Aruba VIA 2.3.4 Windows® Edition

Release Notes

aruba
a Hewlett Packard Enterprise company

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

Aruba VIA 2.3.4 Windows® Edition is a software release that includes new feature enhancements and fixes to the issues identified in previous Aruba VIA Windows® Edition releases.

For more information on all the features, see the latest Aruba VIA User Guide.

About VIA

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

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	licensing.arubanetworks.com
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

This chapter includes the features, resolved issues, and known issues in this release of VIA Windows edition.

Features

This section describes the new features and enhancements introduced in VIA 2.3.4.

Block-All-Traffic

This feature adds the ability for VIA client to block all outbound traffic from a client machine until the tunnel is established. An exception can be created by configuring a whitelist on the controller. Traffic to the IP address configured in the whitelist will be allowed. So, this feature prevents the user from accessing the Internet until VIA connection is established for all IP addresses except the ones white-listed. All outbound traffic is allowed as soon as VIA establishes tunnel.

To enable block-all-traffic, perform the following steps in the controller:

1. Navigate to **Configuration > Security > Authentication > L3 Authentication**.
2. Expand **VIA Connection**, select the connection profile.
3. In the **VIA Connection Profile** pane, click **Advanced**.
4. Select **Block traffic until VPN tunnel is up**.
5. Configure whitelist under **Block traffic rules**:
   a. For **Hostname /IP Address**, enter the IP address that needs to be allowed when tunnel is not up.

Only IP addresses can be configured. Configuring using host names is not yet supported

   b. For **Network Mask**, enter the subnet mask.
   c. For **Description**, enter a description for this rule.
   d. Click **Add**.
6. Click **Apply**.

For example, consider **Block traffic until VPN tunnel is up** is enabled and the IP addresses is 216.50.100.100/24 under **Block traffic rules**, the user downloads the profile and tunnel is established. When the user disconnects, the user will not be able to access internet but will be able to access 216.50.100.100/24.

Certificate Selection during DPC Flow

This feature adds the ability in DPC flow to prefer user-selected certificate over other valid certificate from machine certificate store.

Provision to Configure MTU for Virtual Adapter

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.

NOTE

The **VIA Client mtu value** parameter is introduced in ArubaOS 6.5.1.

To configure the **VIA Client MTU value**, perform the following steps in the controller:

1. Navigate to **Configuration > Security > Authentication > L3 Authentication**.
2. Expand **VIA Connection**, select the connection profile.
3. In the **VIA Connection Profile** pane, click **Advanced**.
4. For **VIA Client mtu value**, enter a value between 576 and 5120. Default: 1452.
5. Click **Apply**.

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.

Resolved Issues

This section describes the issues resolved in this release of VIA.

Table 2: *Resolved Issues in VIA 2.3.3*

Bug ID	Description
35424 145761	**Symptom:** Authentication failed after upgrading to VIA 2.3.3. The fix ensures that authentication is successful even after upgrading to VIA 2.3.3 or later version. **Scenario:** This issue was observed in VIA 2.3.3 when RSA secure-ID server was used for authentication and the save password option was enabled in the connection profile. VIA used the saved password always instead of the the new token generated by RSA, which resulted in authentication faulre.
35598	**Symptom:** A dialog box to enter the pin was displayed by VIA service. The fix ensures that pin input dialog box is not displayed by VIA service when smart card is used for multifactor authentication. **Scenario:** This issue was observed when a smart card was used for multifactor authentication to connect to VIA.

Known Issues and Limitations

There are no new known issues identified in this release.

This chapter describes features or enhancements introduced in previous releases of Aruba VIA for Windows.

Features in VIA 2.3.3

This section describes the new features and enhancements introduced in VIA 2.3.3.

Zero Touch User Provisioning

This feature is supported on controllers running ArubaOS 6.5.x.

VIA 2.3.3 enables administrator to pre-provision VIA profile for new user. This feature automates VIA profiles generation for a new system user and helps the new user by avoiding pre-requisite of providing initial details like VPN gateway address and user credential. Administrator can configure this behavior by following steps:

1. Log in to the controller.
2. Navigate to **Configuration > Security > Authentication > L3 Authentication**, expand **VIA Connection**.
3. Select the connection profile you want to configure.
4. In the **VIA Connection Profile > <Profile name>** page, click **Advanced**.
5. Select **Enable Domain Pre-connect**.
6. Select **Enable Generating Common Profile if DPC is Enabled**.

Features in VIA 2.3.2

This section describes the new feature introduced in VIA 2.3.2.

MOBIKE for VIA Windows Edition

This feature is supported on controllers running ArubaOS 6.4.4.0 version or later.

With MOBIKE support, if the physical IP address changes due to interface change or changes on the same interface, VIA detects for any available interface to reach the controller. If an interface exist, VIA switches tunnel using new the IP address and avoids full IKE negotiation.

MOBIKE helps reduce stress on the controller by avoiding full IKE negotiation especially when user is roaming.

