MERU NETWORKS®

DATA SHEET

Meru Connect

Easy to use, flexible guest access. Simplified BYOD on-boarding and policy management.

For any user on any network with any device

With the increased pervasiveness and user reliance on mobile devices and a new wave of enterprise productivity applications, IT organizations are struggling to keep up with the life-cycle activities associated with on-boarding, policy, reporting across a variety of roles of users—guests (visitors), contractors or other temporary users (students), even employees. Managing expectations of seamless access and pre-provisioned security in the face of this deluge of devices with restricted resources and hard SLAs means some of the tasks need the end user's intervention, particularly for self-provisioning. However, with most non-technical work forces, straightforward automated workflows are essential for successful enablement.

Meru Connect (formerly known as Identity Manager) provides comprehensive answers to issues facing IT pertaining to role management, policy management and reporting across the BYOD life-cycle.

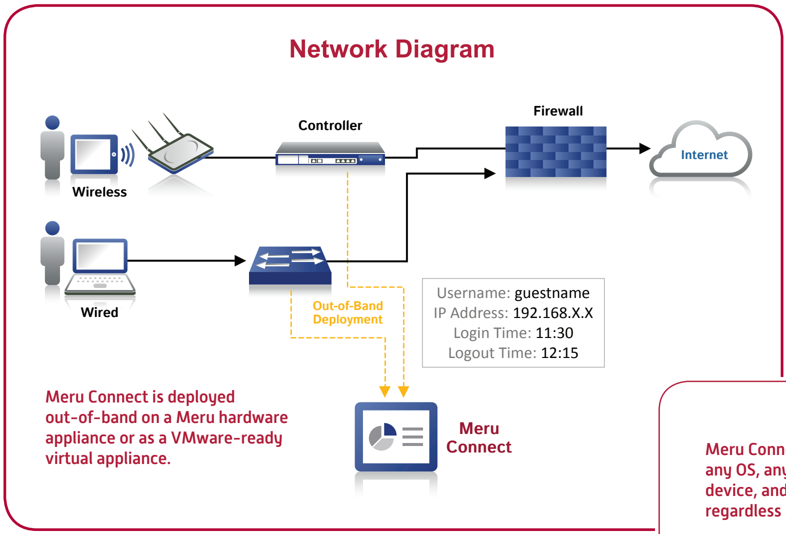
Packaged in a simple, wizard driven application, all facets of managing IT workload in deploying BYOD are addressed effectively:

- On-boarding devices for web and 802.1X authentications, abstracted across multiple OSs and devices (laptops, smart phones, tablets) with iOS, Android™, Microsoft® Windows®, Apple® MacOS X®, Linux®
- Wired and wireless network vendor-agnostic guest access, device on-boarding, policy and access management
- Role (guest, temporary user, employee) and device based policy management
- Integrated reporting and auditing
- Integration across vertical-specific applications (property management systems, payment gateways) for ease of deployment
- Retrieval and verification of identity and group based policies across multiple identity stores (LDAP, RADIUS, social networking identities, other databases)
- Integrated policy and reporting across specialized policy enforcement devices like firewalls
- Integration with leading MDM vendors to define policies based on device compliance
- Enterprise grade clustering for scalability and high-availability
- Tailored to run on Meru SA series appliances or virtualized environments running VMWare or Hyper-V hypervisors.

Meru Connect looks at a variety of device and role trust relationships to provide unique access across common scenarios found in enterprises, schools, universities, hotels and other common places of business. They can be summarized as follows:

USER ROLES	DEVICE TYPES	
	Corporate owned (trusted)	Employee Owned (untrusted)
Employee (trusted) (hotel managers, engineers, doctors, nurses, teachers, faculty)	Trusted access; Tightly controlled corporate identity server (AD, LDAP), Fully MDM controlled. Full access to resources allowed by role.	On-boarding required; restricted access based on policy, MDM registered. Possibly,restricted access to resources allowed by role.
Contractor (trusted) (consultants, temporary workers, vendors at event, students, conference staff)	Trusted access; Tightly controlled corporate identity server (AD, LDAP), Fully MDM controlled. Full access to resources allowed by role.	On-boarding required; restricted access based on policy, MDM registered. Possibly, restricted access to resources
Guest / Visitor (untrusted) (patients, ticketed audience, parents etc.)		Untrusted access – Self provisioning or sponsored guest access. Internet only access.

