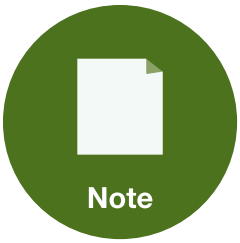

Aruba Virtual Intranet Access (VIA)

Version 1.0

ARUBA networks

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WEATHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACUTALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURSHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an “as is” basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1: Introduction

Virtual Intranet Access (VIA) is part of the Aruba remote access solution that includes remote access points (RAPs), Aruba Instant™ (IAP), and the Remote Node Solution. Aruba RAPs provide a comprehensive remote access solution that extends the corporate LAN to any remote location. RAPs enable seamless wired or wireless data and voice wherever a user finds an Internet-enabled Ethernet port or 3G cellular connection. However, RAPs cannot be used for secure corporate access from mobile hotspots that provide only wireless access, such as those in airport, hotels, and coffee shops. To address the demands of the current mobile workforce, which requires corporate access from these mobile hotspots, Aruba introduced the VIA solution. The Aruba VIA solution is designed to provide secure corporate access to employee laptops and smartphones from mobile hotspots.

This application note explains the implementation of a mobile access solution with Aruba VIA. Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1
ArubaOS (mobility access switch)	7.1
Aruba Instant™	1.1
MeshOS	4.2
AirWave®	7.3
AmigopodOS	3.3
VIA	2.1

Reference Material

Aruba highly recommends that you read the following prerequisite documentation before you read this document:

- Aruba Virtual Branch Networks Validated Reference Design, available at www.arubanetworks.com/vrd.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: https://support.arubanetworks.com/.

Chapter 2: Recommended Deployment Model and Licensing

VIA has two primary purposes:

- to provide secure corporate access to employee laptops and smartphones from anywhere
- to provide ease-of-use for the end users and network administrators

The ease-of-use is what differentiates VIA from other VPN solutions. VIA offers a zero-touch end-user experience and removes the complexity that is associated with configuring VPN clients on end-user devices. VIA provides ease-of-use not only for end users, but it also simplifies configuration and management for the IT team.

The Aruba VIA client that is available for Microsoft Windows computers (Windows XP, Vista, and Windows 7), Apple Mac OS X, and Apple iOS devices is a hybrid Internet Protocol Security (IPsec)/ Secure Sockets Layer (SSL) VPN client. If the user is connected to an untrusted network, the Aruba VIA client scans network connections and automatically establishes a secure connection back to the corporate network. Some additional features include Content Security Services (CSS), single-logon, SSL fallback when IPsec is blocked, and the ability to configure Wireless Local Area Network (WLAN) settings using the supplicant provided by the operating system.

How VIA Works

It is important to understand how VIA works before you begin deployment and configuration. The following steps explain how a VIA connects to a controller and establishes a secure connection back to the corporate network.

- VIA can be preinstalled on the laptop by the network administrators, or the users can download and install VIA.
- After the VIA client is installed, it prompts for the IP address or fully qualified domain name (FQDN) of the remote server and the username and password.
- After successful authentication, VIA downloads the VPN client configuration that belongs to the user and initiates a secure IPsec or SSL (if IPsec fails) connection back to the controller in the DMZ. If the VIA auto upgrade feature is enabled, the VIA image on the user device is upgraded to match the image on the controller or the external hosting server after the IPsec connection is established. For more information on this process, see VIA Bootstrapping on page 33 in Chapter 6: Configuring VIA Profiles.
- After this initial process, whenever a user connects to an untrusted network, VIA automatically detects the untrusted network connection and establishes a secure connection to the corporate network without any user intervention. For information on how VIA detects a trusted network, see VIA Bootstrapping on page 33 in Chapter 6: Configuring VIA Profiles.
- Sometimes, VIA might be unable to establish a secure connection due to changes in IKE pre-shared key, username and password, or IPsec crypto map parameters. If the user credentials have changed, VIA prompts for the new credentials and establishes the connection. However, if the IKE pre-shared key or the IPsec crypto map parameters of the VIA client configuration have changed, the VIA client configuration must be cleared and downloaded again.

Recommended Deployment

Figure 1 depicts a typical Aruba remote access deployment that provides a mobile access solution with VIA.

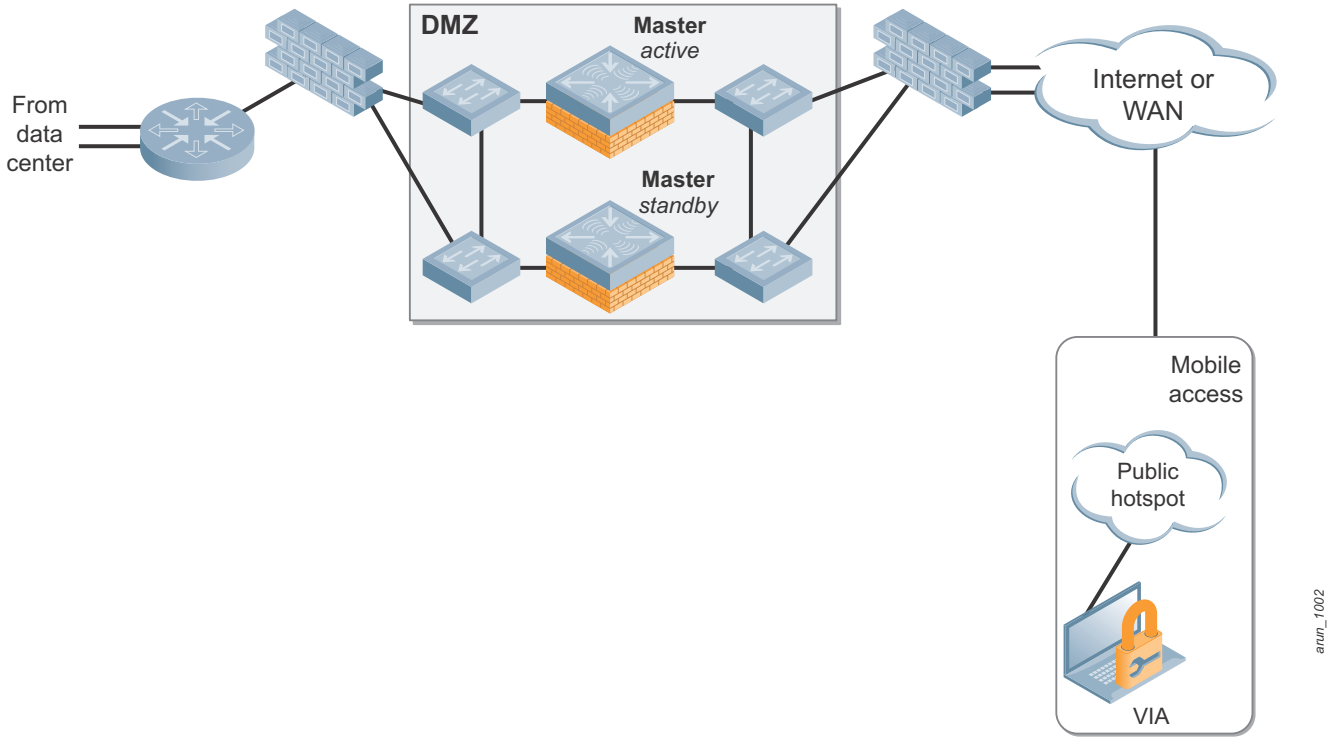

Figure 1 Recommended deployment

In mobile access deployments, the Aruba VIA clients typically terminate on the mobility controllers in the network DMZ. The mobility controllers terminate the VIA clients coming in over the Internet with IPsec or SSL sessions. An all-master design is recommended for Aruba mobile access deployments. The use of redundant controllers and the SSL fallback option on VIA clients ensures high availability of this architecture. For information on other deployment and redundancy models, see the *Aruba Mobility Controllers and Deployment Models Validated Reference Design*.

For the information on VLAN design and configuration of master controller redundancy for the DMZ controllers, see the *Aruba Virtual Branch Networks Validated Reference Design*.

Controller Selection

Selecting the proper mobility controller for a specific deployment depends on a number of factors, including user count, usage model, and AP count. Depending on the size of the deployment, any controller can be chosen as the mobility controller. It is recommended to separate the VIA and RAP deployments onto different mobility controllers to simplify controller selection, configuration, deployment, and troubleshooting. For mobile access deployments that use a dedicated controller for VIA termination, the controller selection process depends only on the IPsec tunnel limit of each controller platform. The number of VIA clients that are supported on a controller also depends on the configuration of SSL fallback. If SSL fallback is disabled, each VIA client accounts for one IPsec tunnel

towards the controller IPsec tunnel limit. In deployments where SSL fallback is enabled, two tunnels must be factored for each VIA client during the controller selection process. When the same controller is used for RAP and VIA termination, the proper calculation of total user count, RAP count, and IPsec tunnels consumed by RAPs and VIA is essential for choosing the right controller for your deployment. For more information on controller selection, see the *Aruba Mobility Controllers Validated Reference Design*.

Licensing

Licensing unlocks the configuration capabilities on the system. A mobility controller that is dedicated for VIA termination needs to be licensed only for VIA functionality. However, master mobility controllers that terminate VIA and RAPs or Remote Nodes should be licensed based on these two requirements:

- functionalities required
- number of APs terminated

Table 2 summarizes the licensing requirements for VIA deployments.

Table 2 Controller Licensing for VIA Deployments

Controller Function	Licenses	Purpose
Terminates VIA	• Policy Enforcement Firewall–VPN (PEFV)	PEFV is required for VIA termination. PEFV allows the configuration of firewall policies, so a separate PEFNG license is not required.
Terminates RAPs	• AP Capacity • Policy Enforcement Firewall–Next Generation (PEFNG) • RFProtect™ (if wireless intrusion prevention system [WIPS] and spectrum functionalities are required)	AP capacity is required for RAP termination. PEFNG is required for configuration of firewall polices and user roles. RFProtect is recommended but only required for functionalities such as WIPS and spectrum.
Terminates RAPs and VIA	• PEFV • AP Capacity • PEFNG • RFProtect (if WIPS and spectrum functionalities are required)	PEFV is required for VIA termination, while the AP capacity, PEFNG, and RFProtect licenses are required for RAPs. RFProtect is recommended but only required for functionalities such as WIPS and spectrum.
Terminates Remote Nodes and VIA	• PEFV • AP Capacity • PEFNG • RFProtect (if WIPS and spectrum functionalities are required)	PEFV is required for VIA termination, while the AP capacity, PEFNG, and RFProtect licenses are required for APs terminating on the remote nodes. RFProtect is recommended but only required for functionalities such as WIPS and spectrum.

VIA optionally can support advanced Suite B cryptographic algorithms, approved for use in government networks to carry classified information. Support for Suite B cryptography requires the Advanced Cryptography license. For information on requirements of Suite B and configuring VIA for Suite B cryptography, see the *Aruba 6.1 User Guide* available at the Aruba support site.

Firewall Requirements

By default, all VIA clients use certain UDP and TCP ports to establish an IPsec connection. However, VIA 1.0 for Mac OS uses some additional ports than those used by VIA for Windows and iOS. VIA 1.0 for Mac OS depends on the IPsec stack of the Mac OS, which uses some additional ports to establish an IPsec connection. All VIA clients use these common ports:

- TCP 443
  - used by the end user to download VIA client software
  - used by the VIA client to download the latest VIA configuration
  - used by the VIA client for trusted network and captive portal checks
  - used for SSL fallback when UDP 4500 is blocked
- UDP 4500
  - used for IPsec NAT-T

VIA 1.0 for Mac OS uses these additional ports:

- UDP 500
  - used by Mac OS for internet key exchange (IKE) along with port 4500
- IP Protocol 50
  - used for forwarding Encapsulating Security Protocol (ESP) traffic

In your network, it is necessary to open these ports on all firewalls that lead up to the controller on which VIA terminates.

Chapter 3: IPsec

IPsec standard is a suite of security protocols that enable the creation of a secure channel for exchange of data over the Internet. IPsec provides cryptographic protection to the IP datagrams that traverse the network between two endpoints. The endpoints can be a pair of VPN gateways, a VPN gateway and a host, or a pair of hosts. IPsec uses one of these two protocols to protect the data:

- Encapsulated Security Payload (ESP): IPsec with ESP provides data confidentiality, data integrity, and source authentication
- Authentication Header (AH): The use of AH only provides data integrity and source authentication. IPsec with AH does not provide confidentiality.

Both AH and ESP can be used in two different modes to protect the data. The two modes used by IPsec are these

- Transport mode: In transport mode, IPsec only protects the IP payload. AH or ESP is applied only to the IP payload and the original IP header is used to forward the IP packet.
- Tunnel mode: In tunnel mode, IPsec protects the entire IP packet. AH or ESP is used to encapsulate the entire IP packet and a new IP header is added. The new IP header is used to forward the packet to the corresponding IPsec peer.

VIA uses ESP in tunnel mode.

Figure 2 through Figure 6 represent the packet format for AH and ESP in different modes.

Figure 2 Original IP packet

Figure 3 AH in transport mode

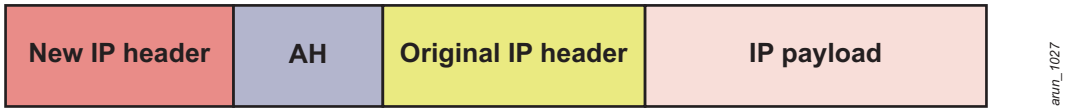

Figure 4 AH in tunnel mode

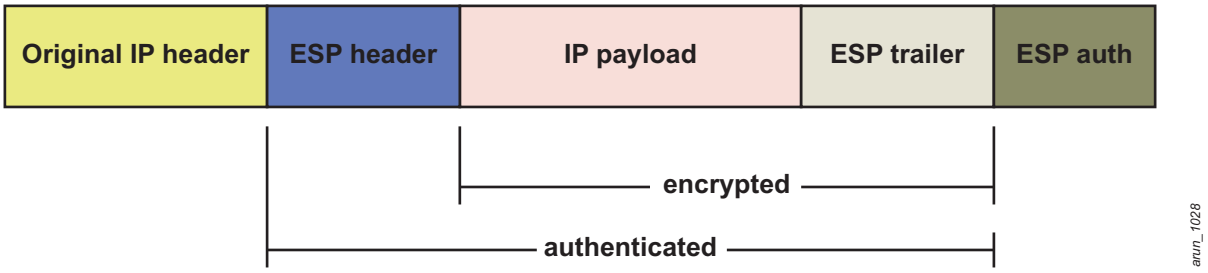

Figure 5 ESP in transport mode

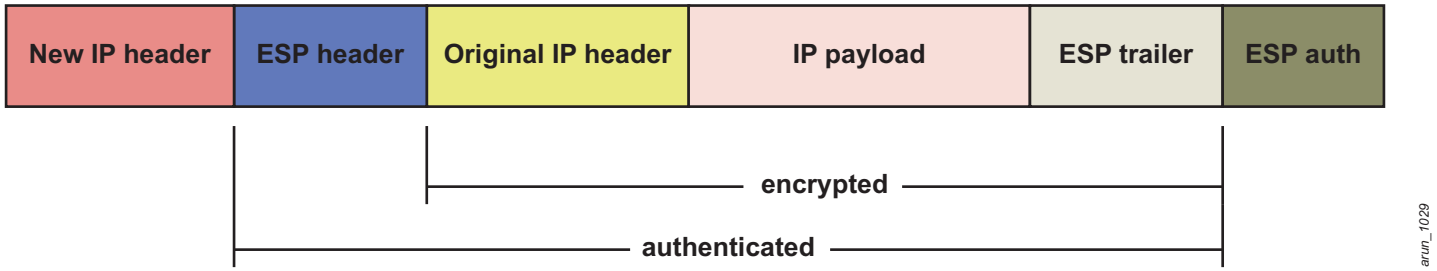

Figure 6 ESP in tunnel mode (VIA operates in this mode)

It is clear that IPsec has several secure protocols and modes to protect the data. So, when an IPsec endpoint has to forward a packet, it must first decide whether the packet has to be protected by IPsec. The decision to protect the packet with IPsec is usually based on the source and destination of the IP packet. If the packet has to be protected by IPsec, then the IPsec endpoint has to decide on a number of other security parameters such as these

- security protocol (AH/ESP)
- IPsec encapsulation mode (tunnel/transport)
- encryption key
- encryption algorithm (DES/3DES/AES)
- authentication key/certificates
- authentication algorithm (SHA/MD5)

In IPsec, it is important that the IPsec peers agree on a common set of the above mentioned security parameters so that the traffic encrypted by one endpoint can be decrypted by the other. Such a set of security parameters agreed upon by IPsec peers to protect the data is known as a security association (SA). A SA is nothing but a collection of security information such as encryption keys and algorithms that enables a secure connection between IPsec peers. Normally, each SA that is formed between IPsec peers has a lifetime associated with it. When an SA lifetime expires, the IPsec peers have to renegotiate the SA. IPsec requires the use of separate SAs for inbound and outbound traffic.

The security of an IPsec connection is completely dependent on how securely the two IPsec peers exchanged the different security parameters. A critical function of IPsec is to ensure that the keys negotiated and the security parameters exchanged by the IPsec peers to form an SA happen in a secure manner. The key management protocol used by IPsec to securely negotiate, manage, and rekey the SAs is the IKE protocol. IKE is an integral part of IPsec and is available in two flavors: IKEv1 and IKEv2. For more information on IKE versions, see Chapter 5: VPN Server Configuration for VIA.

Chapter 4: Defining VIA Requirements

The operating system that is running on a user device determines the type of VIA clients that must be installed on it. Three basic types of VIA clients are available for customers:

- VIA for Windows (available at the Aruba support site)
- VIA for Mac OS (available at the Aruba support site)
- VIA for iOS (available at Apple App store)

These three different VIA clients are available in one or more version. Aruba supports two major VIA versions, VIA 1.x and VIA 2.x. Table 3 shows the various VIA versions available for each type of VIA client.

Table 3 VIA Types and Versions

VIA Type	Legacy VIA Versions	Current VIA Versions
VIA for Windows	1.0, 1.1, 1.2, 2.0, 2.0.1	2.1
VIA for Mac OS	1.0	1.0.0.2
VIA for iOS	_	2.0

Remember that the IKE versions and authentication mechanisms supported by the two major VIA versions (VIA 1.x and VIA 2.x) vary. The following authentication mechanisms and IKE versions are supported by VIA 1.x:

- VIA 1.x supports authentication using IKE version 1(IKEv1) only. IKEv1 has two phases: phase 1 and phase 2.
- Phase 1 authentication, which authenticates the VPN client, can be performed using PSK or X.509 certificates.
- Phase 2 authentication of IKEv1, which authenticates the user, is performed using XAUTH. This authentication phase requires a username and password. This username and password can be authenticated against the RADIUS, Lightweight Directory Application Protocol (LDAP), or internal database. If RADIUS is used, it must support the Password Authentication Protocol (PAP).

VIA supports the use of tokens (two-factor authentication) for authenticating the VIA users.

VIA 2.x supports these authentication mechanisms and IKE versions:

- VIA 2.x supports IKEv1 and all the authentication methods supported by VIA 1.x.
- VIA 2.x also supports IKE version 2 (IKEv2). IKEv2 only has a single authentication phase. It is quicker and more secure than IKEv1.

- VIA 2.x supports these authentication methods for IKEv2:
  - X.509 certificate. The CA certificate corresponding to issued user or device certificates must be loaded on the controller. Controllers running ArubaOS 6.1 or greater support OCSP for the purpose of validating that a certificate has not been revoked.

VIA also supports the use of smart cards that support a Smart Card Cryptographic Provider (SCCP) API within the operating system. VIA looks for an X.509 certificate in the certificate store of the operating system. A smart card that supports a SCCP causes the certificate embedded within the smart card to appear automatically in the certificate store of the operating system.

  - Extensible Authentication Protocol (EAP) including EAP-TLS (using client certificates) and EAP-MSCHAPv2 (using a username/password). The use of EAP methods allows an external RADIUS server to authenticate the client credentials.
- VIA 2.x also supports Suite B cryptography. Suite B cryptography provides the highest level of security available today in public-commercial algorithms. For information on the requirements of Suite B and configuring VIA for Suite B cryptography, see the *Aruba 6.1 User Guide,* available at the Aruba support site.

For more information on the features and capabilities available on the current version of VIA clients, see Appendix B: VIA Client Feature Matrix.

Currently, VIA is not supported for the Android operating system and VIA for Mac OS does not support IKEv2. Both capabilities are under development.

Apart from the different types of VIA clients and versions, it is very important to remember that all VIA types and versions are not supported by all versions of ArubaOS. Table 4 shows the compatibility of different versions of VIA with ArubaOS.

Table 4 ArubaOS and VIA Compatibility

ArubaOS	VIA for Windows 7, Vista, and Windows XP (32-bit)	VIA for Windows 7 and Vista (64-bit)	VIA for Mac OS	VIA for iOS 4.2 and later
5.0.x	1.0, 1.1, 1.2	__	__	__
6.0.x	1.0, 1.1, 1.2	1.2	__	__
6.1.x	1.0, 1.1, 1.2, 2.0, 2.0.1, 2.1	1.2, 2.0. 2.0.1, 2.1	1.0, 1.0.0.2	2.0

It is important for network administrators to clearly determine the minimum ArubaOS and VIA client version requirements before they configure the VIA solution. These factors influence this decision:

- IKE version
- client authentication method
- operating systems on the user devices (Windows, Mac OS, or iOS)

Figure 7 is a simple VIA decision tree based on the IKE version and client authentication method requirements.

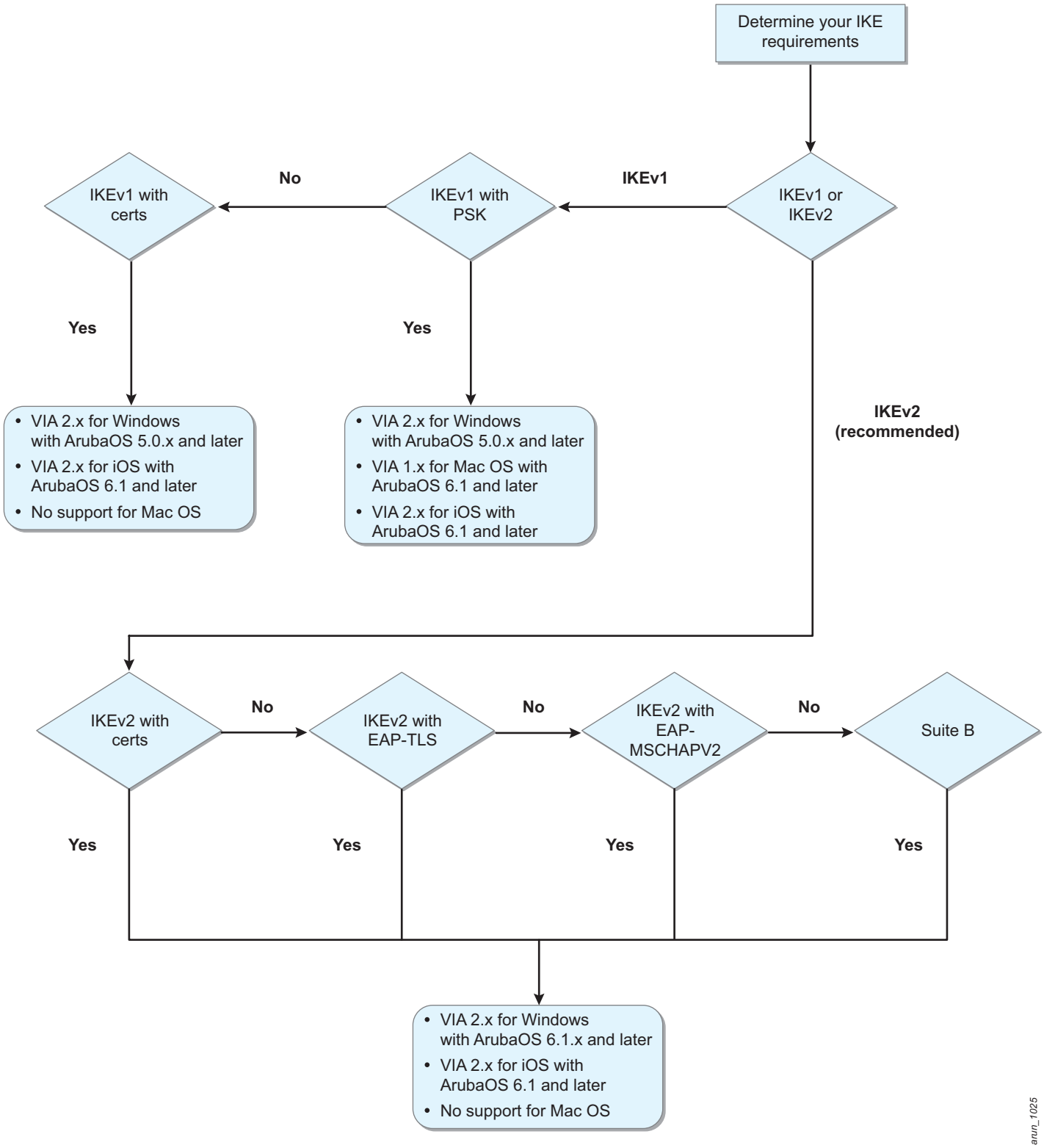

Figure 7 VIA deployment planning

For information on configuring IKEv1-PSK VIA deployments, see these sections:

- Configuring the VPN Server on the Controller on page 16
- Configuring VPN Server for IKEv1-PSK on page 17
- Chapter 6: Configuring VIA Profiles

For information on configuring IKEv1-Certs VIA deployments, see these sections:

- Configuring the VPN Server on the Controller on page 16
- Configuring VPN Server for IKEv1 Certificates on page 23
- Chapter 6: Configuring VIA Profiles

For information on configuring IKEv2-Certs VIA deployments, see these sections:

- Configuring the VPN Server on the Controller on page 16
- Configuring VPN Server for IKEv2 on page 25
- Chapter 6: Configuring VIA Profiles

For information on configuring IKEv2-EAP VIA deployments, see these sections:

- Configuring the VPN Server on the Controller on page 16
- Configuring VPN Server for IKEv2 on page 25
- Chapter 6: Configuring VIA Profiles

Chapter 5: VPN Server Configuration for VIA

Certain tasks are necessary to configure a fully functional mobile access solution using VIA. Most of these tasks are required, but depending on the organizational requirements, some of these tasks may be optional. The following list outlines the tasks necessary to configure the Aruba VIA solution:

1. Configuring the virtual private network (VPN) server on the controller (required)
2. Configuring the VIA user role (required)
3. Configuring a VIA server group for authenticating VIA users (required)
4. Configuring the VIA authentication profile (required)
5. Configuring the VPN authentication profile to support VIA for Mac OS (required only for networks supporting Mac OS VIA clients)
6. Configuring the VIA connection profile (required)
7. Attaching the VIA connection profile to the user role (required)
8. Configuring the VIA web authentication (required)
9. Uploading the VIA installer to the controller or an external server (required)
10. Installing VIA on the end-user device (required)
11. Configuring SSL fallback (optional)
12. Configuring VIA client WLAN profiles (optional)
13. Customizing the VIA logo and the welcome HTML page (optional)

Configuring the VPN Server on the Controller

VIA clients connect to the controller through the public Internet. This communication between VIA clients and the controller across the public Internet is secured using the VPN technology. In the VIA solution, the controllers act as the VPN servers and the VIA clients that are installed on the end-user devices behave as the VPN clients. Secure communication between the controller and VIA clients is achieved using IPsec. As described earlier, the authentication mechanisms and IKE versions used for creating the IPsec tunnel varies depending on the VIA version.

Configuring the VPN Server for IKEv1

IKEv1 protocol defines a two-phase method for providing Internet security. Phase 1 involves the creation of a secure Internet Security Association and Key Management Protocol (ISAKMP) tunnel and phase 2 involves the creation of a secure IPsec tunnel. The IPsec tunnel created in phase 2 is used to secure user data. The initial ISAKMP tunnel ensures that the negotiations for the establishing the IPsec tunnel happen within a secure channel. For more information on IKEv1, see the Internet Engineering Task Force (IETF) RFC-2409 document.

