

Identity Manager Deployment Guide

June 2013

Contents

Introduction
What's New in this Guide 4
What's Changed in this Guide 4
Installing Identity Manager on VMware Platforms5
Identity Manager HTTP Redirection Process 5
Integrating Identity Manager with System Director
Configuring System Director
Configuring Identity Manager
Deployment Examples 15
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 44
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
Where to Find More Information

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 <u>Identity Manager Deployment Guide</u>, 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 <u>Identity Manager HTTP Redirection Process</u> topic was updated to reflect System Director Release 6.0 and Identity Manager Version 13.6.
- In <u>Use Case 1: Providing Enterprise Security in BYOD Environments</u>, 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 Tunneled Mode

Wireless Client	Meru Controller	Identity Manage
		×
HTTP request goog	e.com	
Http redirect to Identity M server_ip,login_url=extern	fanager with POST nalauth,original_url,ssid,station_mac,station_ip	
HTTP respsonse Portal Login Page		
	HTTP Request	
	POST Form with C POST request to login user_id,password : https://server_ip:808 Badius reques	redentials url with station_mac,station_ip
	Radius respo	nse
	POST response to Identity Ma	anager with success or failure page
HTTP response		
Portal Success/Fail pa	age	

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:

- <u>Creating RADIUS Profiles</u>
- Mapping the RADIUS Profile to the Captive Portal and Configuring the External Captive
 Portal URL
- <u>Configuring QoS Rules</u>
- Creating a Security Profile
- <u>Creating an ESS Profile</u>
- 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

WLAN Management MC15	50-VE 6.	0-83			admir	n@172.22.34.6 level:15 2:5	0:58 PM <u>WebTerm</u> <u>Save Loqout</u> <u>He</u>	Meru		
Monitor	RADIUS	ADIUS Configuration Table (2 entries)								
Maintenance		RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Called-Station-ID Type	Owner		
Wizards		IDAU17222328	172.22.32.8	1812	Hyphen (-)	Shared Key	Default	controller		
▼ Configuration		IDAC17222328	172.22.32.8	1813	Hyphen (-)	Shared Key	Default	controller		
System Config Quick Start										
Security Profile										
Radius Captive Portal Guest Users										

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

As shown in <u>Figure 4</u>, 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

WLAN Management	MC15	50-VE 6.0-83			admin@172.22.34.6	level:15	2:52:31 PM
Monitor		Captive Portal - Update					
Maintenance							
Wizards							
 Configuration 	-	Name	Captive Portal				
System Config Quick Start		Server Port	10101	Valid range: [1024-65535]			
Security Profile		Primary RADIUS Profile Name	DAU17222328				
Radius Captive Portal	=	Secondary RADIUS Profile Name Primary Accounting Radius Server Profile Name	No RADIUS				
Guest Users Mac Filtering		Secondary Accounting Radius Server Profile Name	No RADIUS				
VPN Client		Accounting Interim Interval (seconds)	600	Valid range: [600-36000]			
VPN Server Rogue APs		CaptivePortalSessionTimeout	0	Valid range: [0-1440]			
Wired		CaptivePortalActivityTimeout	0	Valid range: [0-60]			
GRE		CaptivePortal Authentication Type	radius 🗨				
Ethernet		CaptivePortal External URL	https://172.22.32.8/portal	Enter 0-255 chars.			
Wireless Radio		L3 User Session Timeout(mins)	1	Valid range: [1-255]			
ESS Mesh		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 <u>Figure 5</u>, allow traffic on port 443 to and from the Identity Manager IP address with the same firewall Filter-ID (string) mapped to each rule.

WLAN Management	t Mo	C155	50-VE 6.	.0-83	;							admin@17	2.22.34.6 I	evel:15 2:5	i6:59 PM	<u>WebTerm</u> <u>Sav</u>	<u>re Loqout He</u>	Meru
Monitor			QoS an	d Fii	rewall Rule	s (10 entries)												
Maintenance			Globa		ity of Service	Parametere	OoS and Fire	vall Dulae	OoS Codec Pul									
Wizards			01000	r ajuur	ity-01-0011100	- drumeter b	quotandrinet		QUU COUCE NU									
Captive Portal Guest Users Mac Filtering		*		ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	Qo S Protocol	Action	Qos Rule Logging	Qos Rule Logging Frequency
Wapi Server				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
VPN Client VPN Server		_		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
Rogue APs				3	0.0.0	0.0.0.0	5060	0.0.0.0	0.0.0.0	0	17		0	0	SIP	CAPTURE	Off	60
Wired VLAN				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
GRE				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
Port				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
Wireless Radio		Ξ		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
ESS				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
Mesh Hotspot				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
ServiceControl OoS Settings				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
Devices System Settings Controller																		

Figure 5: QoS and Firewall Rules Page

Creating a Security Profile

As shown in <u>Figure 6</u>, 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 <u>Configuring QoS Rules</u> must be mapped to the security profile.

Figure 6: Creating a Security Profile

Profile Name	Corp_Guest_Portal
L2 Modes Allowed	✓ Clear 802.1x Static WEP keys ○ WPA ○ WPA PSK ○ WPA2 ○ WPA2 PSK ○ MIXED ○ MIXED_PSK ○ WAI ○ WAI PSK
Data Encrypt	WEP64 WEP128 TKIP CCMP-AES CCMP/TKIP WPI-SMS4 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	PEAP 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 <u>Figure 7</u>, map the security profile to the ESS profile.

Figure	7:	ESS	Profile -	Update	Page
--------	----	-----	-----------	--------	------

WLAN Management MC1	550-VE 6.0-83	admin@172.22.34.6
Monitor	ESS Profile - Update	
Maintenance	ESS Profile ESS-AP Table Security	Profiles Hotspot Profiles
Wizards Roque APs		
Wired VLAN	SSID Number	4
GRE Ethernet	ESS Profile SSID	Corp_Guest_portal Corp Guest Portal
Wireless Radio	Enable/Disable	Enable 🗨
ESS Mesh	Security Profile	Corp_Guest_Portal
Hotspot ServiceControl	Primary RADIUS Accounting Server Secondary RADIUS Accounting Server	
QoS Settings Devices System Settings	Accounting Interim Interval (seconds)	3600 Valid range: [600-36000]
Controller =	Beacon Interval (msec)	100 Valid range: [20-1000]

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

	RADIUS Clients					
Home	Client Attributes SNMP MAC Auth	entication RadSec Authentication Automatic Setup				
Network Access Policy						
Policy Settings	Name:	Example Controller				
Sponsor Portal	Device IP Address / Prefix Length:	10.10.10				
Guest Portals	;;;;;;; _	For example 192.168.1.1/32 or fec0:0001/128				
Smart Connect	Secret:	Confirm: Leave black to keep existing serret				
Devices RADIUS Clients	Туре:	Meru SD 6.0 & Later 💽 If your RADIUS client vendor is not listed please select Generic RADIUS Device				
Email Settings SMS Settings Syslog Monitoring LDAP Server	Description:					
Syslog Servers	Change-of-Authorization					
	Use COA: 🔽					
	Port: 3799					
	Save Cancel					

Captive Portal and RADIUS-specific configuration that needs to be configured on the controller can be automatically pushed from Identity Manager, as shown in <u>Figure 9</u>.

Figure 9: RADIUS Client Automatic Setup

Network Access Policy							
Policy Settings	Client Attributes SNMP MAC Auther	ntication RadSec Authentication Automatic Setup					
roncy settings							
Sponsor Portal		172.22.32.8					
Guest Portals	Identity Manager Address:	This hostname is used to redirect guests to the Identity Manager, it should match the SSL certificate on Identity Manager.					
Smart Connect	Device IP Address:	10.10.10					
Devices PADIUS Clients	Admin user name:	admin					
Email Settings SMS Settings	Admin Password:	Leave blank to keep existing password					
Syslog Monitoring	Configure RADIUS profiles:						
Syslog Servers	Set Captive Portal RADIUS profiles:						
	Set Captive Portal External URL:						
	Configure QoS Rules:						
	Write changes to startup-config:	This will overwrite your startup-config with the current running-config					
Reports & Logs	Setup Controller						

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 <u>Figure 10</u>.

