Dell PowerConnect W-VIA 2.0

User Guide

Open Source Code

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

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Contents

Tables

Figures

Virtual Intranet Access (VIA) is part of the Dell remote networks solution targeted for teleworkers and mobile users. VIA detects the user's network environment (trusted and un-trusted) and automatically connects the user to their enterprise network. Trusted networks typically refers to a protected office networks that allows users to directly access corporate intranet. Un-trusted networks are public Wi-Fi hotspots like airports, cafes, or home network. The VIA solution comes in two parts—VIA connection manager and the controller configuration.

- VIA connection manager—Teleworkers and mobile users can easily install a light weight application on their Microsoft Windows computers to connect to their enterprise network from remote locations (see "VIA Connection Manager" on page 9).
- Controller configuration—To set up virtual intranet access for remote users, you must configure your controller to include setting up user roles, authentication, and connection profiles. You can use either WebUI or CLI to configure your controller (see "VIA Configuration" on page 13).

Topics in this Document

VIA Connection Manager

If a user is connected from a remote location that is outside of the enterprise network, VIA automatically detects the environment as un-trusted and creates a secure IPSec connection between the user and the enterprise network. When the user moves into the trusted network, VIA detects the network type and moves to idle state.

How it Works

VIA provides a seamless connectivity experience to users when accessing an enterprise network resource from an un-trusted or trusted network environment. You can securely connect to your enterprise network from an un-trusted network environment. By default VIA will auto-launch at system start and establish a remote connection. The following table explains the typical behavior:

NOTE: The sequence of events described in Table 1 may not necessarily occur in the order shown in the table.

Table 1 *VIA Connectivity Behavior*

	User action/environment	VIA's behavior
1	The client moves from a trusted to un-trusted environment. *Example: From office to a public hot-spot.*	Auto-launches and establishes connection to remote network.
2	The client moves from an un-trusted to a trusted environment.	Auto-launch and stay idle. VIA does not establish remote connection. You can, however, manually connect to a network by selecting an appropriate connection profile from the Settings tab.

Table 1 *VIA Connectivity Behavior*

	User action/environment	VIA's behavior
3	While in an un-trusted environment, user disconnects the remote connection.	Disconnects gracefully.
4	The client moves to a trusted environment.	Stays idle and does not connect.
5	The client again moves to an un-trusted environment	Stays idle and does not connect. This usually happens, if the user has in a previous occasion disconnected a secure connection by clicking the Disconnect button in VIA (*See Step 3*). Users can manually connect using one of the following methods: Right click on the VIA icon in the system tray and select the Restore option and then select the Connect option to connect using the default connection profile. Right click on the VIA icon in the system tray and select the Connect option.
6	User clicks the Reconnect button.	Establishes remote connection.
7	In an un-trusted environment, user restarts the system.	Auto-launches and establishes remote connection.
8	In an un-trusted environment, user shuts down the system. Moves to a trusted environment and restarts system.	Auto-launches and stays idle.

Compatibility Matrix

The following table shows the compatibility of different versions of VIA with Dell PowerConnect W-ArubaOS:

Table 2 *VIA Compatibility Matrix*

Dell PowerConnect W-ArubaOS Versions	Operating Systems	
	Microsoft Windows (32-bit) [XP, Vista, Windows 7]	Microsoft Windows (64-bit) [Vista, Windows 7]
Dell PowerConnect W-ArubaOS 6.1.x	2.0	2.0

Installing the VIA Connection Manager

Users can download VIA from a URL provided to them by their IT department and install it on their computers. Alternatively, administrators can choose to push the installation using a system management software.

NOTE: VIA 2.0 connection manager can be installed only on machines running Microsoft Windows. For list of supported versions, Chapter 2, "End User Instructions" on page 25.

1. Download the installer from the URL provided by the IT department.
2. Double click the installer file and follow the default prompts.
3. After the installation is complete, the user will be prompted to enter the following:
   a. Remote server URL—This should be provided by your IT department. The administrator can also provision the URL on the controller. In such cases, the user is required to specify only the username and password.
   b. Username—The user's domain user name.
   c. Password—The user's domain password.

4. Click the **Connect** button to initiate a secure VIA connection. VIA will minimize to system tray after a secure connection is established.

Upgrade Workflow

VIA checks for upgrade requirements during the login phase. There are two types of upgrade process: Minimal Upgrade and Complete Upgrade.

Minimal Upgrade

This type of upgrade is initiated for bug fixes and some minor enhancements which requires only some components of the client to be upgraded. When a VPN session is active the upgrade binary is downloaded by VIA from the controller. After the active VIA connection is terminated, the upgrade process is started and the client is upgraded. This type of upgrade does not require a system reboot.

Complete Upgrade

This requires an upgrade to VIA and its underlying network drivers. This type of upgrade requires a system reboot. VIA downloads the upgrade binary from the controller and displays a message about upgrade process after the connection is terminated for that upgrade. The user can choose to proceed or cancel the upgrade process. If the user chooses to upgrade, a system reboot is automatically executed. If the user cancels the upgrade, VIA will prompt the user for an upgrade every time the user terminates a VIA session..

NOTE: See Chapter 2, “End User Instructions” on page 25 for information about using the desktop application.

Contacting Support

Table 4 *Web site contact*

Web Site	
Main Website	dell.com
Support Website	support.dell.com
Documentation Website	support.dell.com/manuals

Chapter 1

VIA Configuration

VIA configuration requires that you first configure VPN settings and then configure VIA settings. See the *Virtual Private Networks* chapter in the latest *Dell PowerConnect W-ArubaOS User Guide* for information on configuring VPN settings on your controller.

Before you Begin

The following ports must be enabled before configuring the VIA controller.

