Hypori Halo Client User Guide

Common Criteria Configuration and Operation

Version 4.3

Acknowledgments

Hypori uses open source and copyrighted third-party software as part of its Hypori Halo Client product. Copyright information, licensing agreements, and general acknowledgments for third-party software usage are listed in separate documents, which are available on request. Contact your Hypori representative for more information.

Contents

1 Introduction and System Overview

Welcome to the *Hypori Halo Client User Guide – Common Criteria Configuration and Operation*. This section describes the Hypori Halo Client experience for users who connect to a Hypori Virtual Device through the Hypori Halo Client. It also provides a brief overview of the Hypori system.

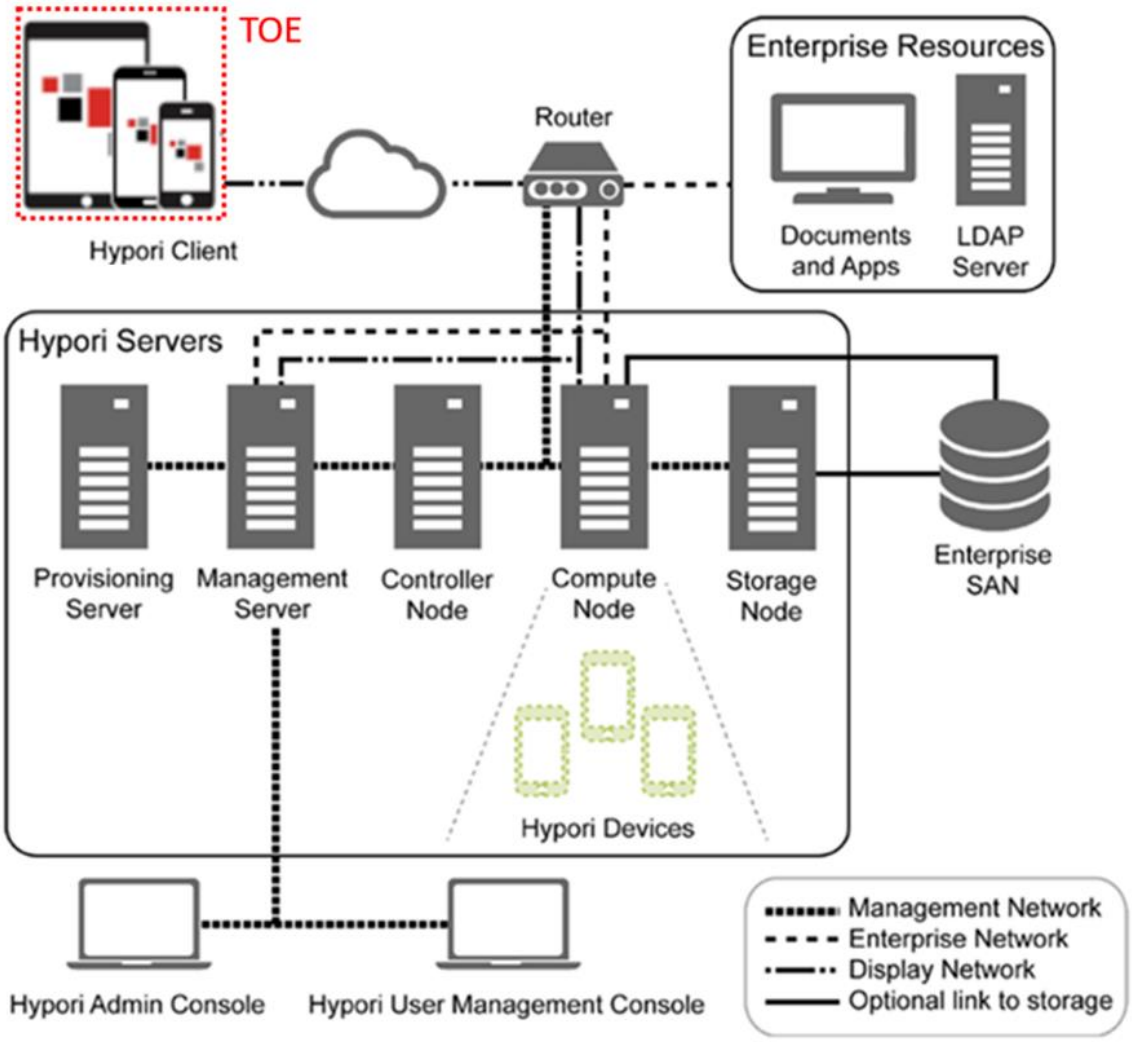
The Hypori Server hosts virtualized devices in the cloud, providing access to these devices through the Hypori Halo Client app on your device. The following diagram shows how these Hypori components interact.