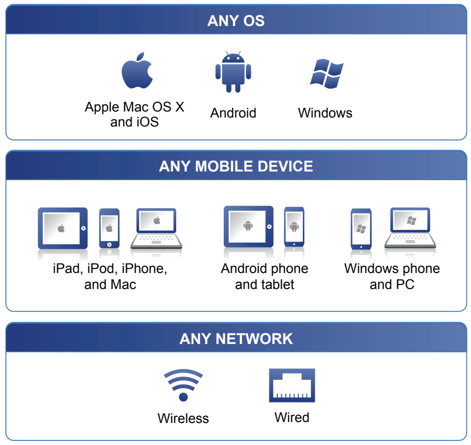
Meru Connect addresses the above scenarios via built in services to integrate guest(visitor) end-to-end access and to securely on-board employees with personal or corporate devices under policy management.



Username: guestname
IP Address: 192.168.X.X
Login Time: 11:30
Logout Time: 12:15

Meru Connect is deployed out-of-band on a Meru hardware appliance or as a VMware-ready virtual appliance.

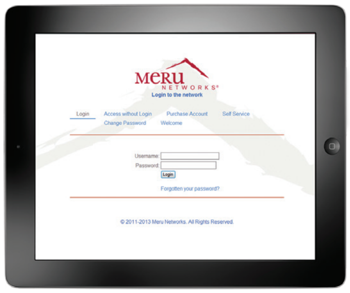
Meru Connect supports any OS, any mobile device, and any network – regardless of vendor.



Simplify guest access for any OS on any network

Introduction

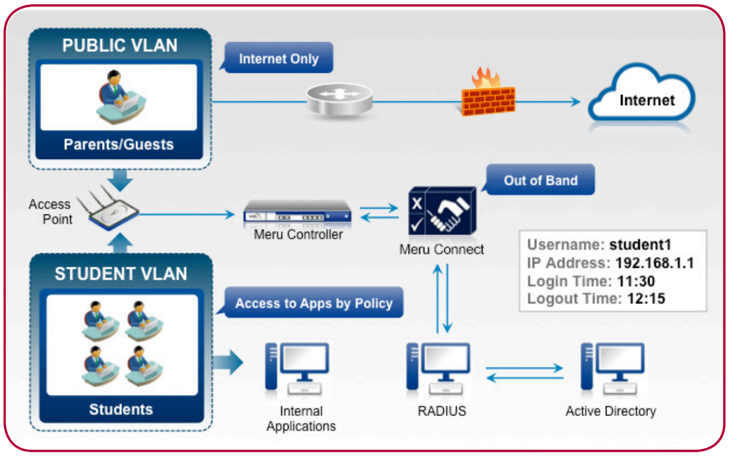
Guest access is no longer a nice-to-have feature in an enterprise. Wired and WLAN guest access is mandatory and web authentication due to its simplicity and ease of deployment has become the prevalent guest access mechanism. Guest access creates a strong brand presence and in some verticals, such as hospitality and event management, has direct revenue and customer satisfaction consequences. To address the myriad of guest access requirements associated with different businesses, the guest access service in Meru Connect provides administrators, sponsors and guests a full toolset of services to provision and manage guest accounts and their activity on the network with appropriate role-based policies.



© 2011-2013 Meru Networks. All Rights Reserved.

Guest access on Tablets

Meru Connect Walkthrough: Guest Access



Username: student1
IP Address: 192.168.1.1
Login Time: 11:30
Logout Time: 12:15

Meru Connect makes it easy to authorize internal sponsors to create guest accounts. You can also enable guests to securely self-provision.

Guest access offers both sponsor and self provisioned guest account creation. Multiple accounts can be easily created by uploading of account information into Meru Connect or bulk creating accounts with random usernames and passwords. Engaging IT staff for managing guest accounts is neither practical nor economic. In some cases such as hospitals or in event centers or arenas, handing this duty to non-IT staff such as security personnel or event coordinators is cumbersome and tedious. In the carpeted enterprise, particularly security conscious enterprises, however, sponsors (such as employees hosting meetings with guests) are required to invite guests and manage their accounts for full audit management. Account management functions – creation, updates, password changes, notifications, deletion and reports; are all customizable based on a variety of types of sponsors (self-sign, front desk at a hotel, front desk at a carpeted enterprise, security at a company etc.)