- **TCP 443**—During the initializing phase, VIA uses HTTPS connections to perform trusted network and captive portal checks against the controller. It is mandatory that you enable port 443 on your network to allow VIA to perform these checks.
- **UDP 4500**—Required for IPSec transport

Authentication Mechanisms Supported in VIA 2.x

VIA 2.x supports IKEv2 which is an updated version that is faster and supports a wider variety of authentication mechanisms. IKEv2 has only single phase authentication process. VIA supports the following IKEv2 authentication methods:

- Username and password
- X.509 certificate. Controllers running Dell PowerConnect W-ArubaOS 6.1 or greater support OCSP for the purpose of validating a certificate that has not been revoked.
- EAP (Extensible Authentication Protocol) including EAP-TLS and EAP-MSCHAPv2.
- Certificates based authentication.
- Smart cards that support a Smart Card Cryptographic Provider (SCCP) API within the operating system. VIA will look for an X.509 certificate in the operating system's certificate store. A smart card supporting SCCP will cause the certificate embedded within the smart card to automatically appear in the operating system's certificate store.

Configuring VIA Settings

The following steps are required to configure your controller for VIA. These steps are described in detail in the subsections that follow.

1. Enable VPN Server Module—Dell PowerConnect W-ArubaOS allows you to connect to the VIA controller using the default user roles. However, to configure and assign specific user roles you must install the Policy Enforcement Firewall Virtual Private Network (PEFV) license.
2. Create VIA User Roles—VIA user roles contain access control policies for users connecting to your network using VIA. You can configure different VIA roles or use the default VIA role—`default-via-role`
3. Create VIA Authentication Profile—A VIA authentication profile contains a server group 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 with *Internal* server group.
4. Create VIA Connection Profile— A VIA connection profile contains settings required by VIA to establish a secure connection to the controller. You can configure multiple VIA connection profiles. A VIA connection

profile is always associated to a user role and all users belonging to that role will use the configured settings. If you do not assign a VIA connection profile to a user role, the default connection profile is used.

5. Configure VIA Web Authentication—A VIA web authentication profile contains 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*) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile (step 3 on page 13) is configured, users can view this list and select one during the client login.
6. Associate VIA Connection Profile to User Role—A VIA connection profile has to be associated to a user role. Users will login by authenticating against the server group specified in the VIA authentication profile and are put into that user role. The VIA configuration settings are derived from the VIA connection profile attached to that user role. The default VIA connection profile is used.
7. Configure 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 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 Step 6.
8. Rebranding VIA and Uploading VIA Installers—You can use a custom logo on the VIA client and on the VIA download web page.

Using WebUI to Configure VIA

The following steps illustrate configuring your controller for VIA using the WebUI.

Enable VPN Server Module

You must install the PEFV license to configure and assign user roles. See the *Software Licenses* chapter in the latest *Dell PowerConnect W-ArubaOS 6.1 User Guide* for more information on licenses.

To install a license:

1. Navigate to **Configuration > Network > Controller** and select the **Licenses** tab on the right hand side.
2. Paste the license key in the **Add New License key** text box and click the **Add** button.

Create VIA User Roles

To create VIA users roles:

1. Navigate to **Configuration > Security > Access Control > User Roles**.
2. Click **Add** to create new policies. Click **Done** after creating the user role and apply to save it to the configuration.

Create VIA Authentication Profile

This following steps illustrate the procedure to create an authentication profile to authenticate users against a server group.

1. Navigate to **Configuration > Security > Authentication > L3 Authentication**.
2. Under the *Profiles* section, expand the VIA **Authentication Profile** option. You can configure the following parameters for the authentication profile:

Table 5 *Authentication Profile Parameters*

Parameter	Description
Default Role	The role that will be assigned to the authenticated users.
Max Authentication Failures	Specifies the maximum authentication failures allowed. The default is 0 (zero).

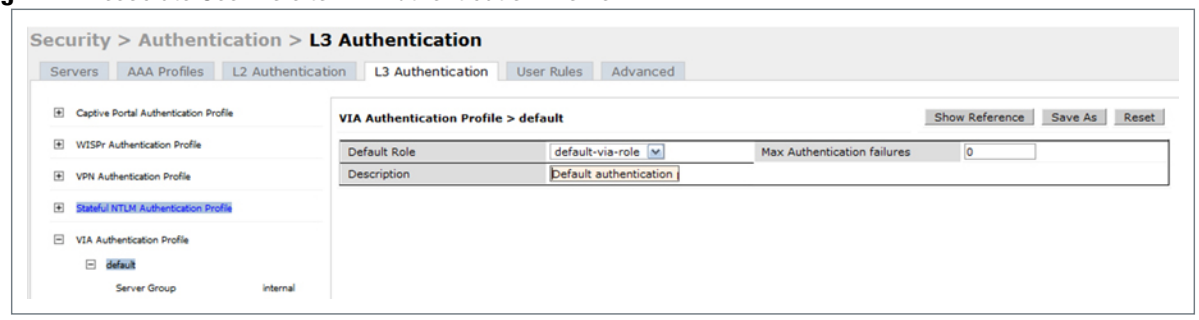
Table 5 *Authentication Profile Parameters*

Parameter	Description
Description	A user friendly name or description for the authentication profile.

