

Ivanti Secure Access Client Mobile Feature Guide

22.5R1 build: 25375

Contents

Feature List for Release 22.5R1	2
Enhanced Host Checker validation	2
Enhanced user experience for nZTA connections	2
Add Connection	2
Delete a Connection	3
Derived Credential Support	4
Introduction	4
Supported Platforms	4
Configuration of derived credentials	4

Feature List for Release 22.5R1

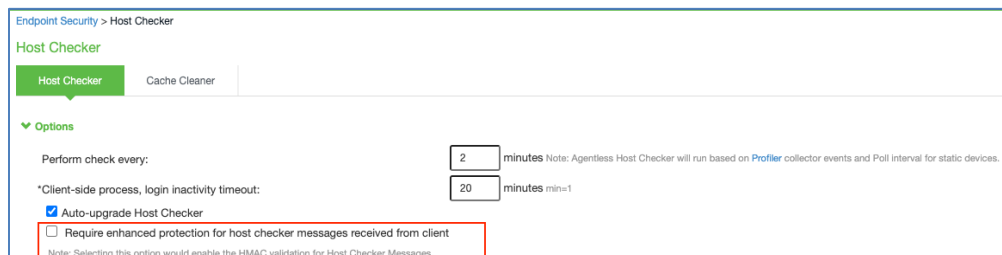
The following table lists features as applicable to Release 22.5R1

Feature Name	Description
Enhanced Host checker validation	An option for admin to enable enhanced host checker validation for an ISAC connection.
Enhanced user experience for nZTA connections	Ivanti Secure Access client allows to enroll and add a nZTA connection using "Add Connection" or delete a connection like other VPN connections.
Derived credential support	This feature provides certificate-based authentication support for VPN profiles where certificates are installed and managed by another application instead of physical smart cards. Note: Use Ivanti Neurons for MDM (Ivanti EPMM and Ivanti MDM) and Entrust application as certificate provider.

Enhanced Host Checker validation

This feature allows the admin to set enhanced protection for the Host Checker messages for ISAC connection from endpoints.

In the ICS **Admin Console** > **Endpoint Security** > **Host Checker**, enable **Require enhanced protection for host checker messages received from client** to notify the end user when host checker validation fails.



Enhanced user experience for nZTA connections


On installing Ivanti Secure Access Client, the user can configure a nZTA connection using the same process used for other, existing connections (VPN Connections). To create an nZTA connection, compatible Ivanti Secure Access Client versions offer a specific connection type: "ZTA".

The tenant administrator must supply the nZTA enrollment URL to their users to create the new nZTA connection.

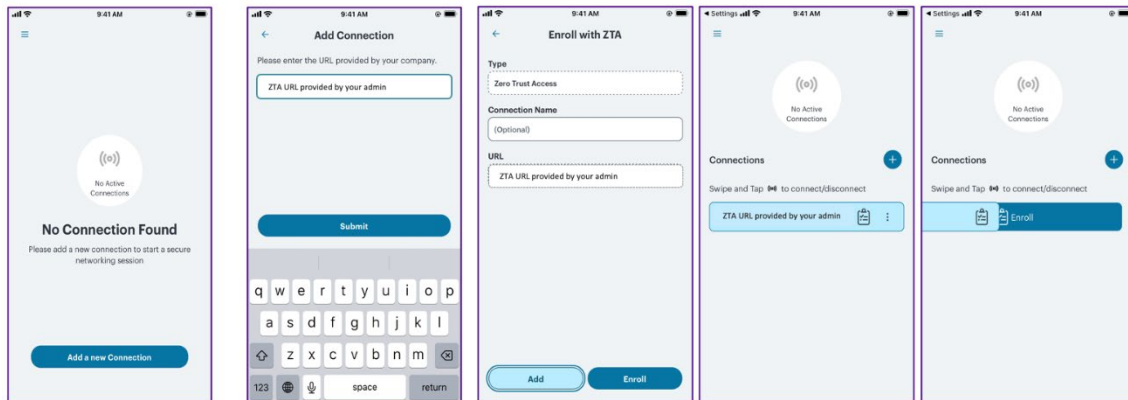
Note: For Mobile Application users, when using default enrolment URL, ensure you omit "/enrol" at the end of the URL.

Add Connection

To add a new nZTA connection:


1. Click . Enter the enrollment URL. The Add Connection dialog box opens.
2. Enter the enrollment URL and click Submit.
3. The network type auto populates as Zero Trust Access.
4. For Name, specify a descriptive name for this connection. The name you specify appears in the Ivanti Secure Access Client interface.

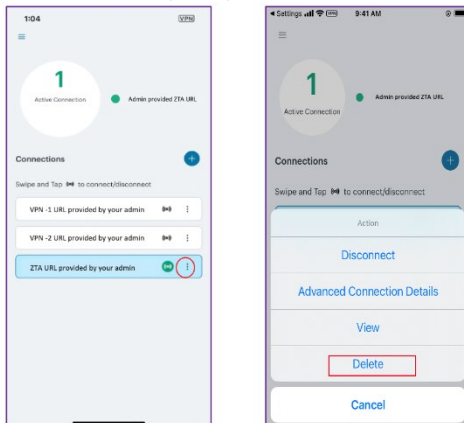
- For Server URL, specify the network that you want to connect to. Enter the nZTA controller URL as provided by the administrator.
- Click **Add** to save your new connection and the connection displays in the Home page. Click **Enroll** to add the connection and initiate a connection to the network.
- On Home page, swipe the connection to Enroll and initiate a connection to the network. Enter the credentials to complete the connection.