Brand presence management is catered to through the fully customizable, mobile-adaptable login portal and walled garden. Guest account notification can be managed through SMS, self-service kiosk or email creating a perfect user experience for the guest. Administrators can also provide a variety of portals for visitors logging into their networks based on their location, language as well as whether or not they are using a traditional laptop, smartphone or tablet. Meru Connect supports 35+ languages out of the box for customizing the guest and sponsor portal to every locale that the business caters to.

Of paramount concern with guest networks is the enforcement of appropriate policies for guest users. Administrator-defined individual, group, or general policies can have customized time-based access, usage based access, or location based access. Access to specific resources as well as bandwidth usage restrictions may be placed on the guest accounts as well.

One of the major complaints against guest access through a web portal is the need for guests to reenter their credentials after their devices “wake up” from the power-save induced (for saving on battery life) sleep mode. Meru Connect securely addresses this concern to reconnect without having to enter credentials and still be under the same policy guidelines that you set up for the guest profile. Guest access is optimized for ease-of-use, for both administrators and end users. It is client platform agnostic and supports any platform with a web browser, including iOS, Android™, Microsoft® Windows®, Apple® MacOS X®, Linux® and more.

Using social identity (Twitter or Facebook accounts) for network access is becoming a larger trend for unpaid access. This creates a win-win for the provider and the subscriber. Capturing the identity is a great marketing asset for service providers lead targeted marketing campaigns for the users and for users it provides exchanging your Facebook “likes” for unpaid access to the WiFi network. Businesses large and small are moving their IT services (email, file shares, archiving, identity services etc.) to the cloud to providers such as Google. Meru Connect integrates with Google Apps to authenticate users and guests to onboard them on the network with appropriate policies.

Meru Connect supports networking switches, APs (and controllers) from most major vendors. Such vendor agnostic interoperability means the ability to leverage your existing investments.

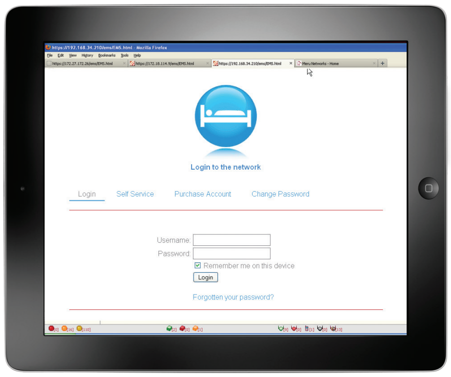
BUSINESS SYSTEMS INTEGRATION

Businesses have existing authentication, billing and network infrastructure. Meru Connect integrates with these business systems seamlessly to avoid duplication of data, maximize appropriate use of these resources and provide a single view into reporting and policies associated with the usage.

HOSPITALITY

In a traditional hospitality setting at a hotel, lodge, or resort, guest access is often considered a value add for individual customers. Integration with existing property management systems makes the guest experience seamless – hotel guests can gain access to the wireless network using their room number and name and if it is a paid service, charge it to the room. Due to integration with a variety of leading PMS (Property Management Systems), centralized billing and account management is easy through Meru Connect using either front desk provisioning or self-registration. Guests with valid accounts can get online as soon as they are in range of the wireless network without entering their credentials to have a better guest experience.

Guest access provides the ability to not only address all of these situations but also provide tiered access. For example, provide free internet access for a short duration of time, based on the user sharing their Facebook account name vs. providing a higher bandwidth account on a paid service.


https://192.168.34.210/ems/EMS.html - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://172.27.172.26/ems/EMS.html
https://172.18.114.9/ems/EMS.html
https://192.168.34.210/ems/EMS.html
Meru Networks - Home
Login to the network
Login
Self Service
Purchase Account
Change Password
Username:
Password:
☑ Remember me on this device
Login
Forgotten your password?
[0] [16] [110]
[2] [0] [1]
[9] [0] [1] [0] [13]

Tiered services (e.g. paid vs. free network services, or higher bandwidth vs. restricted bandwidth network services) may also be provided by checking on a guest account's "status" against a loyalty program. Authentications can be performed not only against a local database but also against other databases such as standards-based SQL or RADIUS or LDAP identity stores.

Meru Connect supports a wide variety of transport-related scenarios as well, such as wireless network services for cruise ships, buses, trains and airplanes. Passengers can readily gain access to the wireless network using their transportation ticket information or pay for it using a variety of payment processing systems. Other options include charging to a loyalty program, cruise ship cabin room, etc. Transportation staff can gain access to additional network, business system & IT resources based on their assigned roles and privileges.