Figure 10: RADIUS Authentications Page

CRU Identity Manage	r Administration					admin user	Logout	
	RADIUS Authenticatio	ons						
lome								
etwork Access Policy	Between:	20 🔻 May 🔻 20	13 💌 🛗					
olicy Settings	between	00 🕶 00 💌						
sponsor Portal		21 💌 May 💌 20	13 💌 🛅					
Guest Portals	and:	00 - 00 -						
Smart Connect	Username:							
evices	Client IP Address:							
eports & Logs	Client MAC Address	5:						
/stem Logs	NAS IP Address:							
ADIUS Authentications	Status:	Successful Auther	tications 💌					
ayments Report	Rup	Successful Auther	tications					
isc Reports	Kun	All Authentications						
		-						
						25 per page 💽 Go		
				Time a A W	NAC TO Address A W			

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
- <u>Creating a Smart Connect Policy</u>
- 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 <u>Figure 12</u>, <u>Figure 13</u>, <u>Figure 14</u>, and <u>Figure 15</u>):

- 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

WLAN Management	MC15	550-VE 6.0-83	
Monitor		ESS Profile - Update	
Maintenance		ESS Profile ESS-AP Table Secu	urity Profiles Hotspot Profiles
 Wizards 			
 Configuration 	-		
System Config Quick Start		SSID Number	3 Corr Frankrus Datel
Security Profile		SSID	Corp_Employee_Portal
Radius			
Guest Users		Enable/Disable	Enable 💌
Mac Filtering	=	Security Profile	Corp_Employee_portal
Wapi Server		Primary RADIUS Accounting Server	
VPN Clienc		Consider BADING Association Consider	
Rogue APs		Secondary RADIUS Accounting Server	NO RADIUS
Wired		Accounting Interim Interval (seconds)	3600 Valid range: [600-36000]
VLAN GRE		Beacon Interval (msec)	100 Valid range: [20-1000]
Ethernet		SSID Broadcast	On 💌
Wireless		Bridging	AirFortress IPV6 AppleTalk
Radio		New AP's Join ESS	On 💌
Mesh		Tunnel Interface Type	No Tunnel

WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6 • Monitor Security Configuration Table (4 entries) ۲ Maintenance ESS Profile ESS-AP Table Security Profiles Hotspot Profiles ۲ Wizards . Configuration System Config Quick Start Clear 🔲 802.1x Static WEP keys Security WPA WPA PSK WPA2 Profile L2 Modes Allowed WPA2 PSK MIXED_PSK Radius WAI PSK 🔲 WAI Captive Portal Guest Users WEP64 WEP128 TKIP Mac Filtering Data Encrypt CCMP/TKIP CCMP-AES WPI-SMS4 Wapi Server Clear VPN Client Primary RADIUS Profile Name No RADIUS VPN Server Rogue APs Secondary RADIUS Profile Name No RADIUS Wired WEP Key (Alphanumeric/Hexadecimal) VLAN GRE Static WEP Key Index 1 Valid range: [1-4] Ethernet Port Re-Key Period (seconds) 0 Valid range: [0-65535] Wireless 0 BKSA Caching Period (seconds) Valid range: [0-65535] Radio ESS WebAuth 🖵 Captive Portal Mesh Captive Portal Authentication Method external 👻 Hotspot

Figure 13: Security Profile Mapped to Provisioning ESS Profile

Figure 14: WPA2-Enabled ESSID

WLAN Management	MC15	50-VE 6.0-83	admin@172.22.34.6
Monitor		ESS Profile - Update	
Maintenance		ESS Profile ESS-AP Table Security Profi	iles Hotspot Profiles
Wizards			
 Configuration 	-		
System Config		SSID Number	1
Quick Start		ESS Profile	Coro dot1x
Security			
Profile		SSID	Corp_dot1x
Radius			
Captive Portal		Enable/Disable	Enable
Guest Users			
Mac Filtering	=	Security Profile	Corp_dot1x
Wapi Server			
VPN Client		Primary RADIUS Accounting Server	IDAC17222328
VPN Server		Secondary RADIUS Accounting Server	
Rogue APs			
Wired		Accounting Interim Interval (seconds)	3600 Valid range: [600-36000]
VLAN			
GRE		Beacon Interval (msec)	100 Valid range: [20-1000]
Ethernet		SSID Broadcast	On 💌
Port			

WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6 level:15 12:29:46 AM WebTerm Save Logout Help мени Monitor **RADIUS Configuration Table (2 entries)** ۲ Maintenance RADIUS Profile Name RADIUS IP **RADIUS Port** MAC Address Delimiter Password Type Called-Station-ID Type Owner Wizards DAU17222328 172.22.32.8 1812 Hyphen (-) Shared Key Default controller Configuration DAC17222328 172.22.32.8 1813 Hyphen (-) Shared Key Default controller System Confin Quick Start WLAN Management MC1550-VE 6.0-83 admin@172.22.34.6 level:15 12:30:45 AM WebTerm Security Profile • Monitor Security Configuration Table - Update Radius Maintenance ۲ Wizards Configuration System Config Clear 🔲 802.1x Static WEP keys Quick Start WPA WPA PSK L2 Modes Allowed Security WPA2 PSK MIXE D PSK Profile 🔲 WAI WAI PSK Radius WEP128 WEP64 Captive Portal Data Encrypt CCMP-AES ССМР/ТКІР WPI-SMS4 Guest Users Clear Mac Filtering Primary RADIUS Profile Name IDAU17222328 -Wapi Server VPN Client -Secondary RADIUS Profile Name No RADIUS

Figure 15: Security and RADIUS Profiles Mapped to ESS Profile

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

Authorization Profiles		
Home		
Network Access Policy	Sho	owing 1-3 of 3 10 per page 💌
Authentication Policy	Name 🔺 🔻	Description A 🔻
uthorization Policy	corporate users	Auth profile for corporate users
uthorization Profiles	<u>Default</u>	Default authorization profile
	Secure Guest Access	For secure guest access
		Page 1 of 1 💌 Go 🕨
	Add Profile	

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. <u>Figure 17</u> shows the information used in his use case.

Figure 17: Adding an Active Directory Server

lame:	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 <u>Figure 18</u>).

Figure 18: Attribute Mappings

Add Authenti	cation Server			
Connection				
connection				
Name:	172.22.32.6			
Server Typ	e: Microsoft Active Directory			
Server:	172.22.32.6			
Domain:	bangalore.merunetworks.com			
Attribute N				
The respon	a from the external server is tested against each rule below in order. If a rule is matched the specified usage profile	and authoriz	ration profile a	heilance er
The respon	a contrate external server is tested against each fulle below in order. If a fulle is matched the specified daage prome	and addition2	adon prome a	e applied
and guest a	uthentication succeeds.			
If no rule	s match Accept authentication 💌 set usage profile to Unlimited 💌 and authorization profile to corporate users	-		
add mappin	<u>g</u>			
		< Back	Next >	Exit
		< Dack	MOXL >	LAIL

3. Make sure that Identity Manager joins the domain that Active Directory server represents, as shown in <u>Figure 19</u>.

Figure 19: Identity Manager Joins Active Directory Domain

dd Authentic	ation Server	
Connection		
Name:	172.22.32.6	
Server Type	: Microsoft Active Directory	
Server:	172.22.32.6	
Domain:	bangalore.merunetworks.com	
Secure Auth	uentication .	
Secure Auto		
To enable se	cure connections from Windows clients this server must be joined to the AD domain.	
This conver it	-	
This server is	s currently joined to the domain.	
Join the dor	nain Disconnect from the domain	
Allow Windows computer authentication (machine/host authentication)		

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.

< Back Next > Exit

Figure 20: Network Settings Page

elcome	Network Settir	ngs	
etwork Settings	Please provide a r	name and type for the network.	
uthentication	Network Name:	Corp_dot1x	
oxy Settings	Network Type:	⊙ wired ⊛ wireless	
eruncates			
the second second	SSID:	Corp_dot1x	
ther Options	SSID: SSID is Broadcast	Corp_dot1x :: 🖉	

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

Smart Connect Profile	e Wizard	
✓ Network Settings	Please provide the authentication details for the network.	*
🖈 Authentication	WDA/WDA2 Enterprise	
Proxy Settings	Authentication: Windows systems will use WPA2	
Certificates	EAP Type: Windows PEAP/MSCHAPv2	
	Apple iOS / OS X PEAP/MSCHAPv2 and PEAP/GTC 💌	
Other Options	Android PEAP/GTC	
	Linux PEAP/GTC •	
	Include Credentials: Include username/password in profile sent to user 	
	Onl't include username/password in profile sent to user	
	Username Format	Ξ
	Authenticate with: 🔘 realm\username	
	💿 realm/ <i>username</i>	
	<i>◎ username</i> @realm	
	(e) username	
	Realm:	
	Detect and override username format and realm when authenticating against Active Directory: ${ar V}$	
	< Back Next > Exit	+
h		

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 2	2: Certific	cates Page
----------	-------------	------------

Smart Connect Profil	e Wizard		
Velcome	Certificates		~
✓ Network Settings	Please select the CA certificates that you want to install into the trusted root CA store on the client.		
 Authentication 		*	
✓ Proxy Settings	Equifax Secure Certificate Authority Entrust.net Secure Server Certification Authority		
🚖 Certificates	☑ Thawte Premium Server CA		
Other Options	Class 3 Public Primary Certification Authority - G2 (c) 1998 VeriSign, Inc For authorized use only VeriSign Trust Network		
	VeriSign Class 3 Secure Server CA - G2		
	localhost.localdomain [localhost]		=
	GeoTrust Global CA	=	
	Thawte DV SSL CA		
	thawte Primary Root CA		
	Thawte SGC CA		
	Entrust Certification Authority - L1C	-	
	Upload Certificate: Upload Upload		
L	< 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 R	ule Wizard
Smart Connect Rt ✓ 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 <u>Figure 24</u>.