1.1 Hypori Platform Overview

The Hypori Halo Client is an application that only communicates with the Hypori Virtual Device on which are virtual Android devices running on a server Hypori server in the cloud. The Virtual Device contains the operating system, data, and applications, and it uses TLS 1.2 encryption to communicate securely with the Hypori Client.

The Hypori Virtual Device, applications running on the Hypori server, the platform device on which the Hypori Halo Client is installed are not included in the Target of Evaluation (TOE) boundary. Any functions not specified in this security target are outside the scope of the TOE.

The following diagram illustrates the Hypori system, including its components and networks. Unlike many software solutions, some of the Hypori servers are installed on virtual servers while others are installed on physical servers.



The Hypori system includes:

- **Hypori Client:** A thin client that installs on the user's device and communicates with the Virtual Device on the server through secure encrypted protocols.
- **Hypori Device:** An Android-based virtualized version of the user's device.
- **Hypori Servers:** The cloud server cluster that hosts the Hypori Virtual Devices.
- **Hypori Admin Portal:** A web app used to manage the Hypori system.
- **Hypori User Management Console:** A web app used to manage users within a domain.

The Hypori Virtual Device, Servers, User Management Console, and Admin Console are not included in the evaluation.

2 Common Criteria Evaluation

Hypori has evaluated the security features of the Hypori Halo Client version 4.3 under the Common Criteria Evaluation and Validation Scheme (CCEVS). The evaluation demonstrates that the Hypori Halo Client conforms to the security requirements specified in *Protection Profile for Application Software* v1.4 when installed and operated in accordance with the *Hypori Halo Client (Windows) 4.3 Security Target*, *Hypori Halo Client (iOS) 4.3 Security Target* and the *Hypori Halo Client (Android) 4.3 Security Target*. CCEVS has posted the results of the evaluation to the National Information Assurance Partnership (NIAP) Product Compliant List (https://www.niap-ccevs.org/Product/index.cfm).

The posting includes the validation certificate, CCEVS Validation Report, Security Target, and applicable guidance. Note that the functionality described in this guidance documentation is limited to the security functionality described in the Security Target. Other product functionality is not applicable to the claimed Protection Profile and was therefore not examined as part of the Common Criteria evaluation of the Hypori Halo Client product.

The evaluated configuration also includes several assumptions and requirements that must be met by the intended environment in order for the installed Hypori Halo Client 4.3 to be in the evaluated configuration. These are as follows:

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

3 Guidance Documentation

This Common Criteria guidance covers the Hypori Halo Client mobile devices running Android versions 12, or 13, and mobile devices running on iOS versions 15 or 16. The Windows-based Hypori Halo Client application installs on an end user's desktop computer, Surface tablet, or laptop that runs Windows 10 or 11. No configuration is required to use the supported cryptographic algorithms and key strengths since Hypori supports the same ones provided by the platform.

The Hypori Halo Administrator Guide is referenced in Section 5 to provide an example of how an administrator configures the Hypori Halo Client policies.

Information about Hypori and the Hypori product and its components can be found at http://www.hypori.com.

4 Required Permissions

4.1 Android Permissions

The Hypori Halo Client for Android requires permission for installation. The following permissions are requested during the Client installation on Android devices:

- Access Network
- Read phone status and identity
- Call phone
- Take pictures and videos (Camera)
- Record audio (Microphone)
- GPS and network-based location
- Add, and remove accounts and set passwords
- Access and change network state
- Access Wi-Fi connection state information
- Retrieve running apps
- Change audio settings
- Read and enable/disable sync settings
- Install/uninstall shortcuts
- Prevent device from sleeping
- Receive boot completed
- Full network access
- Enable Bluetooth connections
- Use fingerprint/touch ID
- USE_BIOMETRIC
- Access flashlight
- Enable vibrate
- POST_NOTIFICATIONS
- com.google.android.c2dm.permission

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted when the permission is first needed. In some cases, user must enable the permission manually if it is required.

