Aruba VIA 2.3 Windows® Edition

Release Notes

aruba®
NETWORKS
an HP company

Aruba VIA 2.3 Windows® Edition is a software release that includes new feature enhancements and fixes to the issues identified in previous Aruba VIA Windows® Edition releases.

Aruba VIA 2.3 Windows® Edition is common criteria (CC) evaluated and validated. For more details, refer to https://www.niap-ccevs.org/st/Compliant.cfm?pid=10616.

For more information on all the features, see the latest Aruba VIA 2.3 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	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Airheads Social Forums and Knowledge Base	https://community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	http://www.arubanetworks.com/support-services/support-program/contact-support/
Software Licensing Site	https://licensing.arubanetworks.com/
End-of-life Information	http://www.arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/security-bulletins/
Support Email Addresses	
Americas, EMEA, and APAC	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com

This chapter describes the features introduced in this release of VIA Windows edition.

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 2: *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.

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.

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

Chapter 3
Resolved Issues

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

Table 3: *VIA 2.3 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.

Chapter 4
Known Issues and Limitations

This chapter describes the known and outstanding issues identified in this release of VIA.

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

Table 4: *VIA 2.3 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 2. **Scenario:** This issue is observed when a user connected using an existing connection profile that does not adhere to Table 2 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 2. **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, the administrator must ensure that the IKEv1 and IKEv2 policies in the connection profile matches with Table 2.

Auto-downgrade to lower versions is not possible after upgrading to VIA 2.3.