Ivanti Secure Access Client Mobile Feature Guide

ISAC Release 22.2.1-22.7.3

Contents

Feature List for Release 22.X

The following table lists the features applicable to Release 22.X.

Feature Name	Description
Release 22.7.3	
Play Integrity for Android	The Play Integrity API makes host checking of the device more robust. This feature helps you to check that interactions and server requests are running on a genuine Android device.
Conditional Access on iOS ISAC client	Conditional access feature allows to use identity-driven signals as part of the access control decisions.
Release 22.6.1	
Integrating NMDM with nZTA	This feature supports the compliance check for mobile devices during log-in and application access. For detailed information, refer to Integrating Ivanti Neurons for MDM with nZTA.
Release 22.5.1	
Host Checker validation	An option for admin to enable enhanced host checker validation for an ISAC connection.
Enrolling 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.
Release 22.4.1	
Device validation support for VoD and Per-App VPN	Ivanti Secure Access Client for Mobile supports Pre-Auth device ID validation with Ivanti Neurons for MDM (previously MobileIron Cloud) and Ivanti Endpoint Manager Mobile (previously MobileIron Core). This feature requires ICS server running 9.1R18 and above.
Release 22.3.1	
Dark theme support	Ivanti Secure Access Client supports dark theme.
Updated voice over support	supports voice over.
UI mode switching	allows Ivanti Connect Secure to switch client UI mode between Classic and New-UX.
Release 22.2.1	
Device ID Validation	This feature allows you to read UDID from MDM application configuration and pass to Ivanti Connect Secure. On validation, Ivanti Connect Secure initiates authentication.
Host Checker support on ChromeOS (Android)Host Checker support on ChromeOS (Android)	Ivanti Secure Access Client for Mobile Android supports Host Checker on ChromeOS.
Host Checker support for VoD and Per-App VPN (Android)	Ivanti Secure Access Client for Mobile Android supports Host Checker for on-demand connections.

Play Integrity for Android

The Play Integrity API makes host checking of the device more robust. This feature helps you to check that interactions and server requests are running on a genuine Android device.

For detailed information, refer Overview of the Play Integrity API.

This feature is qualified for ISAC new-UX only.

Ensure you follow the steps to enable Play Integrity feature.

1. Ensure you have a Google account or create one.
2. Create a Google Cloud project and extract Google Project number.
3. Enable "Google Play Integrity API" from the "API and Services"
   Refer to https://developer.android.com/google/play/integrity/setup#set-google-cloud .

1. Create Key from Service Account from "IAM & others". Refer
   https://cloud.google.com/iam/docs/keys-create-delete .
2. Assign role as "owner", create Key (JSON format only), and save the key
   Note: Key can be downloaded only once. In case the key is lost, remove the existing key and create another key.
3. If in a customer environment, the total number of connection requests per day (number of endpoints X number of connection) exceeds 10K, admin can request for connection quota extension through https://support.google.com/googleplay/android-developer/contact/piaqr.
   Contact Ivanti Support if any information is required to proceed with this request.

On the ICS server, an admin can enable this feature under **System** > **Configuration** > **Mobile**. Enter the Project Number and Upload the JSON key. For more information, refer to ICS Admin Guide.

Conditional Access on iOS ISAC client

Conditional access feature allows to use identity-driven signals as part of the access control decisions. Conditional Access brings signals together, to make decisions, and enforce organizational policies. This feature allows administrators to restrict access to approved client apps using Intune app protection policies.

For detailed information refer What is Conditional Access in Microsoft Entra ID?

Ensure you follow the steps to enable Conditional Access feature.

1. Configure a SAML cloud app on Azure IdP and Ivanti Connect Secure. See, Deploying a BYOD Policy for Microsoft Intune Managed Devices (ivanti.com) and Client application configuration
2. Create Device Feature policy configuration in Intune MDM under **Devices** > **Manage devices** > **Configuration** > **Create** > **New policy**.
3. Under Device feature configuration edit “Single sign-on app extension configuration and add below three key value pairs.

