterprise security with 802.1X authentication. Identity Manager is also integrated with the corporate Active Directory server for user authentication. This use case applies to network administrators who must allow various network devices to connect to the wireless network. This use case illustrates the process of self-provisioning for users with Windows XP laptops to connect to the 802.1 X-enabled networks. The same use case applies to all users, regardless of the type of end device. Smart Connect and Identity Manager automatically detect the type of device connecting to the network and correctly configure the device for secure network access.

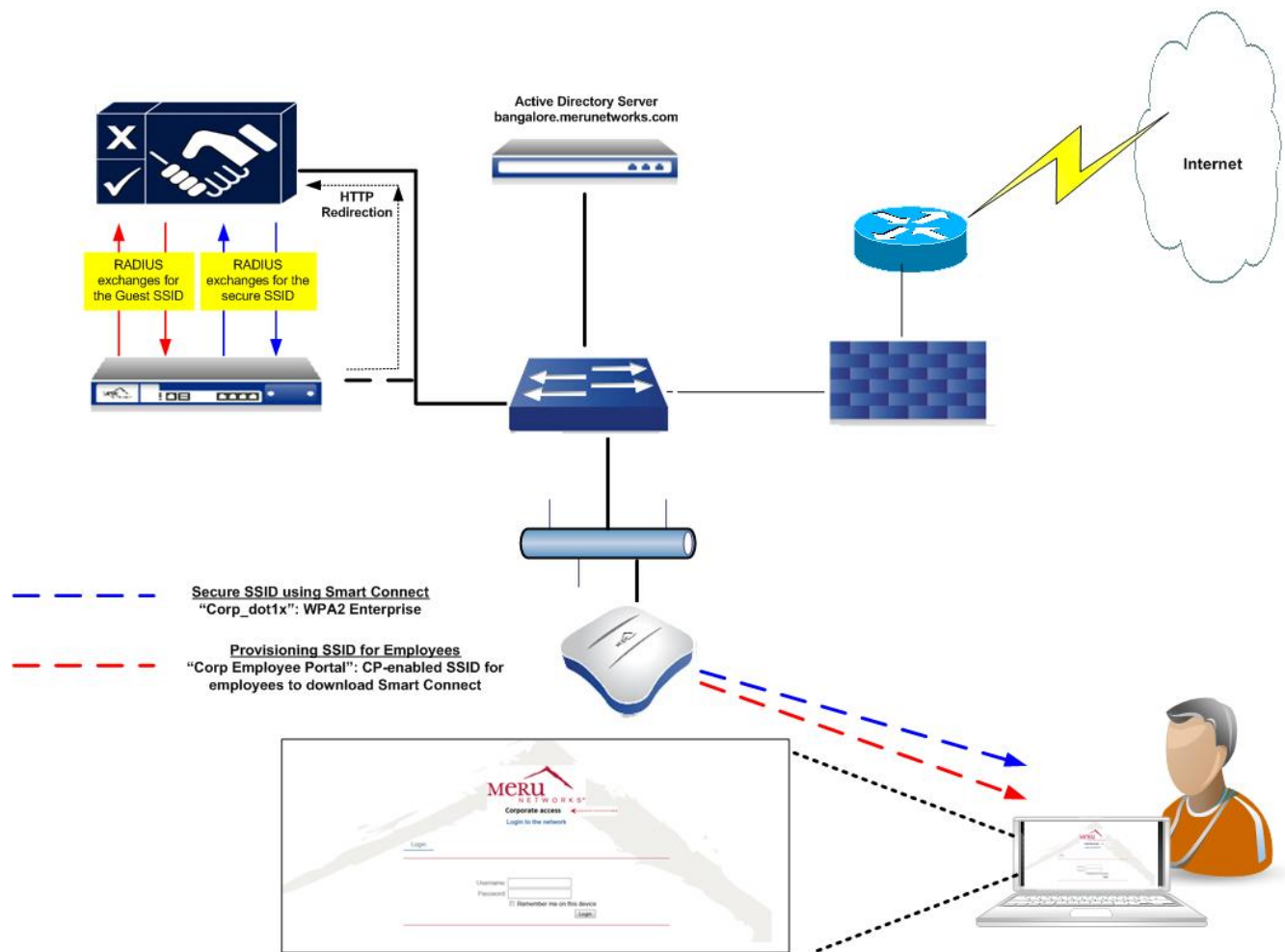
Users initially connect to the provisioning network and are successfully authenticated. They can then download the Smart Connect client. After the client is installed, users are automatically configured and connected to the secure 802.1X-enabled network. Subsequent access to the network is seamless and transparent to the end user on the secure private network.



To implement this use case with an Active Directory server for user authentication, you must use Identity Manager Version 13.2 or later.

[Figure 11](#) shows the network diagram for Use Case 1.

Figure 11: Use Case 1 Network Diagram



You need to perform the following tasks for this use case:

- [Controller Configuration Tasks](#)
- [Creating Authorization Profiles](#)
- [Create an Authentication Policy for an External Active Directory Server](#)
- [Creating a Smart Connect Profile for 802.1X Clients](#)
- [Creating a Smart Connect Policy](#)
- [Enabling Smart Connect on the Employee Provisioning Portal](#)
- [Installing the Smart Connect Plug-In on Windows Clients](#)

Controller Configuration Tasks

For information about how to create and manage ESS and security profiles, see the *Meru System Director Configuration Guide*.

You need to perform the following tasks on the controller (see [Figure 12](#), [Figure 13](#), [Figure 14](#), and [Figure 15](#)):

- Create RADIUS profiles.
- Create two security profiles: one with WPA2 enterprise security and the other with captive portal enabled.
- Create two ESS profiles. One ESS profile (Corp Employee Portal) is for the provisioning network, and the other is the ESSID with 802.1x security (Corp_dot1x).
- Map the security profiles to the ESSIDs. In this use case, employees use ESSID “Corp Employee Portal” to access portal page and download the Smart Connect plug-in for the WPA2-enabled ESS “Corp_dot1x.”

Figure 12: Provisioning ESS Profile

The screenshot displays the 'WLAN Management' interface for 'MC1550-VE 6.0-83'. The left sidebar contains a navigation menu with categories: Monitor, Maintenance, Wizards, Configuration, System Config, Security, Rogue APs, Wired, and Wireless. The 'ESS' option under the 'Wireless' category is highlighted with a red box. The main content area is titled 'ESS Profile - Update' and features three tabs: 'ESS Profile', 'ESS-AP Table', and 'Security Profiles'. The 'ESS Profile' tab is active, showing a summary table and a configuration form. The summary table lists: SSID Number (3), ESS Profile (Corp_Employee_Portal), and SSID (Corp Employee Portal). The configuration form includes: 'Enable/Disable' set to 'Enable'; 'Security Profile' set to 'Corp_Employee_portal' (highlighted with a red box); 'Primary RADIUS Accounting Server' and 'Secondary RADIUS Accounting Server' both set to 'No RADIUS'; 'Accounting Interim Interval (seconds)' set to '3600' (Valid range: [600-36000]); 'Beacon Interval (msec)' set to '100' (Valid range: [20-1000]); 'SSID Broadcast' set to 'On'; 'Bridging' with checkboxes for 'AirFortress', 'IPv6', and 'AppleTalk'; 'New AP's Join ESS' set to 'On'; and 'Tunnel Interface Type' set to 'No Tunnel'.

Field	Value
SSID Number	3
ESS Profile	Corp_Employee_Portal
SSID	Corp Employee Portal

Configuration details:

- Enable/Disable: Enable
- Security Profile: Corp_Employee_portal
- Primary RADIUS Accounting Server: No RADIUS
- Secondary RADIUS Accounting Server: No RADIUS
- Accounting Interim Interval (seconds): 3600 (Valid range: [600-36000])
- Beacon Interval (msec): 100 (Valid range: [20-1000])
- SSID Broadcast: On
- Bridging: AirFortress IPv6 AppleTalk
- New AP's Join ESS: On
- Tunnel Interface Type: No Tunnel

Figure 13: Security Profile Mapped to Provisioning ESS Profile

WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6

Monitor
Maintenance
Wizards
Configuration

System Config
Quick Start

Security
Profile
Radius
Captive Portal
Guest Users
Mac Filtering
Wapi Server
VPN Client
VPN Server

Rogue APs

Wired
VLAN
GRE
Ethernet
Port

Wireless
Radio
ESS
Mesh
Hotspot

Security Configuration Table (4 entries)

ESS Profile | ESS-AP Table | **Security Profiles** | Hotspot Profiles

Profile Name: Corp_Employee_portal

L2 Modes Allowed: Clear, WPA, WPA2 PSK, WAI, 802.1x, WPA PSK, MIXED, WAI PSK, Static WEP keys, WPA2, MIXED_PSK

Data Encrypt: WEP64, CCMP-AES, Clear, WEP128, CCMP/TKIP, TKIP, WPI-SMS4

Primary RADIUS Profile Name: No RADIUS

Secondary RADIUS Profile Name: No RADIUS

WEP Key (Alphanumeric/Hexadecimal):

Static WEP Key Index: 1 (Valid range: [1-4])

Re-Key Period (seconds): 0 (Valid range: [0-65535])

BKSA Caching Period (seconds): 0 (Valid range: [0-65535])

Captive Portal: WebAuth

Captive Portal Authentication Method: external

Figure 14: WPA2-Enabled ESSID

WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6

Monitor
Maintenance
Wizards
Configuration

System Config
Quick Start

Security
Profile
Radius
Captive Portal
Guest Users
Mac Filtering
Wapi Server
VPN Client
VPN Server

Rogue APs

Wired
VLAN
GRE
Ethernet
Port

ESS Profile - Update

ESS Profile | ESS-AP Table | Security Profiles | Hotspot Profiles

SSID Number: 1

ESS Profile: Corp_dot1x

SSID: Corp_dot1x

Enable/Disable: Enable

Security Profile: Corp_dot1x

Primary RADIUS Accounting Server: IDAC17222328

Secondary RADIUS Accounting Server: No RADIUS

Accounting Interim Interval (seconds): 3600 (Valid range: [600-36000])

Beacon Interval (msec): 100 (Valid range: [20-1000])

SSID Broadcast: On

Figure 15: Security and RADIUS Profiles Mapped to ESS Profile

The top screenshot displays the 'RADIUS Configuration Table (2 entries)' with the following data:

RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Called-Station-ID Type	Owner
IDAU17222328	172.22.32.8	1812	Hyphen (-)	Shared Key	Default	controller
IDAC17222328	172.22.32.8	1813	Hyphen (-)	Shared Key	Default	controller

The bottom screenshot shows the 'Security Configuration Table - Update' for the profile 'Corp_dot1x'. The 'WPA2' checkbox is checked, and the 'Primary RADIUS Profile Name' is set to 'IDAU17222328'.

Creating Authorization Profiles

In Identity Manager, you need to create an authorization profile for the corporate users. This profile, which is named “corporate users,” allows Identity Manager to differentiate between corporate employees and visitors or guest users who access the same wireless infrastructure. (See [Figure 16.](#))

Figure 16: Authorization Profiles Page

The screenshot shows the 'Authorization Profiles' page in the Identity Manager Administration interface. The table below lists the existing profiles:

Name	Description
corporate users	Auth profile for corporate users
Default	Default authorization profile
Secure Guest Access	For secure guest access

Create an Authentication Policy for an External Active Directory Server

Create an authentication policy for Identity Manager to authenticate employees using the corporate Microsoft Active Directory server database. In this use case, Identity Manager performs the RADIUS aspect; the user credentials are queried from the Active Directory server for every authentication request that comes in to Identity Manager.

To create an authentication policy:

1. Fill in the basic information. [Figure 17](#) shows the information used in his use case.

Figure 17: Adding an Active Directory Server

Add Authentication Server

Name: 172.22.32.6

Server Type: Microsoft Active Directory

Server: 172.22.32.6

Domain: bangalore.merunetworks.com

Encryption: None

This server supports encryption, but its certificate cannot be validated. You must upload its certificate or its root certificate to continue:

Certificate: Browse...

Base DN: DC=bangalore,DC=merunetworks,DC=com [server default]

< Back Next > Exit

2. Create an attribute mapping to put users in the appropriate authorization profile, which is “corporate users” in this example (shown in [Figure 18](#)).

Figure 18: Attribute Mappings

Add Authentication Server

Connection

Name: 172.22.32.6

Server Type: Microsoft Active Directory

Server: 172.22.32.6

Domain: bangalore.merunetworks.com

Attribute Mappings

The response from the external server is tested against each rule below in order. If a rule is matched the specified usage profile and authorization profile are applied and guest authentication succeeds.

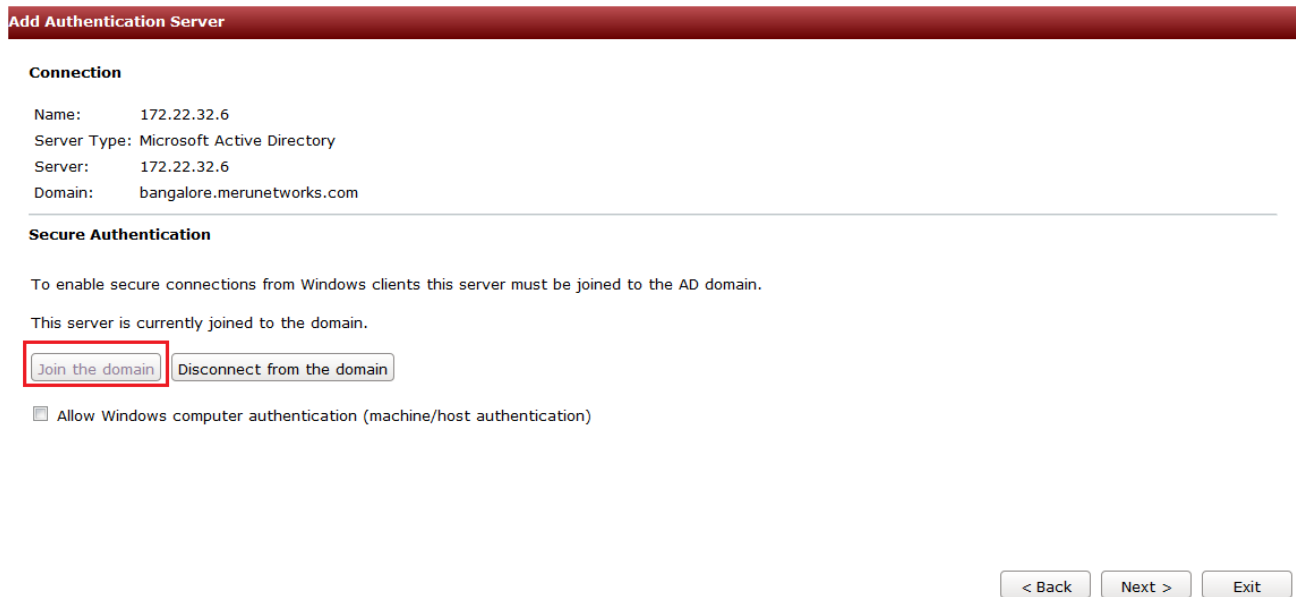
If no rules match Accept authentication set usage profile to Unlimited and authorization profile to corporate users

[add_mapping](#)

< Back Next > Exit

3. Make sure that Identity Manager joins the domain that Active Directory server represents, as shown in [Figure 19](#).

Figure 19: Identity Manager Joins Active Directory Domain



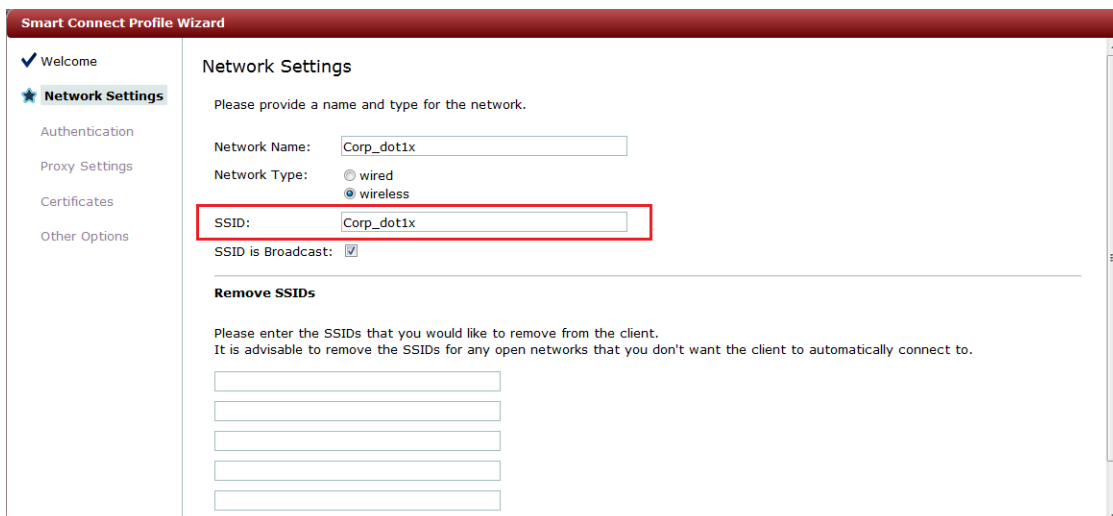
Creating a Smart Connect Profile for 802.1X Clients

You now need to create a Smart Connect profile. For this use case, you create a Smart Connect profile named “Corp_dot1x,” which uses WPA2 enterprise security. Clients using 802.1X use this profile to connect to an SSID named “Corp_dot1x.”

To create a Smart Connect profile:

1. Fill in the appropriate information on the Network Settings page, as shown in [Figure 20](#).

Figure 20: Network Settings Page



2. Select **WPA/WPA2 Enterprise** as the authentication type, and leave the username format as is, as shown in [Figure 21](#).

Figure 21: Authentication Page

The screenshot shows the 'Smart Connect Profile Wizard' window. The left sidebar has 'Authentication' selected. The main area contains the following fields and options:

- Authentication:** WPA/WPA2 Enterprise (dropdown)
- EAP Type:** Windows (PEAP/MSCHAPv2), Apple iOS / OS X (PEAP/MSCHAPv2 and PEAP/GTC), Android (PEAP/GTC), Linux (PEAP/GTC)
- Include Credentials:** Include username/password in profile sent to user, Don't include username/password in profile sent to user
- Username Format:** realm\username, realm/username, username@realm, username
- Realm:** [text input field]
- Detect and override username format and realm when authenticating against Active Directory:**

Navigation buttons at the bottom right: < Back, Next >, Exit.

3. Select any of the default certificates. If an organizational certificate must be used, upload it to Identity Manager and select that certificate for the authentication. In this example, select **Thawte Premium Server CA**, as shown in [Figure 22](#).

Figure 22: Certificates Page

The screenshot shows the 'Smart Connect Profile Wizard' window. The left sidebar has 'Certificates' selected. The main area contains the following elements:

- Certificates:** Please select the CA certificates that you want to install into the trusted root CA store on the client.
- CA Certificates List:** A list of certificates with checkboxes. 'Thawte Premium Server CA' is checked and highlighted with a red box. Other certificates include Equifax, Entrust.net, VeriSign, and Thawte DV SSL CA.
- Upload Certificate:** [text input field] Browse... Upload

Navigation buttons at the bottom right: < Back, Next >, Exit.

Creating a Smart Connect Policy

Smart Connect policies are required to create rules that map authorization profiles (guest roles) to the appropriate Smart Connect profiles. You can have multiple Smart Connect profiles with different security methods, which can be assigned to different sets of users.

1. Create a rule to match the guest role (authorization profile) to “corporate users,” as shown in [Figure 23](#).

Figure 23: Rule Conditions Page

Smart Connect Rule Wizard

✓ Welcome
✓ Details
★ **Conditions**
Assign Profile

Rule Conditions

All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.

✖ If [guest-role](#) equal to [corporate users](#)

[Add Condition](#)

< Back Next > Exit

2. Add a condition to assign “Corp_dot1x” Smart Connect profile to users who belong to guest role “corporate users,” as shown in [Figure 24](#).

Figure 24: Profiles Page

Smart Connect Rule Wizard

✓ Welcome
✓ Details
✓ Conditions
★ **Assign Profile**

Profiles

Select the Smart Connect profiles that you want to assign to users that match this rule.

No Smart Connect
 Assign Smart Connect Profiles

Available Wireless Profiles
Secure_Guest_Access

Selected Wireless Profiles
Corp_dot1x

Available Wired Profiles

Selected Wired Profiles

Up
Down

Up
Down

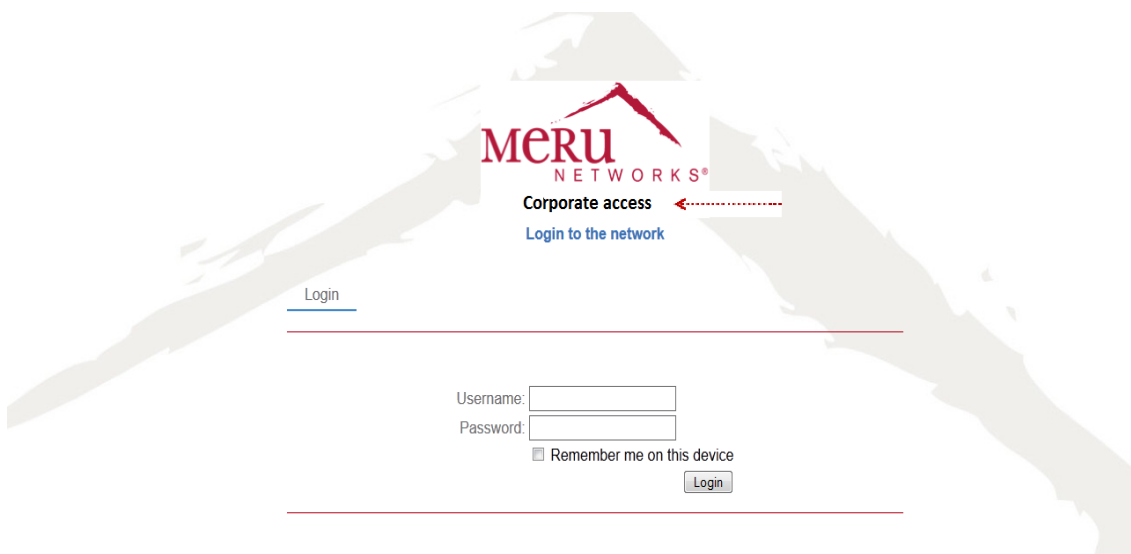
Enabling Smart Connect on the Employee Provisioning Portal

You need to create the employee provisioning portal and enable Smart Connect for the portal. In this use case, users who connect to the ESSID named “Corp Employee Portal” are directed to the employee provisioning portal. After the user is authenticated, the Smart Connect plug-in is available to download from the authentication success page.

To create the provisioning portal and enable Smart Connect:

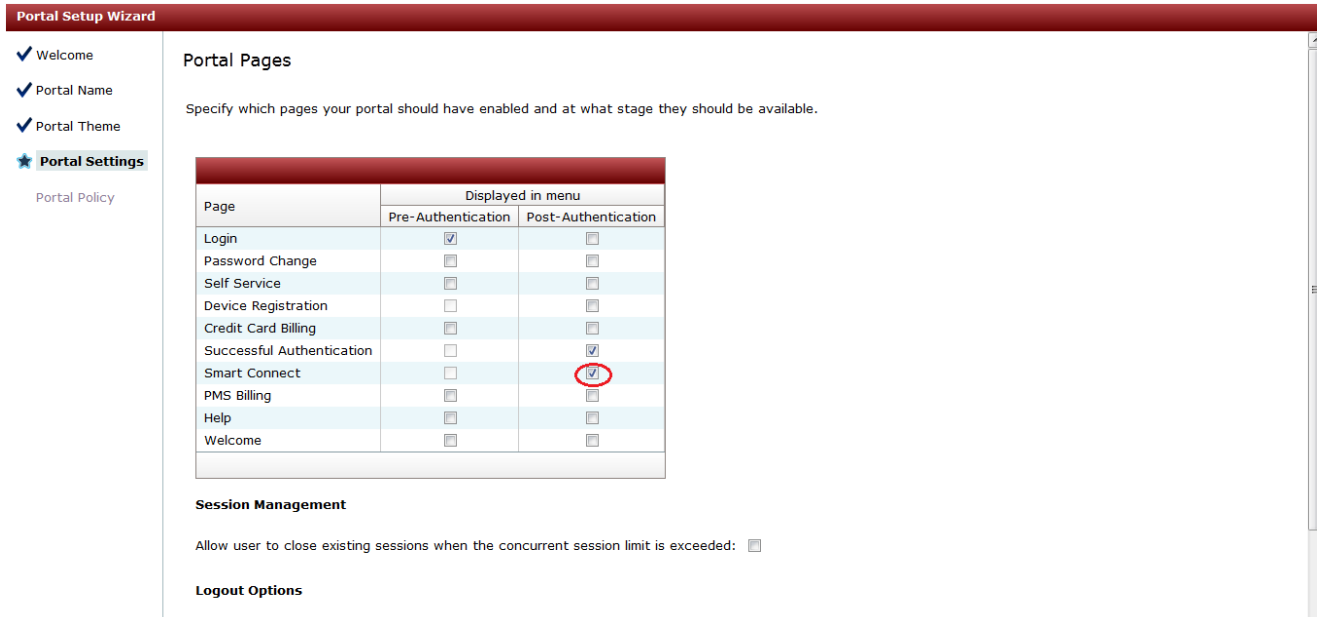
1. Fill in the appropriate information for the initial portal page.
2. Edit the portal theme and change the theme as required. In this example, the same login theme is used, but the logo is modified to identify that the portal is to be used only by corporate employees (shown in [Figure 25](#)).

