Aruba Virtual Intranet Access (VIA) 4.x Client Common Criteria Guidance

Version 1.3

September 2022

1. Overview

It is assumed that the individual responsible for administering VPN connections is familiar with the Aruba Mobility Controllers, Mobility Gateways, and ArubaOS 8.x.

The FIPS module must be enabled (guidance on how to set fips mode) and the product will not be in its evaluated configuration if this is not done.

The connection settings are acquired from the Mobility Controller. To ensure compliance, the administrator should ensure that FIPS has been enabled. Information on how to configure the IPsec profiles for VIA are documented in Section 2 of this document.

The Target of Evaluation was tested on Windows, Linux, and Android.

1.1 Reference Documentation

The purpose of this document is to identify the required guidance content not covered directly through the Help Center Page, cited below.

- Aruba VIA 4.x Help Center

This document was updated in September, 2022, following the addition of VIA 4.3 to the PCL to reflect the release of VIA 4.4 and its addition via Assurance Maintenance. Release notes for VIA 4.4.0 can be found here:

- Aruba VIA 4.4 Release Notes.

2. VPN Client Guidance Requirements

2.1 Initial Configuration

2.1.1 Windows

To download VIA:

1. Login to the Aruba Support Portal.
2. Navigate to **Software and Documents**.
3. In the **Filters** menu, select the following filter options:

File type**: Software**

Product: **Aruba Virtual Intranet Access**

File Category: **Windows**

Major Version: **4**

Patch Version: Select the VIA version you want to download, for example, 4.4.0.

To install VIA:

1. Open the downloaded 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.

VPN profiles must be downloaded in order to connect VIA. If VIA 4.x is newly installed on the device, the VPN download screen opens upon launching VIA. If an existing instance of VIA is upgraded to VIA 4.x, the VPN Server list opens upon launching VIA.

2.1.2 Linux

To download VIA:

1. Login to the Aruba Support Portal.
2. Navigate to Software and Documents.

3. In the **Filters** menu, select the following filter options:

File type**: Software**

Product: **Aruba Virtual Intranet Access**

File Category: **Linux**

Major Version: **4**

Patch Version: Select the VIA version you want to download, for example, 4.4.0.

4. Click the download icon to download the installer file that is appropriate for your operating system and architecture.

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**.

2.1.3 Android

Open the Android Google Play Store and search for Aruba VIA to download the Aruba VIA application. Installation starts automatically once VIA is downloaded.

You must download a VPN profile in order to connect VIA.

1. Open the VIA application on your Android device. The Home screen appears.
2. From the VIA home screen, select **Click to download VPN profile**. The **Download VPN Profiles** screen appears.

3. Enter the IPv4/IPv6 address or FQDN of the VPN server. This information should be provided by the system administrator.
4. Click **Download**.

Note: The Android version of VIA requires access to the system log to record log data.

2.2 IPsec Configuration

This section provides supplemental information for configuring IPsec for VIA. Please reference the help page in Section 1.1 for initial configuration and setup instructions. The VPN Gateway (acting as an administrator) to which the TOE connects, configures the reference identifier of the peer.

ArubaOS will extract the User Principal Name field from the client certificate and pass it through an authentication/authorization process when this functionality has been enabled. VIA clients will be authenticated according to configuration found under "aaa authentication via auth-profile” (See Section 2.2.2).

In compliance with Enterprise Security Policies, the security administrator must ensure that the server certificate used in IPsec session establishment is loaded with the full bundled certificate chain (e.g. Root, Intermediate, Leaf).

Note: Aggressive mode is not supported for IKEv1

2.2.1 VIA Connection Profiles

VIA connection profiles contain settings required by VIA to establish a secure connection to a standalone controller or a Mobility Conductor 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.

<u>Connection Profile Refresh</u>

If a network administrator makes a change to the VIA Connection profile after the user is connected to VIA, users can refresh the Connection profile on their device to obtain the latest updates.

Android users: Disconnect the device from VIA, exit the software, and then immediately relaunch VIA. Perform this operation again a second time to refresh the profile.

Windows/Linux users: Disconnect and then immediately reconnect the device to VIA. Perform this operation again a second time to refresh the profile.

Limitations of VIA Automatic Connection Profile Synchronization.

The following connection parameters cannot be automatically synchronized and require a manual redownload of the VIA profile to update.

1. The external hostname or IP address of the controller or Mobility Conductor
2. Internal IP address of the controller or Mobility Conductor
3. If the synchronization fails, the user will continue using the old profile until that user disconnects and then reconnects again. On the next successful connection, the user will get the new modified profile.

