Aruba VIA 3.x (for ArubaOS 8.x)

User Guide

aruba

a Hewlett Packard Enterprise company

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Contacting Support

Table 1: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

Chapter 3
Overview

VIA is a part of the Aruba remote networks solution intended for teleworkers and mobile users. VIA detects the network environment (trusted and untrusted) of the user and connects the users to the enterprise network. A trusted network refers to a protected office network that allows users to access the corporate intranet directly. Untrusted networks are public Wi-Fi hotspots, such as airports, cafes, or home networks.

The VIA solution includes VIA Client and the standalone controller or Mobility Master and managed device configuration.

- **VIA Client**: Remote workers and mobile users can install VIA on their computers or mobile devices to connect to their enterprise network from remote locations.
- **Standalone Controller or Mobility Master and managed device configuration**: To set up a standalone controller or Mobility Master and a managed device for remote users, configure the user roles, authentication profile, and connection profile using either the WebUI or CLI.

NOTE

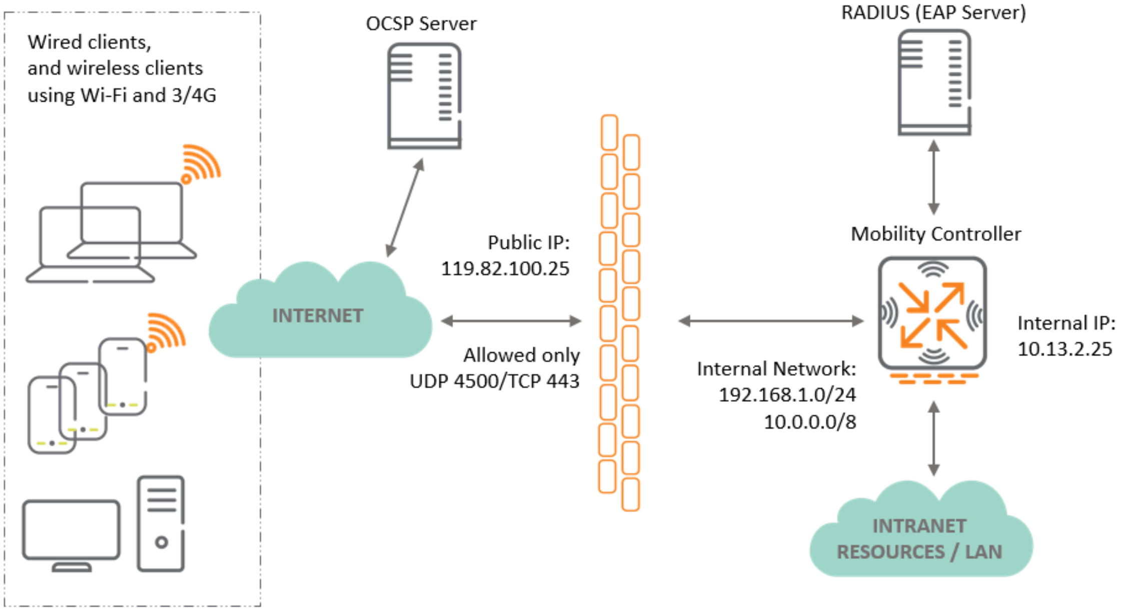
VIA for Mobility Master requires the PEFV license and is supported on 7200 Series, 7000 Series, and virtual mobility controllers.

If a user is connected from a remote location outside the enterprise network, VIA automatically classifies the environment as untrusted and creates a secure IPsec connection between the user and the enterprise network. After the user moves to a trusted network, VIA detects the network type and moves to an idle state by dropping the IPsec connection.

VIA can be downloaded using one of the following methods:

- URL provided by a local system administrator
- App store (for Android and iOS)
- Installation by a system administrator using a system management software.

Figure 1 *VIA Topology*


Wired clients, and wireless clients using Wi-Fi and 3/4G
OCSP Server
RADIUS (EAP Server)
Public IP: 119.82.100.25
Mobility Controller
INTERNET
Allowed only UDP 4500/TCP 443
Internal Network: 192.168.1.0/24 10.0.0.0/8
Internal IP: 10.13.2.25
INTRANET RESOURCES / LAN

VIA Connection Behavior

VIA provides a seamless connectivity experience for users when accessing an enterprise or corporate resource (*example: workstation, server*) from an untrusted or trusted network connection. By default, VIA automatically launches and establishes a remote connection when you log in to your system from an untrusted network.

The following table explains the typical behavior of VIA:

NOTE

The events described in Table 2 do not always occur in the same order.

Table 2: *VIA Connectivity Behavior*

User Action/Environment	VIA Behavior
The client or user moves from a trusted to untrusted environment. *For example, from an office to a public hotspot.*	Automatically launches and establishes connection to the remote network.
The client moves from an untrusted to a trusted environment.	Automatically launches and stays idle. VIA does not establish a remote connection. However, you can connect to a network manually by selecting the appropriate connection profile under **Settings**.
While in an untrusted environment, the user disconnects the remote connection.	Disconnects from the network.
User moves to a trusted environment.	Stays idle and does not connect.
User moves to an untrusted environment.	Stays idle and does not connect. This usually occurs if the user has previously disconnected a secure connection in VIA. Users can manually connect using the default connection profile by right-clicking the VIA icon in the system tray and selecting the **Connect** option.

User Action/Environment	VIA Behavior
User clicks the **Connect** button.	Establishes remote connection.
In an untrusted environment, user restarts the system.	Auto-launches and establishes remote connection.
In an untrusted environment, user shuts down the system, moves to a trusted environment, and restarts the system.	Auto-launches and stays idle.

Minimum Supported VIA Versions

The following table shows the minimum supported versions of VIA for each platform.

Table 3: *Minimum VIA Version Matrix*

Platform	OS Version	Minimum Supported VIA Version
Android	4.x, 5.x	2.2.5
	6.x	2.3.1
	7.x	3.0.0
iOS	6.x, 7.x	2.1.5
	8.x	2.1.6
	9.x	2.1.7
	10.x	3.0.1
Linux	Linux (32/64bit) RHEL and CentOS 6.0; Ubuntu 12.04, 14.04	2.0.2
	Ubuntu 16.04	3.0.0
	Linux command line Installation	2.3.0
MacOS	10.7, 10.8	2.0.0.1
	10.9	2.0.2.0
	10.11	2.0.4.0
	10.12	3.0.1
Windows	7, 8, 8.1	2.1.1.3
	10	2.3.0

VIA Feature Support

The following table describe the features supported by VIA clients running the Windows, Linux, MacOS, Android and iOS platforms.

Feature	Windows	Linux	MacOS	Android	iOS
Auth Profile Selection	YES	YES	YES	YES	YES
Client Auto-Upgrade/Downgrade	YES	YES	YES	YES* *Upgrade/Downgrade is only done from play store and App store	YES* *Upgrade/Downgrade is only done from play store and App store
Split Tunneling	YES	YES	YES	YES	YES
Client side Logging	YES	YES	YES	YES	YES
IKEV1 Policy support	YES	YES	YES	YES	YES
IKEV2 Policy support	YES	YES	YES	YES	YES
Use Windows Credentials	YES	YES	NA	NA	NA
SuiteB cryptography	YES	YES	YES	YES	YES
Allow users to save Passwords	YES	YES	YES	YES	YES
Enable FIPS module	YES	YES	YES	YES	YES
Lockdown all settings	YES	YES	YES	YES	YES
Domain Suffix in VIA authentication	YES	YES	YES	NO	YES
Controller Load Balancing	YES	YES	YES	YES	YES
Domain Preconnect	YES	YES	NO	NA	NA
Logon Banner	YES	YES	YES	YES	YES
Validate Server Certificate	YES	YES	YES	YES	YES
Max Session Timeout	YES	YES	YES	YES	YES
Logon Script	YES	YES	NA	NA	NA
LogOff Script	YES	YES	NA	NA	NA
Email support	YES	YES	YES	YES	YES
Max Reconnect attempts	YES	YES	YES	YES	YES
External Download URL	YES	YES	YES	NA	NA

Feature	Windows	Linux	MacOS	Android	iOS
Allow User to disconnect VIA	YES	YES	YES	NO	NO
Keep VIA window minimized	YES	YES	YES	NA	NA
Block traffic until VPN tunnel is up	YES	NO	NO	NO	NO
IKEV1 SSL-Fallback	YES	YES	YES	NO	NO
IKEV2 SSL-Fallback	YES	YES	YES	NO	NO
Automatic trust/Non-Trust detection	YES	YES	YES	YES	YES
EC certificates	YES	YES	YES	YES	YES
IPSec Rekey	YES	YES	YES	YES	NO
IKE Rekey	YES	YES	YES	YES	NO
Customized logo	YES	YES	YES	YES	YES
Diagnostic logs	YES	YES	YES	YES	YES
Client Auto-Login	YES	YES	YES	YES	YES
Xauth authentication	YES	YES	YES	YES	YES
Automatic connection failover	YES	YES	YES	YES	YES
Command Line Support Installation	YES** **Windows has minimal support	YES	YES	NA	NA
Online certificate request	NO	YES	NO	NO	NO
Heartbeat/Keep alive messages	YES	YES	YES	YES	YES
Unique Device ID	YES	YES	YES	YES	YES
OEM Support	YES	NO	YES	NA	NA
Smart Card support	YES	YES	NO	NO	NO
MOBIKE	YES	YES	YES	YES	NO
Common name against AAA server	YES	YES	YES	YES	YES
PAP for Authentication	YES	YES	YES	YES	YES

Feature	Windows	Linux	MacOS	Android	iOS
MSCHAPV2 for Authentication	YES	YES	YES	YES	YES
RSA certificate length 1024/2048/4096	YES	YES	YES	YES	YES
EC certificate length 256/384	YES	YES	YES	YES	YES
Command line operation	NO	YES	NO	NA	NA
3rd Captive Portal support	NO	NO	YES	NO	NO
VIA Gateway	NO	YES	NA	NA	NA
VIA config (Sideloading profile)	YES	NO	NO	YES	NO
Zero Touch Provisioning (ZTP)	YES	NO	NO	NO	NO
Hex based PSK	YES	YES	YES	YES	NO
OCSP	YES	YES	NO	YES	NO
Integrity check	YES	YES	NO	NA	NA
Knox Integration	NA	NA	NA	YES	NA
Validation of Strength of Symmetric Algorithm	YES	YES	NO	YES	NO
IPSec Drop policy	YES	YES	NO	YES	NO
Verification of DN Values in a Peer Certificate	YES	YES	NO	YES	NO
Certificate based profile download	YES	NO	NO	YES	NO
Certificate Filtering criteria in connection	YES	NO	NO	NO	NO
Certificate Filtering criteria in download	YES	NO	NO	NO	NO
Embedding profile in installer	YES	NO	NO	NO	NO

Chapter 4
VIA Client for Microsoft Windows

This section includes the following topics:

New Features

This section describes the features and enhancements introduced in VIA 3.x.x Windows Editions

Features Introduced in VIA 3.2.2 Windows Edition

GUI Displays Enhanced Certificate Store Data

In the VIA Client GUI, the **Certificate** section of the **VPN Profile** tab displays additional information for certificates, and now indicates whether a certificate is in the machine certificate store and globally available to all users on the device.

3.2.2 Supports Simultaneous Installation with OnGuardVIA-1735

The VIA 3.2.2 installer is enhanced with additional settings that allows a user to install and use both VIA 3.2.2 and W-ClearPass OnGuard 6.7.2 on a single client. This feature requires that both VIA and OnGuard be installed with a specific flag that allows them to coexist on a single device.

To use this feature, OnGuard must be installed by passing the **AllowBothVIAAndOnGuard** flag to the installer in the following format:

```
ClearPassOnGuardInstall.exe /AllowBothVIAAndOnGuard=1
msiexec /i ClearPassOnGuardInstall.msi ALLOWBOTHVIAANDONGUARD=1
```

In addition, VIA must be installed with the **AllowBothVIAAndOnGuard** flag in the following format:

```
msiexec /i Aruba-VIA-3.2.0.0.XXXXX-64(86).msi ALLOWBOTHVIAANDONGUARD=1
```

NOTE

Both OnGuard and VIA must be installed with this flag in order for them to coexist on the same system. If either of them is installed without this flag, the other cannot be installed.

Features Introduced in VIA 3.2.1 Windows Edition

Access to local resources are differentiated in full tunnel mode

VIA clients can now access resources over the tunnel that are in the same network addressing range as the local network in full tunnel mode. If a VIA client and another machine are connected to the same router, the second machine was preventing access to similar addressed devices in the enterprise. The change in application behavior now ensures all network access requests go through the tunnel mode setup.

Features Introduced in VIA 3.2.0 Windows Edition

Importing connection profiles offline

Clients can import connection profiles offline by downloading an XML file containing a valid VIA connection profile.

To import a connection profile while offline, follow the steps below:

1. Navigate to https:/<ControllerIP>/via, and log in using your VIA credentials.
2. After successfully logging in, navigate to https:/<ControllerIP>/via/config?ikever=3.
3. Save the XML file returned by the controller to the following location: %appdata%Aruba Networks\VIA\.
4. Rename the file as **profile.xml**.

Upon startup, if the connection profile has not already been provisioned, VIA will load it from **profile.xml**.

If Auto-login is enabled in the new profile, the device will automatically connect to VIA after instiallation is complete.

Certificate-based authentication for profile downloads

In versions prior to VIA 3.2.0, the client must provide their user credentials as part of the HTTPS communication with the controller in order to download a VIA profile. This feature allows clients to authenticate automatically when a valid certificate is presented to the controller with standard ssl/tls key exchange and certificate validation rules.

When a certificate-based profile is configured on a controller, VIA will attempt to authenticate the client certificate, while downloading the initial connection profile from the controller.

To enable certificate-based authentication for profile downloads, follow the steps below:

1. Navigate to **Configuration > Authentication > L3 Authentication**.
2. From the **L3 Authentication** menu, open the **VIA Authentication** dropdown folder, then select the desired profile.
3. In the **VIA Authentication Profile** menu, select the checkbox for **Client-certificate based authentication for VIA Profile download** to enable this feature.

Once the profile is selected, VIA will show the certificate selection screen instead of the username/password screen.

Connection and failover in a restricted environment

In versions prior to VIA 3.2.0, a connection with the VPN can not be established if external port 443 is blocked. A VPN tunnel can be established for port 4500 when port 443 is blocked and allows the controller to failover to another configured controller if port 4500 is accessible

Certificate filtering for profile downloads

When a VIA client attempts to download a profile using the certificate as authentication (this can be achieved by enabling the certificate-based authentication for profile downloads feature introduced in this release), instead of displaying all of the available certificates for the end user to select, VIA will display only those certificates that are filtered by administrator.

To filter profile downloads by certificate, follow the steps below:

1. Navigate to **Configuration > Authentication > L3 Authentication**.
2. Select the profile from the **VIA connection profile** menu.
3. Enter the criteria for certificate filtering into the **Certificate Criteria** field.

When a user downloads the profile and initiates connection, only certificates that match the filtering criteria will be listed for authentication. If therw is only one certificate available, the connection will be established automatically, without prompting the user to select a certificate.

Pre-provisioning VIA with multiple VPN Gateway info

This feature allows an administrator to preload the VIA Installer with preselected controller addresses. Upon installation, VIA will automatically display the list of controller addresses from which users can download their profile, freeing users from the task of manually entering in the information for the controller.

To embed this profile information into your VIA installer package:

1. Download the build “ansetup64.msi” or “ansetup32.msi” from the Aruba support site to a temporary folder.
2. Create the file GatewayList.xml in the same temporary folder and populate that file with XML data in the format of following example

```
<?xml version="1.0"?>
<MultiProfileConfig Version="1">
<VPNServerList>
<VPNController>
<Name>Controller-ONE</Name>
<URL>10.17.12.12</URL>
<AuthProfile>IKEv2RSA</AuthProfile>
<Authtype>2</Authtype>
<CertFilteringCriteria>certificateIssuer=customer-1-WIN-XSHSQH1EKMR-
CA</CertFilteringCriteria>
<CertAuthPort>8085</CertAuthPort>
</VPNController>
<VPNController>
<Name>Controller-TWO</Name>
<URL>10.17.14.3</URL>
</VPNController>
</VPNServerList>
</MultiProfileConfig>
```

3. Download the file **GenerateCustomVIAinstaller.bat** from the Aruba support site into the same temporary folder as the previous files.
4. Install the NSIS (Nullsoft Scriptable Install System) tool to generate the custom executable filel. The file “nsis-3.01-setup” can be downloaded from http://prdownloads.sourceforge.net/nsis/nsis-3.02.1-setup.exe?download.
5. Use the following command to generate the custom executable file

```
GenerateCustomVIAinstaller.bat Aruba-VIA-3.2.0.0.96992-64.msi GatewayList.xml
```

6. Using this example, an executable VIA installation file file with the name “Aruba-VIA-3.2.0.0.96992-64” is created in the same temporary folder.
7. When you run the executable installatoin file, the VIA UI will display VPN server entries with the controller name(s) configured via the <Name> parameter in the xml script in step 2. The user much select a controller and a controller certificate , then click **Proceed**.
8. If the user has a certificate which is not verified, a certificate warning will appear. (This is an expected behavior). In this case, the user must click **Continue** in the warning message box before profile will be downloaded.

Ability to Mark Outgoing Packets with ToS Bits

The VIA connection profile includes the new configuration setting **tos_dscp** that allows you to mark outgoing IKE and ESP packets with custom DSCP values. This parameter supports values between 0 to 63. When a VIA client downloads the connection-profile, this value will also et pushed. VIA will set the configured DSCP value to the outer IP header's ToS byte.

Features Introduced in VIA 3.1 Windows Edition

Client Certificate-based Authentication

Starting with VIA 3.1, users can authenticate and download VPN profiles using either client certificate-based authentication or the existing credential-based authentication. During certificate-based authentication, the client certificate is verified against the trusted CA certificates imported on the managed device. After the certificate is successfully validated, a user role is derived from the client-identity attributes on the certificate to fetch the corresponding VIA connection profile.

Features Introduced in VIA 3.0.0 Windows Edition

VIA User Interface

VIA 3.0.0 introduces a new User Interface (UI).

System Prerequisites

Ensure that the end-user system meets the following prerequisites:

- Supported Operating Systems:
  - Microsoft Windows 7 (32-bit and 64-bit)
  - Microsoft Windows 8 and 8.1 (32-bit and 64-bit)
  - Microsoft Windows 10 (32-bit and 64-bit)
- On Windows 8 and 8.1, KB2743127 must be installed in order for DPC with machine credentials to work.
- Administrator privileges on the computer.
- Computer connected to a working wired or wireless network.
- .Net Framework 4 or later version installed.

Downloading VIA

To download VIA:

1. Login to the Aruba Support Site.
2. Navigate to **Download Software > VIA > Windows > VIA 3.2.0**.
3. Download the **ansetup32.msi** or **ansetup64.msi** installer file.

Installing VIA

Ensure that all prerequisites have been met before proceeding with installation.

NOTE

VIA 2.x continues to retain the connection profile even after uninstalling VIA 2.x. You can connect using this profile after VIA 3..2.x is installed. If you do not want to connect using the existing connection profile, clear the connection profile in VIA 2.x, and then install VIA 3.2.x.

To install VIA:

1. Open the **ansetup32.msi** or **ansetup64.msi** installer file.
2. An **Open File - Security Warning** message appears. Click **Run** to launch the **VIA Setup Wizard**.

3. After the **VIA Setup Wizard** opens, click **Next** on the **Introduction** screen.
4. On the **End-User License Agreement** screen, select the check box to accept the terms in the License Agreement. Click **Next**.
5. Click **Browse...** on the **Destination Folder** screen to locate and select the folder to which VIA will be installed. Click **Next**.
6. On the **Ready to install** screen, click **Install**.
7. After installation is complete, click **Finish** to exit the setup wizard.

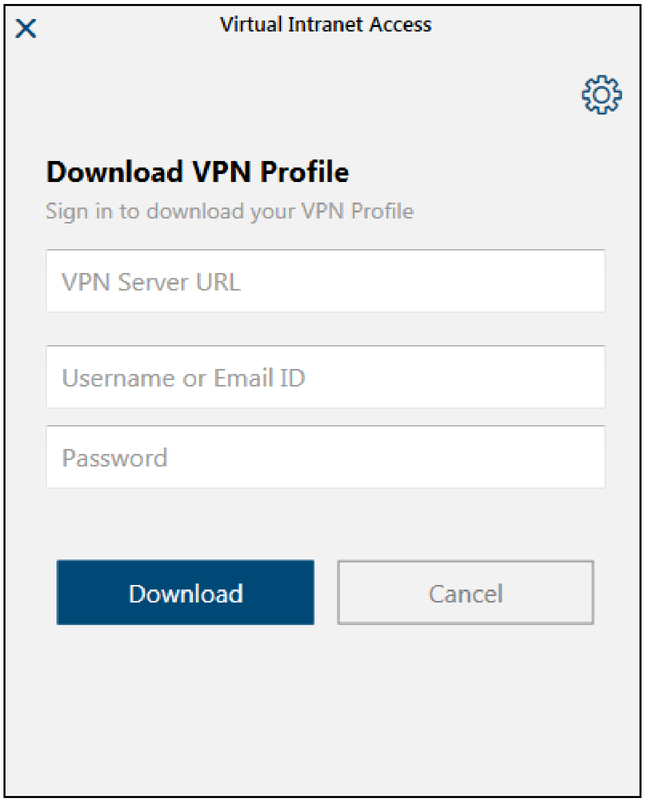
Downloading VPN Profiles

VPN profiles must be downloaded in order to connect VIA.

To download a VPN profile:

1. Open VIA.
2. Select **Click to download VPN profile** on the VPN download screen. The **Download VPN Profile** screen opens.
3. Enter the following details:
   - **VPN Server URL**: IP address or FQDN obtained from the system administrator.
   - **Username**: Username, domain username, or email ID.
   - **Password**: Password or domain password.

Figure 2 *Download VPN Profile Screen*



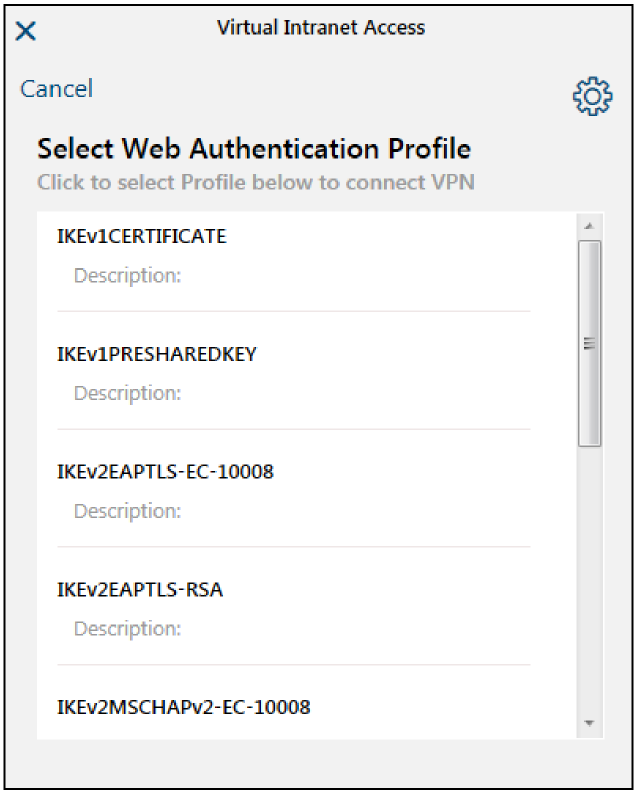
4. Click **Download**.
5. (Optional) A **Server certificate error** message appears if the server certificate does not match the server name. Click **Continue**.
6. (Optional) Select a web authentication profile from the **Web Authentication** list.

This screen only appears if the server has multiple web authentication profiles.

NOTE

If the **Web authentication** list contains more than one VIA authentication profile, users can select a VIA authentication profile. Upon successful authentication, the VIA client downloads the appropriate VIA connection profile.

Figure 3 *Web Authentication Profile List*



Virtual Intranet Access

Cancel

Select Web Authentication Profile

Click to select Profile below to connect VPN

IKEv1CERTIFICATE

Description:

IKEv1PRESHAREDKEY

Description:

IKEv2EAPTLS-EC-10008

Description:

IKEv2EAPTLS-RSA

Description:

IKEv2MSCHAPv2-EC-10008

7. (Optional) Select an **IKE Authentication Profile** from the **IKE Authentication** list.
8. (Optional) A message appears if a login banner has been uploaded to the controller. Click **Agree**.

VPN profile download is now complete.

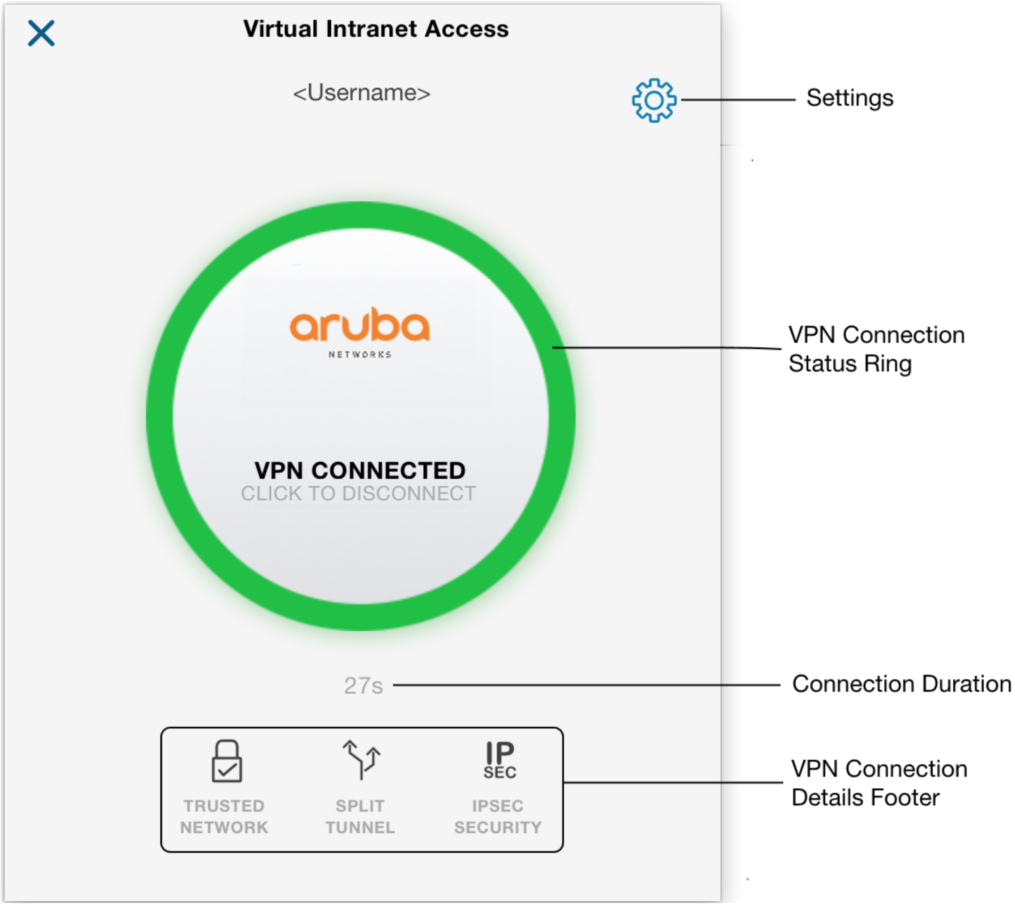
VIA UI Home Screen

The VIA home screen opens upon launching and connecting VIA. See Connecting and Disconnecting VIA and Connection Flows for more details on connecting VIA.

The home screen displays the following information about the VIA connection:

- **VPN Connection Status Ring**: Indicates if VIA is connected or disconnected.
- **Connection Duration**: Indicates the duration of the current session.
- **VPN Connection Details Footer**: Displays details about the VPN connection.
- **Settings Button**: Displays VIA settings, which include the **Network**, **VPN Profiles**, **Logs**, and **About** tabs.

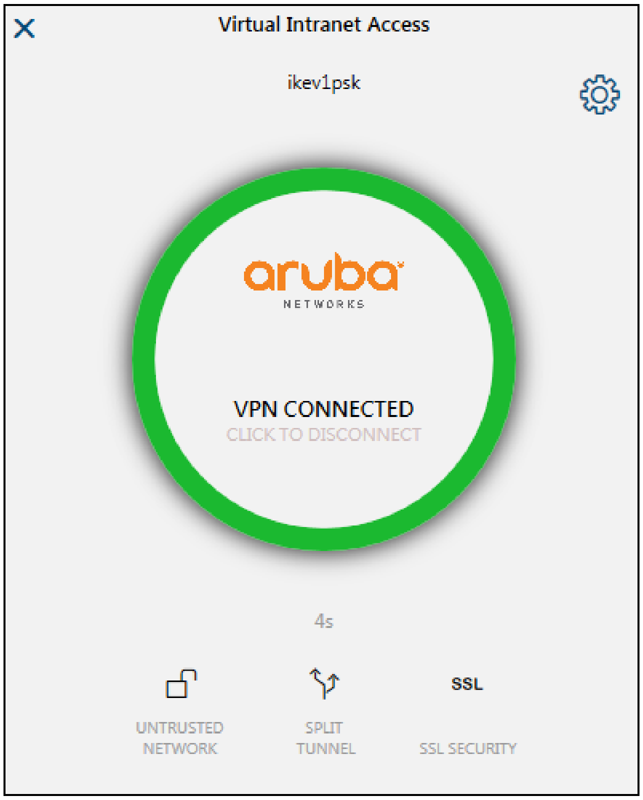
Figure 4 *VIA Home Screen UI Elements*



Connecting and Disconnecting VIA

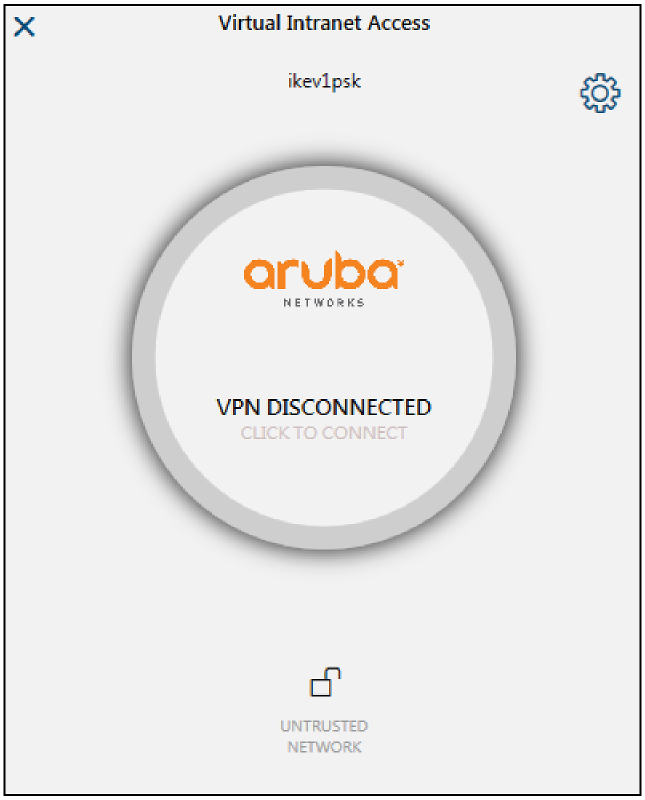
When VIA is connected, the VPN connection status ring on the home screen is green and displays a **VPN CONNECTED** status.

Figure 5 *VIA Connected*



When VIA is disconnected, the VPN connection status ring on the home screen is grey and displays a **VPN DISCONNECTED** status.

Figure 6 *VIA Disconnected*



Click the VPN connection status ring to connect or disconnect VIA.

Connection Flows

After VIA is installed and the VPN profile is downloaded, based on the way VIA is setup in your network, the VPN connection is established in one of the following ways:

Non-Certificate-Based Authentication

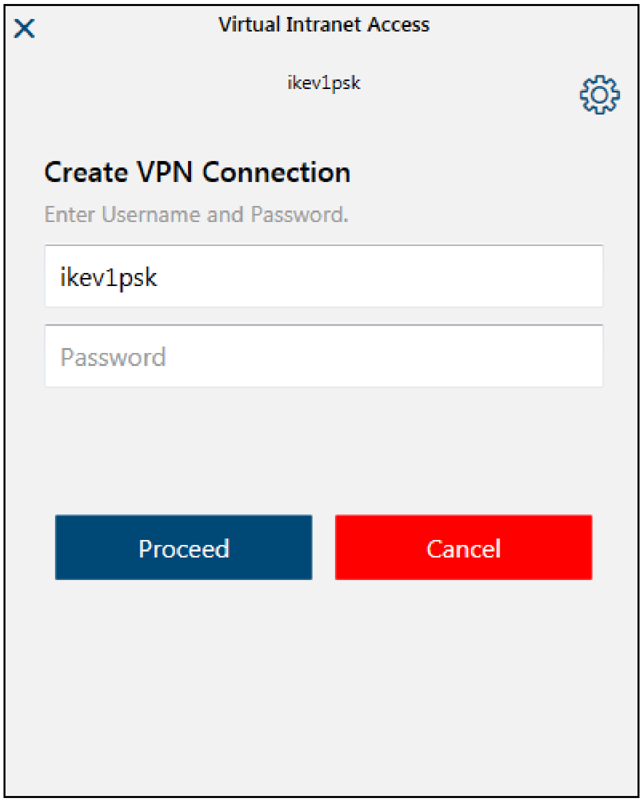
To establish a VPN connection without a using a certificate, click the VPN connection status ring on the VIA home screen. When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Non-Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using XAUTH:

1. Click the VPN connection status ring on the VIA home screen. The **Create VPN Connection** screen appears.
2. Enter your username/email ID and password.
3. Click **Proceed**.