Figure 24: Profiles Page

Smart Connect Rule	Wizard
✔ Welcome	Profiles
✓ Details	Select the Smart Connect profiles that you want to assign to users that match this rule.
Conditions	No Smart Connect
🚖 Assign Profile	Assign Smart Connect Profiles
	Available Wireless Profiles Selected Wireless Profiles
	Secure_Guest_Access
	Available Wired Profiles Selected Wired Profiles
	<<>>> 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

	NETWORKS Corporate access Login to the network
	Login
-	
	Username:
	Password:
	Login
-	

3. To enable Smart Connect, select the Smart Connect check box in the Post-Authentication column, as shown in <u>Figure 26</u>.

Figure 26: Enabling Smart Connect for the Employee Provisioning Portal

Portal Setup Wizard								
✔ Welcome	Portal Pages							
✓ Portal Name								
✓ Portal Theme	Specify which pages your port	tal should have enable	ed and at what stage t					
* Dortal Cattings								
Fortal Settings								
Portal Policy	Page	Displaye	d in menu					
		Pre-Authentication	Post-Authentication					
	Login	V						
	Password Change							
	Self Service							
	Device Registration							
	Credit Card Billing							
	Successful Authentication							
	Smart Connect							
	PMS Billing							
	Help							
	Welcome							
	Session Management							
	Allow user to close existing a	sessions when the cor	ncurrent session limit is					
	, and about to clobe existing a							
	Logout Options							
	· ·							

4. Add the realm (Active Directory domain) to the portal, as shown in <u>Figure 27</u>. 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

Portal Setup Wizar	
✔ Welcome	Portal External Authentication Policy
 Portal Name Portal Theme Portal Settings Portal Policy 	Select which realms should be used for authentication on the login page. If the selection mode is set to automoatic internet services such and Google, Facebook and Twitter will always be checked last. Available Realms default bangalore.merunetworks.cr Down
	Selection Mode Manual: guests have to select the appropriate realm from "Selected Realms" list. Automatic: each realm is tried in the order from "Selected Realms" list.

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

MERU

Identity Manager Administration

	Portais		
Home			
Network Access Policy		Showing 1-5 of 5 10 per	page 💌 Go
Policy Settings	Name	Description	
Sponsor Portal	access-denied	Default portal that denies access	Q 🕸 🖺 🗮 🗑
Guest Portals	Corp Employee port	tal Corp_Employee_portal	Q 🕸 🖺 🛍
Dortals	Corp Guest Portal	Corp_Guest_Portal	Q 🕫 🖺 🖹 🗑
Portal Rules	login	Default login portal	Q 🕫 🖺 🖹 🗑
Themes	mobile	Default portal for mobile devices	Q 🕸 🖺 🕷 🗑
Payment Providers		Rege 1 of	1 - Go > >
Hosted Files Proxy Auto Discovery	Add 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).

To 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 <u>Figure 31</u>), 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. 6. 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.

- 7. 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 <u>Figure 32</u>.
- 8. 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 <u>Figure 33</u>.
- 10. Click Close.

Figure 29: Connecting to Employee Portal and Getting Redirected

Login to the network X	
🗧 🗘 🖒 🕹 🖒 د 🖒 د 🖒 د د د د د د د د د د د د د	
🔍 💿 🖉 🛛 💽 🖌 🔍 🐨 🔍 🐨 🚱 🖌 🔍 🐨 🖉	
Login	
Username: Password: Remember me on this device Login	Currently connected to: 42
© 2011-2013 Meru Networks. All Rights Reserved.	Wirdess Network Jonnettoon
	▲ 🙀 🐠 17:46 16-05-2013

Figure 30: Providing Corporate User Credentials

Q Search Ø F 3 Yuutter CNN · ₩.9 · 🙆 · 🖂 · ≫ ·	
Login	
Username: corp_employee Password: •••••• Remember me on this device	
© 2011-2013 Meru Networks. All Rights Reserved.	
	- No - 17:46 - No - 16-05-2013

Figure 31: Successful Authentication Page

M [*] Authentication successful ×		
 C (* المجلس * //172.22.32.8/portal/login/172.22.34.6/success) 	🕞 Pop-up blocked 👷 🐠 😑	
🔍 💽 Search 💋 📑 â. You🏧 • 🕼 • 🍋 • 🖂 • 😒 •	<u>^</u>	
Client Configuration Successful Authentication Authentication successful, you are connected to the network.		
Secure Network Access		
To configure your device for secure encrypted network access please click: Smart Connect		
Open Network Access		
Alternatively you can continue to access the network unencrypted without doing anything more.		
Your account will expire in: Calculating		
© 2011-2013 Meru Networks. All Rights Reserved.		
🚯 💪 🖸 😼 🔕 🥞 📇 🕄 🕮 🗐 🍡 🛃 🏄 📾		▲ 📴 📲 🌵 17:47 16-05-2013



N R	Logout - Mozilla Firefax Attps://172.22.32.8/portal/login/172.22.34.6/success?command:	showLogout	
MII E V	Cor Logout by clicking the button	MCRUNETWORKS* Welcome to the Smart Connect network configuration tool. This program	
Mi He Go	Your 	 will configure your device so that it can authenticate to the network. 1. Please enter your credentials to access the network: Username corp_employee@bi Password ••••••• 2. Click Start to configure your computer and connect to the network 	
		© 2011-2013 Meru Networks. Al Rights Reserved.	
		1 S, 🖆 🦪 😼 🛃 🖻 🏠 🔶 1802	3

Figure 32: Installing Smart Connect (Continued)

	Logout - Mozilla Firefox https://172.22.32.8/portal/login/172.22.34.6/success?command=showLogout		
R	NETWORK Corporate access	K Meru Smart Connect	
V Mi Ho	Logout by clicking the button Your account is unlimited Logout	Connecting, please wait	
Go	© 2011-2013 Meru Networks, All Rights R	Connecting	
		© 2011-2013 Meru Networks. All Rights Reserved.	
e			▲ 18:03 16:05-2013



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:

- <u>Controller Configuration Tasks</u>
- <u>Creating an Authorization Profile for Guest Users</u>
- <u>Create a Smart Connect Profile</u>
- <u>Create a Smart Connect Policy</u>
- <u>Creating a Guest Portal</u>
- <u>Creating a Portal Rule</u>
- 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.

dmin@172.22.34.6 level:15 10:46:42 AM WebTerm Save Logout Help WLAN Management MC1550-VE 6.0-83 MERU Monitor VLAN Configuration (1 entry) Maintenance Fast Ethernet Interface IP Address of the Default VLAN Name Tag IP Address Netmask Owner Wizards Search: Configuration 255.255.255.128 Guest_access 10 172.22.32.99 172.22.32.1 controlle System Config Quick Start **Security** Profile Radius Captive Portal Guest Users Mac Filtering Wapi Server VPN Client VPN Server Rogue APs /ired VLAN

Figure 35: Creating a VLAN

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 <u>Figure 37</u>.)

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

WLAN Management	MC15	50-VE 6.0-83					WLA	AN Management	MC15	50-VE	6.0-83							
Monitor		Security Co	onfiguration Table	(4 entries)			٠.	Monitor		ESS	Profile - l	Jpdate						
Maintenance		ESS Profile	e ESS-AP Table	Security Profiles	Hotspot Profile	25	•	Maintenance		E	SS Profile	ESS-AP Table	Secu	urity Profiles	Hotspot Pro	ofiles		
Wizards							•	Wizards		-								
 Configuration 	-	Profile	e Name		Secure_Guest_a		• (Configuration	-									_
System Config Quick Start							Sy	ystem Config Quick Start			SSID Num	ber						
Security Profile					Clear	802.1	Se	ecurity Profile			SSID	e			Secure_Gues	Access		
Radius Cratius Partal		L2 Mo	odes Allowed					Radius Captive Portal										
Guest Users					WAI	WAI F		Guest Users			Enable/Di	sable			Enable 💌		_	
Mac Filtering				WEP64	WEP	Mac Filtering			Security Profile				Secure_Guest_access					
VPN Client	E	Data I	Encrypt		CCMP-AES			VPN Client	Ш		Primary R/	ADIUS Accounting) Server		No RADIUS	-		
VPN Server					Clear			VPN Server			Secondary	RADIUS Account	ting Server		No RADIUS	-		
Kogue APs Wired		Prima	iry RADIUS Profile Name	2	No RADIUS	-	W	ogue APs /ired			Accounting	g Interim Interval ((seconds)		3600		Valid rang	e: (600-30
VLAN		Secor	ndary RADIUS Profile Na	ime	No RADIUS	-		GRE			Beacon In	terval (msec)			100		Valid rang	e: [20-10(
Ethernet		WEP	Key (Alphanumeric/Hexa	adecimal)				Ethernet			SSID Broa	dcast			On	•		
Port		Static	WEP Key Index		1	Val	w	Port			Bridging						51.62	
Radio		Re-Ke	ey Period (seconds)		0	Val		Radio			New AP's	Join ESS			On v	5 🗀 1	PVO	
ESS		BKSA	Caching Period (second	ds)	0	Val		ESS			Tunnel Int	erface Type			No Tunnel			
Hotspot		Captio	ve Portal		WebAuth 💌			Hotspot			VI AN Non	10			No VI AN			
ServiceControl QoS Settings		Captio	ve Portal Authentication	Method	external 💌		Se	erviceControl			V LAN Nan	12			NO VEAN			