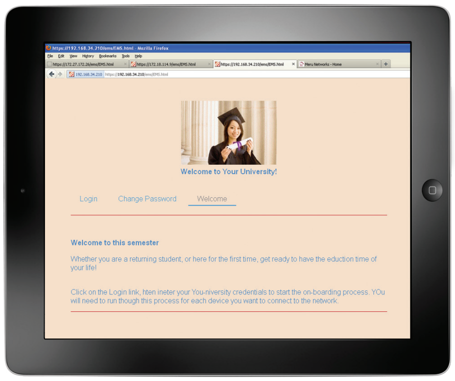
For conventions and conferences, hotels, or convention centers typically want to associate a specific event with an event code to track the users and associate policy based on the tiered service they offer. Meru Connect provides a simple and efficient means for such cases.

Arenas, stadiums, and other public spaces require a different set of access means. While most of these are public spaces, the access to the network could be one of:

- A simple click-though acknowledging the terms of use
- Providing some information (email address or mobile phone number) to subscribe to the network
- Logging on to the network using social media credentials such as your Facebook or Twitter account
- Paid service using credit card or PayPal based payment for network access. A full PCI report is available through the Meru Connect interface for all credit card based transactions.

EDUCATION

The eduroam initiative allows secure, worldwide roaming access for the research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop. Meru Connect supports eduroam for authentication of visiting faculty, students and scholars.


https://192.168.34.210/ems/EMS.html - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://172.27.172.26/ems/EMS.html
https://172.18.114.9/ems/EMS.html
https://192.168.34.210/ems/EMS.html
Meru Networks - Home
192.168.34.210 https://192.168.34.210/ems/EMS.html
Welcome to Your University!
Login
Change Password
Welcome

Welcome to this semester

Whether you are a returning student, or here for the first time, get ready to have the eduction time of your life!

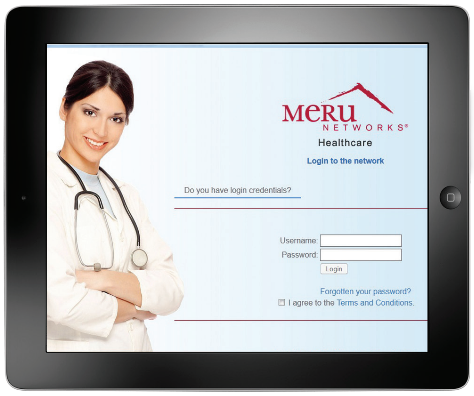
Click on the Login link, hten ineter your You-niversity credentials to start the on-boarding process. YOu will need to run though this process for each device you want to connect to the network.

Guest access for parent-teacher meetings, homecoming or other special events can be easily arranged using dedicated per-user self-registration or open access along with policy management across both wired and wireless networks. Bulk users can be created by importing a list of visitors or creating random usernames and passwords.

Guest access, through security policies set by the enterprise or through government regulations, requires tracking and maintaining audit information regarding the guest account from its creation, activation, usage (including details on what websites / applications were accessed) through its expiry and deletion or reactivation in the system.

Guest access provides integrated, exportable reports at both the administrator as well as the sponsor level. Auditing reports are generated by correlating user information across network infrastructure against the account information in Meru Connect.

HEALTHCARE



Healthcare

Login to the network

Do you have login credentials?

Username:

Password:

Login

Forgotten your password?

☐ I agree to the Terms and Conditions.

With the growing demand for better care for patient and their guests in healthcare institutions outside of medical treatment, providing WiFi access has become a norm. However, with legitimate security and bandwidth management concerns, providing reliable, auditable and self-serviced or free internet access is possible with Meru Connect.

Guest access combines the ability to self-service the guest user creation process via its highly customizable web portal. It also allows the administrator to automatically provision and enforce a preset bandwidth and/or data limit to each individual guest so as to keep the network available for other more mission critical usage. For longer duration guests, devices and usernames can be remembered using a "remember me" feature to make the user experience better while still keeping the network secure. Customization of portals and creation of a sophisticated walled garden provides the ability to provide additional information to visitors as well as manage the branding and marketing for the institute. Guest access portals are available in 30+ languages out of the box and with little customization can be used for a variety of patients from different ethnicities to make them feel at home and comfortable.