IKEv1 for VIA has two authentication phases. Phase 1 authentication of IKEv1 can be implemented using PSK or X.509 certificates. The phase 2 authentication, which is implemented using XAUTH, requires a username and password. So, the VPN server configuration for IKEv1-PSK varies from that of IKEv1-Certs.

Configuring VPN Server for IKEv1-PSK

At the minimum, these parameters should be configured in the VPN server of the controller for VIA deployments using IKEv1 with PSK:

- L2TP and XAUTH parameters
- address pools
- IKE aggressive group name
- IKE shared secret

L2TP and XAUTH Parameters

The L2TP and XAUTH parameters settings that should be configured for IKEv1 VIA deployments are these:

- **Enable XAUTH:** By default, IKEv1 VIA deployments use XAUTH with IPsec tunnel mode to establish secure VPN connections to the controller. So, the XAUTH knob under the L2TP and XAUTH parameters settings should be enabled for IKEv1 VIA deployments.
- **Configure DNS information:** The DNS server options under the L2TP and XAUTH parameters settings must also be configured, with the appropriate corporate DNS servers, for use by VIA clients that connect to the controller. Without the DNS server information, VIA cannot resolve the DNS queries for tunneled networks.

Remember that the intranet hostnames cannot be resolved if you use a public DNS server in this field.

- **Enable L2TP:** VIA for Mac OS uses the built-in IPsec stack of the Mac OS for establishing IPsec connection. The IPsec stack in Mac OS does not use XAUTH. Instead, it uses PPP authentication within an L2TP tunnel to authenticate the users. The L2TP tunnel is also used for exchange of IP information related to the IPsec tunnel. For deployments that support VIA for Mac OS, the L2TP parameter should be enabled. Remember that the L2TP tunnel is built within the secure IPsec tunnel, so all the exchanges are secure.
- **Authentication protocols:** This parameter defines the PPP authentication protocol that should be used to authenticate the credentials presented by the Mac OS VIA users. The various options available are PAP, EAP, CHAP, MSCHAP, and MSCHAPv2. For deployments that support VIA for Mac OS, select an authentication method that suits your network policy. Aruba recommends that you choose a strong authentication method, such as MSCHAPv2, rather than PAP.

Address Pools

Every VPN client (RAPs, third-party VPN clients, and VIA) that successfully authenticates to the VPN server module of the controller is given a valid inner IP address and DNS server information. This inner IP address is issued from the address pool that is configured in the VPN server. More than one pool can be configured and there is no need to assign more addresses in the pool than the number of VPN clients that terminate on that controller. DHCP services are not required for the subnets used in the

VPN address pool. However, it is necessary to define a VLAN for the subnet used in the VPN address pool and ensure that this VLAN is routable from the corporate network.

It is essential that the addresses used in the VPN address pool for VIA are routable from the internal corporate network. If not, the VIA clients cannot connect to the corporate resources and vice-versa. Alternatively, you can implement Network Address Translation (NAT) on the VLAN used for the VPN address pool. Remember that NAT might cause issues with certain applications such as file transfer protocol (FTP). For information on VLAN Design for remote networks, see the *Aruba Virtual Branch Networks Validated Reference Design*.

If only a single pool is configured, all the VPN clients that terminate on that controller are issued an inner IP address from the same pool. When multiple address pools are configured, the controller can be configured to use distinct VPN pools for RAPs, VIA, and third-party VPN clients. This configuration can be achieved by appending a VPN pool to the role assigned to the RAPs, VIA, and third-party VPN clients. For information on adding a distinct VPN address pool to a user role, see Attaching the VIA Connection Profile to a User Role on page 49 in Chapter 6: Configuring VIA Profiles.

When distinct VPN pools are not defined, the controller automatically uses the first pool in the VPN address pool. When this pool expires, the next pool in the list is used and so on. Remember that if the VPN address pool is exhausted, new VIA clients cannot establish the IPsec tunnel until the required number of IP addresses are added to the pool.

Like the VLAN and IP parameters, the VPN address pools are not synchronized from the active controller to the backup controller during database synchronization. Create VPN address pools individually on the active and standby master controllers. The VPN pools used on the active and the backup controller are not required to be the same.

IKE Aggressive Group Name

The IKE aggressive group name is a feature used by certain legacy VPN clients that require an aggressive mode group name. This parameter is not used by VIA. However, this field cannot be empty and requires a value. The default value is “changeme”.

IKE Shared Secret

For VIA deployments that use IKEv1 with PSK, a part of the IPsec process requires the VPN client to present a shared secret. Aruba allows you to configure keys that are specific to a subnet or you can specify a global key. To make the IKE key global, specify 0.0.0.0 for the subnet and subnet mask length fields. Remember, for VIA deployments using IKEv1-PSK, the IKE shared secret should be configured for the IPsec tunnel to be established. From a security perspective, it is very important to make sure that the IKE pre-shared key is long and complex. Aruba recommends no fewer than 16 characters.

Configuring a Routable Address Pool

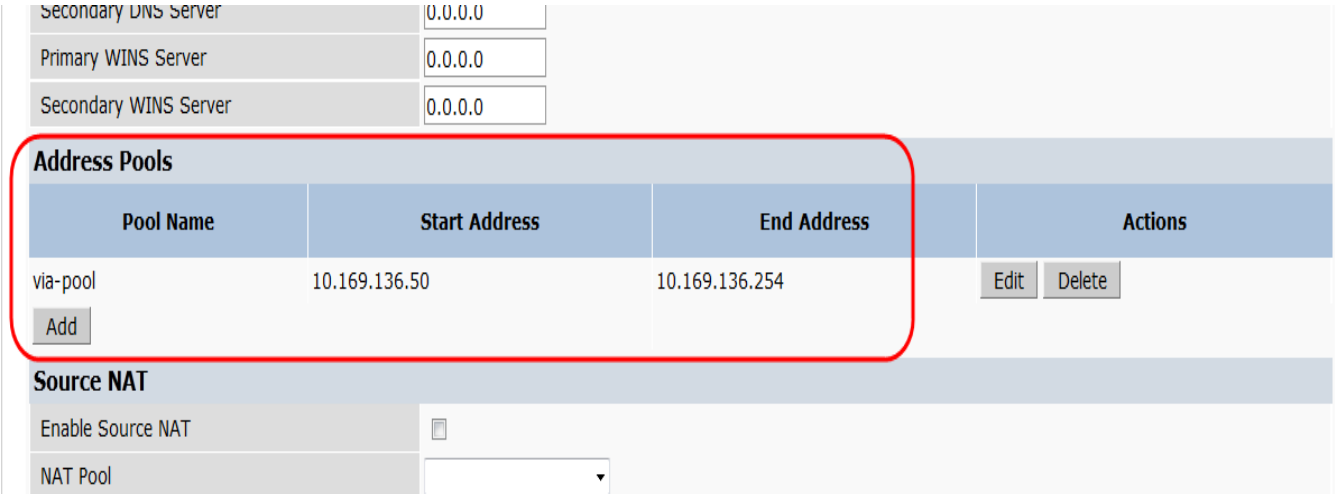

Figure 8 VPN address pool

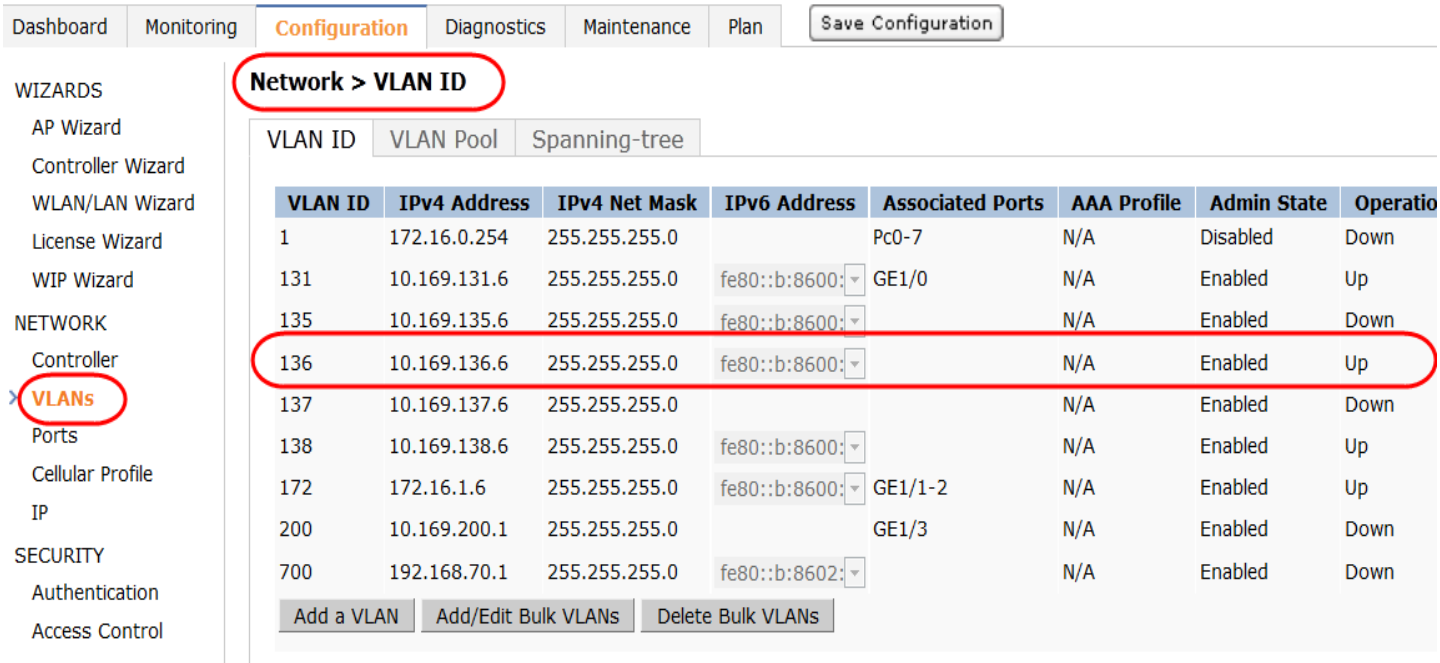

Figure 9 Defining a routable VLAN for the VPN address pool subnet

IKEv1-PSK Configuration

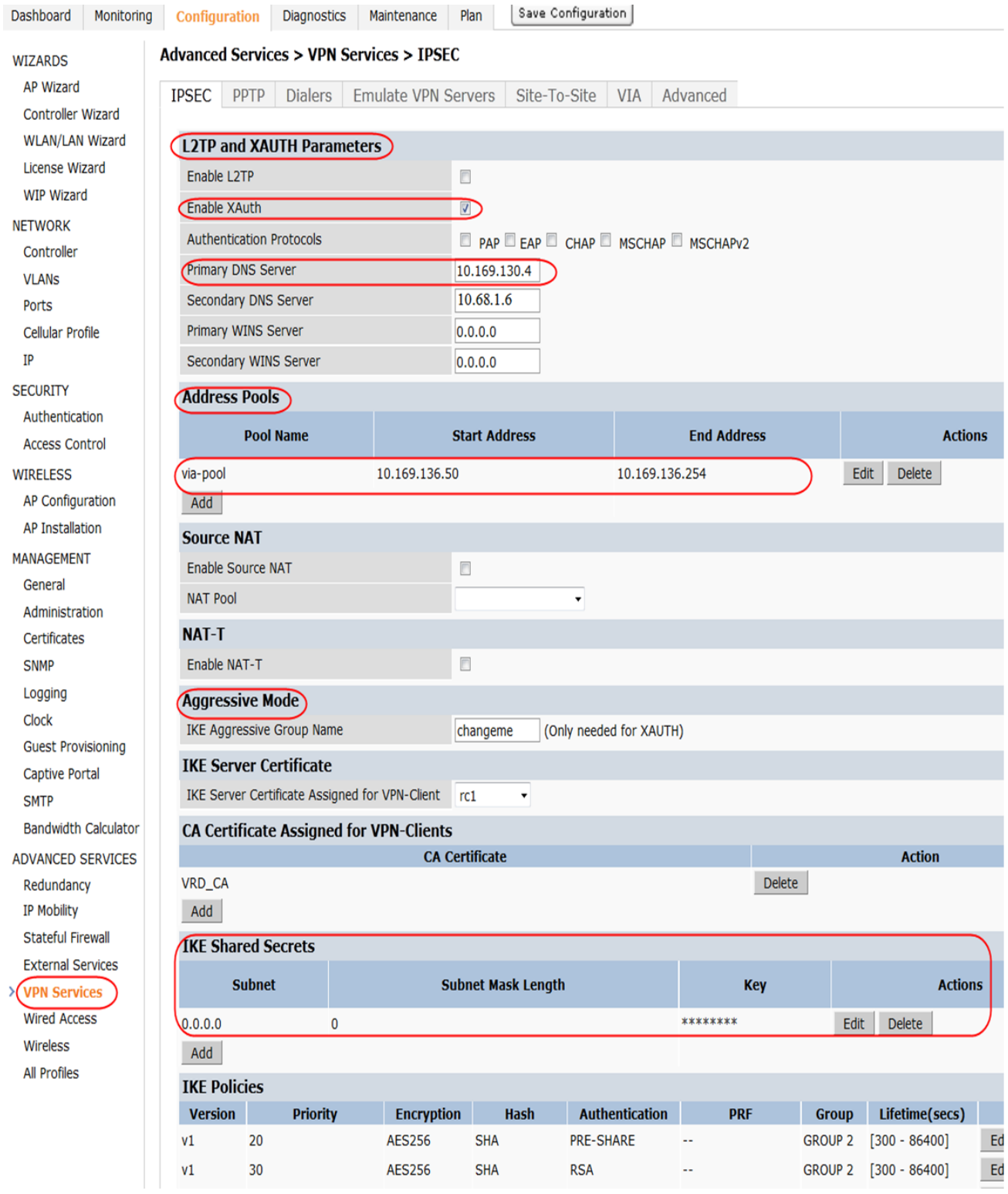

Figure 10 VPN server configuration for IKEv1-PSK on windows and iOS VIA clients

```
!
crypto-local isakmp xauth
client configuration dns 10.169.130.4 10.68.1.6
!
ip local pool "via-pool" "10.169.138.50" "10.169.138.254"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0"
!
```

IKEv1- PSK (Mac OS VIA version 1.0) Configuration

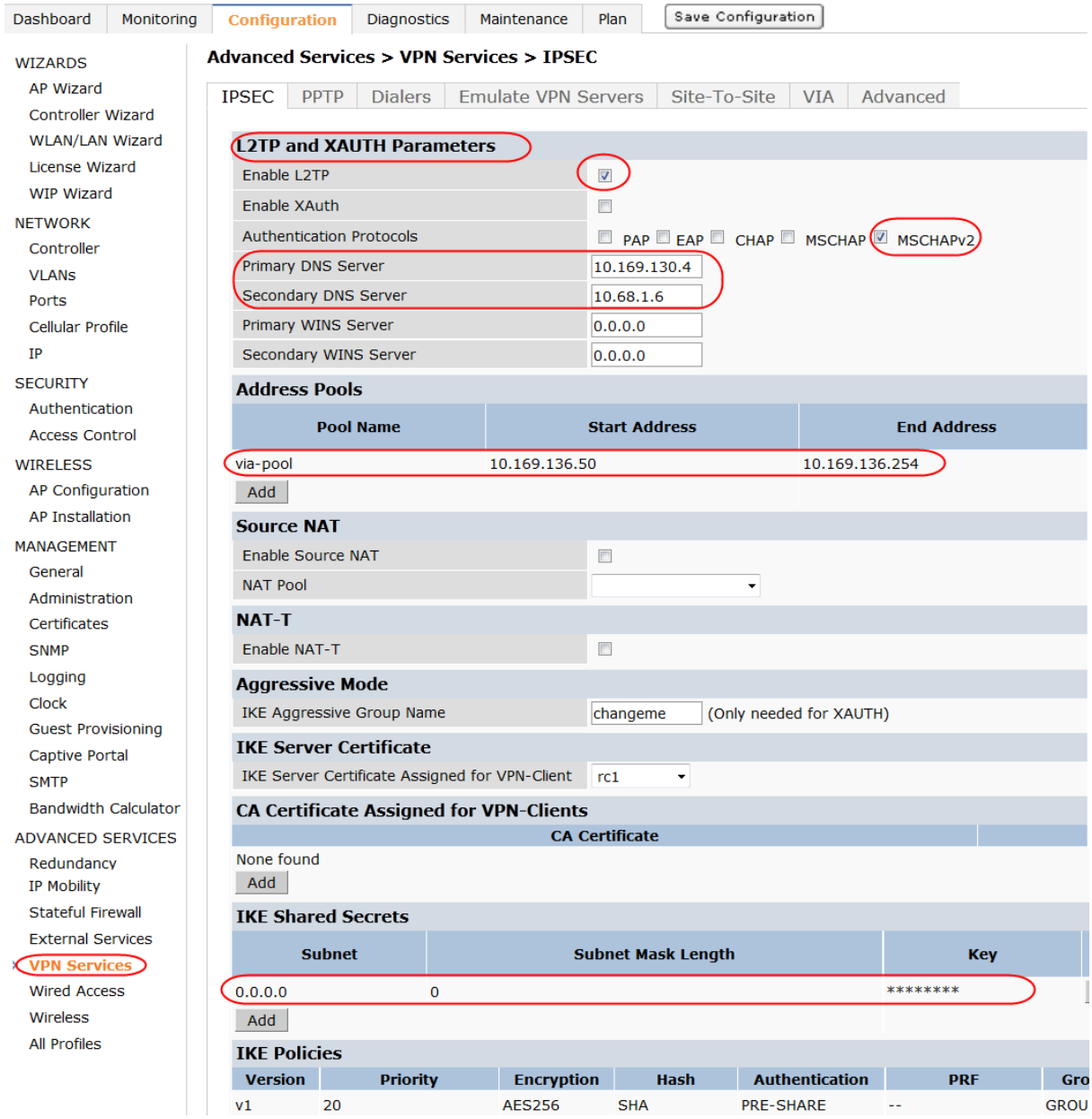

Figure 11 VPN server configuration for Mac OS VIA version 1.0

```
!
vpdn group l2tp
   enable
   no ppp authentication PAP
   ppp authentication MSCHAPv2
   client configuration dns 10.169.130.4 10.68.1.6
!
ip local pool "via-pool" "10.169.138.50" "10.169.138.254"
crypto isakmp key ***** address "0.0.0.0" netmask "0.0.0.0"
!
```

Configuring VPN Server for IKEv1 Certificates

At the minimum, these parameters should be configured in the VPN server of the controller for VIA deployments using IKEv1 with certificates:

- L2TP and XAUTH parameters. For details, see L2TP and XAUTH Parameters in Configuring VPN Server for IKEv1-PSK on page 17.
- Address pools. For details, see Address Pools in Configuring VPN Server for IKEv1-PSK on page 17.
- IKE aggressive group name. For details, see IKE Aggressive Group Name in Configuring VPN Server for IKEv1-PSK on page 17.
- IKE server certificate
- CA certificate assigned for VPN-clients
- Certificate groups for VPN-clients (optional)

VIA 1.0 for Mac OS does not support IKEv1-certs.

IKE Server Certificate

For VIA deployments that use IKEv1 with certificate, the VPN server on the controller and the VIA client present a certificate to each other as a part of phase 1 authentication of IKEv1. The certificate that should be presented by the VPN server module to the VIA client should be selected as the IKE server certificate.

CA Certificate Assigned for VPN-Clients

For clients that use certificates, the certificate presented during phase 1 authentication of IKEv1 is considered valid only if it is signed by a trusted CA. The CA certificate of the trusted CAs that signed the client certificates must be added to the CA Certificate Assigned for VPN-Clients parameter list. Client authentication fails if the presented client certificate is not signed by the CAs in the CA Certificate Assigned for VPN-Clients parameter list.

Aruba controller can be configured as an Online Certificate Status Protocol (OCSP) client to validate the revocation state of the certificates presented by the clients. Support for OCSP requires ArubaOS version 6.1 or later. To configure the Aruba controller as OCSP see the *Aruba 6.1 User Guide* available at the Aruba support site.

Certificate Groups for VPN-Clients

Introduced in ArubaOS 6.1, the certificate groups for VPN-clients parameter allows the use of unique server certificates for different clients. This new parameter enables the pairing of IKE server certificates with trusted CA certificates. The controller uses this list to present the appropriate IKE server certificate to the client. The server certificate presented to the clients depends on the CA cert used to sign the client certificate. With this feature, VPN clients using RSA certificates and Suite B

clients using Elliptic Curve Digital Signature Algorithm (ECDSA) certificates can be terminated on the same controller.

NOTE

In ArubaOS 6.0 and earlier, only a single certificate can be used as IKE server certificate.

IKEv1-Certs Configuration

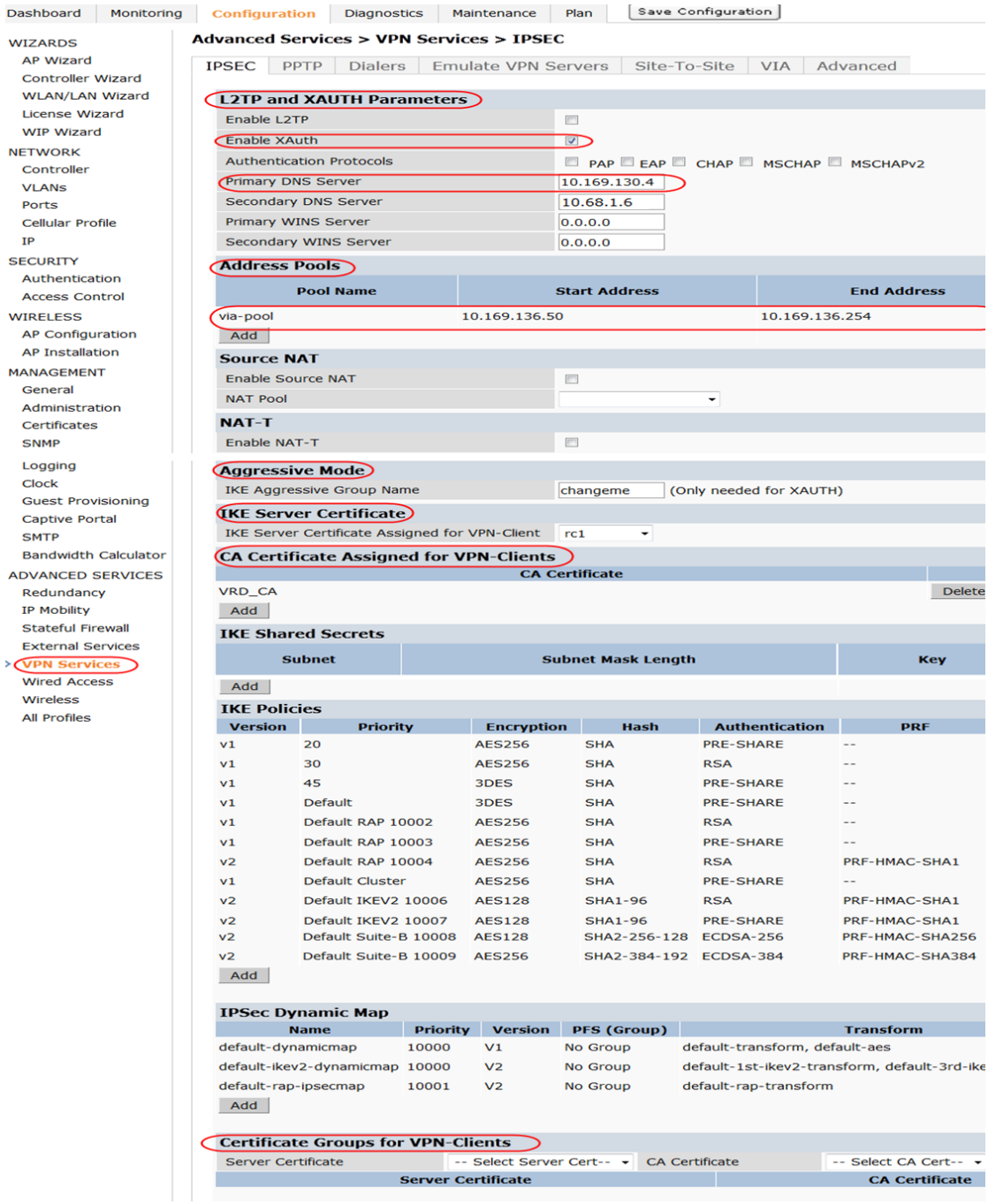

Figure 12 VPN server configuration for IKEv1-Certs

```
!
crypto-local isakmp xauth
   client configuration dns 10.169.130.4 10.68.1.6
crypto-local isakmp server-certificate "rc1"
crypto-local isakmp ca-certificate "VRD-CA"
!
ip local pool "via-pool" "10.169.138.50" "10.169.138.254"
crypto-local isakmp certificate-group server-certificate rc1-ecc ca-certificate ECC-VRD-CA
!
```

IKEv1 Phase 2 Authentication

After the IKEv1 phase 1 is complete using PSK or certificates, a secure ISAKMP tunnel (also known as ISAKMP SA) is formed. When phase 1 is complete, the phase 2 negotiations take place and a secure IPsec tunnel (also known as IPsec SA) is formed. This IPsec tunnel is used to secure the user data.

As per the IKEv1 standard, after the initial phase 1 authentication, no additional authentication is needed to complete the phase 2. IKEv1 authenticates the IPsec devices or VPN clients but does not include any mechanism to authenticate the remote VPN user. However, if desired, the XAUTH mechanism can be used to force a VPN user to authenticate using a username and password or token cards (two-factor authentication) to a VPN gateway before the IKEv1 phase 2. This authentication provides an additional layer of security. XAUTH is not a part of the IKEv1 standard, but it is rather an extension to IKEv1 phase 1. XAUTH takes place after the successful completion of phase 1, and IKEv1 phase 2 negotiations occur only after the successful completion of XAUTH.

By default, VIA uses XAUTH for IKEv1, which requires the VIA user to present valid credentials to establish a secure connection to the corporate resources. The credentials provided by the user during XAUTH are validated against the specified authentication server. Either the internal database or any other authentication server type available on ArubaOS can be used as the authentication server. If an external RADIUS server is used to authenticate IKEv1 VIA users, then it must support PAP authentication. For more information on authentication server requirements and configuring an authentication server, see Configuring a VIA Server Group for Authenticating VIA Users on page 36 in Chapter 6: Configuring VIA Profiles.

Configuring VPN Server for IKEv2

Like IKEv1, IKEv2 also forms two tunnels or SAs to secure the sensitive data. However, IKEv2 is lighter and much faster than IKEv1. IKEv1 is complex and takes up to nine messages to establish a secure IPsec tunnel, but IKEv2 requires just four messages to establish the IPsec tunnel. As a result, IKEv2 significantly reduces the bandwidth requirements. IKEv2 is also more resilient to DOS attacks than IKEv1. IKEv2 also supports EAP authentication and does not require the use of XAUTH. IKEv2 has enhancements such as liveness checks, which make it more reliable than IKEv1. For more information on IKEv2, see the IETF RFC-4306 document.

IKEv2 does not have two phases of authentication, only a single phase. The IKEv2 authentication methods that are supported for VIA clients on ArubaOS are these:

- User authentication with X.509 certificates
  - The VIA client authenticates the controller certificate.
  - The controller authenticates the user certificate. No EAP methods are involved.

- User authentication with EAP-TLS
  - The VIA client authenticates the controller certificate.
  - The controller authenticates the user certificate using EAP-TLS over IKEv2. The controller just acts as an EAP pass-through to an external EAP-compliant server. EAP termination on the controller is not supported for VIA clients.
- User authentication with EAP-PEAP
  - The VIA client authenticates the controller certificate.
  - The controller validates the user credentials (username and password) with an external server. The controller just acts as an EAP pass-through to an external EAP-compliant server. EAP termination is not supported for VIA clients, so the internal database of the controller cannot be used to validate user credentials.

EAP-TLS and EAP-MSCHAPv2 are supported for IKEv2. However, EAP termination and other EAP types are not supported for IKEv2.