MOBIKE is not supported when VIA is running in SSL mode and DPC mode.

Features Added in VIA 2.3.1

No features were introduced in this release.

Features Added in VIA 2.3.0

This section describes the features added in VIA 2.3.

Windows 10 Support

VIA 2.3 introduces the support for Windows 10.

Hex Based Pre-Shared Key

VIA 2.3 introduces the support for Hex based encoding for Pre-Shared Key (PSK).

Validation of the Revocation Status of a Peer Certificate using OCSP

VIA 2.3 is provisioned to perform revocation check of server certificate exchanged during IKE negotiation and EAP-TLS exchange using the Online Certificate Status Protocol (OCSP) method. VIA extract OCSP responder information from certificate being checked. If OCSP responder information is unavailable in certificate, revocation check is skipped. Administrator can configure (enable/disable) OCSP revocation check through VIA connection profile. Administrator can also define if VIA connection should be allowed in case OCSP status cannot be determined for some reason. For example, OCSP responder is not reachable.

Verification of DN Values in a Peer Certificate

VIA 2.3 is provisioned to check for Distinguished Name (DN) values (CN, ORG, OU, Country), configured in VIA connection profile vs values present in server certificate exchanged during IKE negotiation and EAP-TLS exchange. If DN Values present in certificate matches with any pair of configured values, is considered as match. If any value is not configured among configured DN value, for example, if CN is not configured but ORG, OU, and country values are configured, VIA matches only the configured value.

Validation of Strength of Symmetric Algorithm

With FIPS enabled, VIA 2.3 ensures that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection, as shown in the following table:

Table 3: *Strength of the Symmetric Algorithm*

IKEv1 Phase 1/ IKEv2 IKE_SA	IKEv1 Phase 2, IKEv2 CHILD_SA
3DES	3DES
AES128	AES128
AES192	AES128, AES192
AES256	AES128, AES192, AES256

Support for IPSec Drop policy

VIA 2.3 is provisioned to drop certain traffic for values configured in connection profile. VIA can drop only the traffic which is a candidate for routing through tunnel in the absence of this configuration. For example, in the full tunnel mode, an administrator can restrict access to certain network address.

VIA Always Operates in PPP Mode

In earlier versions Windows VIA, VIA operated in the following two modes:

- Driver mode: All packet processing is performed in Aruba VIA driver.
- PPP mode: All packet processing is performed by Aruba VIA process (in user land).

But from VIA 2.3 onwards, all placket processing is performed only in PPP mode.

Upgrade Initiation During Windows Start

VIA 2.3 is provisioned to initiate VIA upgrade during Windows start if VIA auto-upgrade was not completed at the end of the previous session. VIA upgrade is initiated in the following scenarios:

- Windows machine went to Sleep
- Windows machine was Hibernated
- Windows machine was Signed out
- VIA service was killed
- VIA process was killed
- Controller was restarted

Verification of Integrity of Software Updates Prior to Installing the Updates

VIA 2.3 is provisioned to perform integrity check of the downloaded installer before executing the installer. This feature helps avoiding the risk of tampering the installer.

TLS 1.2 in EAP-TLS Flow

VIA 2.3 client introduces the support for Transport Layer Security (TLS) version 1.2 during IKEv2 EAP-TLS based authentications.

This chapter describes the issues resolved in the previous releases of VIA 2.3.x.

Resolved Issues in VIA 2.3.3

Table 4: *Resolved Issues in VIA 2.3.3*

Bug ID	Description
33137 127816	**Symptom:** Domain Pre-connect (DPC) failed to work. This issue is resolved by using the new API in which DNS is resolved. **Scenario:** After the user logged off the Windows computer, user got disconnected, and no tunnels were noticed. This issue was observed in Windows machines with VIA 2.1.1.8, 2.3.0, or 2.3.1.
33489 137740	**Symptom:** The **Logon Unsuccessful** message appeared even before the user entered the VIA credentials. This issue is resolved by removing the message from appearing for this instance. The **Logon Unsuccessful** message appears only when the VIA credentials entered are incorrect. **Scenario:** This issue was observed in Windows machines with VIA 2.3.1.
33826	**Symptom:**VIA frequently disconnected and reconnected when in a trusted network. This issue is resolved by handling route table modification for split-tunnel scenarios. **Scenario:** This issue was observed when VIA packets were dropped when connected from an internal network using split-tunnel configuration. This issue was observed in Windows machines with VIA 2.3.0.
34592 141253	**Symptom:** Configuring VIA with EAP-TLS authentication against CPPM server failed. This issue is resolved by appending signature data even if certificate is of machine type. **Scenario:** This issue was observed when TLS 1.2 was enabled and CPPM 6.5 EAP-TLS was used with machine cert. This issue occurred in VIA 2.3.2 with CPPM as the RADIUS server.
34990 144336	**Symptom:**VIA rejected certificate with error-**7603**. This issue is resolved by adding provision to recognize specific object identifier (OID) and accept certificate. **Scenario:** This issue was observed when a certificate had a specific OID. This issue was observed in Windows machines with VIA 2.3.2.