Figure 7 *XAUTH Credentials*



Enter Username and Password.

ikev1psk

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

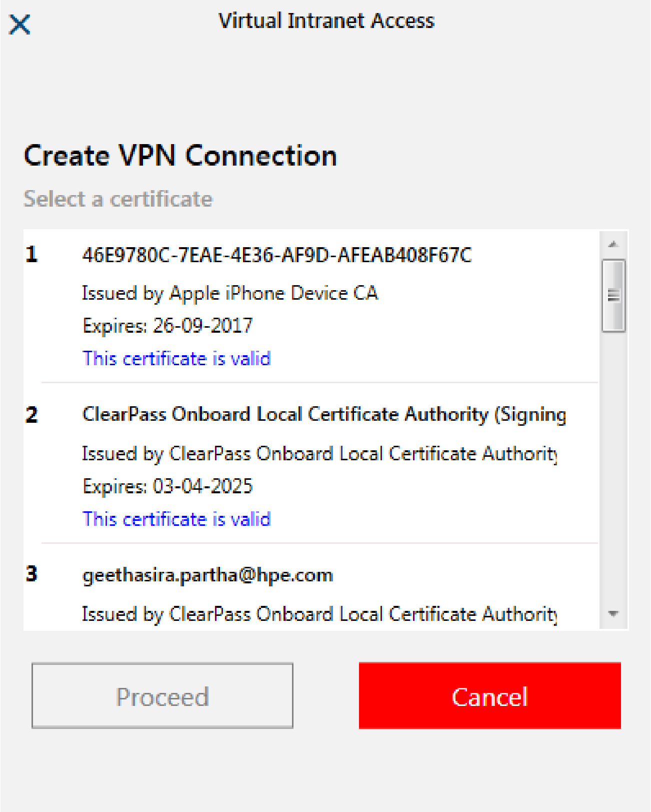
Certificate-Based Authentication

To establish a VPN connection using a certificate:

1. Click the VPN connection status ring on the VIA home screen. The **Select a Certificate** screen appears.

2. Select a certificate from the list.
3. Click **Proceed**.

Figure 8 *Certificate-based Authentication*



1 46E9780C-7EAE-4E36-AF9D-AFEAB408F67C
Issued by Apple iPhone Device CA
Expires: 26-09-2017
This certificate is valid

2 ClearPass Onboard Local Certificate Authority (Signing
Issued by ClearPass Onboard Local Certificate Authority
Expires: 03-04-2025
This certificate is valid

3 geethasira.partha@hpe.com
Issued by ClearPass Onboard Local Certificate Authority

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

NOTE

The Windows VIA client also supports authentication using a Virtual Smart Card (VSC) or Virtual Digital Badge (VDB) certificate stored in the Trusted Platform Module (TPM) of a windows device. Note that authentication using these methods requires configuration of the VSC or VDB by a network administrator prior to VIA configuration, and involve tasks outside the VIA configuration workflow, such as TPM initialization, the submittal of Certificate Signing Requests (CSRs), and key attestation. To unlock the certificate, the client system may prompt for the chosen PIN for the VDB (the first factor of the multi-factor authentication process), and once the certificate is unlocked, use that certificate for the actual authentication by the VIA client (the second factor of the multi-factor authentication.)

Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using a certificate and XAUTH:

1. Follow the steps in Certificate-Based Authentication.
2. Enter your username/email ID and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

VIA Tray Icon Behavior

Upon connecting, VIA automatically minimizes to the icon tray on the taskbar after two seconds. Click the VIA tray icon to display the VIA home screen. The VIA tray icon color indicates the current status of the network connectivity, as described below:

Table 4: *Network Connectivity Status*

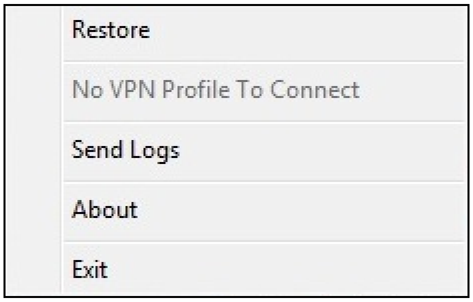
Tray icon Color	Description
⚫	No profile is downloaded in VIA.
🟠	Profile is downloaded but VPN is disconnected.
🟢	Profile is downloaded and VPN is connected.

VIA Tray Icon Menu

Click the VIA tray icon to display the menu with relevant quick options. This menu changes based on the status of the VIA application, as described below.

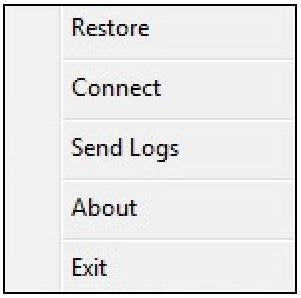
When no profile is downloaded, the following menu is displayed:

Figure 9 *No Profile Downloaded Menu*



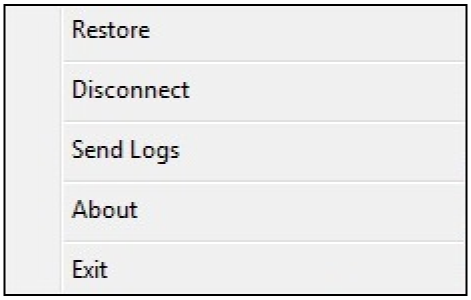
When a profile is downloaded but the VPN is not connected, the following menu is displayed:

Figure 10 *Profile Downloaded but VPN not Connected Menu*



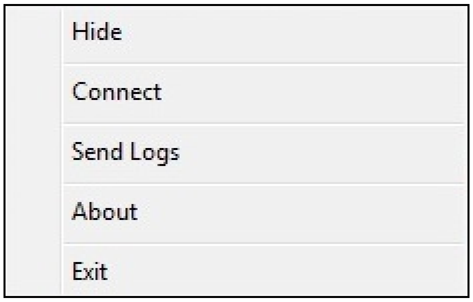
When a profile is downloaded and the VPN is connected, the following menu is displayed:

Figure 11 *VPN Connected Menu*



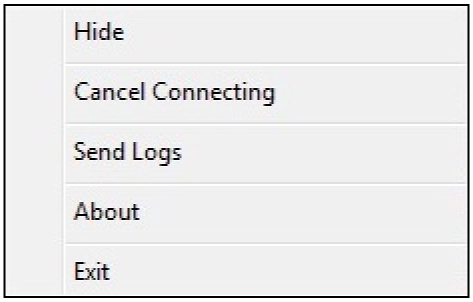
When VIA is detecting the network, the following menu is displayed:

Figure 12 *VIA Detecting Network Menu*



When VIA detects the network and establishes a connection, the following menu is displayed:

Figure 13 *Network Detected and Connection Establishing Menu*



The following list describes the functionality of all menu options:

- **Restore**: This option restores the VIA home screen.
- **Hide**: This option minimizes VIA to the icon tray.
- **Connect**: This option initiates the VPN connection.
- **Cancel Connecting**: This option stops the VPN connection attempt.
- **Disconnect**: This option disconnects the VPN connection.
- **Send Logs**: This option attaches a log file, which contains all logs collected by VIA, to your default email address. These logs can be sent to your help desk.
- **About**: This option displays the VIA **About** tab.
- **Exit**: This option disconnects the VPN connection and closes the VIA applicaion.

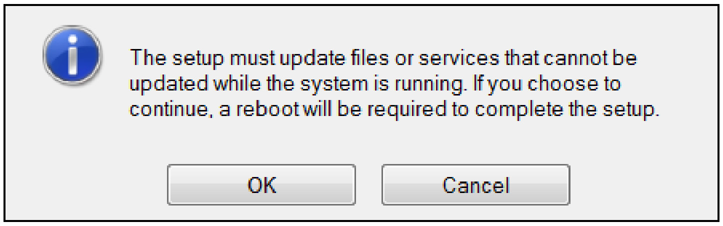
Uninstalling VIA

To uninstall VIA:

1. Navigate to **Control Panel > All Control Panel Items > Programs and Features**.
2. Select the Aruba VIA application.
3. Click **Uninstall**.
4. The **Are you sure you want to uninstall Virtual Intranet Access 3.2.0** message appears.
5. Click **Yes**.

6. The following message appears:

Figure 14 *Uninstall Reboot Message*



The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

7. Click **OK**.
8. Reboot your system.

VIA is successfully uninstalled.

Working with Settings

The following sections describe the different tabs and settings available in the VIA UI for Windows devices. Click the **Settings** button on the VIA home screen to view the following tabs:

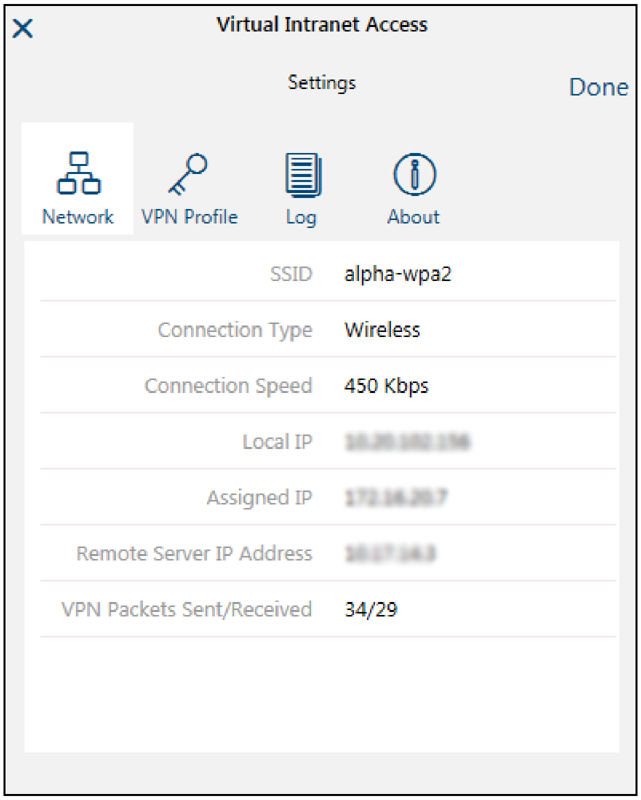
- Network on page 31
- VPN Profile on page 32
- Log on page 35
- About on page 36

Network

The **Network** tab provides the following information about your remote connection:

- **SSID**: SSID of the network.
- **Connection Type**: Type of connection.
- **Connection Speed**: Speed of the VPN connection, in Kbps.
- **Local IP**: Local IP address of the device.
- **Assigned IP**: Assigned IP address of the device.
- **Remote Server IP Address**: IP address of the remote server.
- **VPN Packet Sent/Received**: Number of VPN packets transmitted and received.

Figure 15 *Network Tab*



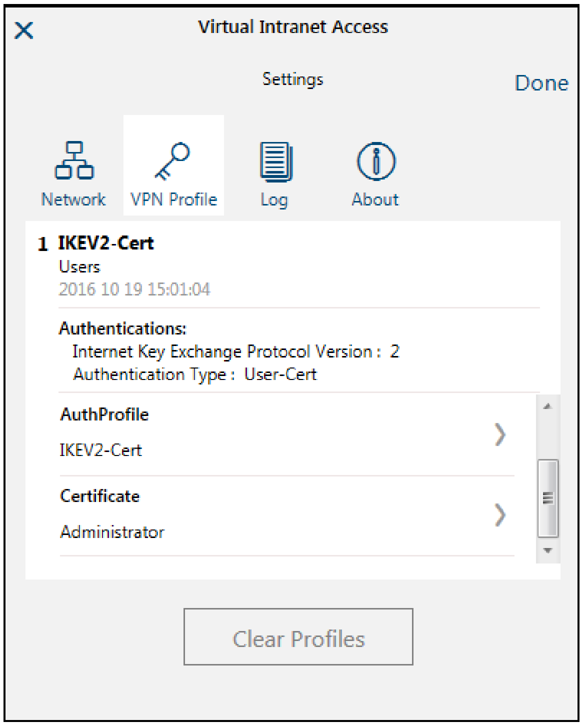
SSID	alpha-wpa2
Connection Type	Wireless
Connection Speed	450 Kbps
Local IP	[redacted]
Assigned IP	[redacted]
Remote Server IP Address	[redacted]
VPN Packets Sent/Received	34/29

VPN Profile

The **VPN Profile** tab displays the following information about each downloaded VPN profile:

- **Profile**: Name of the VPN profile, and the date and time that the profile was added.
- **Authentication**: IKE protocol version and authentication type.
- **Server**: IP address of the VPN server.
- **Auth Profile**: Web authentication profile.
- **Certificate**: VPN connection certificate (only for certificate-based authentication).

Figure 16 *VPN Profile Tab*



1 IKEV2-Cert
Users
2016 10 19 15:01:04

Authentications:
Internet Key Exchange Protocol Version : 2
Authentication Type : User-Cert

AuthProfile
IKEV2-Cert

Certificate
Administrator

Clearing Profiles

To clear a VPN profile:

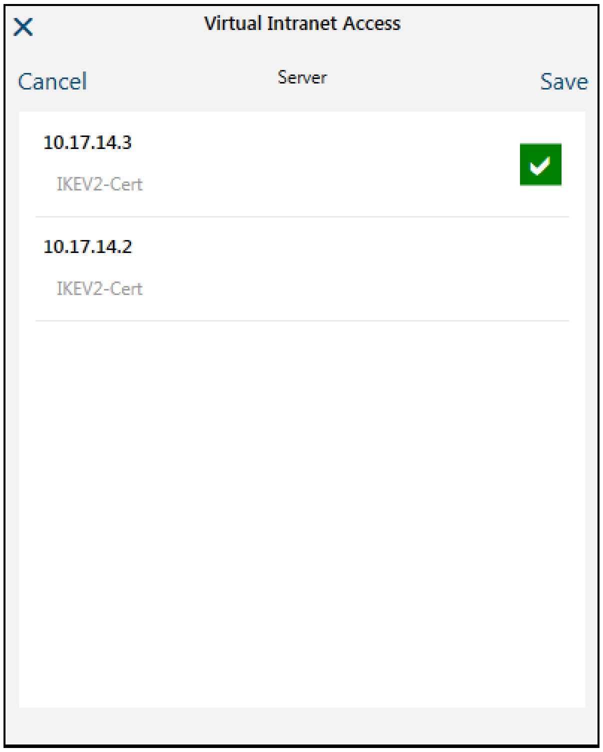
1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Click the **Settings** button, and then navigate to the **VPN Profile** tab.
3. Click **Clear Profiles**.

Changing the Server

To change the server:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Click the **Settings** button, and then navigate to the **VPN Profile** tab.
3. Click **Server**.
4. Select a different server from the list.
5. Click **Save**.

Figure 17 *Selecting a Server*



10.17.14.3 ☑
IKEV2-Cert

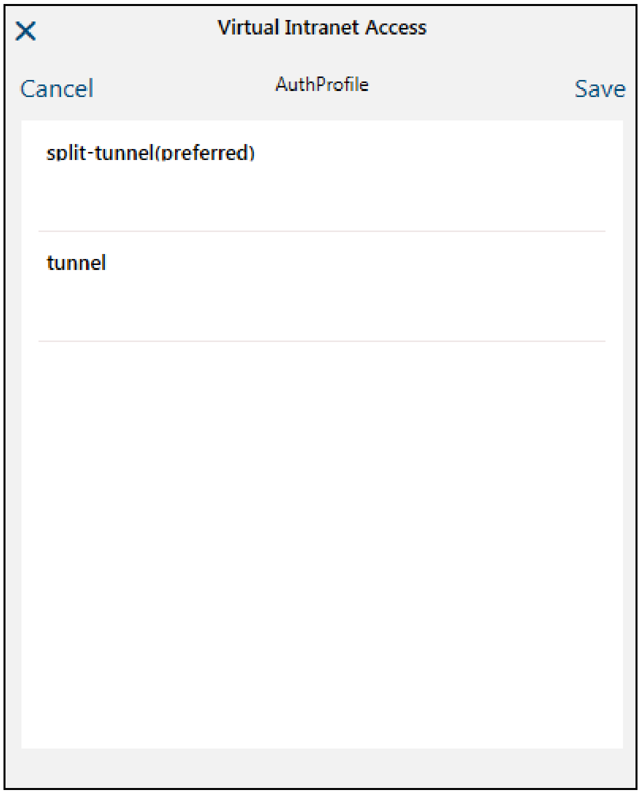
10.17.14.2
IKEV2-Cert

Changing the Authentication Profile

To change the authentication profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Click the **Settings** button, and then navigate to the **VPN Profile** tab.
3. Click **Auth Profile**.
4. Select a different authentication profile from the list.
5. Click **Save**.

Figure 18 *Changing the Authentication Profile*



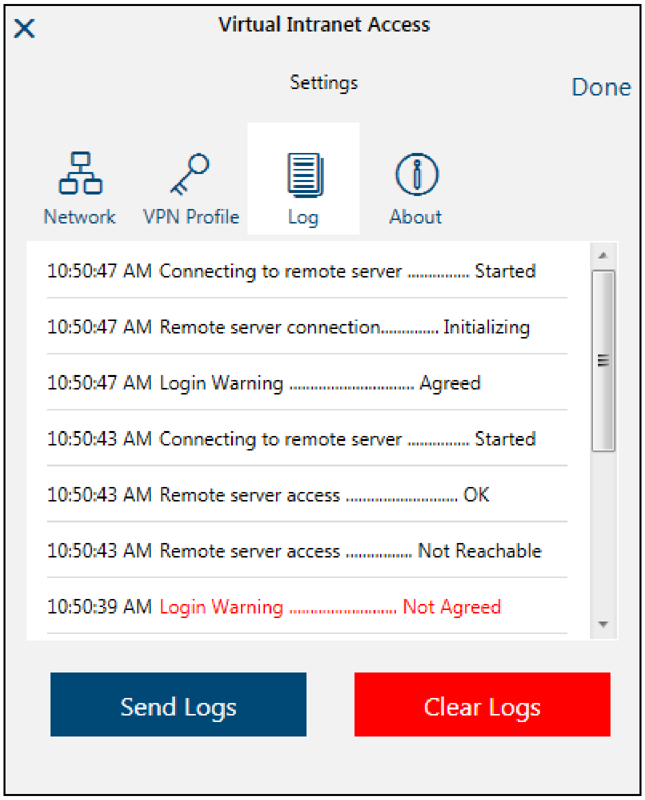
split-tunnel(preferred)

tunnel

Log

The **Log** tab displays all logs from the most recent sequence of events that have taken place since the application was launched.

Figure 19 *Log Tab*



```
10:50:47 AM Connecting to remote server .............. Started
10:50:47 AM Remote server connection............. Initializing
10:50:47 AM Login Warning ............................. Agreed
10:50:43 AM Connecting to remote server .............. Started
10:50:43 AM Remote server access .......................... OK
10:50:43 AM Remote server access ............... Not Reachable
10:50:39 AM Login Warning ........................ Not Agreed
```

- **Send Logs**: Attaches a log file that contains all logs collected by VIA to your default email address, which you can send to your help desk.
- **Clear Logs**: Clears the log history.

About

The **About** tab displays the VIA version and checks for any available upgrades.

Chapter 5
VIA Client for Linux

This section includes the following topics:

New Features

This section describes the features and enhancements introduced in VIA 3.x.x Linux Editions

Features Introduced in VIA 3.1 Linux Edition

Access to local resources are differentiated in full tunnel mode.

VIA clients can now access resources over the tunnel that are in the same network addressing range as the local network in full tunnel mode. If a VIA client and another machine are connected to the same router, the second machine was preventing access to similar addressed devices in the enterprise. The change in application behavior now ensures all network access requests go through the tunnel mode setup.

Features Introduced in VIA 3.0.0 Linux Edition

The following features are introduced in VIA 3.0.0 for Linux:

Auto-Config

Auto-config allows users to save the configuration settings in a configuration file, and then VIA refers to this configuration file to establish an IPsec session.

A copy of the configuration file template, **via-default.cfg**, is available in the **/usr/share/via/** folder. Copy this file template to a local folder and modify the settings based on your requirements. Once the configuration file is ready, execute the **via-cli load** <**config-file path**> command to load the configuration. If <**config-file path>** is not specified, VIA searches for the configuration file in the current folder. If the configuration file is not found, VIA searches for it in **~/.via**.

Table 5 lists the parameters available in the VIA configuration file:

Table 5: *Configuration File Parameters*

Parameter	Description	Input Type
ProfileGateway	IP address or host name of the server from which VIA downloads the profile.	String
ProfileUsername	Username to download the profile.	String
ProfilePassword	Password to download the profile.	String
ProfileAuthenticationProfile	Selected VIA authentication profile when there are multiple profiles.	String
ProfileIgnoreWarning	If this field is set to yes **[Y]**, HTTPS warnings are ignored while the profile is being downloaded.	Char [Y/N]
CertificateStoreKey	Certificate store key used when importing certificates.	String
CertificateDeleteAll	Deletes all existing certificates before importing any new certificates.	Char [Y/N]
CertificateImportPrivate	Imports a given **pfx** or **p12** certificate and certificate encryption key, separated by a comma. If multiple entries are imported, each entry must be separated by a semicolon.	String
CertificateImportPublic	Imports a given **cer** or **der** certificate. If multiple entries are imported, each entry must be separated by a semicolon.	String
AuthUsername	Username for XAUTH or MSCHAPv2.	String
AuthPassword	Password for XAUTH or MSCHAPv2.	String
AuthPIN	PIN number that is used when the certificate is enclosed with a subsystem that uses PIN (for example: smartcards)	4-digits numeric
AuthCertificateSubject	Identifies the certificate to be used for authentication.	String
AuthConnect	If this field is set to yes **[Y]**, VIA connects after the profile is downloaded.	Char [Y/N]
RouteEnable	If this field is set to yes **[Y]**, client side routing is enabled.	Char [Y/N]
RouteNetworks	IP address of the subnets. If multiple entries are added, each entry must be separated by a semicolon.	String

If the downloaded profile is marked as **auto connect**, VIA attempts to connect and uses the configuration file for any inputs.

Connection Failover

During connection failover, when a profile with more than one connection profile is configured, and the primary controller fails, failover to the secondary controller is triggered.

Support for Ubuntu 16.04

VIA 3.0.0 introduces support for Ubuntu 16.04.

NOTE

This feature is only supported on Linux devices.

VIA Gateway

NOTE

This feature is only available on Linux devices.

This feature has been implemented in the following topologies:

Simple Setup

This section describes the prerequisites and procedures for simple VIA gateway setup.

Prerequisites:

- Linux Client machine running Ubuntu 12.04/14.04/16.04 , CentOS 6, or RHEL 6.
- Controller running ArubaOS 6.5 or later.
- The IKEv2 configuration payload support for VIA clients (CFG_SET) feature must be enabled on the controller. Refer to the *ArubaOS 6.5.x User Guide* for more details.

NOTE

CFG_SET is only supported in ArubaOS 6.5 or later.

Procedure:

1. Configure the IKEv2 VIA profile on the controller.
2. Install VIA 3.0.0 on a Linux machine.
3. Enable VIA subnet routes on the controller by executing the **crypto-local isakmp allow-via-subnet-routes** command.
4. Use either the VIA configuration file (see Auto-Config on page 37) or manual operations to install and connect to VIA.
5. Disconnect VIA using the **via-cli vpn disconnect** command.
6. Set the routable networks using one of the following methods:
   - If you are using the auto configuration file, update the configuration file with **RouteEnable=Y**, and set the **RouteNetworks** appropriately. Force load the configuration using the **via-cli load config** command.
   - If you are connecting VIA using the UI, update the **/usr/share/via/via-updated.conf**, and then add the **RouteEnable=Y** and **RouteNetworks** values. Connect to VIA.
7. VIA sends an INFORMATIONAL-CFG_SET with the given subnets, as shown below:

```
Aug 14 17:44:42.686 [VPN INFO config_loader():config_loader.c:152] Loading cached
configuration file /usr/share/via/via-updated.conf
Aug 14 17:44:42.686 [VPN INFO config_loader_load_subnets():config_loader.c:253] Route
Networks(0):192.168.1.0 (108736)
Aug 14 17:44:42.686 [VPN INFO config_loader_load_subnets():config_loader.c:253] Route
Networks(1):255.255.255.0(16777215)
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]    I -->
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]    CFG_SET
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]     IP4_SUBNET(192.168.1.0
/255.255.255.0)
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]  spi={cb37cdce891b8db5
26f868cf9efd78ce} np=E{CP}
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]  exchange=INFORMATIONAL msgid=2
len=96
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678] #SEND 100 bytes to 10.10.2.184
[4500] (37.278)
```

8. The controller replies with an INFORMATIONAL-CFG_ACK, as shown below:

```
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678] #RECV 100 bytes from
10.10.2.184[4500] at 10.0.2.15 (37.483)
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]  spi={cb37cdce891b8db5
26f868cf9efd78ce} np=E{CP}
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]  exchange=INFORMATIONAL msgid=2
len=96
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]   I <--
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]    CFG_ACK
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]     IP4_SUBNET(192.168.1.0
/255.255.255.0)
Aug 14 17:44:42.891 [VPN DEBUG ike_cfg_response():ike_cfg.c:297] Ingoring Subnet config
Aug 14 17:44:42.891 [VPN DEBUG ike_cfg_response():ike_cfg.c:311] Recieved Acknowledgement
for CFG_SET
```

9. In the client machine, add an extra IP address to one of the interfaces and assign an IP address that is part of the subnet being tunneled.

   ```
   sudo ip addr add 192.168.1.1/24 dev eth0
   ```

10. From the subnet, try reaching the internal VLAN of the controller. In the following example, 172.16.31.1 is the internal IP of the controller:

    ```
    ping 172.16.31.1 -I 192.168.1.1
    ```

If a reply is received, setup is successful.

Setup using Virtual Machines

This section describes the prerequisites and procedures to setup a VIA gateway using virtual machines.

Prerequisites:

- Virtual Machine Host (Windows or Linux machine) that can host at least 2 virtual machines
- Two Virtual Machines
  - **VIA-VM**: Virtual machine with Linux running Ubuntu 12.04/14.04/16.04 , CentOS 6 or RHEL 6. Headless configuration (install minimal or server image).
  - **Win-VM**: Windows machine.
- Controller running ArubaOS 6.5 or later
- The IKEv2 configuration payload support for VIA clients (CFG_SET) feature must be enabled on the controller. Refer to the *ArubaOS 6.5.x User Guide* for more details.

Procedure:

1. Configure an IKEv2 VIA profile on the controller.
2. Install two virtual machines, as described in Prerequisites: on page 40.
   a. Configure the network such that VIA-VM has two interfaces, as described below:
      - **eth0**: NAT or bridge to ensure internet connectivity (set to DHCP if the setup environment allows).
      - **eth1**: Internal network (no NAT or bridge) to create a private network. Set to static IP 192.168.1.1/24.

   b. Configure the network such that Windows-VM has one interface with one adapter, as described below:
      - Set the adapter to the internal network (no NAT or Bridge) with either a static or DHCP IP in the range of 192.168.1.2-250, with 192.168.1.1 as the default gateway.

   c. Start both VMs.

   d. Ensure VIA-VM can connect to the Internet.

   e. Ensure Win-VM can connect to the VIA-VM on both interfaces (eth1:192.168.1.1, eth0:other ip assigned by DHCP).

   - Enable routing in VIA-VM (sudo echo 1 > /proc/sys/net/ipv4/ip_forward). Ensure Win-VM can reach the eth0 address of VIA-VM. Restart VIA-VM, if necessary.

3. Install VIA 3.0.0 on a Linux machine.
4. Use the VIA configuration file to install certificates and connect to VIA (see Auto-Config on page 37).
5. Disconnect VIA using the **via-cli vpn disconnect** command.
6. Set the routable networks by updating the configuration file. Update the configuration file with **RouteEnable=Y**, and set the **RouteNetworks** appropriately. Force load the configuration by using the **via-cli load config** command.
7. VIA sends an INFORMATIONAL-CFG_SET with the given subnets, as shown below:

```
Aug 14 17:44:42.686 [VPN INFO config_loader():config_loader.c:152] Loading cached
configuration file /usr/share/via/via-updated.conf
Aug 14 17:44:42.686 [VPN INFO config_loader_load_subnets():config_loader.c:253] Route
Networks(0):192.168.1.0 (108736)
Aug 14 17:44:42.686 [VPN INFO config_loader_load_subnets():config_loader.c:253] Route
Networks(1):255.255.255.0(16777215)
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]    I -->
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]    CFG_SET
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]     IP4_SUBNET(192.168.1.0
/255.255.255.0)
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]  spi={cb37cdce891b8db5
26f868cf9efd78ce} np=E{CP}
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678]  exchange=INFORMATIONAL msgid=2
len=96
Aug 14 17:44:42.686 [VPN DEBUG LOG_from_mocana():log.c:678] #SEND 100 bytes to 10.10.2.184
[4500] (37.278)
```

8. The controller replies with an INFORMATIONAL-CFG_ACK, as shown below:

```
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678] #RECV 100 bytes from
10.10.2.184[4500] at 10.0.2.15 (37.483)
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]  spi={cb37cdce891b8db5
26f868cf9efd78ce} np=E{CP}
Aug 14 17:44:42.890 [VPN DEBUG LOG_from_mocana():log.c:678]  exchange=INFORMATIONAL msgid=2
len=96
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]   I <--
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]    CFG_ACK
Aug 14 17:44:42.891 [VPN DEBUG LOG_from_mocana():log.c:678]     IP4_SUBNET(192.168.1.0
/255.255.255.0)
Aug 14 17:44:42.891 [VPN DEBUG ike_cfg_response():ike_cfg.c:297] Ingoring Subnet config
Aug 14 17:44:42.891 [VPN DEBUG ike_cfg_response():ike_cfg.c:311] Recieved Acknowledgement
for CFG_SET
```

9. From Win-VM, try reaching the internal VLAN of the controller. In the follwoing example, 172.16.31.1 is the internal IP of the controller:

```
Ping 172.16.31.1.
```

If a reply is received, setup is successful.

VIA User Interface

VIA 3.0.0 introduces a new User Interface (UI).

Prerequisites

Ensure that the end-user system meets the following prerequisites:

- Supported Operating Systems:
  - Ubuntu 12.04, 14.04, and 16.04
  - Red Hat Enterprise Linux (RHEL) 6.0
  - CentOS 6.0
- Administrator privileges on the computer.

- Computer connected to a working wired or wireless network.
- Previously installed versions of VIA must be uninstalled. For information on uninstalling VIA, see Uninstalling VIA on page 50.
- Up-to-date computer:
  - Execute the following commands for Ubuntu:

    ```
    sudo apt-get update
    sudo apt-get upgrade
    ```

  - Execute the following command for RHEL and CentOS:

    ```
    yum update
    ```

Downloading VIA

To download VIA:

1. Login to the Aruba Support Site.
2. Navigate to **Download Software > VIA > Linux**
3. Download the installer file that is appropriate for your operating system and architecture. The file-naming format of the installer is **via-<version>.<osname><architecture>.<ext>**, and the supported file extensions are **.deb** and **.rpm**. For example, for RHEL and CentOS 64 bit, the VIA 3.0.0. file name is **via-3.0.0.82618-rhel6-x86_64_bin** whereas for Ubuntu 32 bit , the file name is **via-3.0.0.82618-ubuntu1204-i386_bin**.

Installing VIA

Ensure that all prerequisites have been met before proceeding with installation.

To install VIA:

1. Mark the downloaded installer file as executable:
   a. Right-click the installer file.
   b. Click **Permissions**.
   c. Select the checkbox for **Allow executing file as program**, and then click **Close**.

   Alternatively, you can run the **chmod +x filename** command to mark the downloaded file as an executable file.
2. Double-click the executable installer file to begin the installation process. The **VIA Setup Wizard** opens and displays the welcome screen.
3. Click **Next**.
4. On the **End-User License Agreement** screen, select the checkbox for **I agree to the terms of the license**. Click **Next**.
5. The **Installing** screen appears. After installation is complete, the **Finished** screen appears, indicating successful installation.
6. Click **Finish**. You will be prompted to enter the storage password to initialize VIA.
7. Enter the storage password, and then click **OK** to complete installation.

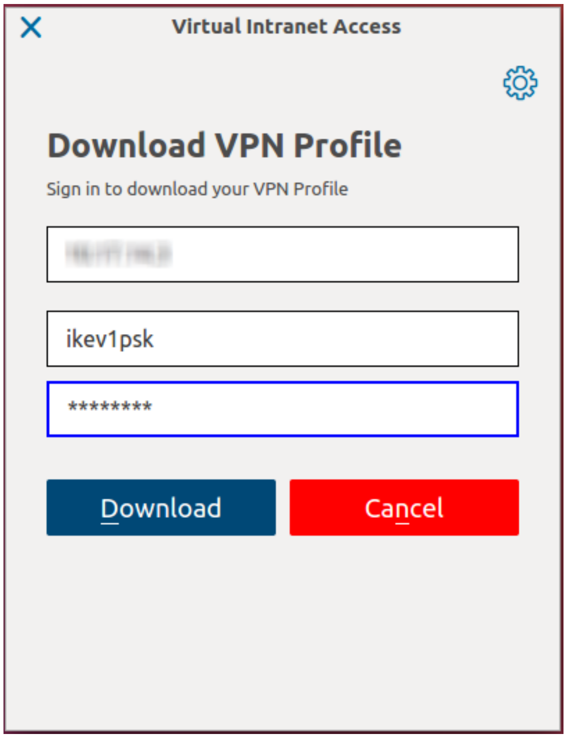
Downloading VPN Profiles

VPN profiles must be downloaded in order to connect VIA.

To download a VPN profile:

1. Open VIA.
2. Select **Click to download VPN profile** on the VPN download screen. The **Download VPN Profile** screen appears
3. Enter the following details:
   a. **VPN Server URL**: IP Address or FQDN provided by the administrator.
   b. **Username or Email ID**: Username, domain username, or email ID.
   c. **Password**: Password or domain password.

Figure 20 *VPN Profile Download*



Virtual Intranet Access

Download VPN Profile

Sign in to download your VPN Profile

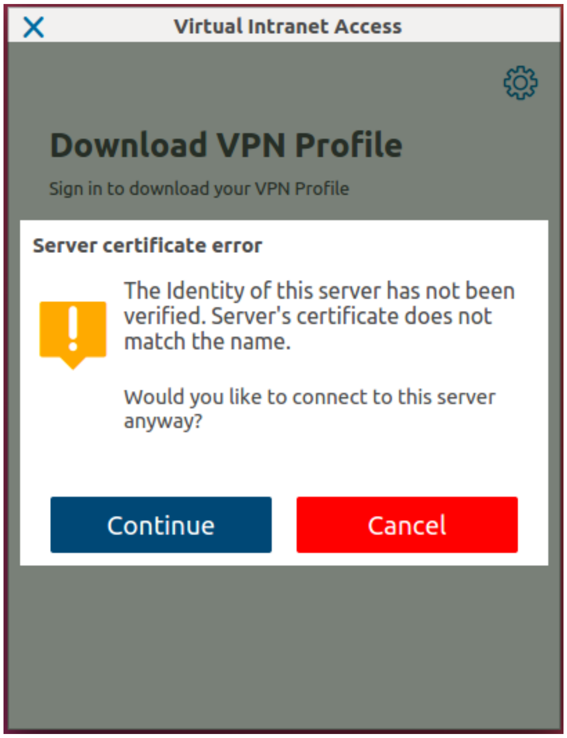
[redacted]

ikev1psk

****

4. Click **Download**.
5. (Optional) A **Server certificate error message** appears if the server certificate name does not match the server name. Click **Continue**.