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

	Authorization Profiles		
lome			
letwork Access Policy	Sho	wing 1-3 of 3 10 per page 💌	Go
uthentication Policy	Name 🔺 🔻	Description A 🔻	
uthorization Policy	corporate users	Auth profile for corporate users	Ŵ
Ithorization Profiles	<u>Default</u>	Default authorization profile	Ŵ
	Secure Guest Access	For secure guest access	Ŵ
		Page 1 of 1 🗨 Go 🕽	
	Add Profile		

Create a Smart Connect Profile

MEDII

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

Smart Connect Profile V	Vizard				
✔ Welcome	Network Settings	*			
🚖 Network Settings	Please provide a name and type for the network.				
Authentication	Network Name: Secure_Guest_Access				
Proxy Settings Certificates	Network Type: © wired © wireless				
Other Options	SSID: Secure Guest Access				
SSID is Broadcast: Remove SSIDs Please enter the SSIDs that you would like to remove from the client. It is advisable to remove the SSIDs for any open networks that you don't want the client to automatically connect to.					
		Ŧ			

Figure 40: Specifying WPA2-PSK

Smart Connect Profil	e Wizard
✔ Welcome	Authentication
✓ Network Settings	Please provide the authentication details for the network.
* Authentication	Authentication: WPA2 Pre-Shared Key
Proxy Settings	Pre-Shared Key: ••••••• Show
Certificates	
Other Options	
	< Back Next > 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

Smart Connect Rule Wizard	
Smart Connect R Uelcome Details Conditions Assign Profile	ule Wizard 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 secure Guest Access Add Condition
	< Back Next > Exit
Figure 42: Assigning Smart Connect Wireless Profiles

Smart Connect Rule	le Wizard									
✔ Welcome	Profiles	^								
✓ Details	Select the Smart Connect profiles that you want to assign to users that match this rule.									
 Conditions 	O No Smart Connect									
🔺 Assign Profile	Assign Smart Connect Profiles									
	Available Wireless Profiles Selected Wireless Profiles									
	Corp_dot1x									
	Down	=								
		_								
	Ψ Ψ	_								
	Available Wired Profiles Selected Wired Profiles									
	^ Up									
	Down									
L	v v	-								

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 <u>Figure 43</u>. <u>Figure 44</u> shows how to enable Smart Connect for the portal.

Figure 43: Guest Access Portal

	NETWORKS Guest access	
Login	_	
	Username: Password:	

Figure 44: Enabling Smart Connect for the Guest Portal

Portal Pages											
	-										
Specify which pages your portal should have enabled and at what stage they should be available.											
✓ Portal Theme											
	Displaye	d in menu									
Page Pre-Authentication Post-Authentication											
Login 🗹											
Password Change		8									
Self Service											
Device Registration		8									
Credit Card Billing											
Successful Authentication		V									
Smart Connect											
PMS Billing											
Help											
Welcome	10 A	8									

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 <u>Figure 45</u>.

Figure 45: Specifying the Default Realm

Portal Setup Wizar	d
✔ Welcome	Portal External Authentication Policy
 Portal Name Portal Theme Portal Settings Portal Policy 	Select which realms should be used for authentication on the login page. If the selection mode is set to automoatic internet services such and Google, Facebook and Twitter will always be checked last. Available Realms Available Realms Selected Realms bangalore.merunetworks.cr default Up Down Down
	Selection Mode Manual: guests have to select the appropriate realm from "Selected Realms" list. Automatic: each realm is tried in the order from "Selected Realms" list. Back Next > Exit

After making and saving the guest portal changes, the Corp_Guest_Portal that you created appears in the list of portals, as shown in <u>Figure 46</u>.

Figure 46: List of Portals



Identity Manager Administration

	Portals				
me					
letwork Access Policy		Showing 1-5 of 5 10 per	page 💌 Go		
Policy Settings	Name	Description			
Sponsor Portal	access-denied	Default portal that denies access	Q 🕸 🖺 🗮 🗑		
Guest Portals	Corp Employee portal	Corp_Employee_portal	Q 🕸 🖺 🛣 🗑		
ortals	Corp Guest Portal	Corp_Guest_Portal	Q 🕸 🖺 🛣 🗑		
Portal Rules	<u>login</u>	Default login portal	Q 🕸 🖺 🛣 🗑		
hemes	mobile	Default portal for mobile devices	Q 🕸 🖺 🛣 🗑		
ayment Providers		🖌 ┥ Page 1 of	1 - Go > >		
lotel PMS					
osted Files roxy Auto Discovery	Add Portal				

Creating a Portal Rule

You need to create a portal rule that directs client devices to the portal that you created in <u>Creating a Guest Portal</u>. 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 <u>Figure 47</u>.

Figure 47: Edit Rule Page

	Edit Rule								
Home									
Network Access Policy	Guests are directed to the specified portal if all the specified conditions are met.								
Policy Settings	Rule Name: Guest Access								
Sponsor Portal	Rule Description: Rule for guest access								
Guest Portals									
Portals Portal Rules Themes Payment Providers Hotel PMS Hosted Files Proxy Auto Discovery	Image: Incomparison Image: Incomparison								

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 <u>Figure 48</u>.
- 2. After successfully logging in, the option to download Smart Connect is provided. See <u>Figure 49</u>.
- 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 <u>Figure 51</u>. 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

iPad	12:38 PM	Not Charging 🖭
	Login to the network	Cancel
	NETWORKS Guest access Login to the network	
	Username:	
	Password:	
	Remember me on this device	
	Login	

© 2011-2013 Meru Networks. All Rights Reserved.

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
- <u>Creating a Custom Captive Portal for Web Authentication</u>

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
17 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7
I Serial-COM1
Switch(config)#ip admission name CP proxy http Switch(config)#interface gigabitEthernet 0/5 Switch(config)fj#exit Switch(config)#ip device tracking Switch(config)# aaa new-model Switch(config)# aaa nutherlication login default group radius Switch(config)# aaa autherlication auth-proxy default group radius Switch(config)# aaa autherlication auth-proxy default group radius Switch(config)# radius source-interface Vlan1 Switch(config)# radius-server host 172.18.33.245 Switch(config)# radius-server key secret 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#

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 <u>Figure 55</u>, 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

~

.

Meru Identity Manager	Administration	
	RADIUS Clients	
Home	Client Attributes SNMP MAC Auther	ntication RadSec Authentication
Network Access Policy		
Policy Settings	Name:	Cisco-3560
Sponsor Portal	Device IP Address / Prefix Length:	172.18.33.248
Guest Portals		For example 192.168.1.1/32 or fec0:0001/128
Smart Connect	Secret:	Confirm:
Devices	Type:	Cisco Switch
RADIUS Clients Email Settings	Form Action:	https://1.1.1.1/
SMS Settings	Description:	
Syslog Monitoring		
Svslog Servers		
-,;	Change-of-Authorization	
	Use COA:	
	Port: 3799	
	Save Cancel	

Figure 55: RADIUS Client Attributes Tab

Meru Identity Manager Administration											
	RADIUS Clients										
Home	RADIUS Client saved.										
Network Access Policy	ient Attributes SNMP MAC Authentication BadSec Authentication										
Policy Settings											
Sponsor Portal	Vendor: IETF										
Guest Portals	Attribute: Access-Loop-Encapsulation										
Smart Connect	Value:										
Devices RADIUS Clients Email Settings SMS Settings Syslog Monitoring LDAP Server Syslog Servers	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
- <u>Configuring the Switch to Permit Traffic to Identity Manager</u>
- Copying the Custom Captive Portal Pages to the Switch
- <u>Registering Custom Captive Portal Pages</u>
- 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

MERU Identity Manager Administration Portals Home Showing 1-4 of 4 10 per page • Go Network Access Policy Description Name Policy Settings Q 💣 🖺 😫 access-denied Default portal that denies access Sponsor Portal Q 💣 🖺 🖳 🗑 login Default login portal **Guest Portals** Q 🔊 🗞 🖳 🕅 mobile Default portal for mobile device Portals Q 🛷 🖺 🔣 🔟 🔒 Login to the Portal Rules je 1 of 1 💌 Go 🕨 🕅 Themes Payment Providers Hotel PMS мекц Hosted Files ORKS Proxy Auto Discovery © 2011 Mere Networks, All Rights Revenued Smart Connect Devices

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.htmlSuccess page: flash:/portalpages/success.htmlFail 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

C Login to the network - Windows Internet Explorer				
🕞 🕞 🔻 💋 https://tme-idm:8443/portal/172.18.33.248/?redirect_url=http://cnr	.com/		🔽 😵 Certificate Error 😽	🗙 🦧 Live Search
File Edit View Favorites Tools Help				
🖕 Favorites 🛛 👍 🛄 httpimsports.rediff.com-sc 🔁 Suggested Sites 🔹 🔊 W	eb Slice Gallery 🔻 🙋 Free Hotmail	💛 "tme-idm" the Identity Manage	er host name	
🔠 🔹 🏠 Identity Manager Administrat 🚮 Identity Manager 🥖 Los	in to the network X			🟠 🔹 🔝 👘 🖃 🍓 🔹 Page 🖬 Safety
X Find: default Previous Next	🖉 Options 👻			
	Username Passwort	ETWORKS* to the network		
	© 2011 You Netw	Login		
🖉 Authentication successful - Windows Internet Explorer				
C C F thtps://tme-idm/portal/login/172.18.33.248/success			💙 😵 Certificate Error	😽 🗙 🥂 Live Search
File Edit View Favorites Tools Help				
Yevonites Yevonites	ul uthentication successful X			🏠 • 🔊 - 🗆 👼 • Page •
	Authentication successful, you Your account will expire in:38 E	AT A CONNECTED OF A C		
	© 2011. Meru Network	s All Rights Reserved		

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 <u>Controller Configuration Tasks</u>.
- Create authorization profiles for personal and corporate devices. See <u>Creating</u> <u>Authorization Profiles</u>.
- Create authorization policies for personal and corporate devices. See <u>Creating</u>
 <u>Authorization Policies</u>.
- Create device accounts for personal and corporate devices. See <u>Creating Device</u> <u>Accounts</u>.