Figure 25: Portal with Modified Logo



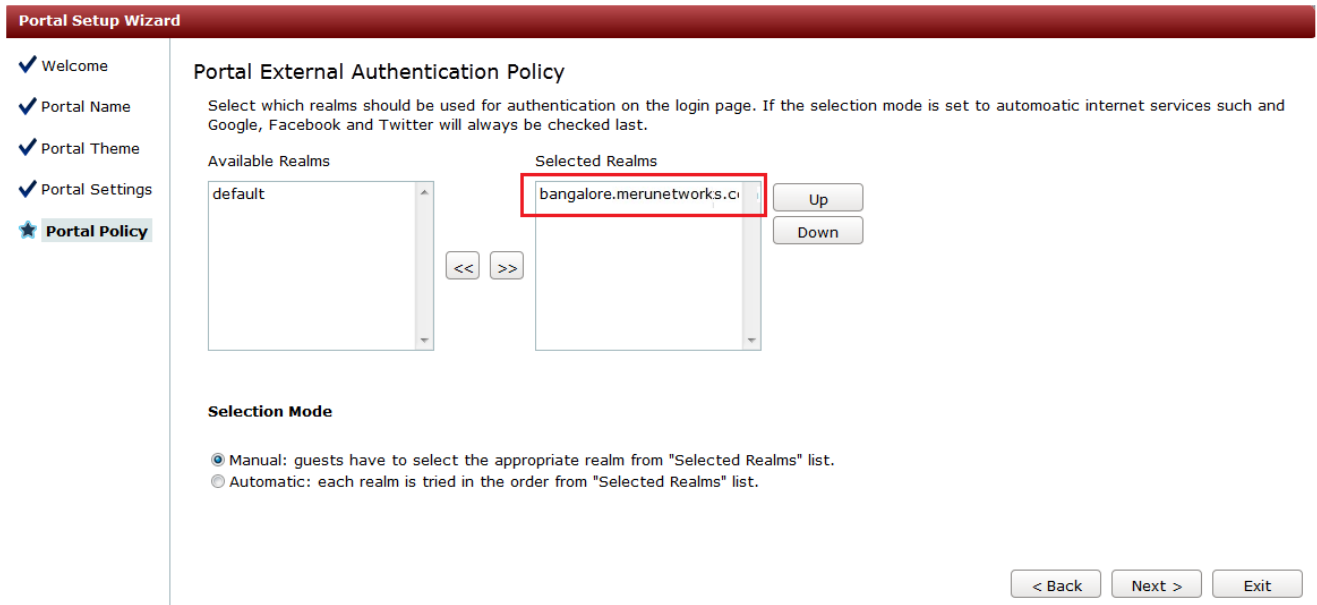
3. To enable Smart Connect, select the Smart Connect check box in the Post-Authentication column, as shown in [Figure 26](#).

Figure 26: Enabling Smart Connect for the Employee Provisioning Portal



4. Add the realm (Active Directory domain) to the portal, as shown in [Figure 27](#). By selecting only the corporate realm, users need to provide only the username and password (and not the full domain).

Figure 27: Adding the Realm to the Portal



After filling out the portal wizard pages, the portal appears in the list of portals, as shown in [Figure 28](#).

Figure 28: Employee Provisioning Portal



Installing the Smart Connect Plug-In on Windows Clients

This example shows how a corporate employee uses a Windows laptop to connect to the self-provisioning network (Corp Employee Portal) to download and install Smart Connect and connect automatically to the secure WPA2 ESSID (Corp_dot1x).

The following describes how to install Smart Connect on Windows clients:

1. Using the Windows client, connect to the provisioning network.
2. Open a Web browser window. The browser is redirected to the Captive Portal page. See [Figure 29](#).
3. Provide authentication credentials. See [Figure 30](#).
4. If authentication is successful (see [Figure 31](#)), a page with network encryption options appears. Two options are available:
 - Downloading the Smart Connect profile so that the device can establish secure encrypted network access.
 - Continue to access the network with an unencrypted network. (The Smart Connect profile is not installed, and the user remains connected to the provisioning network.)
5. Click the Smart Connect button to start the download process.



The button or link that the user clicks varies, depending on the page the Identity Manager administrator has configured to present to users.

- Click the download button to download the Smart Connect plug-in. If a Java browser plug-in is installed on the client device, the Smart Connect plug-in download process starts automatically.



The button or link that the user clicks varies, depending on the page the Identity Manager administrator has configured to present to users.

- Depending on the browser used, click **Save** or **Run** to download the plug-in. After the plug-in is downloaded, it is automatically started. The user credentials are automatically shown. See [Figure 32](#).
- Click **Start**. Progress of the plug-in configuration is shown.
- Click **Connect**. The client is disconnected from the provisioning network and connected to the secure ESSID with the security parameters configured in the Smart Connect profile, as shown in [Figure 33](#).
- Click **Close**.

Figure 29: Connecting to Employee Portal and Getting Redirected



Figure 30: Providing Corporate User Credentials



Figure 31: Successful Authentication Page



Figure 32: Installing Smart Connect

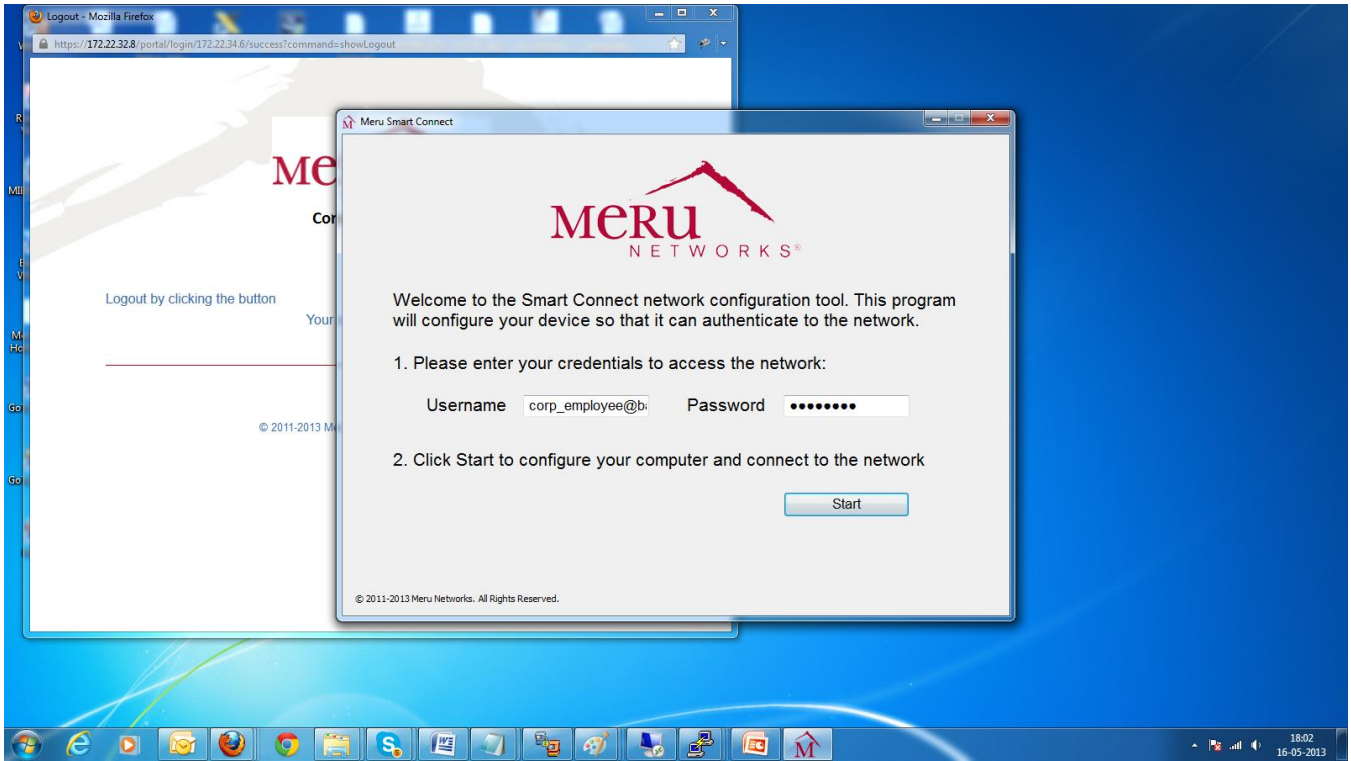


Figure 32: Installing Smart Connect (Continued)

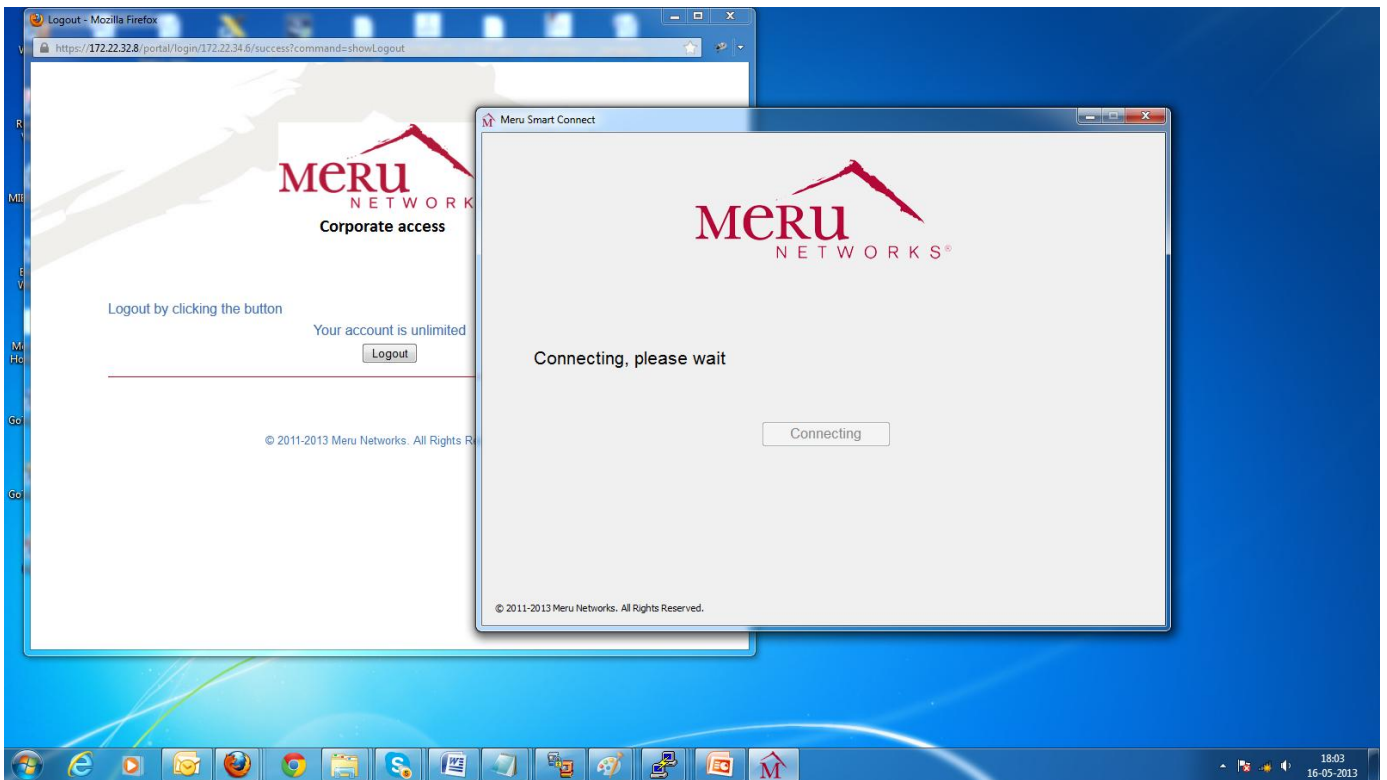
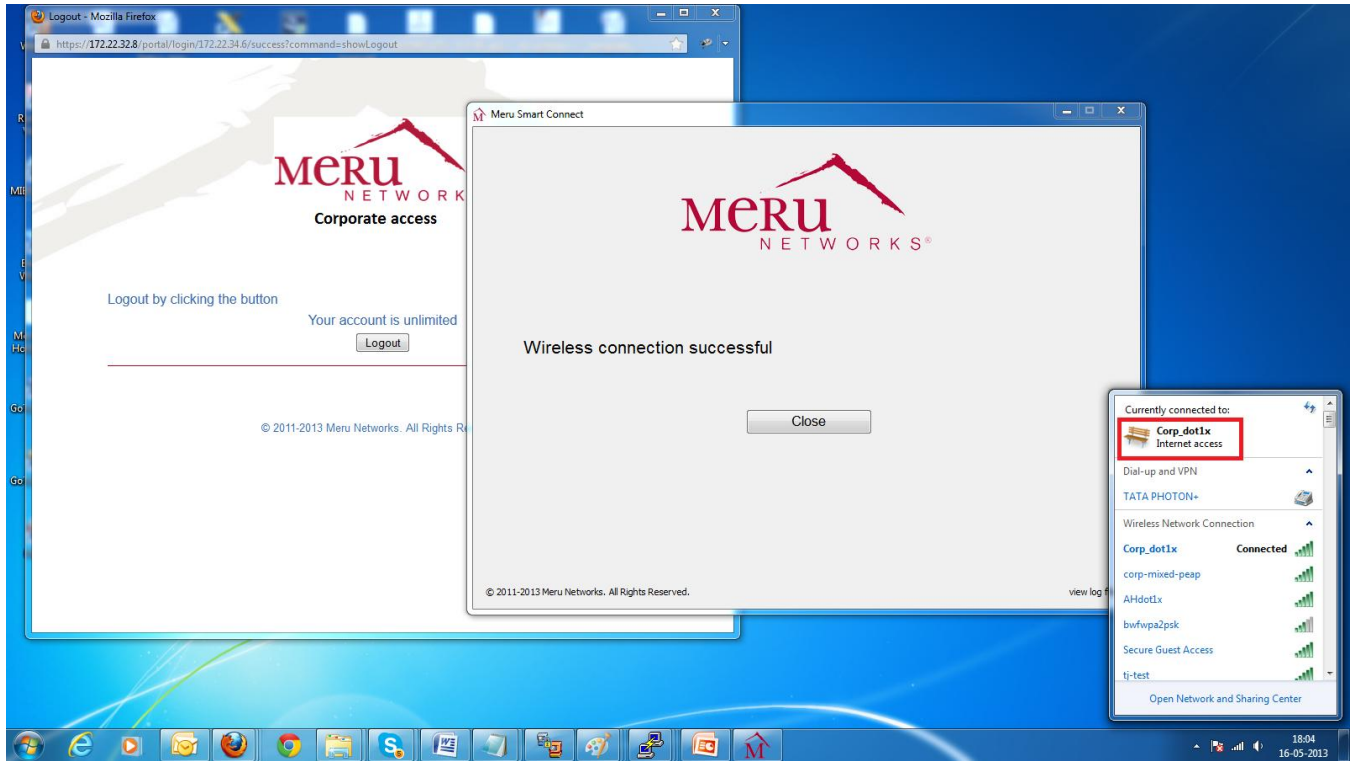


Figure 33: Automatically Connecting to WPA2-Enabled ESSID



Use Case 2: Providing Secure Guest Access

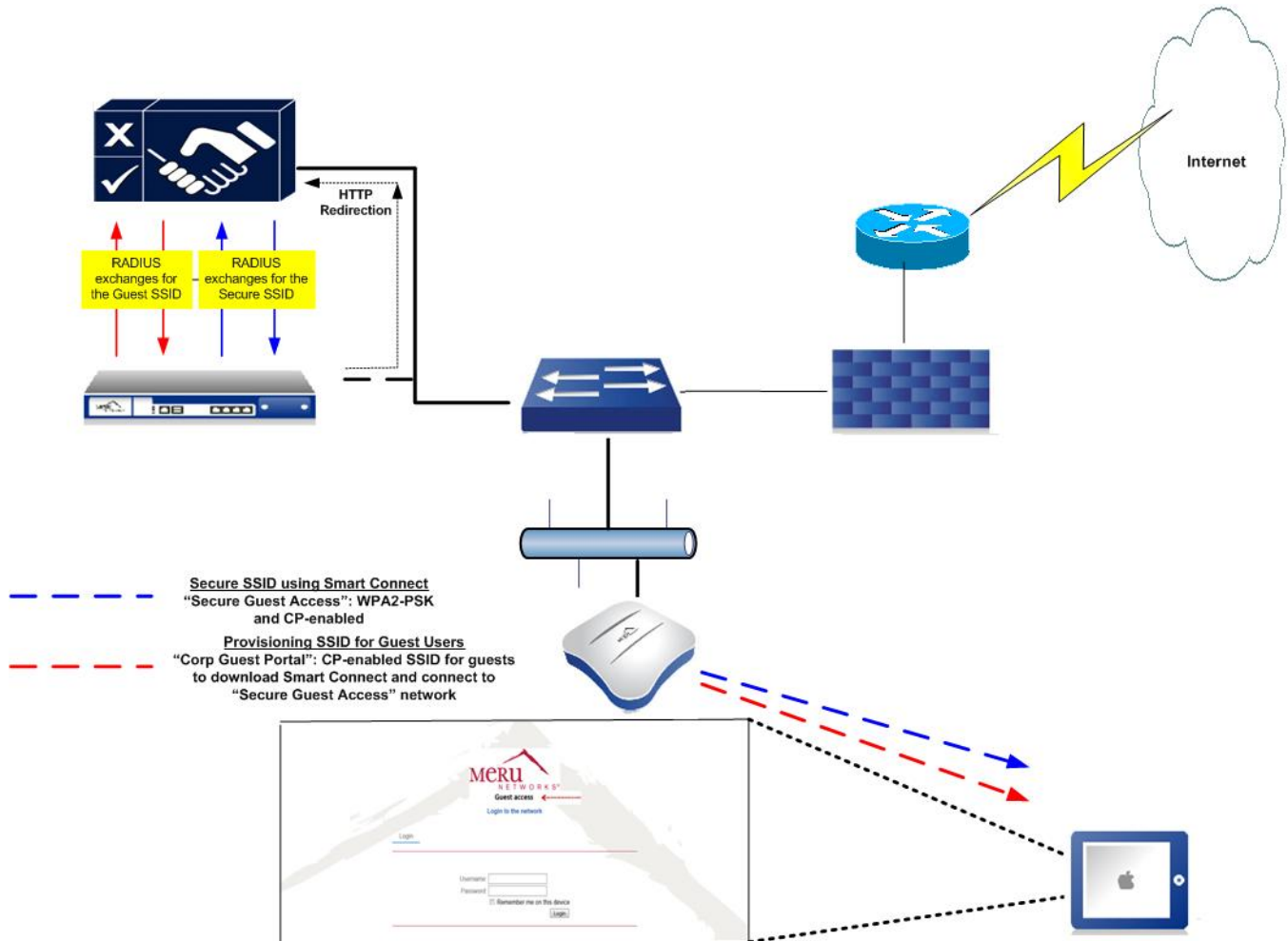
A common security concern about guest networks using Captive Portal authentication is that data sent over the wireless network are not encrypted, making the network and users vulnerable to attacks. Using WPA2-PSK to encrypt data offers increased security, but configuring the pre-shared key for each device that connects to your network can be challenging.

This use case applies to network administrators who must enable network devices to connect to the secure wireless network for guest access. This use case illustrates the process of self-provisioning of users with Apple iPad devices to connect to the WPA2-PSK-enabled network. The same use case applies to all users, regardless of the type of end device. Smart Connect and Identity Manager automatically detect the type of device connecting to the network and correctly configure the device for secure network access.

After users initially connect to the provisioning network and are successfully authenticated using guest credentials, they can download and install the Smart Connect profile, which automatically configures and connects to the secure guest wireless network. On subsequent visits, users are authenticated using the Captive Portal and connected to the secure guest network with the assurance that all their data and transactions are securely encrypted.

[Figure 34](#) shows the network diagram for Use Case 2.

Figure 34: Use Case 2 Network Diagram



You perform the following configuration tasks for this use case:

- [Controller Configuration Tasks](#)
- [Creating an Authorization Profile for Guest Users](#)
- [Create a Smart Connect Profile](#)
- [Create a Smart Connect Policy](#)
- [Creating a Guest Portal](#)
- [Creating a Portal Rule](#)
- [Installing the Smart Connect Profile on iPad Clients](#)

Controller Configuration Tasks

This use case uses the same network environment as Use Case 1 to provide secure network access for guest users in that network. When configuring secure network access for guest users, you can optionally perform additional configuration tasks to control access for the guest users.

Before configuring Smart Connect with Identity Manager, perform the following tasks on the controller:

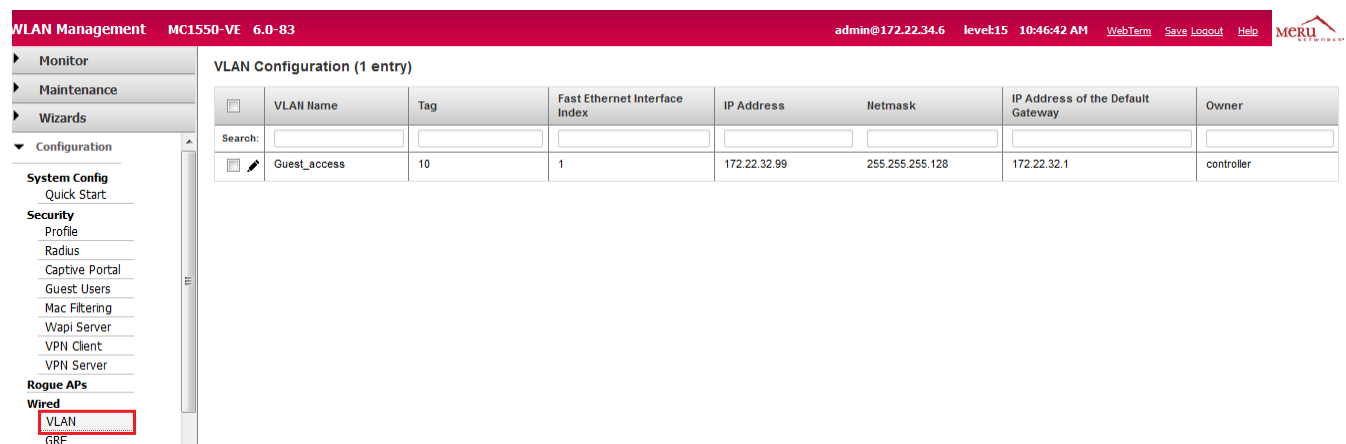
- Create a VLAN for the guest users/network. This VLAN IP address range is used to redirect guest users to the corporate guest portal, rather than the employee provisioning portal, which was configured in Use Case 1.
- Create an ESS profile with a WebAuth-enabled security profile mapped to it.
- Create a secure ESS profile with WPA2-PSK and WebAuth-enabled security profile mapped to it.
- (Optional) Create another VLAN and map it to the WPA2-PSK enabled secure SSID. You can also create a third portal for guest users who connect to the Secure SSID, based on the IP address range of the VLAN to allow additional access control for guest users.

After a guest user connects to the secure SSID, there is no way for you or other administrators to control access for the guests without enabling Captive Portal. Without enabling Captive Portal, guest users who have downloaded the Smart Connect client used to connect to the secure network can access that network as long as they are within range of the network.

Creating a VLAN for Guest Users

In this use case, you need to create a VLAN for guest users called Guest_access, as shown in [Figure 35](#).