A brief summary that describes how these Android permissions are used is given in the following subsections.

4.1.1 Access Network

The Hypori Halo Client must access networks to communicate with the Virtual Device. It can use any of the provided networks (WiFi, 5G/LTE, 4G/LTE) when they are active.

4.1.2 Read phone status and identity

The Hypori Halo Client uses the call information (specifically signal strength) on the mobile device to pass to the Virtual Device so that the information is displayed in the status bar of the Virtual Device.

Read only access to phone state, including the phone number of the device, current cellular network information, the status of any ongoing calls.

The READ_PHONE_STATE is used to make a call to the OS to determine the type of mobile data connection (WiFi or Cellar Network) to be used by the phone.

4.1.3 Call phone

The Hypori Halo Client can initiate a voice call, bypassing the Dialer interface to confirm the call.

4.1.4 Take pictures and videos (Camera)

The Hypori Halo Client provides remote access to the device's camera to multimedia apps that use the camera in the Virtual Device or to set up your account using the QR code.

4.1.5 Record audio

The Hypori Halo Client provides access to the device's microphone to enables voice recording and phone apps in the Virtual Device.

4.1.6 GPS and network-based location

The Hypori Halo Client provides access to the GPS sensors and the Wi-Fi location services of the mobile device for authentication with the Hypori server and for apps in the Virtual Device that require these services.

4.1.7 Add, remove accounts and set passwords

The Hypori Halo Client uses the Android Account Manager APIs to manage Hypori Halo Client accounts on the mobile device.

4.1.8 Access and change network state

The Hypori Halo Client accesses the state of the cellular network interface to determine connectivity, capture statistics, and state that can be communicated to the Virtual Device so that network information can be displayed in the Virtual Device's status bar.

4.1.9 Wi-Fi connection information

The Hypori Halo Client uses the Wi-Fi signal information (specifically signal strength) on the mobile device to pass to the Virtual Device so that the Wi-Fi connection information is displayed in the Virtual Device's status bar.

4.1.10 Retrieve running applications (Deprecated)

As part of the algorithm for detecting compromised devices, the Hypori Halo Client can retrieve the list of running applications to determine if any known root and super user processes are running that indicate a compromised device.

4.1.11 Change audio settings

The Hypori Halo Client can modify audio settings for audio applications running in the Virtual Device.

4.1.12 Read and enable/disable sync settings

The Hypori Halo Client can enable and disable its sync adapter as well as control the polling rate for gathering notifications from the Virtual Device.

4.1.13 Install/uninstall shortcuts

The Hypori Halo Client can install and uninstall application shortcuts to access apps in the Virtual Device.

4.1.14 Prevent device from sleeping

If so configured, the Hypori Halo Client can operate in the background for one minute after the user's phone or tablet has gone to sleep (screen is black). While it is sleeping, it acquires a lock on the Wi-Fi service to keep the Wi-Fi from turning off and disconnecting from the Virtual Device.

4.1.15 Receive boot completed

The receive boot completed permission (run at startup) is used to receive notifications after the system finishes booting up.

4.1.16 Full network access

The Internet permission is required by the Hypori Halo Client to create socket connections to Hypori servers.

4.1.17 Enable Bluetooth connections

The Hypori Halo Client uses the Bluetooth permission to discover and connect to paired Bluetooth devices.

This permission is used by the Hypori Halo Client to provide information about the Bluetooth device connected to the physical device. This is critical for the operation our application. The user is asked if they want to grant this permission to the app and the user can revoke this permission at any time.

4.1.18 Use fingerprint/touch ID (Deprecated)

The Hypori Halo Client uses the fingerprint permission to enable a Biometric Authentication Factor in the form of a fingerprint. The Hypori Halo Client supports biometric fingerprint ID capabilities if the mobile device's underlying platform supports biometric authentication.