Controller Configuration Tasks

- <u>Creating QoS and Firewall Rules</u>
- 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 <u>Figure 59</u>. You can also create firewall policies for bandwidth throttling for users.

Figure 59: QoS and Firewall Rules Page

WLAN Management MC	1550-\	/E 6.0	-83									admin@172.22.	.34.6 level:15	6 4:45:04 P	M <u>WebTerm</u>	Save Logout	Help MCRU
Monitor	QoS and Firewall Rules (10 entries)																
Maintenance		Global	l Qual	itv-of-Service F	Parameters	QoS and Firewall F	Rules Q	oS Codec Rules									
▶ Wizards																	
Mac Filtering A Wapi Server			ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	Qo S Protocol	Action	Qos Rule Logging	Qos Rule Logging
VPN Client VPN Server	LC.		1	0.0.0.0	0.0.0.0	1720	0.0.0	0.0.0.0	0	6		0	0	H.323	CAPTURE	Off	60
Rogue APs Wired			2	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
VLAN GRE			3	0.0.0.0	0.0.0.0	5060	0.0.0	0.0.0.0	0	17		0	0	SIP	CAPTURE	Off	60
Ethernet Port		1	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
Wireless Radio		-	7	0.0.0.0	0.0.0.0	5200	0.0.0	0.0.0.0	0	17		0	0	other	FORWARD	Off	60
Mesh		1	8	0.0.0	0.0.0.0	0	0.0.0	0.0.0.0	5200	17		0	0	other	FORWARD	Off	60
Hotspot	1	/	20	172.22.32.8	255.255.255.255	5 443	0.0.0	0.0.0.0	0	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
QoS Settings Devices		1	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
System Settings Controller		/	30	0.0.0.0	0.0.0	0	0.0.0	0.0.0.0	0	1	corp	0	0	none	DROP	Off	60
APs Antennas		/	31	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
Redirect DHCP SNMP Certificates																	

Creating a Security Profile

You need to create a security profile that dynamically assigns filter IDs using RADIUS, as shown in <u>Figure 60</u>.

Figure 60: Security Profile Page

WLAN Management MC15	50-VE 6.0-83	
Monitor	Static WEP Key Index	Valid range: [1-4]
Maintenance	Re-Key Period (seconds)	0 Valid range: [0-85535]
▶ Wizards	BKSA Caching Period (seconds)	0 Valid range: [0-85536]
▼ Configuration	Captive Portal	Disabled 💌
System Config	Captive Portal Authentication Method	internal 💌
Quick Start Security	802.1X Network Initiation	On 💌
Profile	Tunnel Termination	PEAP TTLS
Captive Portal	Shared Key Authentication	Off 🚽
Guest Users	Pre-shared Key (Alphanumerio/Hexadecimal)	
Wapi Server E	Group Keying Interval (seconds)	0 Valid range: [0-85535]
VPN Client	PMK Caching	On 💌
Rogue APs	Key Rotation	Disabled 👻
Wired VLAN	Backend Auth Server Timeout	30 Valid range: [1-85535]
GRE	Reauthentication	On 💌
Port	MAC Filtering	Off 💌
Wireless Radio	Firewall Capability	radius-configured
ESS	Firewall Filter ID	Enter 0-16 chars.
Hotspot	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 <u>Figure 59</u>.

Figure 61: Creating Authorization Profiles

MCRU Identity Manager Administration	
Authorization Profiles	
Home	
Network Access Policy Showing 1-S of 5 10 per page Go Authentication Policy Name ▲ ▼ Description ▲ ▼ Description ▲ ▼ Authorization Policy Corp Devices Rule for Corp devices W Authorization Profiles Default Default Default authorization profile W Personal devices Rule for Personal Devices W W W	
Authorization Profiles: Corp Devices	Authorization Profiles: Personal devices
RADIUS Attributes Locations Authentication Settings Notification Settings NAC Roles	RADIUS Attributes Locations Authentication Settings Notification Settings NAC Roles
Vendor: IETF Attribute: Access-Loop-Encapsulation Value: Add AV Pair Filter-Id = corp Remove Move down	Vendor: IETF Attribute: Access-Loop-Encapsulation Value: Add AV Pair Filter-Id = pers Move up Move down
Save Cancel	Save Cancel

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

Meru I	dentity Manager	Administration	admin user	Logout	About
	RADIUS Authoriz	ation Rule Wizard			
Home Network Acce	✓Welcome	Rule Conditions			
Authentication Authorization	✓Details	All the conditions below must be met for this rule to match.			
Authorization P	🚖 Conditions	If <u>Calling-Station-Id</u> is a member of device role Personal devices			
	Assign Policy	Add Condition			
Policy Setting					
Sponsor Port					
Smart Conne		_			
Devices			: Back Ne	xt >]•	Exit

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

	Create Device Account							
😤 Home		_						
Getting Started My Settings	MAC Address:	Multiple	Device Accounts	5				
Lo Create Accounts	First Name:				Browse	Import	Download	Templat
Create Guest Account	Last Name:		MAC Addross	First Name	Lact Na		Company	Count
Multiple Guest Accounts	Company:	-	MAC Address	First Name	Last Na	ime	company	Count
Create Device Account Multiple Device Accounts	Email Address:							+1
🔧 Account Management	Mobile Phone Number: +1 V	-						
Report & Manage Guests	Device Role: Default 👻							
Report & Manage Devices	Timezone: Default							
Manage Device Batches	Corp Devices							
Summary Reports	Account Start:							
Sponsors Activity Report Access Report	10 🗸 13 🗸							
Connected Guests Report	1 🗸 Mar 🖌 2012 🗸 🛅							
	Account End:							
		Devic	e Role: Default	~				
	Add Device Cancel	Timor	Default		~			
		rimez	Corp De	al devices				
		Acces	I V	Mar 💙 2012 💙 觉				
		Accor	10 🛩	13 🛩				
				Max 10 2012 10 PM				
		Accou	Int End:	mar Y 2012 Y 10				
			23 🗸	59 🗸				

Note

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 <u>Figure 64</u>.)





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 <u>Figure 67</u> and <u>Figure 68</u>.)
- 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

WLAN Management MC1550-	-VE 6.0-83	
Monitor	WEP Key (Alphanumerio/Hexadecimal)	
Maintenance	Static WEP Key Index	1 Valid range: [1-4]
▶ Wizards	Re-Key Period (seconds)	0 Valid range: [0-85535]
System Config	BKSA Caching Period (seconds)	0 Valid range: [0-65535]
	Captive Portal	WebAuth 🗨
Profile	Captive Portal Authentication Method	external 💌
Captive Portal	802.1X Network Initiation	Off
Guest Users	Tunnel Termination	
Mac Filtering	Charad Kay Authoritization	
VPN Client	Shared Key Authentication	
VPN Server	Pre-shared Key (Alphanumeric/Hexadecimal)	
Rogue APs	Group Keying Interval (seconds)	0 Valid range: [0-65535]
Wired 🗄		
VLAN	PMK Caching	Off
GRE	Key Rotation	Disabled 👻
Ethernet		
Wireless	Backend Auth Server Timeout	30 Valid range: [1-65535]
Radio	Reauthentication	Off 🖃
ESS	MAC Eiltering	0#
Mesh	WAG Pittering	
Hotspot	Firewall Capability	radius-configured 💌
ServiceControl	Eirewall Eilter ID	Enter 0-18 chars
QoS Settings	, new all this to	Enter 0-10 chars.
Devices System Settings	Security Logging	Off 💌
Controller	Passthrough Firewall Filter ID	IDMPREAUTH Enter 0-16 chars
APs		
Antennas 👻		
ALARMS 🗛 🗛 🗛	ROGUE 🔓 💼 ACCESS POIL	NTS 🟝 🔤 STATIONS 💻 🖥 🚱 ESS