Field	Value	Value Type
browser_sso_interaction_enabled	1	Integer
AppAllowList	net.pulsesecure.pulsesecure	String
disable_explicit_app_prompt	1	Integer

4. Configure conditional access policy, See Plan a Microsoft Entra Conditional Access deployment
    1. Create Conditional access policy on Azure IdP:
    2. Select the user to apply the policy:
    3. Select the target resource:
    4. Choose conditions. Select Device platform as iOS for iOS devices,
    5. Select Client apps as **Browser**, mobile devices use browser for login.
    6. Block or grant access to the resources based on the above conditions and device compliance state.

Identity based restriction is configured from MDM, Conditional access policy gets applied based on the compliance state fetched from Intune MDM.

Integrating NMDM with nZTA

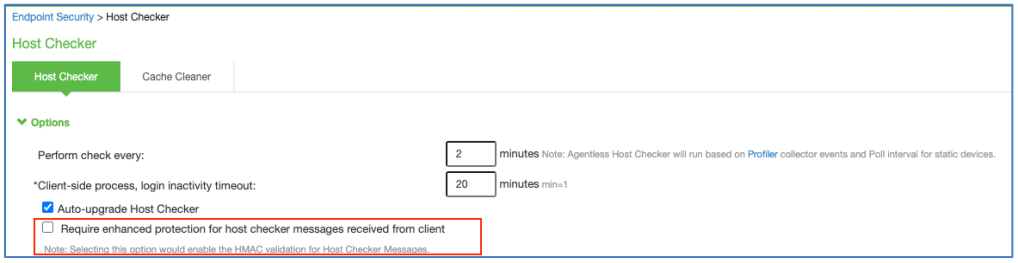
This feature supports the compliance check for mobile devices during log-in and application access.

For detailed information, refer to Integrating Ivanti Neurons for MDM with nZTA.

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.



Enrolling 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: “Zero Trust Access”.

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

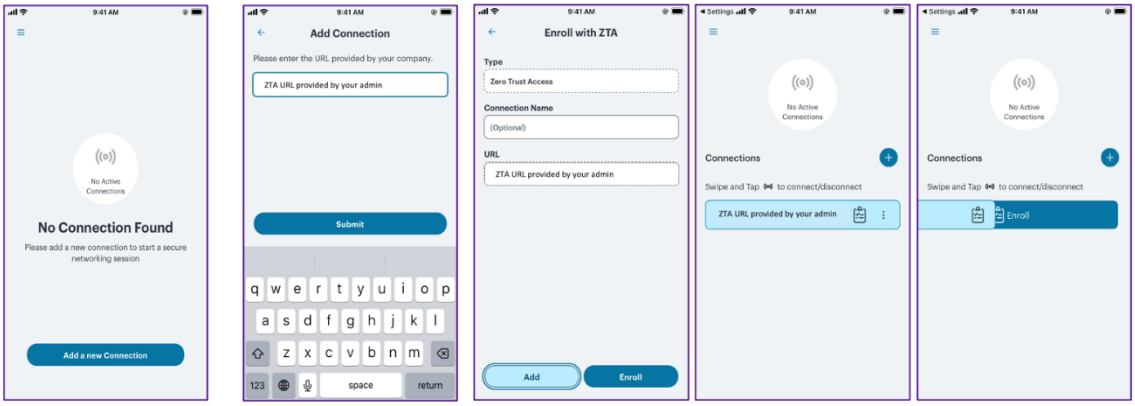
> **Note**: For Mobile Application users, when using default enrolment URL, ensure you omit “/login/enrol” at the end of the URL.

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.
5. For Server URL, enter the nZTA controller URL as provided by the administrator.
6. Click **Add** to save your new connection and the connection displays in the Home page. Click **Enroll** to initiate the enrollment to nZTA.

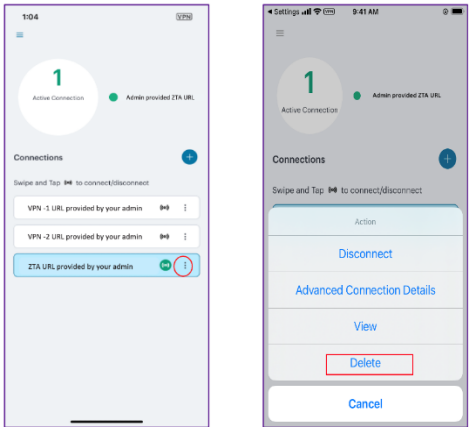
7. On Home page, swipe the connection to Enroll and initiate a connection to the network. Enter the credentials to complete the connection.



