

Enabling High-Performance for
Apple iPads in the Enterprise

Table of Contents

iPad Unleashed in Your Enterprise	3
Challenges of Deploying iPad in the Enterprise	3
Aruba Delivers Scalable Performance in a High Density Network	4
With Aruba, iPads Integrate Easily into the Enterprise WLAN	5
Aruba Delivers Strong Security	5
Ensuring Seamless Mobility for iPad in the Enterprise	6
Aruba's IP Mobility to Support Layer 3 Roaming for Apple Clients	7
Validate PMKID Should be Enabled for All Apple Clients	7
Maximizing the Battery Life of iPad	7
Move iPad Ahead in Your Business	8
Appendix: iPad Setup and Security Configurations	8
Open Network	8
Configuring Static-WEP, WPA (2)-PSK AES and TKIP or Mixed Mode	9
Configuring WPA AES or TKIP, WPA2 AES or TKIP with PEAP-MSCHAPv2	10
Configuring WPA2-AES EAP-TLS to Terminate on an Aruba Controller	11
About Aruba Networks, Inc.	18

iPad Unleashed in Your Enterprise

Apple iPad is more than a great way to experience the web, photos and videos. The #1 reason U.S. consumers would use a tablet device such as Apple iPad is working on the go, according to a recent Zogby International poll.

People are demanding mobile devices that blend consumer and enterprise functionality. Information workers – and their employers – are seeing the clear value of iPad for work-related activities. More than half of Fortune 500 companies bought iPads in the first few months of their availability. It won't take long before a smart phone and an iPad are many workers' constant companions, leaving the hefty laptop grounded.

A leading luxury car maker is piloting the use of iPads. Salespeople can grab the latest details on a car and run credit checks from the showroom floor. A premier U.S. bank is using iPads to approve multi-million wire transfers. Medical professionals use iPads to view patients' medical images, health records and access key medical applications. IT managers use iPads to remotely manage and monitor business-critical systems from anywhere. And without a doubt, universities are filled with students and professions using iPads as an integral part of everyday learning – and life.

Enterprise IT organizations need to prepare for the wave of iPads, iPhones and other mobile devices arriving on the shores of the corporate wireless network. The mobile enterprise is indisputably here, and the pace of enterprise adoption will only accelerate. Laptops outsell desktops. Smart phones are everywhere. Forty-three percent of enterprise workers use wireless networks, according to Gartner, and that number is expected to rise to 58 percent by 2014.



Challenges of Deploying iPad in the Enterprise

Choosing a wireless LAN (WLAN) solution that will meet the needs of mobile users for the next decade is critical. With mobile devices fast becoming must-haves for business, IT must ensure that their WLAN infrastructure is ready to meet new demands for performance, integration, scalability, security and mobility – at the lowest total cost of ownership.

There are five key challenges in an enterprise deployment of iPads:

1. **Scalable performance:** Wi-Fi performance is particularly important for iPad because Wi-Fi is the only way to connect. There is no wired Ethernet port to fall back on if WLAN performance is unsatisfying. Designing a high-density wireless LAN means taking into account that the performance implications of having many iPads, tablets, smart phones and other Wi-Fi clients in a small area.
2. **Ease of integration:** iPads use 802.11n technology, and IT needs to ensure that these high-performance devices will not adversely affect the performance of clients using legacy Wi-Fi technology. To maximize its benefits, iPad performance needs to be guaranteed in the presence of legacy Wi-Fi technology. Appropriate measures should be taken to prevent performance degradation on the existing set of wireless devices and applications, and overall network performance.
3. **Strong security.** How does enterprise IT ensure that iPad users have convenient access – while ensuring that sensitive corporate data is protected? iPad was designed for the consumer, but IT must ensure that it can mitigate the risk of data loss or network compromise to meet growing set of compliance requirements.
4. **Mobility with ease:** Users expect seamless mobility when using iPad or any other mobile device. IT must ensure that users can move across the campus without breaking their connection so that productivity will be unimpeded.
5. **Maximizing battery life:** iPad gets about six hours (in practice) to ten hours (in theory) of battery life. IT must ensure that network infrastructure is designed to improve the available battery life on iPads to improve end user experience and productivity.

Thousands of organizations around the world have deployed Aruba's products to meet their campus wireless LAN, branch networking and remote networking needs. Aruba Networks meets the five biggest challenges of deploying iPads into an enterprise-class environment. To verify, Aruba performed extensive testing of iPad on Aruba wireless LANs to verify enterprise-scale performance, integration, security, mobility, and battery life. In all cases, iPad passed with flying colors. We tested iPad connectivity in an Aruba network using a lab network that consisted of one Aruba Mobility Controller 651-9 and two Aruba AP-105s. We used the Aruba corporate network in our Sunnyvale, CA headquarters to test connectivity, performance, security, roaming and usability.