Figure 67: Configuring QoS Rules

WLAN Management MC1	550-VE 6.0-83		
Monitor	Destination Port	0 Valid range: [0-65535]	
Maintenance			
▶ Wizards	Source IP	0.0.0.0	
System Config Quick Start	Source Netmask	0.0.0.0	\smile
Security Profile	Source Port	0 Valid range: [0-65535]	
Captive Portal Guest Users			
Mac Filtering Wapi Server	Network Protocol	0 Valid range: [0-255]	
VPN Client VPN Server	Firewall Filter ID	Bronzeplan2Mbps Enter 0-16 chars.	
Rogue APs Wired E	Packet minimum length	0 Valid range: [0-1500]	
Ethernet Port	Packet maximum length	0 Valid range: [0-1500]	
Wireless Radio ESS	QoS Protocol Average Packet Rate	0 Valid range: [0-200]	
Mesh Hotspot	Action	2.000 Kbps Mbps Valid rank	De:
QoS Settings	Priority	[1-64]	
System Settings Controller	Traffic Control		
Antennas -			
ALARMS 🗛 🗛 👍	ROGUE Zo Zo	ACCESS POINTS 🚋 🚈 STATIONS 💻	10 20

Figure 68: QoS Rules Specifying Different Token Bucket Rates

WLAN Management MC:	1550-\	VE 6.0	-83								a	admin@172.22	.34.6 level:15	2:24:52 P	M <u>WebTerm</u>	Save Logout	Heb MCRU
Monitor	Q	oS an	d Fir	ewall Rules	; (11 entries)												
Maintenance		Globa	Quali	ity-of-Service P	arameters Qo	S and Firewall R	ules Qo	S Codec Rules									
Wizards																	
System Config Quick Start			ID	Destination IP	Destination Netmask	Destination Port	Source IP	Source Netmask	Source Port	Network Protocol	Firewall Filter ID	Packet minimum length	Packet maximum length	Qo S Protocol	Action	Qos Rule Logging	Qos Rule Logging Frequency
Security Profile			1	0.0.0	0.0.0.0	1720	0.0.0	0.0.0.0	0	6		0	0	H.323	CAPTURE	Off	60
Radius Captive Portal			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
Guest Users Mac Filtering			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
Wapi Server VPN Client			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
VPN Server		-	7	0.0.0.0	0.0.0.0	5200	0.0.0	0.0.0.0	0	17		0	0	other	FORWARD	Off	60
Wired E			8	0.0.0.0	0.0.0.0	0	0.0.0	0.0.0.0	5200	17		0	0	other	FORWARD	Off	60
GRE Ethernet		/	20	172.22.32.8	255.255.255.255	443	0.0.0	0.0.0.0	0	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
Port			21	0.0.0	0.0.0	0	172.22.32.8	255.255.255.255	443	6	IDMPREAUTH	0	0	other	FORWARD	Off	60
Wireless Radio	IΓ		100	0.0.0	0.0.0.0	0	0.0.0.0	0.0.0	0	0	Bronzeplan2Mbps	0	0	none	FORWARD	Off	60
ESS Mesh			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
Hotspot ServiceControl		/	300	0.0.0	0.0.0.0	0	0.0.0	0.0.0.0	0	0	Goldplan7Mbps	0	0	none	FORWARD	Off	60
QoS Settings Devices System Settings																	

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 <u>Identity Manager Deployment Guide</u>.

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

- Creating Authorization Profiles
- Adding Payment Provider Accounts
- <u>Creating a Portal for Login and Credit Card Billing</u>
- Previewing the Portal

Creating Authorization Profiles

You use authorization profiles to define network access for users. For the network scenario in <u>Figure 65</u>, 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 <u>Figure 69</u>.

Figure 69: Authorization Profiles Main Page

Meru Identity Manager	Administration	admin user Logout About A A A C C
	Authorization Profiles	
Home		
Network Access Policy	Showing 1-4 of 4 10 per page 🔽 Go	
Authentication Policy Authorization Policy Authorization Profiles	Name ▲▼ Description ▲▼ bronzeplan bronzeplan Default Default authorization profile goldplan goldplan silverplan silverplan Image: Arrow of the silverplan Image: Arrow of the silverplan Ardd Profile Image: Arrow of the silverplan	
Policy Settings		
Guest Portais		

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.

	Authorization Profiles: Secure Guest Access
Home	RADIUS Attributes Locations Authentication Settings Notification Settings Device Restrictions MAC Registration
Network Access Policy	
Authentication Policy	Vendor: IETF
Authorization Policy Authorization Profiles	Attribute: Filter-Id
1	Value:
	Add AV Pair
	Filter-Id = Bronzeplan2Mbps
	Move up
	Remove
	Move down
Policy Settings	
Sponsor Portal	Save Cancel

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

Adding Payment Provider Accounts

After creating authorization profiles, as described in <u>Creating Authorization Profiles</u>, 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

	anager Administration admin user Logout About A A A C
	Add New Payment Provider
Home	Account Details
Network Access Policy	
Policy Settings	Account Name: test account
Sponsor Portal	Account Description: test
Guest Portals	Payment Provider: Authorize.net
Portals Portal Rules	Operation Mode: Test Ihttps://test.authorize.net/gateway/transact.dll]
Themes	API Login: 6zz6m5N4Et
Hotel PMS	Transaction Key: 9V9wUv6Yd92t27t5
Hosted Files	
Proxy Auto Discovery	Available Cards Supported Cards
	MasterCard American Express Diners Club Discover Card En Route JCB Carte Blanche
	Save Cancel Test Connection

Figure 72: Payment Provider List

	Payment Provide	rs	
Home			
Network Access Policy	Shov	wing 1-1 of 1	10 per page 💌 🛛
Policy Settings	Name 🔺 🔻	Туре ▲▼	Description 🔺 🔻
Sponsor Portal	Test account	Authorize.net	test account
Guest Portals		🖌 🖣 Pag	e 1 of 1 💌 Go 🕨
Portals Portal Rules Themes Payment Providers	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 <u>Figure 65</u>. 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
- <u>Configuring Guest Account Options</u>
- Mapping the Payment Provider to the Portal
- <u>Configuring Access Plans for Credit Card Billing</u>
- <u>Configuring Guest User and Password Policies</u>

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 <u>Figure</u> <u>73</u>. Also select the **Enable Logout Button** check box.

Figure 73: Portal Pages Page

Specify which pages your portal should have enabled and at what stage they should be available.	rtal Pages		
Display-Lin menu Pre-Authentication Post-Authentication Login V Image: Post-Authentication Password Change Image: Post-Authentication Image: Post-Authentication Self Service Image: Post-Authentication Image: Post-Authentication Self Service Image: Post-Authentication Image: Post-Authentication Device Registration Image: Post-Authentication Image: Post-Authentication Successful Authentication Image: Post-Authentication Image: Post-Authentication Smart Connect Image: Post-Authentication Image: Post-Authentication Help Image: Post-Authentication Image: Post-Authentication Welcome Image: Post-Authentication Image: Post-Authentication	ecify which pages your por	tal should have enable	ed and at what stage t
Displayed in menu Pre-Authentication Post-Authentication Login V I Password Change I I Password Change I I Self Service I I Device Registration I I Credit Card Billing V I Successful Authentication V I Smart Connect I I PMS Billing I I Welcome I I			
Pre-Authentication Post-Authentication Login V Password Change Image: Comparison of the comparison	Page	Displaye	d in menu
Login V Password Change Image: Comparison of the system of th	raye	Pre-Authentication	Post-Authentication
Password Change Image: Comparison of the comparison of t	Login		
Self Service	Password Change		
Device Registration	Self Service		
Credit Card Billing V O Successful Authentication V Smart Connect O PMS Billing O Help O Welcome O Longout Options	Device Registration		
Successful Authentication	Credit Card Billing		
Smart Connect	Successful Authentication		
PMS Billing Company Co	Smart Connect		
Help Welcome Hogout Options	PMS Billing		
Velcome	Help		
Logout Options	Welcome		
	ogout Options		
	nable Logout Button:		
Enable Logout Button:	nable Logout Pop-up windo	w:	
Enable Logout Button: 🛛 🐨 📄			
Enable Logout Button: 🛛 😨			

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	Account Options		
✓ Portal Name	The following options define what should happen after an account either guest or device is created.		
 Portal Theme Portal Settings Portal Policy 	 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:Image: Compared to a c		
	Send account details by e-mail: 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 <u>Adding Payment Provider Accounts</u>, to the portal:

On the Select Payment Provider page, as shown in <u>Figure 75</u>, 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

Portal Setup Wizard	
✔ Welcome	Select Payment Provider
✔ Portal Name	The payment provider details are needed to allow your payment provider to perform credit card billing into your
✓ Portal Theme	Select an existing payment provider or enter the details for a new account.
🔺 Portal Settings	
Portal Policy	Payment Provider: Test account Test connection
L	<pre>< Back Next > Exit</pre>

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.

r							
Portal Setup Wizard							
Velcome	Access Plans						
✓ Portal Name	Manage the ac	Manage the access plans users accessing this portal will be able to select.					
✓ Portal Theme	Access plans a	Access plans allows you to define when and where the user will be allowed to access the network by selecting					
🔹 Portal Sottings	a Time Profile a this through Ci	and a Guest R redit Card or F	ole. You can MS billing.	also specify t	ne cost of purchasing a	an account if your p	ortal
Fortal Settings	_		_				
Portal Policy	Access Plans						
	Name	Description	Price	Time Profile	Authorization Profile	Used for	
	goldplan	goldplan	15.00 USD	1 Hour	goldplan	Credit Card Billing	Ŵ
	silverplan	silverplan	10.00 USD	1 Hour	silverplan	Credit Card Billing	Ŵ
	bronzeplan	bronzeplan	5.00 USD	1 Hour	bronzeplan	Credit Card Billing	Ŵ
	Use Access I	Plan for: Cred	lit Card Billing	, 💌			
	Name:						
	Description:						
	Time Profile:	Time Profile: To define Time Profiles go to Policy Settings -> Time Profiles					
	Authorizatior	Profile: Defa	ault 🔻 To	define Authoriz	ation Profiles go to Net	work Access Policy ->	Auth
	Price:	0.00	USD				
	Add						
h.							