Figure 21 *Server Certificate Error*



Virtual Intranet Access

Download VPN Profile

Sign in to download your VPN Profile

Server certificate error

The Identity of this server has not been verified. Server's certificate does not match the name.

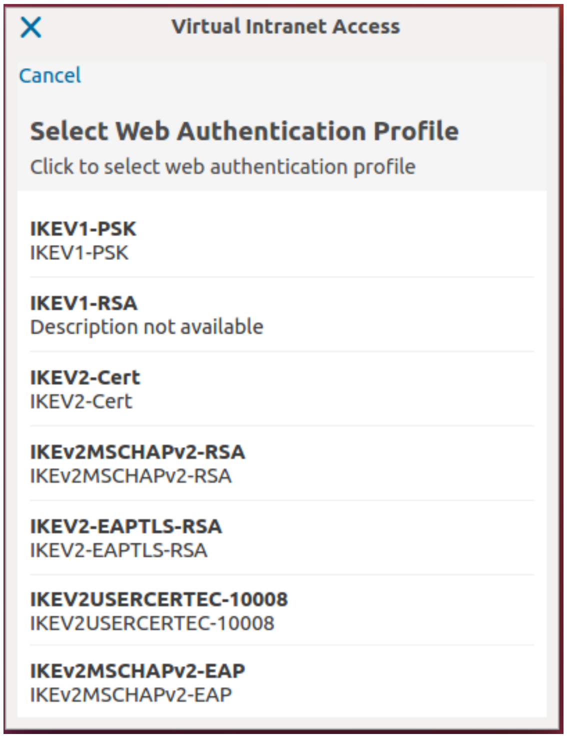
Would you like to connect to this server anyway?

6. (Optional) Select a web authentication profile from the **Web Authentication Profile** list.

NOTE This screen only appears if the server has multiple web authentication profiles.

If the web authentication list has more than one VIA authentication profile, users can select a VIA authentication profile. Upon successful authentication, the VIA client downloads the appropriate VIA connection profile.

Figure 22 *Web Authentication Profile List*



Virtual Intranet Access

Select Web Authentication Profile

Click to select web authentication profile

IKEV1-PSK
IKEV1-PSK

IKEV1-RSA
Description not available

IKEV2-Cert
IKEV2-Cert

IKEv2MSCHAPv2-RSA
IKEv2MSCHAPv2-RSA

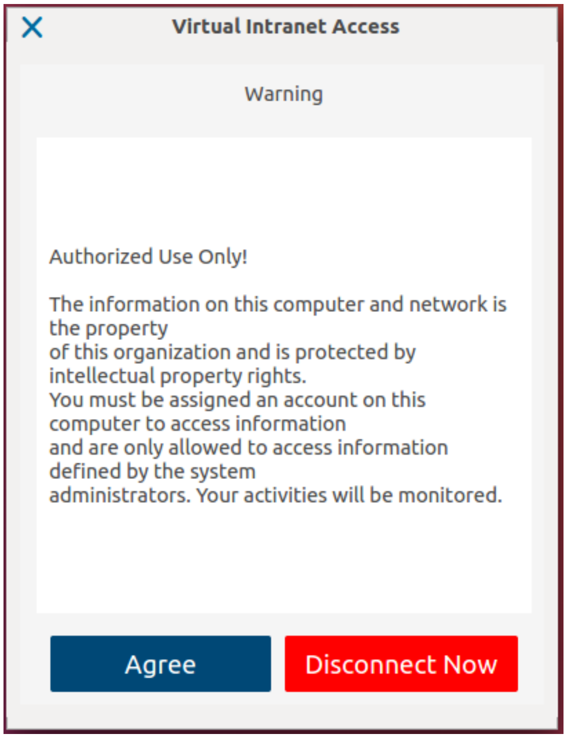
IKEV2-EAPTLS-RSA
IKEV2-EAPTLS-RSA

IKEV2USERCERTEC-10008
IKEV2USERCERTEC-10008

IKEv2MSCHAPv2-EAP
IKEv2MSCHAPv2-EAP

7. (Optional) A message appears if a login banner has been uploaded to the controller. Click **Agree**.

Figure 23 *Login Banner Screen*



Authorized Use Only!

The information on this computer and network is the property
of this organization and is protected by intellectual property rights.
You must be assigned an account on this computer to access information
and are only allowed to access information defined by the system
administrators. Your activities will be monitored.

VPN profile download is now complete.

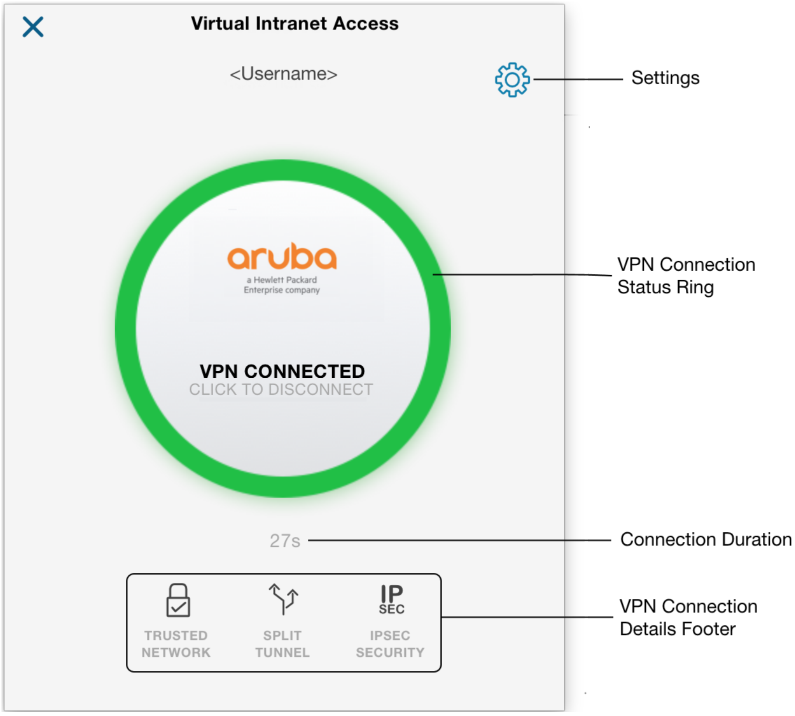
VIA UI Home Screen

The VIA home screen opens upon launching and connecting VIA. See Connecting and Disconnecting VIA on page 46 and Connection Flows on page 47 for more details on connecting VIA.

The home screen displays the following information about the VIA connection:

- **VPN Connection Status Ring**: Indicates if the VPN is connected or disconnected.
- **Connection Duration**: Indicates the duration of the current session.
- **VPN Connection Details Footer**: Displays details about the VPN connection.
- **Settings**: Displays VIA settings, which include the **Network**, **VPN Profiles**, **Logs**, **Certificates**, and **About** tabs.

Figure 24 *VIA Home Screen UI Elements*

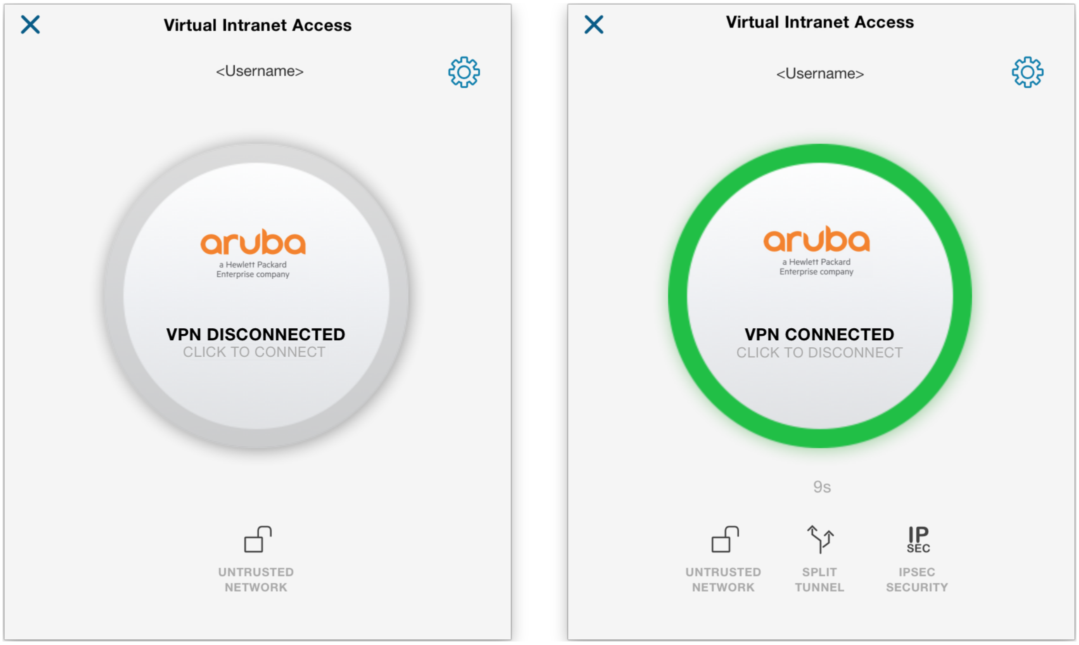


Connecting and Disconnecting VIA

When VIA is connected, the VPN connection status ring on the home screen is green and displays a **VPN CONNECTED** status.

When VIA is disconnected, the VPN connection status ring on the home screen is grey and displays a **VPN DISCONNECTED** status.

Figure 25 *VIA Disconnected and Connected*



Click the VPN connection status ring to connect or disconnect VIA.

Connection Flows

After VIA is installed and the VPN profile is downloaded, based on the way VIA is setup in your network, the VPN connection is established in one of the following ways:

Non-Certificate-Based Authentication

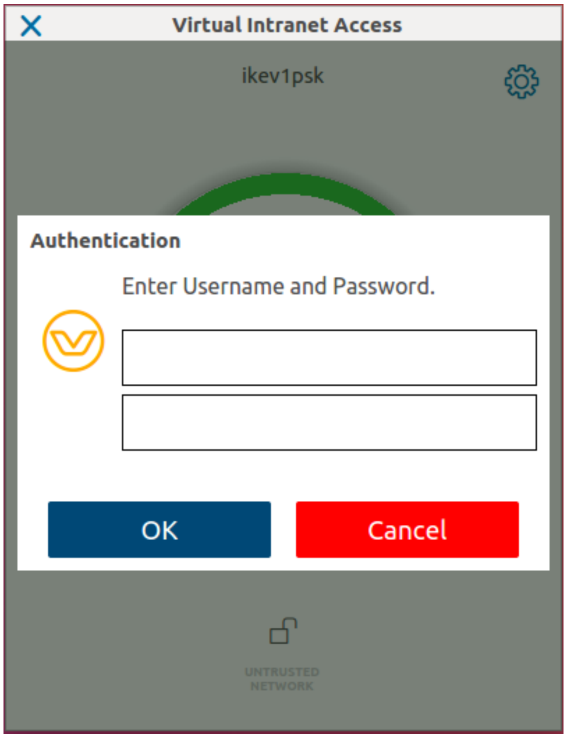
To establish a VPN connection without using a certificate, click the VPN connection status ring on the VIA home screen. When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Non-Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using XAUTH:

1. Click the VPN connection status ring on the VIA home screen. The **Authentication** screen appears.

Figure 26 *XAUTH Credentials*



Authentication

Enter Username and Password.

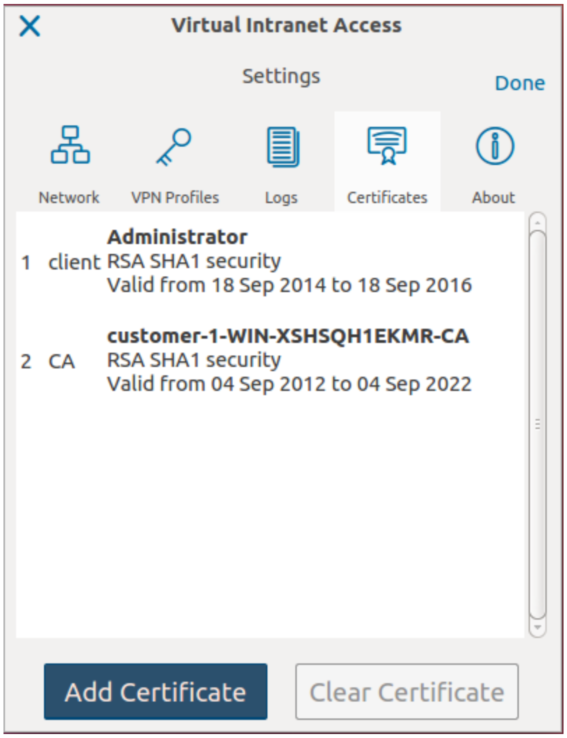
2. Enter your username and password.
3. Click **OK**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication

1. Click the VPN connection status ring on the VIA home screen. The **Select a Certificate** screen appears.

Figure 27 *Selecting a Certificate*



1 client **Administrator**
RSA SHA1 security
Valid from 18 Sep 2014 to 18 Sep 2016

2 CA **customer-1-WIN-XSHSQH1EKMR-CA**
RSA SHA1 security
Valid from 04 Sep 2012 to 04 Sep 2022

2. Select a certificate from the list. If the relevant certificate is not listed, you can add the certificate:
   a. Click **Add Certificate**.
   b. Locate and select the certificate from your local file explorer. The certificate is now added to the list.
   c. Select the newly added certificate.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication with Extended Authentication (XAUTH_

1. Follow the steps in Certificate-Based Authentication on page 47. The XAUTH **Authentication** page appears, as shown in Figure 26.
2. Enter your username and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

VIA Tray Icon Behavior

Upon connecting, VIA automatically minimizes to the top menu bar after two seconds. Click the VIA tray icon to display the VIA home screen. The VIA tray icon color indicates the current status of the network connectivity, as described below:

Table 6: *Network Connectivity Status*

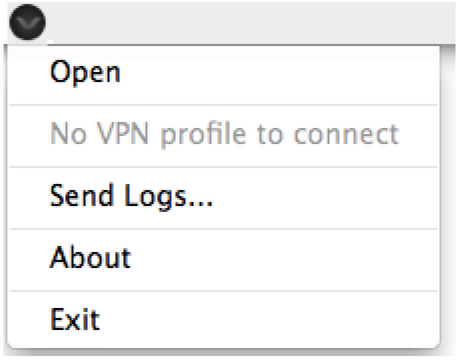
Tray icon Color	Description
⚫	No profile is downloaded in VIA.
🟠	Profile is downloaded but VPN is disconnected.
🟢	Profile is downloaded and VPN is connected.

VIA Tray Icon Menu

Click the VIA tray icon to display the menu with relevant quick options. This menu changes based on the status of the VIA application, as described below.

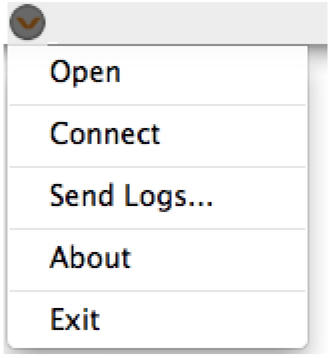
When no profile is downloaded, the following menu is displayed:

Figure 28 *No Profile Downloaded Menu*



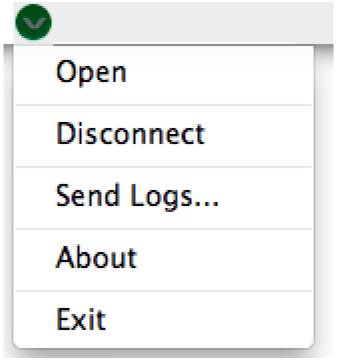
When a profile is downloaded but the VPN is not connected, the following menu is displayed:

Figure 29 *Profile Downloaded but VPN not Connected Menu*



When a profile is downloaded and the VPN is connected, the following menu is displayed:

Figure 30 *VPN Connected Menu*



The following list describes the functionality of all menu options:

- **Open**: This option displays the VIA home page.
- **Connect**: This option initiates the VPN connection.
- **Disconnect**: This option disconnects the VPN connection.
- **Send Logs**: This option attaches a log file, which contains all logs collected by VIA, to your default email address. These logs can be sent to your help desk.
- **About**: This option displays the VIA **About** tab.
- **Exit**: This option disconnects the VPN connection and closes the VIA application.

Uninstalling VIA

To uninstall VIA:

Ubuntu

1. Navigate to the **Ubuntu Software Center**.
2. Select the VIA application, and then click **Remove**.

You can also uninstall the VIA application using the CLI by executing the **sudo apt-get purge via** command.

RHEL and CentOS

1. Navigate to **System > Administration > Add/Remove software**.
2. Deselect **VIA**, and then click **Clear**.

You can also uninstall the VIA application using the CLI by executing the **sudo yum remove via** command.

Working with Settings

The following sections describe the different tabs and settings available in the VIA UI for Linux devices. Click the **Settings** button on the VIA home screen to view the following tabs:

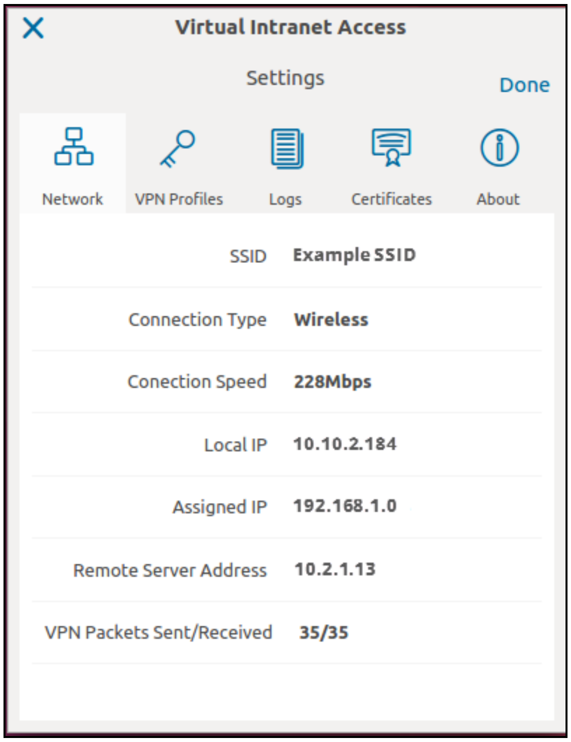
- Network on page 51
- VPN Profiles on page 51
- Logs on page 52
- Certificates on page 53
- About on page 54

Network

The **Network** tab provides the following information about your remote connection:

- **SSID**: SSID of the network.
- **Connection Type**: Type of connection.
- **Connection Speed**: Speed of the VPN connection.
- **Local IP**: Local IP address of the device.
- **Assigned IP**: Assigned IP address of the device.
- **Remote Server IP Address**: IP address of the remote server.
- **VPN Packet Sent/Received**: Number of VPN packets transmitted and received.

Figure 31 *Network Tab*



SSID Example SSID

Connection Type Wireless

Conection Speed 228Mbps

Local IP 10.10.2.184

Assigned IP 192.168.1.0

Remote Server Address 10.2.1.13

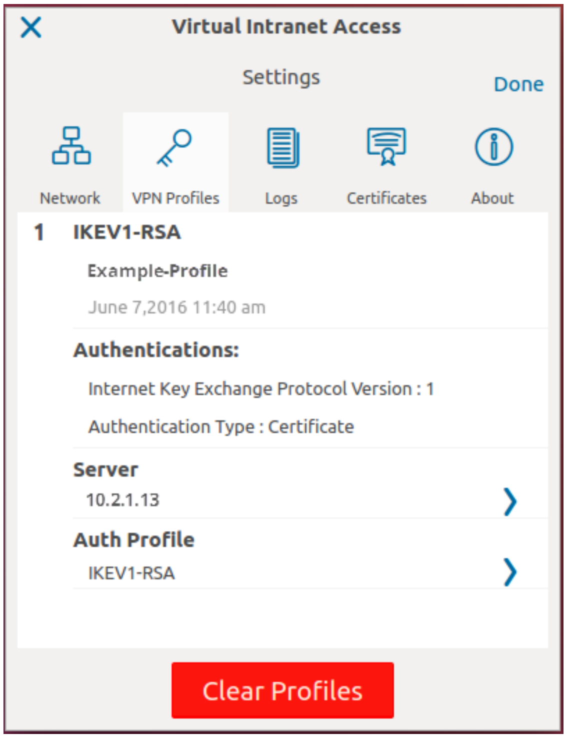
VPN Packets Sent/Received 35/35

VPN Profiles

The **VPN Profile** tab displays the following information about each downloaded VPN profile:

- **Profile**: Name of the VPN profile, and the date and time that the profile was added.
- **Authentications**: IKE protocol version and authentication type.
- **Server**: IP address of the VPN server.
- **Auth Profile**: Web authentication profile.
- **Certificate**: VPN connection certificate (only for certificate-based authentication).

Figure 32 *VPN Profiles Tab*



1 IKEV1-RSA

Example-Profile

June 7,2016 11:40 am

Authentications:

Internet Key Exchange Protocol Version : 1

Authentication Type : Certificate

Server

10.2.1.13

Auth Profile

IKEV1-RSA

Clearing Profiles

To clear profiles:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles**.
3. Click **Clear Profiles**.

Changing the Server

To change the server:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles** > **Server**.
3. Select a different server from the list.
4. Click **Save**.

Changing the Authentication Profile

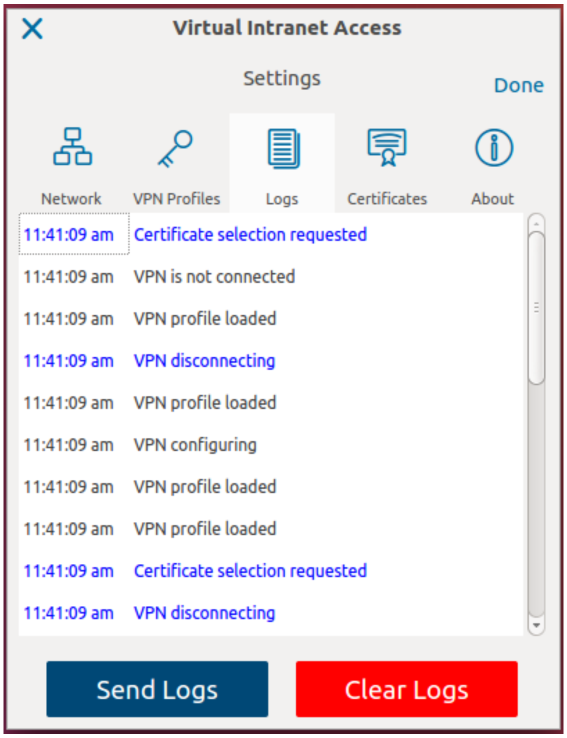
To change the authentication profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles** >**Auth Profile**.
3. Select a different authentication profile from the list.
4. Click **Save**.

Logs

The **Logs** tab displays all logs from the most recent sequence of events that have taken place since the application was launched.

Figure 33 *Logs Tab*



```
11:41:09 am   Certificate selection requested
11:41:09 am   VPN is not connected
11:41:09 am   VPN profile loaded
11:41:09 am   VPN disconnecting
11:41:09 am   VPN profile loaded
11:41:09 am   VPN configuring
11:41:09 am   VPN profile loaded
11:41:09 am   VPN profile loaded
11:41:09 am   Certificate selection requested
11:41:09 am   VPN disconnecting
```

- **Send Logs**: Attaches a log file that contains all logs collected by VIA to your default email address, which you can send to your help desk.
- **Clear Logs**: Clears the log history.

Certificates

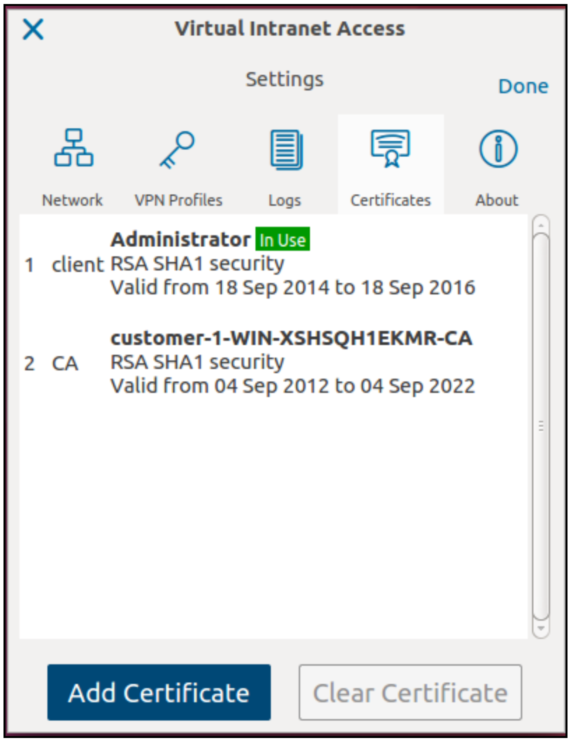
The **Certificates** tab lists all installed certificates. You can also add and clear certificates.

Changing the VPN Connection Certificate

To change the VPN connection certificate for certificate-based authentication:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **Certificates**.
3. Select a different certificate from the list, as shown in Figure 34.

Figure 34 *Certificate List*



1	client	**Administrator** In Use RSA SHA1 security Valid from 18 Sep 2014 to 18 Sep 2016
2	CA	**customer-1-WIN-XSHSQH1EKMR-CA** RSA SHA1 security Valid from 04 Sep 2012 to 04 Sep 2022

4. Click **Done**.

Adding a New VPN Connection Certificate

To add a new VPN certificate:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **Certificates**.
3. Click **Add Certificate**.
4. Locate and select the certificate.
5. Click **Open**.

The certificate is now added to the certificate list in VIA.

NOTE

Only .p12 and .pfx certificate formats are supported.

About

The **About** tab displays the VIA version and checks for any available upgrades.

Chapter 6
VIA Client For Android

This section includes the following topics:

New Features

This section describes the features and enhancements introduced in VIA 3.x.x Android Editions

Features Introduced in VIA 3.0.0 Android Edition

Side Loading

The Android side-loading feature allows users to save configuration settings in a configuration file that VIA can refer to when attempting to establish a VIA connection.

To obtain the configuration file:

1. Navigate to **https://<mobility-master>/via**, where <mobility-master> is the IP address of your Mobility Master server.
2. Enter your VIA user login credentials to log in to Mobility Master.
3. After successfully login in, change the URL to **https://<mobility-master>/via/config?ikever=**
4. Save the xml returned by Mobility Master into a file named **via_config.xml**.

To add the configuration file to Android devices, copy the **via_config.xml** file to the root directory of the file system on the Android device(s) that should use this feature. On startup, if VIA does not have a profile already provisioned on the device, VIA will load the connection profile data from the **via_config.xml** file.

Lockdown All Settings

Network administrators can enable the **Lockdown All Settings** knob on the controller to prevent profile setting changes on the VIA client. When this knob is enabled, users cannot clear profiles or edit any settings on the **VPN Profiles** tab, including the server and authentication profile.

Support for Samsung Knox™

VIA 3.0.0 introduces support for Samsung Knox™ to enhance security and provide mobile device management (MDM) integration. This feature includes:

- Implementation of the Knox VPN service and APIs. Refer to the *Samsung Knox™ Vendor Integration Guide* for more details.
- Automatic VIA profile provisioning in a Knox/MDM-controlled environment.
- Use of a generic Knox VPN framework to setup IPSec VPN tunnels.
- Support for dual IPSec tunnels. VIA can be used as an outer or inner tunnel in a dual tunnel environment.

- Support for IPSec VPN tunnels inside the Knox container.

VIA supports Knox features on Samsung devices with Knox 2.2 and onwards.

This feature is only supported on Android devices.

VIA User Interface

VIA 3.0.0 introduces a new User Interface (UI).

Prerequisites

Ensure that your system meets the following prerequisites:

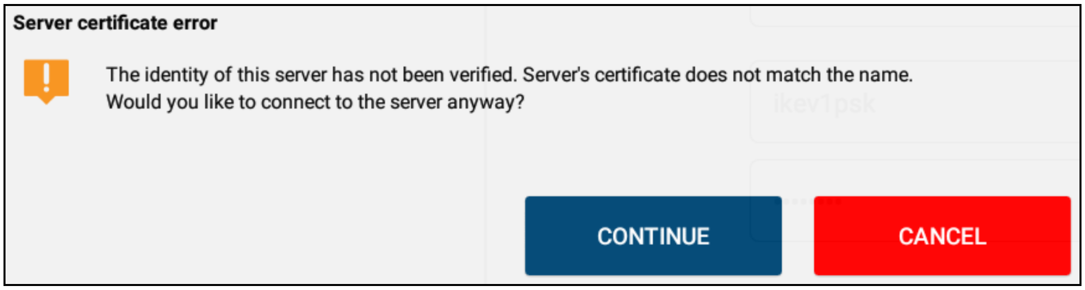
- Device is running one of the following Android versions:
  - 4.x
  - 5.0
  - 6.x
  - 7.x
- Device is connected to a network.

Downloading VIA

To download Aruba VIA:

1. Open **Play Store** to download the Aruba VIA application. Installation is performed automatically once VIA is downloaded.
2. After installation is complete, open VIA.
3. Select **Click to download VPN profile** from the home screen. The **Download VPN Profiles** screen appears.
4. Enter the following details:
   - **Server URL**: IP address or FQDN obtained from the system administrator.
   - **Username**: Username, domain username, or email ID.
   - **Password**: Password or domain password.
5. Click **Download**.
6. (Optional) A **Server certificate error** message appears if the server certificate does not match the server name. Click **Continue**.

Figure 35 *Server Certificate Error*



Server certificate error

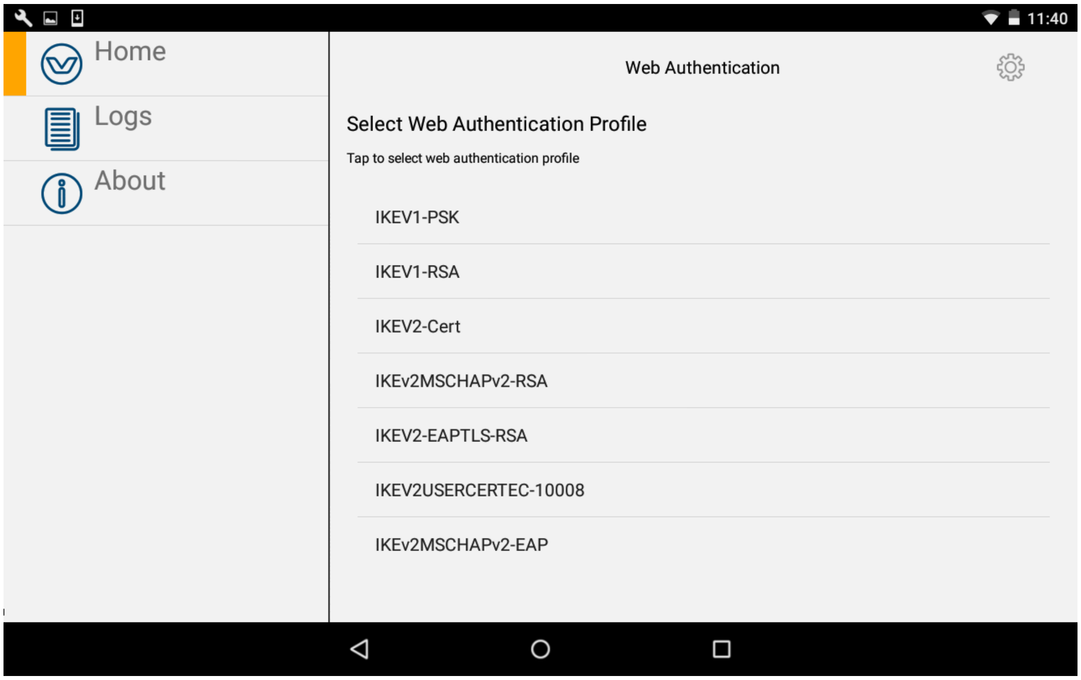
The identity of this server has not been verified. Server's certificate does not match the name.
Would you like to connect to the server anyway?

7. (Optional) Select a web authentication profile from the **Web Authentication** list.

This screen only appears if the server has multiple web authentication profiles.

If the **Web authentication** list contains more than one VIA authentication profile, users can select a VIA authentication profile. Upon successful authentication, the VIA client downloads the appropriate VIA connection profile.

Figure 36 *Web Authentication Profile List on Tablet and Mobile Device*



Select Web Authentication Profile

Tap to select web authentication profile

IKEV1-PSK

IKEV1-RSA

IKEV2-Cert

IKEv2MSCHAPv2-RSA

IKEV2-EAPTLS-RSA

IKEV2USERCERTEC-10008

IKEv2MSCHAPv2-EAP

8. (Optional) Select an **IKE Authentication Profile** from the **IKE Authentication** list.

VPN profile download is now complete.

VIA UI Home Screen

The VIA home screen opens upon launching and connecting VIA. See Connecting and Disconnecting VIA on page 59 and Connection Flows on page 60 for more details on connecting VIA.

The home screen displays the following information about the VIA connection:

- **VPN Connection Status Ring**: Indicates if VIA is connected or disconnected.
- **Connection Duration**: Indicates the duration of the current session.
- **VPN Connection Details Footer**: Displays details about the VPN connection.
- **Settings Button**: (Only for mobile devices) Displays VIA settings, which include the **Network**, **VPN Profiles**, **Logs**, and **About** tabs.