Aruba Delivers Scalable Performance in a High Density Network

When it comes to supporting high density of iPads in the enterprise, organizations can count on the Aruba WLAN.

Aruba's Adaptive Radio Management (ARM) takes the guesswork out of RF management by using automatic, infrastructure-based controls to maximize client performance and enhance the stability and predictability of the entire Wi-Fi network.

Key ARM features include:

- Band steering actively guides faster 802.11a/n clients, including Apple iPad, to the best available wireless channel in the 802.11 5GHz frequency band. The result is better immunity from noise, fewer sources of interference, and more available channels – and ultimately better network performance for end-user applications.
- Spectrum load balancing dynamically shifts Wi-Fi clients to available 802.11 channels instead of individual access point radios. This technique helps prevent degraded network performance due to oversubscription of 802.11 channels.
- Co-channel interference mitigation across all access points and wireless clients that share the same 802.11 channel overcomes the challenges of densely populated deployments, such as lecture halls, airport lounges and conference centers.
- Airtime fairness gives equal opportunity for all Wi-Fi clients to transmit and receive when they are associated to the same access point radio, which is essential for dense client deployments.

With Aruba, organizations can be confident that their enterprise WLAN will deliver scalable performance, even in dense Wi-Fi client deployments that are typical of iPads. Users can continue to use their favorite applications while they move around the corporate campus or building for the vast majority of the workday.

Aruba WLAN makes it easier to deliver a consistent and positive experience for users of a wide variety of smart mobile devices.

The results of Aruba's extensive performance and operations tests for iPads are shown in Table 1. The band steering test results are particularly interesting. In our extensive testing, iPad connected to the 5-GHz band 10 out of 10 times when Aruba ARM band steering was enabled, which demonstrates that band steering improves network performance. When Aruba ARM band steering was disabled, iPad connected seven to five times to the 2.4-GHz band, which shows the unpredictable performance for iPad, depending on the time and place of network connectivity. Latest ArubaOS software release is recommended for best performance of Apple iPad platform within an Aruba WLAN.

Connectivity and Performance	
802.11n connectivity with WPA2-AES	Pass
Range vs. Performance	Pass
Band Steering	Pass
Band Steering with stronger signal on 2.4-GHz	Pass
Roaming with Band Steering	Pass
Roaming with Spectrum Load Balancing	Pass
Performance testing with Air Time Fairness	Pass
Roaming from 5-GHz to 2.4-GHz and back	Pass

Table 1

IT can use the Aruba spectrum analyzer to gain visibility into the RF environment and identify non-802.11 sources of RF interference and their subsequent effects on WLAN performance. The Aruba spectrum analyzer uses Aruba access points to scan the spectral composition of 2.4-GHz and 5-GHz radio bands to identify RF interference, classify its source and provide real-time analysis at the point of the problem.

The resulting data is used to isolate packet transmission problems, over-the-air QoS and traffic congestion caused by RF contention with other devices operating in the same band or channel. When used in conjunction with ARM's infrastructure-based controls, iPad and other Wi-Fi client behavior is optimized automatically and access points stay clear of interference.

With Aruba, iPads Integrate Easily into the Enterprise WLAN

Apple iPad and the applications running on it should not adversely affect the existing set of enterprise devices and applications. IT administrators need to have the necessary tools to make sure that only the required set of applications are enabled on Apple iPad, based on end user demand.

For instance, Aruba WLAN implements application-aware traffic filtering to further improve overall network performance by removing unnecessary multicast and broadcast traffic from the Wi-Fi network. Such traffic utilizes low 802.11 data rates, which requires more transmission time over the air. Removal of this traffic significantly improves channel availability. Aruba's application-aware quality of service (QoS) allows you to ensure the performance of key business applications and limit recreational applications on the network.

After determining that there aren't any critical business applications that must use broadcast or multicast, you can use the Aruba Drop Multicast and Broadcast Traffic feature to limit or drop traffic. This limit can be applied to the SSID, which affects the entire network, or to a specific user role or a specific application, which provides fine-grained control over which clients can't send what type of broadcast and multicast traffic. For instance, IT administrators can limit access to Bonjour and iTunes on Apple iPad by blocking port 5353 and port 3689.