ArubaOS does not support the use of IKEv2 with PSK for VIA. However, site-to-site IKEv2 VPN links can be configured to use PSK.

At the minimum, these parameters should be configured in the VPN server of the controller for VIA deployments using IKEv2:

- L2TP and XAUTH parameters
- Address pools. For details, see Address Pools in Configuring VPN Server for IKEv1-PSK on page 17.
- IKE aggressive group name. For details, see IKE Aggressive Group Name in Configuring VPN Server for IKEv1-PSK on page 17.
- IKE server certificate
- CA certificate assigned for VPN clients. (Required only for IKEv2 authentication with X.509 certificates and not for EAP authentications.)
- Certificate groups for VPN clients. (Optional for IKEv2 authentication with X.509 certificates and is not required for EAP authentications.) For details, see Certificate Groups for VPN-Clients on page 23.

L2TP and XAUTH Parameters

As described earlier, IKEv2 does not use XAUTH, so the XAUTH parameter need not be enabled for IKEv2 VIA deployments. However, the L2TP and XAUTH parameters setting that must be configured for IKEv2 VIA deployments is this one:

- **Configure DNS information:** The DNS server options under the L2TP and XAUTH parameters settings must be configured, with the appropriate corporate DNS servers, for use by VIA clients that connect to the controller. Without the DNS server information, VIA cannot resolve the DNS queries for tunneled networks. Remember that the intranet hostnames cannot be resolved if you use a public DNS server in this field.

IKE Server Certificate

IKEv2 supports asymmetric authentication, which means that both peers do not have to use the same authentication method. For instance, one peer can use certificates and the other can use EAP-MSCHAPv2. For VIA deployments that use IKEv2, the VPN server on the controller always uses a certificate for IKEv2 authentication phase. However, the clients can use certificates, EAP-MSCHAPv2, or EAP-TLS. The certificate that should be presented by the VPN server module to the VIA client should be selected as the IKE server certificate.

CA Certificate Assigned for VPN-Clients

For clients that use certificates, the certificate that is presented during the IKEv2 authentication phase is considered valid only if it is signed by a trusted CA. The CA certificate of the trusted CAs that signed the client certificates must be added to the CA Certificate Assigned for VPN-Clients parameter list. Client authentication fails if the presented client certificate is not signed by the CAs in the CA Certificate Assigned for VPN-Clients parameter list.

Aruba controller can be configured as an OCSP client to validate the revocation state of the certificates presented by the clients. Support for OCSP requires ArubaOS 6.1 or later. To configure the Aruba controller as OCSP client, see the *Aruba 6.1 User Guide* available at the Aruba support site.

Check Certificate Common Name Against AAA Server

In IKEv2 VIA deployments using certificates, the user certificate presented by the VIA clients can be further scrutinized by validating the certificate common name (CN) against an authentication server. This can be achieved by enabling the “check certificate common name against AAA server” parameter available in the default VPN authentication profile. If this option is enabled, the CN that is present in the client certificate is authorized against the specified server. The controller captures and sends the certificate CN name as an authorization string to the specified authentication server. If the authentication server authorizes the CN, the client is authenticated by the controller. These criteria must be satisfied to pass authentication when the “check certificate common name against AAA server” parameter is enabled:

- The client certificate must be signed by a trusted CA.
- The client certificate CN should be authorized by the authentication server.

If the “check certificate common name against AAA server” option is disabled, client authentication is only based on whether the client certificate is signed by a trusted CA or not.

Either the internal database on the controller or an external authentication server can be used for authorizing the CN. If the internal database is used, add all certificate CNs to the internal database of the controller on which the VIA clients terminate. When you add the user name to the internal

database, you must add a password for each user. Add a dummy password because this password does not influence the authorization of CN by the internal database.

Ensure that your authentication sever supports authorization services using only the username because not all authentication servers support this feature. Clearpass has support for authorizing based on just the username. If a RADIUS server is used for authorization, the controller will send the certificate CN as a RADIUS “authorize only” attribute using PAP. So, a RADIUS server used for the certificate CN authorization should support the RADIUS “authorize-only” attribute. An LDAP server can also be used for authorization.

IKEv2 EAP Authentication

For IKEv2 EAP-TLS and EAP-PEAP supported by VIA, an EAP-compatible external authentication server is needed to authenticate the credentials provided by the user during the IKEv2 process. For information on authentication server requirements and configuring an authentication server, see Configuring a VIA Server Group for Authenticating VIA Users on page 36 in Chapter 6: Configuring VIA Profiles.

IKEv2-Certs Configuration

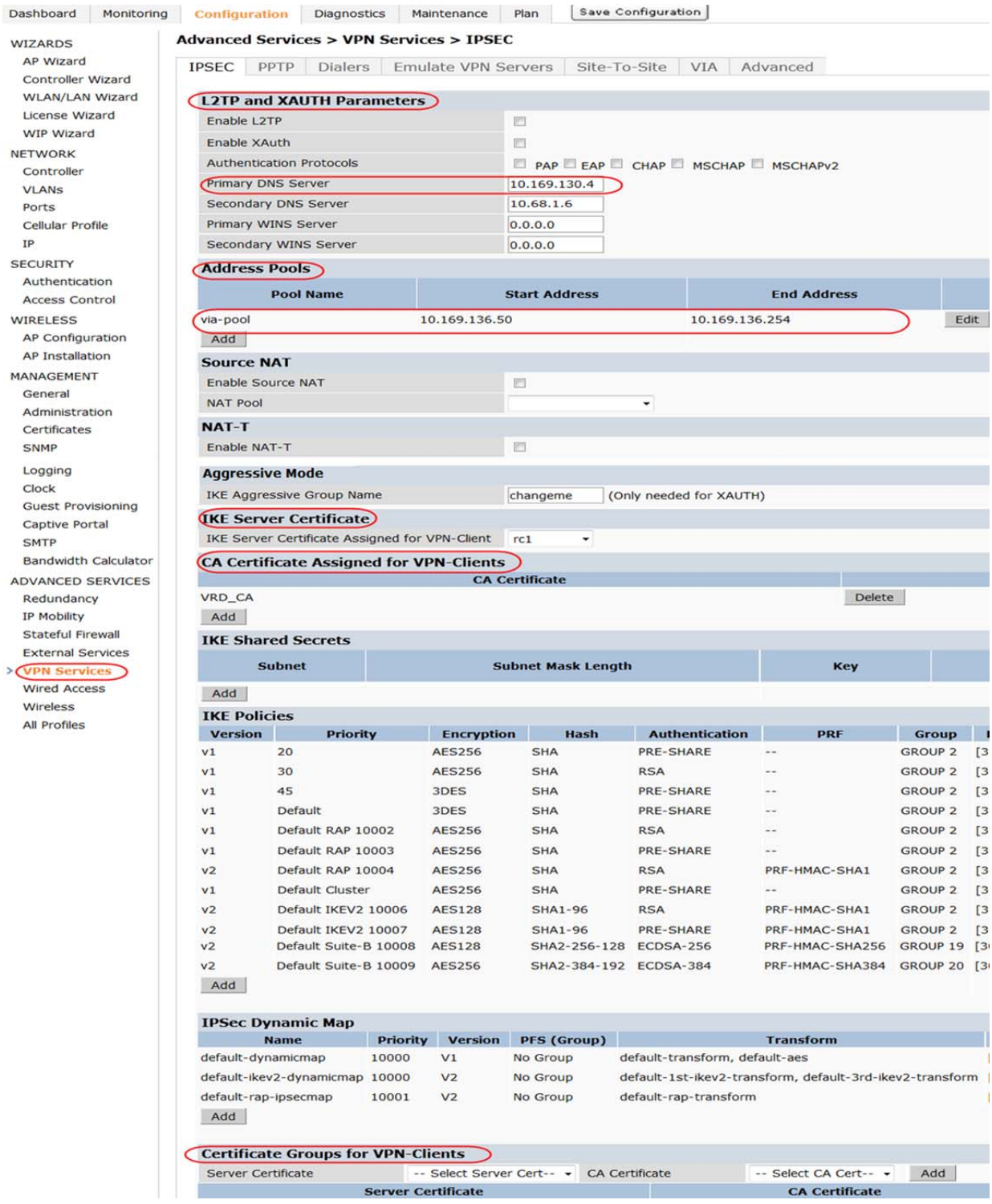

Figure 13 VPN server configuration for IKEv2-Certs

```
!
client configuration dns 10.169.130.4 10.68.1.6
crypto-local isakmp server-certificate "rc1"
crypto-local isakmp ca-certificate "VRD-CA"
!
ip local pool "via-pool" "10.169.138.50" "10.169.138.254"
crypto-local isakmp certificate-group server-certificate rc1-ecc ca-certificate ECC-VRD-CA
!
```

IKEv2-EAP Configuration

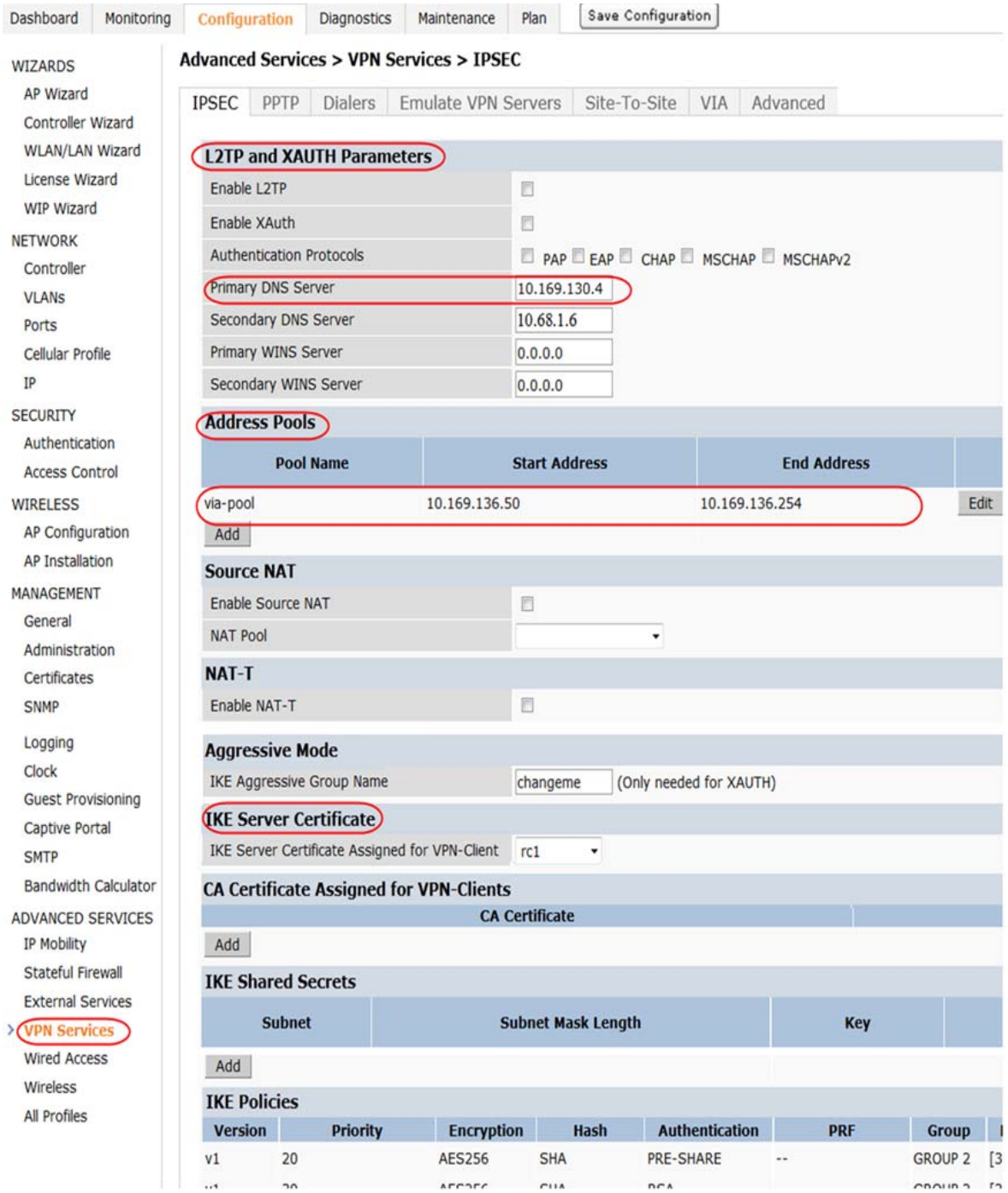

Figure 14 VPN server configuration for IKEv2-EAP

```
!
client configuration dns 10.169.130.4 10.68.1.6
crypto-local isakmp server-certificate "rc1"
!
ip local pool "via-pool" "10.169.138.50" "10.169.138.254"
!
```

IKE Policies and IPsec Maps

The ArubaOS has a predefined list of IKE and IPsec polices (also known as IPsec maps) for different IKE versions. Based on the proposal of the VPN client, the controller dynamically chooses the most appropriate IKE and IPsec policy. Aruba recommends the use of the predefined IKE and IPsec policies for establishing secure IPsec connection to the VPN clients.

In addition to the pre-defined policies, custom IKE and IPsec policies can be created on the ArubaOS. To create a custom IKE and IPsec policy you have to define a number of variables such as the IKE version, encryption type, hashing algorithm, life time, and Diffie-Hellman group. Aruba recommends that you have a good understanding of these variables and their implication before you create custom policies. For information on creating custom IKE and IPsec policies for VPN clients, see the *Aruba 6.1 User Guide* available at the Aruba support site.

Figure 15 IKE and IPsec policies for VIA and VPN clients

Chapter 6: Configuring VIA Profiles

The controller has certain VIA profiles, such as the VIA authentication profile, the VIA connection profile, and the VIA web authentication profile. Each profile plays an important role in authenticating the users and establishing a secure connection back to the corporate resources. To understand the role of each VIA profile, it is important to understand the VIA bootstrapping process.

VIA Bootstrapping

First, the VIA client must be installed on the user device. After the VIA client has been installed on the user machine, the VIA bootstrap process occurs. For information on installing VIA on the end-user device, see Installing the VIA Client on the End-User Device on page 54 The VIA bootstrap process consists of these steps:

1. The VIA client prompts the user for the controller IP address or FQDN and user credentials.
2. The VIA client retrieves the VIA web authentication list and allows the user to select the VIA authentication profile, which will be used to authenticate the user credentials for the configuration download.
3. The VIA client makes an HTTPS POST request to the controller to authenticate the users.
4. If the user is successfully authenticated, the VIA client makes a request to download the VIA configuration. The VIA configuration is tied to the role that is assigned to the user as a part of the authentication process in step 3.
5. If certificates are provisioned in the downloaded VIA configuration, the VIA client requests and checks the CA cert.
6. IKE is performed using the IKE settings received in VIA configuration and an IPsec connection is established using the IPsec settings in the VIA configuration.
7. If the VIA auto upgrade feature is enabled, the VIA client checks for a new VIA image or the external image hosting server. If a new image is available, the VIA client downloads the new image and notifies the user about the pending upgrade. The VIA client upgrades after the user disconnects the current VIA session.

Remember, the VIA client automatically detects whether the user is connected to a trusted or untrusted network by sending a HTTPS HEAD request to the internal IP of the controller <https:// <controller's internal ip>/via >. If the VIA client receives a HTTPS response with the expected X-VIA header, the user is considered to be on a trusted network. An IPsec connection is established only if the user is connected to an untrusted network.

Configuring the VIA User Roles

The VIA user role is the role that is assigned to the users who successfully authenticate through their VIA client. The user role defines the access rights of the users that connect using VIA. Aruba recommends that network administrators configure custom user roles that depict the network access policy of their respective organizations. For information on creating user roles, see the *Aruba Campus Wireless Networks Validated Reference Design*. The ArubaOS has a predefined allow-all role called the default-via-role. All the example configurations in this chapter use this user role.

Figure 16 Predefined default-via-role

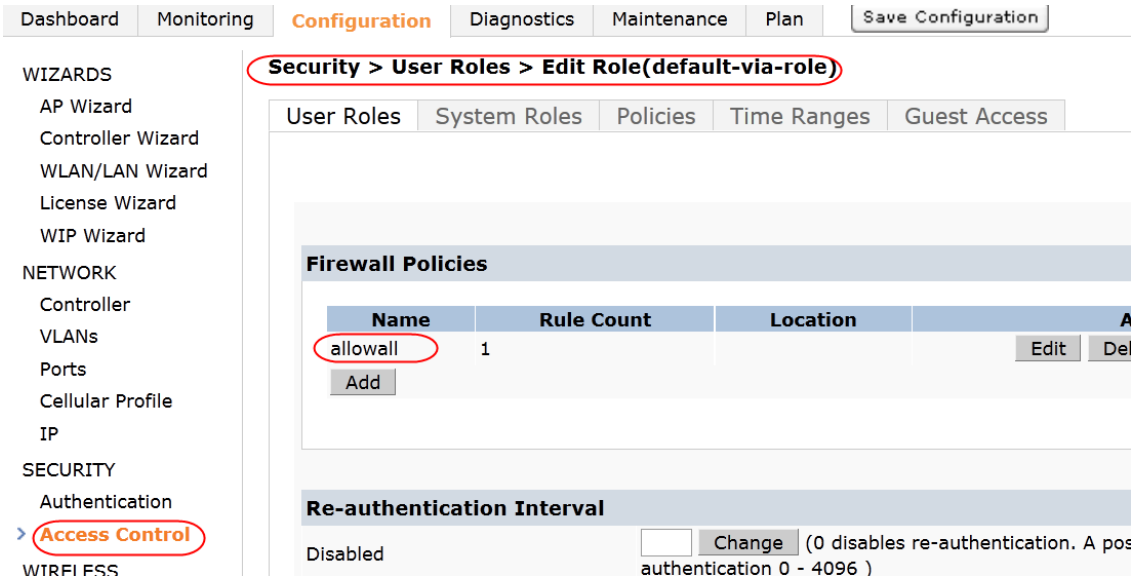

Figure 17 Policies in the default-via-role

Appending VPN Address Pool to the VIA User Role

As discussed earlier, if required, a VPN address pool can be appended to a VIA user role. If a VPN address pool named via-pool is appended to a user role, then all the VIA users in that role are assigned an IP address from the via-pool. For information on configuring VPN address pool, see Address Pools on page 17 in Chapter 5: VPN Server Configuration for VIA.

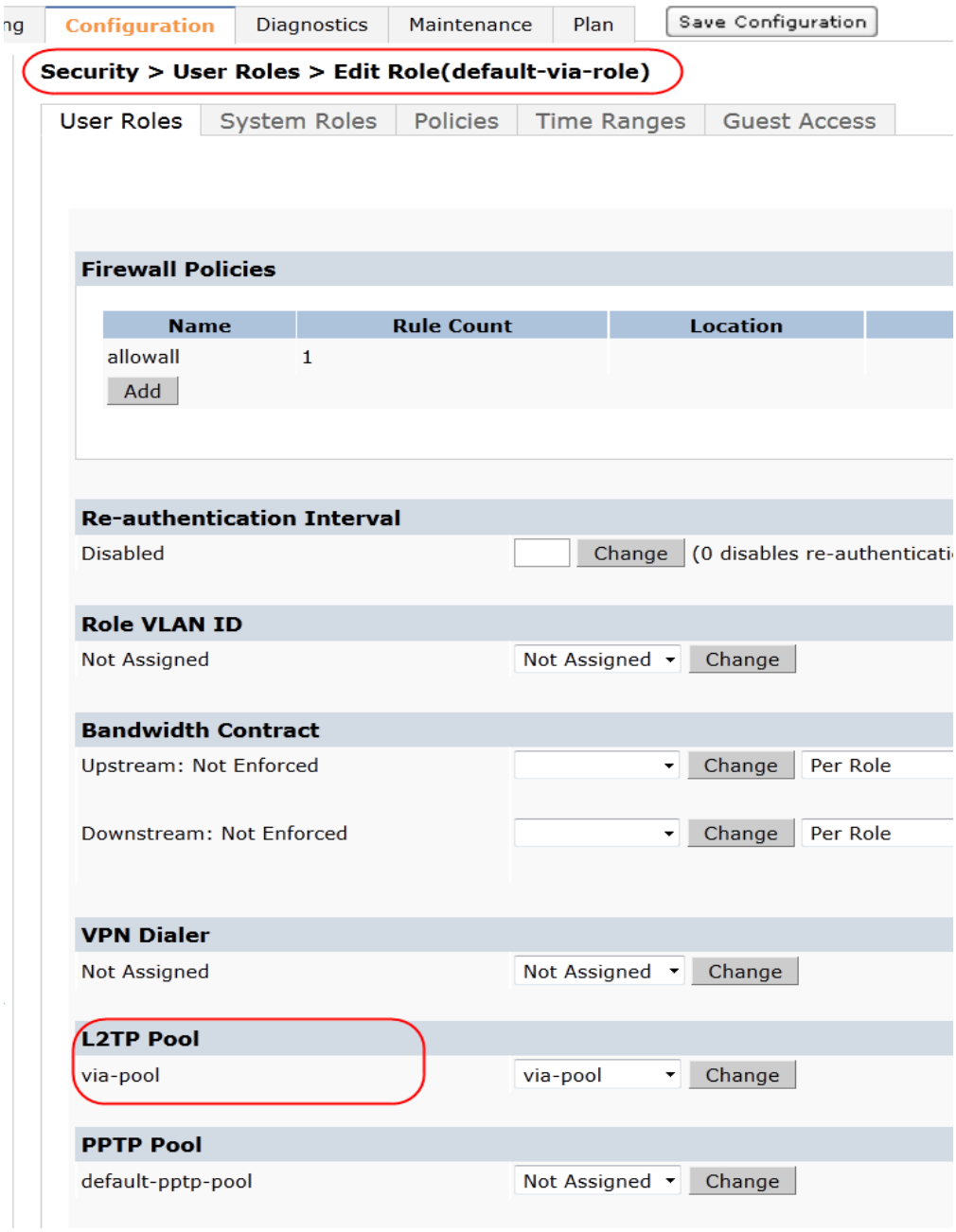

Figure 18 Appending a VPN address pool to the VIA user role

```
!
user-role "default-via-role"
   pool l2tp "via-pool"
!
```

Configuring a VIA Server Group for Authenticating VIA Users

A server group is a collection of servers that are used for authentication. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have different types of authentication servers. For example, you can create a server group that uses an LDAP server as a backup for a RADIUS server.

If a server group has more than one server, the “fail-through” feature can be used to authenticate the users with the other servers in the list if authentication with the first server fails. If the fail-through feature is enabled, it tries to authenticate the users against all the servers in the list until the authentication is successful or until all the servers have been tried. When this feature is disabled, only the first authentication server in the list is used for authenticating the users unless that server is unreachable. Aruba recommends that you consider these facts before you enable this feature:

- Fail-through authentication is not supported for authentication in server groups that consist of external EAP-compliant RADIUS servers, unless authentication is terminated on the controller (AAA FastConnect™). VIA IKEv2-EAP deployments cannot use this fail-through feature because EAP termination is not supported for VIA clients.
- If the server group list is large, this feature can impose a high processing load on the controller. Use dynamic server selection in these situations. For more details about dynamic server selection, see the *ArubaOS 6.1 User Guide* available at the Aruba support site.
- If multiple authentication failures occur, RSA RADIUS server and certain other servers lock out the controller. Do not enable fail-through authentication if these servers are in use.

Authentication Servers for IKEv1 VIA Deployments

For IKEv1 VIA deployments, the internal database or any external server supported by ArubaOS can be used to authenticate the VIA users. If an external RADIUS or TACACS authentication server is used, the controller communicates with them using PAP for these purposes:

- To validate the user credentials submitted on the VIA installer download page of the controller
- To validate the user credentials during the step 3 of VIA bootstrap process
- To validate the user credentials submitted during the XAUTH authentication process. It is important to remember that the username and password submitted by the user is sent to the controller, across the WAN, by the VIA client inside the secure ISAKMP tunnel formed during phase 1 of IKEv1.

So, an external RADIUS or TACACS server used for IKEv1 VIA deployments should support PAP authentication. The PAP requirements discussed here do not apply for external LDAP servers used for VIA authentication.

Authentication Servers for IKEv2 VIA Deployments

For IKEv2 EAP deployments, an internal database cannot be used as the authentication server because EAP termination is not supported for IKEv2 clients. Only an EAP-compliant external server can be used for authenticating IKEv2 EAP clients during the IKE authentication process. Note that IKEv2 deployments using X.509 certificates can use non-EAP-compliant external authentication servers or the internal database for authentication. Like IKEv1 deployments, an external RADIUS

authentication server used for IKEv2-Certs or IKEv2-EAP deployments should also be PAP compatible because the controller uses PAP for these purposes:

- To validate the user credentials submitted on the VIA installer download page
- To validate the user credentials during the step 3 of VIA bootstrap process

For IKEv2 deployments using X.509 certificates, the external server should support authorization services using username if the “check certificate CN against an authentication server” parameter is enabled. For more information, see Check Certificate Common Name Against AAA Server on page 27 in Chapter 5: VPN Server Configuration for VIA.

Table 5 summarizes the authentication servers supported for the various IKE flavors.

Table 5 Authentication Server Support for IKE

Type of IKE	Internal Database	External Database
IKEv1-PSK	Supported	Supported (The external server should support PAP authentication.)
IKEv1-Certs	Supported	Supported (The external server should support PAP authentication.)
IKEv2-Certs	Supported	Supported (The external server should support PAP authentication, but it is not required to be EAP-compliant.)
IKEv2 -EAP-TLS	Not Supported	Supported (The external server should be EAP-compliant and support PAP authentication.)
IKEv2-EAP-MSCHAPv2	Not Supported	Supported (The external server should be EAP-compliant and support PAP authentication.)

Table 6 summarizes a server group named NPS, which defines an EAP and PAP-compliant RADIUS server called NPS1.

Table 6 NPS Server Group

Server Group	RADIUS Server	RADIUS Sever IP	RADIUS Authentication Port	RADIUS Accounting Port
NPS	NPS1	10.169.130.20	1812	1813

NOTE

If the RADIUS server is configured to return specific attributes for the users after authentication, then the server-derived role that corresponds to the returned attributes can be configured under server groups. For information about configuring a server-derived role, see the *ArubaOS 6.1 User Guide* available on the Aruba support site. When using server derived roles, the derived role should also have a VIA connection profile attached to it. For details on VIA connection profile, see Configuring the VIA Connection Profile on page 42.