To create a VIA connection profile:

1. 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.
4. Enter a **Profile name**.
5. Configure the remaining profile settings
6. Click **Submit**.
7. Select **Pending Changes**.
8. In the **Pending Changes** window, select the check box and click **Deploy Changes**

Note: Section 2.2.4 and 2.2.5 document how to configure IKEv1 and IKEv2 configurations for usage with the Connection Profile.

Note: Ensure 'Enable FIPS Module' and 'OCSP Cert verification enabled' are selected and that 'In EAP/IKE, action taken when OCSP Cert verification result is unknown' is unchecked.

Note: To limit the maximum session length regardless of IKE policy configuration, an administrator may set the 'VIA max session timeout value (in minutes)'. The default value is 1440 minutes (24 hours).

2.2.2 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 the 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. These profiles are configured on the ArubaOS Mobility Controller.

To configure a VIA web authentication profile:

1. Navigate to **Configuration** > **Authentication >L3 Authentication**.
2. Expand **VIA Web Authentication** from the **L3 Authentication** list and click on the **default** profile.
3. Under **VIA Web Authentication: default**, click **+** at the bottom of the **VIA Authentication Profiles** list.
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.

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. 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 1.
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. 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. 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. 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**.

2.2.3 Access Controls

PROTECT vs BYPASS can be enabled implicitly through enabling split tunnelling for the connection profile on the mobility controller.

The admin on the controller needs to define an SPD that DISCARDs all traffic that doesn’t match any other rule. This is done by applying a deny all rule as the final row within an access control list. If any conflict occurs within an access control list, the first rule within the policy that matches the criteria is enforced. Example:

- Rule 1 denies port 22 traffic from any host attempting a connection to host 172.16.1.10
- Rule 2 permits all traffic from subnet 10.10.10.X

In the above instance, a device on 10.10.10.x may be able to connect to 172.16.1.10 from the 10.10.10.X subnet but would be denied if they attempted to connect on port 22 based on the rule hierarchy.

The access control lists used by the TOE are read in hierarchical order. When traffic enters or exits the TOE, the first applicable rule in the ACL is applied. Any rule below the initially triggered rule is not applied. Note that if an access rule is applied, a duplicate cannot be entered. If the administrator applied a permit rule and then enters a deny rule with the same parameters, the deny rule will replace the permit rule and vice versa.

To configure an ACL, an administrator can configure an ip access-list route and apply it to the VPN server address. An example is provided below:

```
ip access-list route spd-test

  host <IP address> host <IP address> icmp echo forward

host <IP address> host <IP address> svc-icmp  route ipsec-map <IP address>
  host <IP address> host <IP address> svc-http  route tunnel 10
interface vlan <vlanid>
        ip address <IP address> <subnet>
        operstate up
        ip access-group "spd-test" in
!
```

The configuration above provides SPD control for inbound wired traffic. For VPN client users, multiple ACLs may be sequenced with a user-role container, simplifying this configuration.

2.2.4 IKEv1 Policy Configuration

To configure an IKEv1 Policy:

1. In the **Controller**, navigate to the **Configuration > Services > VPN** tab.
2. Expand **IKEv1**.
3. In the **IKEv1 Policies** table, click an existing policy to edit it, or click **+** to create a new policy.
4. In **Priority**, enter a priority number for this policy. Enter 1 for the configuration to take priority over the default setting.
5. Select the **Enable Policy** check box to enable the policy when it is saved.
6. From the **Encryption** drop-down list, select one of the encryption options
7. From the **Hash algorithm** drop-down list, select one of the listed hash types
8. Aruba VPNs support client authentication using pre-shared keys, RSA digital certificates, or Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. To set the authentication type for the IKE rule, from the **Authentication** drop-down list, select one of the listed options
9. Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret and is used within IKE to securely establish session keys. To set the Diffie–Hellman Group for the ISAKMP policy, from the **Diffie-Hellman group** drop-down list, select one of the listed options
10. In **Lifetime**, enter a value of 86400 seconds to define the lifetime of the security association.
11. Click **Submit**.
12. Click **Pending Changes**.
13. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To configure the dynamic map for IKEv1:

1. In the **MC**, navigate to the **Configuration > Services > VPN** tab.
2. Expand **IKEv1**.
3. In **IKEv1 IPsec Dynamic Maps**, click an existing dynamic map to edit it or click **+** to create a new map.
4. In **Priority**, enter a priority number for this map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next-highest priority map until a match is made.
5. In **Name**, enter a name for the dynamic map.
6. Select the **Dynamic map** check box.
7. In **Transforms**, select an existing transform to edit it, or click **+** to open the **New Transform** window.
8. Enter a name for the transform in the **Name** field.
9. From the **Encryption** drop-down list, select one of the listed encryption types
10. From the **Hash** algorithm drop-down list, select one of the listed hash types
11. Click **Submit**.