Another example is performance protection enabled by Aruba's ARM technology. This prevents performance of higher-speed clients (e.g., 802.11n-capable such as Apple iPad) from being adversely affected by the presence of slower 802.11a/b/g clients. In turn, it also guarantees 802.11 channel availability for legacy 802.11a/b/g clients in the presence of high density of 802.11n clients associated to same access point radio.

Aruba Delivers Strong Security

Aruba's solutions are tailored to meet today's exacting regulatory compliance requirements. Aruba's security measures include identity-based access control, stateful firewall, wireless intrusion detection and logging. These security measures help organizations mitigate risk in a simpler, most cost-effective way.

Both Aruba WLAN and Apple iPad support IEEE 802.1X for end-user and device authentication and Wi-Fi Protected Access WPA2 with Advanced Encryption Standard (AES) for data encryption. Use of WPA2-AES allows the use of 802.11n data rates during wireless client to Aruba AP communication.

Aruba's identity-based security enhances your organization's security posture by eliminating excess privilege on the network while providing identity-based auditing of activity. You can use Aruba's role-based access control to assign roles to users and devices based on their authentication. The role, which is enforced by the firewall policy, can be defined on the basis of user identity, device identity via authentication credentials, device type and other factors.

You can give iPads and other Wi-Fi clients a unique role with access to network resources that are appropriate to your organization's security policy. Roaming employees can have a simple, uniform way to access the network from wherever they are. Guests can be restricted in accordance with IT policies. IT does not need any special VLANs, IP subnets, external firewall ACL configuration, or external network access control appliance configuration to enable role-based policy enforcement for Apple iPads within the Aruba WLAN.

Aruba's stateful firewall enforces security and access policies. The firewall tracks upper-layer flows and ensures that unauthorized traffic cannot bypass access control. Policy violations can be acted upon to deny traffic, quarantine devices or remove devices from the network via a blacklist. Aruba's firewall is certified by ICSA Labs, the industry-recognized benchmark for firewalls.

Aruba's integrated wireless intrusion detection and prevention (WIDS) system reduces deployment and management costs by using access points to simultaneously serve clients and contain wireless threats. With Aruba, there's no need for a costly overlay IDS with dedicated sensors. Automatic threat mitigation protects the network from unauthorized clients and ad hoc devices even as they roam. The IT organization can customize the security policies by criteria such as location, device or configuration. Integrated wireless security within Aruba WLAN ensures increased channel availability hence increased network performance for wireless devices, including Apple iPad.

Table 2 shows the results of Aruba's authentication and encryption testing for iPads.

Authentication and Encryption	Pass/Fail
Open	Pass
WPA2-AES PEAP-MSCHAPv2 (Termination)	Pass
WPA2-AES EAP-TLS (Termination)	Pass
WPA2-AES PEAP-MSCHAPv2 (External Radius)	Pass
WPA2-AES EAP-TLS (External Radius)	Pass
Static-WEP	Pass
Dynamic-WEP	Pass
WPA-AES	Pass
WPA-TKIP	Pass
WPA-PSK-AES	Pass
WPA-PSK-TKIP	Pass
WPA2-TKIP	Pass
WPA2-PSK-AES	Pass
WPA2-PSK-TKIP	Pass
Mixed operational modes (WPA-TKIP and WPA2-AES)	Pass

Table 2

Ensuring Seamless Mobility for iPad in the Enterprise

iPad users are free to move about the Aruba wireless network. Aruba supports fast, seamless roaming across both a single IP domain as well as across multiple IP domains. Clients can move from AP to AP in less than 50 milliseconds while keeping the same IP address. Fast roaming maintains a continuous application connection, which is critical for latency-sensitive applications such as voice and video.

We tested iPad roaming on the production network at Aruba corporate headquarters – a typical corporate office with cubicles, walls, furniture and people. As in any real-world configuration, iPads shared the air and network with other wireless clients, including as laptops, wireless VoIP phones and security cameras.

We used applications, including Skype, YouTube, iTunes and iSIP voice over IP, that require constant, high-quality network availability while moving around the building. This movement forced iPad to roam between APs about every 1 to 1.5 minutes. While on the move, we continuously monitored the quality of the application experience using status indicators. We also took note of any disruptions or decline in the service quality. During our tests, no applications experienced any decline in quality while roaming.

Aruba’s IP Mobility to Support Layer 3 Roaming for Apple Clients

To support Layer 3 roaming for iPad and other Apple clients, IP mobility must be enabled on the Aruba Mobility Controller. Otherwise, an Apple client will not renew its IP address when moving from an AP on one subnet to an AP on another subnet. Since the Apple client retains its original IP address, network connectivity will fail and will not recover automatically.