Server Group Configuration

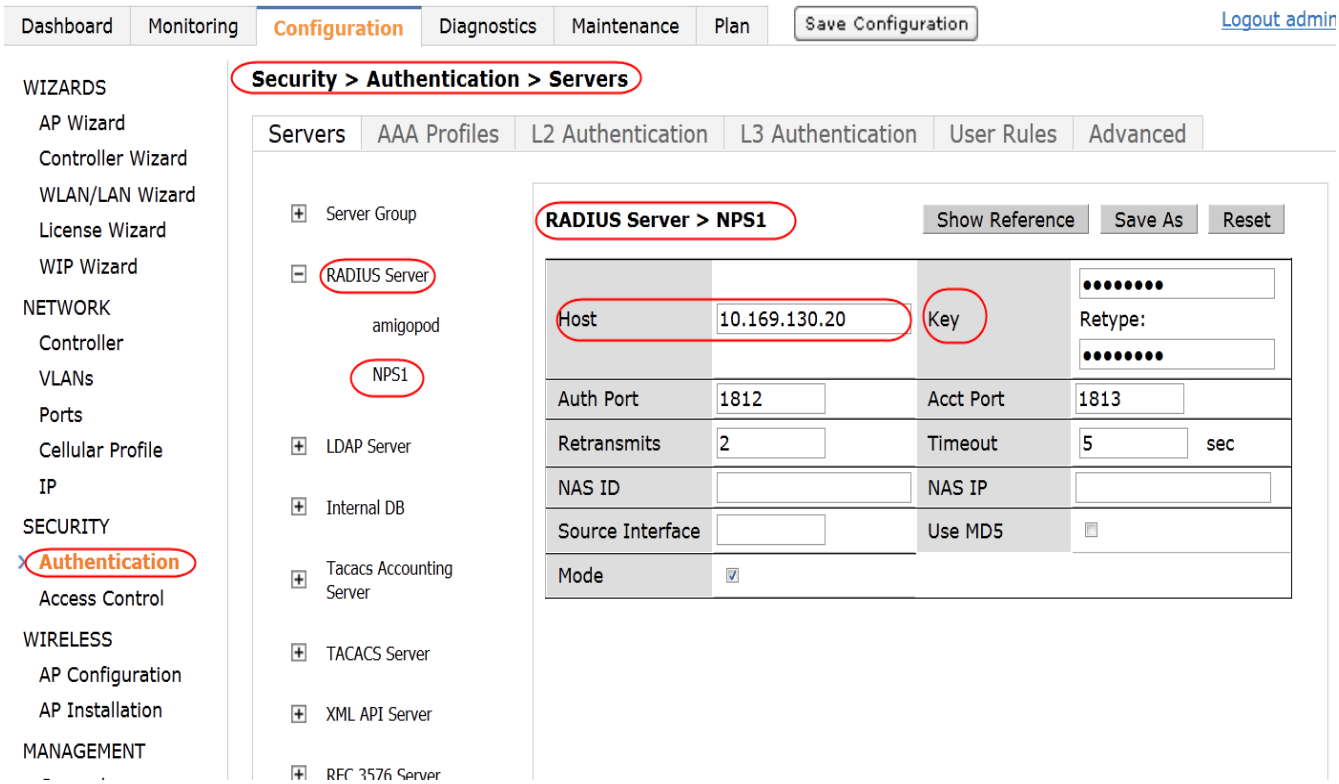

Figure 19 NPS1 RADIUS server

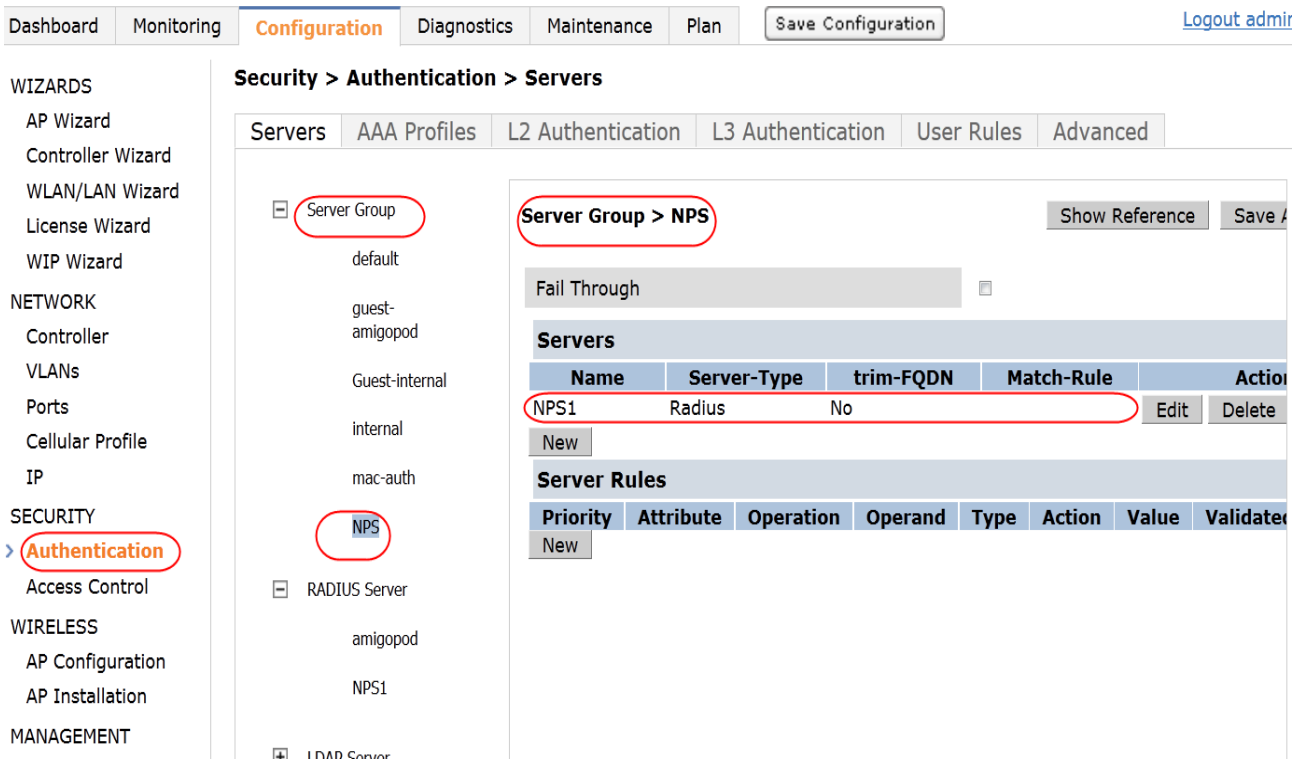

Figure 20 NPS server group

```
!
aaa authentication-server radius "NPS1"
    host "10.169.130.20"
    key **********
    acctport 1813
    authport 1812
!

aaa server-group "NPS"
    auth-server NPS1
```

Configuring the VIA Authentication Profile

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile. The VIA authentication profile is a critical part of VIA configuration and it is used for these purposes:

- To determine the authentication server for the XAUTH authentication phase of IKEv1 and EAP authentications of IKEv2.
- To determine the authentication server for the VIA web authentication. The VIA authentication profile is an integral part of the VIA web authentication, which determines the authentication sever used for the step 3 of VIA bootstrap process and for authenticating users on the VIA installer download page of the controller. For more information on VIA web authentication see Configuring the VIA Web Authentication on page 51.

To configure a VIA authentication profile, you require these:

- a VIA user role
- an authentication server group

Table 7 summarizes a VIA authentication profile named via-auth.

Table 7 VIA Authentication Profile

Profile Name	Default Role	Server Group
via-auth	default-via-role	NPS

VIA Authentication Profile Configuration

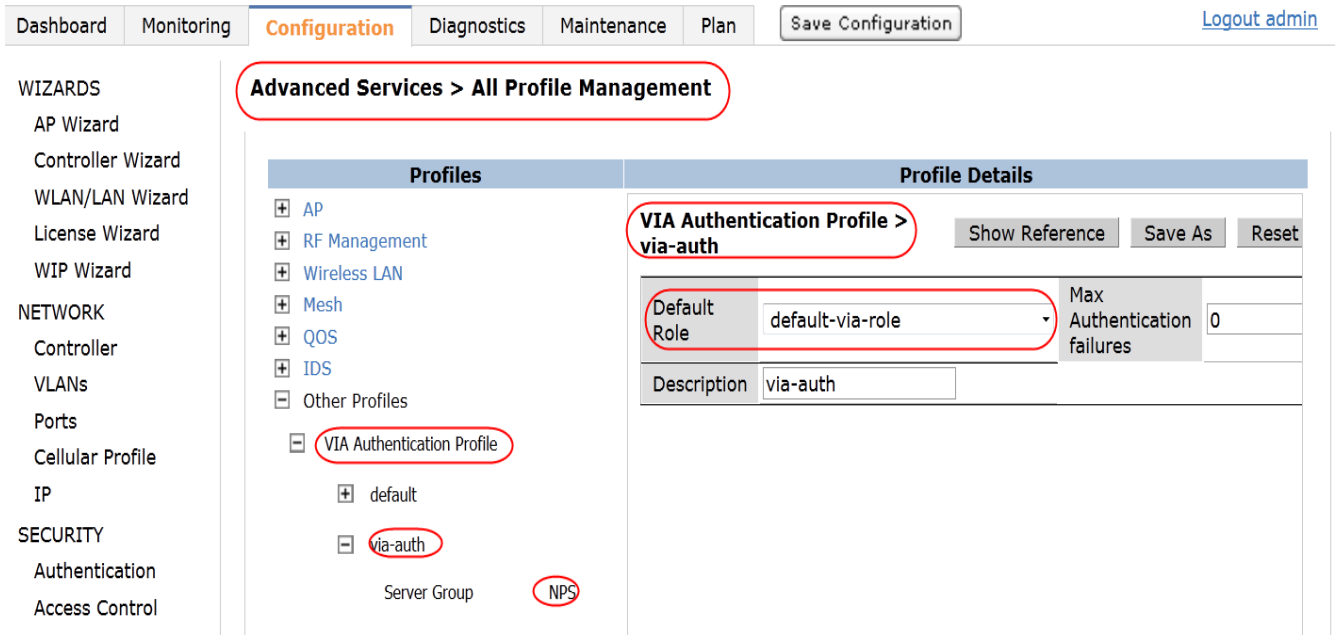

Figure 21 via-auth profile

```
!
aaa authentication via auth-profile "via-auth"
   default-role default-via-role
   desc via-auth
   server-group "NPS"
!
```

Configuring the VPN Authentication Profile to Support VIA for Mac OS

Currently, VIA 1.0 for Mac OS behaves differently than VIA for iOS and VIA for Windows. The Mac OS VIA clients are identified by the controller as generic VPN clients and not as VIA clients during the IKE process. This does not compromise security, but it requires an additional configuration.

For iOS and Windows VIA clients, the VIA authentication profile is used for authentication during the IKE process and the VIA web authentication list is used during the step 2 of VIA bootstrap process. For

Mac OS VIA clients, the web authentication list used during the step 2 of VIA bootstrap process is the same as that for iOS and Windows VIA clients. However, during the IKE authentication process, the VPN authentication profile is used instead of the VIA authentication profile to authenticate the Mac OS VIA users. This behavior is due to the fact that the Mac OS VIA clients are detected as generic VPN clients. So, deployments that support Mac OS VIA clients should configure the default VPN authentication profile with additional information. In these deployments, the default VPN authentication profile must include the appropriate user role and server group that must be used for authenticating VIA clients during the IKE process.

Remember that a VIA web authentication list configured with the appropriate VIA authentication profile is required for Mac OS VIA clients too. All the controller configurations, except the configuration of the default VPN authentication profile, are the same for Mac OS VIA clients and Windows and iOS VIA clients.

VPN Authentication Profile Configuration

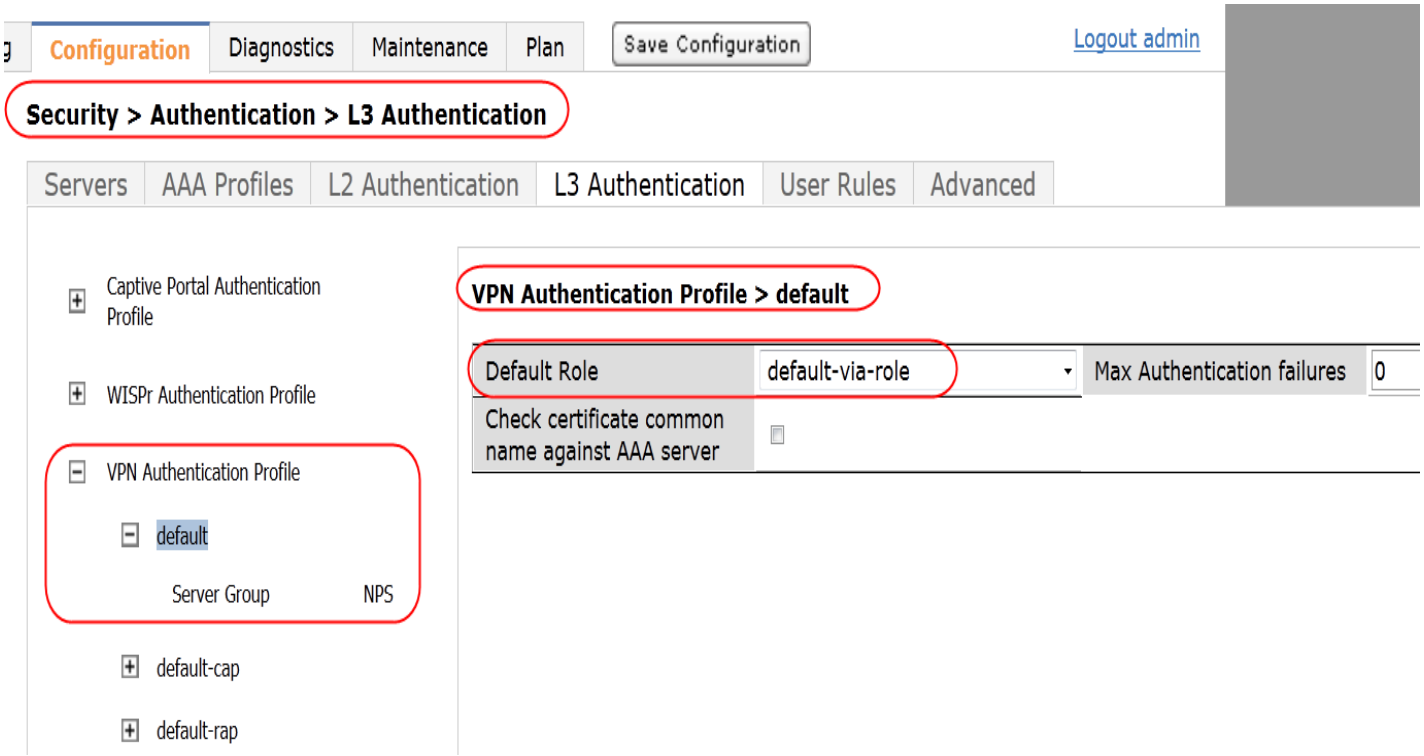

Figure 22 VPN authentication profile for Mac OS VIA

```
!
aaa authentication vpn "default"
   server-group "NPS"
   default-role default-via-role
!
```

In summary, these additional configuration tasks are needed to support VIA 1.0 for Mac OS:

- Enabling the L2TP parameter in the L2TP and XAUTH settings of the VPN server module
- Choosing an authentication protocol in the L2TP and XAUTH settings of the VPN server module
- Configuring the default VPN authentication profile with appropriate server group and user role
- Opening additional ports such as UDP port 500 and IP protocol 50 on all the firewalls that lead up to the controller on which VIA terminates

Configuring the VIA Connection Profile

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection profile contains all the details required for the VIA client to establish a secure IPsec connection to the controller. A VIA connection profile also defines other optional parameters. Such optional parameters can be client auto-login, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

A VIA connection profile is always associated to a user role, and all users that belong to that role use the configured settings. When a user authenticates successfully to a server in an authentication profile, the VIA client downloads the VIA connection profile that is attached to the role assigned to that user.

Table 8 summarizes the various parameters of a VIA connection profile and shows example settings for different IKEv1 and IKEv2 client authentication methods.

Table 8 VIA Connection Profile

Parameter	Purpose	Settings for IKEv1 and IKEv2
VIA Controller	This parameter has these fields: • **Controller Hostname/IP Address:** Add the public IP or DNS hostname of the controller. This is the host name or IP address that the users enter as the remote server information on the VIA client (Step 1 of the VIA bootstrap process). • **Controller Internal IP Address:** Add the IP address of any of the internal VLAN interfaces of the controller. This IP address should not be reachable from the public Internet. The VIA client uses this IP address to determine whether or not the user is connected to a trusted network. • **Controller Description:** Add a human-readable description of the controller. More than one VIA controller can be added to the list.	• Hostname /IP address = 192.168.168.2 (public IP of the controller). The VRD lab uses a simulated Internet, so a private IP is indicated. In actual deployments, a public IP or a publically resolvable DNS name should be used. See the Base designs VRD for the VRD lab setup. • Internal IP address = (10.169.131.6) • Description = via-controller
VIA Authentication Profiles to provision	This VIA authentication profile is used to determine the authentication server used for the IKE authentication process. If more than one VIA authentication profile is added to this list, the users can choose the VIA authentication profile to be used during IKE authentication. If no VIA authentication profile is defined, the users are authenticated against the server group that is specified by the default VIA authentication profile (predefined).	via-auth

Table 8 VIA Connection Profile (Continued)

Parameter	Purpose	Settings for IKEv1 and IKEv2
VIA tunneled networks	When split-tunneling is enabled, the VIA client tunnels traffic to the controller for all the network destinations (IP address and netmask) listed in this parameter. All other network destinations are bridged appropriately on the client. If split-tunnel is disabled, all the traffic is tunneled to the controller irrespective of the destination.	• IP address = 10.0.0.0 • network mask = 255.0.0.0
VIA Client WLAN profiles	This is the list of the VIA client WLAN profiles that are pushed to the client machines that use Windows Zero Config (WZC) on Windows and networksetup on Mac OS X to configure or manage their wireless networks.	—
VIA IKEv2 Policy	This IKE policy is used for IKEv2 connections by the VIA client. Remember that IKEv2 using PSK is not supported for VIA.	***IKEv2 user certs / EAP-TLS / EAP-MACHAPv2:*** Default IKEV2 10006 **(pre-defined)** PSK is not supported for IKEv2 VIA clients, so you must ensure that the authentication type for custom IKEv2 Policy is set to RSA.
VIA IKE Policy	This IKE policy is used for IKEv1 connections by the VIA client. This policy determines whether IKEv1 phase 1 authentication uses PSK or certificates.	***IKEv1-PSK:*** 20 – AES256/SHA/PSK/ Group 2/ [300 - 86400] **(pre-defined)** ***IKEv1-Certs:*** 30 – AES256/SHA/RSA/ Group 2/ [300 - 86400] Remember that the authentication type of the IKE policy determines whether IKEv1 phase 1 uses PSK or certificates.
Use Windows Credentials	This parameter determines whether the Windows credentials are used automatically to login to VIA. If enabled, the single sign-on feature can be utilized by remote users to connect to internal resources. Default: Enabled	enabled
Enable IKEv2	This parameter enables or disables IKEv2.	enabled (required only for IKEv2)
Use Suite B cryptography	This parameter enables or disables Suite B cryptographic methods.	disabled
IKEv2 Authentication method	This parameter indicates the IKEv2 client authentication method. It can be one of these settings: • user-cert • EAP-TLS • EAP-MSCHAPv2 Remember that EAP termination on the controller is not supported.	***IKEv2 -Certs:*** user-cert ***IKEv2-EAP-TLS:*** EAP-TLS ***IKEv2-EAP-MSCHAPv2:*** EAP-MSCHAPv2
VIA IPsec V2 Crypto Map	This IPsec map is used by IKEv2 VIA client to connect to the controller.	default-ikev2-dynamicmap/ 10000 – [300 - 86400]/ PFS-N/ default-1st-ikev2-transform/ default-3rd-ikev2-transform **(predefined)**
VIA IPsec Crypto Map	This IPsec map is used by IKEv1 VIA client to connect to the controller.	default-dynamicmap/ 10000 – [300 - 86400]/ PFS-N/ default-transform/ default-aes **(predefined)**

Table 8 VIA Connection Profile (Continued)

Parameter	Purpose	Settings for IKEv1 and IKEv2
VIA Client Network Mask	This network mask is set on the client after the VPN connection is established. Default: 255.255.255.255	255.255.255.255
VIA Client DNS Suffix List	This is the DNS suffix that is set on the client after the VPN connection is established.	rde.arubanetworks.com
VIA Support Email Address	This is the support email address to which VIA users send client logs using the VIA client. For information on sending VIA logs using the VIA client, see Chapter 8: Establishing VIA Connection.	via-support@rde.arubanetworks.com
VIA external download URL	The VIA installer can be hosted on an external server other than the controller for download by the VIA client during VIA upgrades and by the end users. If the VIA installer is hosted on an external server, this parameter should be configured to redirect the VIA clients to the external URL for the upgrade process. If this parameter is not configured, the VIA clients automatically go to ***https:// <controller IP address or FQDN >/via*** for upgrades.	branch.rde.arubanetworks.com/via
Content Security Gateway URL	When split-tunnel mode is enabled, traffic to external websites is inspected by the CSS. For details on CSS, see the *ArubaOS 6.1 User Guide* available at the Aruba support site.	—
Enable Content Security Services	This parameter enables the CSS. The CSS requires the CSS licenses. For details on CSS, see the *ArubaOS 6.1 User Guide* available at the Aruba support site.	disabled
Client Auto-Login	Enabling client auto-login makes the VIA client detect untrusted network and connect automatically. If you disable auto-login, VIA stays idle after it comes up and the user has to manually click Connect to establish a VPN connection even though an untrusted network is detected. Default: Enabled	enabled
Allow client to auto-upgrade	This parameter allows the VIA client to automatically upgrade if a newer version of VIA is available on the controller. Default: Enabled	enabled
Enable split-tunneling	When enabled, all traffic to the VIA tunneled networks goes through the controller and the rest is bridged directly on the client. If split-tunnel is disabled, all the traffic is tunneled to the controller irrespective of the destination.	enabled
Allow client-side logging	This parameter determines whether client side logging is allowed or not. If enabled, VIA client collects logs that can be sent to the support email address for troubleshooting. Default: Enabled	enabled

Table 8 VIA Connection Profile (Continued)

Parameter	Purpose	Settings for IKEv1 and IKEv2
Allow user to save passwords	This parameter determines whether the users can save the passwords entered in VIA or not. If this is enabled, the user credentials that were able to successfully establish a VIA connection are saved securely until VIA is uninstalled or until IKE authentication fails with stored credentials. If this option is disabled, VIA prompts for credentials every time it establishes a connection. If secure tokens such as the RSA tokens are used for authentication, disable this option to prompt the user for a password/token for each connection attempt. Default: Enabled	enabled
Lockdown all settings	This parameter locks all the configuration options available on the end-user VIA client. If this option is enabled, a VIA user can only connect, disconnect or send logs. Diagnostics such as traceroute and ping can still be used, but no settings can be changed. **NOTE:** This option is available in VIA 2.1 with ArubaOS 6.1.3.1 and later.	disabled
Enable Controllers load balancing	This parameter enables load balancing of VIA clients by randomly choosing a controller from the list of available VIA controllers that can be used for connection. This feature does not take the current load of the controller into account. **NOTE:** This option is available in VIA 2.1 with ArubaOS 6.1.3.1 and later.	enabled
Validate Server Certificate	If enabled, the VIA client validates the server certificate presented by the controller during the IPsec process. Remember that to validate the server certificate, the CA that signed the controller certificate should be a trusted CA in the client certificate store. Default: Enabled	enabled
VIA max session timeout	This parameter defines the maximum time, in minutes, allowed before the VIA session is disconnected. Default: 1440 min	1440
VIA Logon Script	This parameter specifies the name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside on the client computer.	__
VIA Logoff Script	This parameter specifies the name of the logoff script that must be executed after VIA tears down a secure connection. The logoff script must reside on the client computer.	__
Maximum reconnection attempts	This parameter defines the maximum reconnection attempts by the VIA client. If the reconnection attempt is exceeded, the VIA client becomes idle. However, if the connection attempt fails due to an IKE authentication failure error, then the user is prompted to reenter username and password. Default: 3	3

Table 8 VIA Connection Profile (Continued)

Parameter	Purpose	Settings for IKEv1 and IKEv2
Allow user to disconnect VIA	This feature determines whether the users can disconnect VIA or not. Remember that a user with administrative rights to a laptop can always uninstall VIA or disable the Aruba service running on the laptop. For users with restricted access to the laptops, disabling this feature ensures that users cannot disconnect VIA. Default: enabled	disabled
Comma separated list of HTTP ports to be inspected (apart from default port 80)	Traffic to the specified list of ports is verified by the CSS provider.	__
Keep VIA window minimized	When this feature is enabled, the VIA client is minimized to the system tray during the connection phase. Currently, this feature is applicable only for VIA clients installed on Microsoft Windows laptops. Default: disabled	enabled

Separate VIA connection profiles are not required for IKEv1 and IKEv2. A single VIA connection profile can be configured with both IKEv1 and IKEv2 settings. Depending on the capabilities of the VIA client, either an IKEv1 or an IKEv2 connection is established. By default, the VIA 2.x clients first attempt IKEv2 if the “Enable IKEv2” option is set in the VIA connection profile. If the VIA client is not able to establish an IKEv2 connection, it falls back to using IKEv1. All VIA 1.x clients directly establish an IKEv1 connection.