Figure 35: Creating a VLAN



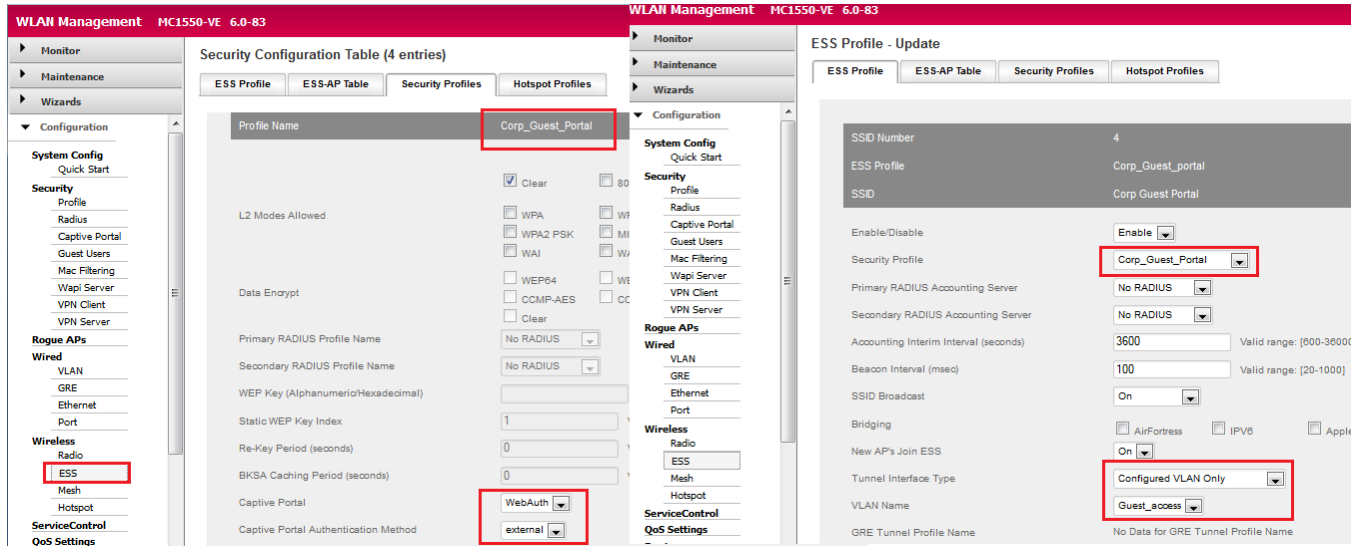
The screenshot displays the Meru Networks WLAN Management interface. The top navigation bar includes the title 'WLAN Management', the device identifier 'MC1550-VE 6.0-83', the user 'admin@172.22.34.6', the level 'level15', the time '10:46:42 AM', and links for 'WebTerm', 'Save', 'Logout', and 'Help'. The left sidebar shows a menu with categories: Monitor, Maintenance, Wizards, Configuration, System Config, Security, Rogue APs, and Wired. The 'Wired' category is expanded, showing 'VLAN' and 'GRE'. The main content area is titled 'VLAN Configuration (1 entry)' and contains a table with the following data:

	VLAN Name	Tag	Fast Ethernet Interface Index	IP Address	Netmask	IP Address of the Default Gateway	Owner
Search:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Guest_access	10	1	172.22.32.99	255.255.255.128	172.22.32.1	controller

Creating a WebAuth-Enabled Security Profile

Create a WebAuth-enabled security profile and map it to an ESS profile (Corp Guest Portal), which is the provisioning network. (See [Figure 36.](#))

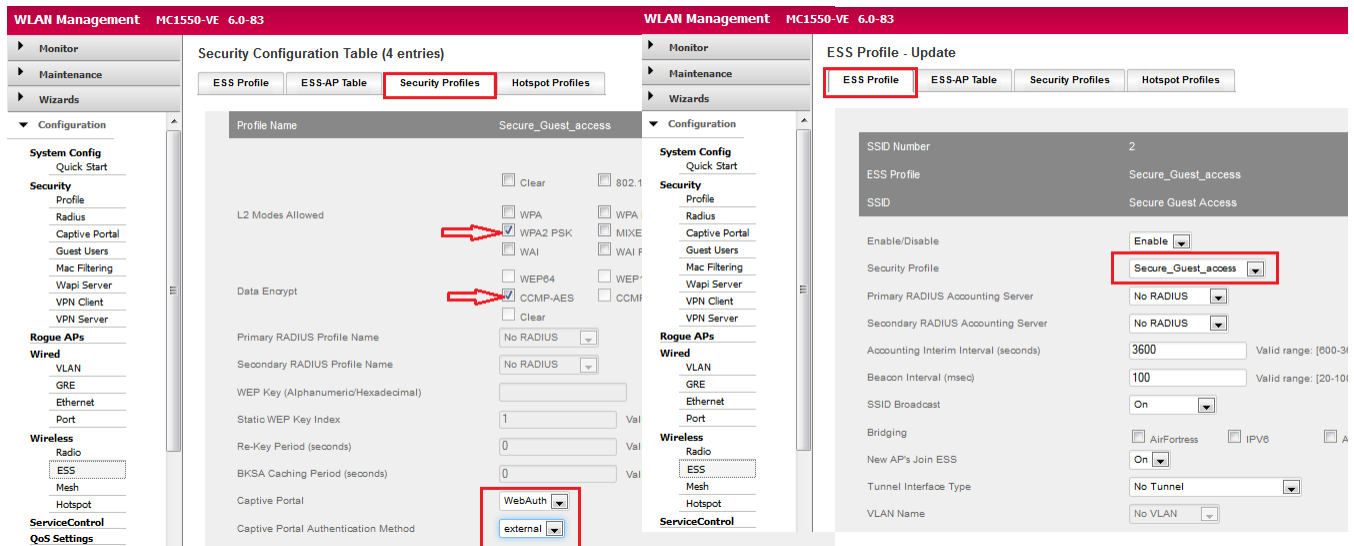
Figure 36: Creating a WebAuth-Enabled Security Profile



Creating a WPA2-PSK-Enabled Security Profile

Create a WPA2-PSK enabled security profile and map to an ESS profile (Secure Guest Access), which is a secure network for guest users. (See [Figure 37.](#))

Figure 37: Creating a WPA2-PSK-Enabled Security Profile

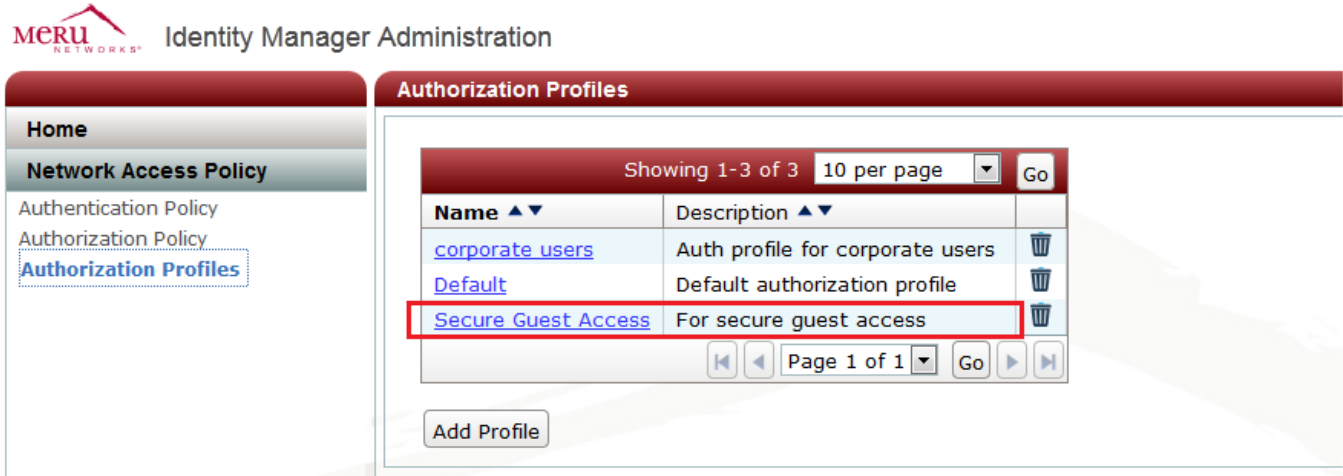


For information about how to create and manage VLANs, ESS profiles, and security profiles, see the *Meru System Director Configuration Guide*.

Creating an Authorization Profile for Guest Users

In this use case, you need to create an authorization profile (guest role) named Secure Guest Access for the users who connects to the provisioning network, as shown in [Figure 38](#).

Figure 38: Creating Authorization Profile for Guest Users



Create a Smart Connect Profile

You need to create a Smart Connect profile with authentication enabled. In this use case, the Smart Connect profile is named Secure_Guest_Access, as shown in [Figure 39](#) and is configured with WPA2-PSK as the authentication method, as shown in [Figure 40](#).

Figure 39: Creating a Smart Connect Profile

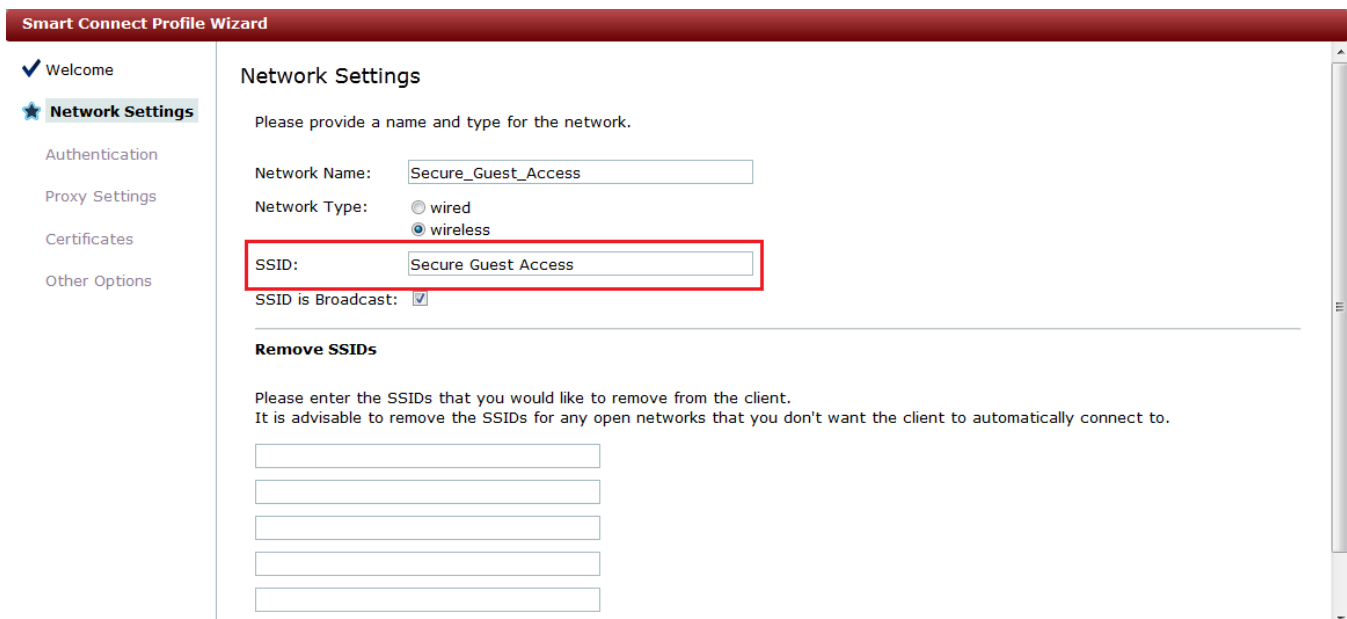
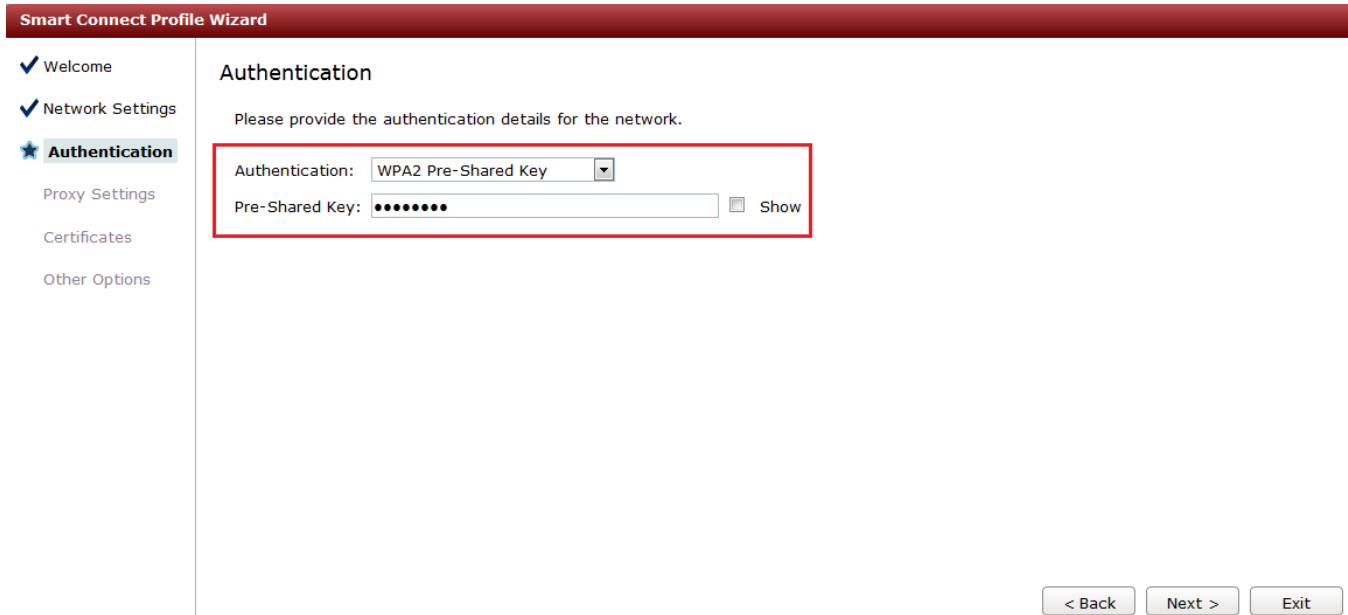


Figure 40: Specifying WPA2-PSK

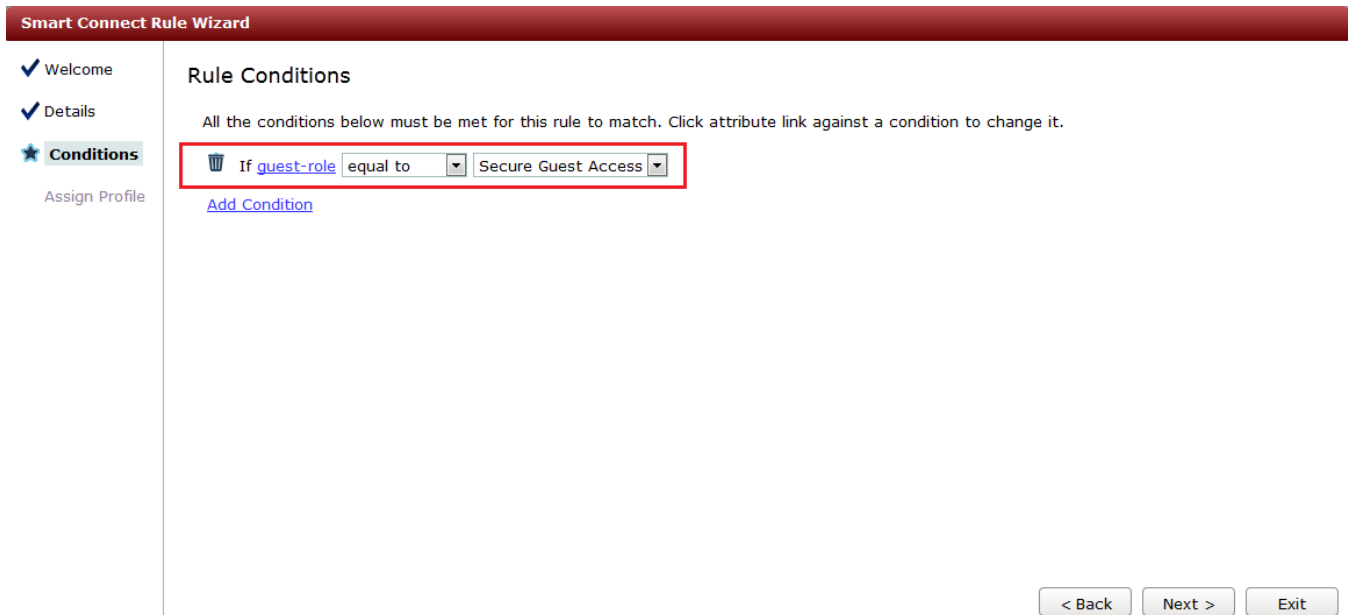


The screenshot shows the 'Smart Connect Profile Wizard' interface. On the left, a navigation pane lists 'Welcome', 'Network Settings', 'Authentication' (highlighted with a star), 'Proxy Settings', 'Certificates', and 'Other Options'. The main area is titled 'Authentication' and contains the instruction 'Please provide the authentication details for the network.' Below this, there are two input fields: 'Authentication:' with a dropdown menu set to 'WPA2 Pre-Shared Key', and 'Pre-Shared Key:' with a text box containing ten dots and a 'Show' button. A red box highlights these two fields. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

Creating a Smart Connect Policy

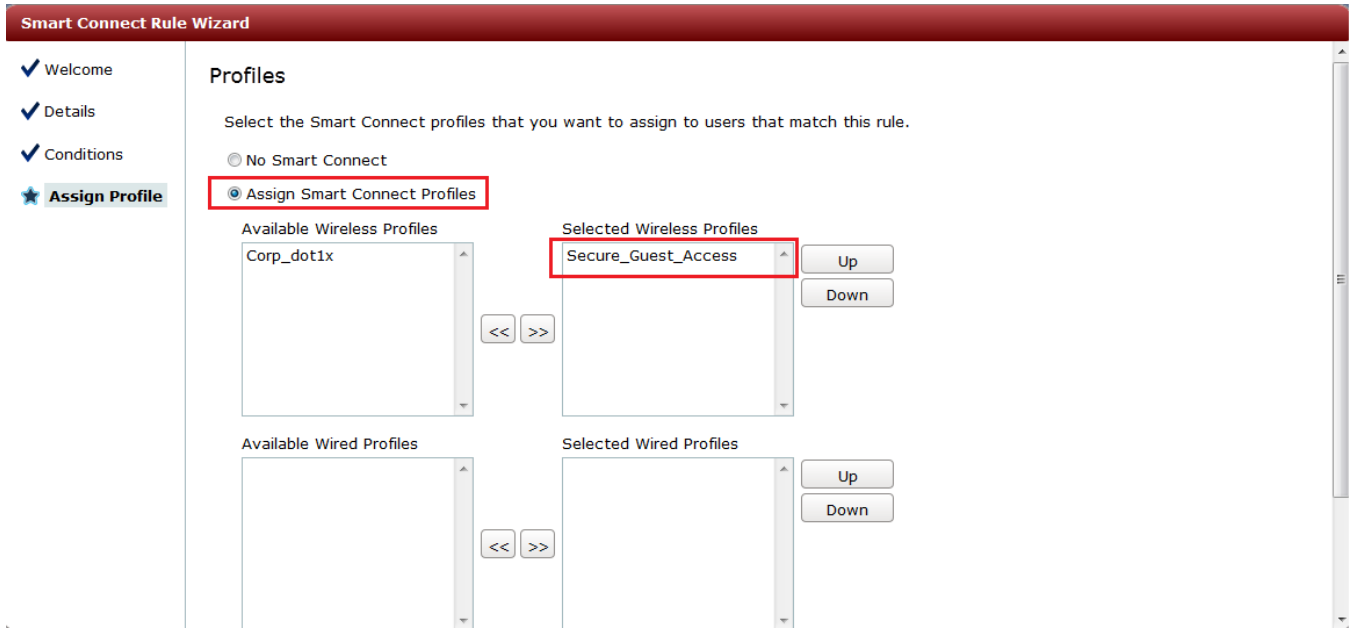
A Smart Connect policy is required to provide users with different Smart Connect profiles. In this use case, all guest users who are part of the “Secure Guest Access” authorization profile are assigned the WPA2-PSK-enabled Smart Connect profile. (See [Figure 41](#) and [Figure 42](#).)

Figure 41: Creating a Rule for Authorization Profile



The screenshot shows the 'Smart Connect Rule Wizard' interface. On the left, a navigation pane lists 'Welcome', 'Details', 'Conditions' (highlighted with a star), and 'Assign Profile'. The main area is titled 'Rule Conditions' and contains the instruction 'All the conditions below must be met for this rule to match. Click attribute link against a condition to change it.' Below this, there is a single condition: 'If guest-role equal to Secure Guest Access'. A red box highlights this condition. Below the condition is a link labeled 'Add Condition'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Exit'.

Figure 42: Assigning Smart Connect Wireless Profiles



Creating a Guest Portal

You need to create a guest portal for which the login page and Smart Connect are enabled. The user device that initially connected to the “Corp Guest Portal” ESSID is now in the “Guest_access” VLAN (172.22.32.0/25) and is redirected to the new portal. This portal login page authenticates the user so that the client and Smart Connect can be downloaded to securely access the guest network using WPA2-PSK (Secure Guest Access).

Edit the portal page and change the logo for the guest portal, which is used for guest access. Users who connect to “Corp Guest Portal” are redirected to the page shown in [Figure 43](#). [Figure 44](#) shows how to enable Smart Connect for the portal.

Figure 43: Guest Access Portal

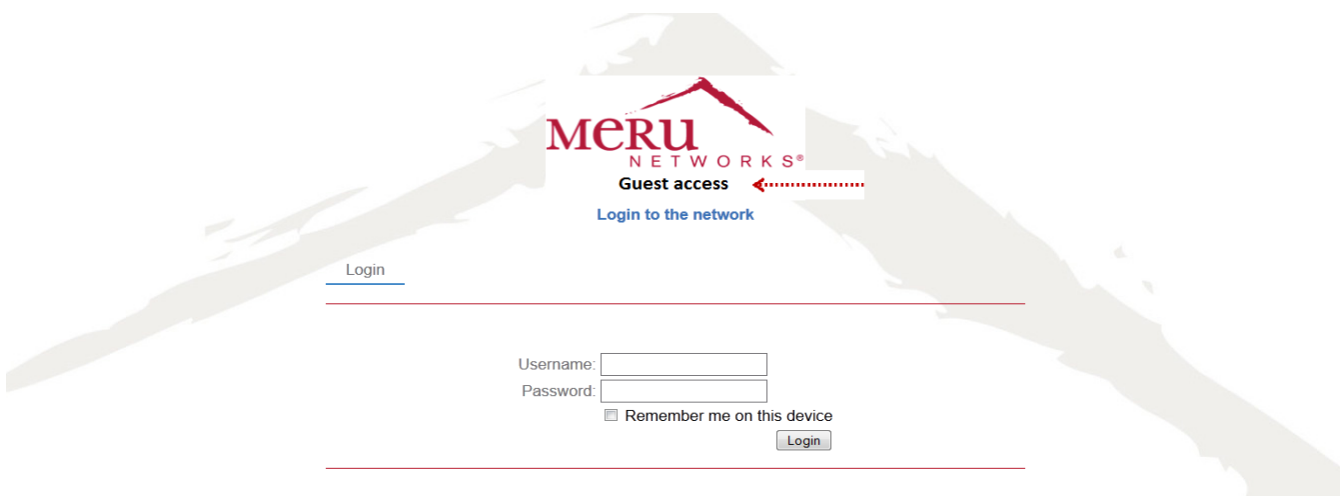
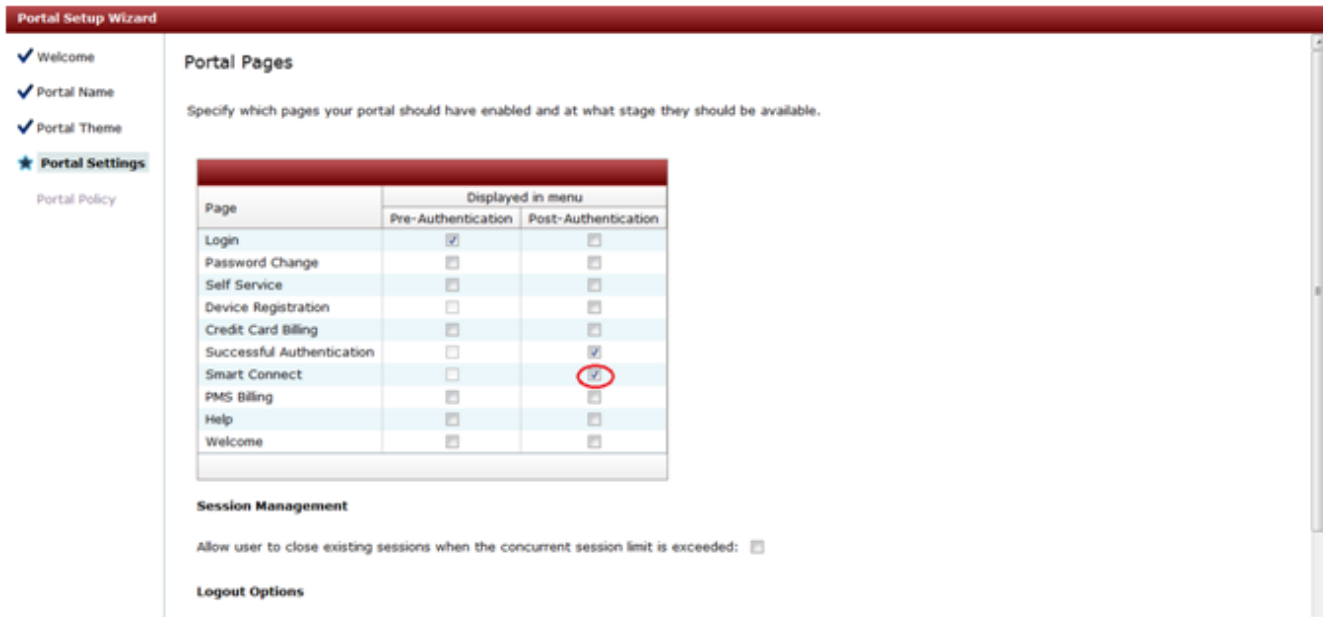


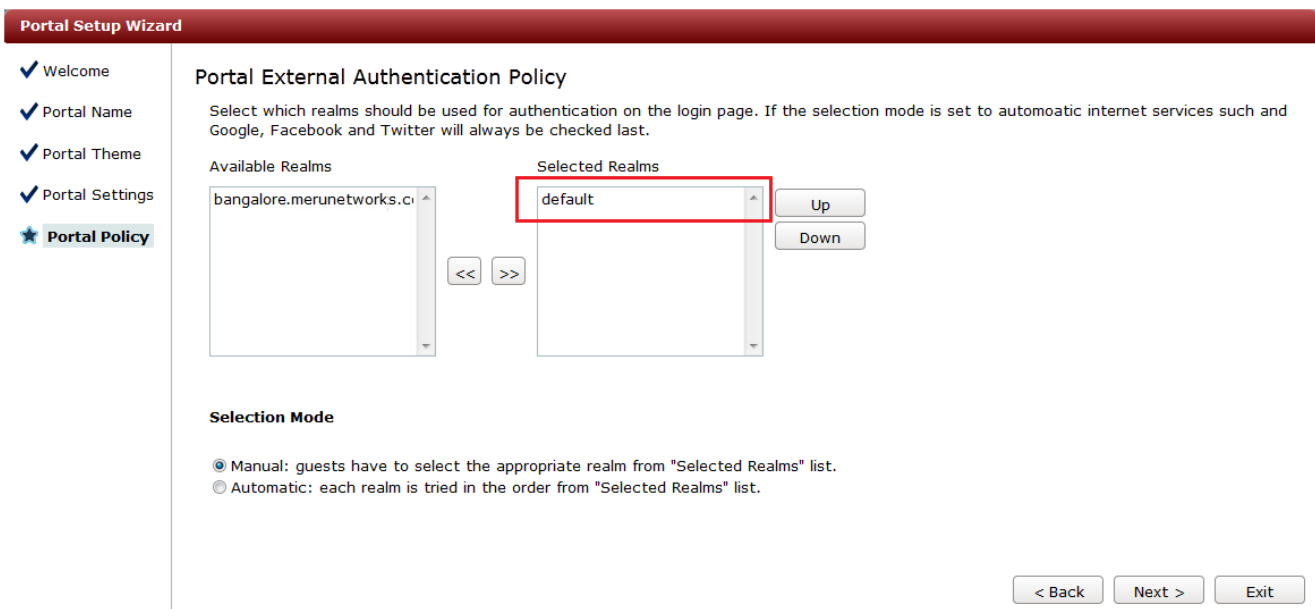
Figure 44: Enabling Smart Connect for the Guest Portal



Specifying the Default Realm

In this use case, you specify the default realm for the guest portal because the guest users who connect to the portal are not users that are defined in the realm for Active Directory users (bangalore.merunetworks.com from Use Case 1). See [Figure 45](#).

Figure 45: Specifying the Default Realm























After making and saving the guest portal changes, the Corp_Guest_Portal that you created appears in the list of portals, as shown in [Figure 46](#).