Aruba Layer 3 IP mobility allows a client that is moving between AP subnets to retain its original IP address, which addresses the connectivity issue. When IP mobility is configured, the client keeps the same IP address as it moves between AP subnet A and subnet B. Without IP mobility enabled, the client must get a different IP as it travels from AP subnet A to subnet B.

Table 3 shows the results of Aruba’s roaming tests with iPad.

Roaming	
Layer 2: Intra-controller VLAN Mobility	Pass
Layer 3: Inter-controller IP Mobility	Pass

Table 3

Validate PMKID Should be Enabled for All Apple Clients

Opportunistic key caching (OKC), also called proactive key caching, can be used to restore latency and overhead in the authentication process when roaming between APs. iPad, however, does not support OKC. Instead, Pairwise Master Key ID (PMKID) is used to facilitate fast, secure roaming.

With validate PKMID enabled, the AP will check if the client supports OKC. If the client doesn’t support OKC (which iPad does not), the AP will start the authentication process in the absence of the PMKID.

Maximizing the Battery Life of iPad

Users can increase the battery life of iPad and other dual-mode handsets by three to five times by taking advantage of several Aruba capabilities. Aruba supports a full network-side implementation of Wi-Fi Multimedia Power Save (WMM Power Save), a Wi-Fi Alliance certification based on IEEE 802.11e Unscheduled Automatic Power Save Delivery (U- APSD).

Aruba WLAN implements proxy ARP where the ARP request for a wireless client IP address is answered by the Aruba infrastructure. This prevents the need for wireless clients, including Apple iPad, to “wake up” and process the ARP request, hence conserving battery life. Multicast and broadcast filtering further helps clean the air from traffic that requires processing by all wireless clients.

Aruba WLAN does not require any special end-user software to improve wireless device battery life, uses a standards-based approach and is agnostic to the wireless device type.

Table 4 shows the results of iPad hibernate and reboot tests.

Hibernate and Reboot	
Sleep and awake at the same AP	Pass
Sleep and awake at different APs	Pass
No effect when battery-operated	Pass
Reboot client	Pass
Reboot AP	Pass
Reboot Controller	Pass

Table 4

Move iPad Ahead in Your Business

In today's hyper-competitive, always-on world, few businesses can afford to have their workers unconnected and off the grid. The iPad allows people to work on the go, and enterprise adoption will be swift. To support the iPad in your enterprise, Aruba WLANs deliver scalable performance for all Wi-Fi clients, deliver strong security, permit cross-IP mobility with ease and conserve the battery life iPads and other wireless clients. To learn more about best practices regarding Aruba WLANs, please see Aruba's Validated Reference Design (VRD) documentation at http://www.arubanetworks.com/technology/design_guides.php.

Appendix: iPad Setup and Security Configurations

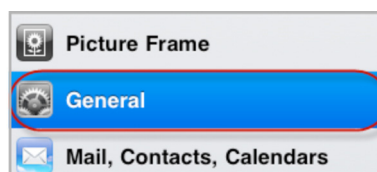
You can configure these simple, visual steps to configure iPad for an Aruba network.

Open network

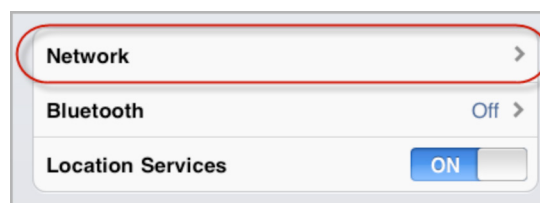
Select Settings on iPad Desktop.



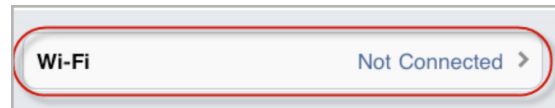
Select General.



Select Network on the right hand side of the screen.



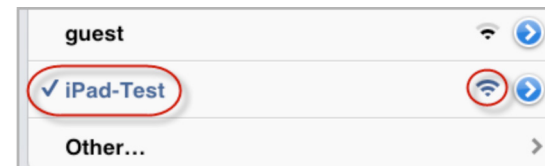
Select Wi-Fi.



Select the network SSID to which iPad should connect. The spinning wheel next to the wireless symbol indicates that iPad is connecting to the network. In the example, iPad is initiating a connection to iPad-Test network.



When you see a checkmark in front of the network name and the wireless symbol changes color to blue, you know iPad has successfully connected to the wireless network.

