

# **Aruba VIA 2.3 Windows® Edition**



Release Notes

## Copyright Information

© 2015 Aruba Networks, Inc. All rights reserved. Aruba Networks®, Aruba Networks™ (stylized), People Move Networks Must Follow®, Mobile Edge Architecture®, RFPProtect®, Green Island®, ClientMatch®, Aruba Central®, Aruba Mobility Management System™, ETips™, Virtual Intranet Access™, Aruba Instant™, ArubaOS™, xSec™, ServiceEdge™, Aruba ClearPass Access Management System™, AirMesh™, AirWave™, Aruba@Work™, Cloud WiFi™, Aruba Cloud™, Adaptive Radio Management™, Mobility-Defined Networks™, Meridian™ and ArubaCareSM are trademarks of Aruba Networks, Inc. registered in the United States and foreign countries. Aruba Networks, Inc. reserves the right to change, modify, transfer or otherwise revise this publication and the product specifications without notice.

## 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. Includes software for Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site:

[http://www.arubanetworks.com/open\\_source](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.

## Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS. Altering this device (such as painting it) voids the warranty.

---

<b>Contents</b>	<b>3</b>
<b>Release Overview</b>	<b>4</b>
About VIA	4
Contacting Support	4
<b>New Features</b>	<b>5</b>
Windows 10 Support	5
Hex Based Pre-Shared Key	5
Validation of the Revocation Status of a Peer Certificate using OCSP	5
Verification of DN Values in a Peer Certificate	5
Validation of Strength of Symmetric Algorithm	5
Support for IPSec Drop policy	6
Verification of Integrity of Software Updates Prior to Installing the Updates	6
VIA Always Operates in PPP Mode	6
Upgrade Initiation During Windows Start	6
<b>Resolved Issues</b>	<b>7</b>
<b>Known Issues and Limitations</b>	<b>8</b>
<b>Upgrade Procedure</b>	<b>9</b>

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	<a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>
Support Site	<a href="https://support.arubanetworks.com">https://support.arubanetworks.com</a>
Airheads Social Forums and Knowledge Base	<a href="https://community.arubanetworks.com">https://community.arubanetworks.com</a>
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	<a href="http://www.arubanetworks.com/support-services/support-program/contact-support/">http://www.arubanetworks.com/support-services/support-program/contact-support/</a>
Software Licensing Site	<a href="https://licensing.arubanetworks.com/">https://licensing.arubanetworks.com/</a>
End-of-life Information	<a href="http://www.arubanetworks.com/support-services/end-of-life/">http://www.arubanetworks.com/support-services/end-of-life/</a>
Security Incident Response Team (SIRT)	<a href="http://www.arubanetworks.com/support-services/security-bulletins/">http://www.arubanetworks.com/support-services/security-bulletins/</a>
<b>Support Email Addresses</b>	
Americas, EMEA, and APAC	<a href="mailto:support@arubanetworks.com">support@arubanetworks.com</a>
Security Incident Response Team (SIRT)	<a href="mailto:sirt@arubanetworks.com">sirt@arubanetworks.com</a>

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 packet 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

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

**Table 3:** *VIA 2.3 Fixed Issues*

Bug ID	Description
25756 102147	<b>Symptom:</b> 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. <b>Scenario:</b> This issue was observed in a Windows machine with VIA 2.3.
29729 121289	<b>Symptom:</b> The VIA client used an incorrect connection profile. This issue is resolved by implementing internal code changes. <b>Scenario:</b> 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 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	<p><b>Symptom:</b> After upgrading to VIA 2.3, connection is established using a connection profile that does not adhere to <a href="#">Table 2</a>.</p> <p><b>Scenario:</b> This issue is observed when a user connected using an existing connection profile that does not adhere to <a href="#">Table 2</a> and continues to use the same connection profile even after upgrading to VIA 2.3. This issue is specific to VIA 2.3.</p> <p><b>Workaround:</b> Administrator must update the connection profile by creating new policies that adheres to <a href="#">Table 2</a>.</p> <p><b>NOTE:</b> Changing the existing policies can cause the connection to fail.</p>
29931	<p><b>Symptom:</b> Windows 10 devices failed to uninstall VIA properly. As a result, the VIA client retains the old profile after a fresh install.</p> <p><b>Scenario:</b> This issue is specific to Windows 10 and VIA 2.3.</p> <p><b>Workaround:</b> Clear the profile before uninstalling VIA 2.3 or clear the profile after reinstalling the VIA client.</p>



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.

---