12. In **Lifetime(seconds)**, enter a value in the range of 28,800 seconds to define the lifetime of the security association for the dynamic peer. The default value is 7200 seconds.
13. In **Lifetime(kilobytes)**, enter a value in kilobytes to define the lifetime of the security association for the dynamic peer.
14. Click **Submit**.
15. Click **Pending Changes**.
16. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To avoid any issues, it is recommended that the following command can be used under the crypto-local ipsec-map to force tunnel mode to be the only option offered. However, it is not necessary with the above configuration.

```
force-tunnel-mode
```

To ensure that disabling of IKEv1 aggressive mode, use the following command:

```
(config) #crypto-local isakmp disable-aggressive-mode
```

2.2.5 IKEv2 Policy Configuration

To configure an IKEv2 Policy:

1. Navigate to the **Configuration > Services > VPN** tab.
2. Expand **IKEv2**.
3. In the **IKEv2 Policies** table, click an existing policy to edit it, or click **+** to create a new policy.
4. In **Priority**, enter a priority number for this policy. Enter 1 for the configuration to take priority over the default setting.
5. Select the **Enable Policy** check box to enable the policy when it is saved.
6. From the **Encryption** drop-down list, select one of the listed encryption types
7. From the **Hash algorithm** drop-down list, select one of the listed hash types
8. VIA supports client authentication using pre-shared keys, RSA digital certificates, or ECDSA certificates. To set the authentication type for the IKE rule, from the **Authentication** drop-down list, select one of the listed options
9. Diffie-Hellman is a key agreement algorithm that allows two parties to agree upon a shared secret, and is used within IKE to securely establish session keys. To set the Diffie–Hellman Group for the ISAKMP policy,
10. from the **Diffie-Hellman group** drop-down list, select one of the listed options
11. Set the **PRF** value. This algorithm is an HMAC function used to hash certain values during the key exchange:

12. In **Lifetime**, enter a value of 86400 seconds to define the lifetime of the security association.
13. Click **Submit**.
14. Click **Pending Changes**.
15. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To configure the dynamic map for IKEv2:

1. Navigate to the **Configuration > Services > VPN** tab.
2. Click **IKEv2** to expand that section.
3. In **IKEv1 IPSec Dynamic Maps**, click an existing dynamic map to edit it or click **+** to create a new map.
4. In **Priority**, enter a priority number for this map. Negotiation requests for security associations try to match the highest-priority map first. If that map does not match, the negotiation request continues down the list to the next-highest priority map until a match is made.
5. In **Name**, enter a name for the dynamic map.
6. Select the **Dynamic map** check box.
7. In **Transforms**, select an existing transform to edit it, or click **+** to open the **New Transform** section.
8. From the **Encryption** drop-down list, select one of the listed encryption types
9. From the **Hash** algorithm drop-down list, select one of the listed hash types
10. Click **Submit**.
11. In **Lifetime(seconds)**, enter a value of 28800 seconds to define the lifetime of the security association for the dynamic peer.
12. In **Lifetime(kilobytes)**, enter a value in kilobytes to define the lifetime of the security association for the dynamic peer.
13. Click **Submit**.
14. Click **Pending Changes**.
15. In the **Pending Changes** window, select the check box and click **Deploy changes**.

To avoid any issues, it is recommended that the following command can be used under the crypto-local ipsec-map to force tunnel mode to be the only option offered. However, it is not necessary with the above configuration.

```
force-tunnel-mode
```

2.2.6 RSA, ECDSA, PSK Authentication

VIA supports both RSA and ECDSA certificates. Loading of certificates onto the controller for both authentication to peers and for verification of other peers is described in the User Guide. Minimally, both a "server certificate" and a "trusted root CA" certificate must be loaded onto the controller in order to perform IPsec operations. Once these certificates are loaded on the controller, configure them for use in IPsec. For configuration of the Authentication Profile, please see:

- https://www.arubanetworks.com/techdocs/VIA/4x/Content/VIA%20Config/aos-cli.htm
- https://www.arubanetworks.com/techdocs/VIA/4x/Content/VIA%20Connection%20Manager/vpn-server-add-delete.htm
- https://support.hpe.com/hpesc/public/docDisplay?docId=a00097855en_us

VIA authentication profile has two parts of configuration:

- VIA user role - It is assigned to the users who successfully authenticate through their VIA client. The user role defines the access rights of the users that connect using VIA.
- Authentication server group - It is a collection of servers that are used for authentication. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have different types of authentication servers

The following flexible authentication methods are supported in the VIA solution

- Tunnel authentication options: PSK or digital certificate
- User authentication options: Username/password, token, or digital certificate

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection profile contains all the details required for the VIA client to establish a secure IPsec connection to the VPNC. A VIA connection profile also defines other optional parameters. Such optional parameters can be client autologin, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

VIA supports IKE pre-shared keys, when certificates are not used for authentication. To use these, create an IKE policy that uses pre-shared keys, then enter the pre-shared key mapped by client IP address. When configuring the pre-shared key, the administrator must ensure that the PSK is at least 22 characters with a maximum length of 256, contains at least one uppercase character, one lowercase character, one special character, and one digit. Allowable special characters are: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')'.