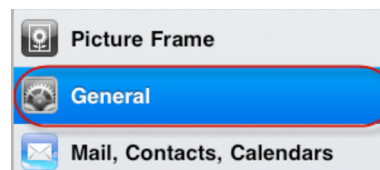


Configuring Static-WEP, WPA (2)-PSK AES and TKIP or Mixed Mode

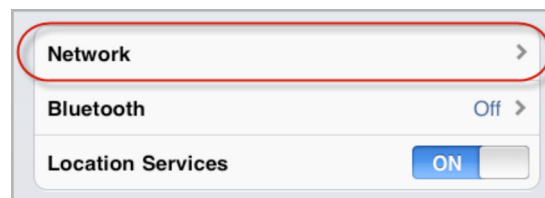
Select Settings on iPad Desktop.



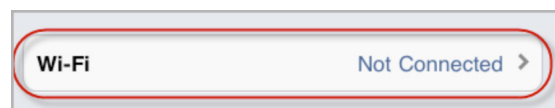
Select General.



Select Network on the right hand side of the screen.



Select Wi-Fi.



Select the network SSID to which iPad should connect. The spinning wheel next to the wireless symbol indicates that iPad is connecting to the network. In the example, iPad is initiating a connection to iPad-Test network.



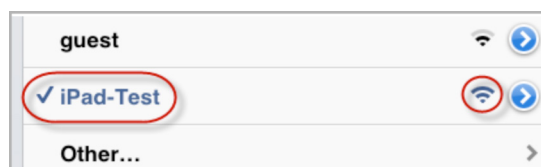
Enter the WEP key into the Password field.



Select Join.



When you see a checkmark in front of the network name and the wireless symbol change color to blue, you know iPad successfully connected to the wireless network.

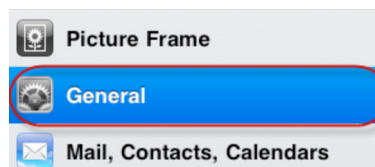


Configuring WPA AES or TKIP, WPA2 AES or TKIP with PEAP-MSCHAPv2

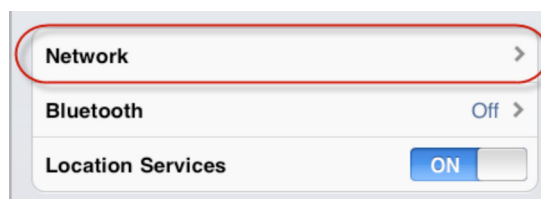
On iPad Desktop select Settings.



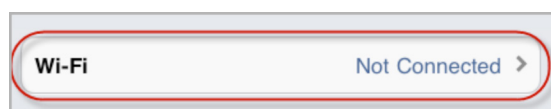
Select General.



On the right side select Network.



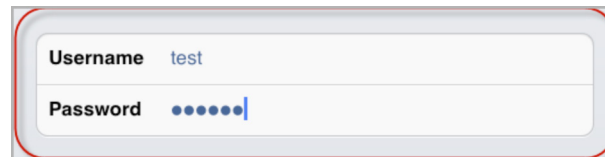
Select Wi-Fi.



Select the network SSID to which iPad should connect. The spinning wheel next to the wireless symbol indicates that iPad is in the process of connecting to the network. In this example, iPad is initiating a connection to iPad test network.



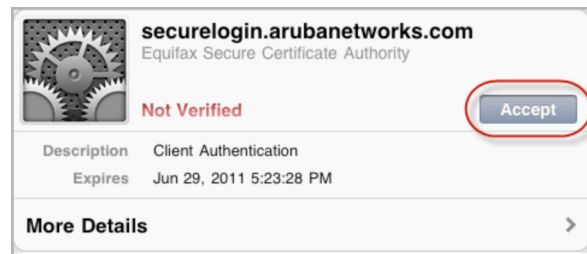
Enter your username and password.



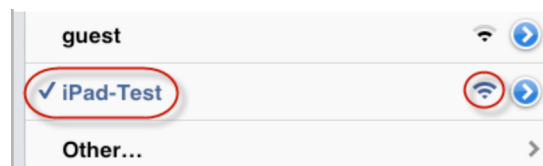
Select Join.



Click on Accept to continue to connect to the wireless network.



When you see a checkmark in front of the network name and the wireless symbol change color to blue iPad successfully connected to the wireless network.



Configuring WPA2-AES EAP-TLS to Terminate on an Aruba Controller

To configure and deploy EAP-TLS with iPad, you must download and install the Apple iPhone Configuration Utility. You can download the utility from these links:

For Windows: <http://support.apple.com/kb/dl926>

For Mac OS: <http://support.apple.com/kb/DL851>

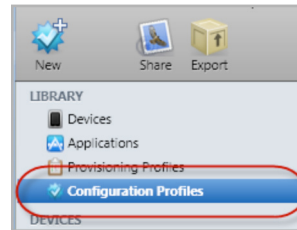
Once you install iPad configuration utility, configure iPad for EAP-TLS.