3. To create a new authentication profile:
   a. Enter a name for the new authentication profile under the VIA *Authentication Profiles* section and click the **Add** button.
   b. Expand the VIA **Authentication Profiles** option and select the new profile name.
4. To modify an authentication profile, select the profile name to configure the default role

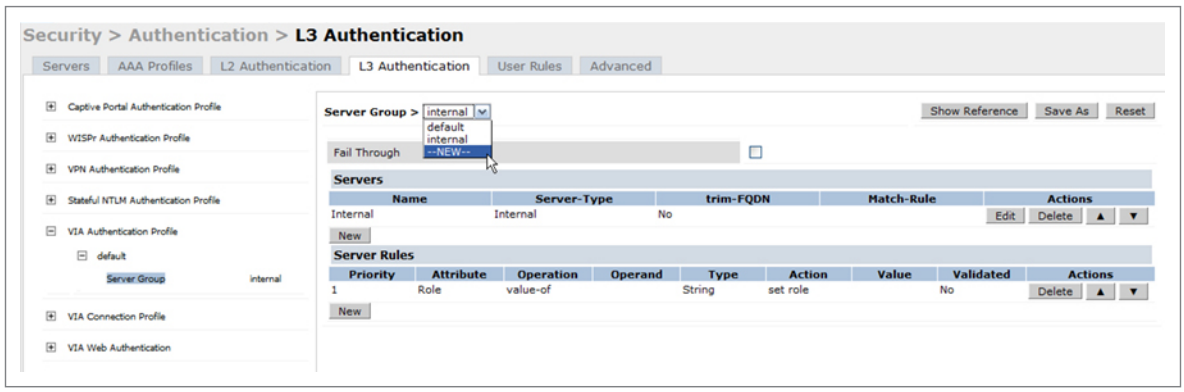
   The following screenshot uses the default authentication profile.

Figure 1 *Associate User Role to VIA Authentication Profile*



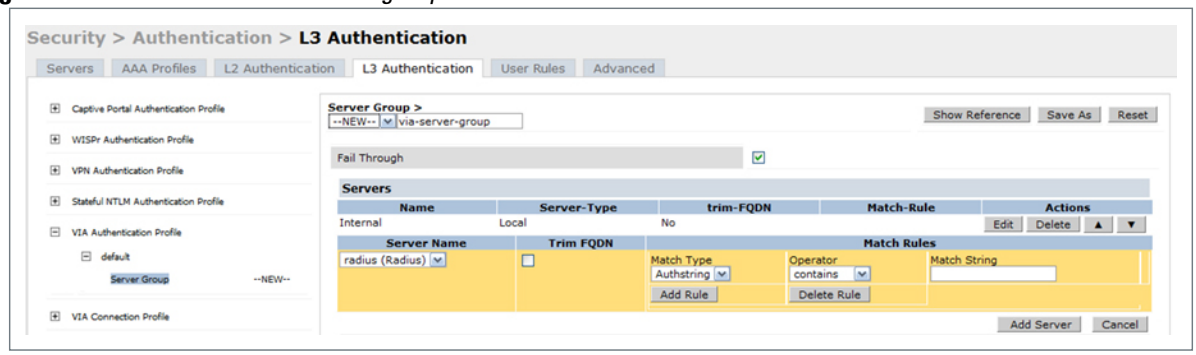
5. To use a different server group, Click *Server Group* under VIA Authentication Profile and select **New** to create a new server group.

Figure 2 *Creating a new server group for VIA authentication profile*



6. Enter a name for the server group.

Figure 3 *Enter a name for the server group*

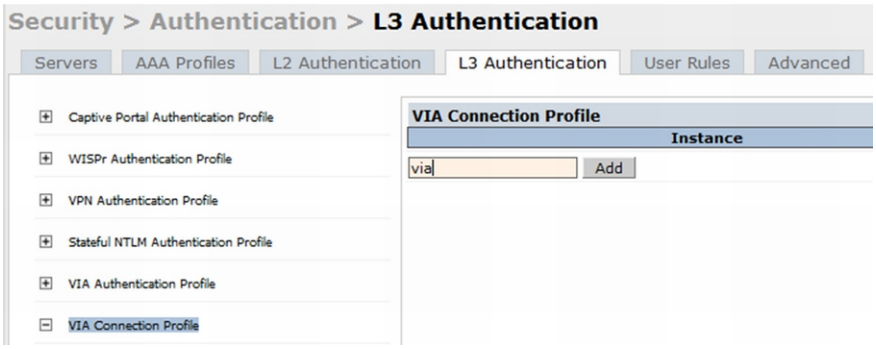


Create VIA Connection Profile

To create VIA connection profile:

1. Navigate to **Configuration > Security > Authentication > L3 Authentication** tab. Click the VIA *Connection Profile* option and enter a name for the connection profile.

Figure 4 *Create VIA Connection Profile*



2. Click on the new VIA connection profile to configure the connection settings. You can configure the following options for a VIA connection profile.

Table 6 *Connection Profile Options*

Configuration Option	Description
VIA Controller	Enter the following information about the VIA 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 belonging 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 VIA controller you re-order them by clicking the *Up* and *Down* arrows. To delete a controller from your list, select a controller and click the Delete button.
VIA Authentication Profiles to provision	This is the list of VIA authentication profiles that will be displayed to users in the VIA client. See "Create VIA Authentication Profile" on page 14. • Select an authentication profile and click the Add button to add to the authentication profiles list. • You can change the order of the list by clicking the *Up* and *Down* arrows. • To delete an authentication profile, select a profile name and click the Delete button.