Features & benefits

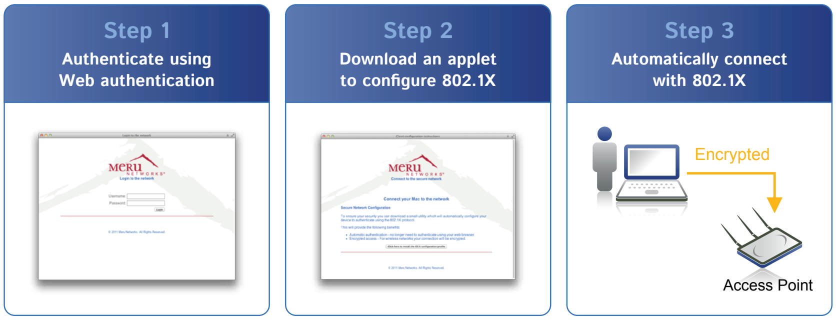
- Automated wireless/wired guest management - optimized for ease-of-use
- Seamless integration with multi-vendor network infrastructure and client platforms
- Fully customizable guest portal
- Comprehensive activity monitoring and reporting
- Simplifies secure guest access to dramatically reduce IT workload
- Supports existing infrastructure and visitor devices
- Promotes your brand and ensures an outstanding end-user experience on any client
- Restricts guest access to authorized users only
- Ensures appropriate use and supports audit requirements

SIMPLIFY BYOD PROVISIONING FOR ANY OS ON ANY NETWORK

Meru Connect also provides employees and other trusted users a way to on-board their trusted and untrusted devices on the secure network. It provides the administrator with flexibility to decide on the correct level of policy for the untrusted devices being brought onto the network by the trusted user.

On-boarding refers to auto-provisioning of corporate- or employee-owned devices to use the secure (typically 802.1X authenticated) networks. This could be true of wireless or wired infrastructures.

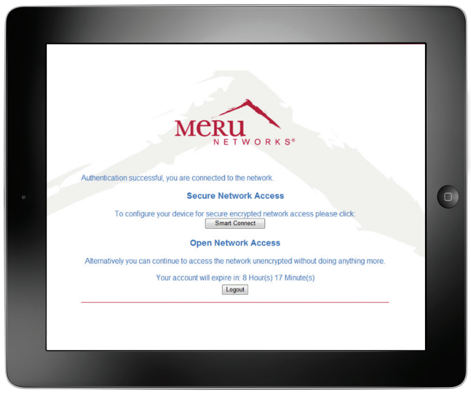
Meru Connect Walkthrough: Smart Access


Step 1
Authenticate using Web authentication
Step 2
Download an applet to configure 802.1X
Step 3
Automatically connect with 802.1X
Encrypted
Access Point

Meru Connect provides a set sequence of events for non-technical employees and contractors to setup their devices with appropriate 802.1X settings for accessing the wired or wireless network. A standard web portal (different from the secure network) is initially presented for the user to enter their corporate credentials. Once a device connects, its type is detected; the credentials verified against a backend device and based on the administrator's configuration appropriate secure network access settings are downloaded to the device. The device is then disconnected from the web portal network and reconnected to the secure network using the new secure settings. All of the steps are done without the need for a client agent residing on the device thus providing ease of deployment and scale. This workflow is very intuitive for the end users and removes their dependence on IT to onboard their devices. Also, from an IT perspective, since the settings are done centrally, policies can be set effectively and uniformly based on both the user role, device role, and the device type.

Policy is managed using user roles from the corporate identity server (AD or RADIUS etc.) as configured into the secure profile. The device policy is added to this to provide a complete view for that session. Meru Connect also integrates with leading MDM vendors to create a unique layered policy management framework to enhance the native user and device based policy with inputs from the MDM server. Using a dynamic authorization mechanism, the session attributes may be changed anytime based on inputs and behavior of the session on the network.

In schools, the beginning of a semester or school year is the busiest time. With new students coming to school new devices need to be on- boarded. Using Smart access capability drastically reduces IT time, complexity and training and reduces errors both from a misconfiguration as well as policy management perspective saving time and resources to troubleshoot and rework client devices. With the introduction of new devices every year, rather than having a new release covering on-boarding, Smart access provides a unique capability to just update the support for the supported devices automatically.



Authentication successful, you are connected to the network.

Secure Network Access

To configure your device for secure encrypted network access please click:

Open Network Access

Alternatively you can continue to access the network unencrypted without doing anything more.