4.1.19 USE_BIOMETRIC

The Hypori Halo Client uses the Enable Biometric permission to enable Biometric Authentication Factors.

4.1.20 Access flashlight

The Hypori Halo Client uses the mobile device's flashlight when the Client scans the QR code during the account provisioning process.

4.1.21 Enable vibrate

The Hypori Halo Client uses the mobile device's vibrator to provide silent notification alerts.

4.1.22 POST_NOTIFICATIONS

This permission is used by the Hypori Halo Client to display local notifications in the notification tray.

4.1.23 com.google.android.c2dm.permission

This permission allows the Hypori Halo Client to receive messages sent by the app's service.

4.2 iOS Permissions

The Hypori Halo Client for iOS requires permission to access the mobile device's features and services. The following permissions are required for proper operation of the client for all use cases:

- Background Operation
- Camera
- Location
- Microphone
- Photo Library
- Notifications
- FaceID/TouchID (optional)
- Cellular Data (optional)

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted

when the permission is first needed. In some cases, user must enable the permission manually if it is required.

A brief summary that describes how these iOS permissions are used is given in the following subsections.

4.2.1 Background Operations

The Hypori Halo Client can be configured to receive notifications. The background operations permission is required to receive notifications when the application is not active. To enable this capability, the user must enable the permission in the iOS settings – it is disabled by default.

4.2.2 Take pictures and video (Camera)

The Hypori Halo Client uses remote access to the device's camera to support multimedia applications that use the camera in the Virtual Device. It can also use the camera when scanning a QR code during account provisioning. The user is prompted for access to the camera when the application is first started.

4.2.3 GPS and network-based location

The Hypori Halo Client provides access to the GPS sensors and the Wi-Fi location services of the mobile device for authentication with the Hypori server and for apps in the Virtual Device that require these services. The user is prompted for access to location information when the application is first started.

4.2.4 Audio input (Microphone)

The Hypori Halo Client provides access to the microphone and audio recording capabilities on the mobile device to support apps in the Virtual Device that require audio input. Access to the microphone is requested the first time an application in the virtual device needs to use the microphone.

4.2.5 Access photo library

The Hypori Halo Client supports access to the camera for video recording and taking pictures. This function in iOS requires the application register for permission to access the photo library – iOS will prompt the user for this permission when a photo or video is stored on the device. However, the Hypori Halo Client never stores the photo or video on the device and never attempts to pick and upload a photo or video from the device, thus there should never be a prompt for this permission.

4.2.6 Enable notifications

The Hypori Halo Client uses the mobile device's notifications permission to support notification display features. The user is prompted for permission to post notifications when the application is first started.

Note: End users can enable or disable these permissions from the mobile device's iOS settings app. Some services used by the client (such as Bluetooth) may result in iOS asking the user for

permission, but this is outside of the control of the Hypori Halo Client and thus is not an explicit permission that we request.

4.2.7 FaceID/TouchID

The Hypori Halo Client uses the mobile device's permission to support biometric scanners as an additional option for authentication. Both the server and the client device have to enable this option for it to be usable.

4.2.8 Cellular Data

The Hypori Halo client uses the mobile device's permission to allow the user to set the client to only use Wi-Fi by turning this feature off. If enabled the Hypori Halo client will use either Wi-Fi or cellular data.

4.3 Windows Permissions

The Hypori Halo Client for Windows 10 and 11 requires permission to access the user's desktop computer, Surface tablet, or laptop features and services. The following permissions are required for proper operation of the client for all use cases:

- Internet Connectivity
- Bluetooth
- Bluetooth GATT
- Bluetooth RFComm
- Graphics Capture
- Location
- Microphone
- Private Network Usage
- WiFi Control
- Camera

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted when the permission is first needed. In one case, it must enable the permission manually if it is required.

A brief summary that describes how these Windows permissions are used is given in the following subsections.

4.3.1 Internet Connectivity

The Internet Connectivity permission is required by the Hypori Halo Client to create socket connections to Hypori servers.

4.3.2 Bluetooth

The Hypori Halo Client uses the Bluetooth permission to discover and connect to paired Bluetooth devices.