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.

Portal Setup Wiza	rd
✓ Welcome	Guest Username Policy
 Portal Name Portal Theme Portal Settings Portal 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 Imail address as username
	Create Username With Case: lowercase Create username based on first and last names Create username based on first and last names Minimum username length: 10 Create Username With Case: Case entered by sponsor Create Username With Separator: None Create random username

Figure 77: Guest Username Policy Page

Figure 78: Guest Password Policy Page

Portal Setup Wizard	d
Velcome	Guest Password Policy
✔ Portal Name	By modifying the following options you can define which characters will be used when generating account passwords and how long the password should be.
✓ Portal Theme	Alphabetic Characters
✓ Portal Settings	Characters to include: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWX
🔺 Portal Policy	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
	Password case: Mixed
	Numeric Characters
	Characters to include: 0123456789
	Number to include: 2 💌
	Other Characters
	Characters to include: !\$^*()=+[]{};:@#~,.<>?
L	Number to include:

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 (\bigcirc) 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/	0.000	☆ #
MCRU NET Purchase you	N O R K S [®] raccount	
Login Purchase Account		
Card Holder Name		
Mobile number: +1		
E-mail address:		
Billing Address:		
Postal/ZIP code:		
Country: United State	s •	
Credit Card Number:		
Security Code:		
Issue Number:		
Expiration Date (month/year): 01 - / 20	13 •	
Access Plan: Bronzeplan	\$5.00 -	
Bronzeplan - Goldpian - S	\$5.00 Generate Account	
Zinterheit - 2	10.00	

Guest Portal Pages

Figure 80 shows the page that users see when accessing the guest portal.

Figure 80: Guest Login Page

Pad	4:28 PM	Not Charging 📖
	Login to the network https://172.22.32.5	
	Log In	Cancel
Login Pu	MERU NETWORKS Login to the network	•
	Username:	
	Password:	3
	© 2011-2012 Meru Networks, All Rights Reserv	ved.

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.

<u>Figure 82</u> shows an example of the page with account credentials that the user gets after the guest account is generated. <u>Figure 83</u> shows a successful authentication page a user sees after successfully logging in.

Figure 81: Self-Registering and Purchasing an Access Plan

iPad	5:55 PM Not Charging 🔳
	Login to the network https://172.22.32.5
	Log In Cancel
M	CRU NETWORKS® Purchase your account
Login Purchase Account	
	Children and Chi
Card Holder Name:	Susan
Mobile number:	+1 4085550000
E-mail address:	susan@example.com
Billing Address:	894 Ross Drive
Postal/ZIP code:	94089
Country:	United States
Credit Card Number:	00000000000000
Security Code:	
Issue Number:	
Expiration Date (month/year):	01 🗴 / 2015 🔨
Access Plan:	Goldplan - \$15.00

© 2011-2013 Meru Networks. All Rights Reserved.

Figure 82: Guest User Generated by the System

PT 2	4:34 PM	Not Charging
	Login to the network https://172.22.32.5	
	Log In	Cancel
	MERU NETWORKS Purchase your account	
Purchase Account	Successful Authentication	
The account crede The account crede	entials were sent to your phone, please use them to entials were sent to your e-mail, please use them to Username: susan@example.com	access the network. access the network.
	Password: Le3dJ8Kn	
	Password: Le3dJ8Kn	

© 2011-2012 Meru Networks. All Rights Reserved.
Figure 83: Successful User Authentication

iPad 穼	2:14 PM	Not Charging
	Authentication successful	Done
	MERU	
	NETWORKS"	
	Purchase Account Successful Authentication	
	Authentication successful, you are connected to the network.	
	Your account will expire in: 1 Hour(s) 0 Minute(s)	
	Logout	
	© 2011-2012 Meru Networks. All Rights Reserved.	

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

Filter:	radius		Expression C	ar Apply		
802.11	Channel:	Channel Offset:	FCS Filter: All Frames - Wire	nark 💌 Wireless	Settings Decryption Keys	
No. 99 99 99	Time 61 13:13:30.712417 72 13:13:30.910878 74 13:13:30.911731 79 13:13:30.931610	Source 172.22.35. 172.22.32. 172.22.32. 172.22.32.	Destination 5 172.22.32.5 5 172.22.35.6 5 172.22.35.6 5 172.22.35.6	Protocol Len RADIUS RADIUS RADIUS RADIUS	ngth Info 204 Access-Request(1) (id=59, l=162) 83 Access-Accept(2) (id=59, l=41) 255 Accounting-Request(4) (id=60, l=213) 62 Accounting-Response(5) (id=60, l=20)	
•					, III	
	ame 9901: 204 bytes hernet II, Src: Lar ternet Protocol Ver er Datagram Protocol Code: Access-Reques Packet identifier: Length: 162 Authenticator: 69fa [The response to tl Attribute Value Pai B AVP: 1=6 t=Servi B AVP: 1=6 t=Servi B AVP: 1=10 t=User B AVP: 1=10 t=User B AVP: 1=10 t=User	s on wire (1632 bits innerE1_14:06:80 (00): rsion 4, src: 172.22 bl, Src Port: 47356 st (1) 0x3b (59) mae3ac1c4f03e30c83ee <u>his request is in fr</u> irs ice-Type(6): Login(1 ed-MTU(12): 1250 Name(1): susan@exa PasSword(2): Encry biog eta rice td(21)	<pre>, 204 bytes captured (1 00:0b124:00:80), DST: He .35.6 (172.22.35.6), DST (47356), DST PORT: radiu 7954e5886 ame 99721) mple.com pred =0.65 pp.48 59.70</pre>	32 DT5) Hettp_60:34:1 172.22.32.5 (1812) 1 Erai 9972 1 Erai 9 Market 9 Market	00 (e4:11:5b:69:34:00) (172.22.32.5) 13:13:30.910878 172.22.32.5 172.22.35.6 RADIUS 83 Access-Accept(2) (id=59, I=41) me 9972: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) ernet Protocol version 4, Src: 172.22.32.5 (172.22.32.5), Dst: 172.22.35.6 r Datagram Protocol, Src Port: radius (1812), Dst Port: 47356 (47356) ius Protocol ode: Access-Accept (2) acket identifier: 0x3b (59) ength: 41 uthenticator: abff613ddc8b9433ee2666c2100b1559a This is a response to a request in frame 9961]	00:90:0b:14:d0:80) (172.22.35.6)
	AVP: 1=19 t=Call ∂ AVP: 1=19 t=Conr ∂ AVP: 1=6 t=NAS-F ∂ AVP: 1=6 t=NAS-F ∂ AVP: 1=6 t=NAS-F ∂ AVP: 1=18 t=Mess	led-Station-Id(30): nect-Info(77): CONNE IP-Address(4): 172.2 Port-Type(61): Wirel Port(5): 0 Sage-Authenticator(8	00-90-0B-14-D0-80 CT 802.11a/n 2.35.6 esss-802.11(19) D): 48c2b4ef2478a2163f89	[□ A ₩ □	Time from request: 0.198461000 seconds] ttribute value pairs AVP: <u>1=6 t=Session-Timeout(27): 3600</u> AVP: <u>1=15 t=Filter-Id(11): Goldplan7Mbps</u> Filter-Id: Goldplan7Mbps	

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

MERU NETWORKS* Login to the network	
Login	
Username: Password:	
Login	
© 2011-2012 Meru Networks. All Rights Reserved.	

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 <u>Figure 87</u>.