Figure 37 *Android Home Screen UI Elements - Tablet*

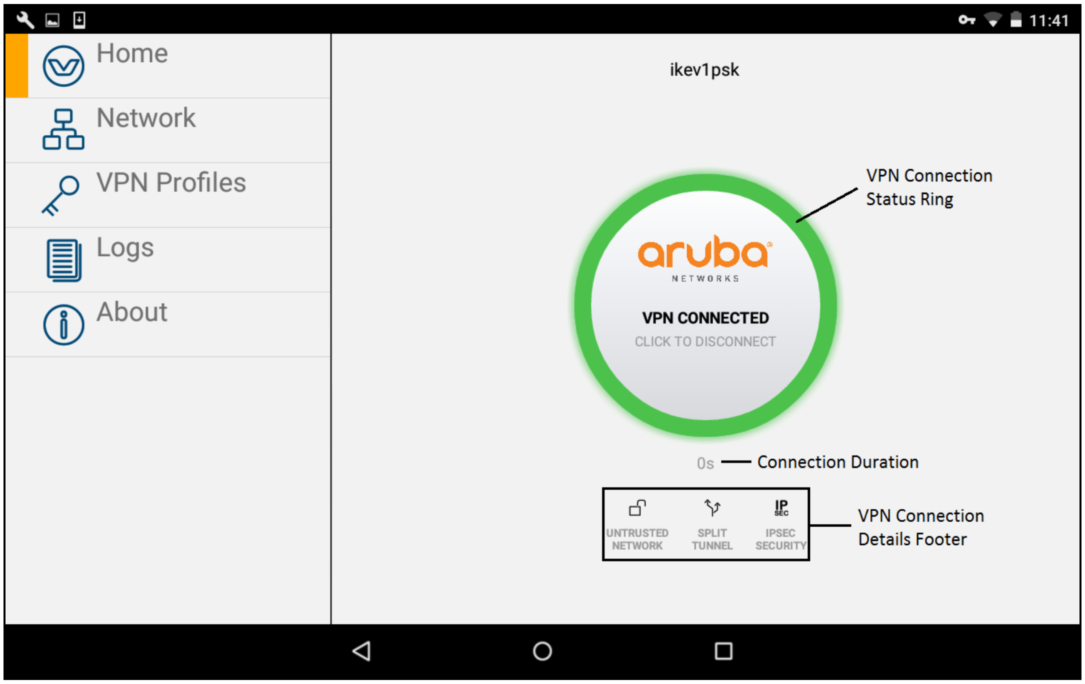
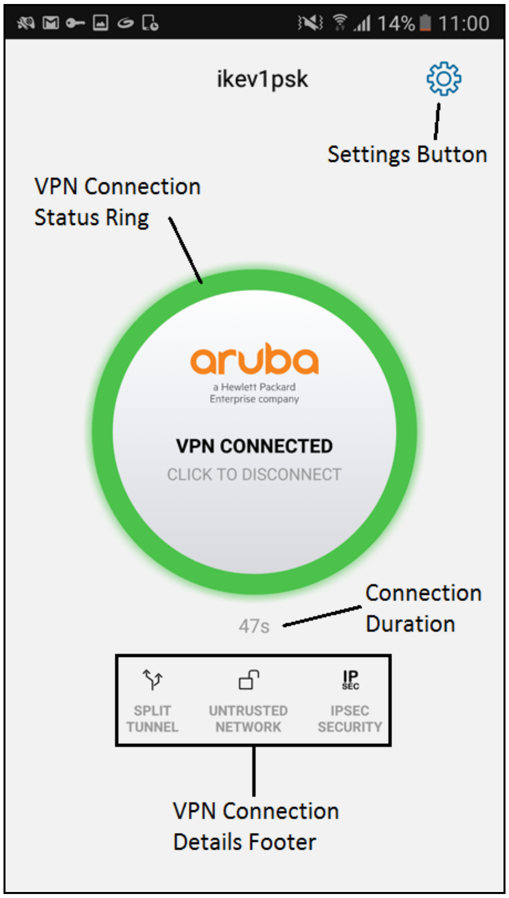


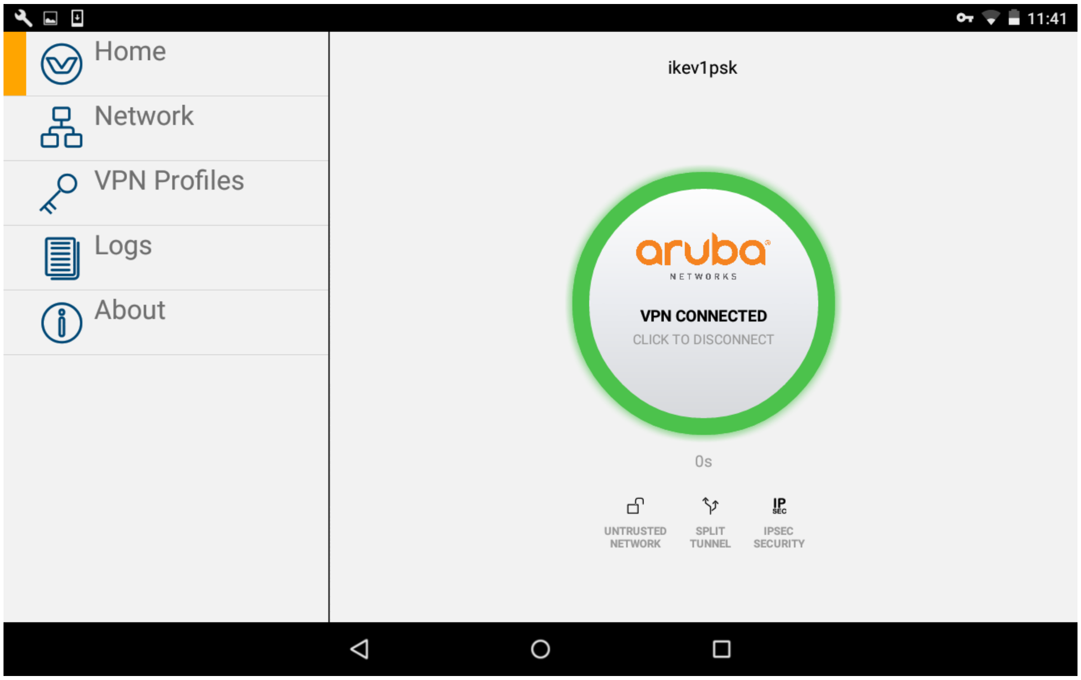
Figure 38 *Android Home Screen UI Elements - Mobile Device*



Connecting and Disconnecting VIA

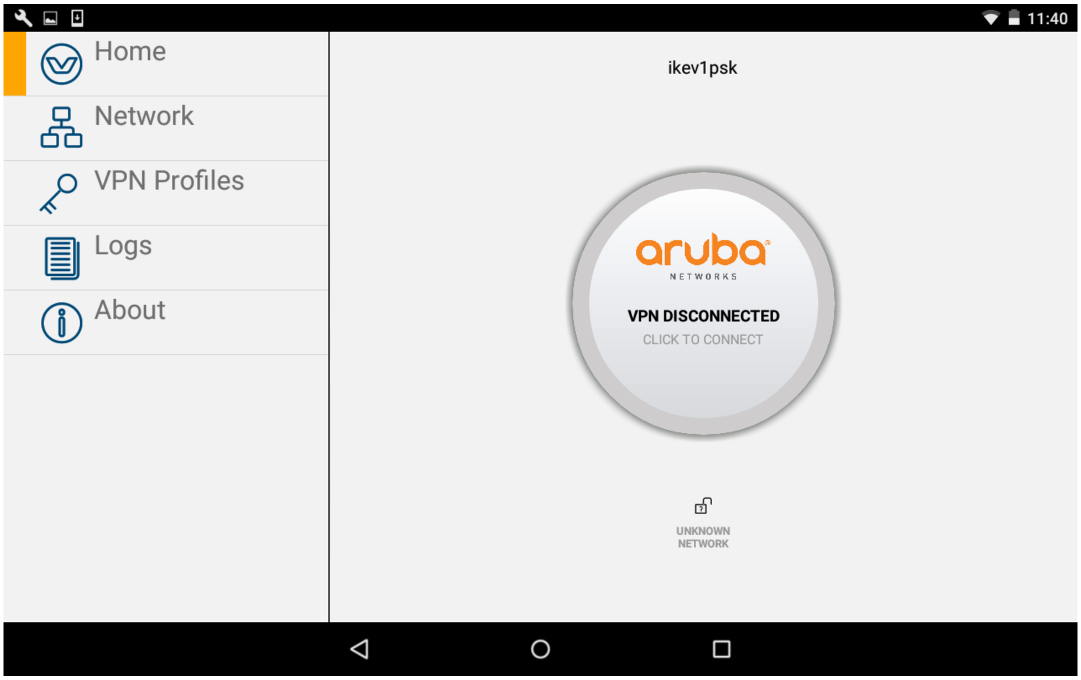
When VIA is connected, the VPN connection status ring on the home screen is green and displays a **VPN CONNECTED** status.

Figure 39 *VIA Connected on Tablet and Mobile Device*



When VIA is disconnected, the VPN connection status ring on the home screen is grey and displays a **VPN DISCONNECTED** status.

Figure 40 *VIA Disconnected on Tablet and Mobile Device*



Click the VPN connection status ring to connect or disconnect VIA.

Connection Flows

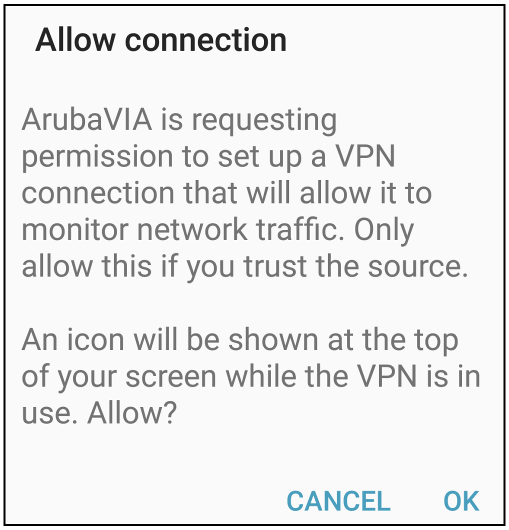
After VIA is installed and the VPN profile is downloaded, based on the way VIA is setup in your network, the VPN connection is established in one of the following ways:

Non-Certificate-Based Authentication

To establish a VPN connection without a using a certificate:

1. Click the VPN connection status ring on the VIA home screen. The **Allow Connection** message appears.
2. Click **OK**.

Figure 41 *Allow Connection Message*



Allow connection

ArubaVIA is requesting permission to set up a VPN connection that will allow it to monitor network traffic. Only allow this if you trust the source.

An icon will be shown at the top of your screen while the VPN is in use. Allow?

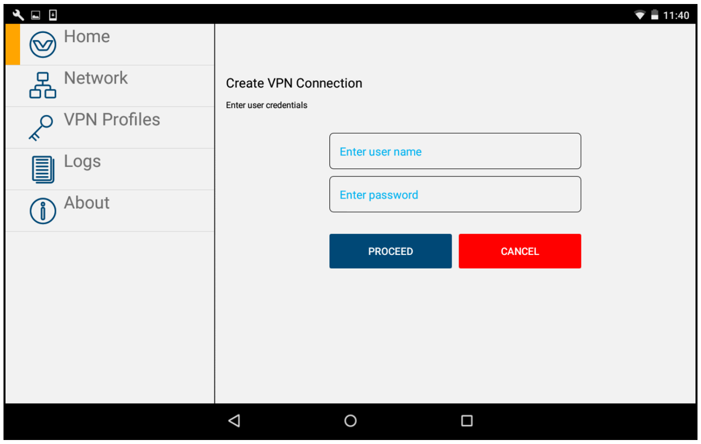
When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Non-Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using XAUTH:

1. Click the VPN connection status ring on the VIA home screen. The **Create VPN Connection** screen appears.

Figure 42 *XAUTH Credentials*



Create VPN Connection

Enter user credentials

Enter user name

Enter password

2. Enter your username/email ID and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication

To establish a VPN connection using a certificate:

1. Click the VPN connection status ring on the VIA home screen. The **Choose Certificate** screen appears.
2. Select a certificate from the list.
3. Click **Install**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Only .p12 and .pfx certificate formats are supported.

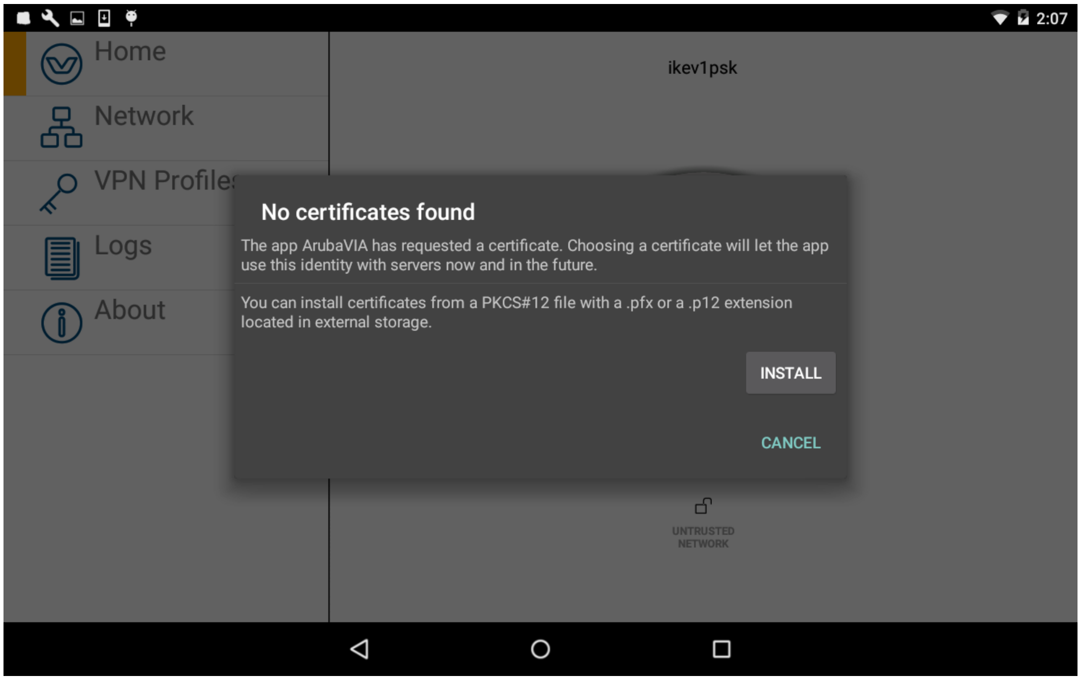
Installing New VPN Connection Certificates

If the required certificate is not listed, you must install the certificate. For devices running Android version 4.4 or earlier, new certificates must be installed on both VIA and the device. For devices running Android versions after 4.4, certificates only need to be installed on the device.

To install a new certificate on VIA:

1. On the VIA home screen, connect to the VPN by clicking on the VPN connection status ring. The **Choose Certificate** screen appears. If no certificates are currently installed, a **No certificates found** message appears.

Figure 43 *No Certificates Found Message on Tablet and Mobile Device*



No certificates found

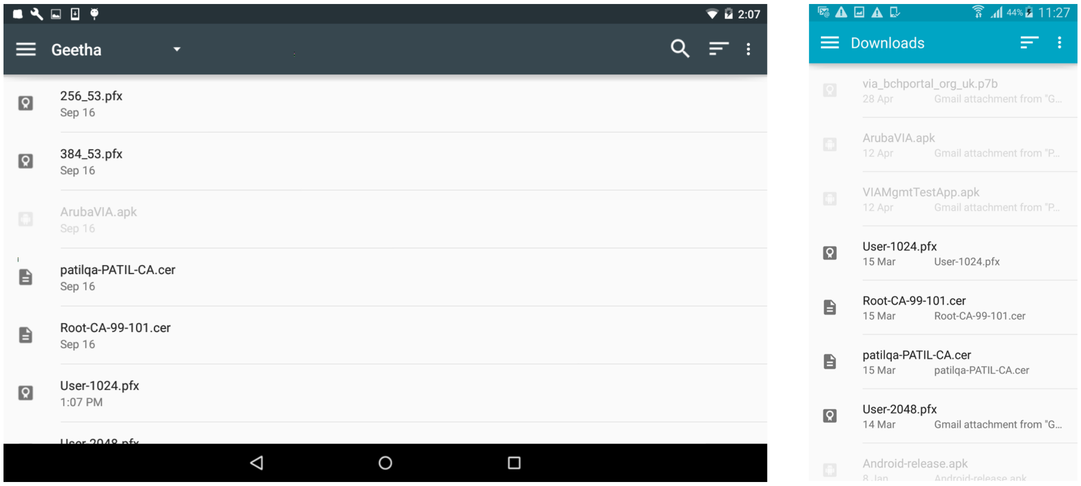
The app ArubaVIA has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.

2. Click **Install**. The **Name the certificate** screen appears.
3. Click **Certificate Name**, and then locate and select the certificate from your device.

Only .p12 and .pfx certificate formats are supported.

Figure 44 *Locating Certificates on Tablet and Mobile Device*



256_53.pfx
Sep 16

384_53.pfx
Sep 16

ArubaVIA.apk
Sep 16

patilqa-PATIL-CA.cer
Sep 16

Root-CA-99-101.cer
Sep 16

User-1024.pfx
1:07 PM

User-2048.pfx

via_bchportal_org_uk.p7b
28 Apr Gmail attachment from "G...

ArubaVIA.apk
12 Apr Gmail attachment from "P...

VIAMgmtTestApp.apk
12 Apr Gmail attachment from "P...

User-1024.pfx
15 Mar User-1024.pfx

Root-CA-99-101.cer
15 Mar Root-CA-99-101.cer

patilqa-PATIL-CA.cer
15 Mar patilqa-PATIL-CA.cer

User-2048.pfx
14 Mar Gmail attachment from "G...

Android-release.apk
8 Jan Android-release.apk

4. Enter the certificate password.

NOTE

Passwords are only applicable to user certificates. Certificate authorities (CA) do not require a password.

5. Click **OK**.

The certificate is now added to the VIA certificate list.

Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using a certificate and XAUTH:

1. Follow the steps in Certificate-Based Authentication.
2. Enter your username/email ID and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Uninstalling VIA

You can uninstall VIA from the running application tab on your Android device.

Working with Settings

The following sections describe the different tabs and settings available in the VIA UI for Android devices.

- Network on page 62
- VPN Profiles on page 63
- Logs on page 65
- About on page 65

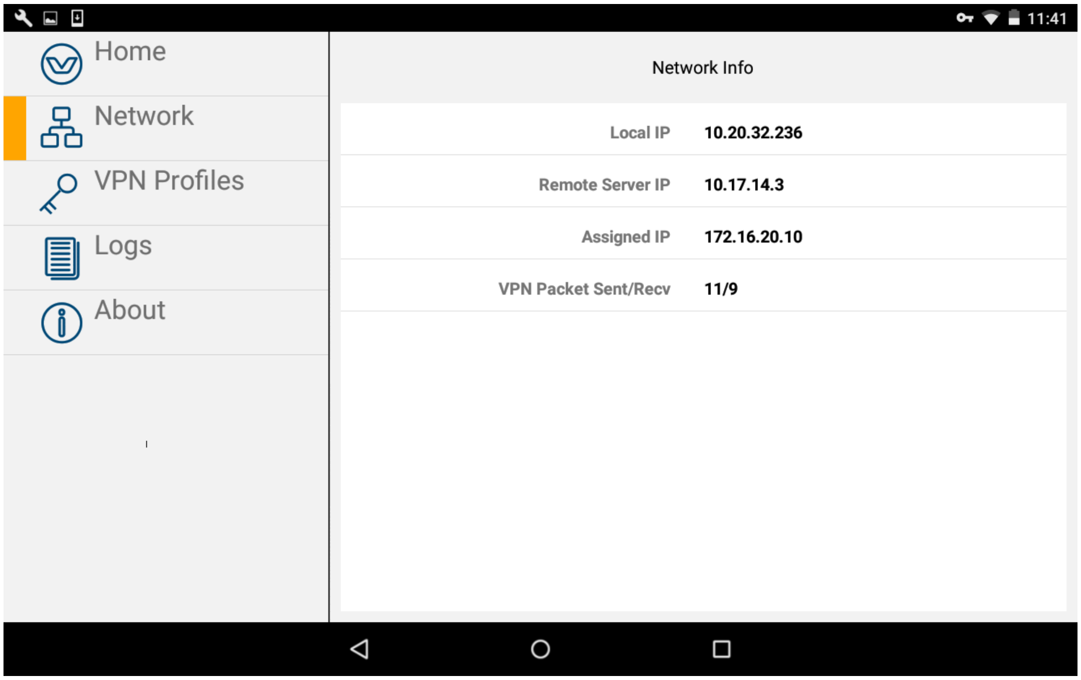
Network

The **Network** tab provides the following information about your remote connection. For mobile devices, click the **Settings** button on the home screen to view the **Network** tab.

- **Local IP**: Local IP address of the device.

- **Remote Server IP**: IP address of the remote server.
- **Assigned IP**: Assigned IP address of the device.
- **VPN Packet Sent/Recv**: Number of VPN packets transmitted and received.

Figure 45 *Network Tab on Tablet and Mobile Device*



Network Info

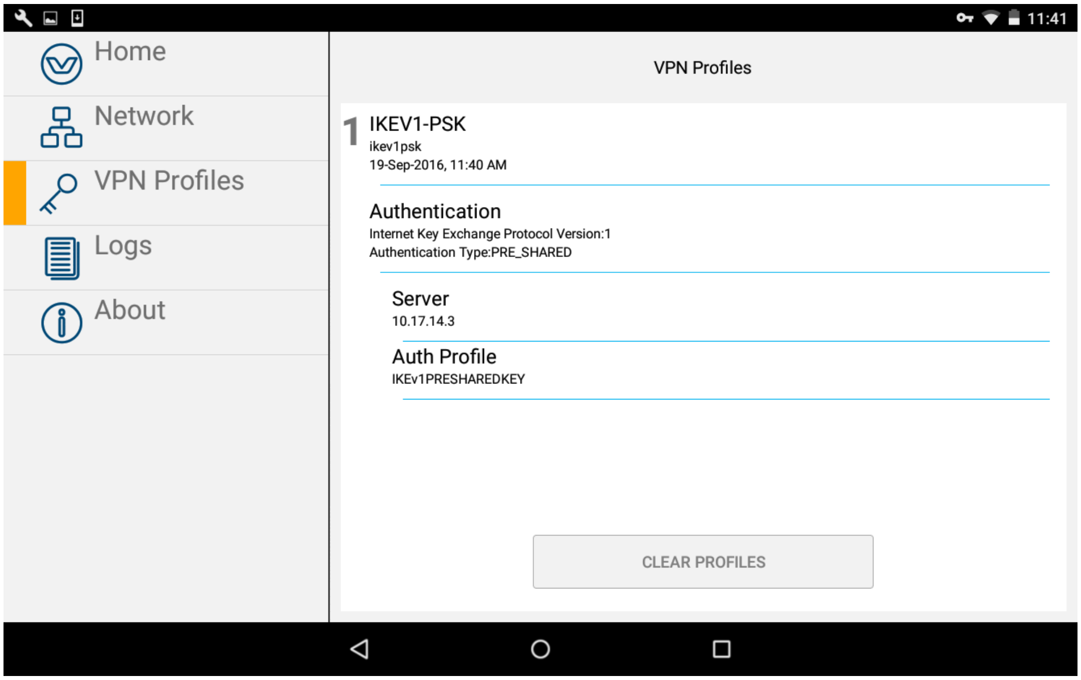
Local IP	10.20.32.236
Remote Server IP	10.17.14.3
Assigned IP	172.16.20.10
VPN Packet Sent/Recv	11/9

VPN Profiles

The **VPN Profiles** tab displays the following information about each downloaded VPN profile. For mobile devices, click the **Settings** button on the home screen to view the **VPN Profiles** tab.

- **Profile**: Name of the VPN profile, and the date and time that the profile was added.
- **Authentication**: IKE protocol version and authentication type.
- **Server**: IP address of the VPN server.
- **Auth Profile**: Web authentication profile.
- **Certificate**: VPN connection certificate (only for certificate-based authentication).

Figure 46 *VPN Profiles Tab on Tablet and Mobile Device*



VPN Profiles

1 IKEV1-PSK
ikev1psk
19-Sep-2016, 11:40 AM

Authentication
Internet Key Exchange Protocol Version:1
Authentication Type:PRE_SHARED

Server
10.17.14.3

Auth Profile
IKEv1PRESHAREDKEY

Clearing Profiles

To clear a VPN profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On a tablet, navigate to the **VPN Profiles** tab. On a mobile device, click the **Settings** button, and then navigate to the **VPN Profiles** tab.
3. Click **Clear Profiles**.

Changing the Server

To change the server:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On a tablet, navigate to the **VPN Profiles** tab. On a mobile device, click the **Settings** button, and then navigate to the **VPN Profiles** tab.
3. Click **Server**.
4. Select a different server from the list.
5. Click **Save**.

Changing the Authentication Profile

To change the auth profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On a tablet, navigate to the **VPN Profiles** tab. On a mobile device, click the **Settings** button, and then navigate to the **VPN Profiles** tab.
3. Click **Auth Profile**.
4. Select a different authentication profile from the list.
5. Click **Save**.

Changing the VPN Connection Certificate

To change the VPN connection certificate for certificate-based authentication:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On a tablet, navigate to the **VPN Profiles** tab. On a mobile device, click the **Settings** button, and then navigate to the **VPN Profiles** tab.
3. Click **Certificate**.
4. Select a different certificate from the list.

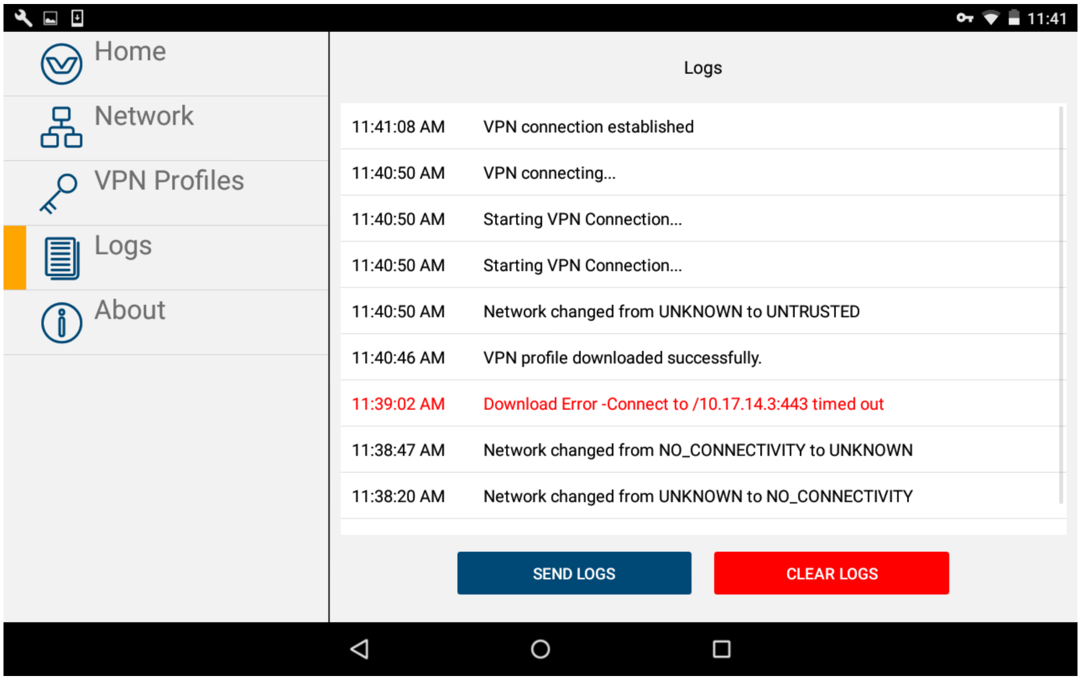
> NOTE
>
> If the selected certificate is not provisioned, a dialog prompts for permission to access the certificate's private key. Click **Allow**.

5. Click **Save**.

Logs

The **Logs** tab displays all logs from the most recent sequence of events that have taken place since the application was launched. For mobile devices, click the **Settings** button on the home screen to view the **Logs** tab.

Figure 47 *Logs Tab on Tablet and Mobile Device*



```
11:41:08 AM   VPN connection established
11:40:50 AM   VPN connecting...
11:40:50 AM   Starting VPN Connection...
11:40:50 AM   Starting VPN Connection...
11:40:50 AM   Network changed from UNKNOWN to UNTRUSTED
11:40:46 AM   VPN profile downloaded successfully.
11:39:02 AM   Download Error -Connect to /10.17.14.3:443 timed out
11:38:47 AM   Network changed from NO_CONNECTIVITY to UNKNOWN
11:38:20 AM   Network changed from UNKNOWN to NO_CONNECTIVITY
```

- **Send Logs**: Attaches a log file that contains all logs collected by VIA to your default email address, which you can send to your help desk.
- **Clear Logs**: Clears the log history.

About

The **About** tab displays the VIA version. For mobile devices, click the **Settings** button on the home screen to view the **About** tab.

Chapter 7 VIA Client for Mac

This section includes the following topics:

New Features

This section describes the features and enhancements introduced in VIA 3.x.x Mac Editions

Features Introduced in VIA 3.1 Mac Edition

Access to local resources are differentiated in full tunnel mode.

VIA clients can now access resources over the tunnel that are in the same network addressing range as the local network in full tunnel mode. If a VIA client and another machine are connected to the same router, the second machine was preventing access to similar addressed devices in the enterprise. The change in application behavior now ensures all network access requests go through the tunnel mode setup.

Features Introduced in VIA 3.0.0 Mac Edition

Automatic Upgrade/Downgrade

VIA supports automatic upgrade and downgrade. When a new version of VIA is available on the server, VIA automatically initiates upgrade/downgrade after disconnecting the VPN.

NOTE

You cannot downgrade from VIA 3.0.0 to any version of VIA 2.x.

NOTE

This feature is only available on Linux, Mac OS, and Windows devices.

Lockdown All Settings

Network administrators can enable the **Lockdown All Settings** knob on the controller to prevent profile setting changes on the VIA client. When this knob is enabled, users cannot clear profiles or edit any settings on the **VPN Profiles** tab, including the server and authentication profile.

NOTE

This feature is not available on iOS devices.

Multiple Email Recipients when Sending Logs

In earlier versions of VIA, users could only send logs to the network administrator. Now users can modify or add to the email recipients list for sending logs.

VIA Uninstaller

The **Uninstaller.app** is used to uninstall VIA on Mac OS devices.

Uninstaller.app is located at **/Users/<username>/Library/ApplicationSupport/Virtual Intranet Access/Uninstaller.app**

NOTE

The VIA uninstaller application is only available on Mac OS devices.

VIA User Interface

VIA 3.0.0 introduces an updated User Interface (UI).

Prerequisites

Ensure that the end-user system meets the following prerequisites:

- Supported Operating Systems: Mac OS X 10.8, 10.9, 10.10, and 10.11.
- Administrator privileges on the computer.
- Computer connected to a working wired or wireless network.

NOTE

VIA has only been tested with the English-language version of Mac OS X.

Downloading VIA

To download VIA:

1. Login to the Aruba Support Site.
2. Navigate to **Download Software** > **VIA >MacOS > VIA 3.2.0**
3. Download the **Aruba VIA Installer.dmg** file.

Installing VIA

Ensure that you have met the prerequisites before proceeding with installation.

NOTE

VIA 2.x continues to retain the connection profile even after uninstalling VIA 2.x. You can connect using this profile after VIA 3.2.x is installed. If you do not want to connect using the existing connection profile, clear the connection profile in VIA 2.x, and then install VIA 3.2.x

To install VIA:

1. Double-click the downloaded **VIA.pkg** file to open the **VIA Installation Wizard** and begin the installation process.

2. The **Introduction** screen of the VIA installation wizard is displayed. Click **Continue**.

In some instances, when you open **macviainstaller.pkg**, an error dialog appears. The workaround is to launch **/Applications/System Preferences.app**, navigate to **Security & Privacy** > **General**, under the section **Allow apps downloaded from:** select **Mac App Store and identified developers**, or right click on **macviainstaller.pkg**, and click **Open**.

3. Click **Continue** on the **Welcome** screen.
4. On the **Software License Agreement** screen, click **Continue.** The **License Agreement** prompt opens.
5. Click **Agree** to agree to the terms of the software license agreement. The **Standard Install** screen appears.
6. Click **Install**. The installation progress screen appears.
7. Upon successful installation, the **Installation was Successful** screen appears. Click **Close** to complete installation and close the installation wizard.

Downloading VPN Profiles

VPN profiles must be downloaded in order to connect VIA.

To download a VPN profile:

1. Open VIA.
2. Select **Click to download VPN profile** on the VPN download screen. The **Download VPN Profile** screen opens.
3. Enter the following details:
   - **VPN Server URL**: IP address or FQDN provided by the system administrator.
   - **Username**: Username, domain username, or email ID.
   - **Password**: Password or domain password.
4. Click **Download**.
5. (Optional) A **Server certificate error** message appears if the server certificate does not match the server name. Click **Continue**.
6. (Optional) Select a web authentication profile from the **Web Authentication Profile** list.

This screen only appears if the server has multiple web authentication profiles.

If the **Web authentication** list contains more than one VIA authentication profile, users can select a VIA authentication profile. Upon successful authentication, the VIA client downloads the appropriate VIA connection profile.

7. (Optional) Select an IKE authentication profile from the **IKE Authentication Profile** list. VPN profile download is now complete.