4.3.3 Bluetooth GATT

The Hypori Halo Client uses the Bluetooth GATT permission for Bluetooth generic attribute profile capabilities.

4.3.4 Bluetooth RFComm

The Hypori Halo Client uses the Bluetooth RFComm permission for Bluetooth data transport via a serial port file transfer.

4.3.5 Graphics Capture

The Hypori Halo Client Graphics Capture permission enables the user to take screen captures when connected to the Virtual Device.

4.3.6 Location

The Hypori Halo Client provides access to the GPS sensors and the Wi-Fi location services on the user's desktop computer, Surface tablet, or laptop for authentication with the Hypori server and for apps in the Virtual Device that require these services.

4.3.7 Microphone

The Hypori Halo Client provides access to the microphone and audio recording capabilities on the user's desktop computer, Surface tablet, or laptop to support apps in the Virtual Device that require audio input.

4.3.8 Private Network Usage

The Hypori Halo Client Private Network Usage permission is used to access Intranet networks that have an authenticated domain controller, or that the user has designated as either home or work networks.

4.3.9 WiFi Control

The Hypori Halo Client WiFi Control permission is used to access the devices WiFi status, including signal strength.

4.3.10 Camera

The Hypori Halo Client uses remote access to the device's camera to support multimedia applications that use the camera in the Virtual Device. It can also use the camera when scanning a QR code during account set up.

5 Controlling Hypori Client Settings

Settings for the Hypori Halo Clients are controlled completely by the Hypori Server using client policies. The administrator defines the Client policies as described in the Hypori Halo Administrator Guide, Version 1.18, 2023, Chapter 6. The TOE will automatically download and update the policies to the Client each time a user authenticates and does not require any client user action. The policy settings control what activities a user can perform on the Client and can be seen from the Accounts screen and tapping the gear icon next to the account name within the Client App. If a particular setting does not show on the client interface, this is because the administrator has not given the user that particular permission. For example, an administrator might decide that they do not want a user to be capable of enabling Bluetooth on their device and therefore they would set the “value” field under “bluetooth-enable” to “false”, "visible" to “false”, and "modifiable" to “false” as shown in the example below. The following is an example of a client policy expressed in JSON, that sets each client setting. The result of this policy is that the user will only be able to access and configure the key account information used by the client to connect to the Hypori Server.