Figure 46: List of Portals

Meru Networks Identity Manager Administration

Portals

Showing 1-5 of 5 10 per page Go

Name	Description	
access-denied	Default portal that denies access	   
Corp_Employee_portal	Corp_Employee_portal	   
Corp_Guest_Portal	Corp_Guest_Portal	   
login	Default login portal	   
mobile	Default portal for mobile devices	   

Page 1 of 1 Go

Add Portal

Creating a Portal Rule

You need to create a portal rule that directs client devices to the portal that you created in [Creating a Guest Portal](#). In this use case, this rule directs client devices in the 172.22.32.0/25 network to the “Corp Guest Portal,” which allows users to provide authentication credentials to use the secure guest network (Secure Guest Access), as shown in [Figure 47](#).

Figure 47: Edit Rule Page


Meru Networks Identity Manager Administration

Edit Rule

Guests are directed to the specified portal if all the specified conditions are met.

Rule Name:

Rule Description:

 /

[add condition](#)

Rule Action: Go to portal

No portal (sends HTTP 403 Unauthorised header)

Save Cancel

Installing the Smart Connect Profile on iPad Clients

After you have configured Smart Connect, users can install the Smart Connect profile so that they can connect to your network with the authentication and encryption parameters that you set.

When users access your provisioning network for the first time, they are redirected to the Captive Portal page. After successfully providing login credentials, they have the option to download the Smart Connect profile or continue guest access using the provisioning network (user data and transactions are not encrypted).

The Smart Connect profile installation procedure is illustrated in the following procedure for iPad devices. The general installation procedure is the same for other network devices.

1. Establish a connection to the provisioning network (Corp Guest Portal), and provide user credentials in the guest login page. See [Figure 48](#).
2. After successfully logging in, the option to download Smart Connect is provided. See [Figure 49](#).
3. Install the Smart Connect profile. See [Figure 50](#).

After the Smart Connect profile is installed, the device is initially connected to the secure guest network (“Secure Guest Access”), as shown in [Figure 51](#). The Web browser is again redirected to a Captive Portal page in which the user must provide the same authentication credentials. Enabling WebAuth in the secure ESSID is an optional step; however, without captive portal authentication, administrators cannot control or account for user activity in the secure network using WPA2-PSK. When the user subsequently tries to connect to this network, authentication is required only once.



If the iPad device has an ESSID configured as a known network, the iPad device might automatically connect to the known network if the signal strength for that network is stronger than the network specified by the Smart Connect profile.

Figure 48: Guest Login Page



Figure 49: Successful Authentication Page



Figure 50: Installing Smart Connect Profile

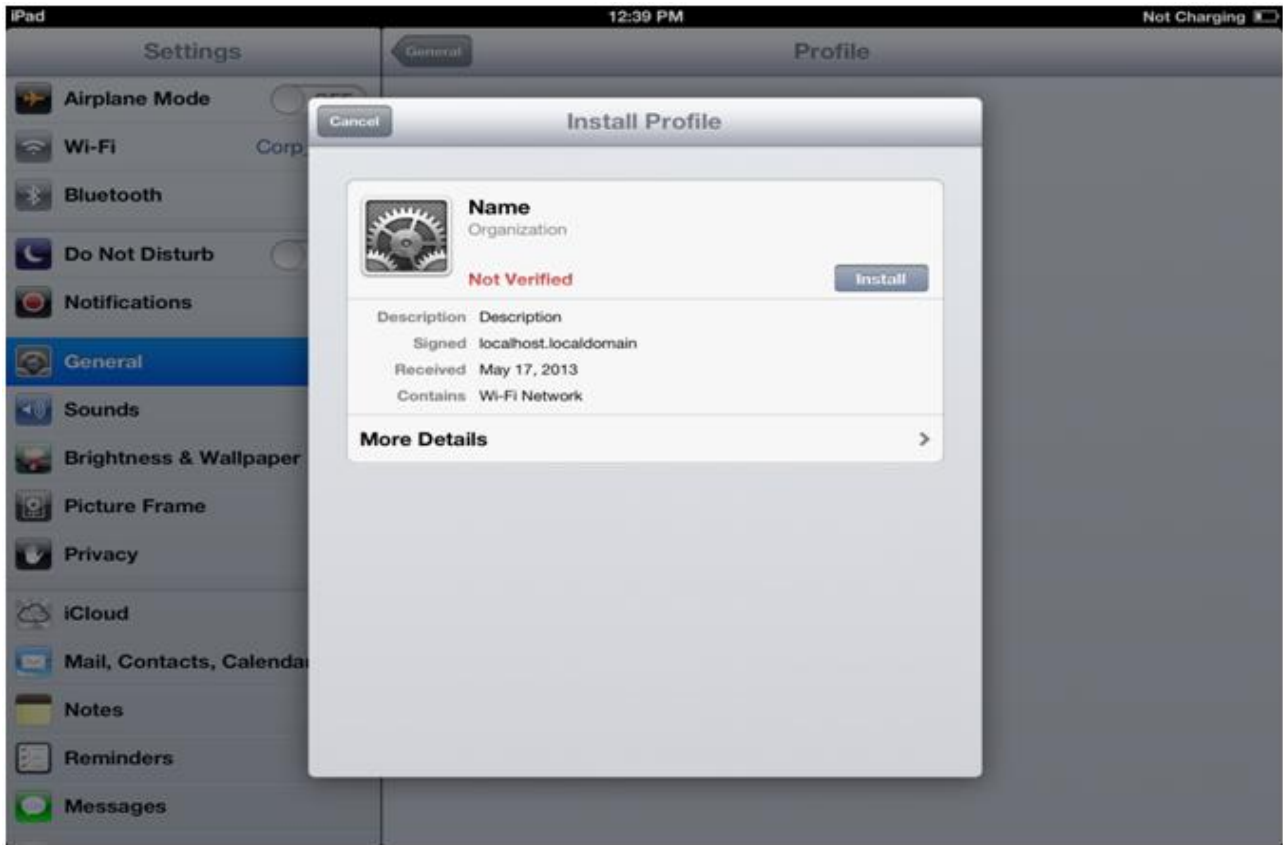
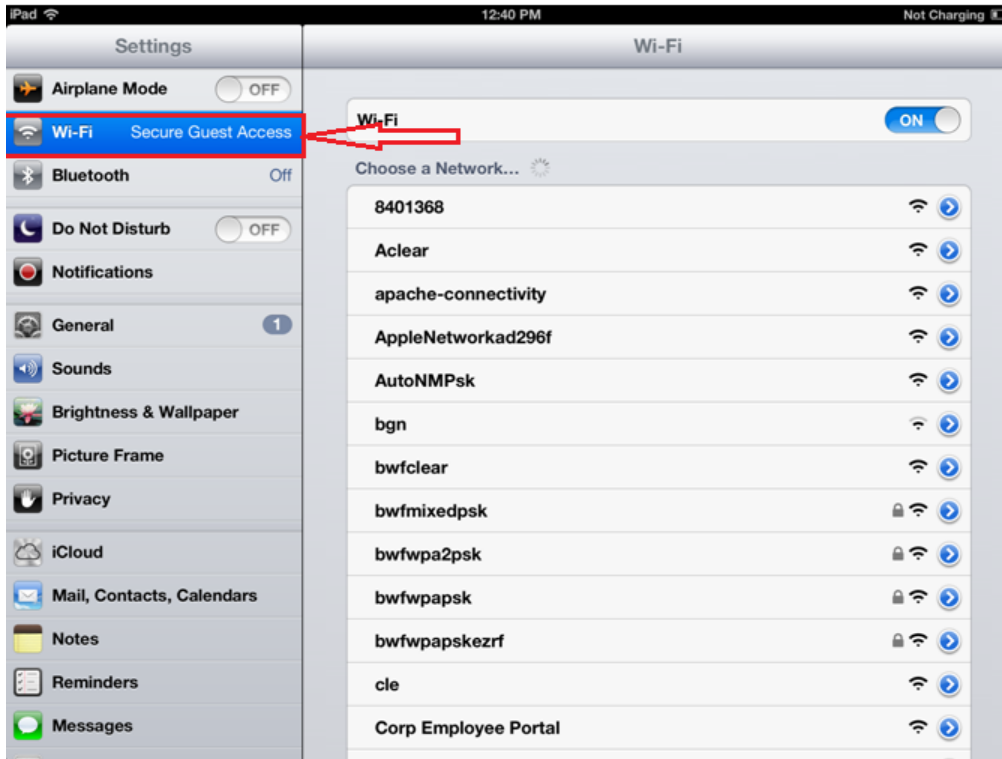


Figure 51: Automatically Connect to Secure Guest Network

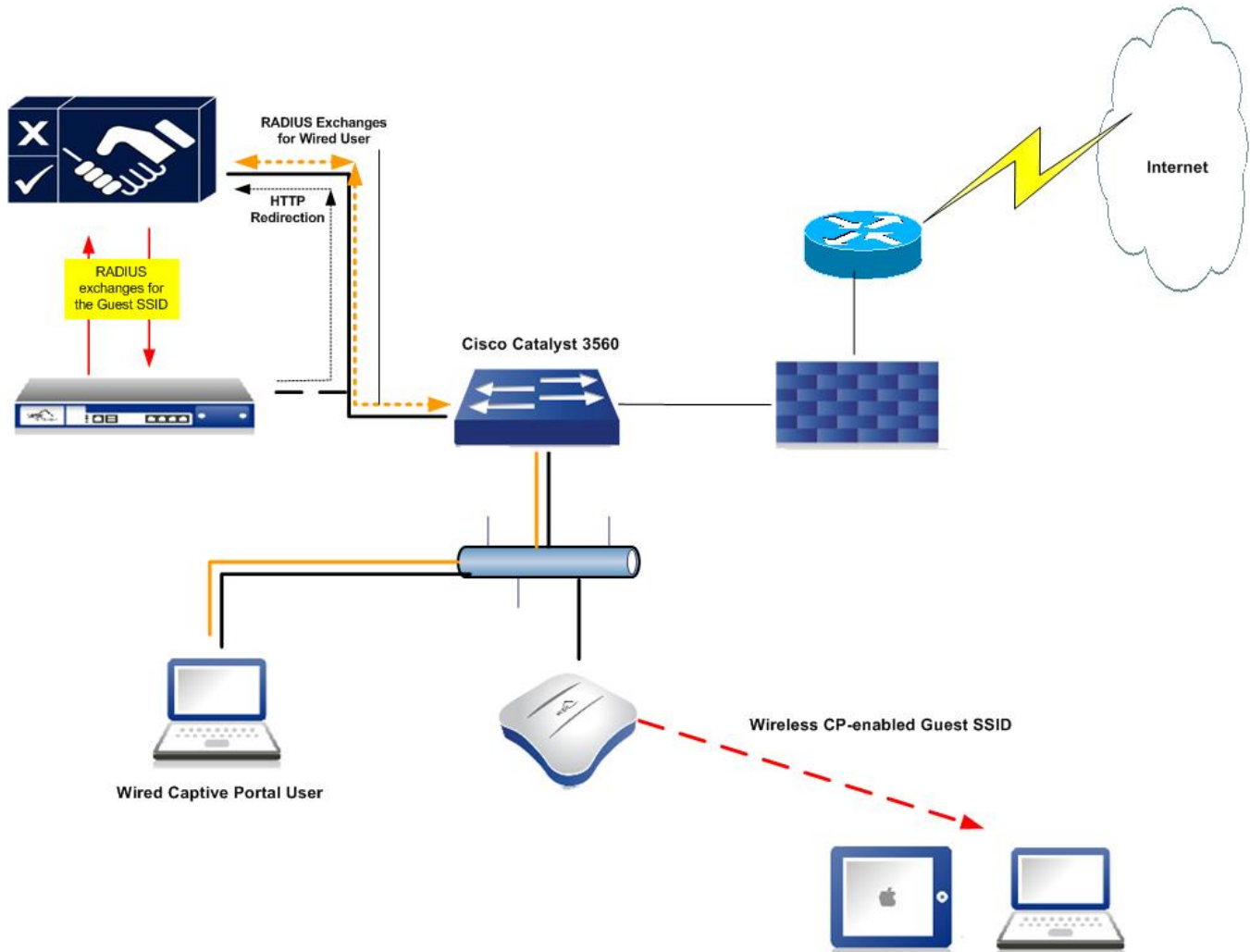


Use Case 3: Configuring Captive Portal for Wired Clients

You can configure wired switches to use a captive portal and Identity Manager to provide the same look and feel for wired and wireless guest users. In this use case, a Cisco Catalyst 3560 switch is used to enable Web authentication, with Identity Manager handling only the RADIUS authentication. If you are using a different network device, the configuration steps can vary; see the documentation for your device for vendor-specific configuration information.

[Figure 52](#) shows the network diagram for Use Case 3.

Figure 52: Use Case 3 Network Diagram



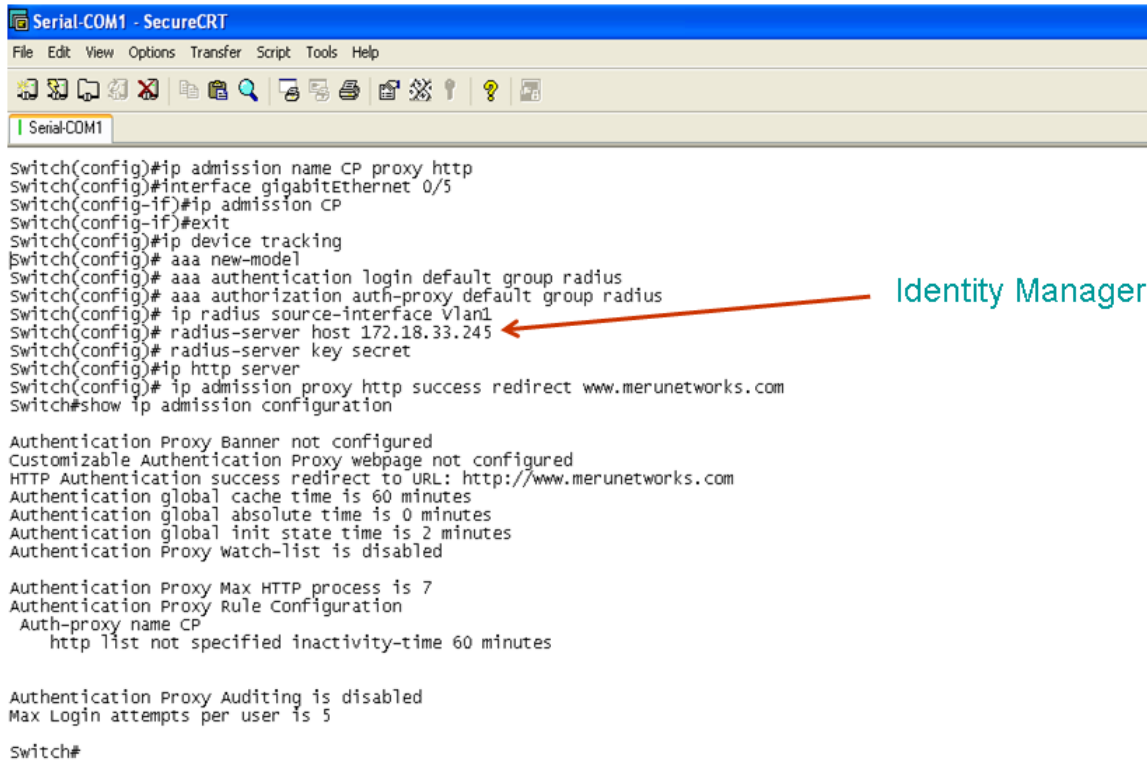
You perform the following tasks to configure Captive Portal for wired clients:

- [Configuring the Switch](#)
- [Configuring Identity Manager](#)
- [Creating a Custom Captive Portal for Web Authentication](#)

Configuring the Switch

[Figure 53](#) shows the configuration for the switch. Note that Identity Manager, whose IP address is 172.18.33.245, is identified as a RADIUS server in the configuration.

Figure 53: Switch Configuration



```
Serial-COM1 - SecureCRT
File Edit View Options Transfer Script Tools Help
Serial-COM1

Switch(config)#ip admission name CP proxy http
Switch(config)#interface gigabitEthernet 0/5
Switch(config-if)#ip admission CP
Switch(config-if)#exit
Switch(config)#ip device tracking
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group radius
Switch(config)# aaa authorization auth-proxy default group radius
Switch(config)# ip radius source-interface vlan1
Switch(config)# radius-server host 172.18.33.245
Switch(config)# radius-server key secret
Switch(config)#ip http server
Switch(config)# ip admission proxy http success redirect www.merunetworks.com
Switch#show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.merunetworks.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Rule Configuration
  Auth-proxy name CP
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5

Switch#
```

Identity Manager

Configuring Identity Manager

You need to configure Identity Manager to recognize the switch as a RADIUS client. The switch has an IP address of 172.18.33.248.

When configuring a RADIUS client in Identity Manager:

- Specify the type of RADIUS client as **Cisco Switch**, as shown in [Figure 54](#).
- As shown in [Figure 55](#), add the following AV pair value: `cisco-AVPair "priv-lvl=15"`. Adding this value specifies that the highest privilege level on the router is used so that you can permit all user traffic for the port after successful user authentication.
- Add the following AV pair value: `cisco-AVPair " auth-proxy:proxyacl#1=permit ip any any"`. Adding this value allows all user traffic after successful user authentication.

Figure 54: RADIUS Client Tab

MCRU NETWORKS Identity Manager Administration

RADIUS Clients

Client | Attributes | SNMP | MAC Authentication | RadSec Authentication

Name: Cisco-3560

Device IP Address / Prefix Length: 172.18.33.248
For example 192.168.1.1/32 or fec0:0001/128

Secret: Confirm:

Type: Cisco Switch
If your RADIUS client vendor is not listed please select Generic RADIUS Device

Form Action: https://1.1.1.1/

Description:

Change-of-Authorization

Use COA:

Port: 3799

Save Cancel

Figure 55: RADIUS Client Attributes Tab

MCRU NETWORKS Identity Manager Administration

RADIUS Clients

✓ RADIUS Client saved.

Client | Attributes | SNMP | MAC Authentication | RadSec Authentication

Vendor: IETF

Attribute: Access-Loop-Encapsulation

Value:

Add AV Pair

Cisco-Call-Filter = "prv-lvl=15"
Cisco-Call-Filter = "auth-proxy:proxyacl#1=permit ip any any"

Move up
Remove
Move down

Save Cancel

You can now connect a wired station to the interface for which Captive Portal is enabled, and the user is redirected to the default Captive Portal splash page for the switch. [Figure 56](#) shows an example of the switch's default Captive Portal page and successful authentication window. To create a custom Captive Portal, see [Creating a Custom Captive Portal for Web Authentication](#)

Figure 56: Example of Switch Default Captive Portal Page and Successful Authentication Window



Creating a Custom Captive Portal for Web Authentication

To create a custom Captive Portal for Web authentication, you perform the following tasks:

- [Defining Custom Captive Portal Pages](#)
- [Previewing the Wired Guest Portal Configured in Identity Manager](#)
- [Configuring the Switch to Permit Traffic to Identity Manager](#)
- [Copying the Custom Captive Portal Pages to the Switch](#)
- [Registering Custom Captive Portal Pages](#)
- [Verifying Authentication Using the Captive Portal Pages](#)

Defining Custom Captive Portal Pages

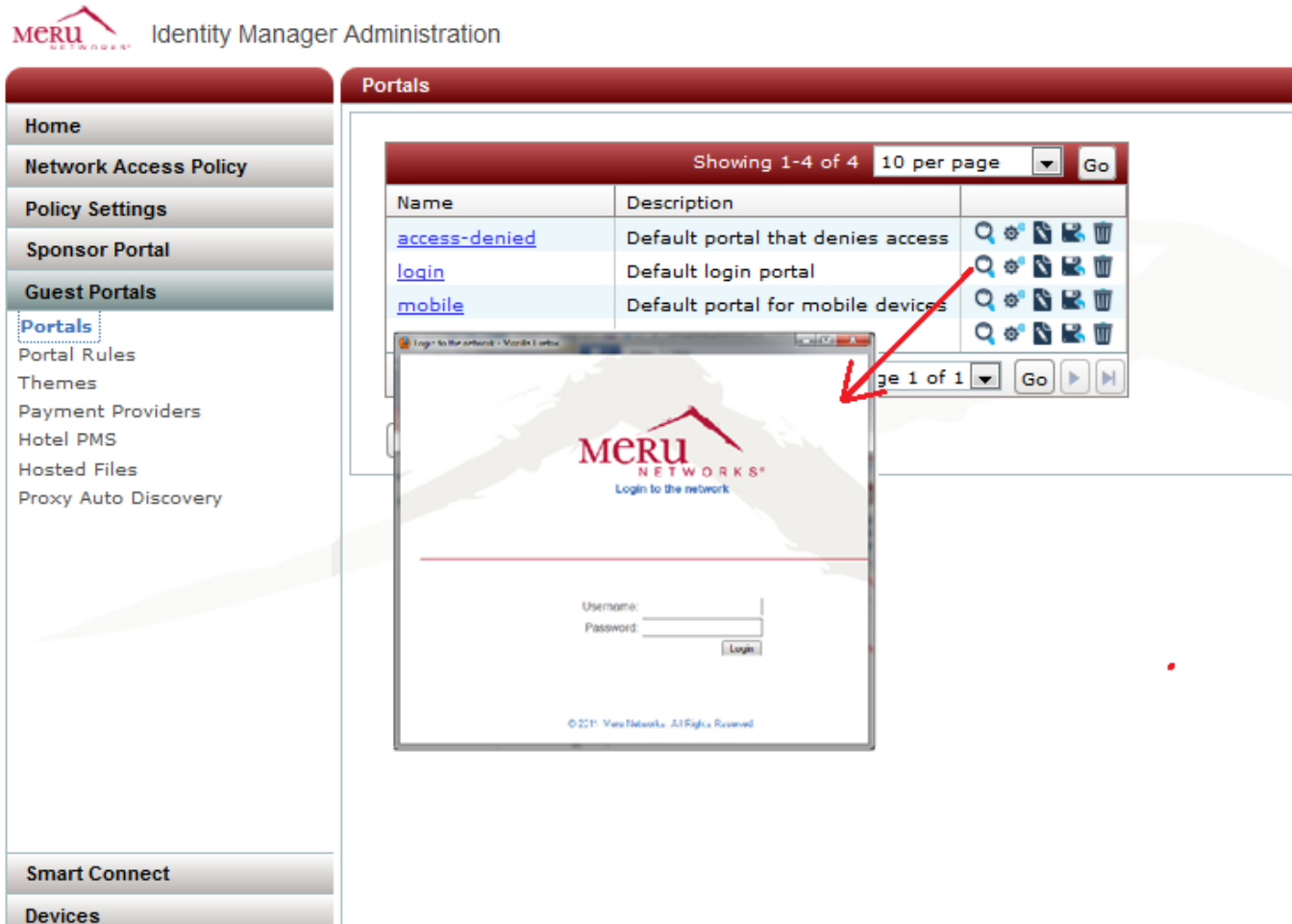
If you do not want to use the switch's default Captive Portal pages that are provided, you can transfer Identity Manager guest portal pages to use for the Captive Portal. In this use case, a set of default Identity Manager portal pages is used. You can customize guest portal pages using Identity Manager. For more information, see the *Meru Identity Manager User Guide*.

Previewing the Wired Guest Portal Configured in Identity Manager

To preview the wired guest portal:

1. In the Identity Manager Administration Interface, select **Guest Portals > Portals**.
2. Click the Preview icon of the wired guest portal, as shown in [Figure 57](#).