VIA UI Home Screen

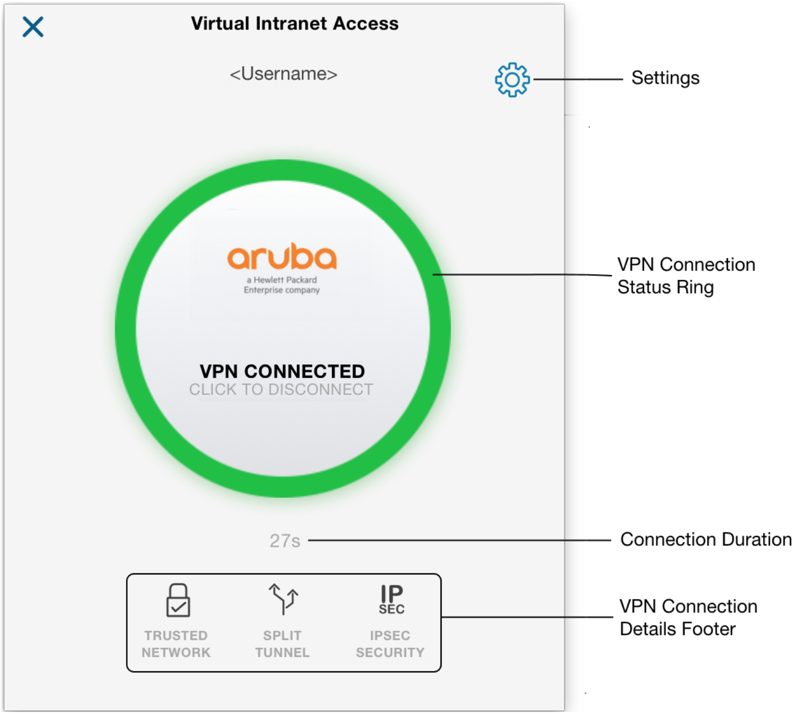
The VIA home screen opens upon launching and connecting VIA. See Connecting and Disconnecting VIA on page 69 and Connection Flows on page 70 for more details on connecting VIA.

The home screen displays the following information about the VIA connection:

- **VPN Connection Status Ring**: Indicates if VIA is connected or disconnected.
- **Connection Duration**: Indicates the duration of the current session.
- **VPN Connection Details Footer**: Displays details about the VPN connection.

- **Settings Button**: Displays VIA settings, which include the **Network**, **VPN Profiles**, **Logs**, and **About** tabs.

Figure 48 *VIA Home Screen UI Elements*

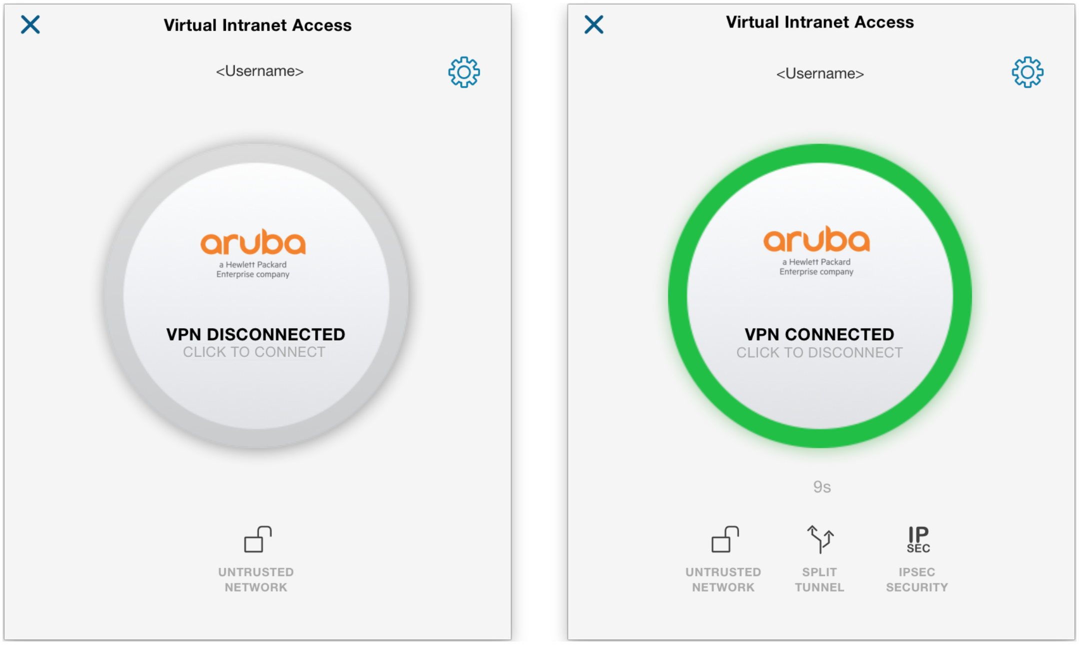


Connecting and Disconnecting VIA

When VIA is connected, the VPN connection status ring on the home screen is green and displays a **VPN CONNECTED** status.

When VIA is disconnected, the VPN connection status ring on the home screen is grey and displays a **VPN DISCONNECTED** status.

Figure 49 *Connected and Disconnected VIA Screen*



Click the VPN connection status ring to connect or disconnect VIA.

Connection Flows

After VIA is installed and the VPN profile is downloaded, based on the way VIA is setup in your network, the VPN connection is established in one of the following ways:

Non-Certificate-Based Authentication

To establish a VPN connection without a using a certificate, click the VPN connection status ring on the VIA home screen. When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Non-Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using XAUTH:

1. Click the VPN connection status ring on the VIA home screen. The **Create VPN Connection** screen appears.
2. Enter your username/email ID and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication

To establish a VPN connection using a certificate:

1. Click the VPN connection status ring on the VIA home screen. The **Select a Certificate** screen appears.
2. Select a certificate from the list, and then click **Proceed**.

NOTE

If the selected certificate was not provisioned previously a certificate permission popup window appears. Click **Allow**.

   a. Click **+** at the top-right corner of the **Select a Certificate** screen.
   b. Locate and select the certificate.
   c. Click **Open**. The certificate is now added to the certificate list.
   d. Select the certificate from the list, and then click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication with Extended Authentication (XAUTH)

1. Follow the steps in Certificate-Based Authentication on page 70. The XAUTH **Create VPN Connection** screen appears.
2. Enter your username/email ID and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

VIA Tray Icon Behavior

Upon connecting, VIA automatically minimizes to the top menu bar after two seconds. Click the VIA tray icon to display the VIA home screen. The VIA tray icon color indicates the current status of the network connectivity, as described below:

Table 7: *Network Connectivity Status*

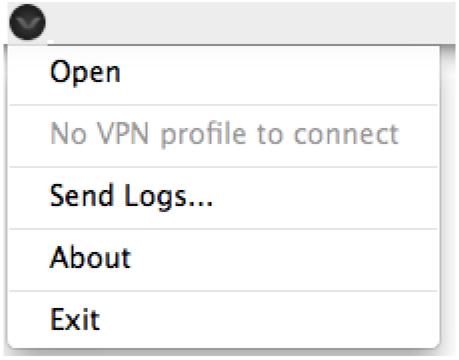
Tray icon Color	Description
⚫	No profile is downloaded in VIA.
🟠	Profile is downloaded but VPN is disconnected.
🟢	Profile is downloaded and VPN is connected.

VIA Tray Icon Menu

Click the VIA tray icon to display the menu with relevant quick options. This menu changes based on the status of the VIA application, as described below.

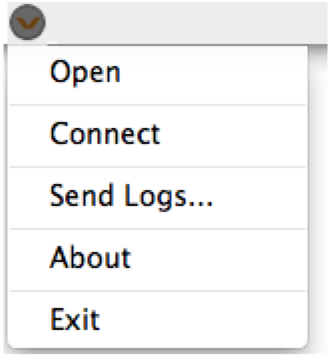
When no profile is downloaded, the following menu is displayed:

Figure 50 *No Profile Downloaded Menu*



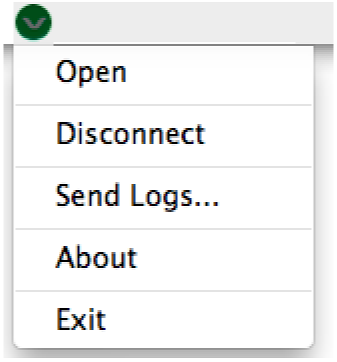
When a profile is downloaded but the VPN is not connected, the following menu is displayed:

Figure 51 *Profile Downloaded but VPNnot Connected Menu*



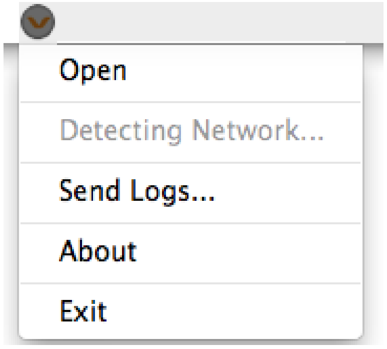
When a profile is downloaded and the VPN is connected, the following menu is displayed:

Figure 52 *VPN Connecting Menu*



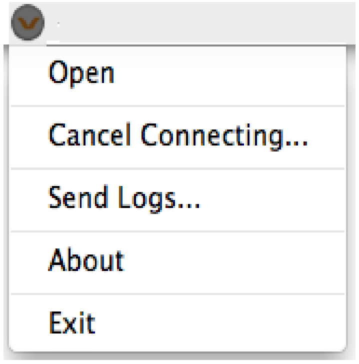
When VIA is detecting the network, the following menu is displayed:

Figure 53 *VIA Detecting Network Menu*



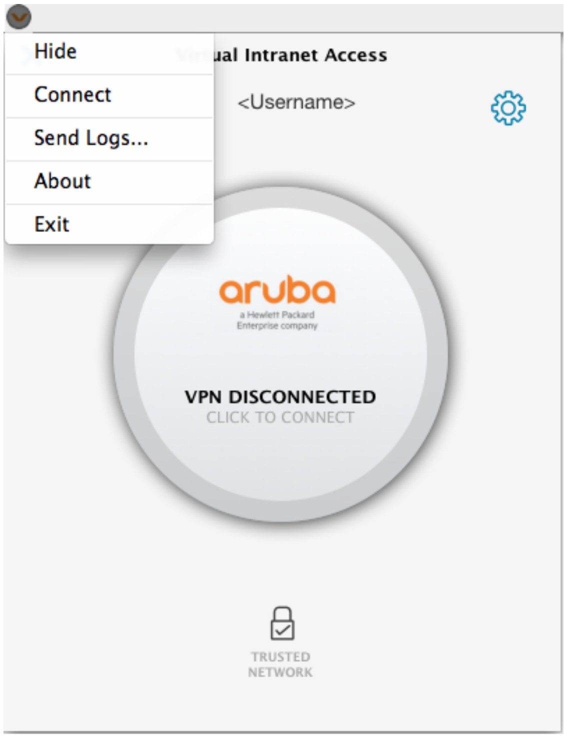
When VIA detects the network and establishes a connection, the following menu is displayed:

Figure 54 *Network Detected and Connection Establishing Menu*



When the VIA UI is displayed on the screen, the following menu is displayed:

Figure 55 *VIA UI Displayed Menu*



The following list describes the functionality of all menu options:

- **Open**: This option displays the VIA home screen.
- **Hide**: This option minimizes VIA to the icon tray.
- **Connect**: This option initiates the VPN connection.
- **Cancel Connecting**: This option stops the VPN connection attempt.
- **Disconnect**: This option disconnects the VPN connection.
- **Send Logs**: This option attaches a log file, which contains all logs collected by VIA, to your default email address. These logs can be sent to your help desk.
- **About**: This option displays the VIA **About** tab.
- **Exit**: This option disconnects the VPN connection and closes the VIA application.

Uninstalling VIA

To uninstall VIA:

1. Launch the VIA uninstaller application, which is located at **/Users/<username>/Library/Application Support/Virtual Intranet Access/Uninstaller.app**. The **Are you sure you want to uninstall Virtual Intranet Access?** screen appears.
2. Click **Yes**. Enter your system user credentials.
3. Click **OK**. The **Virtual Intranet Access uninstalled successfully** screen appears.
4. Click **OK**.

VIA is successfully uninstalled.

Working with Settings

The following sections describe the different tabs and settings available in the VIA UI for Mac devices. Click the **Settings** button on the VIA home screen to view the following tabs:

- Network on page 74
- VPN Profiles on page 74
- Logs on page 76
- About on page 76

Network

The **Network** tab provides the following information about your remote connection:

- **SSID**: SSID of the network.
- **Connection Type**: Type of connection.
- **Connection Speed**: Speed of the VPN connection.
- **Local IP**: Local IP address of the device.
- **Assigned IP**: Assigned IP address of the device.
- **Remote Server IP Address**: IP address of the remote server.
- **VPN Packet Sent/Received**: Number of VPN packets transmitted and received.

VPN Profiles

The **VPN Profiles** tab displays the following information about each downloaded VPN profile:

- **Profile**: Name of the VPN profile, and the date and time that the profile was added.

- **Authentications**: IKE protocol version and authentication type.
- **Server**: IP address of the VPN server.
- **Auth Profile**: Web authentication profile.
- **Certificate**: VPN connection certificate (only for certificate-based authentication).

Clearing Profiles

To clear profiles:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles**.
3. Click **Clear Profiles**.

Changing the Server

To change the server:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles** > **Server**.
3. Select a different server from the **Servers** list.
4. Click **Save**.

Changing the Authentication Profile

To change the authentication profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles** > **Auth Profile**.
3. Select a different authentication profile from the **Auth Profiles** list.
4. Click **Save**.

Changing the VPN Connection Certificate

To change the VPN connection certificate for certificate-based authentication:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. Navigate to **Settings** > **VPN Profiles** > **Certificate**.
3. Select a different certificate from the **Certificates** list.

NOTE

> If the selected certificate is not provisioned, then a dialog prompts for permission to access the certificate's private key. Click **Allow**

Figure 56 *Dialog for Permission to Access the Certificate*

4. Click **Save**.

Adding a New VPN Connection Certificate

To add a new VPN certificate:

1. **In the VIA home screen, CLICK TO DISCONNECT VPN.**
2. Navigate to **Settings** > **VPN Profiles** > **Certificate**.
3. Click **Add Certificates**. The open panel appears.
4. Locate and select the certificate.
5. Click **Open**.

The certificate is now added to the certificate list in VIA.

NOTE

Only .p12 and .pfx certificate formats are supported.

Logs

The **Logs** tab displays all logs from the most recent sequence of events that have taken place since the application was launched.

- **Send Logs**: Attaches a log file that contains all logs collected by VIA to your default email address, which you can send to your help desk.
- **Clear Logs**: Clears the log history.

About

The **About** tab displays the VIA version and checks for any available upgrades.

VIA Client for iOS

This section includes the following topics:

New Features

This section describes the features and enhancements introduced in VIA 3.x.x iOS Editions

Features Introduced in VIA 3.0.0 iOS Edition

The following features are introduced in VIA 3.0.0 for iOS:

Auto-Login

The auto-login feature allows clients to automatically login and establish a secure connection to the controller as soon as the connection profile is downloaded on a device. This feature works even after restarting the device.

Login Banner

The login banner feature allows you to display a static warning message that provides information related to your corporate policies or terms and conditions of using VIA. The login banner is displayed when the VIA connection is initiated and contains the **Agree** and **Disconnect Now** buttons. The VIA connection is processed only if the user clicks **Agree**. If the user clicks **Disconnect Now**, the warning message closes and the VIA connection is aborted.

VIA User Interface

VIA 3.0.0 introduces a new User Interface (UI).

Prerequisites

Ensure that the system meets the following prerequisites:

- Device is running one of the supported operating systems:
  - iOS 7.x
  - iOS 8.x
  - iOS 9.0
  - iOS 9.1
  - iOS 9.2
  - iOS 10.0

- iOS 10.1
- Device is connected to a network.

Downloading VIA

Download the latest version of Aruba VIA 3.2.x from the App Store. VIA is automatically installed on the iOS device after download is complete. After installation is complete, the VIA app icon appears on the iOS device.

Downloading VPN Profiles

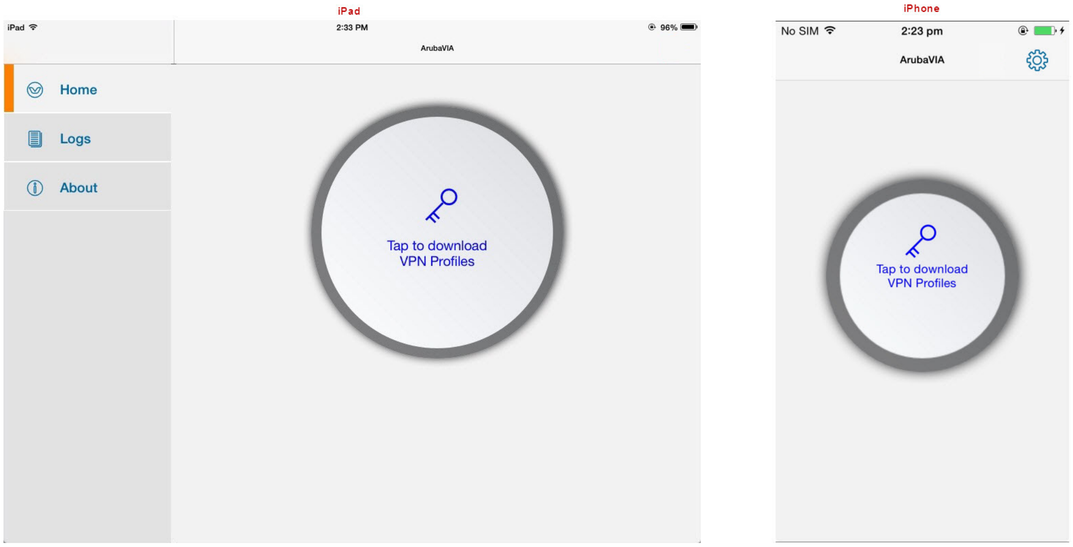
VPN profiles must be downloaded in order to connect VIA.

> NOTE
>
> The VIA screen appears different between iPhones and iPads. In iPhones, the tabs are placed horizontally at the top of the screen. In iPads, the tabs are placed vertically on the left side of the screen. However, the procedures to perform tasks are the same.

To download a VPN profile:

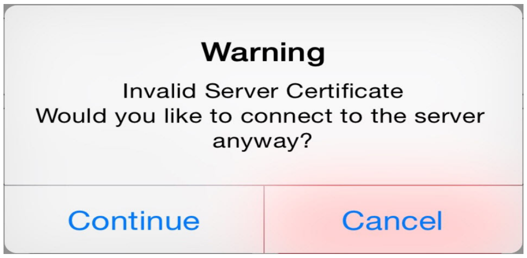
1. Open the VIA application on your iOS device. The home screen appears.

Figure 57 *VIA Home Screen on iPad and iPhone*



2. Click **Tap to Download VPN Profiles**. The **Download VPN Profiles** screen appears.
3. Enter the following details:
   a. **Server URL**: URL obtained from the system administrator.
   b. **Username**: Domain username.
   c. **Password**: Domain password.
4. Click **Download**.
5. (Optional) A warning message appears if the server certificate does not match the server name. Click **Continue**.

Figure 58 *Server Certificate Error*



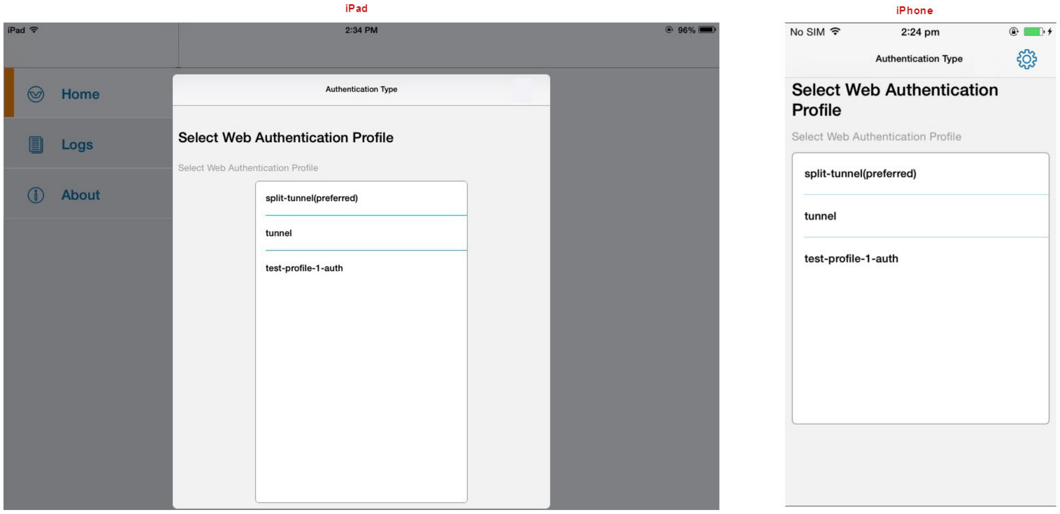
Warning

Invalid Server Certificate
Would you like to connect to the server anyway?

6. (Optional) Select a web authentication profile from the **Web Authentication Profile** list.

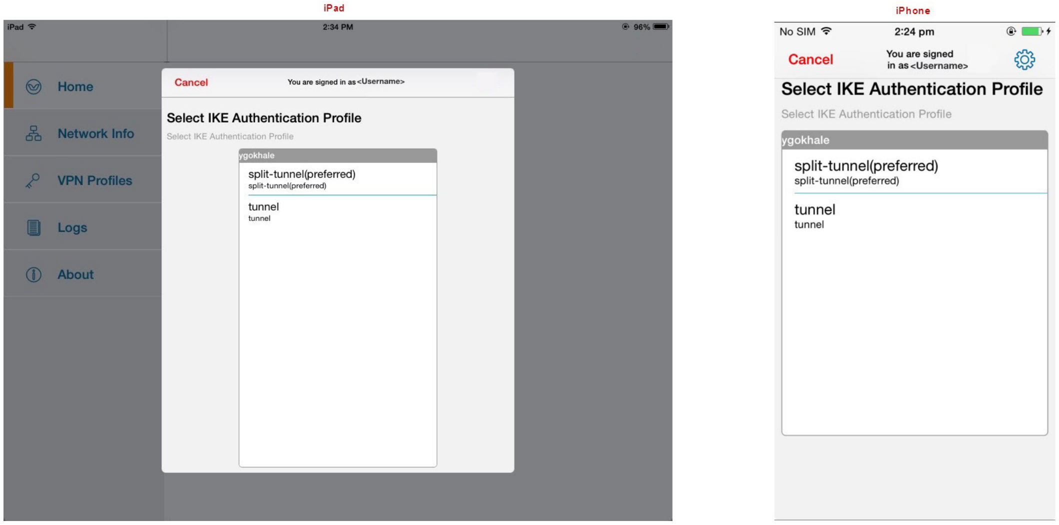
> **NOTE**
>
> This screen only appears if the server has multiple web authentication profiles.
>
> If the web authentication list has more than one VIA authentication profile, users can select a VIA authentication profile. Upon successful authentication, the VIA client downloads the appropriate VIA connection profile.

Figure 59 *Web Authentication Profile List on iPad and iPhone*



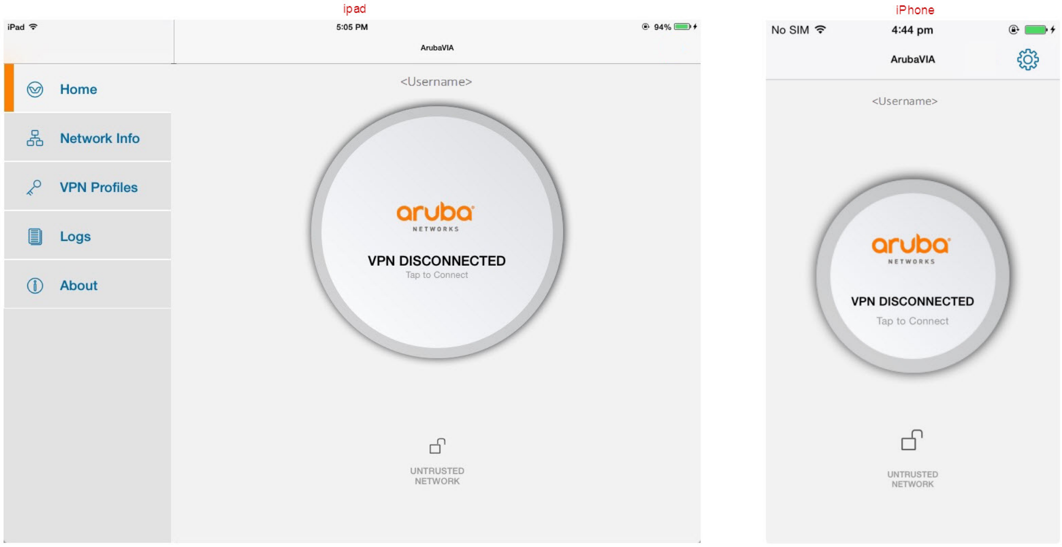
7. (Optional) Select an IKE authentication profile from the **IKE Authentication Profile** list.

Figure 60 *IKE Authentication Profile List on iPad and iPhone*



VPN profile download is now complete, and the following screen appears:

Figure 61 *VIA Home Screen on iPad and iPhone following VPN Profile Download*



VIA UI Home Screen

The VIA home screen opens upon launching and connecting VIA. See Connecting and Disconnecting VIA on page 81 and Connection Flows on page 82 for more details on connecting VIA.

The home screen displays the following information about the VIA connection:

- **VPN Connection Status Ring**: Indicates if the VPN is connected or disconnected.
- **Connection Duration**: Indicates the duration of the current session.
- **VPN Connection Details Footer**: Displays details about the VPN connection.
- **Settings**: (Only for iPhones) Displays VIA settings, which include the **Network**, **VPN**, **Logs**, and **About** tabs.

Figure 62 *VIA Home Screen UI Elements - iPad*

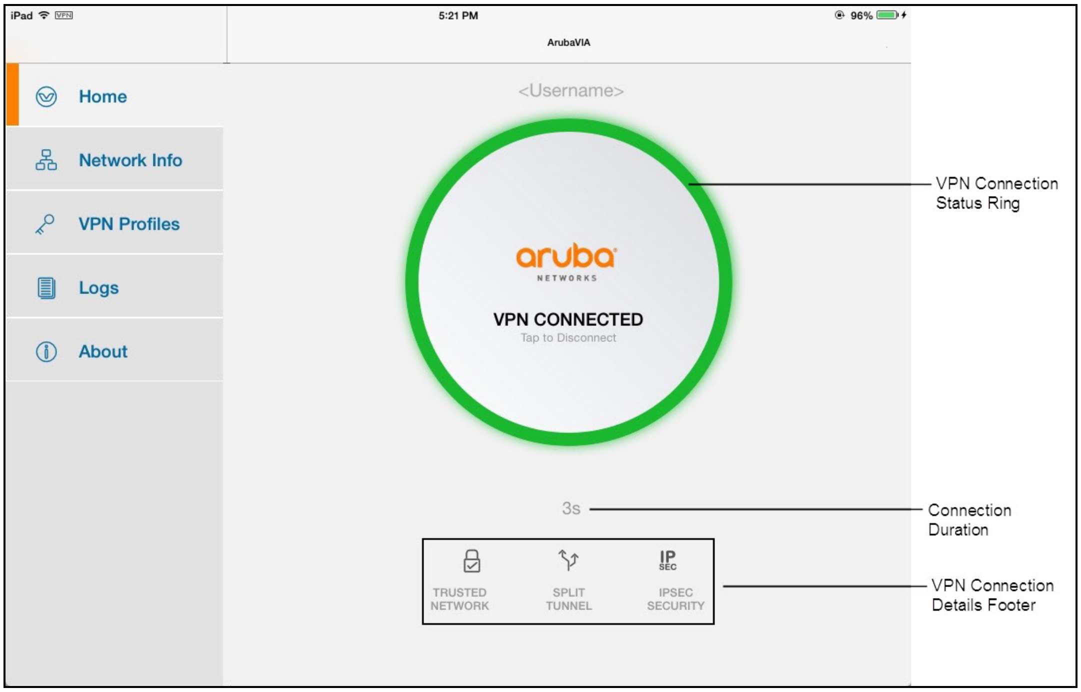
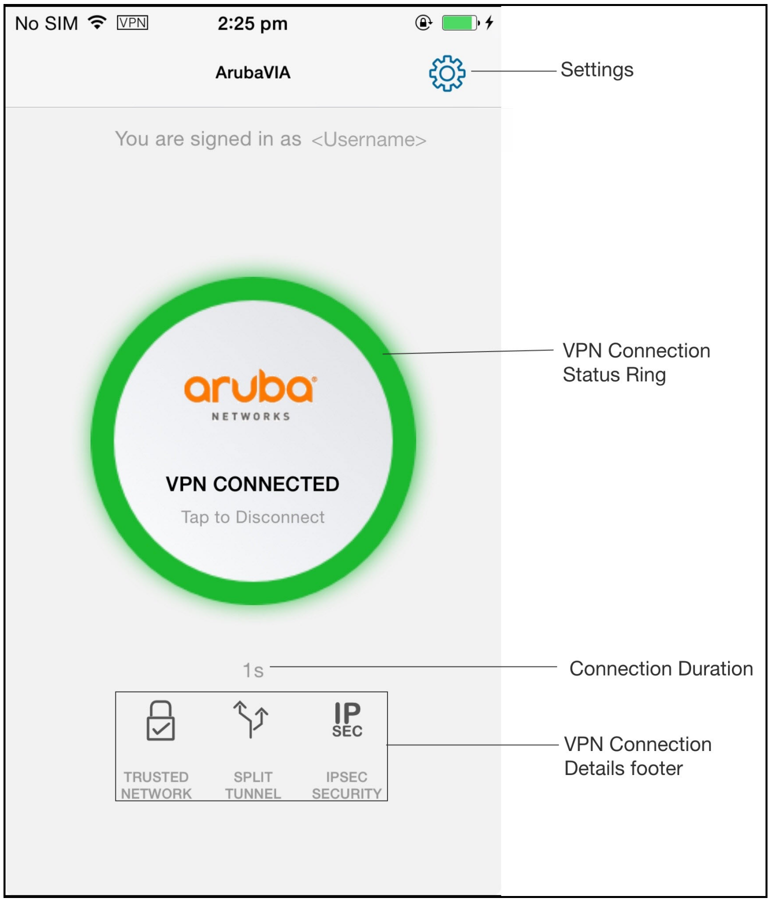


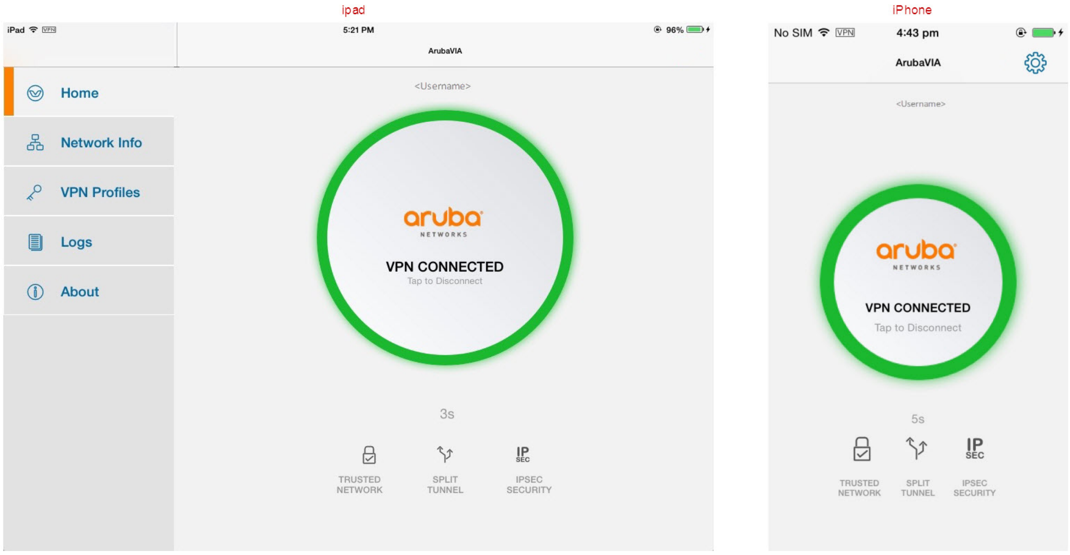
Figure 63 *VIA Home Screen UI Elements - iPhone*



Connecting and Disconnecting VIA

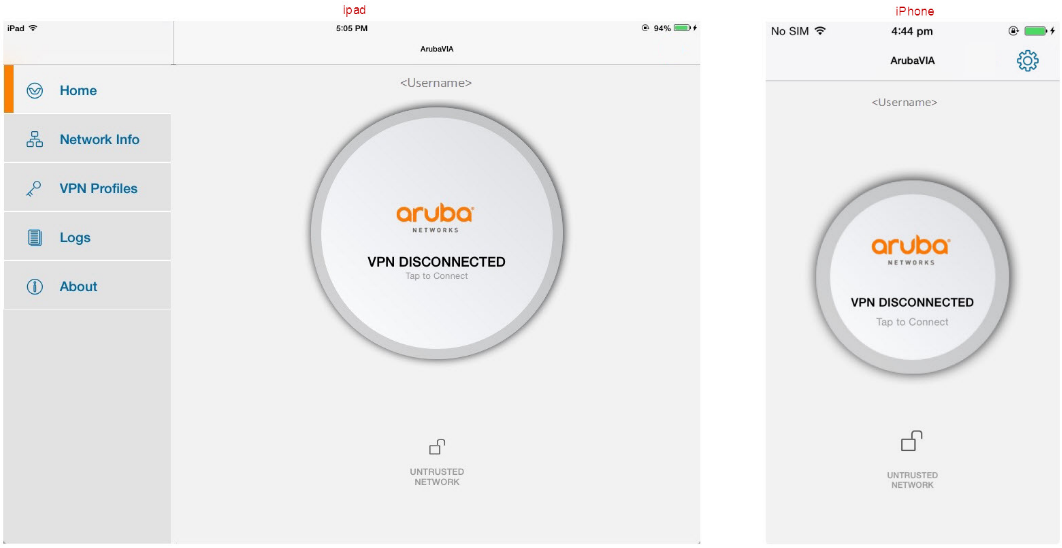
When VIA is connected, the VPN connection status ring on the home screen is green and displays a **VPN CONNECTED** status.

Figure 64 *VIA Connected on iPad and iPhone*



When VIA is disconnected, the VPN connection status ring on the home screen is grey and displays a **VPN DISCONNECTED** status.

Figure 65 *VIA Disconnected on iPad and iPhone*



Click the VPN connection status ring to connect or disconnect VIA.