VIA Connection Profile Configuration

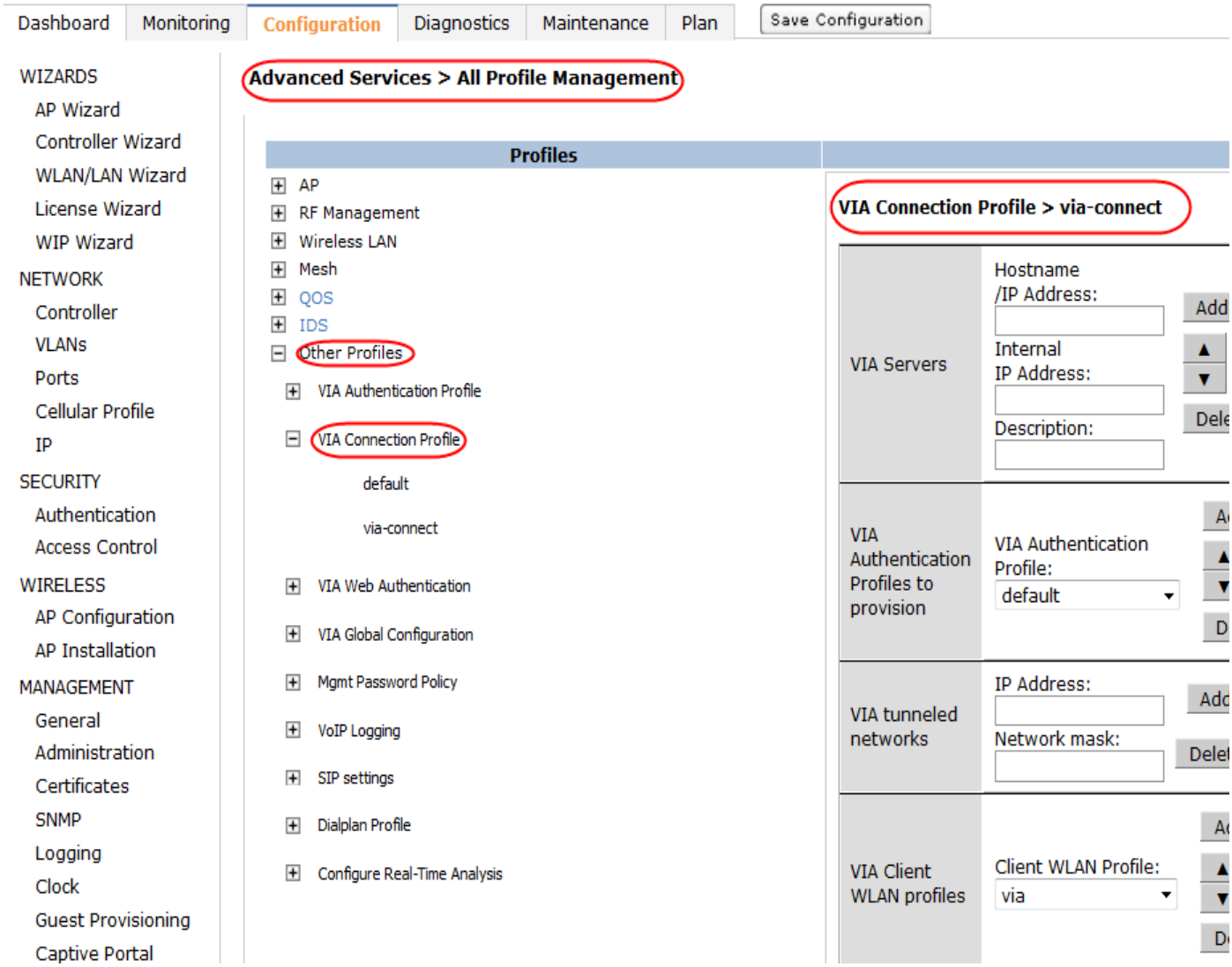

Figure 23 VIA connection profile

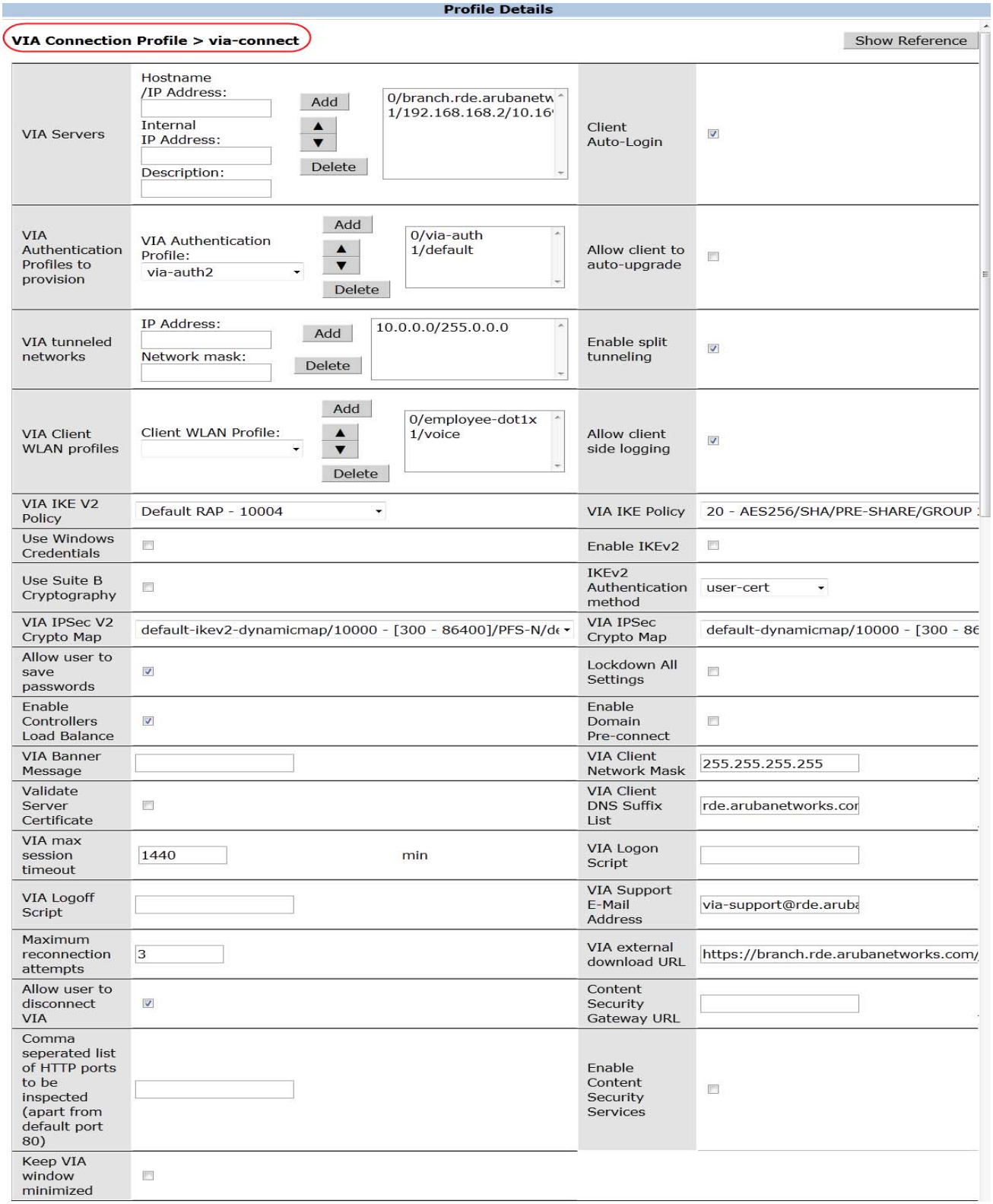

Figure 24 via-connect VIA connection profile (ArubaOS 6.1.3.1)

```
!
aaa authentication via connection-profile "via-connect"
   server addr "192.168.168.2" internal-ip 10.169.131.8 desc "via-controller" position 0
   auth-profile "via-auth" position 0
   tunnel address 10.0.0.0 netmask 255.0.0.0
   split-tunneling
   client-wlan-profile "employee" position 0
   ikev2-policy "10006"
   ike-policy "20"
   ikev2-proto
   ikev2auth eap-mschapv2
   dns-suffix-list "rde.arubanetworks.com"
   support-email "via-support@rde.arubanetworks.com"
   ext-download-url "https://branch.rde.arubanetworks.com/via"
   auto-login
   client-logging
   windows-credentials
   controllers-load-balance
   save-passwords
   validate-server-cert
   allow-user-disconnect
   minimized
!
```

Attaching the VIA Connection Profile to a User Role

The VIA connection profile that the VIA client has to download should be attached to the user role that is assigned to the user. In the example configuration described in Configuring the VIA Authentication Profile on page 39 the users authenticating to the “via-auth” authentication profile are assigned the default-via-role. To assign the “via-connect” connection profile to these users, the “via-connect” connection profile should be attached to the default-via-role.

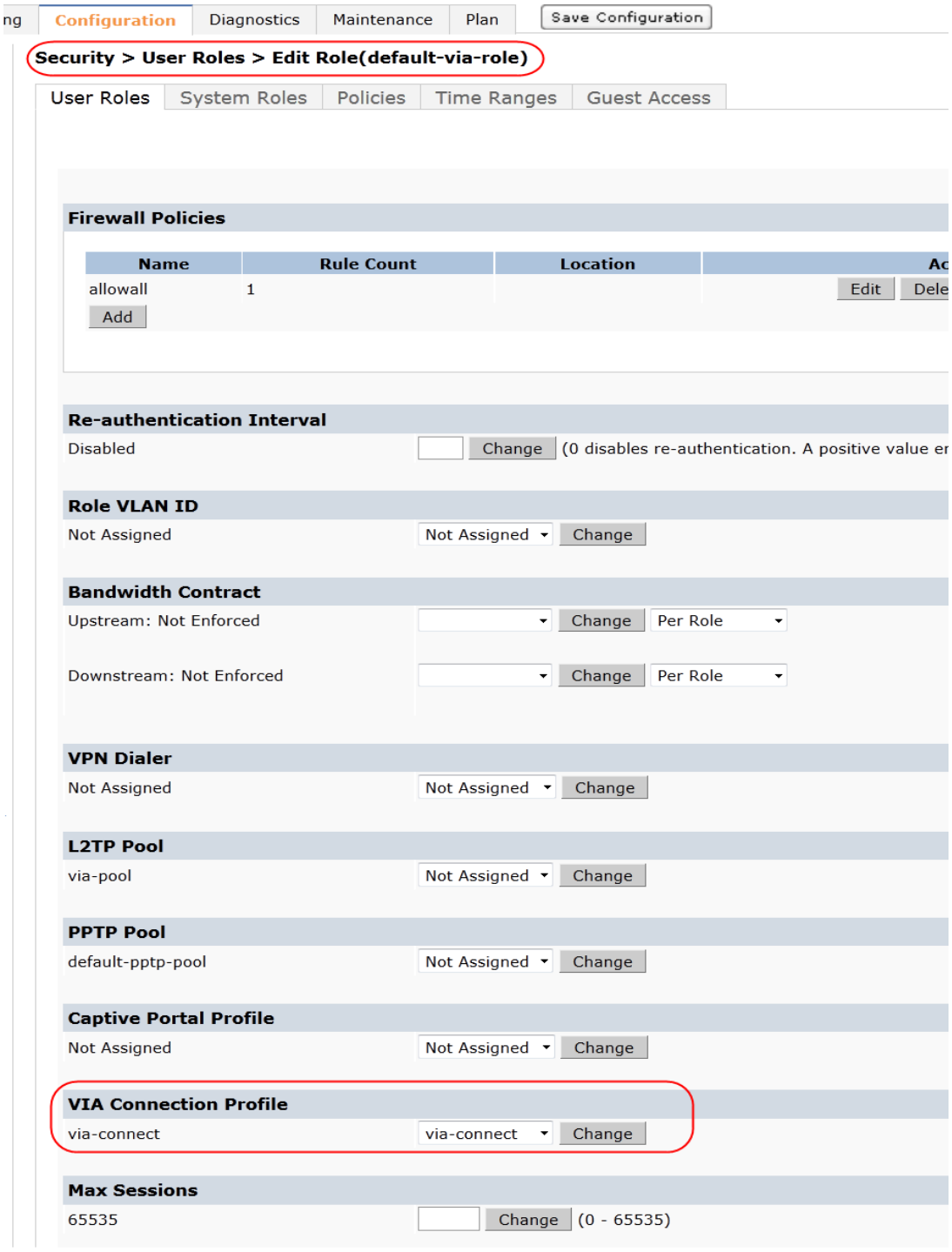

Figure 25 Attaching via-connect connection profile to the default-via-role

```
!
 user-role "default-via-role"
   via "via-connect"
!
```

Configuring the VIA Web Authentication

The VIA web authentication is a list of VIA authentication profiles. The web authentication list allows the users to login to the VIA download page *<https://<controller IP address>/via>* to download the VIA client. To successfully login to the VIA download page, the users must authenticate successfully against the VIA authentication profile in the list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile before authenticating to the VIA installer download page.

The web authentication list also is used during the initial user authentication process that determines the VIA user role (step 3 in the VIA bootstrap process). The VIA users are authenticated against the authentication server defined by the VIA authentication profile in the VIA web authentication list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile during step 2 of the VIA bootstrap process.

ArubaOS has a default web authentication list to which multiple VIA authentication profiles can be added. Additional VIA web authentication lists cannot be created. To configure the VIA web authentication list, add one or more VIA authentication profiles to the default web authentication list and order them according to the priority. Configuring more than one VIA authentication profile in the VIA web authentication list allows the users to use the backup authentication server if the primary server becomes unavailable temporarily.

VIA Web Authentication Configuration

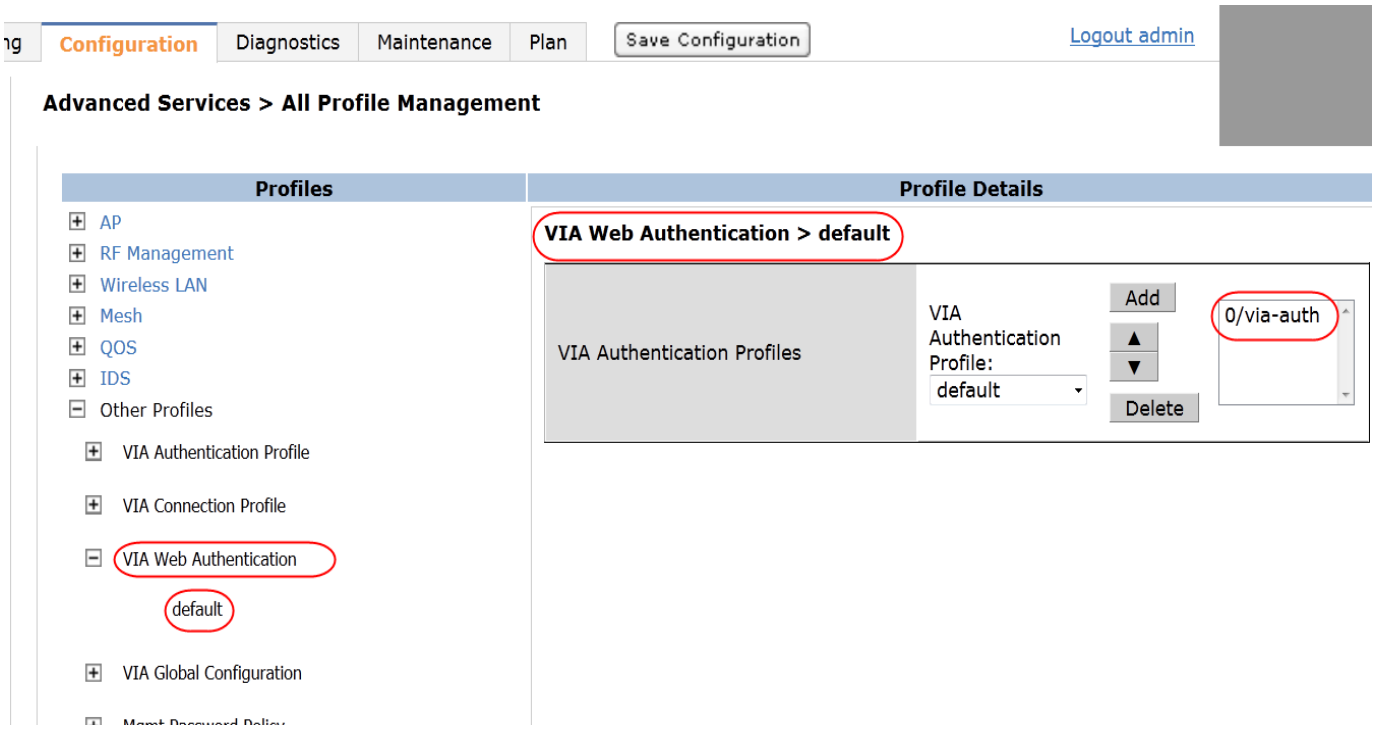

Figure 26 VIA web authentication list

```
!
aaa authentication via web-auth "default"
    auth-profile "via-auth" position 0
!
```

Uploading the VIA Installer to the Controller or an External Server

The VIA image version is independent of the ArubaOS version on the controller. This fact eliminates the need to downgrade or upgrade the controller when a different version of VIA is used. As mentioned earlier, separate VIA installers are needed for Apple Mac OS X, Apple iOS devices, and Windows 32-bit and 64-bit operating systems. The Apple iOS VIA installer is available in the Apple App store. All other VIA installers are available at the Aruba support site and they should be uploaded to the controller or an external hosting server for download by the users. If the controller is used to host the VIA images, the controller automatically detects the operating system of the device that is connecting to the VIA download page. The controller learns the parameters of the web browser used to connect to the VIA download page to determine the operating system. After the users login to the VIA download page, the controller presents the appropriate VIA installer image. After the initial installation, the VIA clients are capable of automatically upgrading their image (depends on VIA connection profile setting). If the network administrator uploads a new version of VIA installer to the controller or to the server indicated by the VIA external download URL parameter of the VIA connection profile, the VIA clients automatically upgrade their image.

If a user with a 64-bit Windows computer connects to the default VIA download page on the controller using a 32-bit browser the user is presented with the 32-bit image. However, the 32-bit image cannot be installed on the 64-bit Windows computer. A simple workaround is for the user to browse to https://<controllerIP or FQDN>/via/download?os=win64 to download the 64-bit installer. Alternatively, a custom HTML page that displays all the available images can be uploaded as the VIA welcome page. For information on customizing the VIA welcome page, see Customizing the VIA Welcome Page for VIA Web Login on page 65 in Chapter 7: Optional VIA Configuration and Appendix C: Custom VIA Welcome Page.

Figure 27 Uploading a VIA installer

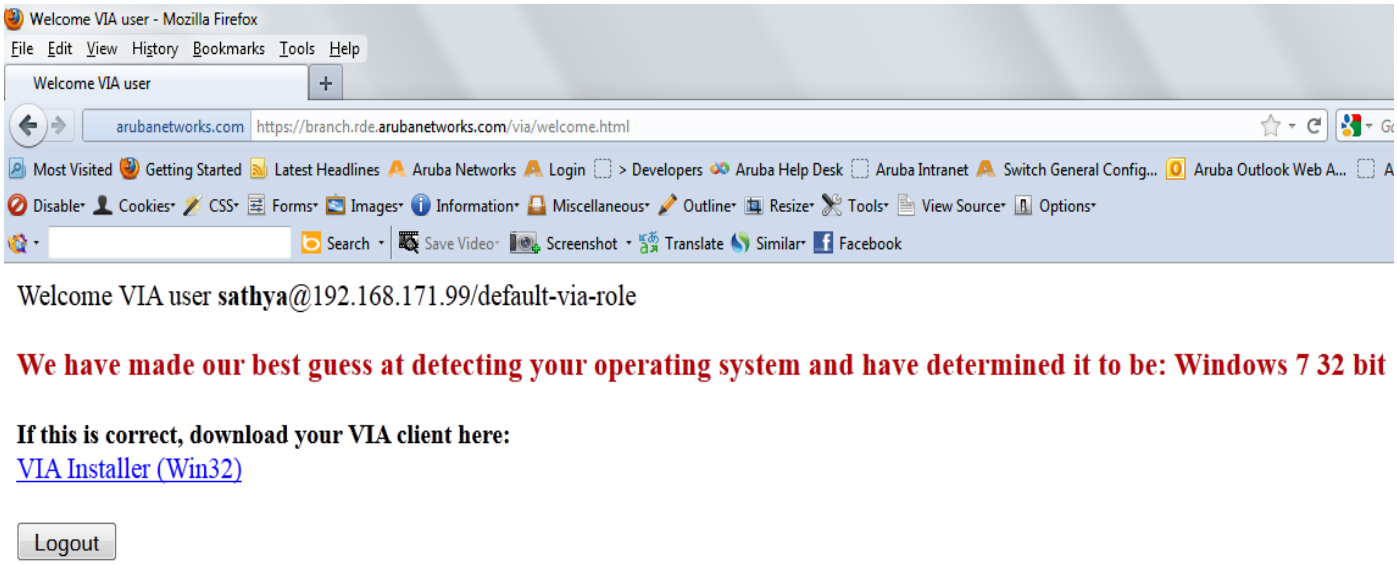

Figure 28 Controller automatically detects the operating system of the device on the VIA welcome page

Installing the VIA Client on the End-User Device

VIA can be downloaded from the controller and installed by the user, or it can be pushed to the user machine using system management services. For information on the VIA installer options available for Windows VIA installations, see Appendix A: Installer Options for the VIA Microsoft Installer (MSI) Package. The end users can download VIA from the URL <*https://< controller>/via/*>. When the controller is used for distributing the VIA installer, users must pass authentication to download the installer. As discussed earlier, the VIA web authentication list is used for authenticating the users on the VIA download page. The controller automatically detects the operating system of the device that is connecting to the VIA download page and presents the appropriate VIA installer. If required, the VIA installer can also be hosted on an external web server for download.

To run the downloaded VIA installer on a Microsoft Windows computer or an Apple Mac Book, the users require these access rights on the device:

- For Microsoft Windows computers, the users need administrative rights for the initial installation because VIA changes the network stack in the system. Thereafter, users do not require administrative rights for connecting, downloading profiles, or upgrading VIA.
- For Apple Mac Books, the users are prompted for the root password during initial VIA installation and for downloading profiles. The users are not prompted for root password for initiating a VIA connection.

Chapter 7: Optional VIA Configuration

The configurations discussed in the previous chapters are essential for establishing a secure connection using VIA. In addition to those configurations, VIA supports other features and customization options. This chapter explains these optional configurations in detail.

Configuring SSL Fallback for VIA

Some network firewalls block UDP ports 4500 and 500 that are essential to establish an IPsec connection. If a user is connected to such a network, the IPsec connection that is initiated by VIA fails. In these situations, the SSL fallback option of VIA can take advantage of the UDP port 443 (used for HTTPS) allowed by almost all firewalls. If the SSL fallback option is enabled, it allows VIA to connect securely to the controller by wrapping the IPsec packets in an SSL header.

During SSL fallback, each VIA client consumes two IPsec tunnels on the controller. If SSL fallback is enabled, each VIA client accounts for two IPsec tunnels toward the controller IPsec limit calculation. The SSL fallback can be enabled or disabled in the VIA global configuration.

NOTE

Currently, SSL fallback option is available only for VIA IKEv1 deployments.

SSL Fallback Configuration

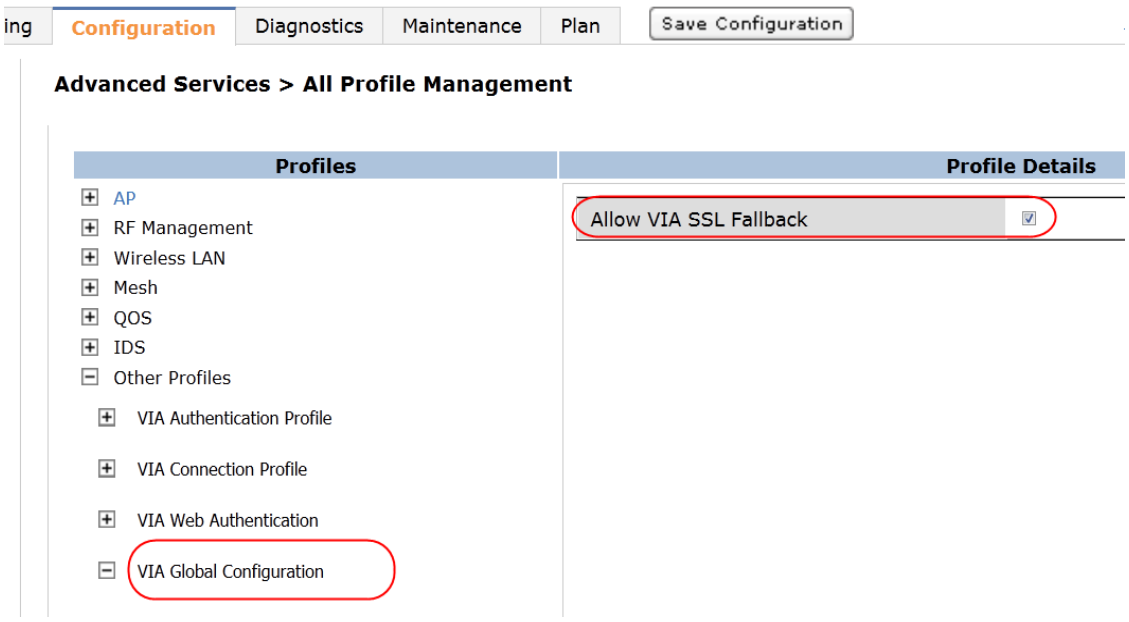

Figure 29 VIA SSL fallback

```
!
aaa authentication via global-config
   ssl-fallback-enable
!
```

Configuring VIA Client WLAN Profiles

VIA client WLAN profiles can push wireless local area network (WLAN) profiles to Windows laptops that use the Microsoft Windows Wireless Zero Config (WZC) service to configure and maintain their wireless networks. For laptops that run Mac OS X, VIA pushes the WLAN profiles using the networksetup system utility. After the WLAN profiles are pushed to end-user laptops, they are automatically displayed as an ordered list in the preferred networks. Two steps are needed to push the WLAN profiles to end-user laptops:

- Defining the required VIA client WLAN profiles
- Adding the VIA client WLAN profiles to the VIA connection profile that is assigned to the VIA users

Defining the VIA Client WLAN Profile

Each VIA client WLAN profile is considered a container that includes an SSID profile. This SSID profiles defines the name, authentication type, and encryption type of the WLAN profile that is pushed to the end user. In addition to the SSID profile, the VIA client WLAN profile defines a number of parameters related to the 802.1X, such as EAP type, certificate options, and inner EAP type options. The VIA client WLAN profile should be configured with the appropriate settings of the WLAN profile that has to be pushed to the end-user device. Table 9 lists the VIA client WLAN profile parameters that are configured for a WPA2-enterprise and a WPA2-PSK WLAN profile that must be pushed to the end-user laptop.

Table 9 Sample VIA Client WLAN Profiles

WLAN Profile Type	VIA Client WLAN Profile	VIA Client WLAN Profile Settings	SSID Profile	SSID Profile Settings
WPA2-Enterprise	employee-dot1x	EAP Type: eap-peap Inner EAP type: eap-mschapv2 EAP-PEAP options: • validate-server-certificate • enable-fast-connect Inner EAP Authentication options: • mschapv2-use-windows-credentials Enable IEEE 802.1X authentication for this network. Automatically connect when this WLAN is in range.	employee	SSID: employee Authentication: WPA2 Encryption: AES
WPA2-PSK	voice-psk	Automatically connect when this WLAN is in range.	voice	SSID: employee Authentication: WPA2-PSK Encryption: AES