Figure 57: Preview Wired Guest Portal



Configuring the Switch to Permit Traffic to Identity Manager

You need to configure an access list on the switch to permit traffic to Identity Manager. The following configuration configures access list rules to allow incoming TCP traffic to ports 80, 8080, 443, and 8443 of Identity Manager.

```
Switch(config-ext-nacl)#10 permit tcp any host 172.18.33.245 eq www
Switch(config-ext-nacl)#20 permit tcp any host 172.18.33.245 eq 8080
Switch(config-ext-nacl)#30 permit tcp any host 172.18.33.245 eq 443
Switch(config-ext-nacl)#40 permit tcp any host 172.18.33.245 eq 8443
```

Copying the Custom Captive Portal Pages to the Switch

Next, you copy the custom Captive Portal pages to the switch. Four custom pages (success.html, failed.html, expired.html, and login.html) located on Identity Manager (172.18.33.245) are extracted and copied to the portalpages directory on the flash drive of the switch (173.18.33.248).

```
Switch#archive tar /xtract http://admin:admin@172.18.33.245/switch/tme-  
idm/172.18.33.248/ flash:/portalpages  
Loading http://*****@172.18.33.245/switch/tme-idm/172.18.33.248/  
extracting success.html (572 bytes)!  
extracting failed.html (291 bytes)!  
extracting expired.html (291 bytes)!  
extracting login.html (1116 bytes)!!!!  
Switch#
```

Registering Custom Captive Portal Pages

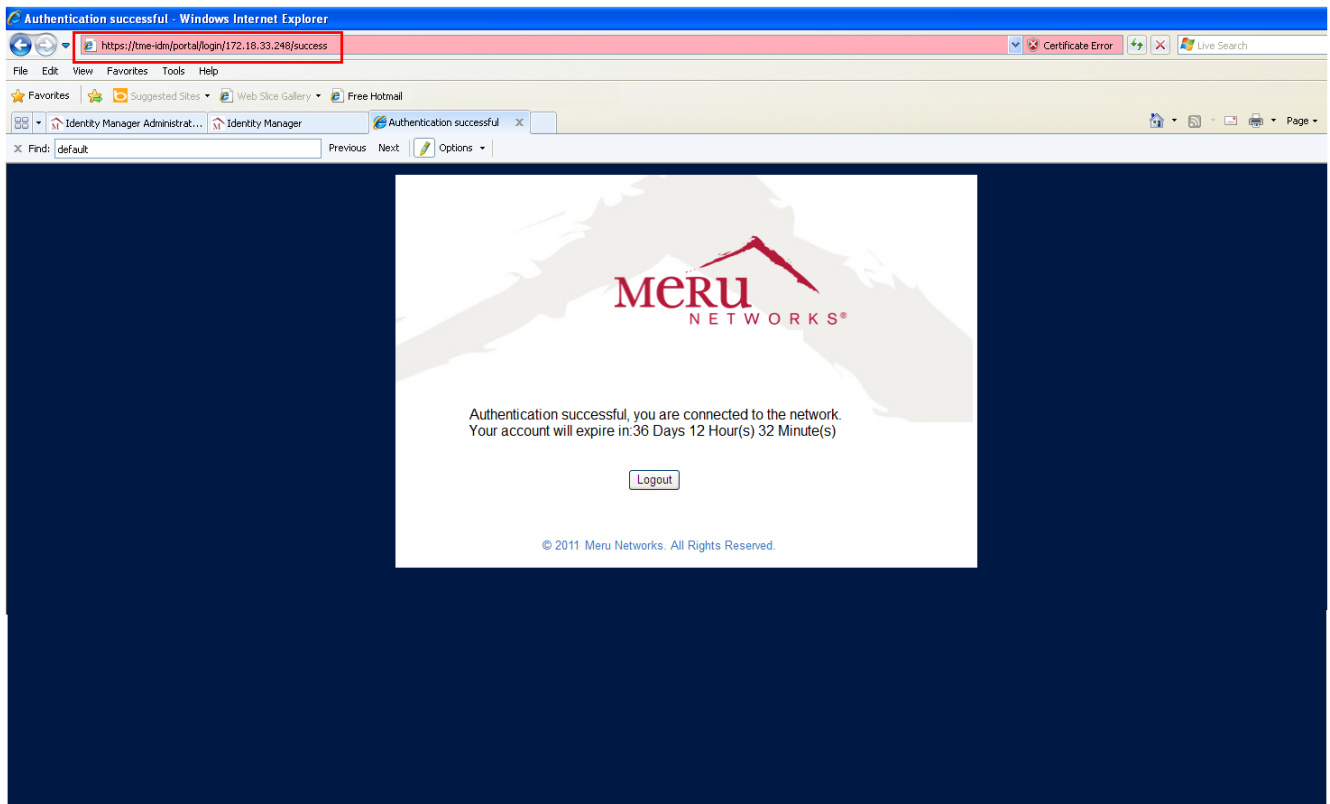
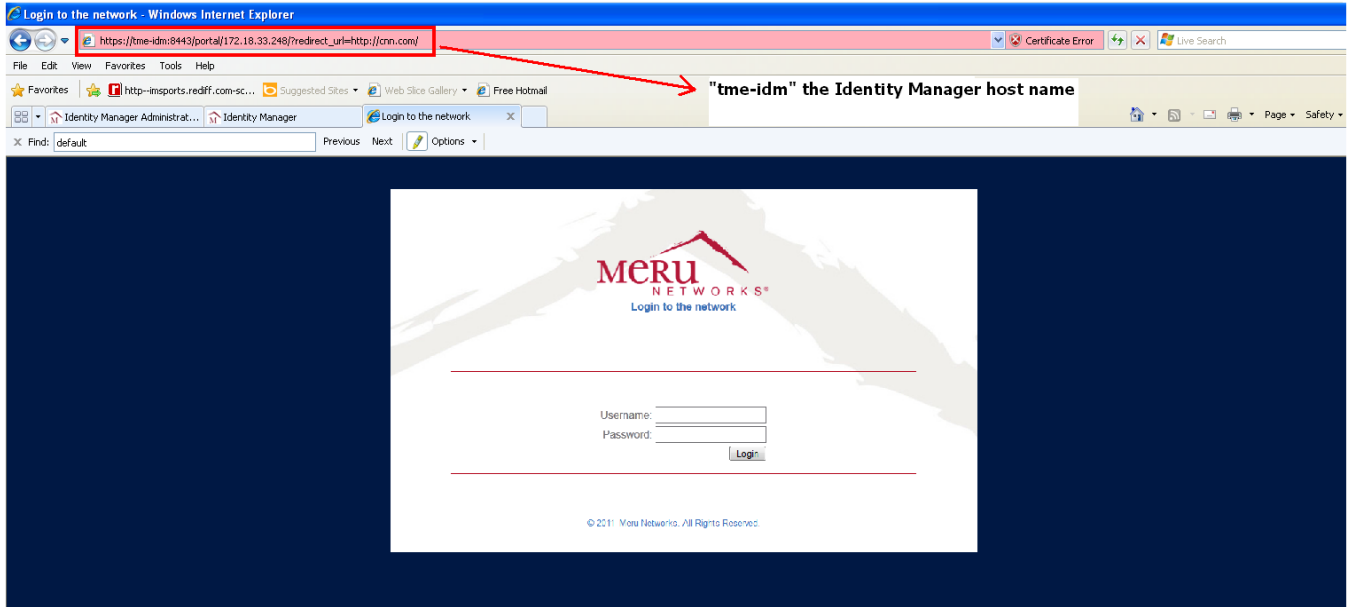
After copying the Captive Portal pages, you need to register them on the switch:

```
Switch(config)#ip admission proxy http login page file  
flash:/portalpages/login.html  
Switch(config)#ip admission proxy http success page file  
flash:/portalpages/success.html  
Switch(config)#ip admission proxy http fail page file  
flash:/portalpages/failed.html  
Switch(config)#ip admission proxy http login expired page file  
lash:/portalpages/expired.html  
Switch#show ip admission configuration  
  
Authentication Proxy Banner not configured  
Authentication Proxy webpage  
    Login page           : flash:/portalpages/login.html  
    Success page        : flash:/portalpages/success.html  
    Fail page           : flash:/portalpages/failed.html  
    Login Expire page   : flash:/portalpages/expired.html  
HTTP Authentication success redirect to URL: http://www.merunetworks.com  
Authentication global cache time is 60 minutes  
Authentication global absolute time is 0 minutes  
Authentication global init state time is 2 minutes  
Authentication Proxy Watch-list is disabled  
  
Authentication Proxy Max HTTP process is 7  
Authentication Proxy Rule Configuration  
    Auth-proxy name CP  
    http list not specified inactivity-time 60 minutes  
  
Authentication Proxy Auditing is disabled  
Max Login attempts per user is 5
```

Verifying Authentication Using the Captive Portal Pages

After configuring the switch, verify the configuration by connecting a system with a wired connection to the interface on which Captive Portal is enabled. Provide user credentials to test the authentication process. (See [Figure 58](#).)

Figure 58: Verifying Authentication



Use Case 4: Configuring Role-Based Access Control for Personal and Corporate Devices

Using Identity Manager Version, you can configure role-based access control for corporate and personal devices. For example, you can restrict access to your network for personal devices but allow corporate devices to access some or the entire network.

To configure role-based access control for personal and corporate devices, perform the following tasks:

- Perform controller configuration tasks. See [Controller Configuration Tasks](#).
- Create authorization profiles for personal and corporate devices. See [Creating Authorization Profiles](#).
- Create authorization policies for personal and corporate devices. See [Creating Authorization Policies](#).
- Create device accounts for personal and corporate devices. See [Creating Device Accounts](#).

Controller Configuration Tasks

- [Creating QoS and Firewall Rules](#)
- [Creating a Security Profile](#)

Creating QoS and Firewall Rules

Using Identity Manager, you create authorization profiles with filter ID strings for personal and corporate devices. The Filter-Id strings you use in authorization profiles must match the controller's firewall filter ID values in its QoS configuration, as shown in [Figure 59](#). You can also create firewall policies for bandwidth throttling for users.

Figure 59: QoS and Firewall Rules Page

ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	QoS Protocol	Action	QoS Rule Logging	QoS Rule Logging Frequency
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0	6		0	0	H.323	CAPTURE	Off	60
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720	6		0	0	H.323	CAPTURE	Off	60
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	17		0	0	SIP	CAPTURE	Off	60
5	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	6		0	0	SIP	CAPTURE	Off	60
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0	17		0	0	other	FORWARD	Off	60
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200	17		0	0	other	FORWARD	Off	60
20	172.22.32.8	255.255.255.255	443	0.0.0.0	0.0.0.0	0	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
21	0.0.0.0	0.0.0.0	0	172.22.32.8	255.255.255.255	443	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
30	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	1	corp	0	0	none	DROP	Off	60
31	0.0.0.0	0.0.0.0	80	0.0.0.0	0.0.0.0	0	0	pers	0	0	none	DROP	Off	60

Creating a Security Profile

You need to create a security profile that dynamically assigns filter IDs using RADIUS, as shown in [Figure 60](#).

Figure 60: Security Profile Page

Static WEP Key Index: [] Valid range: [1-4]

Re-Key Period (seconds): [0] Valid range: [0-65535]

BKSA Caching Period (seconds): [0] Valid range: [0-65535]

Captive Portal: [Disabled]

Captive Portal Authentication Method: [internal]

802.1X Network Initiation: [On]

Tunnel Termination: PEAP TTLS

Shared Key Authentication: [Off]

Pre-shared Key (Alphanumeric/Hexadecimal): []

Group Keying Interval (seconds): [0] Valid range: [0-65535]

PMK Caching: [On]

Key Rotation: [Disabled]

Backend Auth Server Timeout: [30] Valid range: [1-65535]

Reauthentication: [On]

MAC Filtering: [Off]

Firewall Capability: [radius-configured]

Firewall Filter ID: [] Enter 0-16 chars.

Security Logging: [Off]

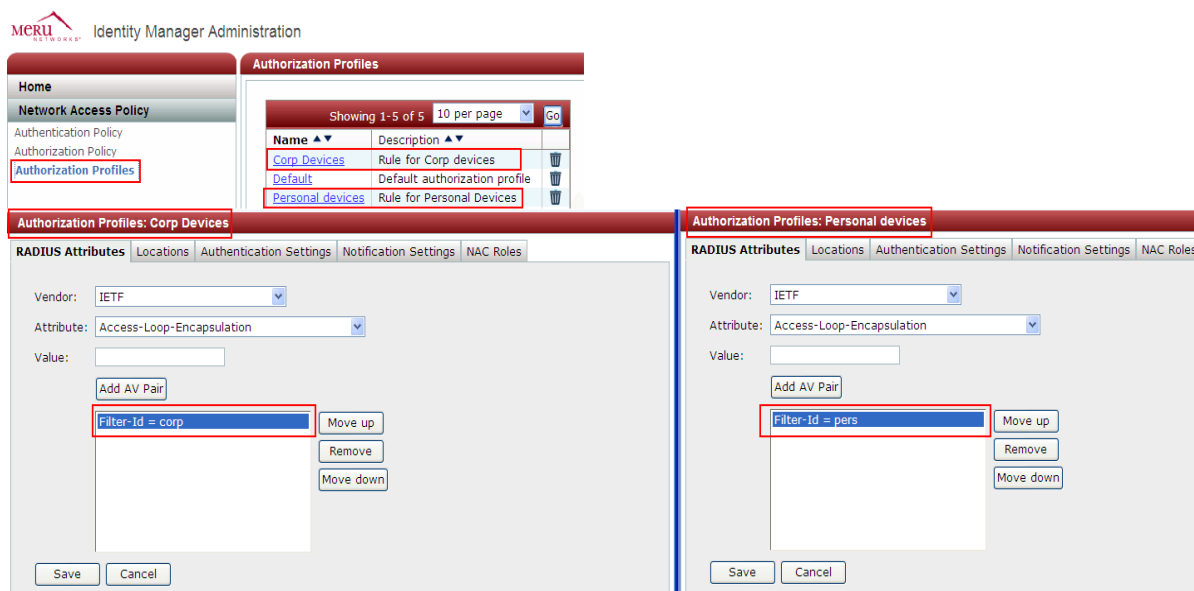
Creating Authorization Profiles

For this use case, you need to create authorization profiles for personal devices and corporate devices: “Corp Devices” for corporate devices and “Personal devices” for personal devices.

When creating each authorization profile:

- Specify the RADIUS attribute as Filter-Id.
- Specify the value of the RADIUS attribute as **corp** for corporate devices and **pers** for personal devices.
- Make sure that the RADIUS attribute values are specified in QoS and firewall rules on the controller, as shown in [Figure 59](#).

Figure 61: Creating Authorization Profiles



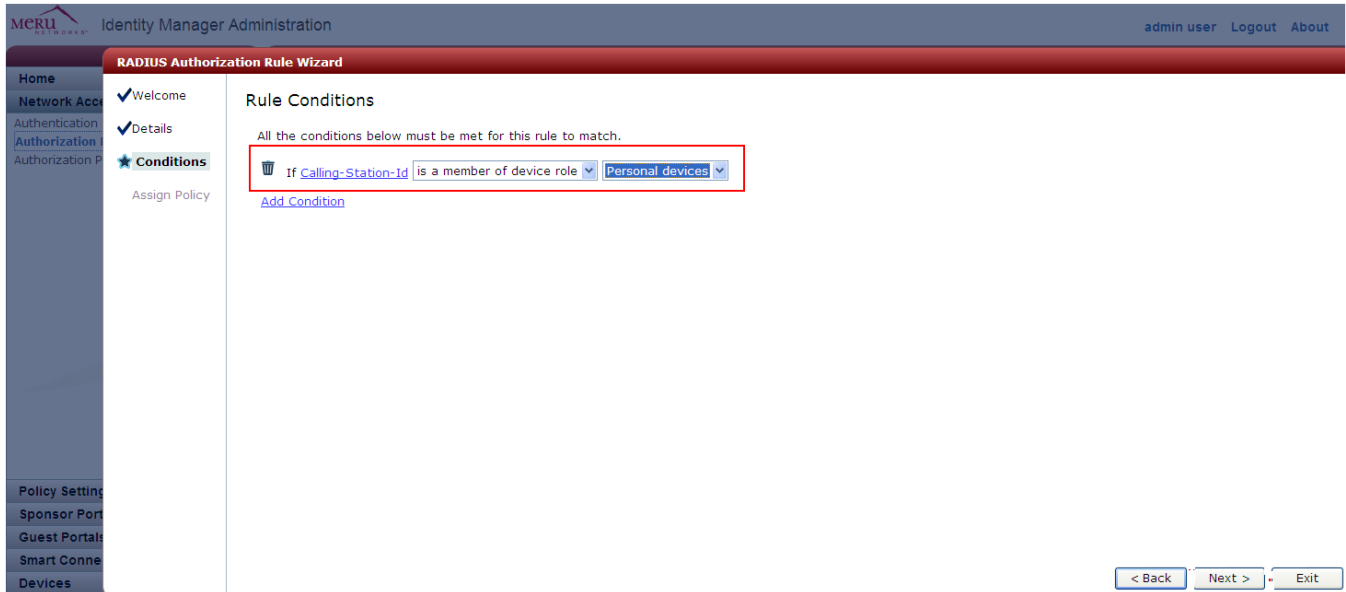
Creating Authorization Policies

For this use case, you need to create authorization policies for personal devices and corporate devices: “Personal” for personal devices and “Corporate” for corporate devices.

Before creating the authorization policies, make sure that the mode for assigning authorization profiles to user is set to Advanced.

When creating the “Personal” policy, on the Rule Conditions page, set RADIUS as the attribute type. Also, as shown in [Figure 62](#), specify the rule conditions for the authorization policy as **is a member of device role** and **Personal devices**. On the Policy page, specify the profile to assign to users to **Personal devices**.

Figure 62: Rule Conditions Page



Creating Device Accounts

Now you need to create device accounts for the corporate and personal devices. Make sure that you have the MAC addresses of the devices when creating device accounts.



You need only maintain a list of MAC addresses of the corporate-owned devices and can create rules for the personal devices to make them part of a "personal" role with access restrictions.

To create a device account:

1. Log in to Identity Manager using a sponsor account.
2. Create a device accounts one at a time, or create multiple device accounts all at once, as shown in [Figure 63](#).
3. Make sure to select Corp Devices from the Device Role list.

Figure 63: Creating Device Accounts



If you need to change the Device Role value for a device account, suspend the account and create a new device account with the new Device Role value. You can also suspend device accounts if they are no longer necessary.

To review device accounts, select **Account Management > Report & Manage Devices**. To see device account details, click the MAC address link for the device. (See [Figure 64](#).)

Figure 64: Reviewing Device Accounts

Use the personal device to connect to your network, and verify the firewall restriction on user traffic defined by the rule in the QoS policy that you created for personal devices. For personal devices, HTTP traffic is denied, and for corporate devices, ICMP traffic is denied.

Use Case 5: Providing Guest Access Paid Subscription Systems for Wi-Fi Hotspots

Many public Wi-Fi hotspots in hotels, airports, casinos, and holiday resorts provide for guest on-boarding, such as provisioning self-service guest portals, PMS billing (hotels), and so on. A guest access system can also include paid subscriptions; usually, the sign-up process involves providing credit card information online to gain Internet access.

This use case shows how you can configure a Meru controller and Identity Manager so that users can self-register using a guest portal and choose access plans with different speeds. Allowing users to self-register and choose access plans allows for better subscription management. For example, the ability to provide different classes of service in the business lounge of an airport enhances the individual Wi-Fi experience while still using the same Wi-Fi infrastructure.

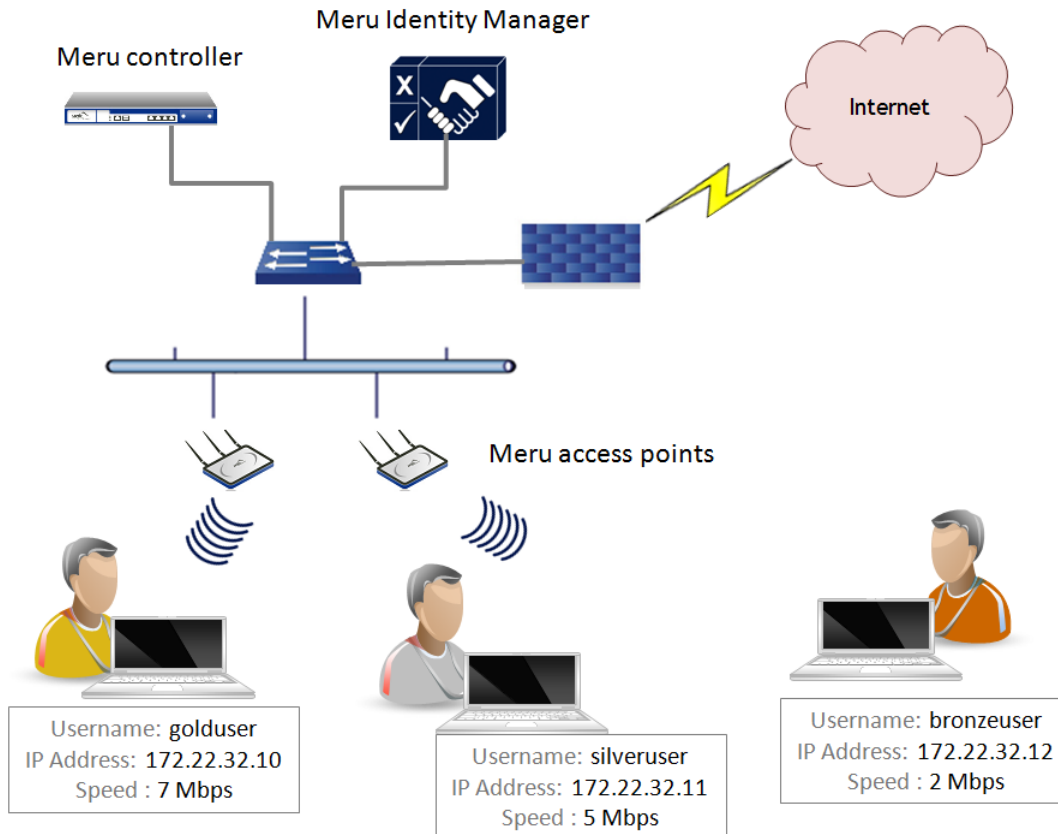
Guest Access Paid Subscription System Deployment

In this deployment, after connecting to the Meru guest portal, users have the option to purchase one of the following access plans:

- Gold plan, which provides network access at a speed of 7 Mbps for \$15 (United States dollars) per hour
- Silver plan, which provides network access at a speed of 5 Mbps for \$10 per hour
- Bronze plan, which provides network access at a speed of 2 Mbps for \$5 for per hour

[Figure 65](#) shows a network diagram of the deployment described in this document.

Figure 65: Network Infrastructure



Configuring the Meru Controller and Identity Manager

To deploy a guest access paid subscription system, you must perform configuration tasks on the Meru controller before configuring Identity Manager.

Controller Configuration Tasks

The following is a high-level list of configuration tasks that you must perform with System Director. For more information, see the *Meru Identity Manager User Guide* and the *Meru System Director Configuration Guide*.

- Create a RADIUS profile that references Identity Manager.
- Map the RADIUS profile to the Captive Portal configuration page.
- Create a security profile with WebAuth enabled, firewall capability defined as RADIUS-configured, and a pass-through Filter-Id specified for Identity Manager access.
- Configure an ESS profile, and map it to the security profile. (See [Figure 66](#).)
- Create two QoS rules for the controller to permit pre-authentication traffic to and from Identity Manager. For configuration information, see the *Meru Identity Manager User Guide*.

- Create a QoS rule for each access plan (total of three) to match any source and destination subnet with Filter-IDs. (See [Figure 67](#) and [Figure 68](#).)
- Make sure that QoS rules for rate limiting have the following configured:
 - Firewall Filter-ID with Match and Flow class enabled.
 - Token Bucket rate.
 - Action option value is set to Forward.
 - Flow Class is enabled for the source (any source). You must enable Flow Class to allow clients to be rate limited individually.
- Change the Captive Portal mode.
- Verify that the QoS rules work correctly.
- Verify authentication for Captive Portal.

Figure 66: Set Up an ESS Profile Mapped to the Security Profile

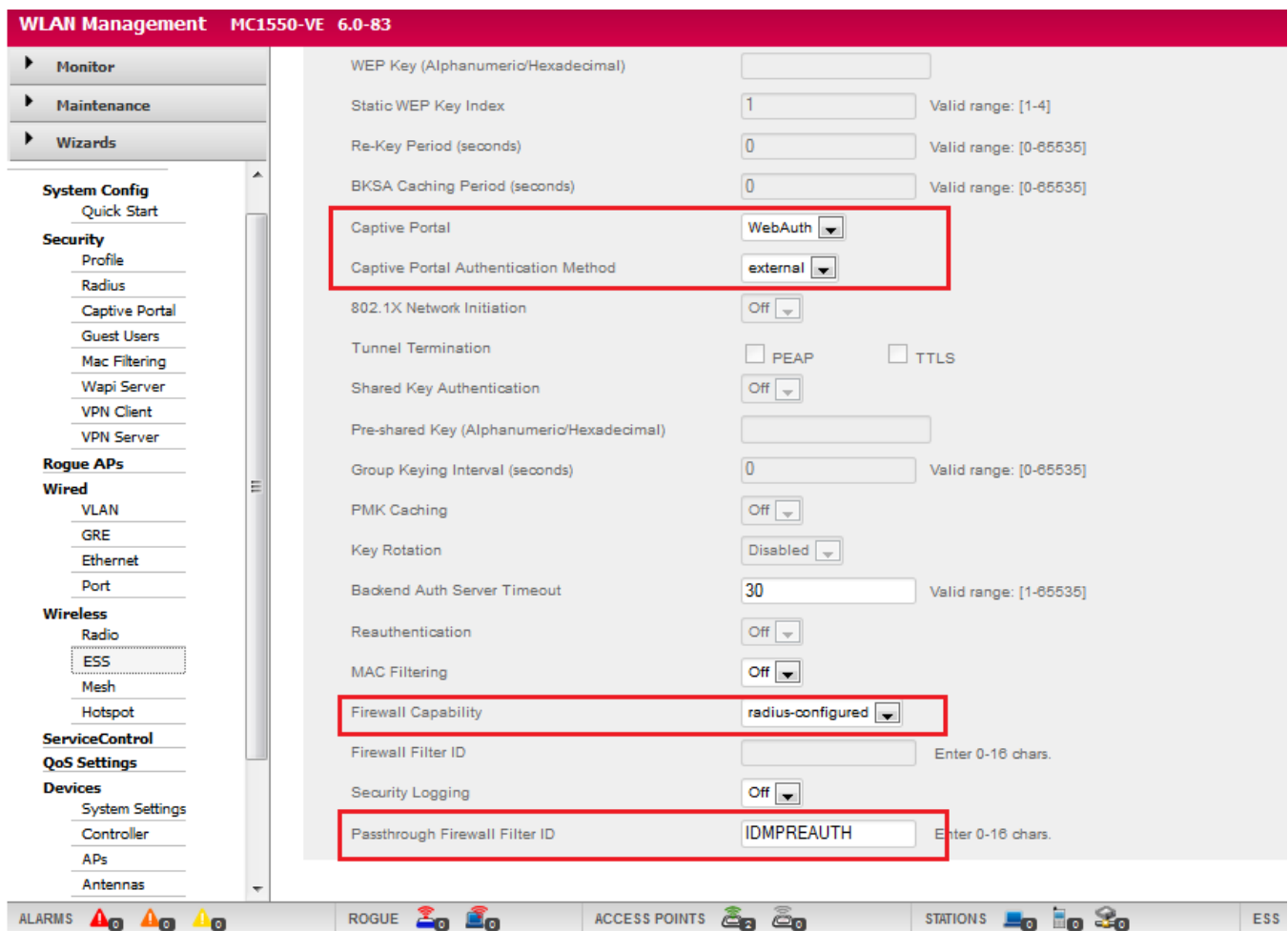


Figure 67: Configuring QoS Rules

WLAN Management MC1550-VE 6.0-83

Monitor
Maintenance
Wizards

System Config
Quick Start

Security
Profile
Radius
Captive Portal
Guest Users
Mac Filtering
Wapi Server
VPN Client
VPN Server

Rogue APs

Wired
VLAN
GRE
Ethernet
Port

Wireless
Radio
ESS
Mesh
Hotspot

ServiceControl
QoS Settings
Devices
System Settings
Controller
APs
Antennas

Destination Port: 0 Valid range: [0-65535]

Source IP: 0.0.0.0

Source Netmask: 0.0.0.0

Source Port: 0 Valid range: [0-65535]

Network Protocol: 0 Valid range: [0-255]

Firewall Filter ID: Bronzeplan2Mbps Enter 0-16 chars.