Connection Flows

After VIA is installed and the VPN profile is downloaded, based on the way VIA is setup in your network, the VPN connection is established in one of the following ways:

Non-Certificate-Based Authentication

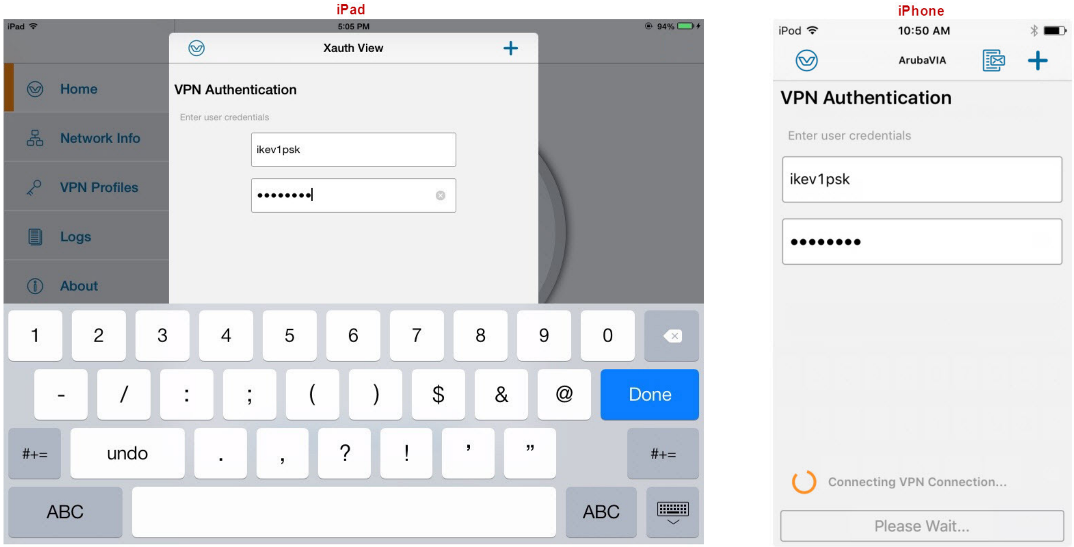
To establish a VPN connection without using a certificate, click the VPN connection status ring on the VIA home screen. When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Non-Certificate-Based Authentication with Extended Authentication (XAUTH)

To establish a VPN connection using XAUTH:

1. Click the VPN connection status ring on the VIA home screen. The **VPN Authentication** screen appears.

Figure 66 *XAUTH Credentials on iPad and iPhone*



2. Enter your username and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication for RSA

To establish a VPN connection using an RSA certificate:

1. Download the RSA certificate on your device.
2. Install both CA and user certificates.

NOTE

RSA certificates can be installed directly by downloading them from your email as a file.

3. Open VIA and click the VPN connection status ring on the home screen. The **Select a Certificate** screen appears.
4. Select the certificate that you installed from the list, and then click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate based Authentication for EC

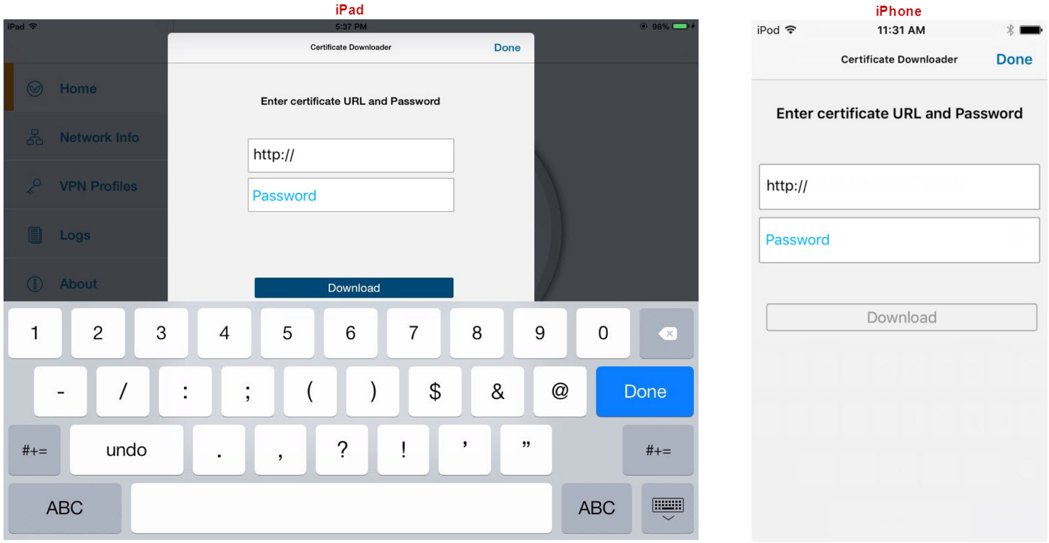
To establish a VPN connection using an EC certificate:

NOTE

VIA does not recognize EC certificates installed on the device store. EC certificates must be installed only through the VIA Certificate Downloader.

1. Click the VPN connection status ring on the home screen. The **Select a Certificate** screen appears.
2. Click **+** at the top-right corner of the **Select a Certificate** screen. The **Certificate Downloader** opens.
3. Enter the certificate URL and password on the **Enter certificate URL and Password** screen.

Figure 67 *EC Certificate Downloader Screen on iPad and iPhone*



4. Click **Download**.The **Select a Certificate** screen appears.
5. Select the EC certificate that you downloaded from the list, and then click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Certificate-Based Authentication with Extended Authentication (XAUTH)

1. Follow the steps in Certificate-Based Authentication for RSA on page 83. The XAUTH **VPN Authentication** screen appears, as shown in Figure 66.
2. Enter your username and password.
3. Click **Proceed**.

When the VPN connection is established, the VPN ring becomes green and displays a **VPN CONNECTED** status.

Uninstalling VIA

Press and hold the VIA app icon for a few seconds, and then click the **x** to uninstall.

Working with Settings

The following sections describe the different tabs and settings available in the VIA UI for iOS devices.

NOTE

The VIA screen appears different between iPhones and iPads. In iPhones, the tabs are placed horizontally at the top of the screen. In iPads, the tabs are placed vertically on the left side of the screen. However, the procedures to perform tasks are the same.

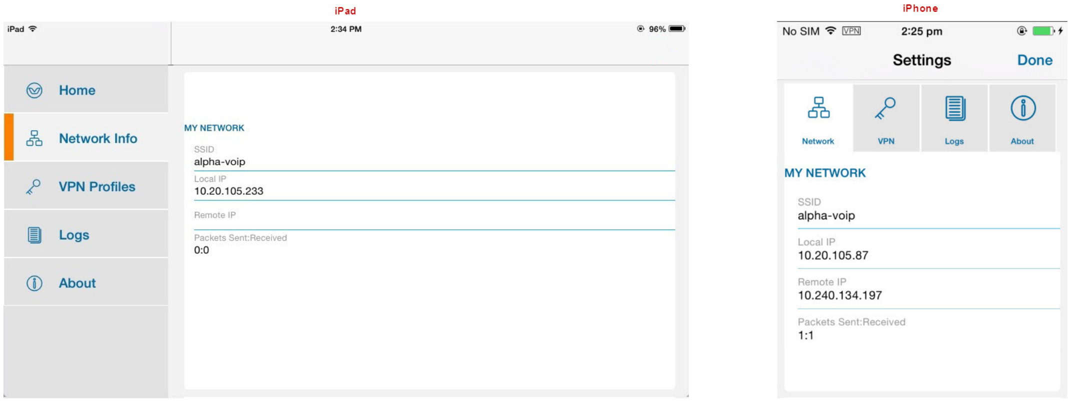
- Network Info or Network on page 84
- VPN Profiles or VPN on page 85
- Logs on page 87
- About on page 87

Network Info or Network

The **Network Info** (iPad) or **Network** (iPhone) tab provides the following information about your remote connection. For iPhones, click the **Settings** button on the home screen to view the **Network** tab.

- **SSID**: SSID of the network.
- **Local IP**: Local IP address of the device.
- **Remote IP**: IP address of the remote server.
- **Packets Sent:Received**: Number of VPN packets transmitted and received.

Figure 68 *Network Info or Network Tab on iPad and iPhone*



MY NETWORK

SSID
alpha-voip

Local IP
10.20.105.233

Remote IP

Packets Sent:Received
0:0

MY NETWORK

SSID
alpha-voip

Local IP
10.20.105.87

Remote IP
10.240.134.197

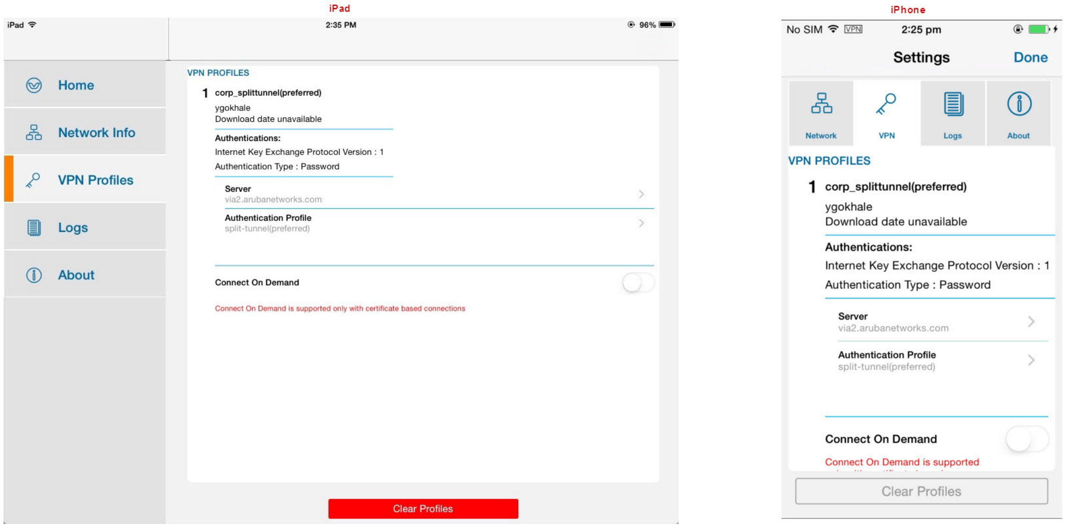
Packets Sent:Received
1:1

VPN Profiles or VPN

The **VPN Profiles** (iPad) or **VPN** (iPhone) tab displays the following information about each downloaded VPN profile. For iPhones, click the **Settings** button on the home screen to view the **VPN** tab.

- **Profile**: Name of the VPN profile, and the date that the profile was added.
- **Authentications**: IKE protocol version and authentication type.
- **Server**: IP address of the VPN server.
- **Authentication Profile**: Web authentication profile.
- **Certificate**: VPN connection certificate (only for certificate-based authentication).

Figure 69 *VPN Profiles or VPN Tab on iPad and iPhone*



VPN PROFILES

1 corp_splittunnel(preferred)
ygokhale
Download date unavailable

Authentications:
Internet Key Exchange Protocol Version : 1
Authentication Type : Password

Server
via2.arubanetworks.com

Authentication Profile
split-tunnel(preferred)

Connect On Demand

Connect On Demand is supported only with certificate based connections

Clearing Profiles

To clear a VPN profile:

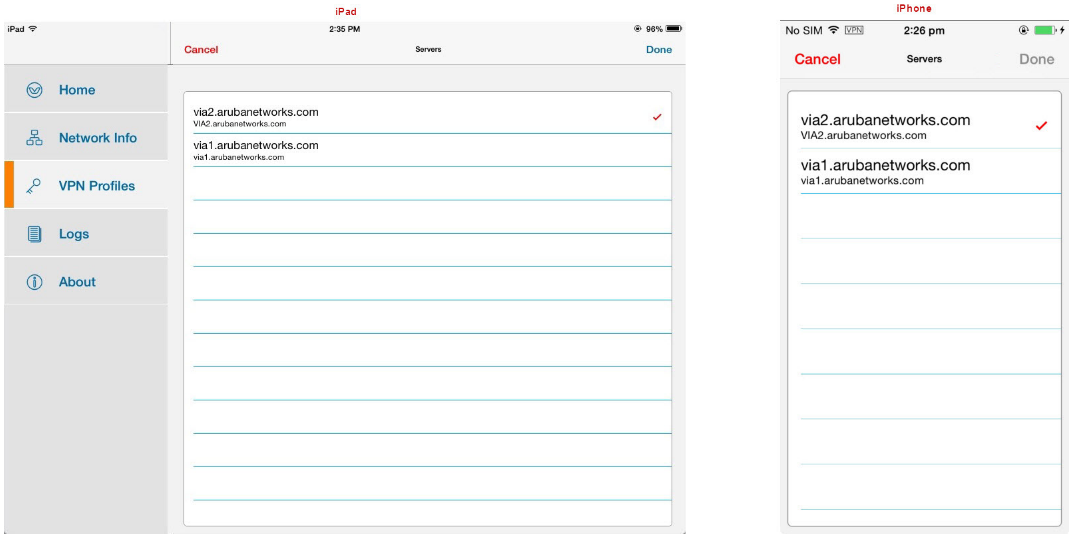
1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On an iPad, navigate to the **VPN Profiles** tab. On an iPhone, click the **Settings** button, and then navigate to the **VPN** tab.
3. Click **Clear Profiles**.

Changing the Server

To change the server:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On an iPad, navigate to the **VPN Profiles** tab. On an iPhone, click the **Settings** button, and then navigate to the **VPN** tab.
3. Click **Server**.
4. Select a different server from the list, as shown in Figure 70.

Figure 70 *Server List*



via2.arubanetworks.com
VIA2.arubanetworks.com ✓

via1.arubanetworks.com
via1.arubanetworks.com

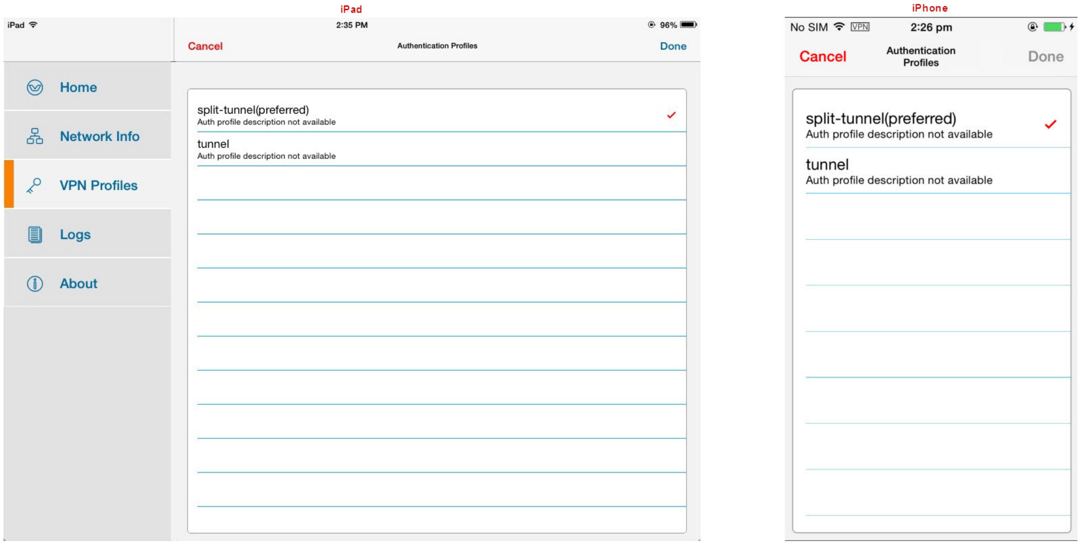
5. Click **Done**.

Changing the Authentication Profile

To change the authentication profile:

1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.
2. On an iPad, navigate to the **VPN Profiles** tab. On an iPhone, click the **Settings** button, and then navigate to the **VPN** tab.
3. Click **Authentication Profile**.
4. Select a different authentication profile from the list, as shown in Figure 71.

Figure 71 *Authentication Profile List*



split-tunnel(preferred)
Auth profile description not available ✓

tunnel
Auth profile description not available

5. Click **Done**.

Changing the VPN Connection Certificate

To change the VPN connection certificate for certificate-based authentication:

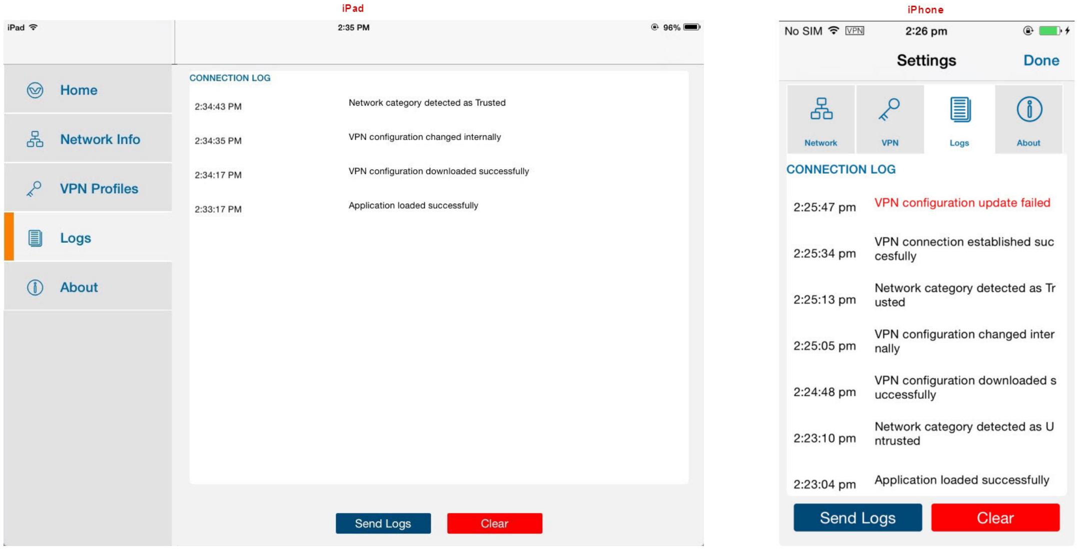
1. On the VIA home screen, disconnect from the VPN by clicking on the VPN connection status ring.

2. On an iPad, navigate to the **VPN Profiles** tab. On an iPhone, click the **Settings** button, and then navigate to the **VPN** tab.
3. Click **Certificate**.
4. Select a different certificate from the list
5. Click **Done**.

Logs

The **Logs** tab displays all logs from the most recent sequence of events that have taken place since the application was launched. For iPhones, click the **Settings** button on the home screen to view the **Logs** tab.

Figure 72 *Logs Tab on iPad and iPhone*



CONNECTION LOG

```
2:34:43 PM    Network category detected as Trusted
2:34:35 PM    VPN configuration changed internally
2:34:17 PM    VPN configuration downloaded successfully
2:33:17 PM    Application loaded successfully
```

CONNECTION LOG

```
2:25:47 pm    VPN configuration update failed
2:25:34 pm    VPN connection established suc
              cesfully
2:25:13 pm    Network category detected as Tr
              usted
2:25:05 pm    VPN configuration changed inter
              nally
2:24:48 pm    VPN configuration downloaded s
              uccessfully
2:23:10 pm    Network category detected as U
              ntrusted
2:23:04 pm    Application loaded successfully
```

- **Send Logs**: Attaches a log file that contains all logs collected by VIA to your default email address, which you can send to your help desk.
- **Clear Logs**: Clears the log history.

About

The **About** tab displays the VIA version and checks for any available upgrades. For iPhones, click the **Settings** button on the home screen to view the **About** tab.

Controller Configuration

Before configuring VIA settings on your controller, ensure that the VPN settings are configured on your standalone controller or your Mobility Master and managed device. See the *Virtual Private Networks* chapter in the latest *ArubaOS 8.x.x.x User Guide* for information on configuring VPN settings.

Before you Begin

Note the following licensing and port requirements before you begin configuring your VIA deployment.

License Requirements

Controllers running ArubaOS 8.x require one of two available license types to support VIA users, the **PEFV** license, or the **VIA** license.

The **PEFV** license allows a network administrator to apply firewall policies to clients using a VPN to connect to the controller. This PEFV license is purchased as a single controller-specific license that enabled the functionality up to the full user capacity of the controller.

ArubaOS 8.2.0.0 and later supports a sharable **VIA** license. Each VIA client or 3rd party VPN client consumes a single VIA license. (VIA licenses are not consumed by site-to-site VPNs.) If a standalone controller or a controller managed by Mobility Master has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that controller.

NOTE

For more information on purchasing, installing and managing licenses in ArubaOS 8.x, refer to the ArubaOS Licensing Guide for your ArubaOS version.

Port Access

The following ports must be enabled before configuring VIA on Mobility Master and a managed device:

- **TCP 443**: During the initialization phase, VIA uses HTTPS connections to perform trusted network and captive portal checks. It is mandatory that you enable port 443 on your network to allow VIA to perform these checks.
- **UDP 4500**: This port is used for a VPN connection.
- **Custom Port/Port 8085**: If you have enabled the **Client-certificate based authentication** feature in the VIA authentication profile, you can define the port used for profile downloads in the **Web server Configuration** profile. The supported range is port 1025-65535, and the default value is 8085.

NOTE

The port configured for VIA client certificate-based authentication must also be added to the controller ACL whitelist using the **firewall cp** command or the **Configuration > Services > Firewall > ACL White List** pages of the Mobility Master WebUI. If the port is not configured on the control plane firewall, all packets sent to the controller port will be dropped, and the HTTPS connection will not be established.

Table 8: *VIA Features Requiring TCP Port 443 Access*

Functionality	TCP Port 443				
	Windows	**Linux**	**Android**	**Mac**	**iOS**
Web Auth	✓	✓	✓	✓	✓
Download VIA client software	✓	✓	N/A	✓	N/A
Credential based connection-profile download	✓	✓	✓	✓	✓
Certificate based connection-profile download	✓	N/A	N/A	✓	N/A
VPN Connection		✓		✓	✓
Trusted network check	✓	✓	✓	✓	✓
SSL fallback	✓	✓	N/A	✓	N/A
Captive portal detect	N/A	N/A	N/A	✓	N/A

Table 9: *VIA Features Requiring UDP Port 4500 Access*

Functionality	UDP port 4500				
	Windows	**Linux**	**Android**	**Mac**	**iOS**
VPN Connection	✓	✓	✓	✓	✓

Table 10: *Features Supporting a Custom Port*

Functionality	Custom Port <1025-65535>				
	Windows	**Linux**	**Android**	**Mac**	**iOS**
Certificate based connection-profile download (default, port 8085)	✓	N/A	N/A	✓	N/A

Authentication Methods Supported in VIA

VIA supports the following authentication methods using the IKEv1 and IKEv2 protocols. See the *Virtual Private Networks* chapter in the *ArubaOS 8.x.x.x User Guide* for information on configuring the authentication method on Mobility Master.

Support for two-factor authentication is provided in VIA using devices such as security tokens and smart cards. For more information on multi-factor authentication, see Multi-Factor Authentication on page 128.

IKEv1

IKEv1 consists of two authentication phases: phase 1 and phase 2. IKEv1 phase 1 authenticates the VPN client using either a pre-shared key or an X.509 certificate (the X.509 certificate must appear in the operating system's "user" certificate store). If extended authentication (XAUTH) is used for phase 2 authentication, a username and password are required. The username and password is authenticated against the managed device's internal database, which is either a RADIUS server or an LDAP server. If a RADIUS server is used, the PAP or MSCHAPv2 protocol must be supported.

Support for two-factor authentication is provided in VIA using devices such as security tokens and smart cards. For more information on multi-factor authentication, see Multi-Factor Authentication on page 128.

VIA supports the following authentication methods in IKEv1:

Table 11: *Authentication Methods in IKEv1*

Authentication Method	IKE Information	Description
Pre-Shared Key	IKEv1 PSK	Authentication is not required after the VPN profile is downloaded.
Username and Password	IKEv1 XAUTH	Credentials or token data is required when prompted.
PKI - Client Certificate	IKEv1 Cert	Authentication is not required after the VPN profile is downloaded.
PKI - Smart Card (PIN-based)	IKEv1 Cert	Smart cards support two-factor authentication: Certificate and PIN number. The PIN number is required when prompted. See Authentication using a Smart Card on page 131 for more information on smart cards.
Security Token - Hardware	IKEv1 XAUTH	Code from the physical token is required when prompted. See Multi-Factor Authentication on page 128 for more information on security tokens.
Security Token - Software	IKEv1 XAUTH	Code from the token software is required when prompted. See Multi-Factor Authentication on page 128 for more information on security tokens.
Mobile Authentication	IKEv1 XAUTH	OTP or human interaction is required for authentication. See Authentication using Duo on page 129 for more information on mobile authentication.
Biometric Authentication	IKEv1 XAUTH	Human interaction is required for authentication.

IKEv2

IKEv2 is an updated version of IKE that is faster and supports a wider variety of authentication mechanisms. IKEv2 only uses a single-phase authentication process and supports both RSA and ECDSA certificate-based authentication. VIA locates an X.509 certificate in the operating system's certificate store.

VIA supports the following authentication methods in IKEv2:

Table 12: *Authentication Mechanisms in IKEv2*

Authentication Method	IKE Information	Description
Username and Password	IKEv2 EAP-MSCHAPv2	Credentials are required when prompted.
PKI - Client Certificate	IKEv2 Cert	Authentication is not required after the VPN profile is downloaded.
	IKEv2 EAP-TLS	Authentication is not required after the VPN profile is downloaded.
PKI - Smart Card (PIN-based)	IKEv2 Cert	Smart cards support two-factor authentication: Certificate and PIN number. The PIN number is required when prompted. See Authentication using a Smart Card on page 131 for more information on smart cards.
	IKEv2 EAP-TLS	Smart cards support two-factor authentication: Certificate and PIN number. The PIN number is required when prompted. See Authentication using a Smart Card on page 131 for more information on smart cards.
Mobile authentication	IKEv2 EAP-MSCHAPv2	OTP or human interaction is required for authentication. See Authentication using Duo on page 129 for more information on mobile authentication.
Biometric Authentication	IKEv2 EAP-MSCHAPv2	Human interaction is required for authentication.

Features Supported in VIA

The following table shows the VIA features supported in each platform.

Table 13: *VIA Supported Features*

Feature	Windows	Linux	Android	iOS	MacOS
Authentication Profile Selection	Yes	Yes	Yes	Yes	Yes
Client Auto-Upgrade/Downgrade	Yes	Yes	No	No	Yes
Split Tunneling	Yes	Yes	Yes	Yes	Yes
Client-Side Logging	Yes	Yes	Yes	Yes	Yes
IKEv1 Policy Support	Yes	Yes	Yes	Yes	Yes
IKEv2 Policy Support	Yes	Yes	Yes	Yes	Yes
Use Windows Credentials	Yes	Yes	No	No	No
SuiteB Cryptography	Yes	Yes	Yes	Yes	Yes

Feature	Windows	Linux	Android	iOS	MacOS
Allow User to Save Passwords	Yes	Yes	Yes	Yes	Yes
Enable FIPS Module	Yes	Yes	Yes	Yes	Yes
Lockdown All Settings	Yes	Yes	Yes	Yes	Yes
Domain Suffix in VIA Authentication	Yes	Yes	No	Yes	Yes
Controller Load Balancing	Yes	Yes	Yes	Yes	Yes
Domain Pre-Connect	Yes	Yes	No	No	No
Login Banner	Yes	Yes	Yes	Yes	Yes
Validate Server Certificate	Yes	Yes	Yes	Yes	Yes
Max Session Timeout	Yes	Yes	Yes	Yes	Yes
Logon Script	Yes	Yes	No	No	No
Logoff Script	Yes	Yes	No	No	No
Email Support	Yes	Yes	Yes	Yes	Yes
Maximum Reconnection Attempts	Yes	Yes	Yes	Yes	Yes
External Download URL	Yes	Yes	No	No	Yes
Allow User to Disconnect VIA	Yes	Yes	No	No	Yes
Keep VIA Window Minimized	Yes	Yes	No	No	Yes
Block Traffic Until VPN Tunnel is Up	Yes	No	No	No	No
VIA Installation	Yes	Yes	Yes	Yes	Yes
VIA Uninstallation	Yes	Yes	Yes	Yes	Yes
IKEv1 SSL-Fallback	Yes	Yes	No	Yes	Yes
IKEv2 SSL-Fallback	Yes	Yes	No	Yes	Yes
Automatic Trust/Non-Trust Detection	Yes	Yes	Yes	Yes	Yes
EC Certificates	Yes	Yes	Yes	Yes	Yes
IPsec Rekey	Yes	Yes	Yes	No	Yes
IKE Rekey	Yes	Yes	Yes	No	Yes
Customized Logo	Yes	Yes	Yes	Yes	Yes

Feature	Windows	Linux	Android	iOS	MacOS
Diagnostics Logs	Yes	Yes	Yes	Yes	Yes
Client Auto-Login	Yes	Yes	Yes	Yes	Yes
XAUTH Authentication	Yes	Yes	Yes	Yes	Yes
Connection Failover	Yes	Yes	Yes	Yes	Yes
Command Line Support for Installation	Yes	Yes	No	No	Yes
EULA Support	Yes	Yes	Yes	Yes	Yes
Online Certificate Request	No	Yes	No	No	No
Heartbeat/Keep-Alive Messages	Yes	Yes	Yes	Yes	Yes
Unique Device ID	Yes	Yes	Yes	Yes	Yes
OEM Support	Yes	No	No	No	Yes
Smart Card Support	Yes	No	No	No	No
MOBIKE	Yes	Yes	Yes	No	Yes
Common Name Against AAA Server	Yes	Yes	Yes	Yes	Yes
PAP for Authentication	Yes	Yes	Yes	Yes	Yes
MSCHAPv2 for Authentication	Yes	Yes	Yes	Yes	Yes
RSA Certificate Length 1024/2048/4096	Yes	Yes	Yes	Yes	Yes
EC Certificate Length 256/384	Yes	Yes	Yes	Yes	Yes
Command Line Operation	No	Yes	No	No	No
Third Party Captive Portal Support	No	No	No	No	Yes
VIA Gateway	No	Yes	No	No	No
VIA Auto-Config	No	Yes	Yes	No	No
Zero Touch Provisioning (Windows)	Yes	No	No	No	No
Hex-Based PSK	Yes	Yes	Yes	No	Yes
OCSP	Yes	Yes	Yes	No	No
Integrity Check	Yes	Yes	No	No	No
Samsung Knox Integration	No	No	Yes	No	No

Feature	Windows	Linux	Android	iOS	MacOS
Validation of Strength of Symmetric Algorithm	Yes	Yes	Yes	No	No
IPsec Drop Policy	Yes	Yes	Yes	No	No
Verification of DN Values in a Peer Certificate	Yes	Yes	Yes	No	No

Configuring VIA Settings

The following steps are required to configure your Mobility Master and managed devices for VIA. VIA can be configured using the WebUI or CLI. These steps are described in detail in the following subsections:

- Configuring VIA using the WebUI on page 95
  1. Configuring the Pre-Shared Key (PSK) on page 95
  2. Uploading Certificates for Certificate-Based Authentication on page 96
  3. Enabling VPN Server Modules on page 97
  4. Creating VIA User Roles on page 97
  5. Creating VIA Authentication Profiles on page 99
  6. Creating VIA Connection Profiles on page 101
  7. Associating VIA Connection Profiles to User Roles on page 107
  8. Configuring VIA Web Authentication Profiles on page 108
  9. Configuring VIA Client WLAN Profiles on page 109
  10. Configuring Additional VIA Options on page 111
  11. Rebranding VIA on page 113
  12. Uploading VIA Installers on page 114
  13. Downloading VIA Installer on page 115
- Configuring VIA using the CLI on page 115
  1. Enabling VPN Server Modules on page 115
  2. Creating VIA Roles on page 115
  3. Creating VIA Authentication Profiles on page 116
  4. Creating VIA Connection Profiles on page 116
  5. Configuring VIA Web Authentication on page 116
  6. Associating VIA Connection Profiles to User Roles on page 116
  7. Configuring VIA Client WLAN Profiles on page 117
  8. Rebranding VIA and Uploading VIA Installers on page 117

Configuring VIA using the WebUI

Perform the following steps to configure VIA using the WebUI.

NOTE

Certain features are not available in every platform. Refer to Features Supported in VIA on page 91 to view the list of features that are supported for each platform.

Configuring the Pre-Shared Key (PSK)

To configure a pre-shared key for VIA:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Click **Shared Secrets** to expand that section.
3. Click **+** at the bottom of the **IKE Shared Secrets** table.
4. Under **Create IKE Group**, enter the **Subnet** and **Subnet mask**. Use the default value of **0.0.0.0** if you are only using one pre-shared key.
5. Select the format in which your pre-shared key is displayed from the **Representation type** drop-down list.

6. Enter your pre-shared key, and then retype the key to confirm.
7. Click **Submit**.
8. Select **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Uploading Certificates for Certificate-Based Authentication

To upload certificates for VIA:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **System** > **Certificates**.
2. Click **Import Certificates** to expand that section.
3. Click **+** at the bottom of the **Import Certificates** table. The **New Certificate** page opens.
4. Enter a **Certificate name**.
5. Click **Browse** to locate and select a certificate from your local file explorer.
6. (Optional) Enter a passphrase, and then retype the passphrase to confirm.
7. Select the format of the certificate from the **Certificate format** drop-down list.
8. Select **TrustedCA** or **ServerCert** from the **Certificate type** drop-down list.
9. Click **Submit**.
10. Select **Pending Changes**.
11. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

NOTE

VIA allows use of certificates stored in smart cards for Windows and Linux devices.

NOTE

Both server certificates and trusted CAs (**Certificate type**) must be uploaded for VIA.

NOTE

For Linux devices, VIA can request certificates from a CA server using either the HTTP or SCEP protocol.

To select a server certificate for certificate-based authentication:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Click **General VPN** to expand that section.
3. Select a server certificate from the **Server-certificate for VPN clients** drop-down list.
4. Click **Submit**.
5. Click **Certificates for VPN Clients** to expand that section.
6. Under the **CA Certificate Assigned for VPN-Clients** table, click **+** and select a CA certificate from the drop-down list.
7. (Optional) Under the **Certificate Groups for VPN-Clients** table, click **+** and select a **CA Certificate** and **Server Certificate** from the respective drop-down lists.
8. Click **Submit**.
9. Select **Pending Changes**.
10. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Enabling VPN Server Modules

ArubaOS allows you to connect to VIA using the default user roles. However, you must install the Policy Enforcement Firewall Virtual Private Network (PEFV) license in order to configure and assign specific user roles. Refer to the *Aruba Mobility Master Licensing Guide* for more information on licenses.