Table 6 *Connection Profile Options*

Configuration Option	Description
VIA tunneled networks	A list of network destination (IP address and netmask) 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. Click the Add button to add them to the tunneled networks list. • To delete a network entry, select the IP address and click the Delete button.
VIA Client WLAN profiles	A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks. • Select a WLAN profile and click the Add button to add to the client WLAN profiles list. • To delete an entry, select the profile name and click the Delete button. See "Configure VIA Client WLAN Profiles" on page 19 for more information.
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.
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.
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 `crypto-local ipsec-map <ipsec-map-name>` command.
VIA Client Network Mask	The network mask that has to be set on the client after the VPN connection is established. Default: 255.255.255.255
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.
VIA Support E-mail Address	The support e-mail address to which VIA users will send client logs. Default: None.
VIA external download URL	End users will use this URL to download VIA on their computers.
Content Security Gateway URL	If the split-tunnel is enabled, access to external (non-corporate) web sites will be verified by the specified content security service provider. See the *Content Security Service* chapter in the latest *Dell PowerConnect W-ArubaOS User Guide* for details about Dell content security service.
Enable Content Security Services	Select this checkbox to enable content security service. You must install the Content Security Services licenses to use this option. See the *Software Licenses* chapter in the latest *Dell PowerConnect W-ArubaOS User Guide* for more information on licenses..
Client Auto-Login	Enable or disable VIA client to auto login and establish a secure connection to the controller. Default: Enabled
Allow client to auto-upgrade	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the controller. Default: Enabled

Table 6 *Connection Profile Options*

Configuration Option	Description
Enable split-tunneling	Enable or disable split tunneling. • If enabled, all traffic to the VIA tunneled networks (Step 3 in this table) 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
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
Allow user to save passwords	Enable or disable users to save passwords entered in VIA. Default: Enabled
Validate Server Certificate	Enable or disable VIA from validating the server certificate presented by the controller. Default: Enabled
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 log-off script that must be executed after the VIA connection is disconnected. The logoff script must reside in the client computer.
Maximum reconnection attempts	The maximum number of re-connection attempts by the VIA client due to authentication failures. Default: 3
Allow user to disconnect VIA	Enable or disable users to disconnect their VIA sessions. Default: on
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.
Keep 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.

Configure VIA Web Authentication

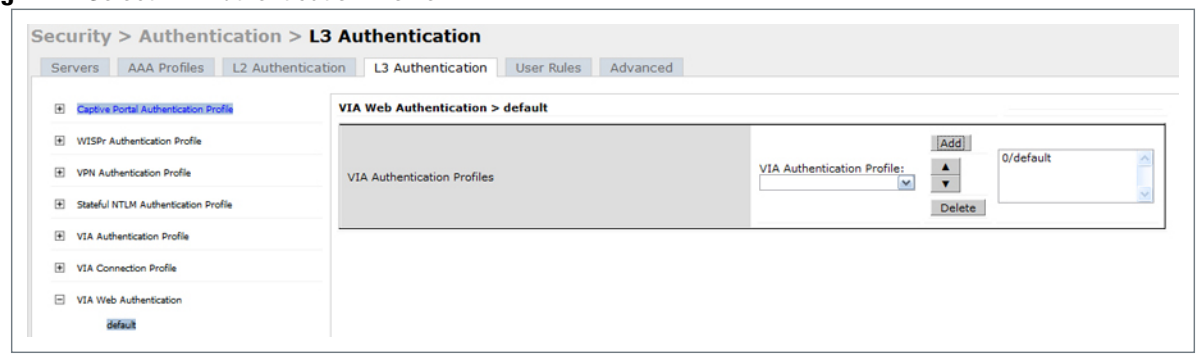
To configure VIA web authentication profile:

1. Navigate to **Configuration > Security > Authentication > L3 Authentication** tab.
2. Expand VIA Web Authentication and click on *default* profile.

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

3. Select a profile from VIA **Authentication Profile** drop-down list box and click the **Add** button.
   - To re-order profiles, click the *Up* and *Down* button.
   - To delete a profile, select a profile and click the **Delete** button.
4. If a profile is not selected, the *default* VIA authentication profile is used.

Figure 5 *Select VIA Authentication Profile*

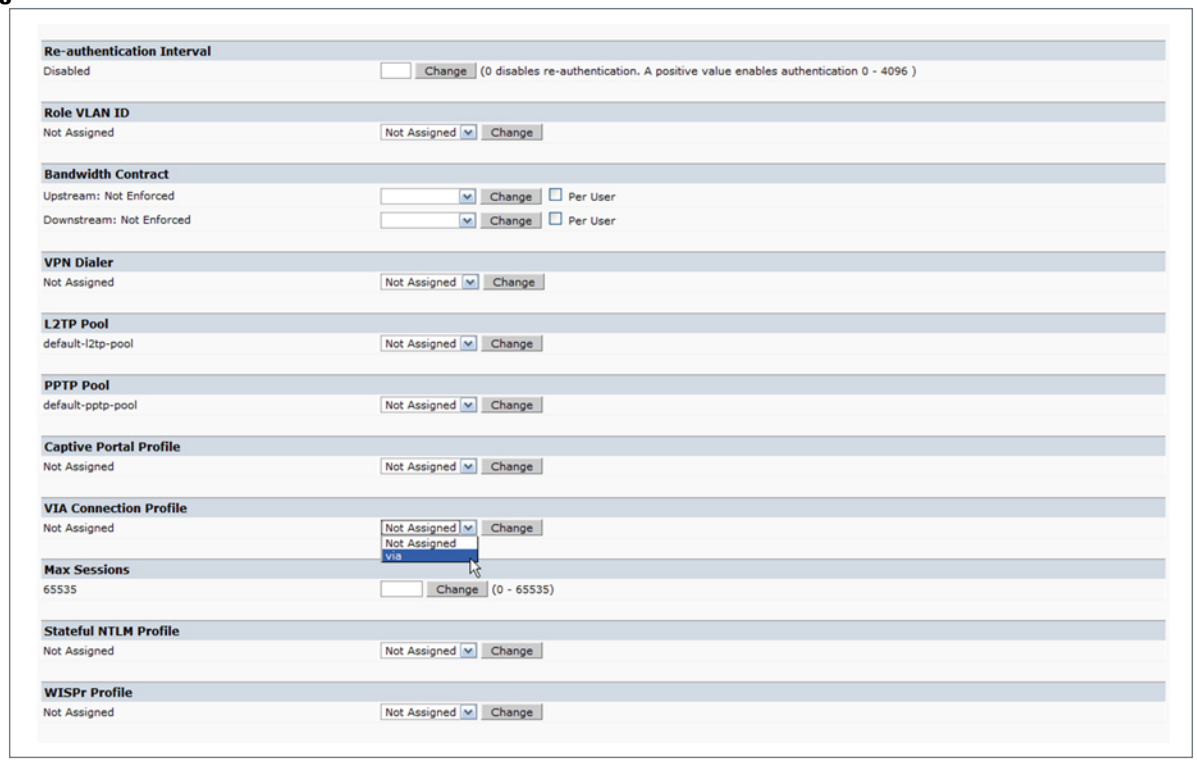


Associate VIA Connection Profile to User Role

To associate a VIA connection profile to a user role:

1. Navigate to **Configuration** > **Security** > **Access Control** > **User Roles** tab.
2. Select the VIA user role (See "Create VIA User Roles" on page 14) and click the **Edit** button.
3. In the *Edit Role* page, navigate to VIA Connection Profile and select the connection profile from the drop-down list box and click the **Change** button.
4. Click the **Apply** button to save the changes to the configuration.

Figure 6 *Associate VIA Connection Profile to User Role*

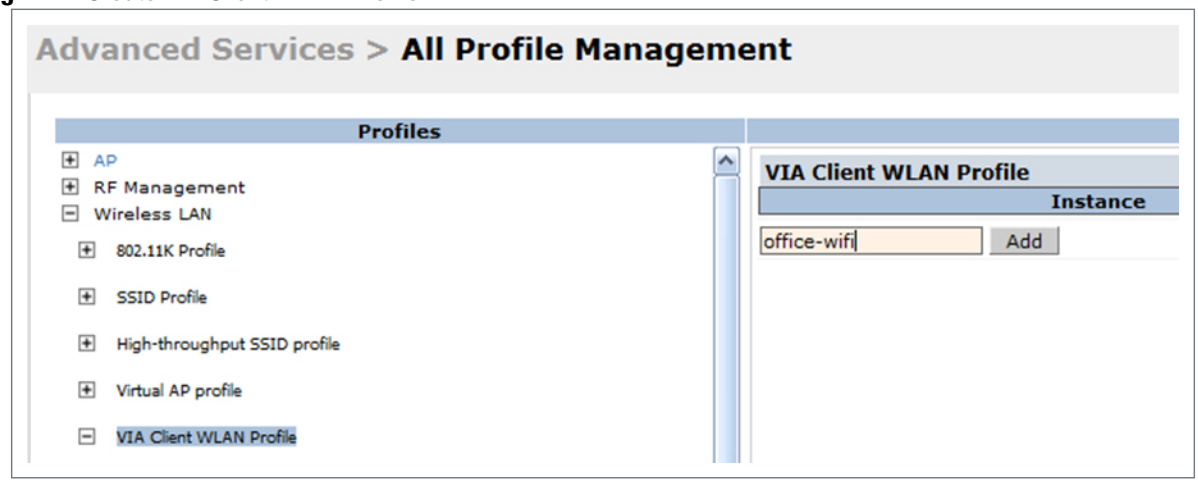


Configure VIA Client WLAN Profiles

To configure a VIA client WLAN profile:

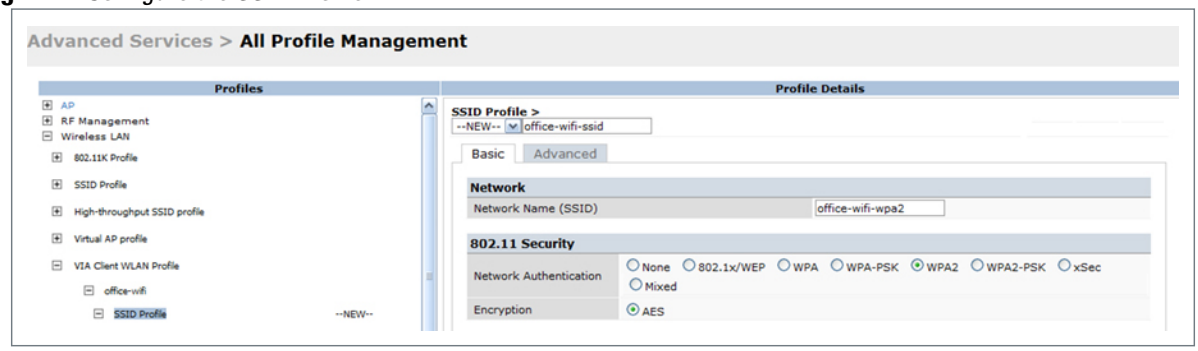
1. Navigate to **Configuration** > **Advanced Services** > **All Profiles**.
2. Expand *Controller Profiles* and select VIA **Client WLAN Profile.**
3. In the Profile Details, enter a name for the WLAN profile and click the **Add** button.