VIA Client WLAN Profile Configuration

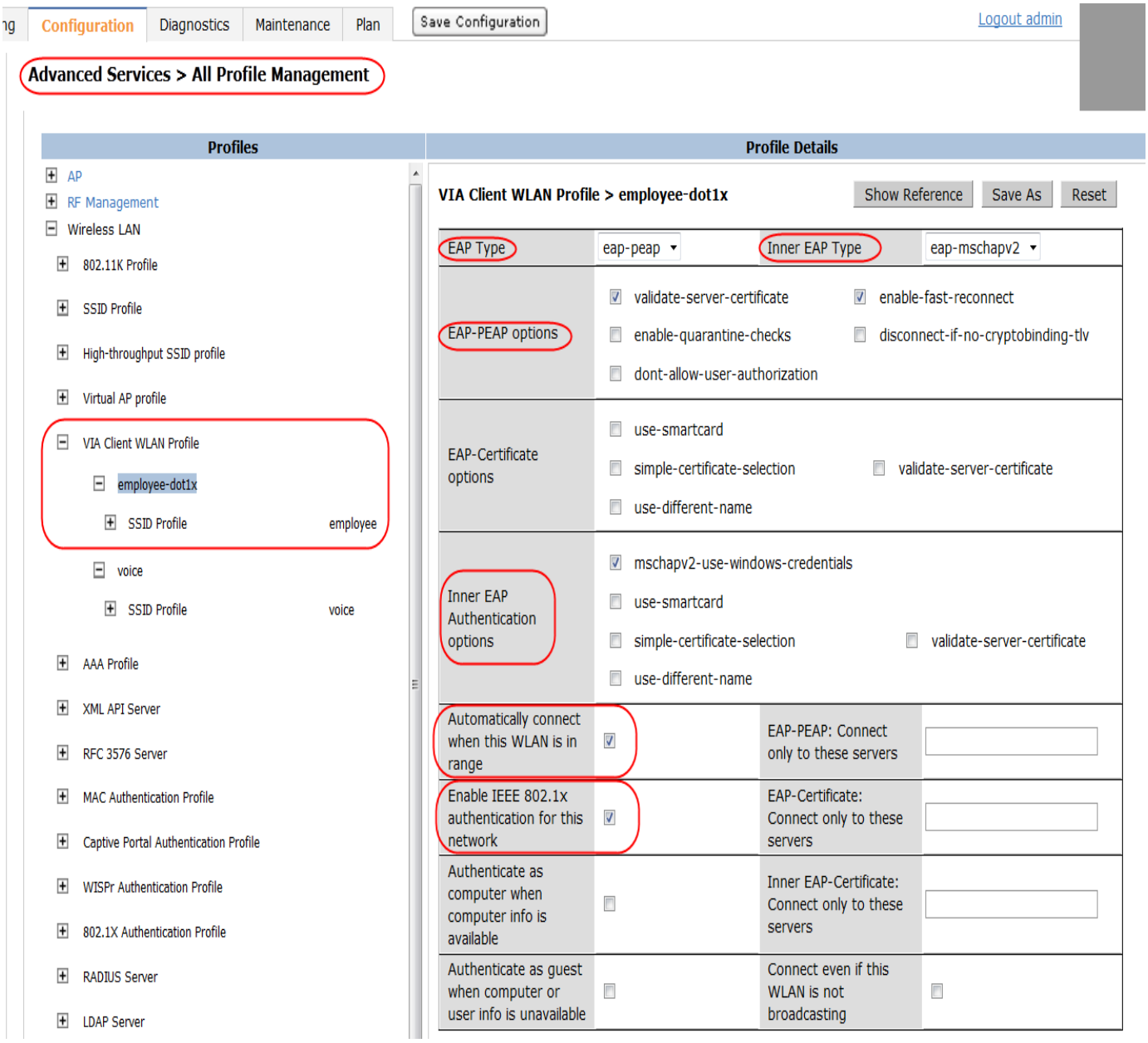

Figure 30 employee-dot1x: VIA client WLAN profile

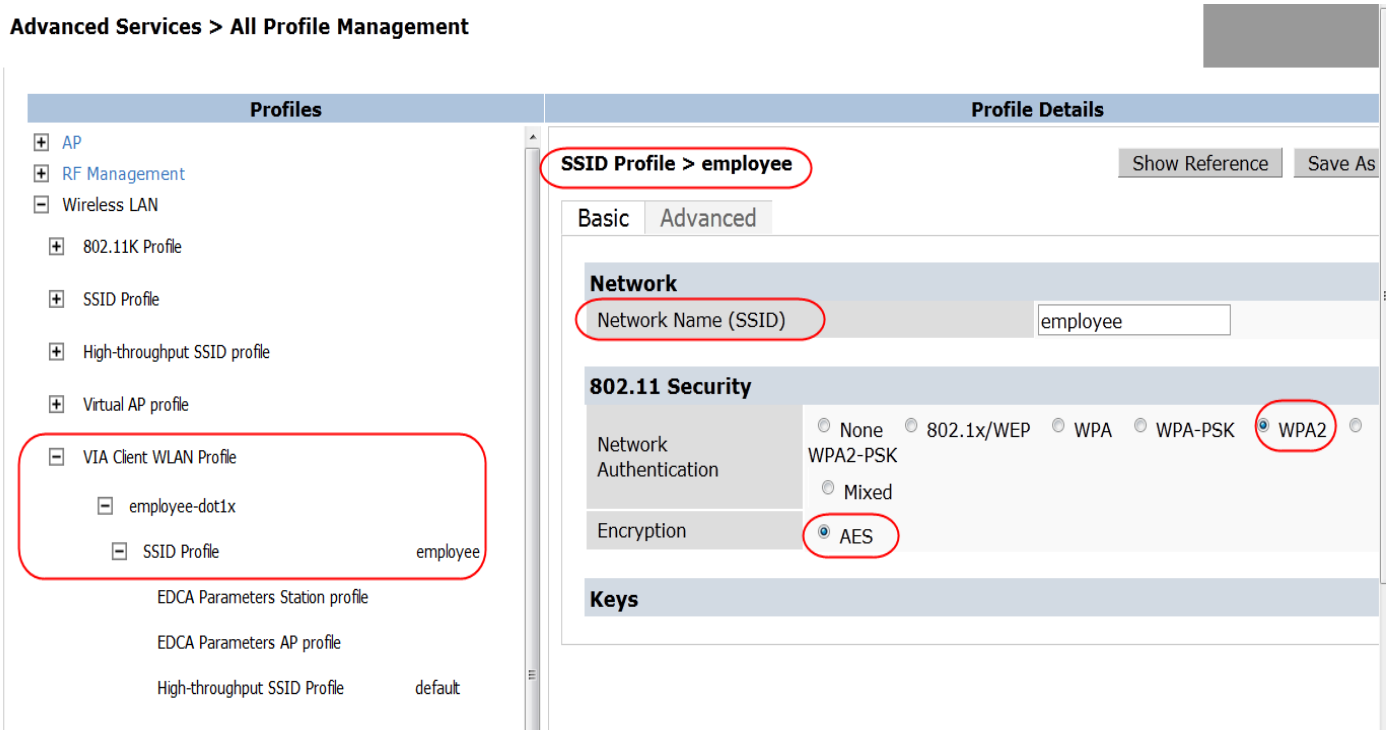

Figure 31 Employee SSID profile

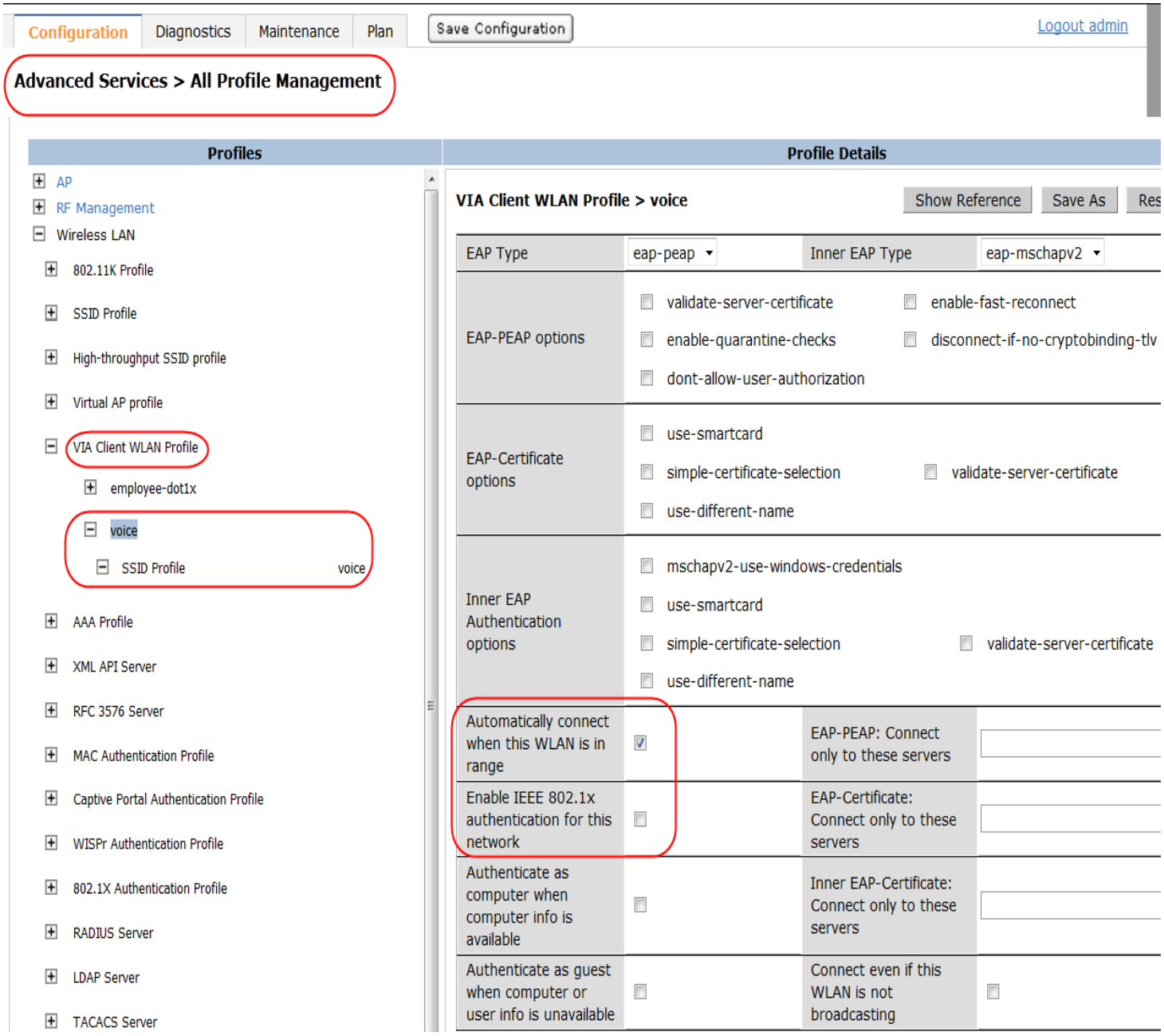

Figure 32 Voice VIA client WLAN profile

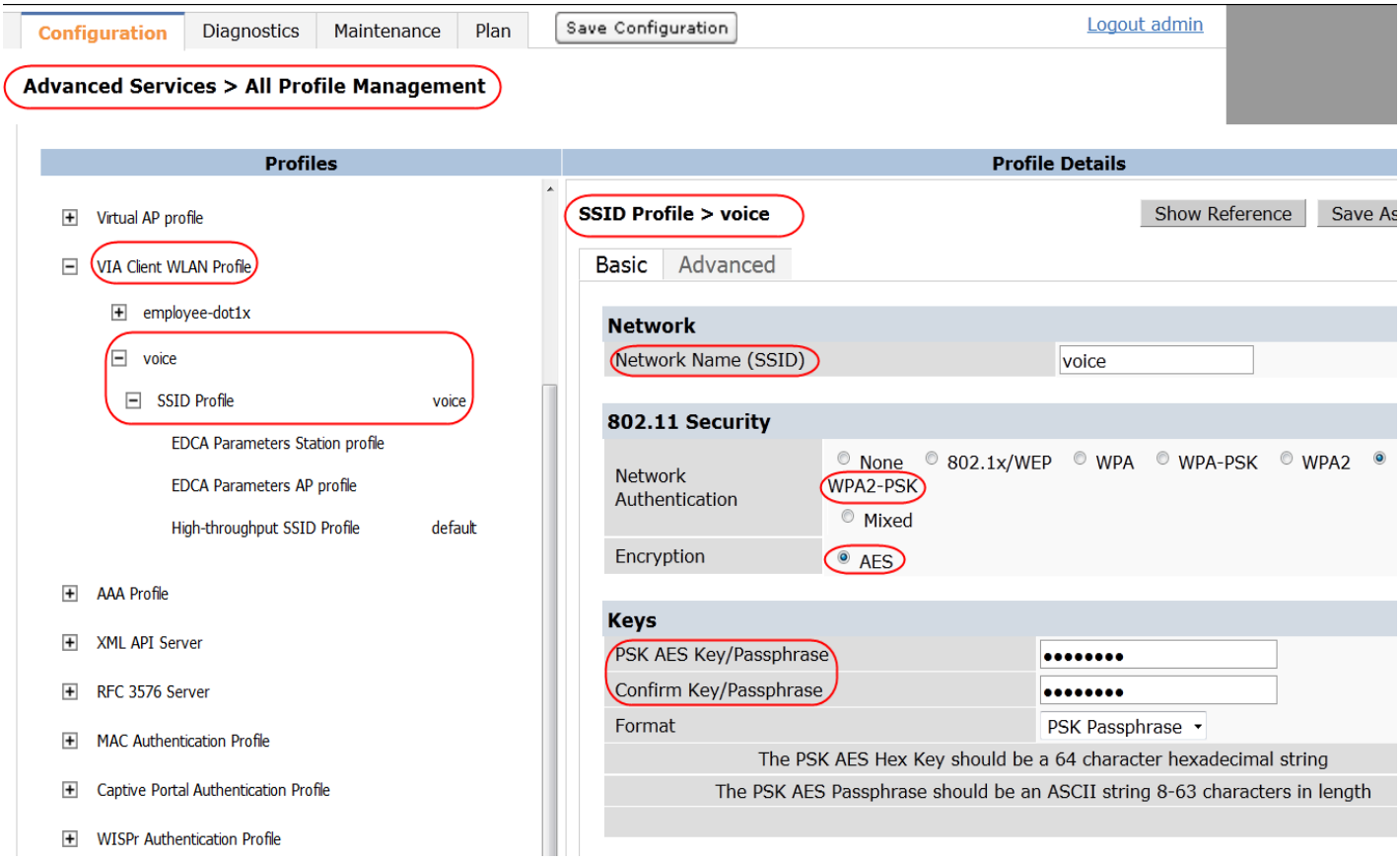

Figure 33 Voice SSID profile

Appending VIA Client WLAN Profiles to VIA Connection Profile

All the VIA client WLAN profiles that should be pushed to the end-user device must be appended to the VIA connection profile that is assigned to the VIA user. The end-user device is configured only with the VIA client WLAN profiles that were added to the VIA connection profile that is assigned to the VIA user.

Appending VIA Client WLAN Profiles to VIA Connection Profile

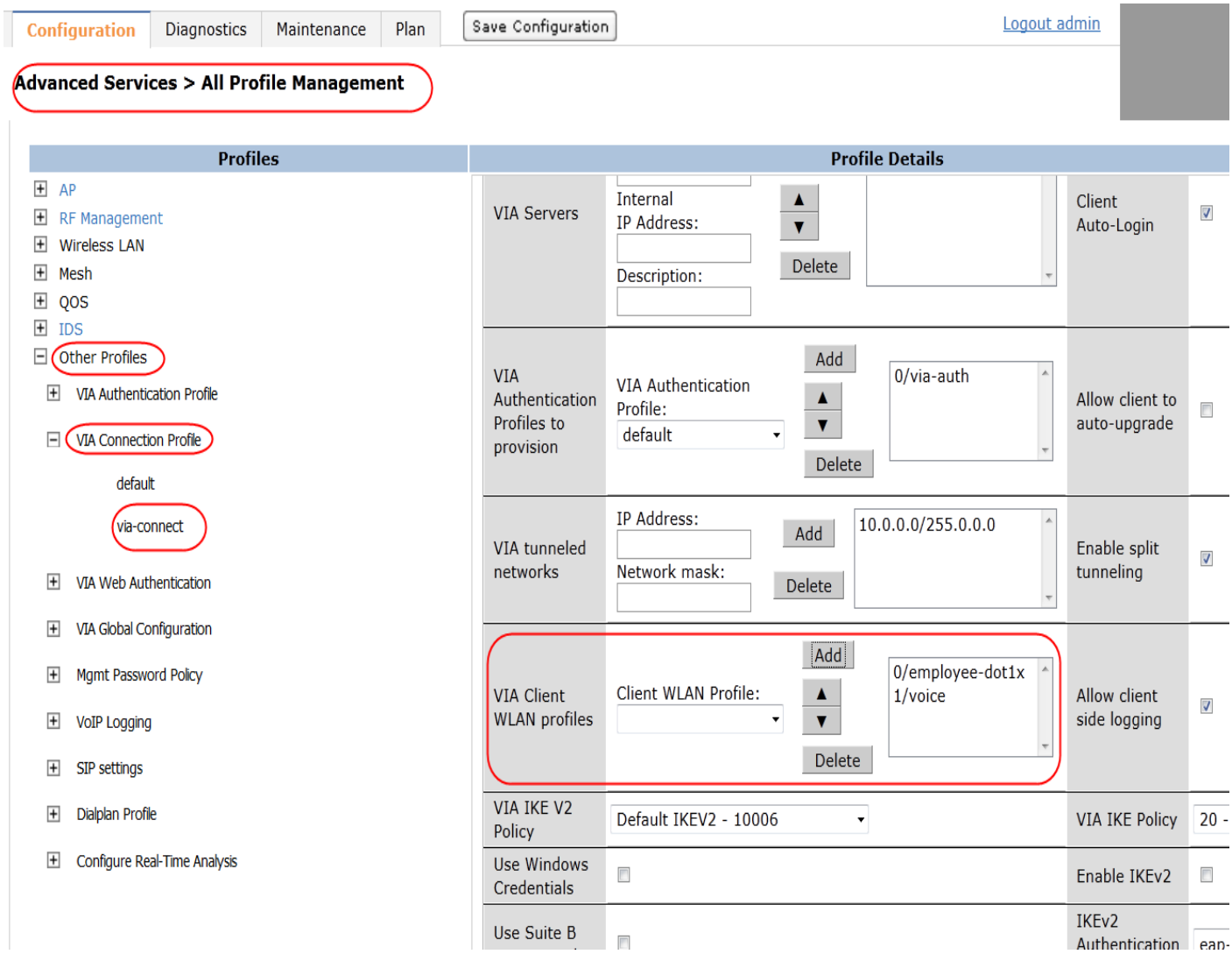

Figure 34 Appending the VIA client WLAN profile to the VIA connection profile

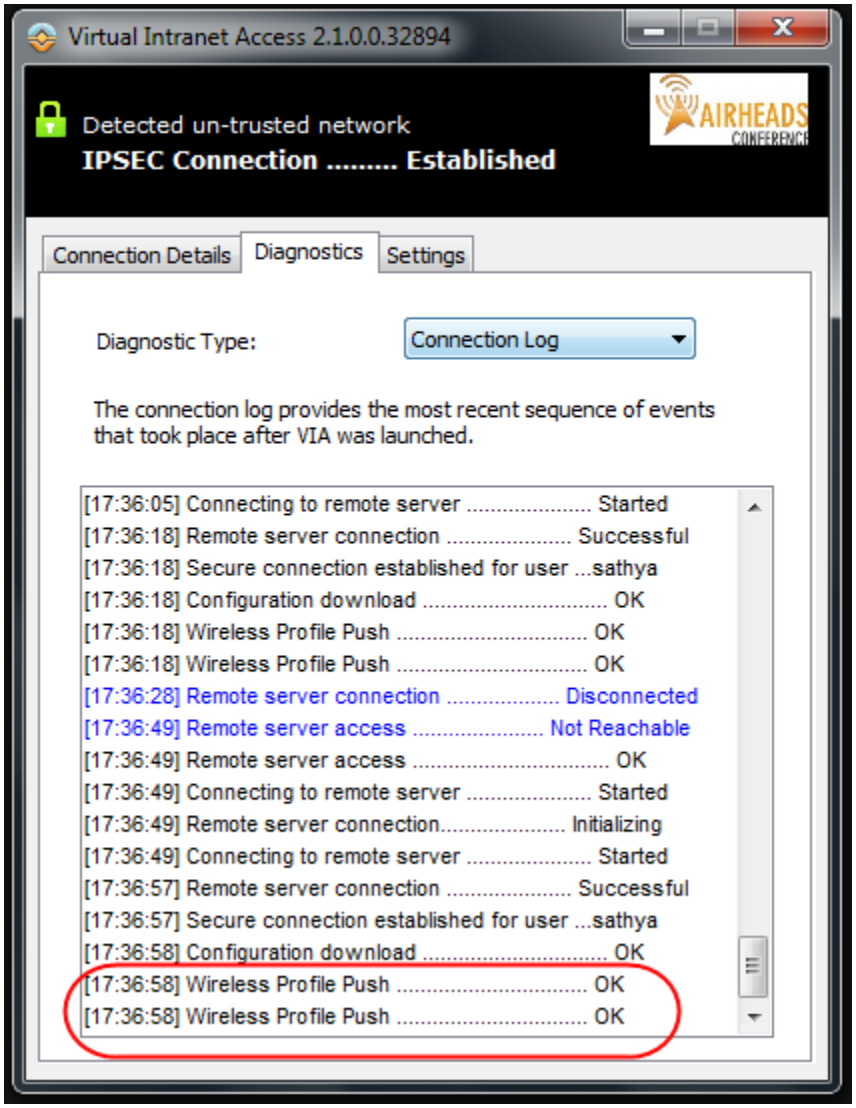

Figure 35 VIA client downloading the WLAN profiles

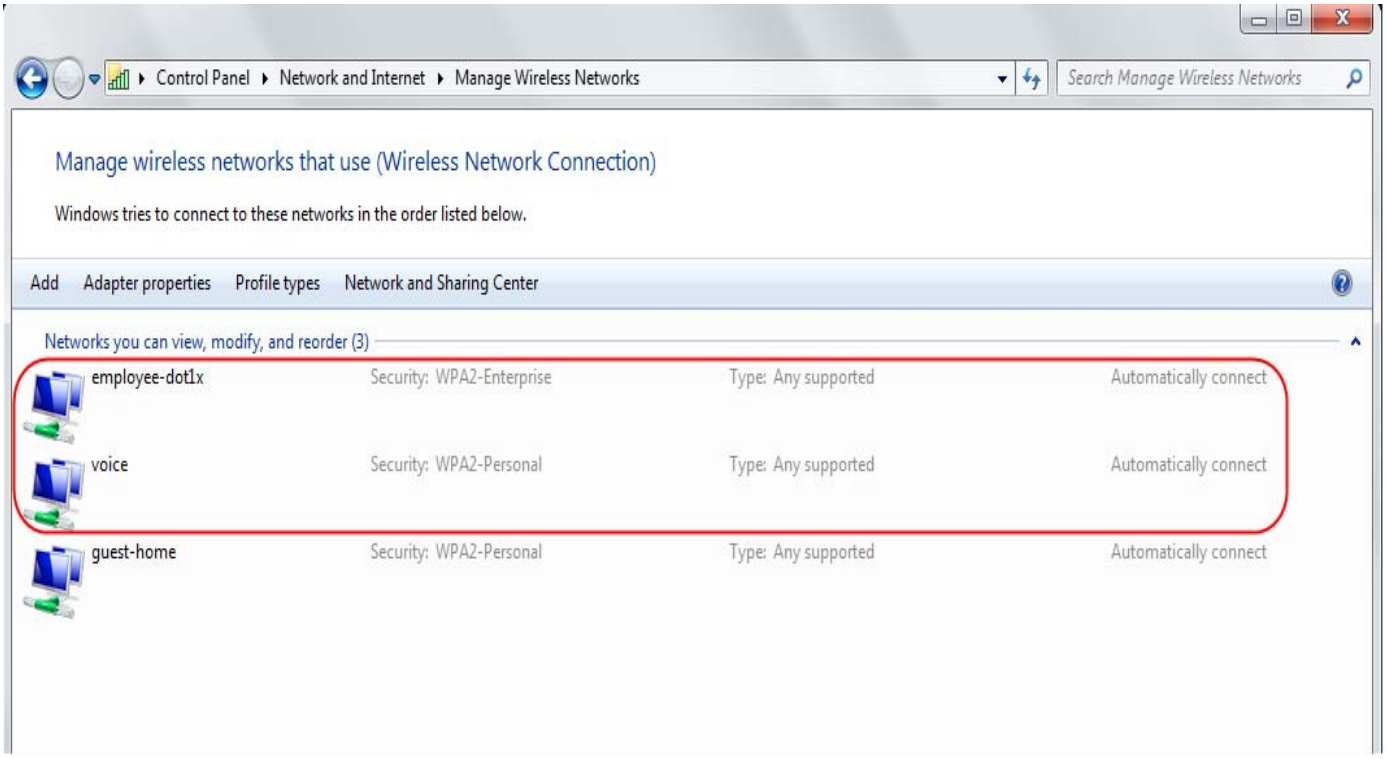

Figure 36 WLAN profiles are automatically added to the preferred network list

```
!
 aaa authentication via connection-profile "via-connect"
   client-wlan-profile "employee-dot1x" position 0
   client-wlan-profile "voice" position 1
!
```

Customizing VIA Logo

The Aruba logo is the default logo that appears on the VIA download page and the end-user VIA client. However, a custom logo can be uploaded to appear on the VIA download page and the VIA client using the customization options available for VIA. The custom logo should be a bmp, jpg, or gif file. The default dimension of the VIA logo for VIA clients 2.0 and earlier is 79(width) x 25(height) pixels. For VIA 2.1 clients the default VIA logo dimension is 79(width) x 69(height) pixels. If the logo is a little larger or smaller than the default dimensions, VIA automatically scales the logo to fit the default dimensions and preserves the aspect ratio.

NOTE

Click **Reset** in the Customize Logo section to reload the default Aruba logo.

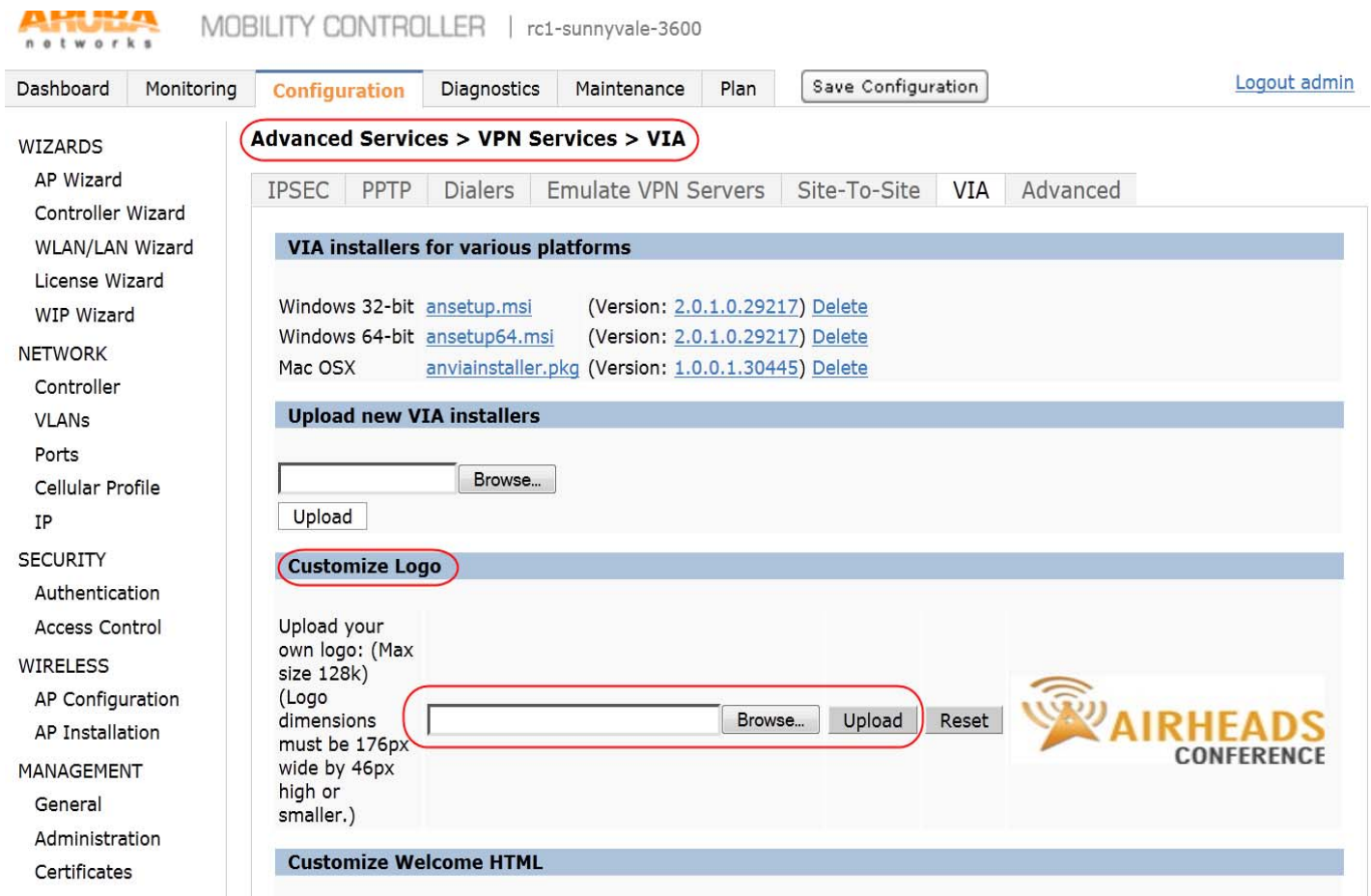

Figure 37 Uploading VIA logo

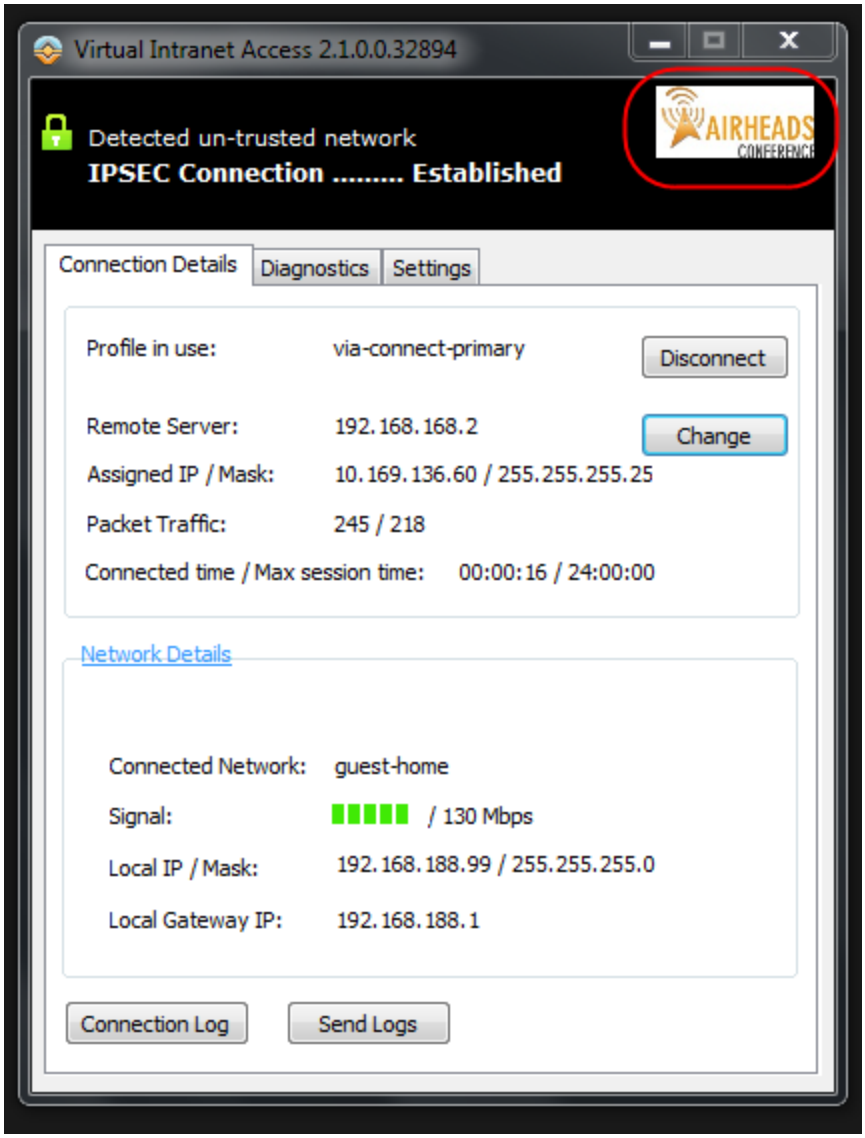

Figure 38 Custom VIA logo on the VIA client

Customizing the VIA Welcome Page for VIA Web Login

Standard HTML can be used to customize the welcome page that is displayed to users after they successfully authenticate on the VIA download page. The variables in the custom HTML file have the following notation:

- <% user %>: displays the username
- <% ip %>: displays the IP address of the user
- <% role %>: displays the user role
- <% logo %>: the custom logo (Example: <img src="<% logo %>">)
- <% logout %>: the logout link (example: <a href="<% logout %>">VIA Web Logout)
- <% download %>: the installer download link (Example: <a href="<% download %>">Click here to download VIA)

To customize the VIA welcome page, upload the custom HTML file to the controller. The Reset button erases all the changes made to the VIA welcome page and reloads the default welcome page. For more information on configuring the VIA welcome HTML page, see the *ArubaOS 6.1 User Guide* available at the Aruba support site.