To install a license:

1. On a standalone controller or in the **Mobility Master** hierarchy on Mobility Master, navigate to **Configuration > System > Licensing**.
2. Under the **Mobility Master Licenses** tab, click **+** to add a new license. The **Install Licenses** window opens.
3. Enter the license key(s) in the text box.
4. Click **OK**.

Creating VIA User Roles

VIA user roles contain access control policies for users connecting to the network through VIA. You can configure different VIA roles or use the default VIA role **default-via-role**.

To create a VIA user role:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration > Roles & Policies > Roles**.
2. Click **+** at the bottom of the **Roles** table to add a new user role. The **New Role** window opens.
3. Enter a name for the role.
4. Click **Submit**.
5. Select **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.
7. Select the new role from the **Roles** table.
8. Click **+** at the bottom of the **RULES FOR THIS ROLE ONLY** table. The **New Rule for <rule name>** window opens.
9. Select **Access Control** or **Application** under **Rule Type**, and then click **OK**.
10. Under **forwarding Rule**, configure the parameters listed in Table 14.

Table 14: *User Role Rule Parameters*

Parameter	Description
IP version	Internet Protocol version: - **IPv4** - **IPv6**
Source	The traffic source: - **Alias**: Network alias - **Any**: Any traffic source - **Host**: Single host IP address - **Local IP**: All local IP addresses in the system - **Network**: IP address and netmask - **User**: IP address of the user
Destination	The traffic destination: - **Alias**: Network alias - **Any**: Any traffic source - **Host**: Single host IP address - **Local IP**: All local IP addresses in the system - **Network**: IP address and netmask - **User**: IP address of the user
Scope	Scope of the rule: - **Application** - **App Category** - **Web Category/Reputation** **NOTE:** For application rules only.
Service/app	The service or application to which this rule applies: - **Protocol**: IP protocol - **Any**: Any service or application - **Service**: Network service - **TCP**: TCP port - **UDP**: UDP port **NOTE:** For access control rules only.
Action	Denies or permits access to the network through VIA.
TOS	The 8-bit TOS/DSCP/ECN field in the IP header.
Time range	Time range for the rule. - Click **+** at the bottom of the **Time range** drop-down list to add a new time range. - Hover your mouse over an existing time range to edit or delete that time range. - Click **Reset** to use the default time range.
802.1p priority	802.1p priority level of the rule.
Options	Enables or disables additional options for the rule: - **Log**: Generates a log message each time the rule is applied. - **Mirror**: Mirrors all session packets to the destination. - **Blacklist**: Blacklists users matching the rule. - **Disable Scanning**: Disables ARM scanning while traffic is present.

11. Click **Submit**.
12. Select **Pending Changes**.
13. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

For more information on user roles, refer to the latest *ArubaOS 8.x.x.x User Guide*.

Creating VIA Authentication Profiles

VIA authentication profiles contain server groups for authenticating VIA users. The server group contains the list of authentication servers and server rules to derive user roles, based on the user authentication. You can configure multiple VIA authentication profiles and/or use the default VIA authentication profile created in the **Internal** server group.

To create an authentication profile:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > L3 Authentication**.
2. Select **VIA Authentication** from the **L3 Authentication** list.
3. Under **VIA Authentication Profile: New Profile**, click **+** to add a new authentication profile.
4. Configure the parameters listed in Table 15. Note that not all parameters available in ArubaOS 8.3 may be available in earlier versions of ArubaOS 8.x.

Table 15: *VIA Authentication Profile Parameters in ArubaOS 8.3.x*

Parameter	Description
Profile Name	Name of the VIA authentication profile.
Default Role	Role to be assigned to authenticated users.
Max Authentication Failures	Maximum authentication failures permitted. The default is 0.
Description	A user-friendly name or description for the authentication profile.
Check Certificate Common Name against AAA Server	If you are using client certificates for user authentication, enable this option to verify that the certificate's common name exists in the server.
Client-certificate based authentication for VIA profile download	If selected, this option enables client certificate-based authentication for VPN profile download on port 8085. This option is disabled by default. You can configure a different port number for certificate-based profile downloads using the **VIA client-cert port number** parameter in the **Web server Configuration** profile, configurable on the **Configuration** > **Authentication>L3 Authentication>Web Server Configuration** page of the Mobility Master WebUI. **NOTE:** This feature was introduced in ArubaOS 8.1.
Authentication Protocol	PAP and MSCHAPv2 protocols used to authenticate VIA users. Default: PAP

Parameter	Description
PAN Firewalls Integration	If enabled, this option requires IP mapping at Palo Alto Networks (PAN) firewalls.
Downloadable Role from CPPM	Enable this feature to allow Aruba ClearPass Policy manager to assign a role to a VIA user after successful authentication to ClearPass Policy Manager. ClearPass Policy Manager sends the **Aruba-CPPM-Role** vendor-specific attribute (VSA) in the RADIUS Access-Accept message once the user is authenticated. If the role is not already defined on Mobility Master, Mobility Master will automatically download the role for that VIA user from ClearPass Policy Manager. Mobility Master retains these downloaded roles until there are no more users referencing that role, at which time Mobility Master removes the downloadable role. This feature supports roles obtained when VIA user is authenticated through XAuth, and is implemented only for IKEV1. **NOTE:** This feature is supported in ArubaOS 8.1.0 and later releases and is enabled in ArubaOS 8.x using the VIA authentication profile in the WebUI, or by issuing the **aaa authentication via auth-profile <profile > download-role** command in the command-line interface. For detailed information on configuring downloadable ClearPass Policy manager user roles for VIA users, refer to the *ClearPass Policy Manager Integration* chapter of the ArubaOS User Guide.
Encoding format for the user credentials	Select one of the following encoding formats for the VIA user credentials. The Default is UTF-8. ● UTF-8 ● UTF-16 ● ANSI

5. Click **Submit**.
6. Select **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To modify an existing authentication profile:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > L3 Authentication**.
2. Expand **VIA Authentication** from the **L3 Authentication** list.
3. Select an existing VIA authentication profile.
4. Modify the profile settings under **VIA Authentication Profile: <profile name>**.
5. Click **Submit**.
6. Select **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To change the server group for an authentication profile:

1. IOn a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > L3 Authentication**.
2. Expand **VIA Authentication** from the **L3 Authentication** list.
3. Expand the VIA authentication profile.
4. Click **Server Group** under the selected authentication profile.
5. Under **Server Group: <server group name>**, select a different server group from the drop-down list.
6. (Optional) To enable authentication fail through and load balancing, select the check boxes for **Fail Through** and **Load Balance**.
7. Click **Submit**.

8. Select **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To add a new server group:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > Auth Servers**.
2. Click **+** at the bottom of the **Server Groups** table. The **Add Server Group** window opens.
3. Enter a name for the new server group.
4. Click **Submit**.
5. Select the server from the Server Groups table.
6. Modify the **Servers**, **Options**, and **Server Rules** as necessary. See the *Authentication Servers* chapter in the latest *ArubaOS 8.x.x.x User Guide* for more details on modifying server groups.
7. Click **Submit**.
8. Select **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Creating VIA Connection Profiles

VIA connection profiles contain settings required by VIA to establish a secure connection to a standalone controller or a Mobility Master managed device. VIA connection profiles are always associated to a user role, and all users belonging to that associated role use the configured settings. If you do not assign a VIA connection profile to a user role, the default connection profile is used. Multiple connection profiles can be configured.

NOTE

After establishing a connection to a standalone controller or a managed device ,VIA sends heartbeat/keep-alive messages every 15 seconds.

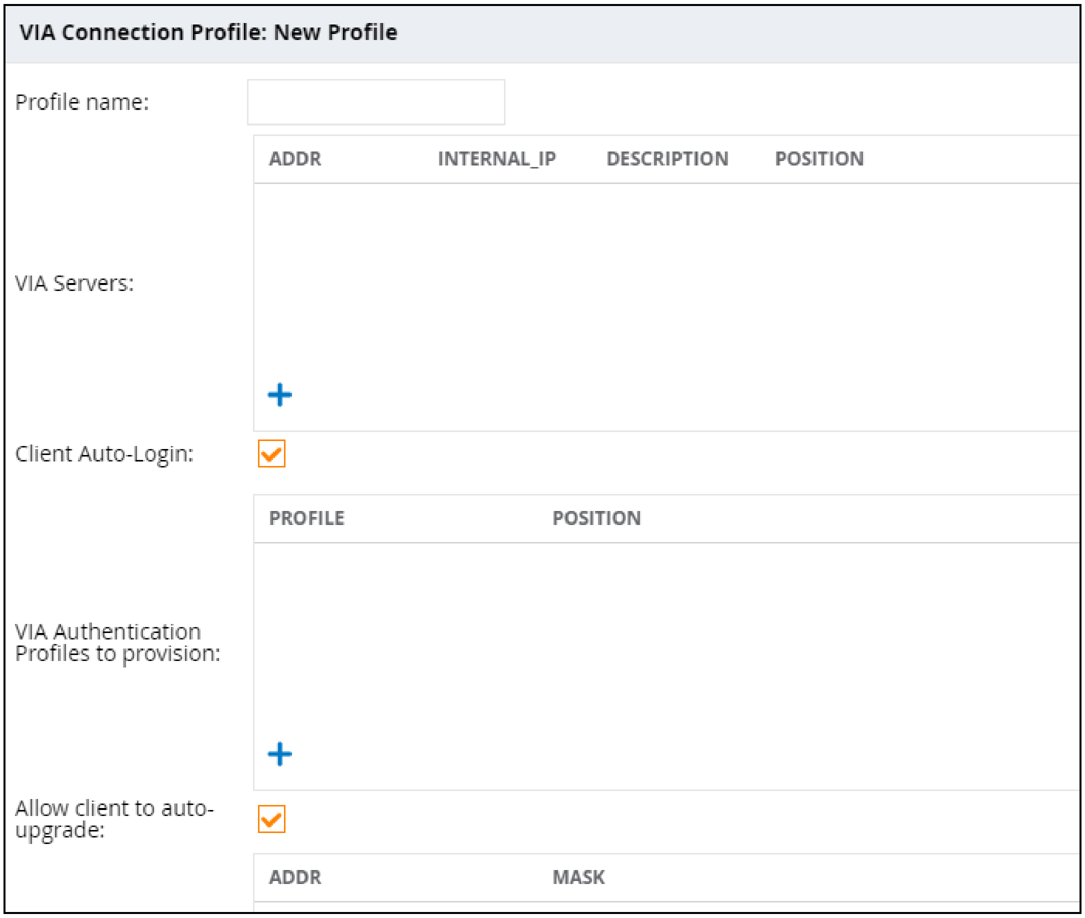
NOTE

In Windows devices, VIA is functional with proxy settings configured in the system, but connection profiles with proxy settings cannot be downloaded.

To create a VIA connection profile:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > L3 Authentication**.
2. Select **VIA Connection** from the **L3 Authentication** list.
3. Under **VIA Connection Profile: New Profile**, click **+** to add a new VIA connection profile.

Figure 73 *Creating a VIA Connection Profile*



VIA Connection Profile: New Profile

Profile name:

VIA Servers:

ADDR	INTERNAL_IP	DESCRIPTION	POSITION

Client Auto-Login: ☑

VIA Authentication Profiles to provision:

PROFILE	POSITION

Allow client to auto-upgrade: ☑

ADDR	MASK

4. Enter a **Profile name**.
5. Configure the remaining profile settings listed in Table 16.

> NOTE
>
> Certain settings are not available in every platform. Refer to Features Supported in VIA on page 91 to view the list of features that are supported for each platform.

Table 16: *VIA - Connection Profile Options*

Configuration Option	Description
VIA Servers	Enter the following information about the controller. - *Controller Hostname/IP Address*: This is the public IP address or the DNS hostname of the VIA controller. Users will connect to remote server using this IP address or the hostname. - Controller Internal IP Address: This is the IP address of any of the VLAN interface IP addresses belongs to this controller. - Controller Description: This is a human-readable description of the controller. Click the **Add** button after you have entered all the details. If you have more than one controller you order them by clicking the *Up* and *Down* arrows. To delete a controller from your list, select a controller and click the **Delete** button.
Client Auto-Login	Enables or disables automatic login on VIA client and establishes a secure connection to the managed device as soon as the connection profile is downloaded. This option is applicable even after restarting the device. Default: Enabled
VIA Authentication Profiles to provision:	Select an authentication profile to add a VIA authentication profile for IKE/IPsec authentication. If you have multiple VIA authentication profiles, you can re-order them by changing their position in the list.
Allow client to auto-upgrade	Enables or disables automatic upgrade for VIA client when an updated version is available. Default: Enabled
VIA tunneled networks	A list of network destinations (IP addresses and netmasks) that the VIA client will tunnel through the controller. All other network destinations will be reachable directly by the VIA client. - Enter an IP address and network mask and click **Add** to add to the tunneled networks list. - To delete a network entry, select the IP address and click **Delete**.
Enable split-tunneling	Enable or disable split tunneling. - If enabled, all traffic to the VIA tunneled networks will go through the controller and the rest is just bridged directly on the client. - If disabled, all traffic will flow through the controller. Default: off
VIA Client WLAN Profiles	A VIA client WLAN profile must be pushed to client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks. Click **+** at the bottom of the **VIA Client WLAN profiles** table, select a WLAN profile from the **profile** drop-down list, then click OK
Allow client-side logging	Enable or disable client side logging. If enabled, VIA client will collect logs that can be sent to the support email-address for troubleshooting. Default: Enabled
VIA IKE V2 Policy	List of available IKEv2 policies.
VIA IKE Policy	List of IKE policies that the VIA Client has to use to connect to the controller. These IKE policies are configured under **Configuration** > **Advanced Services** > **VPN Services** > **IPSEC** > **IKE Policies**.

Configuration Option	Description
Use Windows Credentials	Enable or disable the use of the Windows credentials to login to VIA . If enabled, the SSO (Single Sign-on) feature can be utilized by remote users to connect to internal resources. Default: Enabled
Enable IKEv2	Select this option to enable or disable the use of IKEv2 policies for VIA.
Use Suite B Cryptography	Select this option to use Suite B cryptography methods. You must install the advanced cryptography license to use the Suite B cryptography.
IKEv2 Authentication method	List of all IKEv2 authentication methods.
VIA IPSec V2 Crypto Map	List of all IPsec V2 that the VIA client uses to connect to the controller.
VIA IPSec Crypto Map	List of IPsec Crypto Map that the VIA client uses to connect to the controller. These IPsec Crypto Maps are configured in CLI using the command **crypto-local ipsec-map <ipsec-map-name>**.
Allow user to save Passwords	Allow user to save the VIA password
Enable Supplicant	If enabled, VIA starts in bSec mode using L2 suite-b cryptography. This option is disabled by default.
Enable FIPS Module	Enable the VIA (Federal Information Processing Standard) FIPS module so VIA checks for FIPS compliance during startup. This option is disabled by default.
Auto-Launch Supplicant	Select this option to automatically connect to a configured WLAN network.
Lockdown all Settings	If enabled, all user options on the VIA client are disabled.
Domain Suffix in VIA Authentication	Enables a domain suffix on VIA authentication, so client credentials are sent as **domainname\username** instead of just **username.**
Enable Controllers Load Balance	Enable this option to allow the VIA client to failover to the next available selected randomly from the list as configured in the VIA Servers option. If disabled, VIA will failover to the next in the sequence of ordered list of VIA servers.
Enable Domain Preconnect	Enable this option to allow users with lost or expired passwords to establish a VIA connection to corporate network. This option authenticates the user's device and establishes a VIA connection that allows users to reset credentials and continue with corporate access.
Enable Generating common profile if DPC is enabled:	Enable this option to preprovision a VIA profile for new users. This feature is useful if multiple users on your network share the same system, because after the first user downloads the VPN connection profile, when subsequent users log in, those additional users do not have provide initial details like the VPN gateway address and user credentials
VIA Banner Message Reappearance Timeout(minutes)	The maximum time (minutes) allowed before the VIA login banner reappears. Default: 1440 min

Configuration Option	Description
VIA Client Network Mask	VIA client network mask, in dotted decimal format.
Validate Server Certificate	Enable or disable VIA from validating the server certificate presented by the controller. Default: Enabled
VIA Client DNS Suffix List	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established. Default: None.
OCSP Cert verification enabled	Enables or disables verification of certificates using the Online Certificate Status Protocol (OCSP).
In EAP/IKE, action taken when OCSP Cert verification result is unknown	The action taken when the revocation status of an OCSP certificate is unknown.
VIA domain name profiles	To select a domain name profile, click **+** at the bottom of the **VIA Domain Name Profiles** table, and Enter the following information for the domain name: - **CN**: Common name of the organization. - **ORG**: Name of the organization. - **OU**: Organizational unit, such as a department. - **Country**: Two letter ISO country code for the country in which the organization is located.
Destination Traffic to be blocked:	To block traffic for a specific destination or user, click **+** at the bottom of the **Destination Traffic to be blocked** table and enter the following information: - **addr**: IP address of the user or destination. - **netmask**: Network mask
block-destination-traffic-selector (ON/OFF):	Enable this option to block traffic to the selected destinations
VIA max session timeout	The maximum time (minutes) allowed before the VIA session is disconnected. Default: 1440 min
VIA Logon Script	Specify the name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside in the client computer.
VIA Logoff Script	Specify the name of the logoff script that must be executed after the VIA connection is disconnected. The logoff script must reside in the client computer.
VIA Support Email Addresses	The support e-mail address to which VIA users will send client logs.
Maximum reconnection attempts	The maximum number of re-connection attempts by the VIA client due to authentication failures. Default: 3
VIA external download URL	End users will use this URL to download VIA on their computers.

Configuration Option	Description
Allow user to disconnect VIA	Enable or disable users to disconnect their VIA sessions. Default: on
Content Security Gateway URL	If split-tunnel forwarding is enabled, access to external (non-corporate) web sites will be verified by the specified content security service provider.
Comma separated list of HTTP ports to be inspected (apart from default port 80)	Traffic from the specified ports will be verified by the content security service provider.
Certificate Criteria	Allows admin users to filter the certificates that can be used to establish the IPsec connection when a user certificate or EAP-TLS is used as the authentication method. Use the following certificate attributes or OIDs to set the certificate criteria: ● **commonName** (OID 2.5.4.3) ● **organizationalUnitName** (OID 2.5.4.11) ● **organizationName** (OID 2.5.4.10) ● **subjectAltName** (OID 2.5.29.17) ● **certificateIssuer** (OID 2.5.29.29) ● **userPrincipalName** (OID 1.3.6.1.4.1.311.20.2.3) ● **emailAddress** (OID 1.2.840.113549.1.9.1) ● **friendlyName** (OID 1.2.840.113549.1.9.20) The maximum length is 256 characters. Each attribute or OID must be separated by a semicolon. If an attribute or OID contains any spaces, the entire string must be enclosed in quotation marks.
Enable Content Security Services	Select this check box to enable content security service. You must install the Content Security Services licenses to use this option.
VIA window minimized	Enable this option to minimize the VIA client to system tray during the connection phase. Applicable to VIA client installed in computers running Microsoft Windows operating system.
Block traffic until VPN tunnel is up	If enabled, this feature will block network access until the VIA VPN connection is established. Note that VIA automatically adds exceptions for the following IP addresses: ● Default gateway ● DNS server ● DHCP server ● Controller's internal and external addresses ● Any local subnet that can be reached through a single hop **NOTE:** Use the **Block Traffic Rules** parameter in this profile to define a whitelist of IP addresses for which this setting will not apply (for example, a list of target IP addresses that should be allowed through to a captive portal).
Block traffic rules	Specify a hostname or IP address and network mask to define a whitelist of users to which the **Block traffic until VPN tunnel is up** setting will not apply.

Configuration Option	Description
User idle timeout	Select the **Enable** check box to configure user idle timeout value for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.
VIA Client MTU value	VIA calculates optimal MTU value for the virtual adapter based on the physical network interface on the client machine. But in some situations, this optimal value may not be desired. This feature allows the administrator to change the MTU value used by VIA. VIA compares the VIA-calculated MTU and configured MTU, and uses the lesser MTU value. For example, if the VIA-calculated MTU value is 1300 and the configured MTU value is 1452, VIA uses 1300.
tos-dscp value	This feature provides the ability to mark outgoing IKE and ESP packets with DSCP, values from 0 to 63. The VIA client will use this value it to mark the IP packets for both IKE (during tunnel creation) and ESP/IPSec (post-tunnel establishment), so packets receive appropriate QoS treatment by other/intermediate network devices between the client and the managed device or standalone controller. **NOTE:** If this value is left to default setting (value of 0), the Windows VIA client copies the original DSCP marking of inner packet to outer packet, hence retaining the original QoS marking. This behavior can be considered as equivalent or greater than best effort service. On all other platforms (non-Windows), if this value is not explicit set other than 0, would mark the outer packet with DSCP of 0 (best effort).

6. Click **Submit**.
7. Select **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

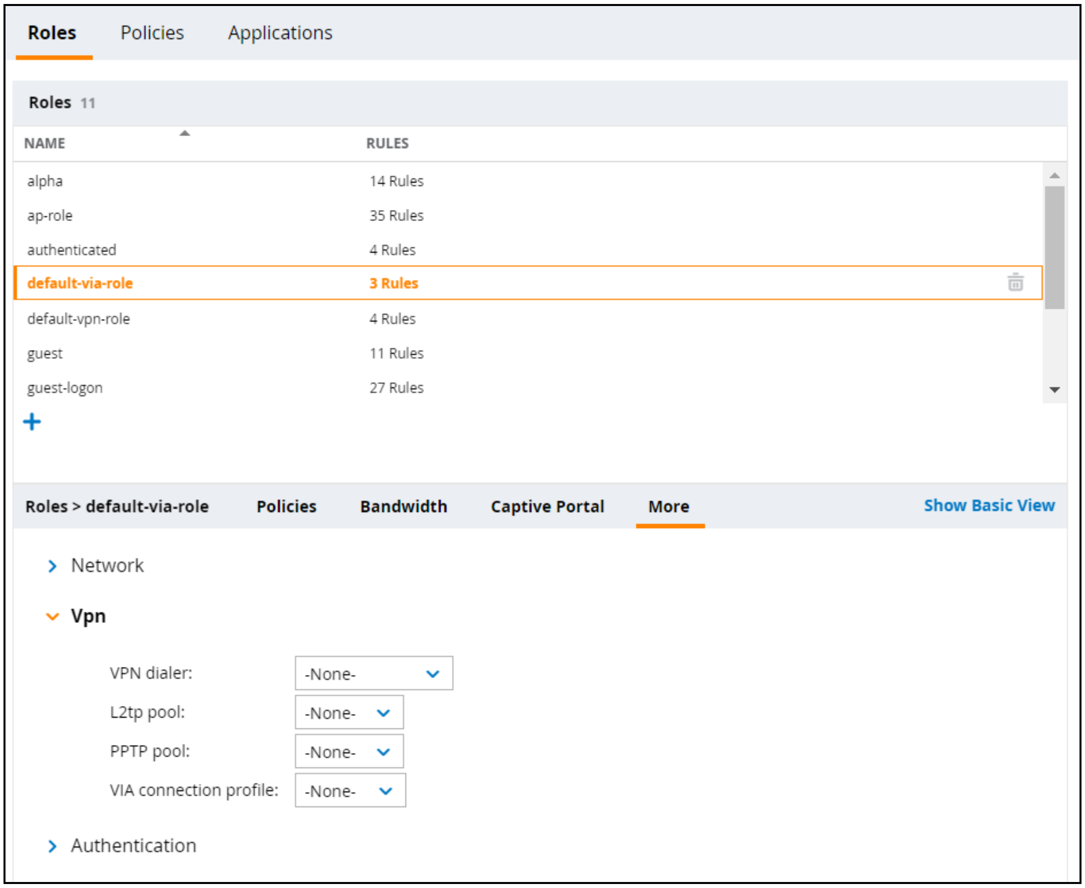
Associating VIA Connection Profiles to User Roles

VIA connection profiles must be associated to a user role. Users can login by authenticating against the server group specified in the VIA authentication profile, after which they are placed into a user role. If the VIA configuration settings are derived from the VIA connection profile attached to the user role, the default VIA connection profile is used.

To associate a VIA connection profile to a user role:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Roles & Policies > Roles**.
2. Select the VIA user role from the **Roles** table (see Creating VIA User Roles on page 97 for details on creating user roles).
3. Click **Show Advanced View**.
4. Under the **More** tab, click **VPN** to expand that section.

Figure 74 *Associating a VIA Connection Profile to a User Role*



Roles 11

NAME	RULES
alpha	14 Rules
ap-role	35 Rules
authenticated	4 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
guest	11 Rules
guest-logon	27 Rules

VPN dialer: -None-

L2tp pool: -None-

PPTP pool: -None-

VIA connection profile: -None-

5. Select a VIA connection profile from the drop-down list.
6. Click **Submit**.
7. Select **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Configuring VIA Web Authentication Profiles

VIA web authentication profiles contain an ordered list of VIA authentication profiles. The web authentication profile is used by end-users to login to the VIA download page (*https://<server-IP-address>/via*), where they can download VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select a profile during client login.

To configure a VIA web authentication profile:

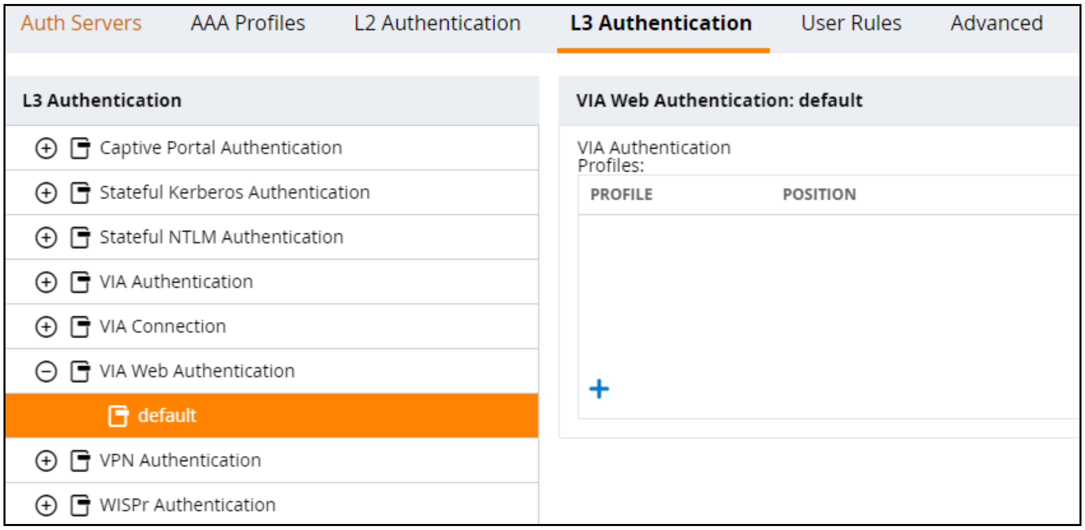
1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Authentication > L3 Authentication**.
2. Expand **VIA Web Authentication** from the **L3 Authentication** list, and click on the **default** profile.

NOTE

You can have only one profile for VIA web authentication.

3. Under **VIA Web Authentication: default**, click **+** at the bottom of the **VIA Authentication Profiles** list.

Figure 75 *Configuring the Default VIA Web Authentication Profile*



4. Select a profile from the drop-down list, and then click **OK**.
5. Click **Submit**.
6. Select **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

If you have multiple VIA authentication profiles, you can re-order them by changing their **Position**. Click the **Trash** icon to delete an authentication profile from the list.

Configuring VIA Client WLAN Profiles

You can push WLAN profiles to end-user computers that use the Microsoft Windows Wireless Zero Config (WZC) service to configure and maintain their wireless networks. After the WLAN profiles are pushed to the end-user computers, they are automatically displayed as an ordered list in the preferred networks. The VIA client WLAN profiles provisioned on the client can be selected from the VIA connection profile described in Creating VIA User Roles on page 97.

To configure a VIA client WLAN profile:

1. IOn a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **System** > **Profiles**.
2. Expand **Wireless LAN** from the **All Profiles** list.
3. Select the **VIA Client WLAN** profile**.**
4. Under **VIA Client WLAN Profile: New Profile**, click **+** to add a new WLAN profile.
5. Enter a **Profile name**.
6. Configure the profile settings listed in Table 17.

Table 17: *VIA Client WLAN Profile Settings*

Parameter	Description
EAP Type	EAP type used by clients to connect to the wireless network. Default: EAP-PEAP
Inner EAP Type	Inner EAP type.
EAP-PEAP options	If you are using EAP-PEAP (Protected EAP), you can select the following options to connect to the network: ● **validate-server-certificate**: Validates the server certificate. ● **enable-fast-reconnect**: Allows fast reconnect. ● **enable-quarantine-checks**: Performs quarantine checks. ● **disconnect-if-no-cryptobinding-tlv**: Disconnects if server does not present cryptobinding TLV. ● **dont-allow-user-authorization**: Disables user prompts for authorizing new servers or trusted certification authorities.
EAP-Certificate Options	If you are using EAP-certificate, you can select the following options to connect to the network: ● **use-smartcard:** Uses a smart card. ● **simple-certificate-selection:** Uses a certificate on the user's computer or a simple certificate selection method (recommended). ● **use-different-name:** Uses a different user name for the connection (and not the CN on the certificate). ● **validate-server-certificate:** Validates the server certificate.
Inner EAP Authentication options:	If you are using Innter EAP authentication, you can select the following options to connect to the network: ● **mschapv2-use-windows-credentials:** Uses the Windows logon name and password (and domain if any). ● **use-smartcard:** Uses a smart card. ● **simple-certificate-selection:** Uses a certificate on the user's computer or a simple certificate selection method (recommended). ● **use-different-name:** Uses a different user name for the connection (and not the CN on the certificate). ● **validate-server-certificate:** Validates the server certificate.
Automatically connect when this WLAN is in range	If enabled, this option allows WZC (Microsoft Windows Wireless Zero Config tool) to connect when the network (SSID) is available. Default: Enabled
EAP-PEAP: Connect only to these servers	List of servers to which users can connect with EAP-PEAP, separated by commas.
Enable IEEE 802.1x authentication for this network	If selected, this option enables 802.1x authentication for the network. Default: Enabled
EAP-Certificate: Connect only to these servers	List of servers to which users can connect with an EAP certificate, separated by commas.
Authenticate as computer when computer info is available	Select this option when computer information is available. If enabled, the client performs computer authentication during login.

Parameter	Description
Inner EAP-Certificate: Connect only to these servers	List of servers to which users can connect with an inner EAP certificate, separate by commas.
Authenticate as guest when computer or user info is unavailable	Select this option when computer or user information is not available. If enabled, the client authenticates as a guest during login.
Connect even if this WLAN is not broadcasting	Allows VIA to connect, even if the WLAN is not broadcasted. Default: Disabled

7. Click **Submit**.
8. Select **Pending Changes**.
9. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Configuring Additional VIA Options

The following sections describe additional VIA options.

Manual Upgrade and Downgrade

Users can install a later version of VIA on top of an earlier version, or an earlier version of VIA on top of a later version (unsupported fields are omitted during a downgrade).

NOTE

Manual downgrade is not available in iOS devices.

IKE Rekey

IKE rekey occurs at a configured interval in the IKE proposal.

NOTE

IKE Rekey is not available in iOS devices.

To configure the rekey (security association) interval in the WebUI:

1. In the **Mobility Master** node hierarchy, navigate to **Configuration** > **Services** > **VPN**.
2. Click **IKEv1** or **IKEv2** to expand that section.
3. Select an existing IKE policy from the **IKEv1 Policies** or **IKEv2 Policies** table, or click **+** to add a new policy.
4. Under the **Lifetime** field, enter a rekey interval, in seconds.
5. Click **Submit**.
6. Select **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To configure the rekey (security association) interval in the CLI, execute the following command:

```
(host) [mm] (config) #crypto isakmp policy <priority> lifetime <seconds>
```

IPsec Rekey

IPsec rekey occurs at a configured interval in the IPsec proposal.

NOTE

IPsec Rekey is not available in iOS devices.

To configure the rekey (security association) interval in the WebUI:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration > Services > VPN**.
2. Click **Site to Site** to expand that section.
3. Select an existing IPsec map from the **IPSec Maps** table, or click **+** to add a new IPsec map.
4. Under the **SA lifetime (seconds)** or **SA lifetime (kb)** field, enter a rekey interval, in seconds or kilobytes.
5. Click **Submit**.
6. Select **Pending Changes**.
7. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To configure the rekey (security association) interval in the CLI, execute the following commands:

```
(host) [mm] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
   set security-association lifetime kilobytes <kilobytes>
   set security-association lifetime seconds <seconds>
```

IKEv1 and IKEv2 SSL-Fallback

When port 4500 is blocked , VIA establishes IPsec over SSL using TCP 443.

To enable this option in the WebUI:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration > Profiles > Other Profiles > VIA Global Configuration**.
2. Select the **Allow SSL Fallback** check box.
3. Click **Submit**.
4. Select **Pending Changes**.
5. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To enable this option in the CLI, execute the **aaa authentication via global-config ssl-fallback-enable** command.

NOTE

IKEv1 SSL-fallback and IKEv2 SSL-fallback are not available in Android devices.

Extended Authentication (XAUTH)

Extended Authentication (XAUTH) is an Internet Draft that permits user authentication after IKEv1 authentication. XAUTH prompts the user for a username and password, which are authenticated through an external RADIUS or LDAP server or the Mobility Master/managed device's internal database. Alternatively, users can start client authentication with a smart card, which contains a digital certificate to verify the client credentials. IKEv1 authentication can be done with either an IKE pre-shared key or digital certificates.

To enable XAUTH in the WebUI:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration > Services > VPN**.
2. Click **IKEv1** to expand that section.
3. Select **Enabled** from the **XAuth** drop-down list.
4. Click **Submit**.
5. Select **Pending Changes**.

6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Management APIs

Management APIs are based on Android messages and intents. For more details, refer to the *Android VIA Management API Guide.*

Rebranding VIA

ArubaOS allows you to rebrand VIA client and the VIA download page with a custom logo, HTML page, and login banner.

NOTE

VIA supports Alcatel-Lucent and Dell OEMs.