These instructions assume that you have access to your organization's root and personal certificates, which are needed for authentication. The root certificate and client certificate must be installed on the computer you are using to configure iPad with the iPhone Configuration Utility.

Connect your iPad to your PC.

Open iPad configuration Utility.

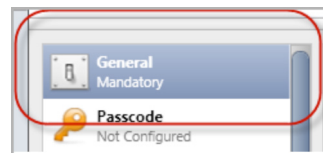
Select Configuration Profiles.



Click on New.



Select General in the center column.



Fill in the fields in the form on the right side.

Identity

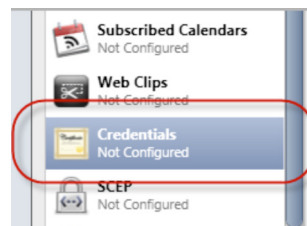
Name
Display name of the profile (shown on the device)
EAP-TLS

Identifier
Unique identifier for the profile (e.g. com.company.profile)
iPad-Test

Organization
Name of the organization for the profile
TME

Description
Brief explanation of the contents or purpose of the profile
EAP-TLS Profile

Select Credentials in the center console.



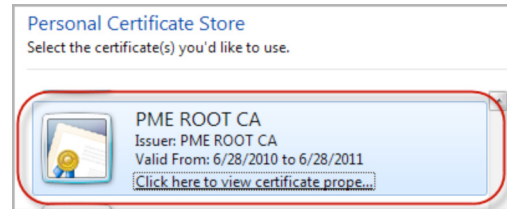
Select Configure.

Configure Credentials

Use this section to specify the PKCS1 and PKCS12 certificates you want to install on the device. Add your corporate certificate, and other certificates necessary to authenticate the device's access to your network. For more information about certificates, refer to the iPhone OS Enterprise Deployment Guide.

Configure

In the certificate dialog window, select your organization's root certificate and click OK.

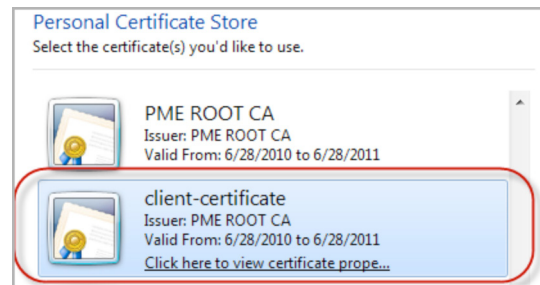


In the iPhone configuration utility, click on the + in the upper right corner to add the Client Certificate needed for authentication.



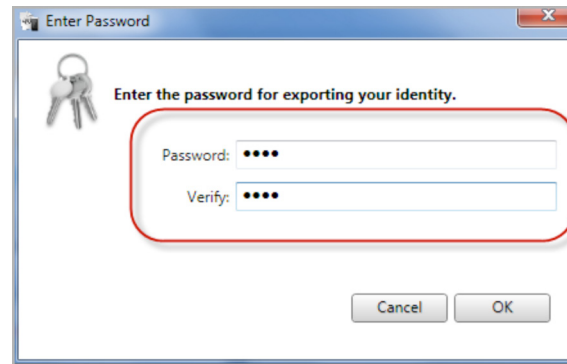
In the certificate dialog window, select your client certificate and click OK.

If your client certificate is password-protected for export, the iPhone Configuration Utility will prompt you to enter this password. You will have to contact your organization's IT department for the password.



Enter the password for the client certificate export and click OK.

You should see two Certificates in the iPhone Configuration Utility. The first certificate is your organization's Root certificate and the second is the Client certificate, which is used for authentication.



Select Wi-Fi in the center column.



Click on Configure on the right side.



Type the Network Name (SSID) into the Service Set Identifier field and select WPA / WPA2 Enterprise from the Security Type dropdown menu.

Wi-Fi

Service Set Identifier
Identification of the wireless network to connect to
iPad-Test

☐ **Hidden Network**
Enable if the target network is not open or broadcasting

Security Type
Wireless network encryption to use when connecting

- None
- WEP
- WPA / WPA2
- Any (Personal)
- WEP Enterprise
- WPA / WPA2 Enterprise**
- Any (Enterprise)

Select TLS for Accepted EAP Types.