Delete a Connection

To delete an nZTA connection:

1. Click the connection to select it.
2. Select ⋮ and select **Delete.**
3. 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.

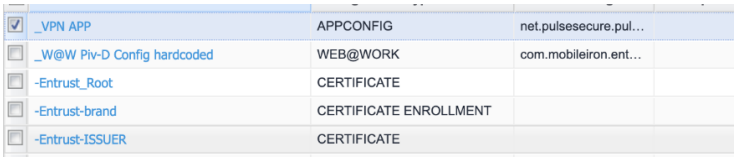
Note: Ivanti secure Access Client 22.5R1 supports Ivanti Neurons for MDM (Ivanti EPMM and Ivanti MDM) and Entrust application as certificate provider.

Supported Platforms

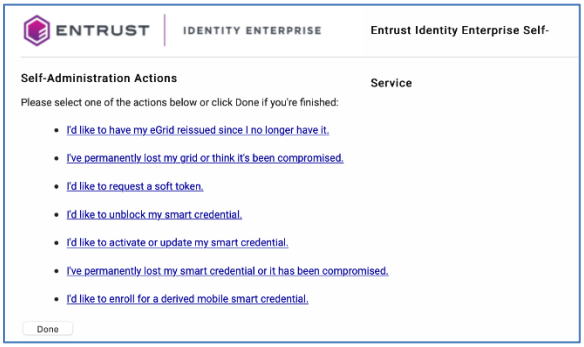
- Ivanti Secure Access client 22.5.1
- PIV-D manager application
- Ivanti Mobile@Work 8.6/ Ivanti Go 3.1 for core and cloud respectively
- iOS 14 / Android 10 onwards

Configuration of derived credentials

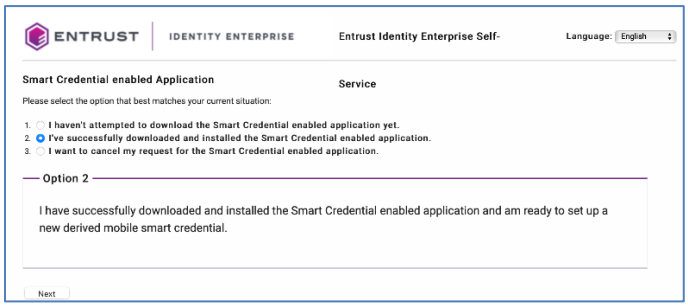
1. Admin can configure the CA root certificates, and the User certificates provided by the vendor in the MDM.



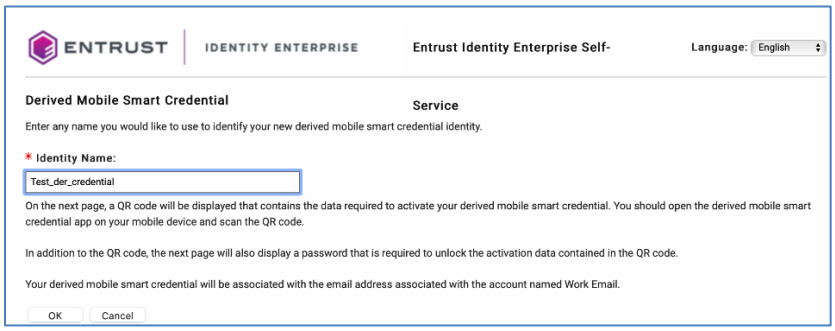
2. Admin to add appconfig policy to config ISAC client details in the MDM.
3. Admin installs corresponding CA root certificates on ICS for cert chain validation.
4. End user to enroll to MDM to fetch the appconfig policy.
5. End users can browse the Entrust portal and select ***I'd like to enroll for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



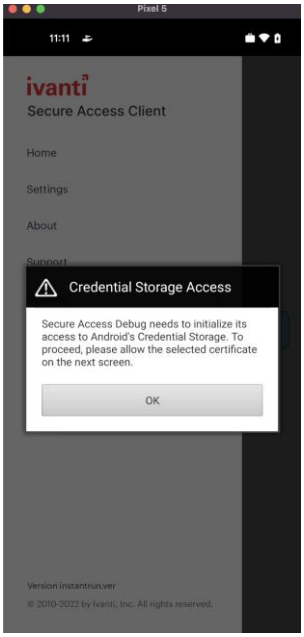
6. In the next screen, select the option ***I've successfully downloaded and installed the Smart Credential enabled application***. and click Next.