Packet minimum length: 0 Valid range: [0-1500]

Packet maximum length: 0 Valid range: [0-1500]

QoS Protocol: none

Average Packet Rate: 0 Valid range: [0-200]

Action: FORWARD

Token Bucket Rate: 2,000 (1-64) Kbps Mbps Valid range:

Priority: 0 Valid range: [0-8]

Traffic Control: On

ALARMS ROGUE ACCESS POINTS STATIONS

Figure 68: QoS Rules Specifying Different Token Bucket Rates

WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6 level:15 2:24:52 PM WebTerm Save Logout Help MCRU

Monitor
Maintenance
Wizards

System Config
Quick Start

Security
Profile
Radius
Captive Portal
Guest Users
Mac Filtering
Wapi Server
VPN Client
VPN Server

Rogue APs

Wired
VLAN
GRE
Ethernet
Port

Wireless
Radio
ESS
Mesh
Hotspot

ServiceControl
QoS Settings
Devices
System Settings

QoS and Firewall Rules (11 entries)

Global Quality-of-Service Parameters QoS and Firewall Rules QoS Codec Rules

ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	QoS Protocol	Action	QoS Rule Logging	QoS Rule Logging Frequency
1	0.0.0.0	0.0.0.0	1720	0.0.0.0	0.0.0.0	0	6		0	0	H.323	CAPTURE	Off	60
2	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	1720	6		0	0	H.323	CAPTURE	Off	60
3	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	17		0	0	SIP	CAPTURE	Off	60
5	0.0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	6		0	0	SIP	CAPTURE	Off	60
7	0.0.0.0	0.0.0.0	5200	0.0.0.0	0.0.0.0	0	17		0	0	other	FORWARD	Off	60
8	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	5200	17		0	0	other	FORWARD	Off	60
20	172.22.32.8	255.255.255.255	443	0.0.0.0	0.0.0.0	0	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
21	0.0.0.0	0.0.0.0	0	172.22.32.8	255.255.255.255	443	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
100	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	0	Bronzeplan2Mbps	0	0	none	FORWARD	Off	60
200	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	0	Silverplan5Mbps	0	0	none	FORWARD	Off	60
300	0.0.0.0	0.0.0.0	0	0.0.0.0	0.0.0.0	0	0	Goldplan7Mbps	0	0	none	FORWARD	Off	60

Identity Manager Configuration Tasks

After configuring the controller as described in Controller Configuration Tasks, you must add the controller as a RADIUS client in Identity Manager. (Also make sure to specify that the guest portal pages you configure in Identity Manager are automatically transferred to the controller.) For more information, see the [Identity Manager Deployment Guide](#).

The following topics describe the additional configuration tasks that you need to perform in Identity Manager:

- [Creating Authorization Profiles](#)
- [Adding Payment Provider Accounts](#)
- [Creating a Portal for Login and Credit Card Billing](#)
- [Previewing the Portal](#)

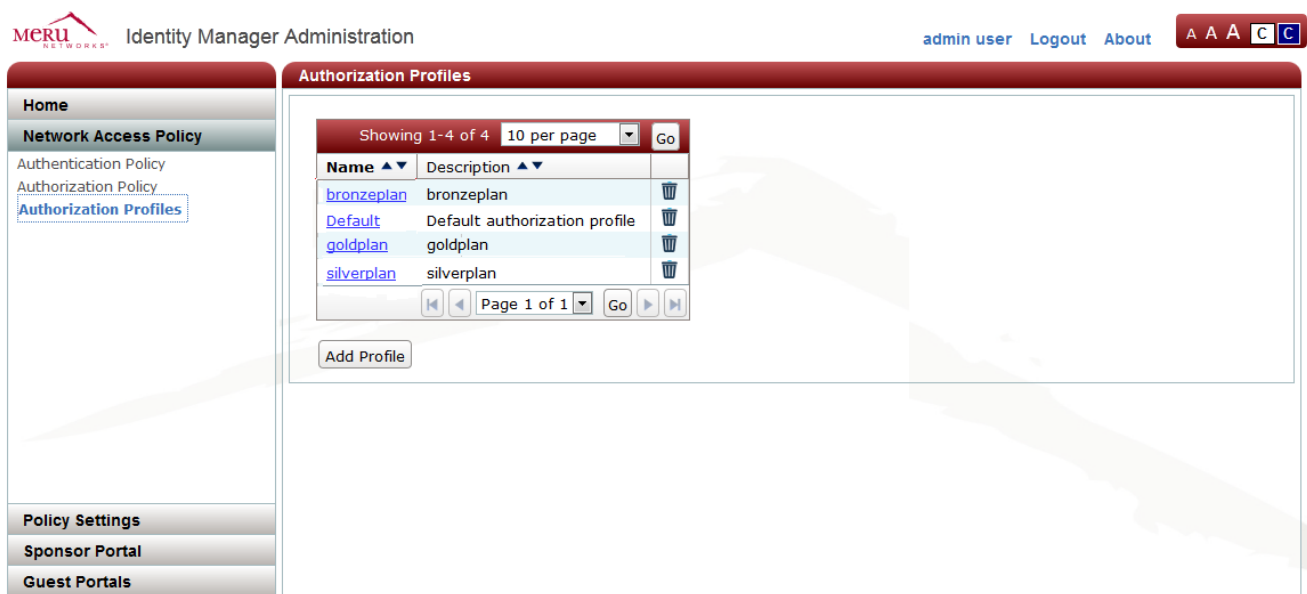
Creating Authorization Profiles

You use authorization profiles to define network access for users. For the network scenario in [Figure 65](#), three authorization profiles must be created:

- bronzeplan: Access plan of 2 Mbps
- goldplan: Access plan of 5 Mbps
- silverplan: Access plan of 7 Mbps

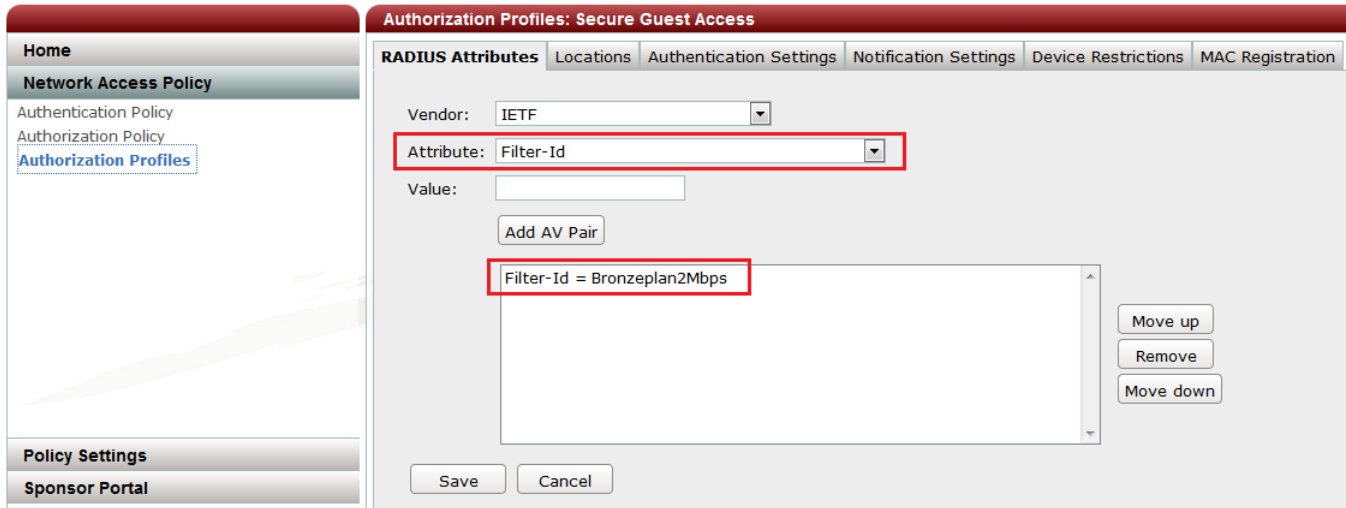
The authorization profile is added to the list of authorization profiles on the Authorization Profiles main page, as shown in [Figure 69](#).

Figure 69: Authorization Profiles Main Page



After an authorization profile has been added, edit the profile so that you specify the Filter-Id values that you previously configured with System Director as RADIUS attributes for the authorization profile. For example, the Filter-Id value for the bronzeplan profile is "Bronzeplan2Mbps," as shown in [Figure 70](#).

Figure 70: Configuring Filter-Id as a RADIUS Attribute for Authorization Profile



Adding Payment Provider Accounts

After creating authorization profiles, as described in [Creating Authorization Profiles](#), you need to add a payment provider.

The account created in this example is only for illustrative purposes. When adding a payment provider, use the appropriate information for your payment provider account. (See [Figure 71](#).)

To test the connection to the payment provider, click **Test Connection**. A test transaction is sent, and a message appears with the results of the test.

The payment provider is added, as shown in [Figure 72](#).

Figure 71: Configuring Payment Gateways

Identity Manager Administration admin user Logout About

Add New Payment Provider

Account Details

Account Name:

Account Description:

Payment Provider:

Operation Mode: [https://test.authorize.net/gateway/transact.dll]

API Login:

Transaction Key:

Available Cards

- MasterCard
- American Express
- Diners Club
- Discover Card
- En Route
- JCB
- Carte Blanche

Supported Cards

- Visa

Save Cancel Test Connection

Figure 72: Payment Provider List

Payment Providers

Showing 1-1 of 1 10 per page Go

Name ▲▼	Type ▲▼	Description ▲▼	
Test account	Authorize.net	test account	

Page 1 of 1 Go

Add

Creating a Portal for Login and Credit Card Billing

When creating a portal, Identity Manager provides many options for customization in the wizard. This document describes only the configuration for the wizard pages required to deploy the guest access paid subscription system, as shown in [Figure 65](#). Depending on your organization’s requirements, modify other wizard pages as appropriate.

Creating a portal for the guest access paid subscription system consists of the following tasks:

- [Enabling Display of Pre-Authentication and Post-Authentication Pages](#)
- [Configuring Guest Account Options](#)
- [Mapping the Payment Provider to the Portal](#)
- [Configuring Access Plans for Credit Card Billing](#)
- [Configuring Guest User and Password Policies](#)

You must create a portal that users access to purchase an access plan and log in to for Internet access.

Enabling Display of Pre-Authentication and Post-Authentication Pages

In this use case, the display of pre-authentication and post-authentication pages is enabled. On the Portal Pages page, select the Pre-Authentication check box for Login and Credit Card Billing, and Post-Authentication check box for Successful Authentication, as shown in [Figure 73](#). Also select the **Enable Logout Button** check box.

Figure 73: Portal Pages Page

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ★ **Portal Settings**
- Portal Policy

Portal Pages

Specify which pages your portal should have enabled and at what stage they should be available.

Page	Displayed in menu	
	Pre-Authentication	Post-Authentication
Login	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password Change	<input type="checkbox"/>	<input type="checkbox"/>
Self Service	<input type="checkbox"/>	<input type="checkbox"/>
Device Registration	<input type="checkbox"/>	<input type="checkbox"/>
Credit Card Billing	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Successful Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Smart Connect	<input type="checkbox"/>	<input type="checkbox"/>
PMS Billing	<input type="checkbox"/>	<input type="checkbox"/>
Help	<input type="checkbox"/>	<input type="checkbox"/>
Welcome	<input type="checkbox"/>	<input type="checkbox"/>

Logout Options

Enable Logout Button:

Enable Logout Pop-up window:

< Back Next > Exit

Configuring Guest Account Options

To configure guest account options, make sure that the check boxes are selected for the following, as shown in [Figure 74](#):

- Auto Login
- Display account details
- Send account details by SMS
- Send account details by e-mail

Figure 74: Account Options Page

Portal Setup Wizard

✓ Welcome
✓ Portal Name
✓ Portal Theme
★ **Portal Settings**
Portal Policy

Account Options

The following options define what should happen after an account either guest or device is created.

- Auto login — If this option is selected the user will be presented with a login button that will allow them to authenticate without having to type in the new account credentials.
- Display account details - If this option is selected the new account credentials will be displayed on the screen.
- Send account details via SMS - If this options is selected the new account credentials will be sent to the user's mobile phone.
- Send account details via e-mail - If this options is selected the new account credentials will be sent to the user's e-mail address.

Auto Login:
Display account details:
Send account details by SMS:
Send account details by e-mail:

< Back Next > Exit

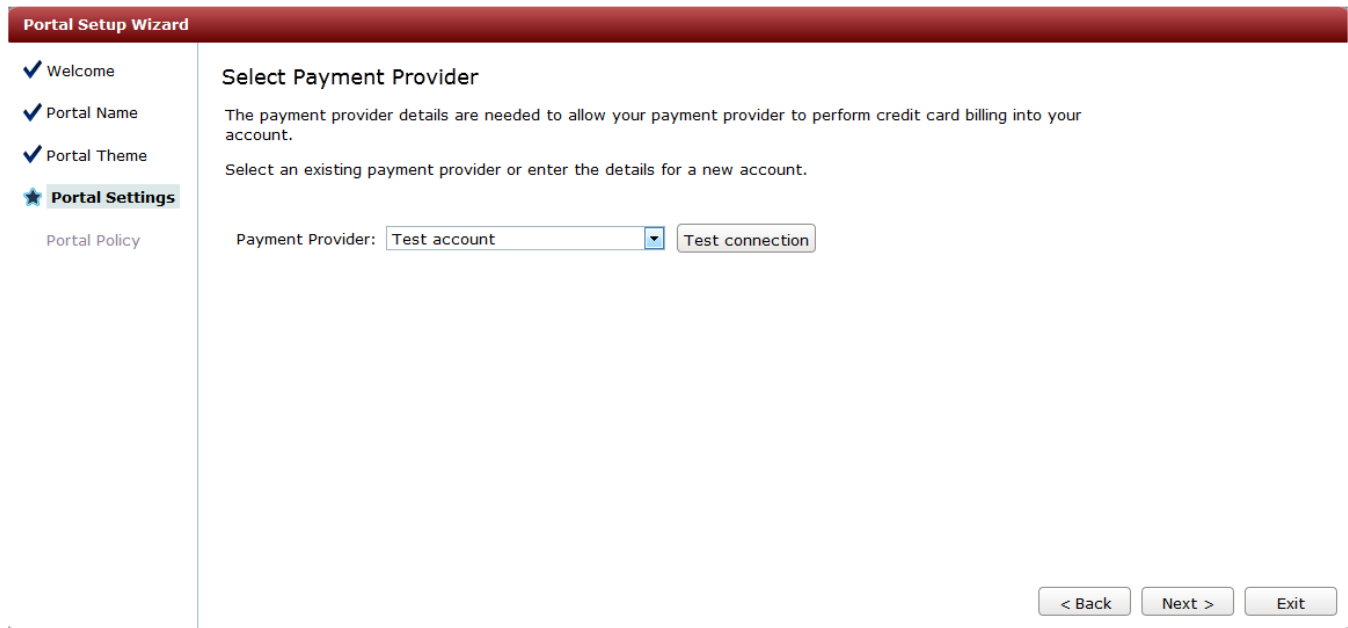
Mapping the Payment Provider to the Portal

To map the payment provider, which you added in [Adding Payment Provider Accounts](#), to the portal:

On the Select Payment Provider page, as shown in [Figure 75](#), select your payment provider. In this example, select **Test account**.

To test the connectivity to the payment provider, click **Test connection**.

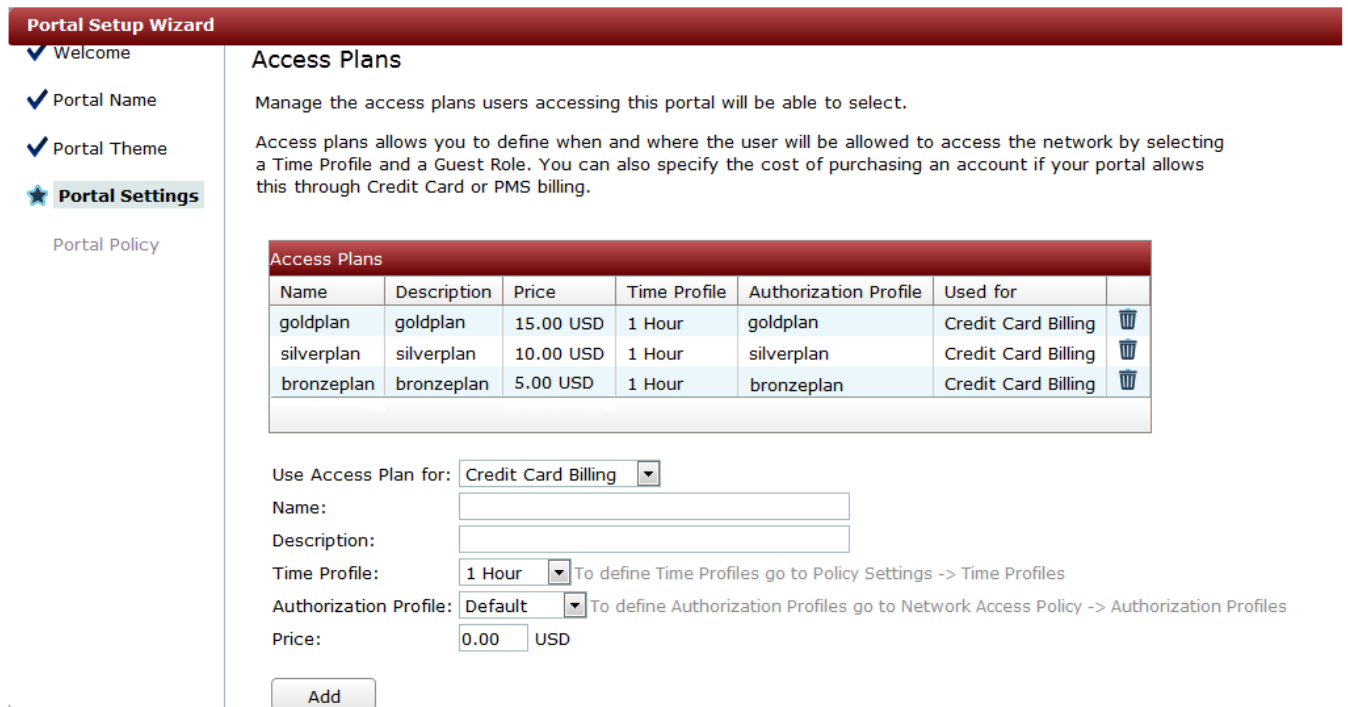
Figure 75: Select Payment Provider Page



Configuring Access Plans for Credit Card Billing

In Identity Manager, you need to create an access plan for each level of service (goldplan, silverplan, and bronzeplan). [Figure 76](#) shows the Access Plans page after the access plans have been created.

Figure 76: Access Plans Page



Configuring Guest User and Password Policies

You need to define the guest username and password policies for the portal, as shown in the Guest Username Policy page, as shown in [Figure 77](#), and the Guest Password Policy page, as shown in [Figure 78](#).

Figure 77: Guest Username Policy Page

The screenshot shows the 'Portal Setup Wizard' interface. On the left is a navigation sidebar with the following items: 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy' (which is highlighted with a star icon). The main content area is titled 'Guest Username Policy' and contains the following text: 'The following options allow you to specify how the usernames for the guest accounts created through this portal should be generated.' Below this text are three radio button options: 'Email address as username' (which is selected and highlighted with a red box), 'Create username based on first and last names', and 'Create random username'. Under the selected option, there is a dropdown menu labeled 'Create Username With Case:' with 'lowercase' selected. Under the second option, there are three dropdown menus: 'Minimum username length:' (set to 10), 'Create Username With Case:' (set to 'Case entered by sponsor'), and 'Create Username With Separator:' (set to 'None').

Portal Setup Wizard

- ✓ Welcome
- ✓ Portal Name
- ✓ Portal Theme
- ✓ Portal Settings
- ★ **Portal Policy**

Guest Username Policy

The following options allow you to specify how the usernames for the guest accounts created through this portal should be generated.

- E-mail address as username — The guest e-mail address will be used as the username for the account.
- Create username based on first and last names — The guest's first and last names will be combined to generate the account username.
- Create random username — The username for the account will be randomly generated.

Email address as username

Email address as username

Create Username With Case:

Create username based on first and last names

Create username based on first and last names

Minimum username length:

Create Username With Case:

Create Username With Separator:

Create random username


Figure 78: Guest Password Policy Page

The screenshot shows the 'Portal Setup Wizard' interface. On the left, a navigation menu includes 'Welcome', 'Portal Name', 'Portal Theme', 'Portal Settings', and 'Portal Policy' (which is highlighted with a star). The main content area is titled 'Guest Password Policy' and contains the following sections:

- Alphabetic Characters:** A text input field contains 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'. Below it, 'Password case:' is set to 'Mixed' and 'Number to include:' is set to '6'.
- Numeric Characters:** A text input field contains '0123456789'. Below it, 'Number to include:' is set to '2'.
- Other Characters:** A text input field contains '!\$%^*()-_+=+[]{};:@#~.,<>?'. Below it, 'Number to include:' is set to '0'.

Previewing the Portal

After creating a portal, you can use the portal preview feature to verify that the portal works properly:

1. In the Identity Manager Administration interface, select **Guest Portals > Portals**.
2. Click the Portal Preview icon () for the portal.

[Figure 79](#) shows an example of a portal.

Figure 79: Previewing Portal Content

https://172.22.32.5/portal/Wifi_Access_portal/preview/

MERU
NETWORKS®
Purchase your account

Login Purchase Account

Card Holder Name:

Mobile number: +1

E-mail address:

Billing Address:

Postal/ZIP code:

Country: United States

Credit Card Number:

Security Code:

Issue Number:

Expiration Date (month/year): 01 / 2013

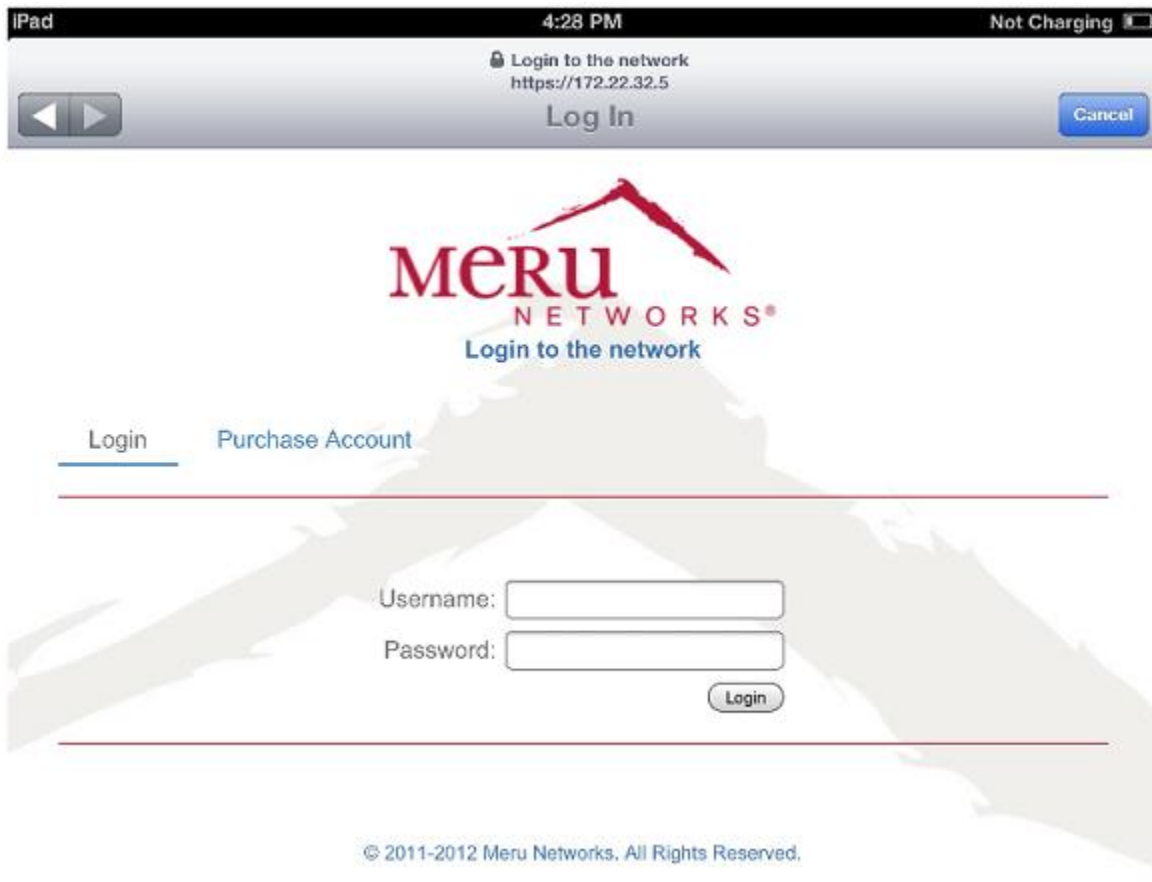
Access Plan: Bronzeplan - \$5.00
Goldplan - \$15.00
silverplan - \$10.00

Generate Account

Guest Portal Pages

[Figure 80](#) shows the page that users see when accessing the guest portal.

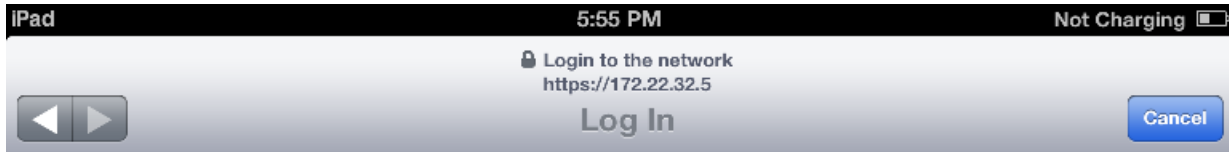
Figure 80: Guest Login Page



Users who want to purchase an access plan can click Purchase Account. [Figure 81](#) shows the purchase page. After providing user and credit card information, the user clicks Generate Account to purchase the plan and receive guest account credentials to log in to the portal and access the Internet.

[Figure 82](#) shows an example of the page with account credentials that the user gets after the guest account is generated. [Figure 83](#) shows a successful authentication page a user sees after successfully logging in.