Enterprise Settings
Configuration of protocols, authentication, and trust

Protocols Authentication Trust

Accepted EAP Types
Authentication protocols supported on target network

☒ TLS ☐ LEAP ☐ EAP-FAST
☐ TTLS ☐ PEAP ☐ EAP-SIM

EAP-FAST

Click on Authentication and select the client certificate from the Identity Certificate dropdown menu.

Enterprise Settings
Configuration of protocols, authentication, and trust

Protocols **Authentication** Trust

Username
Username for connection to wireless network

☐ **Use Per-connection Password**
Request during connection and send with authentication

Identity Certificate
Credentials for connection to wireless network

client-certificate

Outer Identity
Externally visible identification (for TTLS, PEAP, and EAP-FAST)

Click on Trust and select your CA certificate.

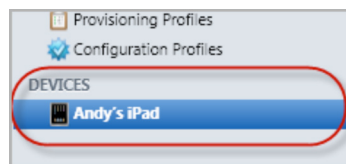
Enterprise Settings
Configuration of protocols, authentication, and trust

Protocols Authentication Trust

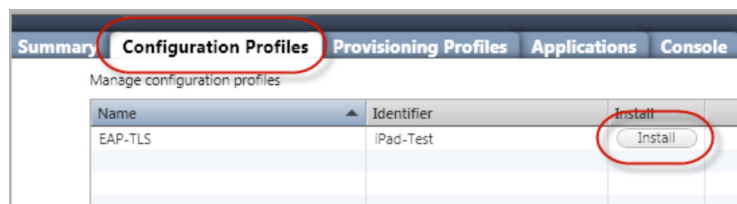
Trusted Certificates
Certificates trusted/expected for authentication

☒ PME-SRV-CA

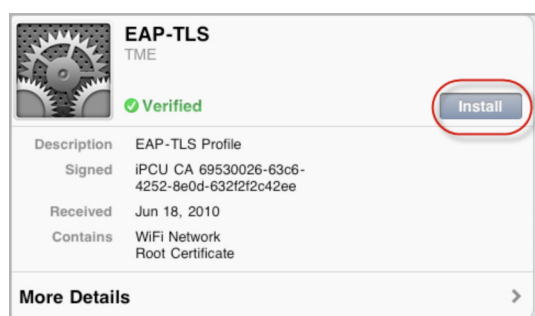
Select your iPad on the left side.



Select the Configuration Profiles tab on the right side and select Install for the EAP-TLS profile you just created.



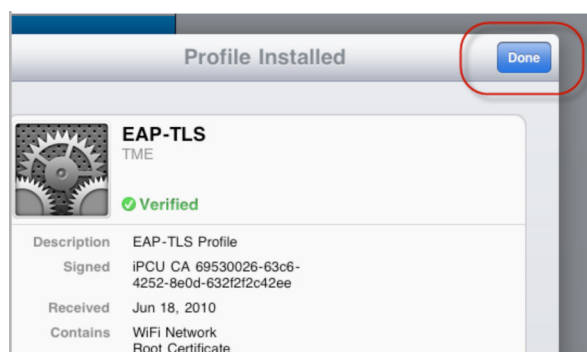
When prompted on iPad, select Install to continue.



Select Install Now to continue.



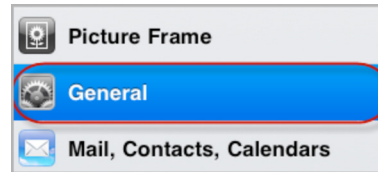
Select Done to finish the installation.



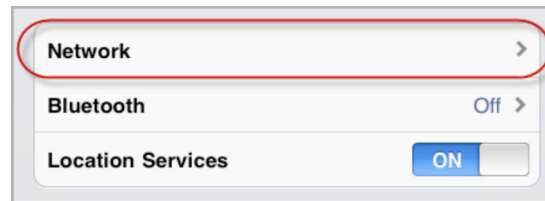
On iPad Desktop select Settings.



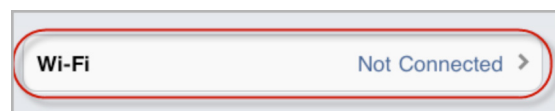
Select General.



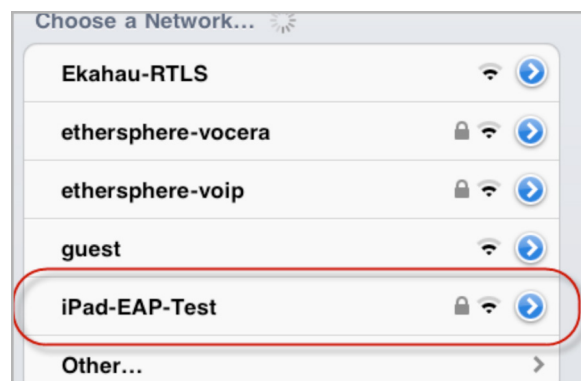
Select Network on the right side.