Resolved Issues in 2.3.2

Table 5: *Resolved Issues in VIA 2.3.2*

Bug ID	Description
30322 114428	**Symptom:**VIA system tray icon was green indicating that VIA was connected although VIA connection was not established. The fix ensures that tray icon displays the correct status of the VIA connection. **Scenario:** This issue was specific to Surface Pro 3 devices and was observed only when device resumed from the sleep mode.
30325	**Symptom:** After the client operating system was upgraded to Windows 8.1, VIA services failed to start. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in Windows 8.1 clients running VIA 2.3.
31160	**Symptom:**VIA took longer time (close to a minute) to disconnect and reconnect to the network. This issue is resolved by implementing internal code changes to handle change in network interface. **Scenario:** This issue was observed in case of events like loss of IP address and disabled network adapter. This issue occurred in Windows clients running VIA 2.3.1 or earlier.
31285	**Symptom:** Maximum session time out failed. This issue is resolved by making maximum session timer independent of the rekey timer. **Scenario:** This issue was observed if rekey happens before reaching max session time out.
32306	**Symptom:** VIA EAP-TLS fails when an onboarded certificate is used. This issue is resolved by implementing internal code changes to handle the certificates issued by the onboarding server. **Scenario:** This issue was observed when an onboarded client certificate provisioned in Windows Cert Store caused authentication failure. This issue was observed in VIA 2.3.0.

Resolved Issues in VIA 2.3.1

Table 6: *VIA 2.3.1 Fixed Issues*

Bug ID	Description
123902	**Symptom:** In IKEv2 EAP-TLS, the username from the certificate was not displayed in VIA. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed in VIA 2.3 for Windows when displaying the certificate common name was not handled correctly.
124217	**Symptom:** Although VPN connection was established, VIA used local Domain Name Server (DNS). This issue is resolved by provisioning VIA to use the DNS provided by the controller during tunnel. **Scenario:** This issue was observed in Windows 10 clients running VIA 2.3.
125194	**Symptom:**VIA 2.3 fails to authenticate using the IKEv1 user certificate . This issue is resolved by implementing internal code changes to handle this certificate correctly. **Scenario:** This issue was observed in VIA 2.3 for Windows when some certificate properties was not handled.
29849 123888	**Symptom:**VIA 2.3 failed to establish a connection. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when the virtual adapter was disabled and VIA failed to enable the virtual adapter to configure. This issue was observed in Windows 10 clients running with VIA 2.3.

Resolved Issues in VIA 2.3.0

Table 7: *VIA 2.3.0 Fixed Issues*

Bug ID	Description
25756 102147	**Symptom:** VIA 2.3 proposed multiple encryption algorithm during IKE negotiation. This issue is resolved by ensuring that VIA proposes only the algorithm, which is configured in the connection profile. **Scenario:** This issue was observed in a Windows machine with VIA 2.3.
29729 121289	**Symptom:** The VIA client used an incorrect connection profile. This issue is resolved by implementing internal code changes. **Scenario:** This issue was observed when the auto-login feature was disabled on the profile and the profile had multiple connection profiles configured. This issue was observed in a Windows machine with VIA 2.1.1.8.

This chapter describes the known and outstanding issues identified in previous releases of VIA 2.3.x.

Contact Aruba Technical Support with your case number, if there is any specific bug that is not documented in this section.

Known Issues in VIA 2.3.3

Known issues identified in this release are now resolved.

Known Issues in VIA 2.3.2

Known issues identified in this release are now resolved.

Known Issues in VIA 2.3.1

Known issues identified in this release are now resolved.

Known Issues in VIA 2.3.0

Table 8: *VIA 2.3.0 Known Issues*

Bug ID	Description
29844	**Symptom:** After upgrading to VIA 2.3, connection is established using a connection profile that does not adhere to Table 3. **Scenario:** This issue is observed when a user connected using an existing connection profile that does not adhere to Table 3 and continues to use the same connection profile even after upgrading to VIA 2.3. This issue is specific to VIA 2.3. **Workaround:** Administrator must update the connection profile by creating new policies that adheres to Table 3. **NOTE:** Changing the existing policies can cause the connection to fail.
29931	**Symptom:** Windows 10 devices failed to uninstall VIA properly. As a result, the VIA client retains the old profile after a fresh install. **Scenario:** This issue is specific to Windows 10 and VIA 2.3. **Workaround:** Clear the profile before uninstalling VIA 2.3 or clear the profile after reinstalling the VIA client.

When upgrading from any of the earlier Windows VIA version to Windows VIA 2.3.x, the administrator must ensure that the IKEv1 and IKEv2 policies in the connection profile matches with Table 3.

Auto-downgrade to lower versions is not possible after upgrading to VIA 2.3.0. However, auto-downgrade to a lower versions of VIA 2.3.x from a higher version of VIA 2.3.x is possible.