Figure 7 *Create VIA Client WLAN Profile*



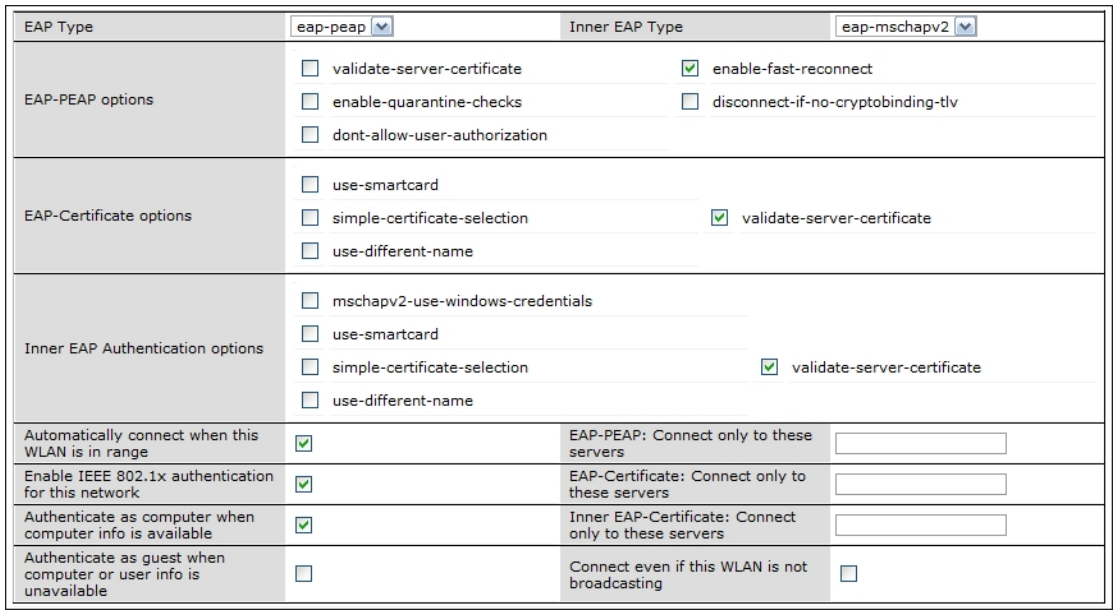
4. Expand the new WLAN profile and click on the SSID Profile. In the profile details page, select **New** from the SSID Profile drop-down box and enter a name for the SSID profile.
5. In the Basic tab, enter the network name (SSID) and select 802.11 security settings. Click the **Apply** button to continue.

Figure 8 *Configure the SSID Profile*



6. You can now configure the SSID profile by selecting the SSID profile under VIA Client WLAN Profile option.

Figure 9 *Configure VIA Client WLAN Profile*



The VIA client WLAN profiles are similar to the authentication settings used to set up a wireless network in Microsoft Windows. The following table shows the Microsoft Windows equivalent settings:

Table 7 *Configure VIA client WLAN profile*

Option	Description
EAP-PEAP options	Select the following options, if the EAP type is PEAP (Protected EAP): • validate-server-certificate: Select this option to validate server certificates. • enable-fast-reconnect: Select this option to allow fast reconnect. • enable-quarantine-checks: Select this option to perform quarantine checks. • disconnect-if-no-cryptobinding-tlv: Select this option to disconnect if server does not present cryptobinding TLV. • dont-allow-user-authorization: Select this to disable prompts to user for authorizing new servers or trusted certification authorities.
EAP Type	Select an EAP type used by client to connect to wireless network. Default: EAP-PEAP
EAP-Certificate Options	If you select EAP type as certificate, you can select one of the following options: • mschapv2-use-windows-credentials • use-smartcard • simple-certificate-selection • use-different-name • validate-server-certificate
Inner EAP Type	Select the inner EAP type. Currently supports only EAP-PEAP.
Inner EAP Authentication options:	• mschapv2-use-windows-credentials: Automatically use the Windows logon name and password (and domain if any) • use-smartcard: Use a smart card • simple-certificate-selection: Use a certificate on the user's computer or use a simple certificate selection method (recommended) • validate-server-certificate: Validate the server certificate • use-different-name: Use a different user name for the connection (and not the CN on the certificate)
Automatically connect when this WLAN is in range	Select this option if you want WZC (Microsoft Windows Wireless Zero Config tool) to connect when this network (SSID) is available.

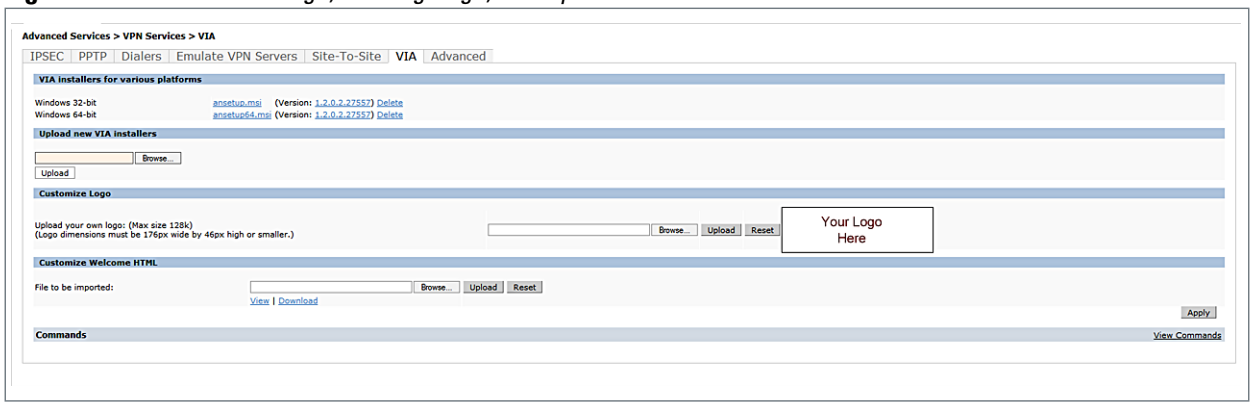
Table 7 *Configure VIA client WLAN profile*

Option	Description
EAP-PEAP: Connect only to these servers	Comma separated list of servers.
Enable IEEE 802.1x authentication for this network	Select this option to enable 802.1x authentication for this network. Default: Enabled.
EAP-Certificate: Connect only to these certificates	Comma separated list of servers.
Inner EAP-Certificate: Connect only to these servers	Comma separated list of servers.
Connect even if this WLAN is not broadcasting	Default: Disabled

Rebranding VIA and Uploading VIA Installers

You can rebrand the VIA client and the VIA download page with your custom logo and HTML page. Additionaly you can now upload latest versions of VIA installers.