Delete a Connection

To delete an nZTA connection:

- Click the connection to select it.
- Select  and select **Delete**.
- Confirm to the prompt to delete the connection.



Derived Credential Support

Introduction

This feature provides certificate-based authentication support for classic L3 VPN profiles where certificates are installed and managed by another application. These applications install digital certificates in device keystore for Android, or the MDM appconfig for iOS, and replace the need of physical smartcards for authentication.

Note: Ivanti secure Access Client 22.5R1 supports Ivanti Neurons for MDM (Ivanti EPMM and Ivanti MDM) and Entrust application as certificate provider.

Supported Platforms

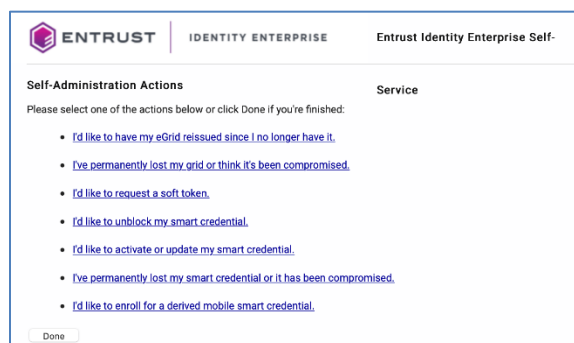
- Ivanti Secure Access client 22.5.0
- PIV-D manager application
- Ivanti Mobile@Work 8.6/ Ivanti Go 3.1 for core and cloud respectively
- iOS 14 / Android 10 onwards

Configuration of derived credentials

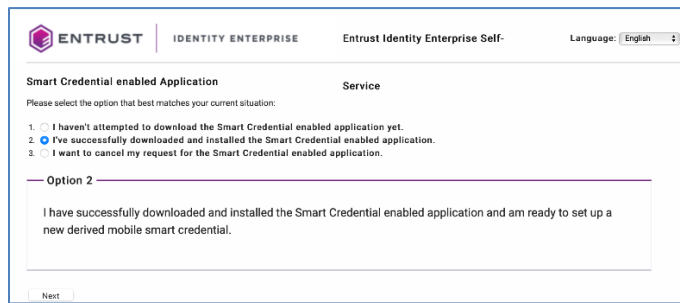
1. Admin can configure the CA root certificates, and the User certificates provided by the vendor in the MDM.

<input checked="" type="checkbox"/>	VPN APP	APPCONFIG	net.pulsesecure.pul...
<input type="checkbox"/>	_W@W Piv-D Config hardcoded	WEB@WORK	com.mobileiron.ent...
<input type="checkbox"/>	-Entrust_Root	CERTIFICATE	
<input type="checkbox"/>	-Entrust-brand	CERTIFICATE ENROLLMENT	
<input type="checkbox"/>	-Entrust-ISSUER	CERTIFICATE	

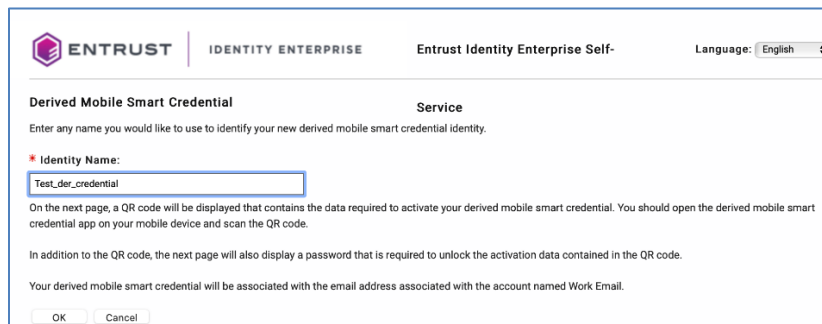
2. Admin to add appconfig policy to config ISAC client details in the MDM.
3. Admin installs corresponding CA root certificates on ICS for cert chain validation.
4. End user to enroll to MDM to fetch the appconfig policy.
5. End users can browse the [Entrust portal](#) and select ***I'd like to enroll for a derived mobile smart credential.***



6. In the next screen, select the option ***I've successfully downloaded and installed the Smart Credential enabled application.*** and click Next.



7. Enter the name for the derived credential and click OK.



8. A QR code displays, use the PIV-D Manager application to scan and enter the password to install the certificates.
For iOS, the certificates are installed in the MDM.
For Android, the certificates are installed in the Android Keystore.
9. On iOS, ISAC fetches the user certificate from MDM client application.
On Android, a pre-defined alias is auto selected under Choose certificate. Click Select and continue when prompted.