NOTE

Appendix C: Custom VIA Welcome Pageincludes a sample HTML script that can be uploaded to the controller to display all the available installers to the VIA users.

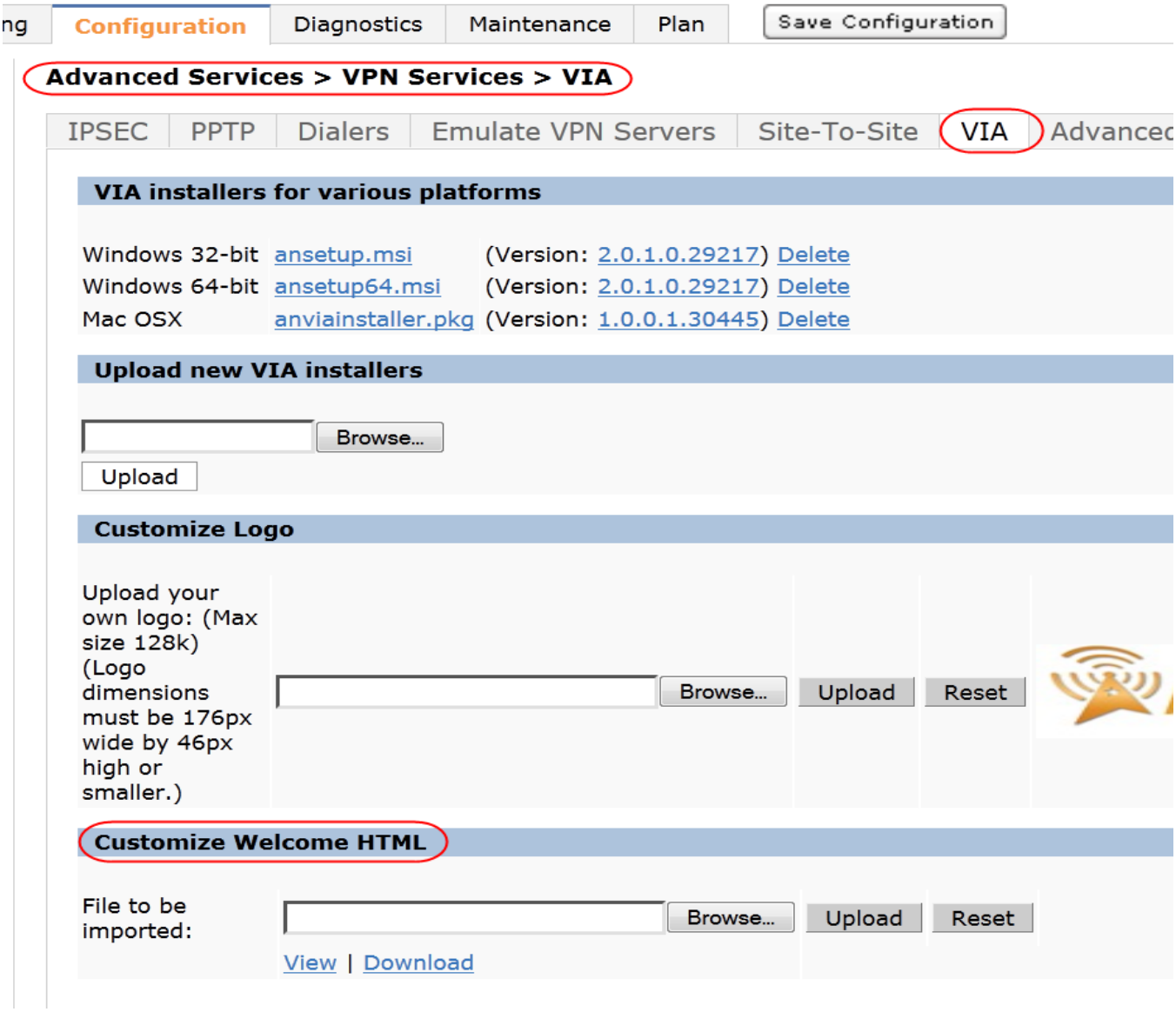

Figure 39 Uploading the custom HTML file

Chapter 8: Establishing VIA Connection

When VIA is launched for the first time after successful VIA installation, the user is prompted for these things:

- remote server: This is the IP address or FQDN of the controller that terminates VIA.
- username
- password

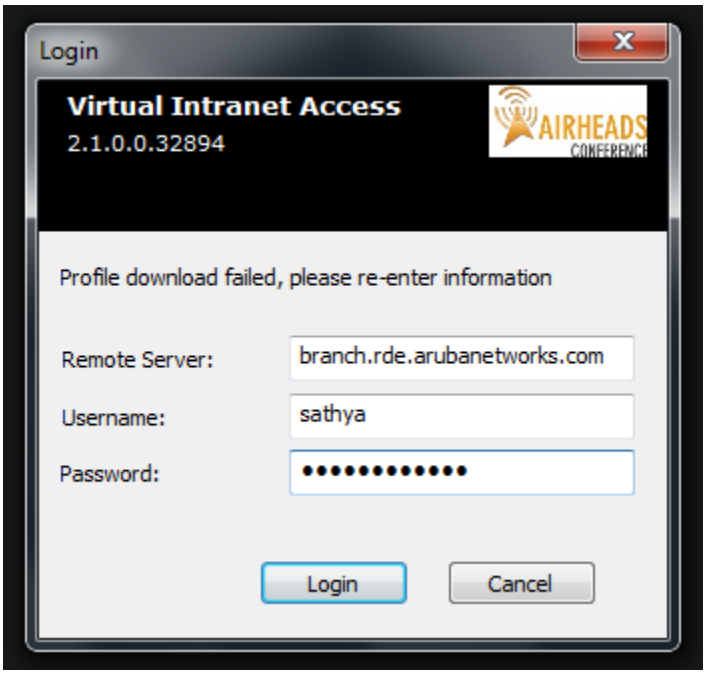

Figure 40 VIA initial setup

If the VIA web authentication list has more than one VIA authentication profile, the user can choose a VIA authentication profile from the available ones.

Figure 41 Choosing a VIA authentication profile

After successful authentication, the VIA client downloads the appropriate VIA connection profile and establishes the IPsec connection if the user is connected to an untrusted network.

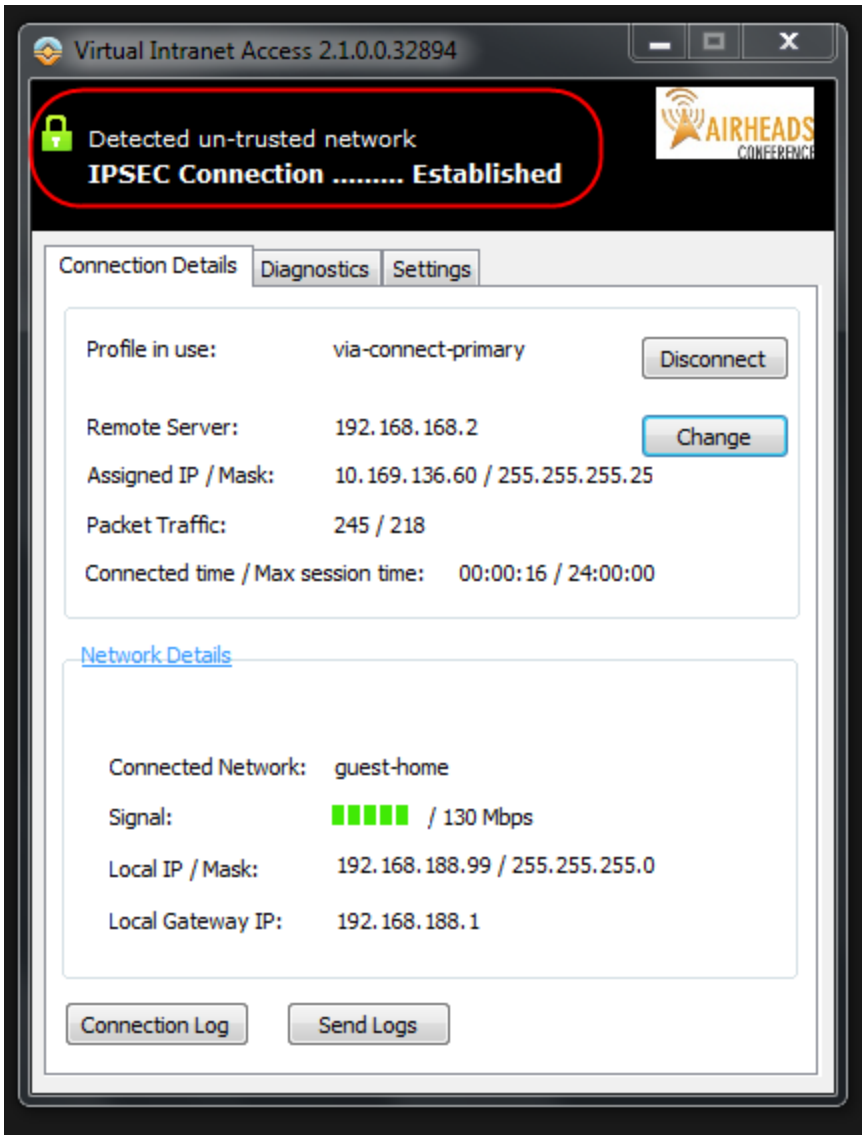

Figure 42 Successfully established VIA connection

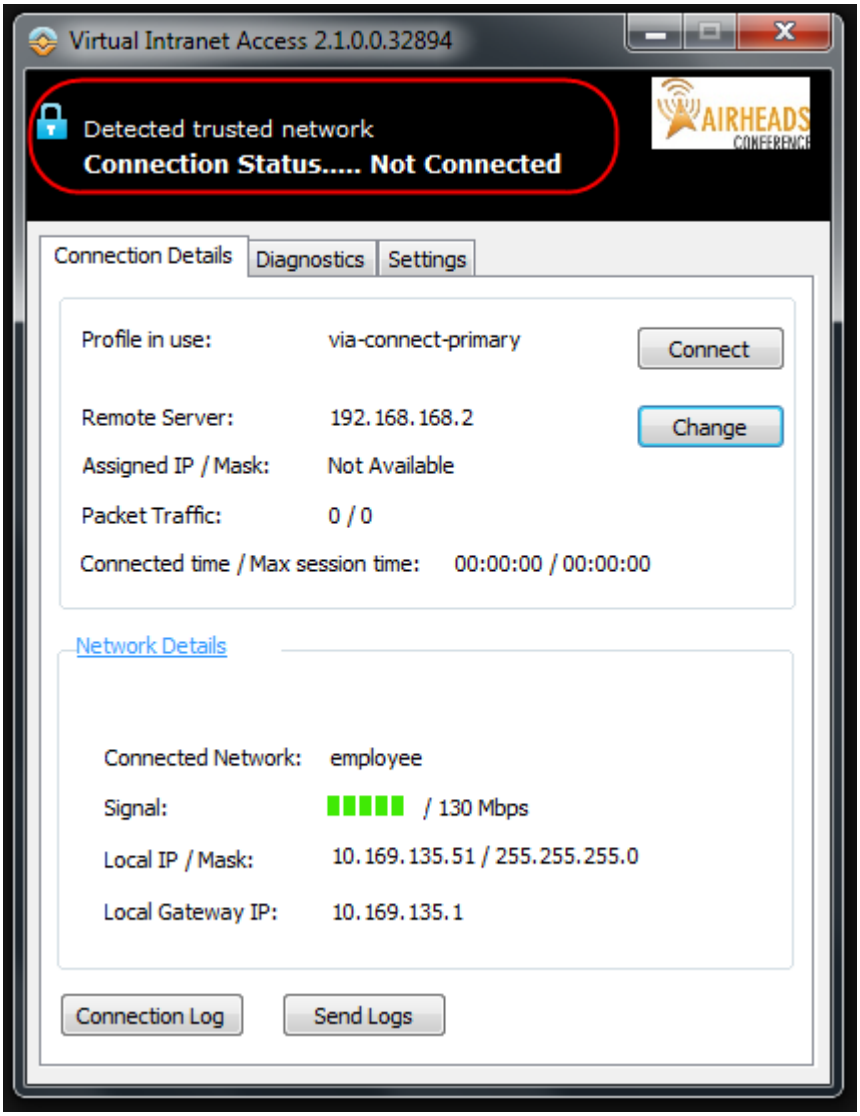

Figure 43 VIA not connected because the device is in a trusted network

If multiple authentication profiles are added to the “VIA Authentication Profiles to Provision” parameter of the VIA connection profile, the user can select a different authentication profile for IKE authentication if one of the authentication servers is unavailable.

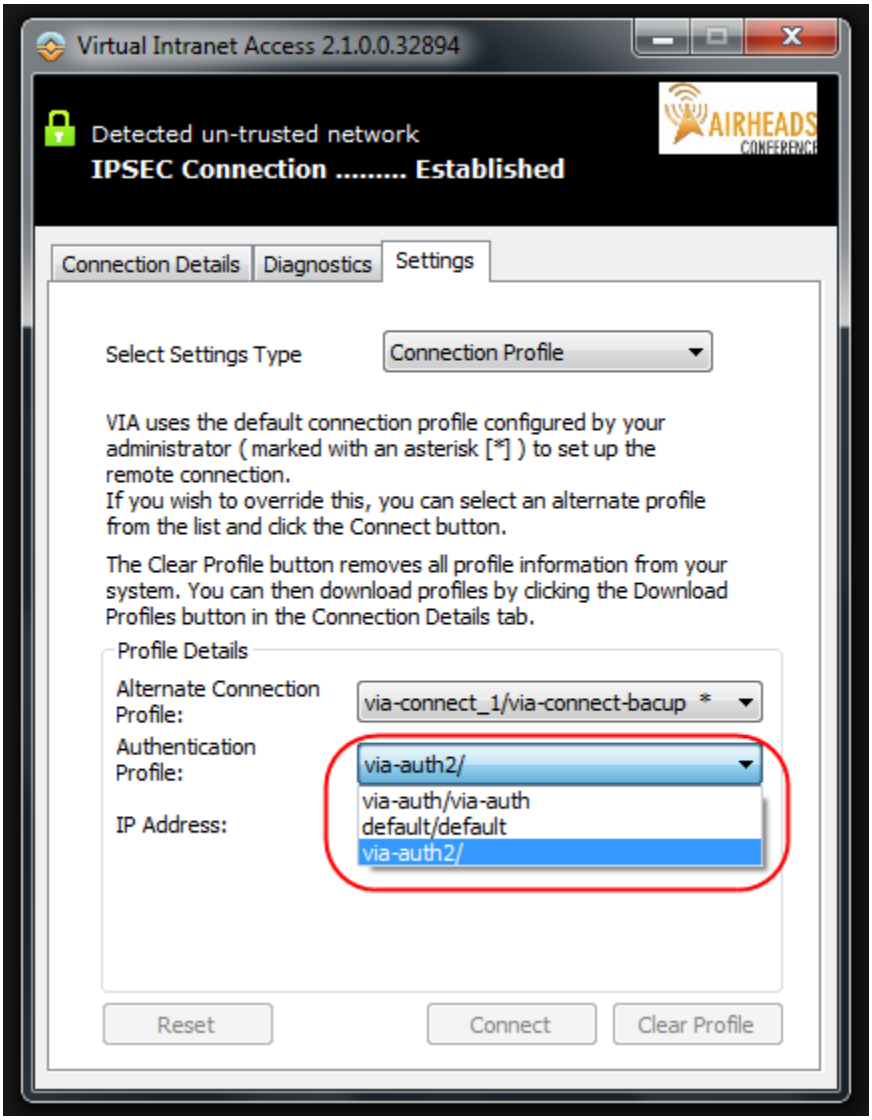

Figure 44 Choosing a VIA authentication profile for IKE authentication

If multiple controllers are added to the VIA Controller list of the VIA connection profile, the user can manually select a different controller to establish a secure connection if the primary controller becomes unavailable.

NOTE

VIA 2.1 clients will automatically switch to a backup controller and do not require the user to manually select the backup controller when the primary controller is unavailable. If more than one VIA controller is available and if the “enable controllers load balancing” feature of the VIA connection profile is enabled, VIA 2.1 for windows provides load balancing by randomly selecting a controller as the primary controller during each connection attempt. By default, all other versions of VIA clients will select the controller at the top of the VIA Controller list (available in the VIA connection profile) as the primary controller.

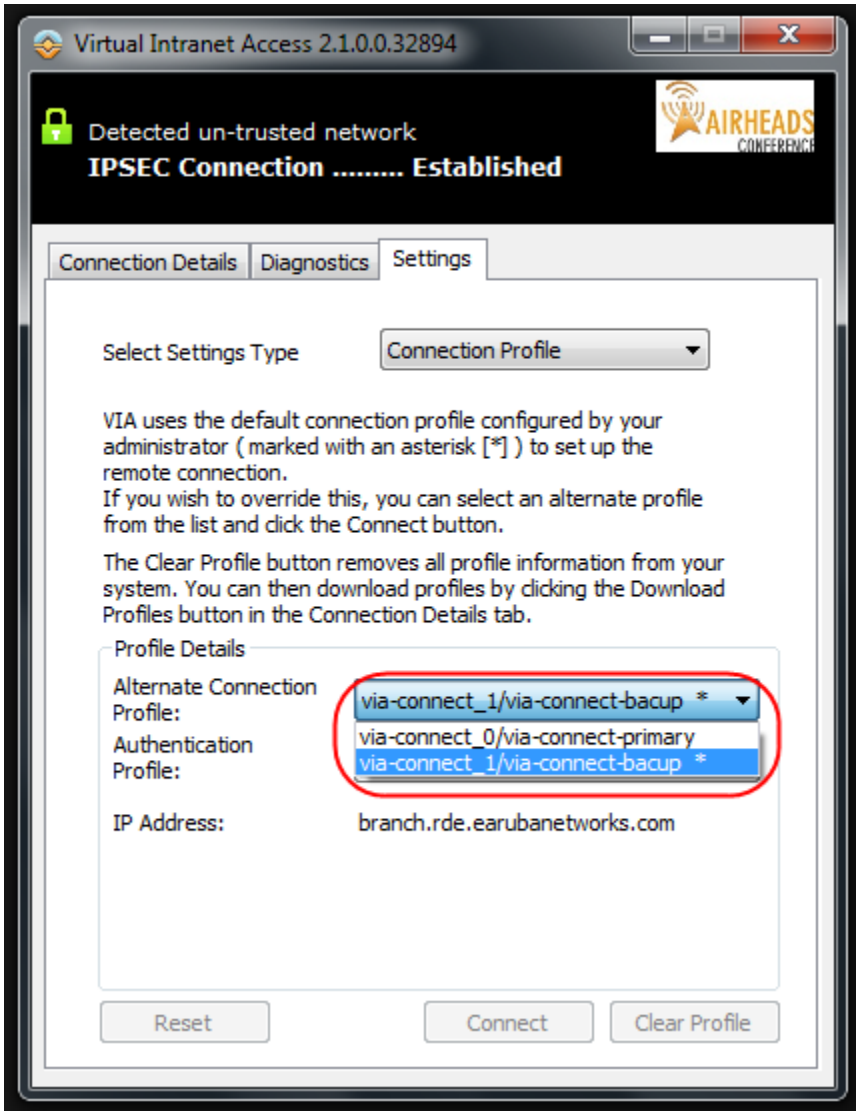

Figure 45 Choosing a VIA controller to terminate VIA

The VIA client has several tabs that provide various settings options and valuable information about the connection status and diagnostics. The three main tabs available on the VIA client are these:

- Connection: Provides the details about the connection status.
- Diagnostics: Provides various diagnostics details that are very useful in troubleshooting connectivity issues. The Diagnostics tab provides these options:
  - Connection Logs: Lists the events that happened during the recent connection.
  - Send Logs: Allows you send the list of logs collected by VIA to the IT support team.
  - View system info & advanced info: Displays the system and network configuration details of the device.
  - Connectivity tests: Provides ping and trace-route capabilities to test network connections.
  - Detected Networks: Displays a list of all the detected wireless networks.
  - VIA info: Displays information about the current VIA client installed on the end-user device.
  - Compatibility info: Provides compatibility information between VIA and certain applications that are detected on the end-user device. This tab can be used to check whether VIA failure is due to incompatible software.
- Settings: The Settings tab provides these options:
  - Connection profiles: Allows users to select different VIA controller and authentication profiles if multiple controllers and authentication profiles are made available by the network administrator.
  - Proxy settings: Displays the proxy server information that will be used by VIA for http, https, and SSL fallback traffic. This information is read automatically from the Internet Explorer settings. This page also allows the user to save a username and password for the proxy authentication. Note that proxy settings cannot be read from other browsers such as Firefox, Safari and Google Chrome.
  - Log settings: Allows users to select VIA logging levels. The default logging level is trace.
  - Wireless connection profiles (VIA 2.1): This tab available in VIA 2.1 allows the user to select and connect to a wireless connection profile pushed by the controller.