Figure 10 *Customize VIA logo, Landing Page, and Upload VIA Installer*



Download VIA Installer and Version File

To download the VIA installer and version file:

1. Navigate to **Configuration > Advanced Services > VPN Services > VIA** tab.
2. Under VIA installers for various platforms section, click the installer file to download the installation file.

Upload VIA Installer

To upload a new VIA installer:

1. Navigate to **Configuration > Advanced Services > VPN Services > VIA** tab.
2. Under **Upload new VIA Installers**, browse and select the installer from your computer. Click the **Upload** button to upload the installer to the controller.

Customize Logo

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

1. Navigate to **Configuration > Advanced Services > VPN Services** > VIA tab.
2. Under the **Customize Logo** section, browse and select a logo from your computer. Click the **Upload** button to upload the image to the controller.

- To use the default Dell logo, click the **Reset** button.

Customize the Landing Page for Web-based Login

To use a custom landing page for VIA web login:

1. Navigate to **Configuration** > **Advanced Services** > **VPN Services** > VIA tab.
2. Under Customize Welcome HTML section, browse and select the HTML file from your computer. Click the **Upload** button to upload the image to the controller. The following variables are used in the custom HTML file:

   All variables in the custom HTML file have the following notation

   - `<% user %>`: this will display the username.
   - `<% ip %>`: this will display the IP address of the user.
   - `<% role %>`: this will be display the user role.
   - `<% logo %>`: this is 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>`)

   To use the default welcome page, click the Reset button.
3. Click the **Apply** button to continue.

Using CLI to Configure VIA

The following steps illustrate configuring VIA using CLI. Install your Policy Enforcement Firewall Virtual Private Network (PEFV) license key.

NOTE: Commands that achieve specific task are described in this section. For detailed information on the VIA command line options, see the latest *Dell PowerConnect W-ArubaOS Command Reference Guide*.

```
(host) (config)# license add <key>
```

Create VIA Roles

```
(host) (config) #user-role example-via-role
(host) (config-role) #access-list session "allowall" position 1
(host) (config-role) #ipv6 session-acl "v6-allowall" position 2
```

Create VIA Authentication Profiles

```
(host) (config) #aaa server-group "via-server-group"
(host) (Server Group "via-server-group") #auth-server "Internal" position 1
(host) (Server Group "via-server-group") #aaa authentication via auth-profile default
(host) (VIA Authentication Profile "default") #default-role example-via-role
(host) (VIA Authentication Profile "default") #desc "Default VIA Authentication
Profile"
(host) (VIA Authentication Profile "default") #server-group "via-server-group"
```

Create VIA Connection Profiles

```
(host) (config) #aaa authentication via connection-profile "via"
(host) (VIA Connection Profile "via") #server addr 202.100.10.100 internal-ip
10.11.12.13 desc "VIA Primary Controller" position 0
(host) (VIA Connection Profile "via") #auth-profile "default" position 0
(host) (VIA Connection Profile "via") #tunnel address 10.0.0.0 netmask 255.255.255.0
(host) (VIA Connection Profile "via") #split-tunneling
(host) (VIA Connection Profile "via") #windows-credentials
```

```
(host) (VIA Connection Profile "via") #client-netmask 255.0.0.0
(host) (VIA Connection Profile "via") #dns-suffix-list example.com
(host) (VIA Connection Profile "via") #support-email via-support@example.com
```

To enable content security services (CSS), do the following. CSS is available only if you have installed the content security services license. See the *Software Licenses* chapter in the latest *Dell PowerConnect W-ArubaOS User Guide* for more information on licenses..

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

Enter the following command after you create the client WLAN profile. See "Configure VIA Client WLAN Profiles" on page 19

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

Configure VIA Web Authentication

```
(host) (config) #aaa authentication via web-auth default
(host) (VIA Web Authentication "default") #auth-profile default position 0
```

NOTE: You can have only one profile (*default*) for VIA web authentication.

Associate VIA Connection Profile to User Role

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

Configure VIA Client WLAN Profiles

```
(host) (config) #wlan ssid-profile "via_corporate_wpa2"
(host) (SSID Profile "via_corporate_wpa2") #essid corporate_wpa2
(host) (SSID Profile "via_corporate_wpa2") #opmode wpa2-aes
(host) (SSID Profile "via_corporate_wpa2") #wlan client-wlan-profile
"via_corporate_wpa2"
(host) (VIA Client WLAN Profile "via_corporate_wpa2") #ssid-profile
"via_corporate_ssid"
```

For detailed configuration parameter information, see *"wlan client-wlan-profile"* command in the latest *Dell PowerConnect W-ArubaOS Command Reference Guide*.

Rebranding VIA and Uploading VIA Installers

This step can only be performed using the WebUI. See "Rebranding VIA and Uploading VIA Installers" on page 22.

Chapter 2

End User Instructions

This section of the document provides end user instructions and information on using the VIA connection manager.

Pre-requisites

Ensure that the end-user system meets the following pre-requisites:

- VIA can be installed on systems running:
  - Microsoft Windows XP with SP2
  - Microsoft Windows Vista (32-bit and 64-bit)
  - Microsoft Windows 7 (32-bit and 64-bit)

NOTE: VIA is supported only in the English versions of Microsoft Windows. International versions of Microsoft Windows are not supported.

- Requires the following Microsoft KB on the end-user systems:
  - On Microsoft Windows XP SP2—KB918997 (http://support.microsoft.com/kb/918997)

    Install this to see the list of detected wireless networks in the VIA client (**Diagnostics** tab > **Detected Networks** page).
  - On Microsoft Windows XP SP3—KB958071 (http://support.microsoft.com/kb/958071)

    Install this if you receive the "*1206 (ERROR_BAD_PROFILE)*" error code.
- Administrator rights on the computer.
- The computer must have a working wired or wireless network hardware.