Figure 81: Self-Registering and Purchasing an Access Plan



[Login](#) [Purchase Account](#)

Card Holder Name:

Mobile number:

E-mail address:

Billing Address:

Postal/ZIP code:

Country:

Credit Card Number:

Security Code:

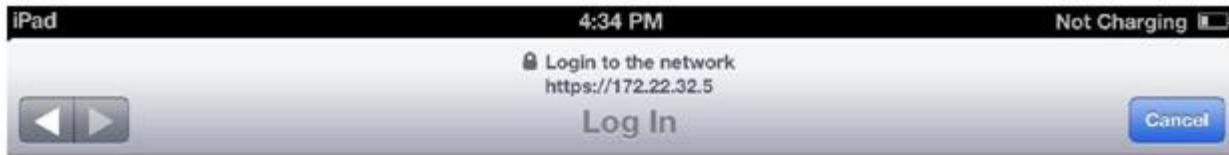
Issue Number:

Expiration Date (month/year): /

Access Plan:

© 2011-2013 Meru Networks. All Rights Reserved.

Figure 82: Guest User Generated by the System



[Purchase Account](#)

[Successful Authentication](#)

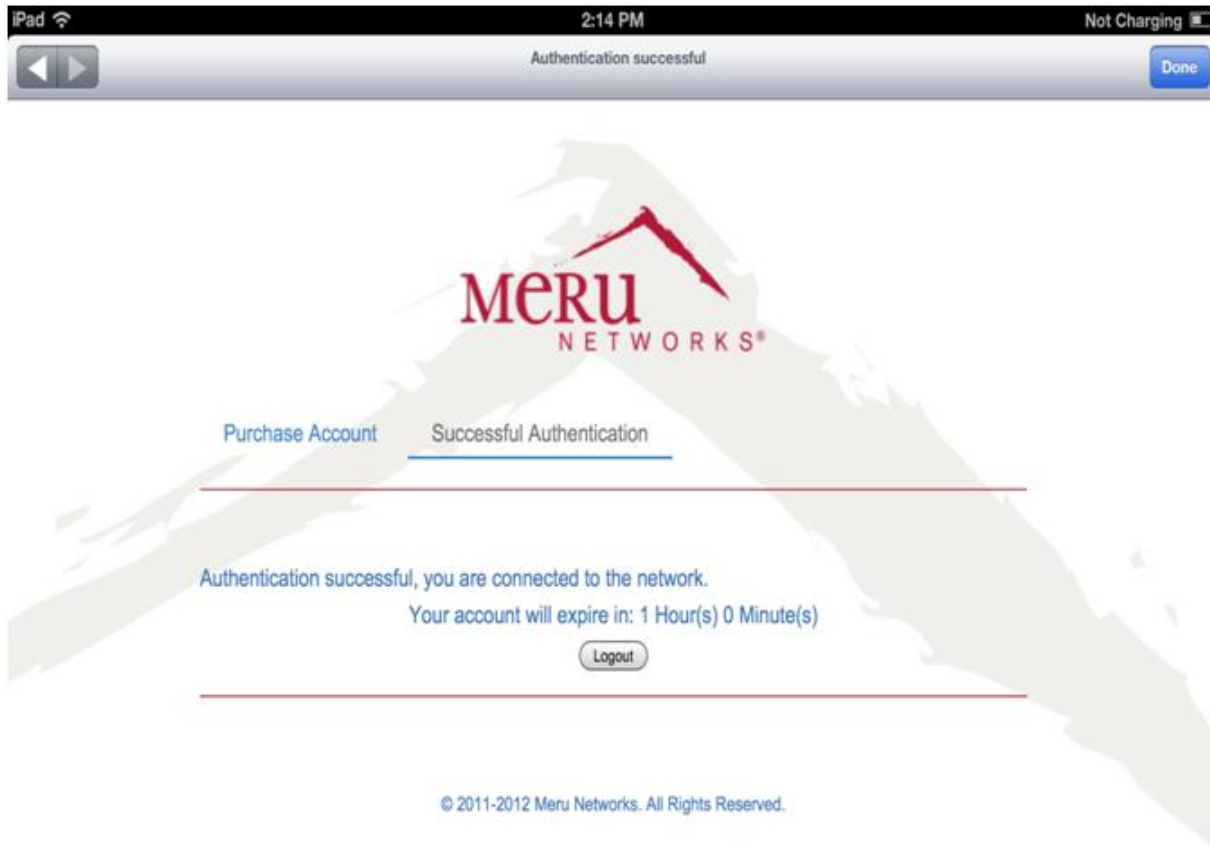
The account credentials were sent to your phone, please use them to access the network.
The account credentials were sent to your e-mail, please use them to access the network.

Username: **susan@example.com**
Password: **Le3dJ8Kn**

Login

© 2011-2012 Meru Networks. All Rights Reserved.

Figure 83: Successful User Authentication



Verifying Connectivity

To test that the configuration is working correctly:

- Run a packet-capture on the controller or Identity Manager and filter the packets for the RADIUS protocol. Make sure the correct Filter-ID is returned for "Access-accept," as configured for the access plans. [Figure 84](#) shows an example of packet-capture results.
- Run throughput tests using common tools, FTP file transfer, or a speed test to the Internet and verify that client traffic is rate limited, as defined by your configuration.

Figure 84: Verifying Connectivity Using Packet Capture

The image displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom pane shows the detailed view of a selected RADIUS Access-Accept(2) packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and RADIUS Protocol details.

No.	Time	Source	Destination	Protocol	Length	Info
9961	13:13:30.712417	172.22.32.5	172.22.32.5	RADIUS	204	Access-Request(1) (id=59, l=162)
9972	13:13:30.910878	172.22.32.5	172.22.32.5	RADIUS	83	Access-Accept(2) (id=59, l=41)
9974	13:13:30.911731	172.22.32.5	172.22.32.5	RADIUS	255	Accounting-Request(4) (id=60, l=213)
9979	13:13:30.931610	172.22.32.5	172.22.32.5	RADIUS	62	Accounting-Response(5) (id=60, l=20)

The detailed view of the selected packet (Frame 9972) shows the following structure:

- Frame 9972: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
- Ethernet II, Src: HewlettP_69:34:00 (e4:11:5b:69:34:00), Dst: LanerE1_14:d0:80 (00:90:0b:14:d0:80)
- Internet Protocol Version 4, Src: 172.22.32.5 (172.22.32.5), Dst: 172.22.32.5 (172.22.32.5)
- User Datagram Protocol, Src Port: 47356 (47356), Dst Port: radius (1812)
- Radius Protocol
 - Code: Access-Accept (2)
 - Packet Identifier: 0x3b (59)
 - Length: 41
 - Authenticator: abff613ddc8b9433ee266c2100b1559a
 - [This is a response to a request in frame 9961]
 - [Time from request: 0.198461000 seconds]
 - Attribute Value Pairs
 - AVP: l=6 t=Service-Type(6): Login(1)
 - AVP: l=6 t=Framed-MTU(12): 1250
 - AVP: l=19 t=User-Name(1): susan@example.com
 - AVP: l=18 t=User-Password(2): Encrypted
 - AVP: l=19 t=Calling-Station-Id(31): 80-65-BD-4B-59-7D
 - AVP: l=19 t=Called-Station-Id(30): 00-90-0E-14-D0-80
 - AVP: l=19 t=Connect-Info(77): CONNECT 802.11a/n
 - AVP: l=6 t=NAS-IP-Address(4): 172.22.32.5
 - AVP: l=6 t=NAS-Port-Type(61): wireless-802.11(19)
 - AVP: l=6 t=NAS-Port(5): 0
 - AVP: l=18 t=Message-Authenticator(80): 48c2b4ef2478a2163f89f8bc8e

Use Case 6: Basic Customization of a Guest Portal Using Default Tools

In this use case, you create a basic portal using the default Meru Networks (white) theme. You upload a custom logo and a custom background to Identity Manager to customize the portal. You also configure the portal with only login and logout features enabled.

[Figure 85](#) shows the default login page for the Meru Networks (white) theme. [Figure 86](#) shows the login page after customization.

Figure 85: Default Login Page

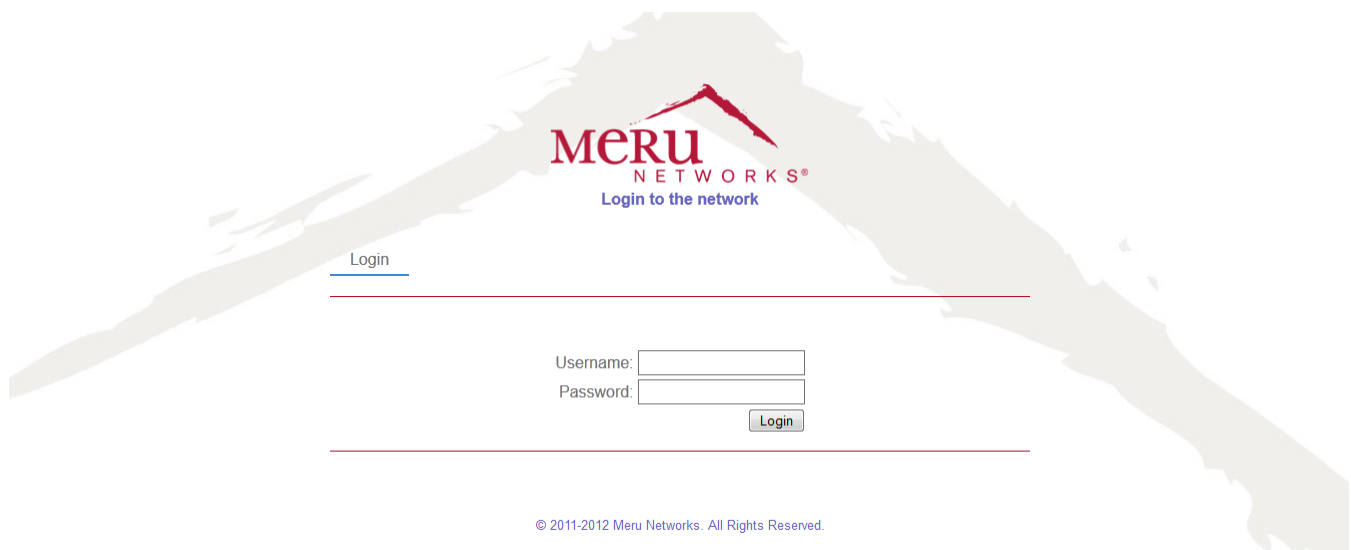
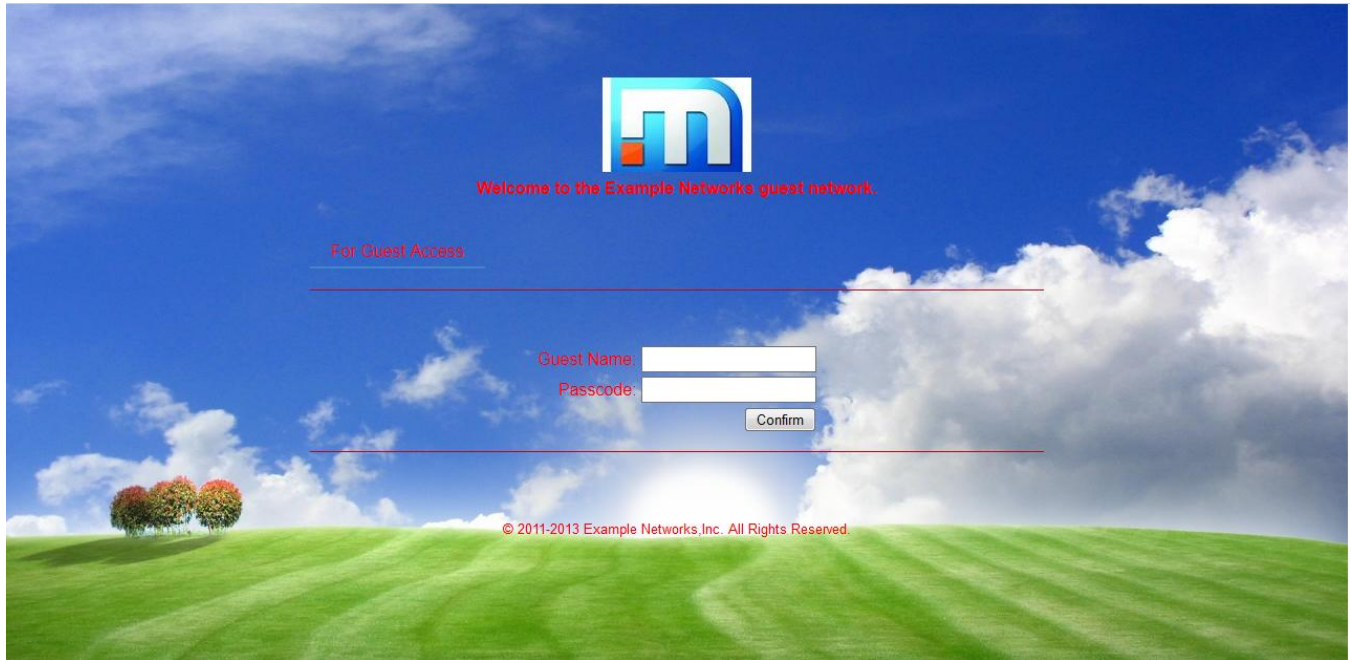


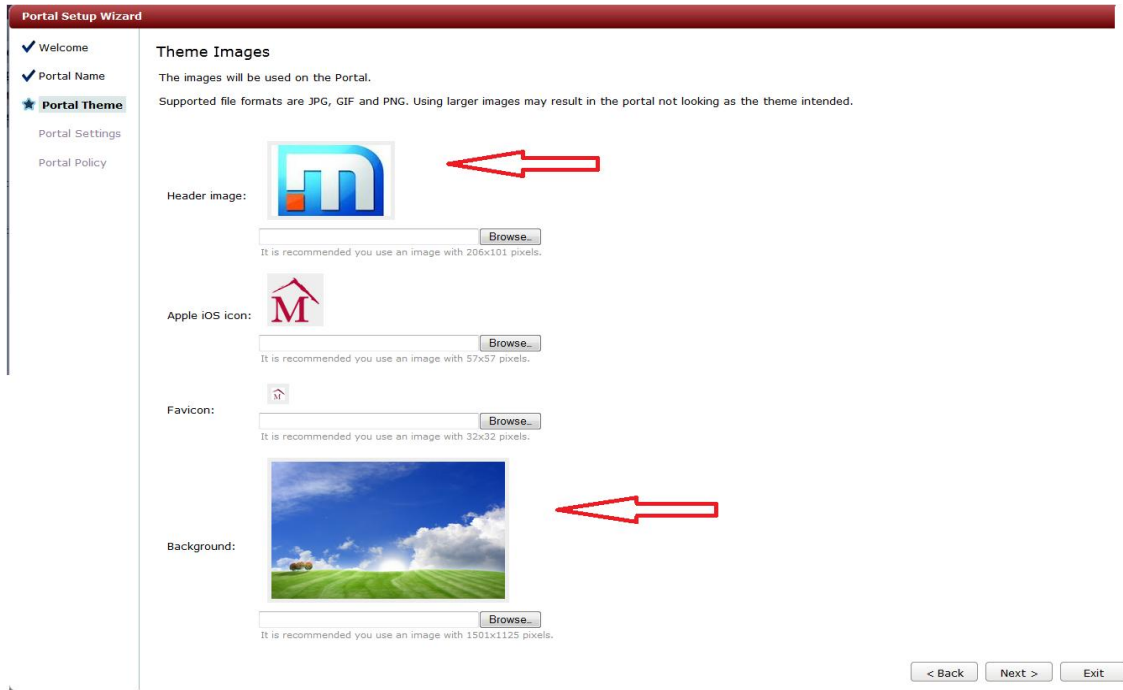
Figure 86: Customized Login Page



Create a customized portal:

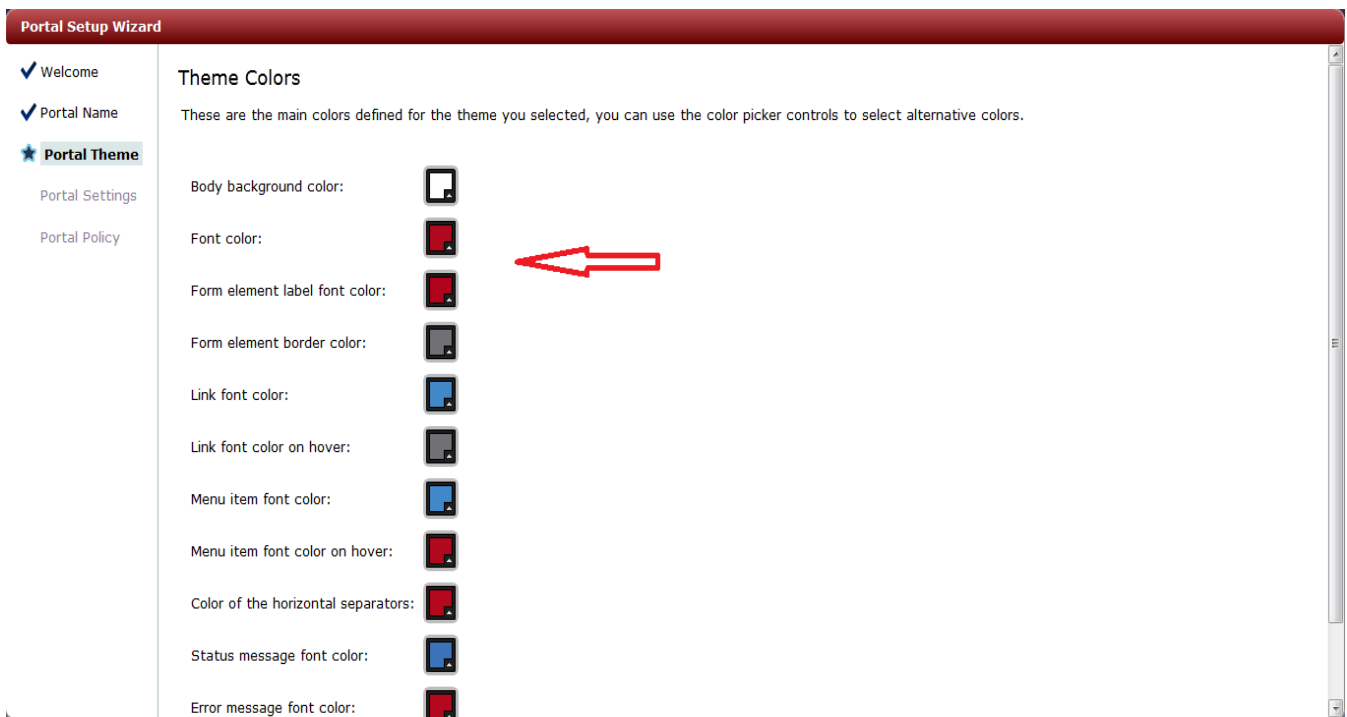
1. On the Theme Images page, specify the logo and background for the portal by uploading the new logo and background images for the portal theme, as shown in [Figure 87](#).

Figure 87: Theme Images Page



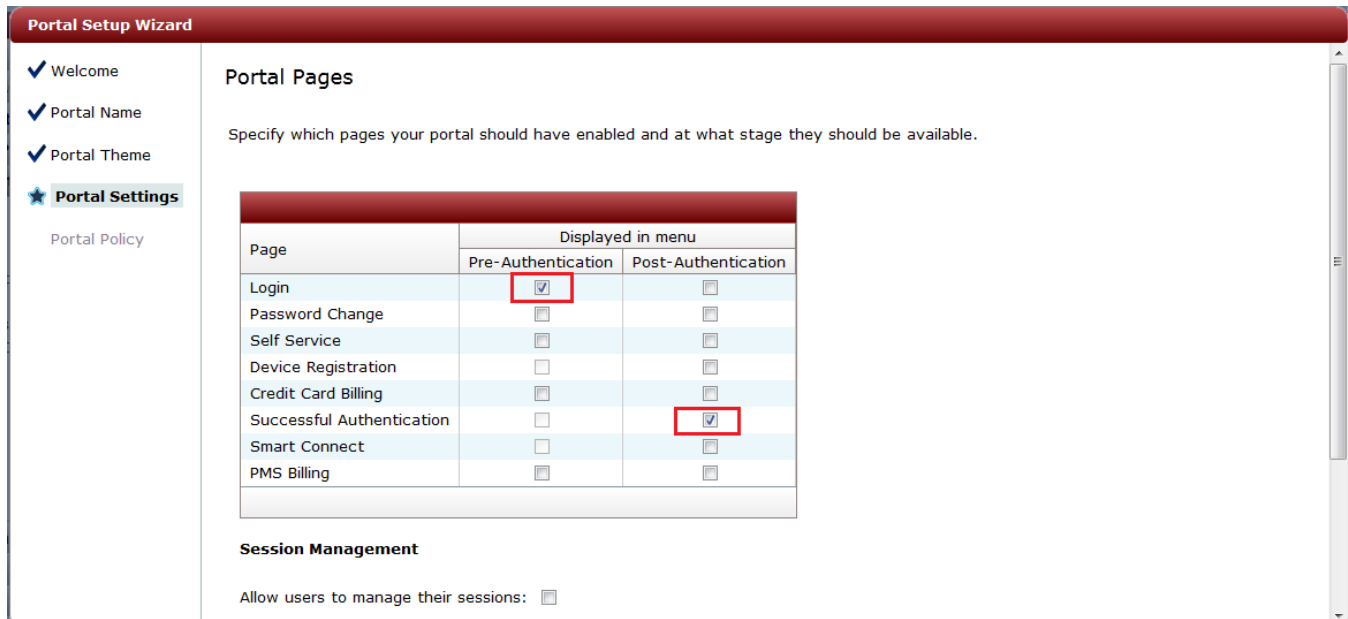
2. On the Theme Colors page, change the font colors to match the newly uploaded background image, as shown in [Figure 88](#).

Figure 88: Theme Colors Page



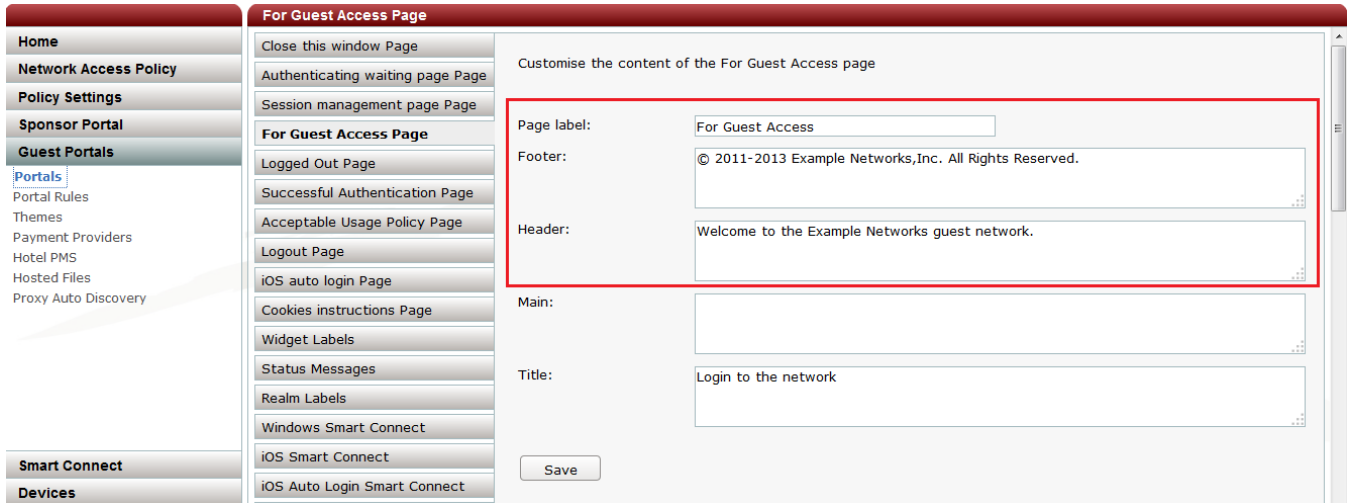
3. On the Portal Pages page, enable the following changes, as shown in [Figure 89](#):
 - Select the **Login** check box in the Pre-Authentication Column.
 - Select the **Successful Authentication** check box in the Post-Authentication column.
 - Make sure that the Session Management and Logout Options check boxes are clear.

Figure 89: Portal Pages Page



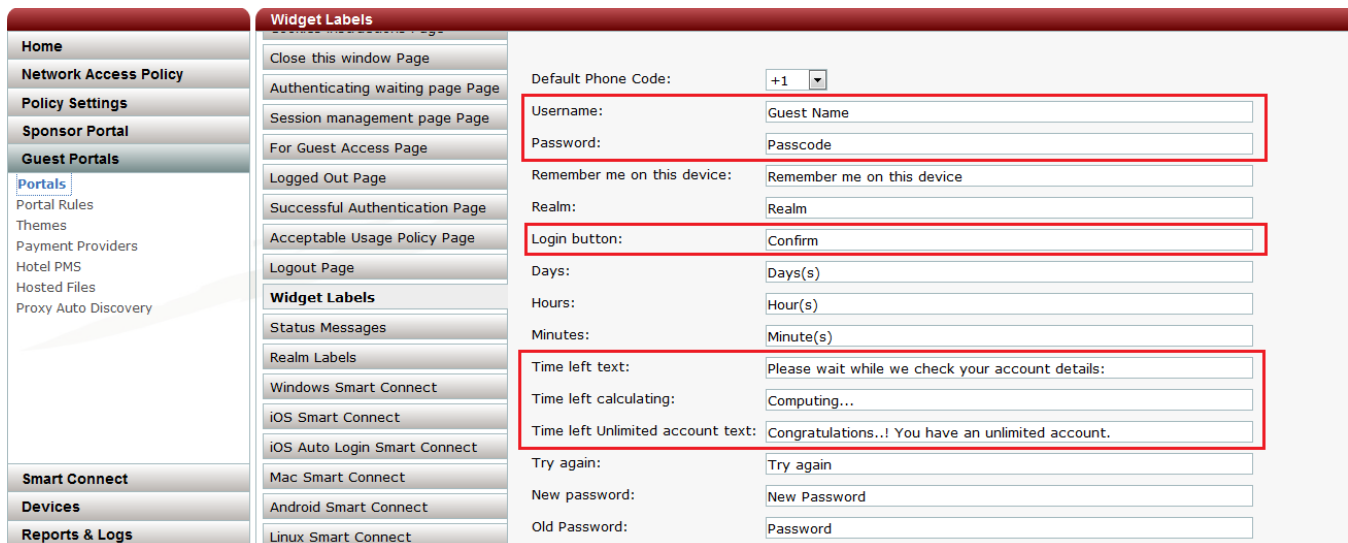
4. Complete the wizard pages to save the portal.
5. Edit the portal settings, and make the following changes on the Login Page, as shown in [Figure 90](#).
 - Page label: For Guest Access
 - Footer: © 2011-2013 Example Networks Inc. All Rights Reserved.
 - Header: Welcome Example Networks guest network

Figure 90: Changing the Login Page



6. Make the following changes to the widget labels, as shown in [Figure 91](#).
 - Login: Guest Name
 - Password: Passcode
 - Time left text: Please wait while we check your account details:
 - Time left calculating: Computing...
 - Time left unlimited account text: Congratulations..! You have an unlimited account.