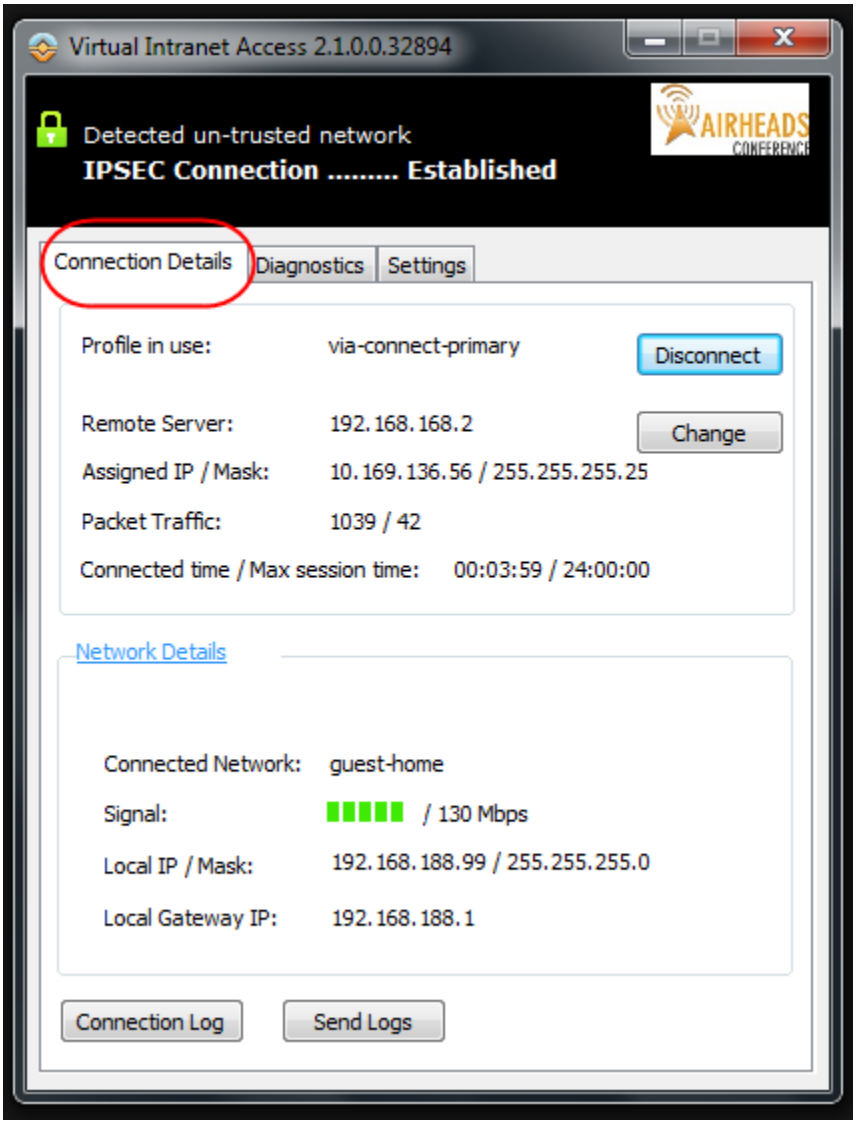

Figure 46 Connection tab

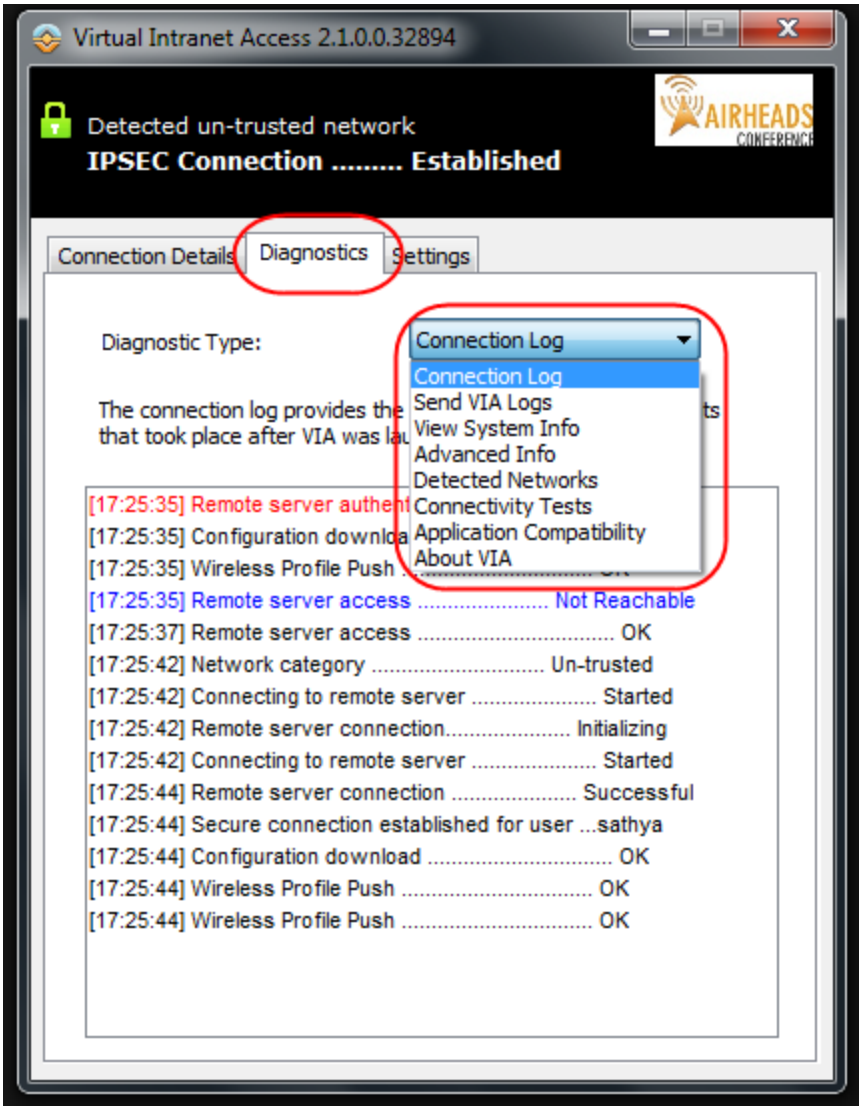

Figure 47 Diagnostics tab

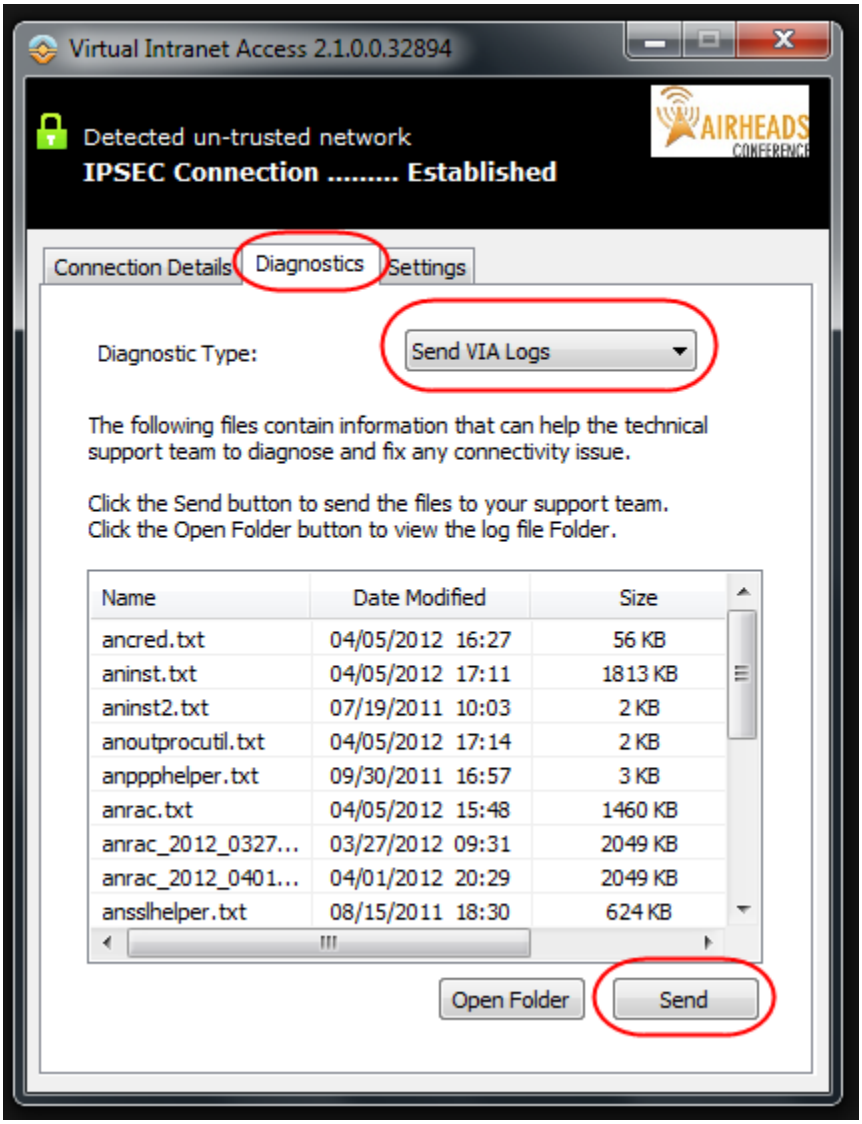

Figure 48 Diagnostics tab: Send VIA Logs option

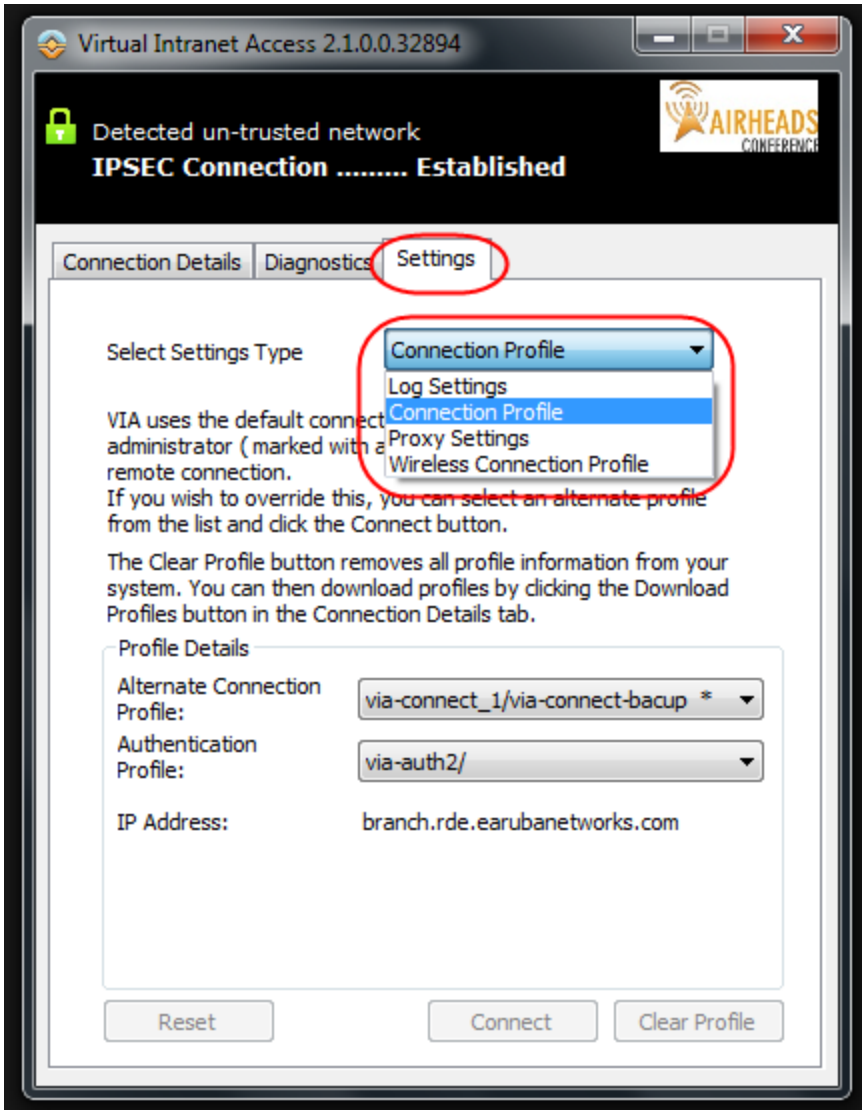

Figure 49 Settings tab

In addition to the connection, diagnostics and settings tabs, VIA 2.1 for windows has an additional tab called “VIA cert store” available exclusively for Windows XP devices. This tab allows users to import and use ECDSA certs on Windows XP operating system which does not natively support ECDSA certificates.

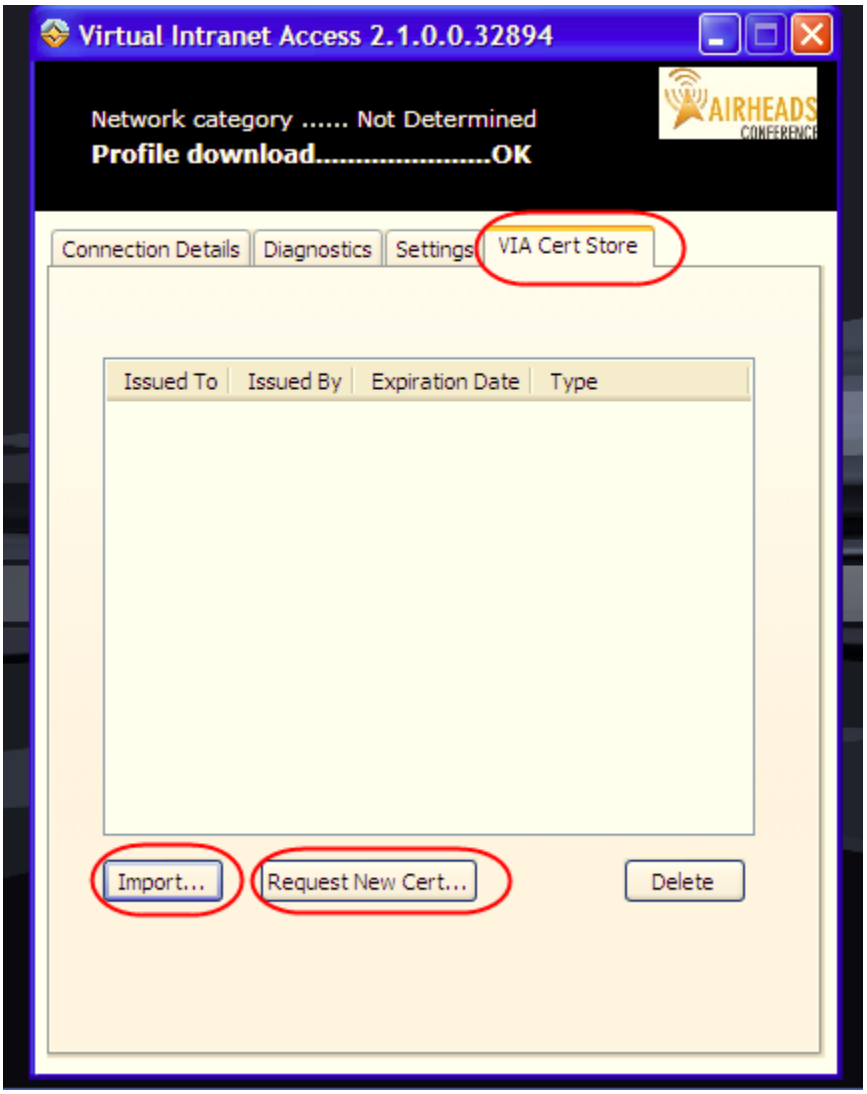

Figure 50 VIA cert store tab available only on Windows XP

Apple Mac OS VIA Client

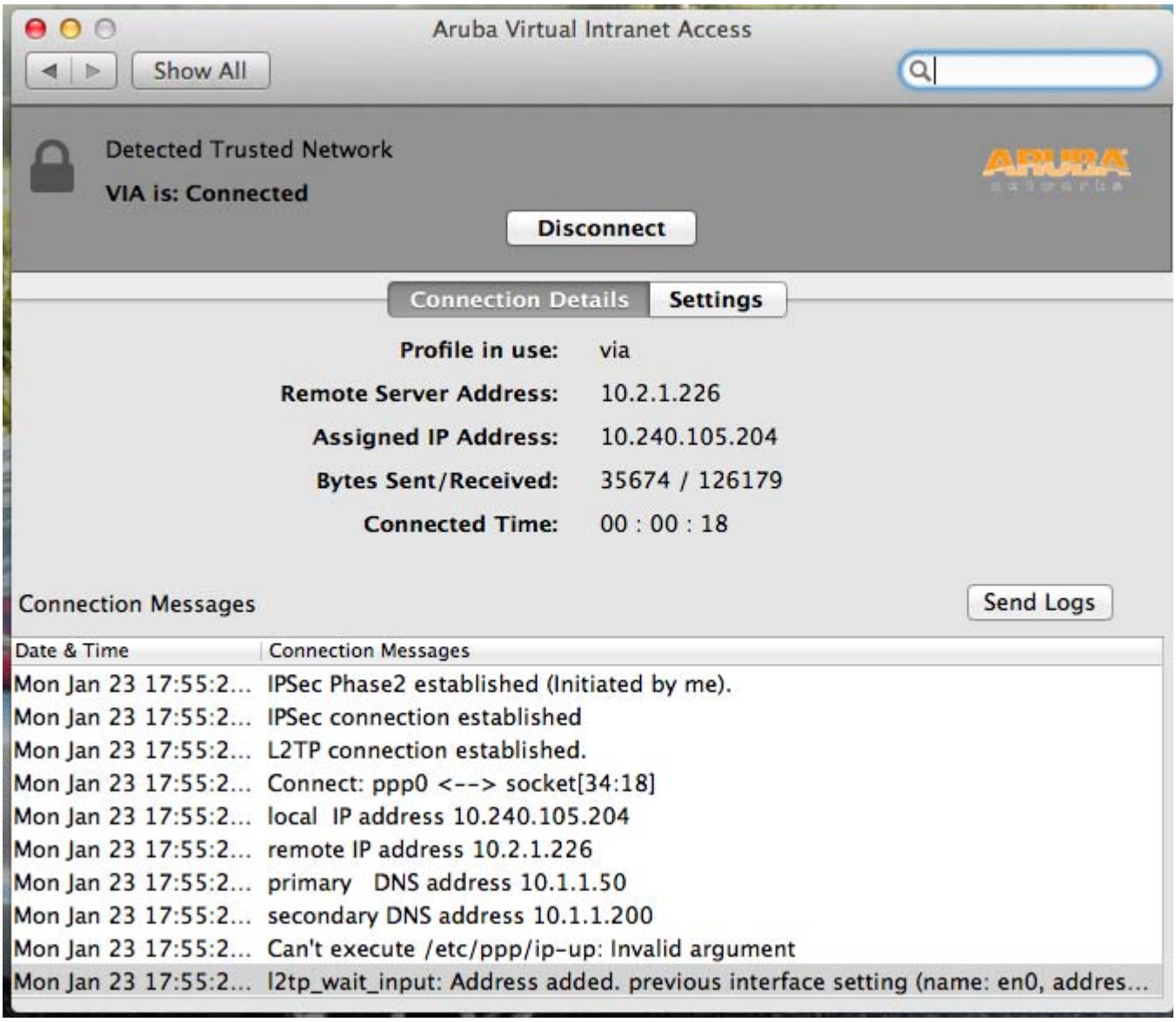

Figure 51 Apple Mac OS VIA client

Apple iOS VIA Client

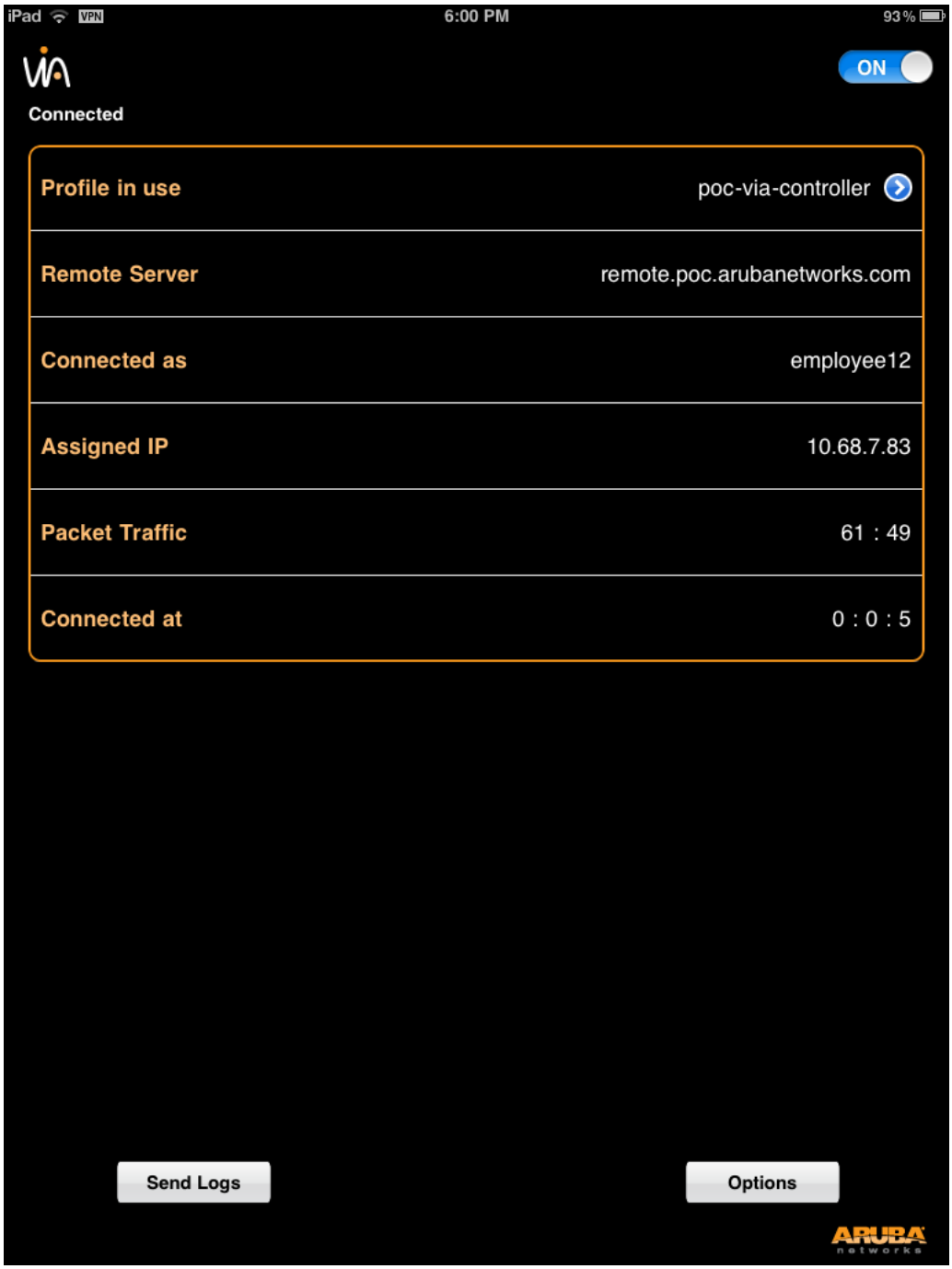

Figure 52 Apple iOS VIA client

Appendix A: Installer Options for the VIA Microsoft Installer (MSI) Package

The installer used to install VIA on a Windows computer is a MSI package. With the MSI package, you can use the command-line tool called msiexec. The msiexec tool allows you to customize the installation process by using certain vendor-specified installer options. These are the common installer options available for the Windows VIA clients (all versions):

- GATEWAY="<name or IP of the controller>"
  - This option can be used to preset the controller IP address so that the user gets a prompt only for username and password while downloading the configuration.
- AUTHPROFILE="<authprofilename>"
  - This option can be used to preset the VIA authentication profile used by the VIA client for tunnel establishment, which avoids the authentication profile choice dialog box.

Additional installer options that are available for the Windows VIA client version 2.1 are these:

- CUSTOMNAME="custom name for VIA"
  - This option can be used to define a custom name for VIA application on the user device.
- CUSTOMFOLDER="custom folder name with the entire path" -
  - This option can be used to specify a custom installation folder for VIA installation.
- CUSTOMSTART=<0 or 1>
  - This option can be used to modify VIA auto launch settings. If the value is set to 1, VIA Auto-launch will be turned on.
- GETCONFIG=1 USER=<username> PASSWORD=<password>–
  - If these options are defined during installation, the VIA client will download VIA profiles after installation without any prompts for username and password.
- AUTOSTART=1
  - If this option is used during installation, a VIA startup shortcut is created for all user accounts on the device.
- NOCERTWARN=<0 or 1>
  - This option can be used to configure whether a prompt should be displayed when the server does not have a valid certificate. If the value is set to 1, VIA will suppress the server validation prompt while retrieving the configuration.

The VIA installer options can be pushed to Windows computers using login or logoff scripts of system management tools such as the group policy object (GPO) in Windows server 2008 or can be used by advanced windows users on the Windows command prompt (cmd) during installation.

A sample msiexec command that can be used to perform a complete installation of VIA 2.1 from the Windows cmd looks like this:

```
msiexec.exe /i <VIA Installer (msi)>/qb GATEWAY=<gateway IP address> AUTHPROFILE=<name
of the authentication profile> GETCONFIG=1 USER=<domain username> PASSWORD=<password>
```

For information on the standard msiexec options and how to use vendor-specified installer options during installation, see the Microsoft Technet documentation.

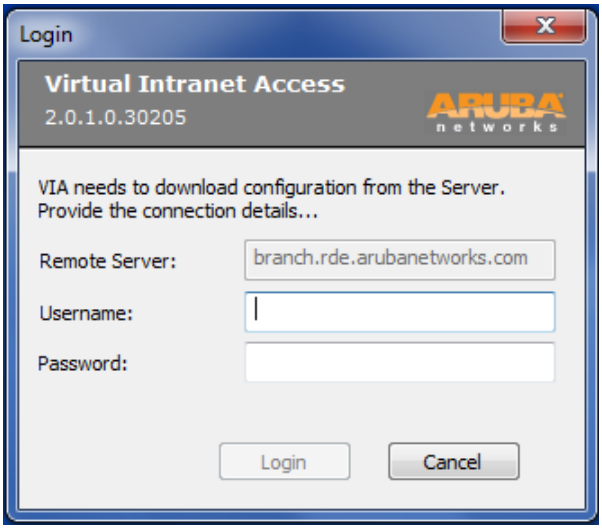

Figure 53 GATEWAY option presets the remote server name

Appendix B: VIA Client Feature Matrix

Table 10 summarizes the features and capabilities available on the current version of VIA client for Windows, Mac OS and iOS.

Table 10 VIA client feature matrix

Feature Name	VIA 2.1 for Windows	VIA 1.0 for Mac OS	VIA 2.0 for iOS
Not supported = ✗ Supported = ✓			
IKEv1	✓	✓	✓
Phase 0 using X.509 certificate	✓	✗	✓
Phase 0 using pre-shared key	✓	✓	✓
Phase 1 using username/password	✓	✓	✓
Phase 1 using token card/SecureID (supports new/next-pin)	✓	✗	✓
IKEv2	✓	✗	✓
X.509 certificate authentication	✓	✗	✓
EAP-MSCHAPv2	✓	✗	✓
EAP-TLS	✓	✗	✓
Suite B ciphers for IPsec (RFC 6379)	✓	✗	✓
Authentication using certificates on smartcards	✓	✗	✗
ECDSA certificate support (p256, p384)	✓	✗	✓
Authentication using machine certificate	✓	✗	✗
Post-connection script execution	✓	✗	✗
Auto-launch at system startup	✓	✓	✗
Automatic trusted/untrusted network detection	✓	✓	✗
Automatic configuration profile download	✓	✓	✓

Table 10 VIA client feature matrix (Continued)

Feature Name	VIA 2.1 for Windows	VIA 1.0 for Mac OS	VIA 2.0 for iOS
Automatic sign-on	✓	✗	✓ (Only available with X.509 certificate-based authentication using the iOS “VPN On Demand” feature. Apple iOS does not permit automatic sign-on when password-based authentication is used)
SSL fallback (available only for IKEv1)	✓	✗	✓
Configuration of Wi-Fi client settings	✓	✓ (Not available with Mac OS 10.7 due to change in underlying APIs)	✗
HTTPS proxy support	✓	✗	✗
Simple diagnostics which “send logs to helpdesk” button	✓	✓	✓
Prevent user from disabling/ disconnecting/modifying VIA	✓	✓ (User can still turn the connection off using Preference Pane->Network settings->VPN, but the Aruba Service will detect it and re-establish it. There may be a few seconds in between when VIA is not connected)	✗
Configurable tunneled subnets	✓	✗	✓
Configurable split-tunnel behavior	✓	✗	✓
Integration with Content Security Service (ZScaler)	✓	✗	✗
Automatic upgrade	✓	✗	✓
Local ECDSA certificate store	✓	✗	✓
Automatic Connection Failover	✓	✗	✗
Controller Statistical Load Balancing	✓	✗	✗
Lockdown all settings	✓	✗	✗

Appendix C: Custom VIA Welcome Page

The sample HTML script below can be uploaded to the VIA welcome page. This HTML script will display all the VIA installers on the VIA download page. Modify this script to match your specific needs.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>Welcome VIA Users</title>
</head>
<body>
Welcome VIA user <b><% user %></b>@<% ip %>/<% role %> <p>
<div>
<table border="1">
  <tbody>
     <tr>
          <th align="left" colspan="2">Download the VIA installer required for your devices from
          this list</th>
     </tr>
     <tr>
          <td>Windows 32-bit</td>
          <!-- ***comment*** below is the link for triggering download. This link has to be added
          within href="" -->
          <td><a href="/screens/cmnutil/viadownload?os=win32" title="Download">ansetup.msi</a></
td>
     </tr>
     <tr>
          <td>Mac OSX</td>
          <td><a href="/screens/cmnutil/viadownload?os=osx"
          title="Download">anviainstaller.pkg</a></td>
     </tr>
     <tr>
          <td>Windows 64-bit</td>
          <td><a href="/screens/cmnutil/viadownload?os=win64" title="Download">ansetup64.msi</
          a></td>
     </tr>
  </tbody>
</table>
</div> <p>
</div>
```

```
<input type="button" name="Logout" value="Logout" onclick="javascript:location.href='<% logout
%>'">
</body>
</html>
```

NOTE

Ensure that all the required VIA installers are uploaded to the controller. All VIA installers should be uploaded to the controller in .arb format. The .arb files are available on the Aruba support site.

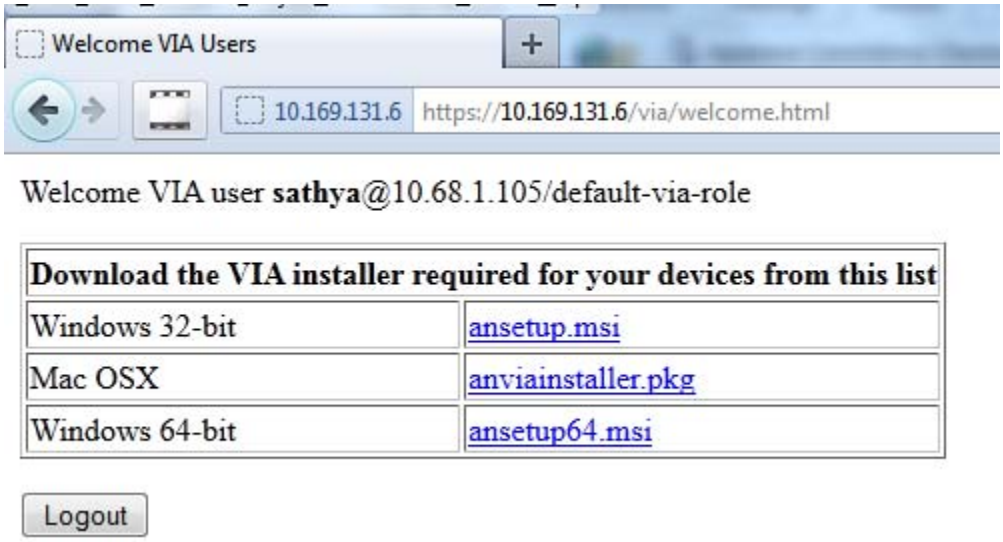

Figure 54 VIA welcome page for the sample HTML script

Appendix D: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://community.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
• United States	+1-800-WI-FI-LAN (800-943-4526)
• Universal Free Phone Service Numbers (UIFN):	
▪ Australia	Reach: 1300 4 ARUBA (27822)
▪ United States	1 800 9434526 1 650 3856589
▪ Canada	1 800 9434526 1 650 3856589
▪ United Kingdom	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

● Universal Free Phone Service Numbers (UIFN):	
■ Japan	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
■ Korea	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
■ Singapore	Singapore Telecom: 1 822 494 34526
■ Taiwan (U)	CHT-I: 0 824 494 34526
■ Belgium	Belgacom: 0 827 494 34526
■ Israel	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
■ Ireland	EIRCOM: 0 806 494 34526
■ Hong Kong	HKTI: 1 805 494 34526
■ Germany	Deutsche Telkom: 0 804 494 34526
■ France	France Telecom: 0 803 494 34526
■ China (P)	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
■ Saudi Arabia	800 8445708
■ UAE	800 04416077
■ Egypt	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
■ India	91 044 66768150