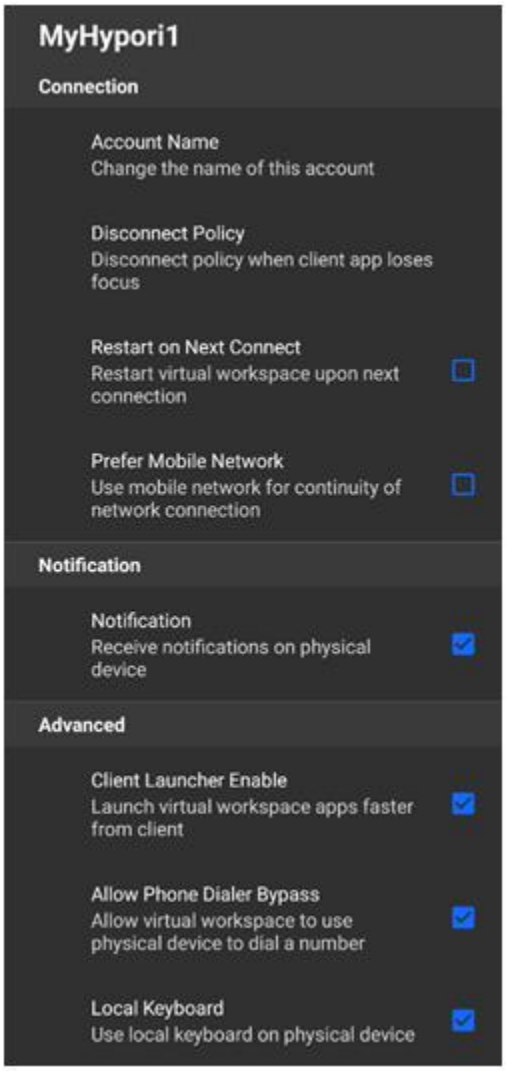
```
{
   "version":{
      "major":2,
      "minor":0
   },
   "system":{
      "client-launcher-border-color":{
         "title":"Client Launcher Border Color",
         "type":[
            "blue",
            "green",
            "orange",
            "red",
            "yellow",
            "none"
         ],
         "value":"none",
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "require-device-admin":{
         "title":"Require Device Administrator",
         "type":"boolean",
         "value":false,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "camera-enable":{
         "title":"Enable Camera",
         "type":"boolean",
         "value":true,
         "platforms":[
            "Android",
```

```
            "iOS",
            "Windows"
         ]
      },
      "screenshots-enable":{
         "title":"Enable Screenshots",
         "type":"boolean",
         "value":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "connect-restart-enable":{
         "title":"Enable Restart on Next Connect",
         "type":"boolean",
         "value":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "push-notifications-enable":{
         "title":"Enable Push Notifications",
         "type":"boolean",
         "value":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "notification-interval":{
         "title":"Notification Interval",
         "type":"number",
         "value":0,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      }
   },
   "settings":{
      "allow-phone-dialer-bypass":{
         "title":"Enable Client Phone Dialer",
         "type":"boolean",
         "value":true,
         "visible":false,
         "modifiable":false,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
```

```
      },
      "use-local-soft-keyboard":{
         "title":"Use Local Keyboard",
         "type":"boolean",
         "value":true,
         "visible":true,
         "modifiable":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "bluetooth-enable":{
         "title":"Enable Bluetooth",
         "type":"boolean",
         "value":false,
         "visible":false,
         "modifiable":false,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "client-launcher-enable":{
         "title":"Use Client Launcher",
         "type":"boolean",
         "value":true,
         "visible":true,
         "modifiable":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "notification-enable":{
         "title":"Enable Notifications",
         "type":"boolean",
         "value":true,
         "visible":true,
         "modifiable":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "disconnect-policy":{
         "title":"Disconnect Policy",
         "type":[
            "immediately",
            "delayed1",
            "keepopen"
         ],
         "value":"delayed1",
```

```
         "visible":true,
         "modifiable":true,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "allow-unsavory-devices":{
         "title":"Allow Compromised Devices",
         "type":"boolean",
         "value":false,
         "visible":false,
         "modifiable":false,
         "platforms":[
            "Android",
            "iOS",
            "Windows"
         ]
      },
      "logging-level":{
         "title":"Log Level",
         "type":[
            "none",
            "error",
            "warning",
            "info",
            "debug",
            "verbose"
         ],
         "value":"warning",
         "visible":false,
         "modifiable":false,
         "platforms":[
            "Android"
         ]
      }
   }
}
```

The following is an example of the default client policy settings that the Hypori Server administrator configured to be accessible by the end user of an Android Client. If desired, the user can tap the settings to change or toggle the values. The interface presentation will be slightly different depending on the client device.



6 Updates and Update Verification

Android

Hypori distributes the Hypori Halo Client as a .APK file for Android devices. A user may obtain the installation package through Google Play or the enterprise IT group of the user. A user obtains Hypori Halo Client updates using the platform's update mechanism or from the user's IT group. Hypori digitally signs the installation package as well as updates with a unique certificate and corresponding private key; and includes the corresponding public key certificate in the package. Android verifies the digital signature on the package using the public key in the certificate. The installation or software update process will only occur if the signature validation is successful. It can be delivered via the Google Play store, MDM, or other enterprise app stores.

If the application is installed using the Google Play Store, it may be updated automatically if your App Store configured to do so. If it is not, selecting the "update" option for the application in the Store application will verify that the application package is valid and install it over the older version.

To verify the version of the Hypori Halo Client, open the Hypori Halo Client, but do not connect to the Virtual Device. On the Hypori Client Accounts screen, select the ellipses menu and click on 'About'. The About screen will display the version number, build information and copyright.

iOS

Hypori distributes the Hypori Halo Client as an .IPA file for iOS devices. A user may obtain the installation package through Apple App Store or the enterprise IT group of the user. A user obtains Hypori Halo Client updates using the platform's update mechanism or from the user's IT group. The Hypori Halo Client (iOS) installation package is signed by Hypori and Apple re-signs it. On iOS devices, iOS will only install a package from the Apple App Store if it has a valid signature from both Apple and the app developer.