NOTE

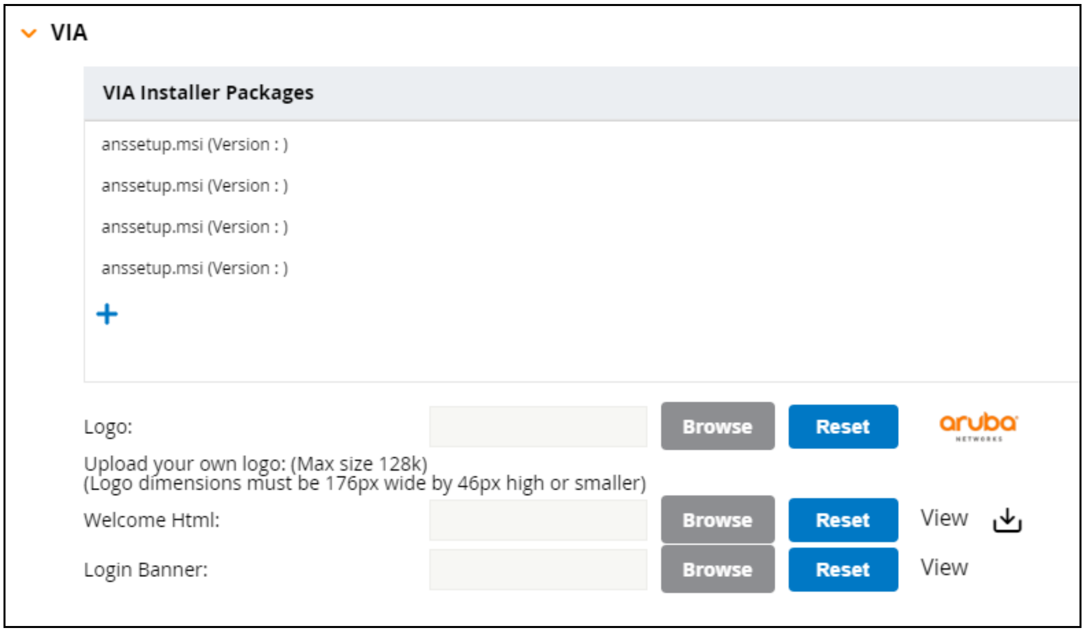
OEMs and rebranding are only supported in Windows and Mac OS devices.

Customizing the Logo

To use a custom logo on VIA client and the VIA download page:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Select **VIA** to expand that section.
3. Under the **Logo** section, click **Browse** to locate and select a logo from your local file explorer.
4. Click **Submit**.
5. Select **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

Figure 76 *Customizing the VIA Logo*



VIA

VIA Installer Packages

anssetup.msi (Version :)

anssetup.msi (Version :)

anssetup.msi (Version :)

anssetup.msi (Version :)

Logo:

Upload your own logo: (Max size 128k)
(Logo dimensions must be 176px wide by 46px high or smaller)

Welcome Html:

Login Banner:

To use the default VIA logo, click **Reset**.

Customizing the Landing Page for Web-based Login

To use a custom landing page for VIA web login:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Select **VIA** to expand that section.
3. Under the **Welcome HTML** section, click **Browse** to locate and select the HTML file from your local file explorer.

   Variables that are used in the custom HTML file must 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</a>`)
   - `<% download %>`: The installer download link (Example: `<a href="<% download %>">Click here to download VIA</a>`)
4. Click **Submit**.
5. Select **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To use the default welcome page, click **Reset**.

Customizing the Login Banner

The login banner ensures that end-users agree to a customized terms-of-service before using the private network established by VIA. To use a custom login banner for VIA client:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Select **VIA** to expand that section.
3. Under the **Login Banner** section, click **Browse** to locate and select the custom login banner from your local file explorer.
4. Click **Submit**.
5. Select **Pending Changes**.
6. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

To use the default login banner, click **Reset**.

Uploading VIA Installers

To upload a new VIA installer on the web page:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Select **VIA** to expand that section.
3. Click **+** at the bottom of the **VIA Installer Pacakges** table. The **New VIA Installer Package** window opens.
4. Click **Browse** to locate and select the installer from your local file explorer.
5. Click **OK**.
6. Click **Submit**.
7. Select **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**.

NOTE

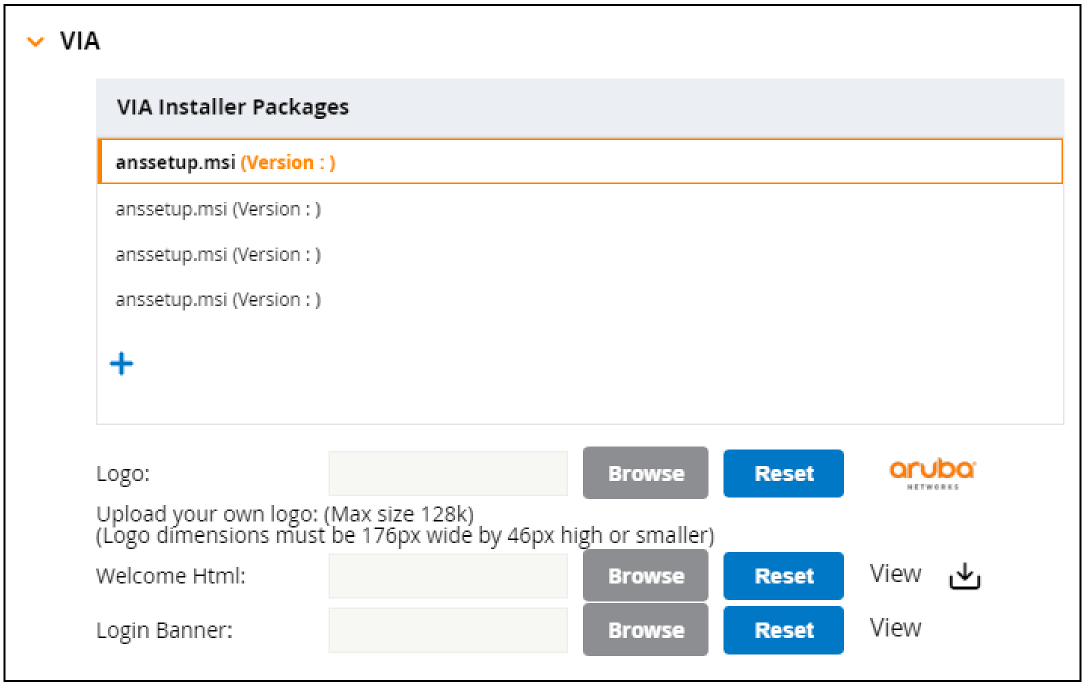
The installer file must be in the **.msi** format.

Downloading VIA Installer

To download the VIA installer:

1. On a standalone controller or in the **Managed Network** hierarchy on Mobility Master, navigate to **Configuration** > **Services** > **VPN**.
2. Select **VIA** to expand that section.
3. Select an **anssetup.msi** package from the **VIA Installer Packages** table to download the installation file.

Figure 77 *Downloading a VIA Installer*



VIA

VIA Installer Packages

anssetup.msi (Version :)

anssetup.msi (Version :)

anssetup.msi (Version :)

anssetup.msi (Version :)

Logo:

Upload your own logo: (Max size 128k)
(Logo dimensions must be 176px wide by 46px high or smaller)

Welcome Html:

Login Banner:

Additionally, you can download the VIA installer from the Aruba Support Site or the App store for mobile devices.

Configuring VIA using the CLI

The following steps describe how to configure VIA using the CLI.

NOTE

A Policy Enforcement Firewall Virtual Private Network (PEFV) license key must be installed.

NOTE

This section only describes commands that achieve specific tasks. For detailed information on the VIA command line options, see the latest *ArubaOS 8.x.x.x CLI Reference Guide*.

Enabling VPN Server Modules

You can only add licenses to a managed device via the Mobility Master configuration node.

```
(host) [mm] (config) #license add <PEFV_license_key>
```

Creating VIA Roles

```
(host) [md] (config) #user-role example-via-role
(host) [md] (config-role) #access-list session "allowall" position 1
(host) [md] (config-role) #access-list session "v6-allowall" position 2
```

Creating VIA Authentication Profiles

```
(host) [md] (config) #aaa server-group "via-server-group"
(host) [md] (Server Group "via-server-group") #auth-server "Internal" position 1

(host) [md] (config) #aaa authentication via auth-profile default
(host) [md] (VIA Authentication Profile "default") #default-role example-via-role
(host) [md] (VIA Authentication Profile "default") #desc "Default VIA Authentication Profile"
(host) [md] (VIA Authentication Profile "default") #server-group "via-server-group"
(host) [md] (VIA Authentication Profile "default") #client-cert-enable
```

If client certificate-based authentication is enabled on the VIA authentication profile and you do not want to use the default port 8085 for profile downloads, execute the following command to configure the port for certificate-based authentication:

```
(host) [md] (config) #web-server profile via-client-cert-port <via-client-cert-port>
```

NOTE

The valid range for the port number used for VIA client-cert based profile downloads is <1025-65535>, and the default value is 8085. The port configured for VIA client certificate-based authentication must also be configured on the control plane firewall using the **firewall cp** command. If the port is not configured on the control plane firewall, all packets sent to the port will be dropped, and the HTTPS connection will not be established.

Creating VIA Connection Profiles

```
(host) [md] (config) #aaa authentication via connection-profile "via"
(host) [md] (VIA Connection Profile "via") #server addr 192.1.30.100 internal-ip 192.1.30.09
desc "VIA Primary Controller" position 0
(host) [md] (VIA Connection Profile "via") #auth-profile "default" position 0
(host) [md] (VIA Connection Profile "via") #tunnel address 192.1.1.45 netmask 255.255.255.0
(host) [md] (VIA Connection Profile "via") #split-tunneling
(host) [md] (VIA Connection Profile "via") #windows-credentials
(host) [md] (VIA Connection Profile "via") #client-netmask 255.0.0.0
(host) [md] (VIA Connection Profile "via") #dns-suffix-list example.com
(host) [md] (VIA Connection Profile "via") #support-email via-support@example.com
(host) [md] (VIA Connection Profile "via") #certificate-criteria certificateIssuer="HPE Root
CA"; 2.5.4.10=SmartCard; emailAddress=support@example.com
```

To enable content security services (CSS), execute the following commands. CSS is only available if you have installed the content security services license. See the *Aruba Mobility Master Licensing Guide* for more information on licenses.

```
(host) [md] (VIA Connection Profile "via") #enable-csec
(host) [md] (VIA Connection Profile "via") #csec-gateway-url https://css.example.com
(host) [md] (VIA Connection Profile "via") #csec-http-ports 8080,4343
```

Enter the following command after you create the client WLAN profile (see Configuring VIA Client WLAN Profiles on page 109 for more details):

```
(host) [md] (VIA Connection Profile "via") #client-wlan-profile "via_corporate_wpa2" position
0
```

Configuring VIA Web Authentication

```
(host) [md] (config) #aaa authentication via web-auth default
(host) [md] (VIA Web Authentication "default") #auth-profile default position 1
```

NOTE

You can have only one profile (`default`) for VIA web authentication.

Associating VIA Connection Profiles to User Roles

```
(host) [md] (config) #user-role "example-via-role"
(host) [md] (config-role) #via "via"
```

Configuring VIA Client WLAN Profiles

```
(host) [md] (config) #wlan ssid-profile "via_corporate_wpa2"
(host) [md] (SSID Profile "via_corporate_wpa2") #essid corporate_wpa2
(host) [md] (SSID Profile "via_corporate_wpa2") #opmode wpa2-aes

(host) [md] (config) #wlan client-wlan-profile "via_corporate_wpa2"
(host) [md] (VIA Client WLAN Profile "via_corporate_wpa2") #ssid-profile "via_corporate_ssid"
```

For detailed configuration parameter information, see the **wlan client-wlan-profile** command in the latest *ArubaOS 8.x.x.x CLI Reference Guide*.

Rebranding VIA and Uploading VIA Installers

Rebranding VIA and uploading the installer can only be performed using the WebUI. See Rebranding VIA on page 113 and Uploading VIA Installers on page 114.

Chapter 10
Troubleshooting VIA

This section provides information to help you troubleshoot the issues you may encounter when installing, connecting, and using VIA.

- Troubleshooting VIA on Linux
- Troubleshooting VIA on Windows

Troubleshooting VIA on Linux

The following table shows the steps to troubleshoot VIA on Linux.

Table 18: *Linux VIA Troubleshooting Steps*

Action	Issue	Troubleshooting Steps
Installation	Unable to install	1. Ensure that you are using a supported Operating System. 2. Ensure that the system is up-to-date by running the following commands: — RHELor CentOS: **yum update** — Ubuntu: **sudo apt-get update** and **sudo apt-get upgrade** 3. Ensure that all dependency packages are installed before installing VIA. 4. Ensure that you are using the correct installation file for Linux. 5. If the installer fails to install correctly, use the platform installer **.deb** or **.rpm** 6. If installation fails due to upgrade, remove the previous version of VIA before installing a newer version.
	Unable to locate VIA for uninstalling	Run the following command to remove VIA: • RHELor CentOS: **su -c yum remove via** • Ubuntu: **sudo apt-get purge via**
Profile Download	Unable to download VIA profile	1. Ensure that profile network connectivity to the VIA controller is available. 2. Ensure that the profile can be downloaded from a browser with the link: **https://<controller IP or hostname>/via**. 3. Remove browser plug-ins or change to the correct proxy settings to enable downloading VIA from the browser.

Action	Issue	Troubleshooting Steps
Connect VIA	Unable to establish VPN connection	1. Check if VIA works on other platforms (Windows, MacOS, Android, or iOS) for the same controller. 2. Check if the authentication method used to connect VIA is supported in VIA Linux Edition. For more information, refer to VIA Client for Linux.
	VIA does not connect automatically when a network interface is up	1. Ensure that VIA is managed by the Network Manager. To check this, ensure that the active network interface device ID is not listed in the **/etc/network/interfaces** file. 2. Ensure that network access to port 443 is allowed on internal and external IP addresses of the controller.
	VIA does not initiate automatically on system start	This is observed when VIA is installed when logging in as a different user. Ensure that VIA is installed on the same user account as VIA.
Certificate Storage	Trouble using or importing certificates	1. Import the certificate into the VIA Certificate store, and import the corresponding CA certificate. 2. If the Enterprise has a CA server that can issue certificates for users, use the **Request User certificate** option.
Detect Network Events	VIA is unable to detect the network events	The Network Manager may not be in use for managing network interfaces.
	Checking if an interface is being managed by the Network Manager or not	Ensure that the file **/etc/network/interfaces** does not have any references to the interfaces on which you attempt to connect the VIA application.
Send Logs	Sending logs when the system does not have a mail account configured	Click **Send Logs** to create a **via_logs_<date>_<time>.tar.gz** file in the **/usr/share/via/logs** folder. Send this file using your email.

Troubleshooting VIA on Windows

To help your support team effectively resolve your VIA connection issues, it is mandatory that you send logs generated by VIA. To do this, click the **Send Logs** button from the **Log** tab.

Table 19: *Windows VIA Troubleshooting Steps*

Action	Issue	Troubleshooting Steps
Installation	Unable to install	1. Ensure that you are using the correct installation file for Windows. 2. Generate an installation log by running **msiexec.exe ansetup.msi /l*v log.txt** from an administrator command prompt. The file **log.txt** captures the installation errors if any. 3. If installation due to upgrade fails, remove the previous version of VIA before installing a newer version.
	Unable to locate VIA application for uninstalling	1. Open **Control Panel** > **Add/remove program** or **Programs and Features** 2. Select **Virtual Intranet Access**, and then click **Uninstall**. Alternatively, issue the **msiexe.exe /x ansetup.msi** command to uninstall from an administrator command prompt.
Profile Download	Unable to download profile	1. Ensure that profile network connectivity to the VIA controller is available. 2. Ensure that the profile can be downloaded from a browser with the link: **https://<controller IP or hostname>/via**. 3. Remove browser plug-ins or change to the correct proxy settings to enable downloading VIA from the browser.
Connect VIA	Unable to establish VPN connection	1. Ensure that the correct VIA client is installed. 2. Check if VIA works on other platforms (Linux, MacOS, Android, or iOS) for the same controller. 3. If you used Captive Portal to download a VIA profile or connect to the VPN, ensure that Internet connectivity through the browser is working correctly. 4. Check if the authentication method used to connect VIA is supported in VIA Windows Edition. For more information, refer to VIA Client for Microsoft Windows.

Action	Issue	Troubleshooting Steps
	VIA does not connect automatically when a network interface is up	Ensure that network access to port 443 is allowed on the internal and external IP addresses of the controller.
	VIA does not initiate automatically on system start	This is observed when VIA is installed by logging in as a different user. Ensure that VIA is installed on the same user account as VIA.
Send Logs	Sending logs when the system does not have a mail account configured	Click the **Send Logs** button to create a **via_logs_<date>_<time>.tar.gz** file in the **%programdata%\Aruba networks\VIA** folder. Send this file using your email.

Appendix A
VIA for Linux CLI

This section is designed for an administrator. Some of these commands have reduced user interaction with one or more command line parameters supplying the required parameters.

IPsec

VIA Help

Execute the following commands to get help on VIA CLI commands.

```
via-cli-help

via-cli -h
```

Start VIA Session

Execute the following commands to run VIA session.

```
via-cli session start

via-cli session start -keypass <Password>

via-cli session start -keypass <keyring password> --force
```

NOTE

Only one VIA client instance either CLI or GUI can be ran at the same time.

The force parameter restarts VIA CLI session and interrupts a session is started by VIA Daemon in a machine connection mode

```
via-cli session --force
```

Stop VIA Session

Execute the following commands to stop a VIA session that is in progress.

```
via-cli stop

via-cli session stop --force
```

Display Session Info

Execute the following command to view the VIA session details that is in progress.

```
via-cli session info
```

Get Authentication Profile List

Execute the following download connection profile command without authentication profile name, if an authentication profile name is unknown.

```
via-cli profile load \
--gateway 119.82.100.27 \
--username internal04 \
--userpass aruba123
```

Or

```
via-cli -u <username> -p <Password> profile load

-proxy <proxy settings> <gatewayip>

--nocertwarn
```

2 auth. profiles available:

```
#1 : AU0101IKEv1PSK [AU0101IKEv1PSK].

#2 : AU0102IKEv1RSA [AU0102IKEv1RSA].
```

Download a Connection Profile

Execute the following commands and specify the name of the authentication profile or the corresponding number, to download the authentication profile.

```
via-cli profile load \

--gateway 119.82.100.27 \

--username internal04 \

--userpass aruba123 \

--authprofile AU0101IKEv1PSK \
```

OR

```
via-cli-nocertwarn profile load \

--gateway 119.82.100.27 \

--username internal04 \

--userpass aruba123 \

--authprofile AU0101IKEv1PSK \
```

OR

```
via-cli-nocertwarn profile load \

--gateway 119.82.100.27 \

--username internal04 \

--userpass aruba123 \

--authprofile-index 1 \
```

NOTE

The ‘nocertwarn’ parameter enables the VIA CLI to ignore the VIA Web HTTPS error.

Print Profile

Execute the following command to print the downloaded authentication profile details.

```
via-cli profile print
```

Clear Profile

Execute the following command to erase the downloaded profile.

```
via-cli profile clear
```

List Certificates

Execute the following command to list the certificates available in the store

```
via-cli cert list
```

```
via-cli cert list --client
```

```
via-cli cert list --CA
```

Remove Certificates

Execute the following command to erase the certificates from the store.

```
via-cli cert remove <alias>
```

Archive logs

Execute the following command to archive logs.

```
via-cli logs archive
```

Send Logs

Execute the following command to send the archived logs.

```
via-cli logs send
```

```
via-cli logs send --directory <pathtosavelogs>
```

Version

Execute the following command to check the CLI version.

```
via-cli -v
```

Establish VPN Connection with PSK

Execute the following command to establish a VPN connection with PSK.

```
via-cli vpn connect
```

NOTE

After successful profile downloading VIA starts VPN connection automatically if the Client AutoLogin parameter is set in a connection profile.

Terminate VPN Tunnel

```
via-cli vpn disconnect
```

Clear Profile

```
via-cli profile clear
```

Certificate Operations

Import User Certificate

Execute the following command to import the user certificates to the VIA store.

```
via-cli cert import \
--user

--keypass <keyring password> \

--certpass <certificate password><filepath/name> \

Certificate '/home/user01/internal05.p12' was successfully imported.

Alias: 836e85d5069f7620108fcb83ca37020999ddded1b90b399f71f1a2563f74b716

Subject: internal05

Issuer: ARB Internal A

StartDate: '121201115800Z'

EndDate: '131201115800Z'

Type: client

Algorithm: RSA

Hash: 5
```

OR

```
via-cli--user \

--keypass <keyring password> \

--cert import <filepath/name><certificate password> \
```

Import CA Certificate from File

Execute the following command to import the CA certificates to VIA store

```
via-clicert import --user --keypass <PW> --CA <filepath/name>
```

Establish VPN Connection with Certificate

Execute the following command to establish a VPN connection with certificate.

```
via-cli vpn connect --username <name> --userpass<PW> --keypass<PW> --cert <Alias>
via-cli vpn connect -u <name> -p<PW> --keypass<PW> --cert <Alias>
```

VPN Status

Execute the following command to print the status of the VPN connection.

```
via-cli vpn status
```

Appendix B
VIA for Windows CLI

This section is designed for an administrator. Some of these commands have reduced user interaction, with one or more command line parameters supplying the required parameters. There are also standard command line options from **msiexec,** like **/q**, that can be used.

The installer command line options are used with either the **msiexec.exe** program or by using the complete path of the msi file as follows:

- **msiexec.exe /I < installation msi> <OPTION>=<VALUE> [<OPTION>=<VALUE>]**

  or
- **<installation msi> <OPTION=<VALUE> [<OPTION>=<VALUE>]**

Multiple command line options can be used by appending the OPTION,VALUE pairs such as:

- **msiexec /I c:\temp\ansetup.msi INSTALLDESKTOPSHORTCUT=0**
- **C:\temp\ansetup.msi INSTALLDESKTOPSHORTCUT=0**
- **Ansetup.msi CUSTOMFOLDER="Aruba Networks" CUSTOMNAME="Aruba VIA"**

Install Desktop Shortcut

To create a desktop shortcut for VIA, set the installation parameter to 1. The shortcut is created under **ALLUSERS\Desktop**. The parameter can take values 0 and 1, with a default value of 1. Setting the value to 0, as shown in the following example, does not install the desktop shortcut for VIA.

"msiexec /I c:\temp\ansetup.msi INSTALLDESKTOPSHORTCUT=0"

Install Location

The default installation location is set to **%ProgramFiles%\Aruba Networks\Virtual Internet Agent** (for Aruba OEM). The default location can be configured using this parameter. For example, **msiexec /I c:\temp\ansetup.msi INSTALLLOCATION="D:\Programs\Aruba Networks\VIA** installs the program in the **D:\Programs\Aruba Networks\VIA** folder.

Custom Folder

This parameter allows you to create a customized folder to install the shortcut for VIA. By default, the folder is Aruba Networks. To change the default folder location, execute the following command: **msiexec /I c:\temp\ansetup.msi CUSTOMFOLDER="Aruba Tools".** In this example, the default location for the VIA shortcut is changed to Aruba Tools and is nested under **Start menu > Programs**.

Custom Name

This parameter allows you to create a customized application name under **Start Menu > Programs**. By default, the application name is **Virtual Intranet Access**. The customized name is also used when creating a desktop shortcut. The following command creates an application shortcut and file name: **msiexec /I c:\temp\ansetup.msi CUSTOMNAME="VIA".**

Custom Start

This parameter customizes the functionality of launching the VIA application upon installation. You can assign values of 0 and 1. The default value is 1, which indicates that the application launches automatically after installation. Setting the value to 1 does not auto-start the VIA application on system startup. See Autostart on page 127 for more information.

The following command prevents VIA from starting automatically after an install: **ansetup.msi CUSTOMSTART=0.**

Gateway

This parameter provides a gateway for the VIA application during the initial connection. This command updates the **Remote Server** field of the VIA login dialog box. The default value is an empty string. The following example updates the **Remote Server** field to 10.17.96.140: **msiexec /I c:\temp\ansetup.msi GATEWAY=10.17.96.140.**

Authprofile

The **Authprofile** parameter provides the authentication profile value for VIA as part of the login process. If the user configuration has multiple authentication profiles, then a profile selection window is displayed. When this command is executed and the required details are supplied, the profile selection window is not displayed to the user. The default value is an empty string. The following example automatically sets the authentication profile to **viauser** without prompting the user to select a profile: **msiexec /I c:\temp\ansetup.msi AUTHPROFILE=viauser.**

Getconfig+User+Password

If the **Getconfig** value is set to 1, installation instructs the VIA application to retrieve the initial configuration automatically. The login dialog box is not displayed if the **Getconfig** parameter is set for the installer. The default value for this option is 0.

The **User** and **Password** parameters must be set in order to fetch the initial configuration automatically. Each of these parameters is a string value, and the default value is an empty string. The values of **User** and **Password** are encrypted before they are passed on to the VIA application from the installer. The **Password** is masked from all installation logs.

The following command automatically downloads the default profile from server 10.17.96.140 using the given credentials: **ansetup.msi /qb GATEWAY=10.17.96.140 AUTHPROFILE=default GETCONFIG=1 USER=nag PASSWORD=password**

Nocertwarn

The VIA application may display certificate errors while downloading the configuration from the server. The application displays a standard https certificate warning window, and the user can either cancel the operation or continue with errors. If the **Nocertwarn** parameter is set to 1, the installer instructs the VIA application to ignore any server certificate errors for initial and subsequent configuration downloads.

The following command automatically establishes a VIA session with 10.17.96.140 using the default profile with the given set of credentials: **msiexec.exe /i c:\test\en-us\ansetup.msi /qb GATEWAY=10.17.96.140 AUTHPROFILE=default GETCONFIG=1 USER=nag PASSWORD=password NOCERTWARN=1**

Autostart

This parameter creates an autostart shortcut to allow the VIA application to start at system boot. This shortcut is created for all system users. The value for a specific user can be changed at a later point if the connection profile for the user does not have **Client Auto-Login** checked. This parameter can be assigned values 0 and 1. The default value is 0. The following example enables VIA to start automatically for all system users: **msiexec /I c:\temp\ansetup.msi AUTOSTART=1**

This section describes the various multi-factor authentication (MFA) mechanisms supported by VIA. For more information on VIA authentication, see Authentication Methods Supported in VIA on page 89.

The following table displays the MFA methods:

Table 20: *Multi-Factor Authentication Mechanisms Supported by VIA*

Authentication Mechanism	Authentication Device	Windows	Linux	Android	iOS	MacOS
Virtual Digital Badge in TPM	TPM certificate	Yes	--	--	--	--
Security Token	RSA SecureID token	Yes	No	Yes	No	Yes
Mobile authentication	Duo	Yes	Yes	Yes	Yes	Yes
PKI - Smart Card (PIN-based)	Smart Card	Yes	Yes	No	No	No

Authentication using a Virtual Digital Badge

VIA supports authentication using a Virtual Digital Badge (VDB) certificate stored in the Trusted Platform Module (TPM) of a windows device.

Authentication using an RSA SecurID Token

RSA SecurID is a hardware and software-based authentication mechanism that generates unique authentication (token) codes at a specified interval using an RSA SecurID token. Security tokens can be used for IKEv1 XAUTH.

Prerequisites

- Access to an RSA SecurID server
- Access to an RSA SecurID device (token)
- User is enrolled and associated with the RSA SecurID token

NOTE

Each user is provided with a username configured on the RSA SecurID server.

NOTE

When enrolling with RSA SecurID, users must create a PIN to authenticate and connect VIA.

Configuring VIA with an RSA SecurID Token

To configure and connect VIA with security token authentication:

1. Map an authentication server to the RSA SecureID server:

    a. In the **Managed Network** node hierarchy of your Mobility Master, navigate to **Configuration > Authentication > L3 Authentication**.
    b. Expand **VIA Authentication** under the **L3 Authentication** list.
    c. Select the **Server Group** entry below a VIA authentication profile.
    d. Select the RSA SecureID server from the **Server Group** drop-down list.
    e. Click **Save.**
    f. Select **Pending Changes**.
    g. In the **Pending Changes** window, select the check box and click **Deploy changes**.

2. Run a AAA test to ensure RADIUS authentication is working:
    a. In the **Mobility Master** node hierarchy, navigate to **Diagnostics > AAA Test Server Test**.
    b. Select the RADIUS server from the **Server Name** drop-down list.
    c. Set the **Authentication method** to **PAP**.
    d. Enter your username and password.
    e. Click **Begin Test**.
3. Open VIA and download the VPN connection profile:
    a. Select **Click to download VPN profile** from the home screen. The **Download VPN Profile** screen appears.
    b. Enter the server URL and your login credentials. Under **Username**, enter the username configured on the RSA server. Under **Password**, enter your PIN followed by the unique token code displayed on the RSA token (no spaces).
    c. Click **Download**.
    d. In the **Web Authentication Profile** list, select the authentication profile for which you have assigned the RSA SecureID server as the authentication server.
4. Connect VIA by clicking the VPN connection status ring on the VIA home screen. When prompted, enter your username and password:
    a. Under **Username**, enter the username configured on the RSA server.
    b. Under **Password**, enter your PIN followed by the unique token code displayed on the RSA token (no spaces).
    c. Click **Proceed**.

> NOTE
>
> The token code used to download the profile should not be the same code used to connect VIA. Since a new token code is generated during each specified interval, allow the token code to change on the RSA SecureID device before entering the code to connect VIA.

The VIA connection is established.

Authentication using Duo

Authentication on mobile devices is supported by an application called Duo. Mobile device authentication can be used for IKEv1 XAUTH and IKEv2 EAP-MSCHAPv2.

Prerequisites

- Users are enrolled and registered with Duo
- Duo application is installed on a device with the same mobile number that the user has registered

Configuring VIA using Duo

To configure and connect VIA with mobile device authentication:

1. Install the authentication proxy and connect it to **AD(ike-v1-pap)/NPS(ike-v1-pap & ike-v2-eap-mschapv2) (https://duo.com/docs/radius)**. For example, if the proxy is **10.17.12.53**, and the port is **2000**, the sample file in **C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy file**, is as follows:

```
[ad_client]
host=10.17.12.53
service_account_username=Administrator
service_account_password=Aruba&123
search_dn=DC=patilqa,DC=com

[radius_server_auto]
ikey=DI45H91IZH4BE1J1HUOK
skey=WoqOi61AkCHo6W07p5tIyEy66lxYNtCz6oA5Eqgb
api_host=api-515e66d1.duosecurity.com
radius_ip_1=10.17.14.3
radius_secret_1=aruba123
client=ad_client
port=2000
```

2. Configure the RADIUS server that is used as the proxy (as shown in step 1 on page 130), and set it as the authentication server for the profile that is being used:
   a. In the **Managed Network** node hierarchy of your Mobility Master, navigate to **Configuration > Authentication > L3 Authentication**.
   b. Expand **VIA Authentication** under the **L3 Authentication** list.
   c. Select the **Server Group** entry below the VIA authentication profile.
   d. Select the RADIUS server that is being used as the proxy from the **Server Group** drop-down list.
   e. Click **Save.**
   f. Select **Pending Changes**.
   g. In the **Pending Changes** window, select the check box and click **Deploy changes**.
3. Run a AAA test to ensure RADIUS authentication is working:
   a. In the **Mobility Master** node hierarchy, navigate to **Diagnostics > AAA Test Server Test**.
   b. Select the RADIUS server from the **Server Name** drop-down list.
   c. Select an authentication method.
   d. Enter your username and password.
   e. Click **Begin Test**.
4. Open VIA and download the VPN connection profile:
   a. Select **Click to download VPN profile** from the home screen. The **Download VPN Profile** screen appears.
   b. Enter the server URL and your login credentials.
   c. Click **Download**.
   d. In the **Web Authentication Profile** list, select the authentication profile for which you set the authentication server as the Duo proxy. A **Login Request** message is sent to the Duo application on your mobile device.
   e. Open the message, and then click **Approve**.
5. Connect VIA by clicking the VPN connection status ring on the VIA home screen. If XAUTH is enabled, enter your username and password when prompted.

The VIA connection is established.

Authentication using a Smart Card

Smart cards provide two-factor authentication for IKEv1 Cert, IKEv2 Cert, and IKEv2 EAP-TLS using a certificate and PIN number. Smart cards support a Smart Card Cryptographic Provider (SCCP for Windows or OpenSC for Linux) API in the operating system that causes the certificate embedded within the smart card to appear in the operating system's certificate store automatically.

Smart card devices include:

- Smart card
- USB Token
- Virtual SC
- TPM Certificate

Windows

To configure and use VIA for smart card authentication in Windows devices:

1. Install the software drivers related to the smart card.
2. VIA does not support certificate import to the smart card. Use the smart card utility to install certificates on the smart card.
3. Open VIA and download a certificate-based VPN connection profile.
4. Click the VPN connection status ring on the VIA home screen to connect VIA. The **Select a Certificate** screen appears.
5. Select a certificate from the list.
6. Click **Proceed**.
7. Enter your username and PIN number when prompted.
    a. Under **Username**, enter the username configured on the smart card.
    b. Under **Pin**, enter the smart card PIN number.

The VIA connection is established.

NOTE

If the **Allow user to save passwords** setting is enabled on the VIA connection profile, users are not required to enter the PIN number during subsequent connections.

Linux

To configure and use VIA for smart card authentication in Linux devices:

1. Install the software drivers related to the smart card.
2. VIA does not support certificate import to the smart card. Use the smart card utility to install certificates on the smart card.
3. Issue the following commands:

```
<cryptoki_lib_path>:
#cat /usr/share/via/via_config.xml
<via_config_profile>
...
<cryptoki_lib_path>/usr/lib/ libeTPkcs11.so</cryptoki_lib_path>
...
</via_config_profile>
```

4. Open VIA and download a certificate-based VPN connection profile.
5. To select the certificate from your VIA application:
    a. Plug the card reader into your PC.

b. Click the VPN connection status ring on the VIA home screen to connect VIA.

c. Navigate to the **VIA Cert Store** tab.

d. Select **Storage** as token-1. The list of available certificates appears.

e. Select the certificate, and then click **OK**.

6. Enter the smart card PIN number when prompted to **Enter the Storage Pin**.

The VIA connection is established.

NOTE

If the **Allow user to save passwords** setting is enabled on the VIA connection profile, users are not required to enter the PIN number during subsequent connections.