For configuration of Pre-shared Key Authentication:

1. On a standalone controller or in the Managed Network hierarchy on Mobility Conductor, 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.

More information on authentication features for VIA can be found here: https://www.arubanetworks.com/techdocs/VIA/4x/Content/VIA%20Config/PSK.htm

2.3 Certificate Checking

To properly configure certificates and implement validation checking on the authentication step, the security administrator must ensure in compliance with Enterprise Security Policies that the server certificate is loaded with the full chain (e.g. Root, Intermediate, Leaf).

The following steps should be followed to upload certificates for VIA:

1. 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. Select the format of the certificate from the **Certificate format** drop-down list.
7. Select **TrustedCA** or **ServerCert** from the **Certificate type** drop-down list.
8. Click **Submit**.
9. Select **Pending Changes**.

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

To select a server certificate for certificate-based authentication:

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

NOTE: Ensure that ‘Validate Server Certificate’ setting is enabled in the VIA connection profile.

NOTE: For compliance, certificates should be uploaded as a bundle (chain certificate) to ensure checking of the full certificate chain.

To ensure that the certificate DN is checked during the IPsec session establishment, the following command can be used:

```
(config) #aaa authentication via connection-profile "cert-via-conn-prof"
```

```
(VIA Connection Profile "cert-via-conn-prof") # dn-profile [CN <entry> | ORG <entry> | OU <entry> | Country <entry>]
```

2.4 Self-Tests

The VIA client performs known answer power on self-tests (POST) on its cryptographic algorithms to ensure that they are functioning correctly. The VIA client utilizes the Aruba VIA Cryptographic Module (AVCM) library which implements known answer tests on its cryptographic algorithms to ensure they are working correctly. These known answer tests involve using the ACCM library functions to encrypt blocks of data and comparing the resulting encrypted block of data to a block that is known to be correct. The result of encrypting a block of data is the same every time if the encryption library operates properly. These tests cover the following algorithms, known answers tests, and pairwise consistency tests:

- AES-GCM - 128-bits, 256-bits
- AES-CBC - 128-bits, 256-bits
- SHA-1, SHA-256, SHA-384
- HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384,
- RSA Pairwise Consistency Test
- RSA Encrypt/Decrypt Known Answer Test,
- DSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test,
- ECDH Pairwise Consistency Test,
- DH Pairwise Consistency Test, and
- FIPS 186-2 RNG Known Answer Test

On Windows and Linux platforms, the VIA client also runs an integrity test on the cryptographic module at startup. The Android version (through the OS platform) runs an integrity test on the entire application at startup.

If any power-on self-tests fail, the application will fail to start. The log file in the application directory will also record a message if the self-tests succeed or fail. This can be used to confirm that the reason for the application fails to start is due to the self-tests. The following are the debug messages for successful and failed self-tests.

- Windows:
  - Success: “FIPS Powerup Self Finished Successfully”
  - Failure: “FIPS_powerupSelfTest() failed error <code>”
- Android:
  - Success: “Finished Mocana initialization...”
  - failure: “Mocana initialization error <code>”
- Linux:
  - Success: “Power up self test passed...”
  - Failure: “!!ERROR!! :Power up self test failed: <error code>”

In the event of a self-test failure, uninstall and reinstall the VIA client. If the issue persists, contact Aruba support.

2.5 Software Updates

Note: VIA 4.x does not support downgrading to VIA 3.x.

The VIA client can automatically update to newer versions of the VIA client software when the update is made available by the administrator. Please note that VIA software for Android devices is managed by the Google application stores and can’t be pushed using the VIA automatic update feature. This feature is enabled by default and can be disabled by unselecting the Allow client to auto-upgrade option in the VIA connection profile.

Windows Clients can be auto upgraded using installation files uploaded on the controller or using an or external downloadable URL. Linux clients can be auto upgraded using external downloadable URL only.

External Downloadable URL

Linux and Windows clients can automatically upgrades their VIA software from a URL defined in the VIA external download URL field in the VIA Connection profile. This option is available for Linux and Windows clients.

when you enter a URL into the VIA external download URL field, use the following folder structure

- For a VIA version file: <External URL>/via_version.txt
- For one or more ansetup files: <External URL >/ansetup

VIA for Linux looks for http://hostname/ip/via/via_version.txt and VIA for Windows looks for http://hostname/ip/via/via_version.xml file from the upgrade server. VIA also fetches /ansetup-* url download the installation binary subsequently.