Your account will expire in: 8 Hour(s) 17 Minute(s)

Secure Network Access using Smart acesss

Healthcare demands flexibility for doctors and caregivers to bring their own devices but regulations and privacy policies mandate severe restrictions on data being shared or stored on these devices. Meru Connect meets this challenge two fold – user and device role-based policy access, and applications that the user can access. Based on the device the user is accessing the network with, even if the user is a trusted user, Meru Connect can distinguish the untrusted device and not allow access to the network. However for a trusted device and user, full network access can be granted. Also, based on whether the device is registered with the MDM system and in compliance with application policies, Meru Connect can change the necessary privileges on the fly based on input from the MDM systems.

Device authentication and policy management can also be done using Smart access for devices such as printers, connected hospital equipment (Infusion pumps, heart monitors, blood pressure monitors etc.) and other devices that need to be authenticated before being let onto the network. This is especially true of devices that are temporary or short-term leased and do not warrant being managed in the corporate identity servers.

Meru Connect seamlessly integrates mobile and traditional laptop platforms including Windows, Linux, MAC OS, iOS and Android operating systems for on-boarding purposes. It also supports setting up supplicants for a variety of secure 802.1X protocols including PEAP-MSCHAPv2, PEAP-GTC, EAP-TLS as well as non-802.1X authentication mechanisms PAP and CHAP.

Features & benefits

- Seamless integration with multi-vendor network infrastructure and client platforms
- Policy and role-based provisioning of wireless/wired network access
- Optimized for ease-of-use for both IT staff and end users
- Enterprise-strength authentication and encryption
- Simplifies device onboarding
- Dramatically reduces IT workload
- Supports existing infrastructure and employee devices
- Protects the network and sensitive data
- Enterprise-strength 802.IX authentication

Features	Benefits
Fully integrated platform for policy- and role-based provisioning of wireless/wired network access	Simplifies secure guest access and BYOD
Fully integrated platform for policy- and role-based provisioning of wireless/wired network access	Simplifies secure guest access and BYOD
Seamless integration with multi-vendor network infrastructure and client platforms	Supports existing infrastructure and employee/visitor devices
Enterprise-strength authentication and encryption	Protects the network and sensitive data
Comprehensive activity monitoring and reporting	Ensures appropriate use and supports audit requirements

Technical Specifications

HARDWARE APPLIANCE PLATFORMS

SA250 Services Appliance
SA2000 Services Appliance

PLATFORMS:

- SA200 Services Appliance supports up to 500 active users
- SA2000 Services Appliance supports up to 10,000 active users
- VIrtual Appliance supports up to 50,000 active users (with appropriate hardware)

Virtual Appliance System Requirements:

– Minimum hardware specifications: 1GB memory, 20GB disk space, 2.0GHz CPU
– VMware support:
– ESX 3.5
– ESX 3.5i
– ESX 4.x
– ESX 4.xi
– ESX 5.xi
– Workstation 5.0 or later
– Server 1.0 or later
– Fusion 2.0 or later

- Microsoft Hyper-V on Windows 2008 and later

CLIENT PLATFORMS SUPPORTED:

- Android 2.1 and greater
- Apple iOS (iPhone/iPad) 2.0 and greater
- Apple Mac OSX 10.7
- Windows 7, Vista, XP SP3
- Linux Ubuntu

AUTHENTICATION:

- Active Directory
- LDAP
- RADIUS / RadSec
- Kerberos
- Facebook
- Twitter
- Google Apps
- SQL Database

PROTOCOLS SUPPORTED:

- 802.1X PEAP-GTC
- PEAP-MSCHAPv2
- PEAP-TTLS WPA
- WPA-PSK WPA2
- WPA2-PSK

BROWSERS SUPPORTED:

- IE 7.0 and higher
- Safari
- Chrome
- Firefox

SKUS:

Meru Connect

MCT-100-U
Includes licenses for up to 100
guest and smart access users

MCT-1000-U
Includes licenses for up to 1,000 guest and
smart access users

MCT-10000-U
Includes licenses for up to 10,000 guest and
smart access users

MCT-ESL-U
One year enterprise license support

Support and virtual appliance or hardware
appliance quoted separately

Meru delivers an all-wireless network that fully supports the enterprise, delivering a consistent, interactive experience for all users. No matter what applications they are running. No matter how many other users are on the network. For more information, visit **www.merunetworks.com** or email your questions to: meruinfo@merunetworks.com.

Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089

T +1 (408) 215-5300
F +1 (408) 215-5301

E meruinfo@merunetworks.com