Downloading VIA

In a typical scenario, end users will receive an email from their IT department with details to download VIA from a URL (controllers public IP address). See Table 6 on page 16.

In this example, they can download VIA set up files from `https://115.52.100.10/via` after entering their corporate credentials.

Figure 11 *Login to Download VIA*

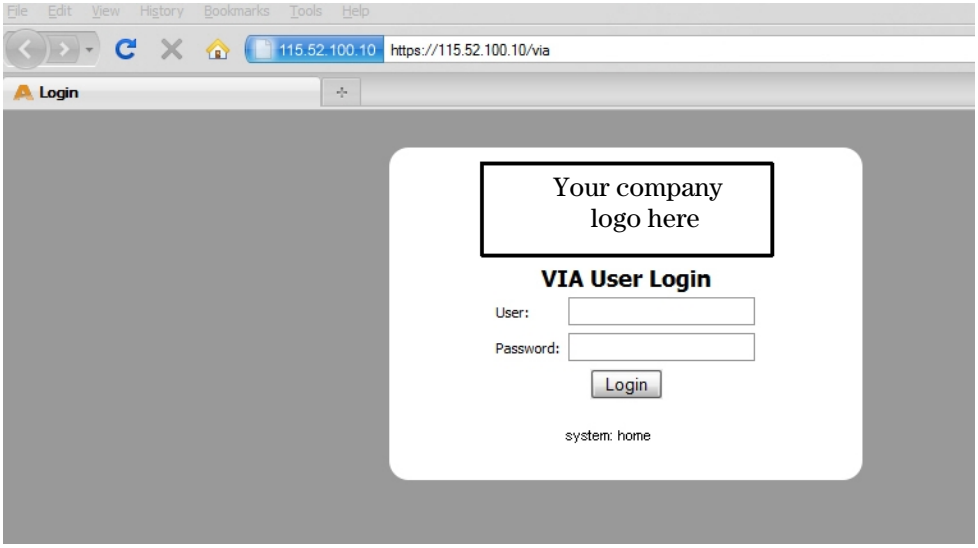
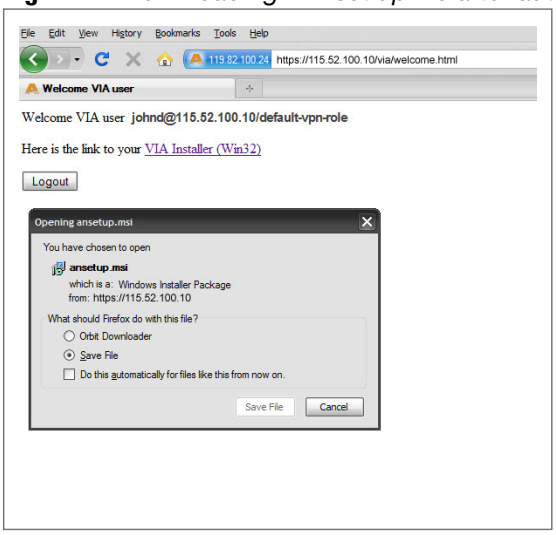


Figure 12 *Downloading VIA set up file after authentication*



Installing VIA

Double click the downloaded set up file to start the installation process. Ensure that you have met the pre-requisites before proceeding with the installation.

Using VIA

The VIA desktop application has three tabs:

- Connection Details
- Diagnostics
- Settings

Connection Details Tab

This tab provides all required details about your remote connection. After a successful connection, you can see the assigned IP from your remote server, the profile used for the connection and other network related information.

- Disconnect—Click this button to disconnect the current remote connection. You will have to manually connect for the next connection. VIA will not automatically start connection.
- View Connection Log—Click this button to view the sequence of events that took place during the last or current connection. The log also provides information about upgrade requirement, missing pre-requisites, or other encountered errors.
- Change Profile—Click this button to select an alternate connection profile. This button is enabled only if your administrator has configured more than one connection profile. This button toggles to **Download Profile**, if you clear your profile from the Settings tab.

More Details

This section gives information about your local connection.

- Click **Network Details** to view local network connection information.
- Click **VIA Details** to view error or other connection messages.

Diagnostic Tab

Provides information and tools for troubleshooting your connectivity issues. Select a diagnostic tool from this tab for more information.

Diagnostics Tools

- Connection Logs—Sequence of events that happened during the recent connection.
- Send Logs—List of log files collected by VIA. You can send this to your technical support when required. Click **Open Folder** to see the folder with the most recent logs and click the **Send** button to send log files archive using your default e-mail client.
- View system info & Advanced info—System and network configuration details of your system.
- Connectivity tests—Basic tests (ping and trace-route) to verify your network connection.
- Detected Networks—If your system has wireless network capability, this option will show all detected wireless networks.
- VIA info—Information about the current VIA installation.
- Compatibility info—Compatibility information about some applications detected in your system.

Settings Tab

This tab allows you to configure extra settings required to collect log, use a different connection profile and set up proxy server details.

- Log Settings—Allows you to set VIA log levels. By default, the log level is set to *Trace*. This setting captures extensive activity information about VIA.
- Connection Profile—Allows you to select and connect to a different connection profile. This is usually useful if you are in remote location and you need to connect to your corporate (secure) network. In such situation, you can select a profile that uses the nearest remote server to provide secure connection to your network. Alternate connection profiles are available only if it is configured by your IT administrator.
- Proxy Settings—Detects and displays Microsoft Internet Explorer proxy server details. It also allows you to enter the proxy authentication credentials to be used for HTTP/HTTPS connection to the controller.

Troubleshooting

To enable your support team to 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 **Connection Details** tab.