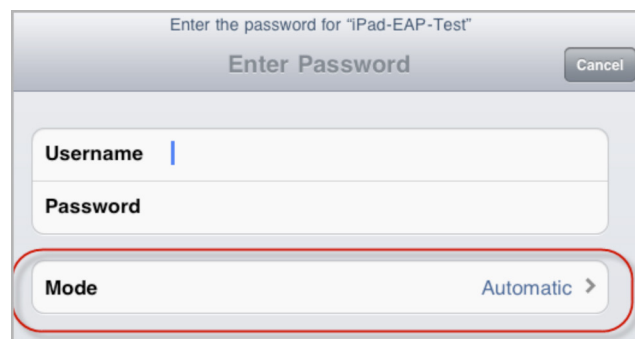
Select Wi-Fi.



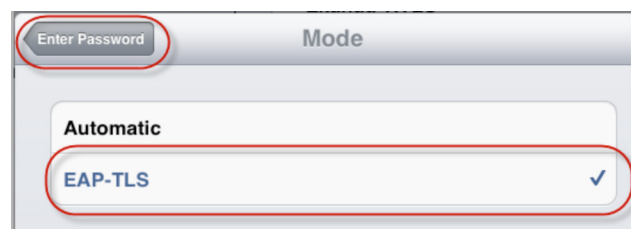
Select the network SSID to which iPad should connect. The spinning wheel next to the wireless symbol indicates that iPad is connecting to the network. In this example, iPad is initiating a connection to iPad test network.



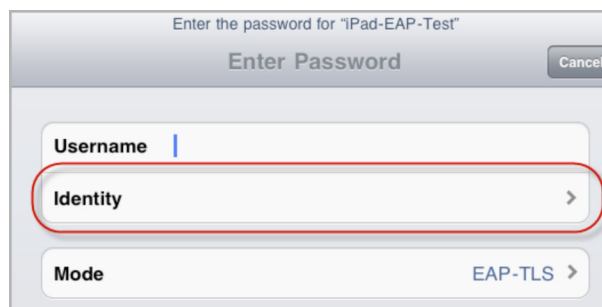
You will be prompted to enter the connection credentials. Select Mode.



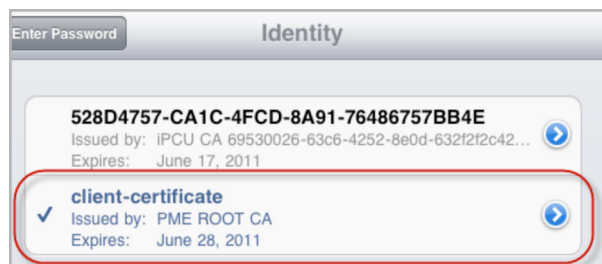
In the Mode selection screen, first select EAP-TLS and then Enter Password to return to the previous screen.



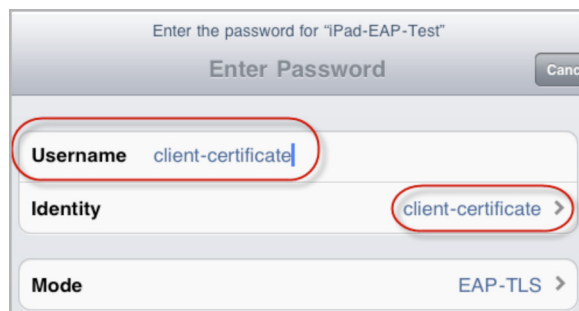
At the Enter Password screen, select Identity.



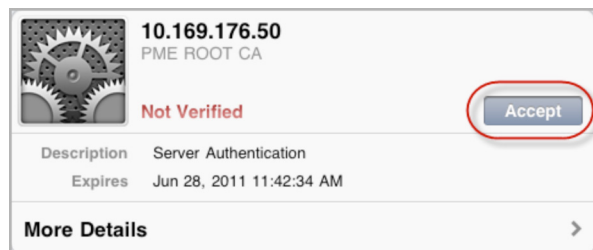
In the Identity screen, first select your Client Certificate and then select Enter Password to go back to the previous screen.



Type in the Username exactly as it appears in the Identity name field.



Select Accept when prompted to validate the Server Certificate to connect to the wireless network.



When you see a checkmark in front of the network name and the wireless symbol change color to blue, you know iPad successfully connected to the wireless network.



About Aruba Networks, Inc.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#).



www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com