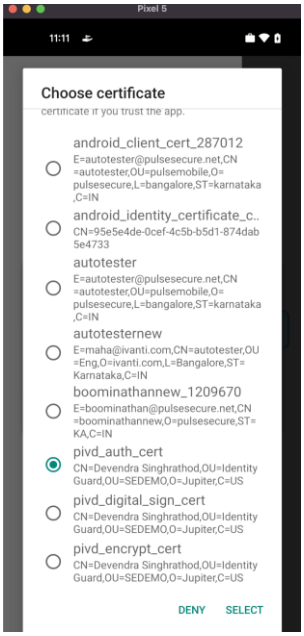


7. Enter the name for the derived credential and click OK.



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.





Device validation support for VoD and Per-App VPN

Android ON-Demand VPN

Apps can be configured to automatically connect to VPN when they are launched. This feature is intended to be used only within the Android work profile since it is predominantly being used at an app level and only Enterprise Mobility Management (EMM) is aware of the apps in the work profile. Using this feature, only the corporate-managed apps will transfer the data over the VPN and the employee's other personal data like personal web browsing, and connections to gaming and social networks will not use the VPN.

When the VPN On Demand profile is applied to the device, VPN will be started automatically in the following two conditions:

- When the applications are launched.
- When the application sends traffic in the background.

In VPN On Demand, a blocking interface is set up on the device which monitors the configured apps for the network traffic. Whenever an application whose network access type is require VPN, tries to perform any network activity, the blocking interface detects this. It thereafter authenticates the user, tears down the blocking interface, and establishes the VPN connection.

EMM Configuration

The configuration needed to be enabled on EMMs. Following Parameters should be configured by the EMM Vendor to set up a VPN On-Demand profile:

Parameters	Value
AppVPN Action	0 (To allow) 1 (To deny)
AppVPN Packages	CSV for package identifiers to Allow/Deny eg. com.chrome.android, com.android.dropbox
Authentication Type	1 (Certificate Based)
Certificate Alias	The client certificate alias
Profile Name	Any
Route Type	1 (Per App)
URL	ICS URL
VPN Trigger Type	1(On Demand)

VPN On Demand Limitations

- No Support for FQDN based Split Tunneling.

Dark theme support

Ivanti Secure access client supports Dark mode or bright mode as per mobile settings.

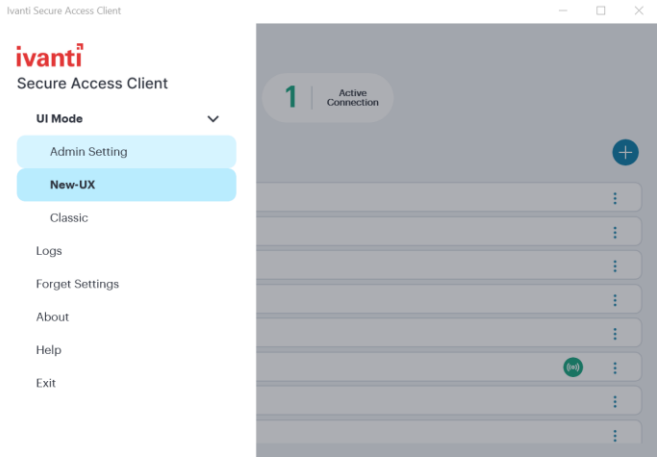
Updated voice over support

Ivanti Secure Access Client supports voice over instructions as per mobile settings.

UI mode switching

Ivanti Secure Access Client supports switching between classic UI and New-UX.

Use Menu and UI mode to switch between the modes.



Device ID Validation

This feature allows to read Unique Device ID (UDID) from MDM application configuration and pass to Ivanti Connect Secure. On validation, Ivanti Connect Secure initiates authentication.

Host Checker support on ChromeOS (Android)

Ivanti Secure access client supports Host Checker on ChromeOS devices running Android.

Host Checker support for VoD and Per-App VPN (Android)

Ivanti Secure access client supports Host Checker for VoD and Per-App VPN Android devices.