Figure 87: Theme Images Page

Portal Setup Wizard	đ
✔ Welcome	Theme Images
✓ Portal Name	The images will be used on the Portal.
\star Portal Theme	Supported file formats are JPG, GIF and PNG. Using larger images may result in the portal not looking as the theme intended.
Portal Settings Portal Policy	
	Header image:
	Apple iOS icon: It is recommended you use an image with 57x57 pixels.
I	Favicon: Favicon: It is recommended you use an image with 32x32 pixels:
	Background:
	Browse It is recommended you use an image with 1501x1125 pixels. < Back

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

Portal Setup Wizard	d	
✔ Welcome	Theme Colors	
V Portal Name	These are the main colors defined for the theme you selected, you can use the color picker controls to select alternative colors.	
🔺 Portal Theme	_	
Portal Settings	Body background color:	
Portal Policy	Font color:	
	Form element label font color:	
	Form element border color:	Ш
	Link font color:	
	Link font color on hover:	
	Menu item font color:	
	Menu item font color on hover:	
	Color of the horizontal separators:	
	Status message font color:	
	Error message font color:	+

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

Welcome Portal Pages Portal Name Specify which pages your portal should have enabled and at what stage to portal Theme Portal Settings Portal Settings Portal Policy Page Displayed in menu Post-Authentication Login Image: Compare the set of the set
Portal Name Portal Theme Portal Settings Portal Policy Page Page Page Displayed in menu Pre-Authentication Login Password Change Self Service Device Registration Credit Card Billing Successful Authentication
Portal Theme Specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify which pages your portal should have enabled and at what stage to specify the specify the specify and the specify the specif
Portal Settings Displayed in menu Page Displayed in menu Pre-Authentication Post-Authentication Login Image Password Change Image Self Service Image Device Registration Image Credit Card Billing Image Successful Authentication Image
Portal Policy Displayed in menu Page Pre-Authentication Post-Authentication Login Image: Comparison of the second s
Page Pre-Authentication Post-Authentication Login Image: Comparison of the comparison of t
LoginImage: Comparison of the sector of the sec
Password ChangeImage: ChangeSelf ServiceImage: ChangeDevice RegistrationImage: ChangeCredit Card BillingImage: ChangeSuccessful AuthenticationImage: Change
Self ServiceImage: ComparisonDevice RegistrationImage: ComparisonCredit Card BillingImage: ComparisonSuccessful AuthenticationImage: Comparison
Device Registration Image: Credit Card Billing Successful Authentication Image: Credit Card Billing
Credit Card Billing Successful Authentication
Successful Authentication
Smart Connect
PMS Billing

- 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

	For Guest Access Page			
Home	Close this window Page			ľ
Network Access Policy	Authenticating waiting page Page	Customise the content of	of the For Guest Access page	
Policy Settings	Session management page Page			
Sponsor Portal	For Guest Access Page	Page label:	For Guest Access	E
Guest Portals	Logged Out Page	Footer:	© 2011-2013 Example Networks,Inc. All Rights Reserved.	
Portals Portal Rules	Successful Authentication Page			
Themes	Acceptable Usage Policy Page	Hender		ŀ
Payment Providers	Logout Page	Header:	Welcome to the Example Networks guest network.	
Hosted Files	iOS auto login Page			
Proxy Auto Discovery	Cookies instructions Page	Main:		
	Widget Labels			
	Status Messages	Title:	Login to the network	
	Realm Labels			
	Windows Smart Connect			
Smart Connect	iOS Smart Connect			
Devices	iOS Auto Login Smart Connect	Save		

- 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

	Widget Labels		
Home	Close this window Page		
Network Access Policy	Authenticating waiting page Page	Default Phone Code:	+1 •
Policy Settings	Session management hage Page	Username:	Guest Name
Sponsor Portal		Password:	Passonde
Guest Portals	For Guest Access Page	1 dobitordi	Passoue
Portals	Logged Out Page	Remember me on this device:	Remember me on this device
Portal Rules	Successful Authentication Page	Realm:	Realm
Payment Providers	Acceptable Usage Policy Page	Login button:	Confirm
Hotel PMS	Logout Page	Days:	Days(s)
Hosted Files Proxy Auto Discovery	Widget Labels	Hours:	Hour(s)
	Status Messages	Minutes:	Minute(s)
	Realm Labels	Time left text:	Please wait while we check your account details:
	Windows Smart Connect	Time left calculating:	Computing
	iOS Smart Connect	Time left Unlimited account texts	
	iOS Auto Login Smart Connect	Time left offinitied account text.	Congratulations! You have an unlimited account.
Smart Connect	Mac Smart Connect	Try again:	Try again
Devices	Android Smart Connect	New password:	New Password
Reports & Logs	Linux Smart Connect	Old Password:	Password

7. Save the changes for the portal.

<u>Figure 86</u> shows the customized login page. <u>Figure 92</u> shows the customized initial successful authentication page, with the modified text that appears while the system checks the guest user account information. <u>Figure 93</u> 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 <u>Figure 95</u>. 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

Usin to the network - Mozilla Firefox	and the second s		
https://172.22.32.5/portal/Advanced_custom/preview/?show		 ☆ * ▽	
Login_	MERUNETWORKS* Healthcare Login to the network	—— New logo	
	Username: Password: Login I agree to the Terms and Conditions.		
	© 2011-2013 Meru Networks. All Rights Reserved.		
			image

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

Home		,	0032(2)
Network Access Policy	Logout Page	Hours:	Hour(s)
Policy Settings	Widget Labels	Minutes:	Minute(s)
Sponsor Portal	Status Messages	Time left text:	Your account will expire in:
Guest Portals	Realm Labels	Time left calculating:	Calculating
Portals	Windows Smart Connect	Time left Unlimited account text:	Your account is unlimited
Portal Rules	iOS Smart Connect		
Themes Payment Providers	iOS Auto Login Smart Connect	iry again:	I ry again
Hotel PMS	Mac Smart Connect	New password:	New Password
Hosted Files	Android Smart Connect	Old Password:	Password
Proxy Auto Discovery	Linux Smart Connect	Change password button:	Change Password
	Generic Smart Connect	Confirm new password:	Confirm New Password
	Approval Notification Email	Accept AUP button:	Accept
	Account Rejection Email	Reject AUP button:	Reject
	Account Rejection SMS	Access plan:	Access Plan
Smart Connect	"From Creation" Email	First name:	First name
Devices	"From Creation" SMS	Last name:	Last name
Reports & Logs	"From First Login" Email	Company:	Company

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

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.

MCRU Identity Mana	ger Administration		admin user Logout About A A A C	:
	Acceptable Usage Policy Page			
Home	Login Page			
Network Access Policy	Logged Out Page	Customise the content of	of the Acceptable Usage Policy page	
Policy Settings	Successful Authentication Page			
Sponsor Portal	Acceptable Usage Policy Page	Page label:	Acceptable Usage Policy	=
Guest Portals	Logout Page	Footer:	© 2011-2013 Meru Networks. All Rights Reserved.	
Portals Portal Rules	iOS auto login Page			
Themes	Cookies instructions Page	Header:	Accentable Lisage Policy	
Payment Providers Hotel PMS	Close this window Page			
Hosted Files	Authenticating waiting page Page			
Proxy Auto Discovery	Session management page Page	Main:	A service of the s	
	Widget Labels		agree to be bound by these Terms of Use, Disclaimer of Warranties, and Limitation of	
	Status Messages	Title:	Login to the network	
	Realm Labels			
	Windows Smart Connect			
Smart Connect	iOS Smart Connect	Save		
Devices	iOS Auto Login Smart Connect	0010		

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

	Themes		
Access Policy		Showing 1-7 of 7 10 per page	Go
ettings	Name	Description	
Portal	Access Denied	This theme only displays an access denied message. It is based on the Meru Networks white theme.	b 🗑
ortale	Identity Networks (Blue)	The default Identity Networks theme.	۵ 🛈
UTTAIS	Mobile Theme (All Devices)	This theme is for mobile devices.	L T
0.5	Identity Networks (white)	Theme based on the Identity Networks color scheme and logo	L T
	meru_healthcare(white)	Theme based on the Meru Networks color scheme and logo	L II
Providers	Meru Networks (white)	Theme based on the Meru Networks color scheme and logo	μÌŴ
	White Mobile Theme (All Devices)	This theme is for mobile devices.	L T
es			
o Discovery			
	Import Theme: E:\Arun\Service assur	rance collateral\IDM u Browse_	

10. Edit the Advanced_custom portal, and select the newly uploaded theme, as shown in Figure 99.

Figure 99: Selecting New Portal Theme

Portal Setup Wizard				
	٢		Description: The default Identity Networks theme.	^
	0	Hot S Hot No Hot No Antice An	Name: Mobile Theme (All Devices) Author: <i>Meru Networks</i> Description: This theme is for mobile devices.	
	۲		Name: meru_healthcare(white) Author: <i>Meru Networks</i> Description: Theme based on the Meru Networks color scheme and logo	m
			< Back Next > Exit	•

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

Portal Setup Wizard				
✔ Welcome	Portal Setup Complete			
✓ Portal Name	The wizard has finished building your portal.			
✓ Portal Theme	You can preview the portal at https://172.22.32.5/portal/Advanced_custom/preview/?show			
✓ Portal Settings	You should configure your network devices to redirect to the following URL:			
✓ Portal Policy	https://{IDENTITY_MANAGER}/portal/Advanced_custom/{DEVICE_IP}			
	Please replace {IDENTITY_MANAGER} with the fully qualified domain name of the Identity Manager and {DEVICE_IP} with the IP address of the network device (wireless controller, switch, firewall etc) you have added as a RADIUS client.			
	You must also ensure the following conditions are met:			
	1. The fully qualified domain name of the Identity Manager should be in DNS and resolvable by guest clients so they can reach the Identity Manager.			
	2. The SSL certificate CN should contain the fully qualified domain name of the Identity Manager and be signed by a trusted CA authority to ensure clients do not receive SSL warnings.			
	< Back Close			

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.)

Meru Networks | Copyright © 2013 Meru Networks, Inc. All rights reserved worldwide. Meru Networks is a registered trademark of Meru Networks. Inc. All other trademarks. trade names. or service marks mentioned in this document are the property of their respective owners.