Figure 91: Widget Labels Page



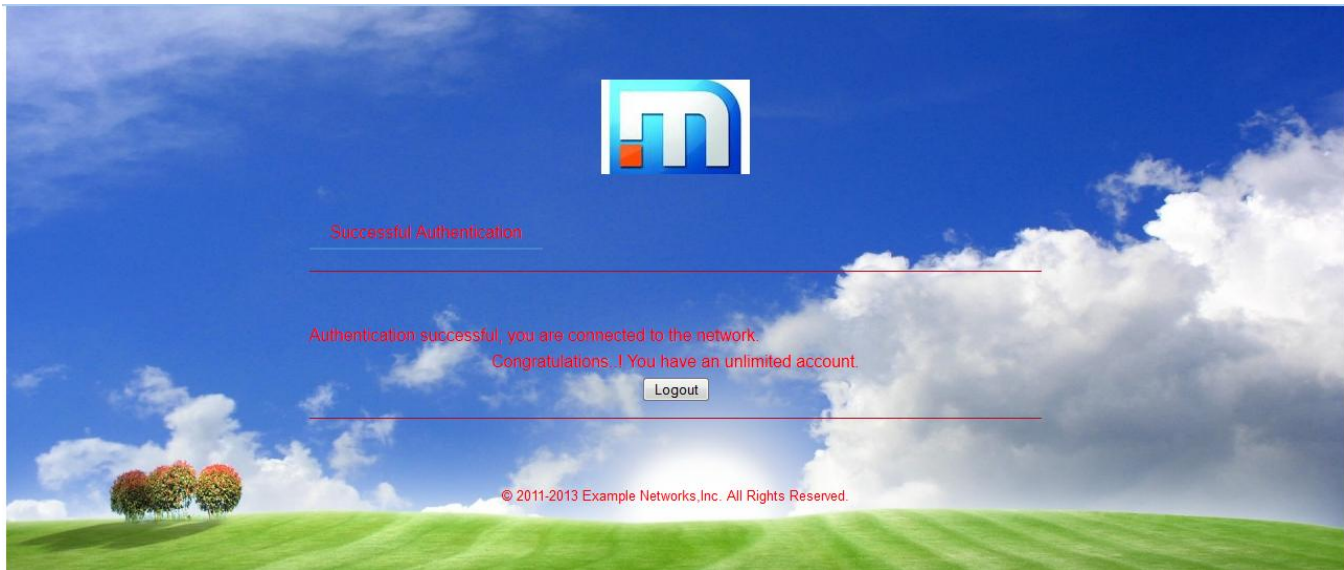
7. Save the changes for the portal.

[Figure 86](#) shows the customized login page. [Figure 92](#) shows the customized initial successful authentication page, with the modified text that appears while the system checks the guest user account information. [Figure 93](#) shows the customized authentication success page.

Figure 92: Customized Initial Successful Authentication Page



Figure 93: Successful Authentication Page After Customization



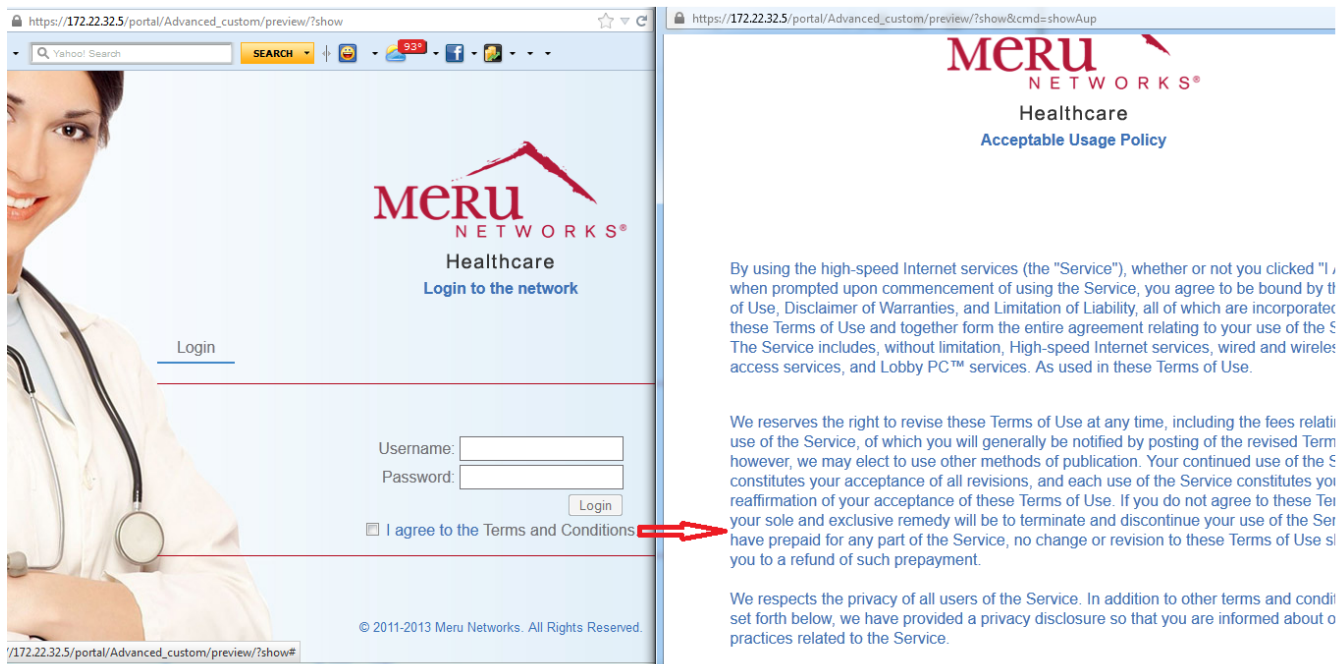
Use Case 7: Advanced Customization of Guest Portals by Importing a New Theme

You can completely change the look and layout of portal pages by importing custom HTML files that contain images and scripts. Depending on the complexity of pages, you need to be experienced in HTML coding, CSS, and JavaScript. This use case illustrates how you can use your images and JavaScript to customize the look of a portal.

In this use case, you create a customized portal that consists of the following elements, as shown in [Figure 94](#):

- New logo.
- New background image.
- Addition of "I agree to the Terms and Conditions" link and check box on login page.
- Enabling of login button only after user clicks "I agree to the Terms and Conditions" check box.
- Clicking the "Terms and Conditions" link opens a new window that provides the usage policy.

Figure 94: Customized Portal



In this use case, you create a portal named `Advanced_custom` that initially uses the default Meru_Networks (white) theme with only login and logout features enabled.

To customize the portal design, you edit the following theme files:

- `theme.xml`
- `aup.html`

You also need to provide new logo and background images, as shown in [Figure 95](#). You then create a new zip file with the modified theme files, which you upload to Identity Manager. After uploading, you can select the new theme for the portal customization.

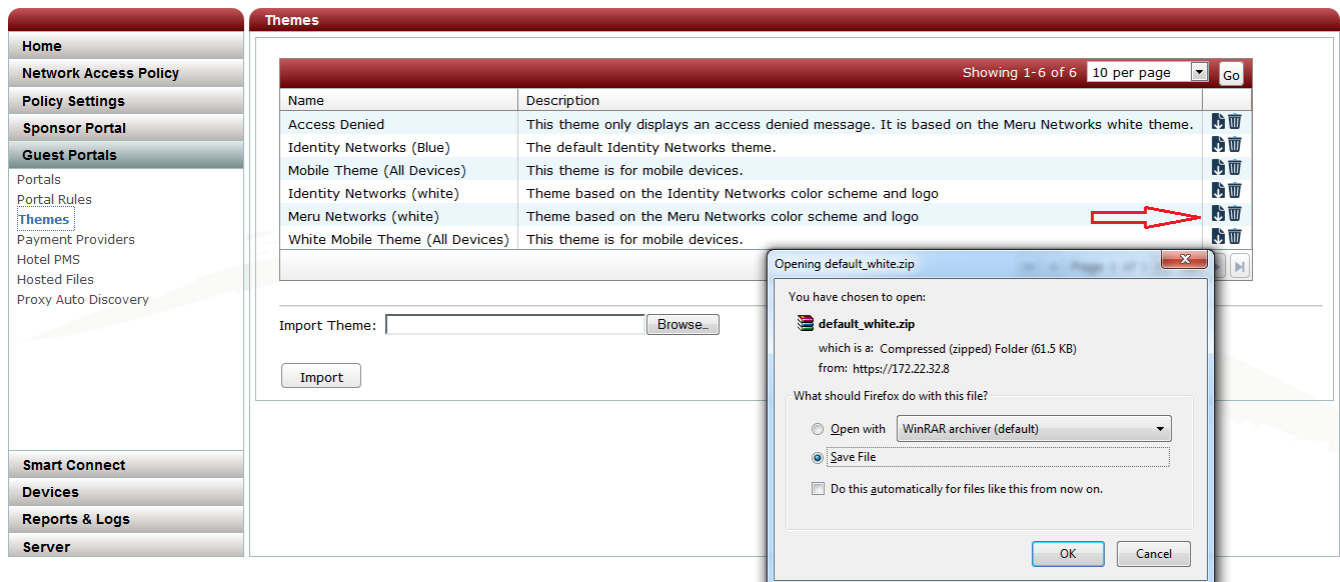
Figure 95: New Logo and Background



Customizing the Portal Theme

To customize the portal theme:

1. Download the default theme named “Meru Networks (white)” and save it to a local folder.



2. Extract the contents of the zip file.

3. Edit the theme.xml file to make the following changes:

- Replace the <name> value of meru_white with meru_healthcare.
- Replace the <publicName> value of Meru Networks (white) with meru_healthcare(white).

```
<hotspotTheme>
  <name>meru_healthcare</name>
  <publicName>meru_healthcare(white)</publicName>
  <description>Theme based on the Meru Networks color scheme and
  logo</description>
```

These changes rename the theme, which you will see after you upload the theme to Identity Manager.

4. Copy the new logo and background files to the images directory.

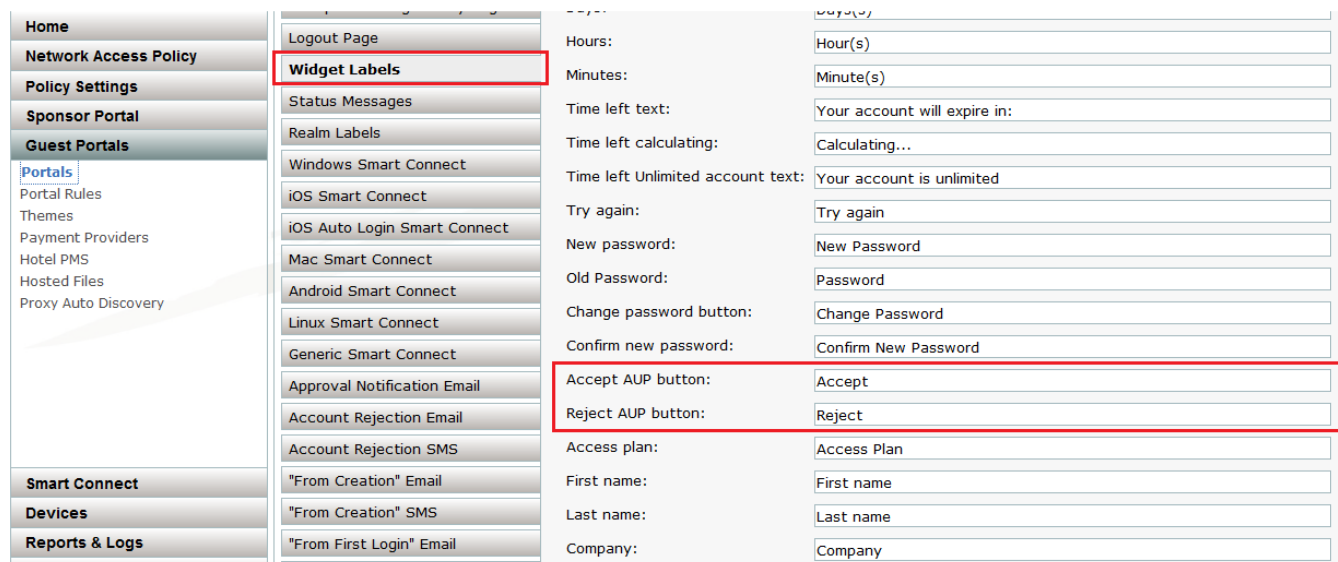
5. Edit the aup.html, which contains the acceptance usage policy (in the html directory), by adding the following code to the end of the file:

```
<script type="text/javascript">
  window.onload = function() {
    document.body.style.backgroundImage = "none";
  }
</script>

<script>
$(".widgetContainer").hide();
</script>
```

Editing the AUP page as previously described creates a blank background and also hides the widget labels for accepting or rejecting the terms and conditions. [Figure 97](#) shows the new AUP page.

Figure 97: New AUP Page



6. In the login.html file, find the following lines (labeled "a" and "b" in this document but not in the file itself):

- a.

```
<div id="feedback">
  <div class="feedbackContent">%FEEDBACK_AREA%</div>
</div>
```
- b.

```
<div id="main">
  <div class="mainContent">%MAIN%</div>
  <div class="widgetContainer">%LOGIN_WIDGET%</div>
```

Add the following JavaScript code between lines "a" and "b":

```
<script language="javascript">
window.onload = function() {
    document.getElementById("form").cmd_doLogin.disabled = true;

    if(!document.forms['form'].chkboc_tnc.checked) {
        document.getElementById("form").cmd_doLogin.disabled = true;
    }
}
function btn_display() {
    if(!document.forms['form'].chkboc_tnc.checked) {
        document.getElementById("form").cmd_doLogin.disabled = true;
    }
    else
        document.getElementById("form").cmd_doLogin.disabled = false;
}
$(document).ready(function() {
$("#testAup").click(function (event) {
    var pathArray = window.location.pathname.split( '/' );
    var newURL = window.location.protocol + "://" + window.location.host + "/"
+ pathArray[1] + "/" + pathArray[2] + "/" + pathArray[3] +
"/?show&cmd=showAup";
    var w = window.open(newURL,
                        "AUP",

"menubar=no,location=no,status=no,scrollbars=yes,resizable=yes,height=650px,w
idth=900px");
    w.focus();
    event.preventDefault();

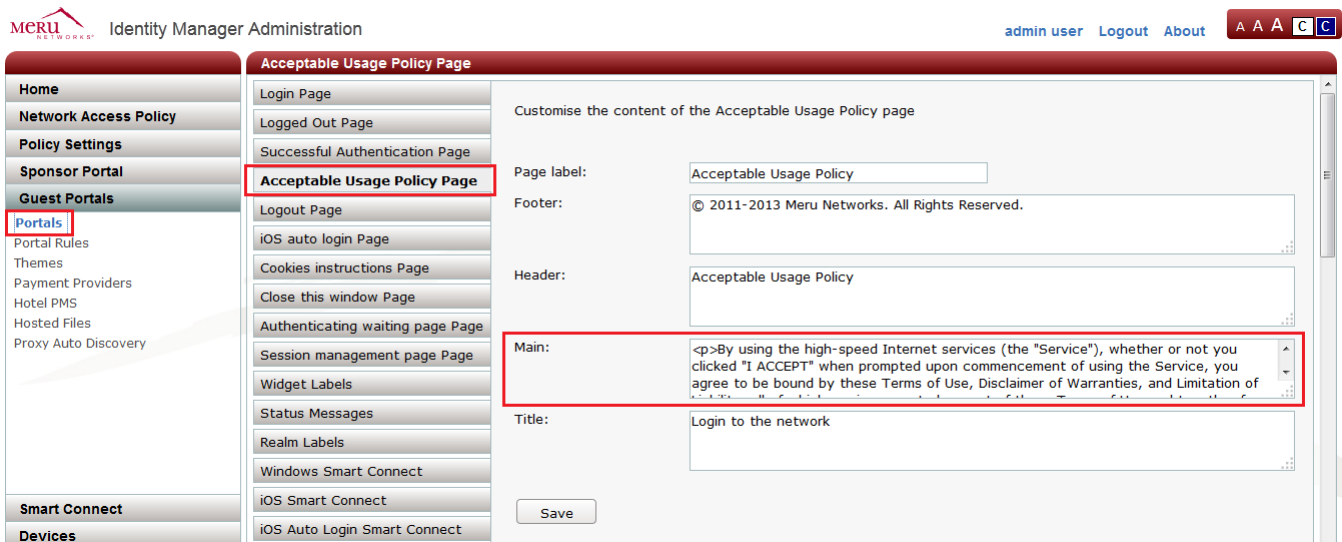
});
});
</script>
```

Add the following code after line "b":

```
<div class="frm_blk tnc"><input name="" id="chkboc_tnc" type="checkbox"
value="" onclick="btn_display()" /> I agree to the
<a id="testAup" href="#">Terms and Conditions</a>.
<a href="#tclink" onclick="submitForm('showAup'); return false;"
accesskey="0" title="Terms and Conditions" pagetype="aup" command="showAup"
style="display:none">Terms and Conditions</a>
</div>
```

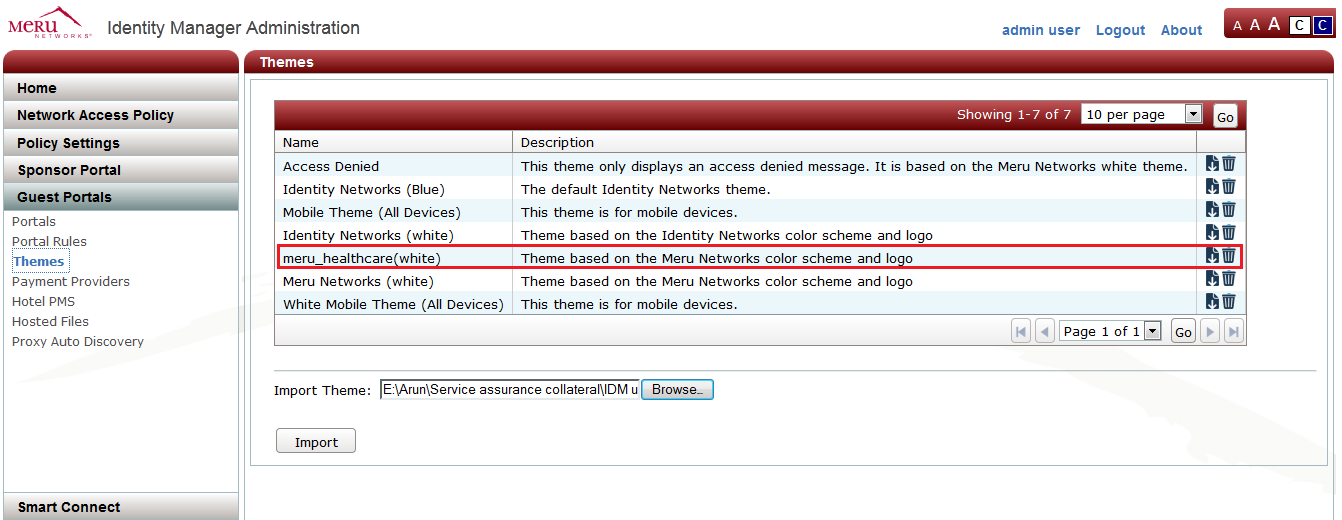
The previous script specifies that the login button remains disabled unless the check box for the "I agree to the Terms and Conditions" link is enabled. The script also calls the function to open the "acceptance usage policy" in a new window (AUP) by clicking the Term and Conditions.

7. Save the login.html file.
8. Edit the Advanced_custom portal settings, and add contents to the Main section on the Acceptable Usage Policy page. The content added is dependent on the requirements of your organization or the service provider who hosts the guest network.



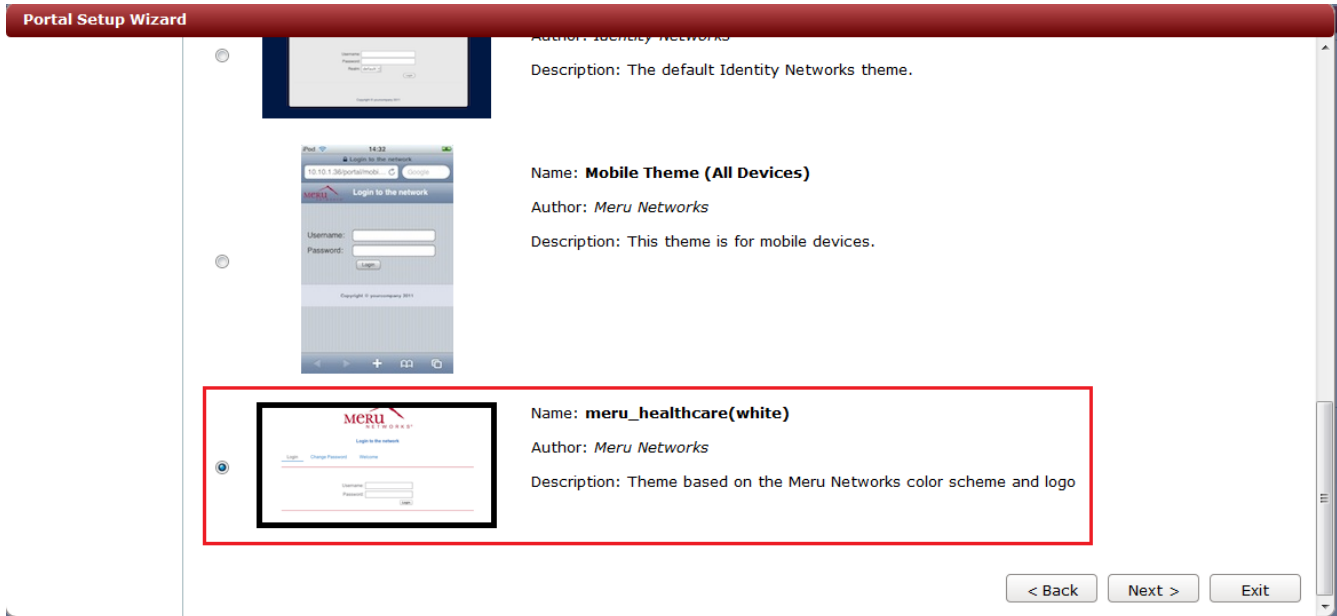
9. Create a new zip file containing the files, and upload the zip file to Identity Manager. In this example, the file is changed to meru_healthcare.zip, as shown in [Figure 98](#).

Figure 98: New Theme Uploaded to Identity Manager



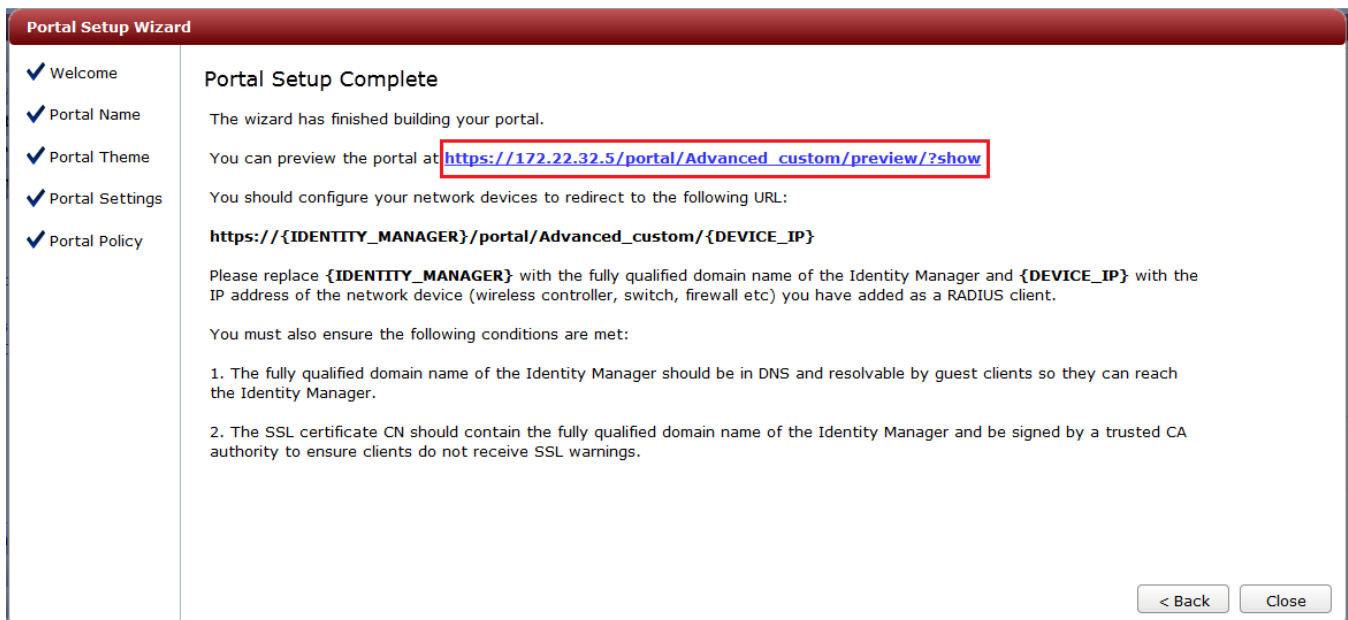
10. Edit the `Advanced_custom` portal, and select the newly uploaded theme, as shown in [Figure 99](#).

Figure 99: Selecting New Portal Theme



11. Before closing the wizard, preview the portal to make sure everything works correctly, as shown in [Figure 100](#).

Figure 100: Portal Setup Complete Page



Where to Find More Information

Refer to the following documents for additional information:

- *Meru Identity Manager User Guide*
- *Meru System Director Configuration Guide* (On the Software Downloads & Documentation page, click the link for the release of System Director that you are using.)