If the application is installed using the Apple App Store, it may be updated automatically if your App Store is configured to do so. If it is not, selecting the "update" option for the application in the Store application will verify that the application package is valid and install it over the older version.

To verify the version of the Hypori Halo Client, open the Hypori Halo Client, but do not connect to the Virtual Device. On the Hypori Halo Client Accounts screen, select the ellipses menu and click on 'About'. The About screen will display the version number, build information and copyright.

Windows

Hypori distributes the Hypori Halo Client as a Windows standard .appx file for Windows devices.

The TOE relies on the Windows Store to provide application updates. Updates are automatically handled by the Windows Operating System, so notifications will be given to the user about existing application updates. Hypori digitally signs the installation package as well as updates and includes the corresponding public key certificate in the package. Windows verifies the digital signature on the package using the public key in the certificate. The installation or software update process will only occur if the signature validation is successful. The client is signed with a unique certificate. It can be delivered via the Windows Store or the enterprise IT group of the user.

If the application is installed using a Mobile Device Management (MDM) tool, the MDM tool will be able to push updates to the applications based upon the management policies of the

administrators of the MDM tool. The application installation packages are made available from Hypori using the Hypori support portal at https://hypori.com/support.

To verify the version of the Hypori Halo Client, open the Hypori Halo Client, but do not connect to the Virtual Device. On the Hypori Client Accounts screen, select the ellipses menu and click on ‘About’. The About screen will display the version number, build information and copyright.

7 Provisioning of Hypori Client Credentials

To configure a Hypori Halo Client account, the user receives an enrollment email from the Hypori Halo administrator titled "Your Hypori account is ready". This email contains information needed to add the account as well as the account information including a hostname and port number for the Hypori server, a name for the account, and an email address. The server's URL and port number is specified in the Server Name field using the URL and a colon (i.e. user.hypori.com:7443).

The 4.3 version of the Hypori Halo Client **does not create credentials**. When using the "Add Account" screen with QR code or OTP options, the Hypori Halo Client acquires the user's credentials from the Hypori provisioning server and installs it into the Android Keystore System, iOS keychain, or the Windows Certificate Stores on the platforms and directs the Hypori Halo Client's user to name the account to associate it with the installed credential.

7.1 Android Credential Provisioning

Android provides the Android Keystore System to securely store and use cryptographic keys. The Hypori Halo Client uses the Android Keystore System's APIs to access and authenticate the user to Hypori Servers. There are two primary use models for the Android Keystore System:

1. The system-wide Android KeyChain is used when the user's credentials are to be shared across multiple applications. The credentials are maintained in the underlying system key store and the user or administrator grants access to various applications to access the credentials in the Android KeyChain.

2. The application-specific Android Keystore provider can be used when the user's credentials should not be shared across multiple applications.

There are many possible mechanisms to create and install credentials into the Android Keystore System.

The Hypori Halo Client can be used to contact the Hypori provisioning portal and download the user's credentials and store them into either the Android KeyChain or via the application-specific Android Keystore provider.

Configure the Hypori Halo Client Account using a QR Code

The QR code method to add your account is the easiest means to set up your Hypori Halo account on your physical device.

Prerequisite:

Before you begin:

- Make sure you have received the enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the QR code you need to add your account as well as your account information.
- It is recommended to use a second device, which has access to your onboarding email, to display the emailed QR code, so you can scan it with your phone or tablet.
- Verify your device is using a supported operating system. (Android versions 12, and 13)

Install the Hypori Halo Client app on the mobile phone or tablet you will use to access your virtual workspace. You can install the app through the Google Play Store or in some cases through your

organization's private mobile app distribution service. **Add your account using the QR code method**

1. From your phone or tablet's home screen, tap your Hypori Halo Client icon.

   If this is the first Hypori Halo account on the physical device, your Hypori Halo Client will prompt you for permission to:

   - Access the Camera Tip: This permission is required to complete the QR code setup.
   - Access your Location
   - Send you Notifications
   - Access the Microphone
   - Manage your Phone Calls

2. When you see the Hypori Halo splash screen, tap LET'S GO!

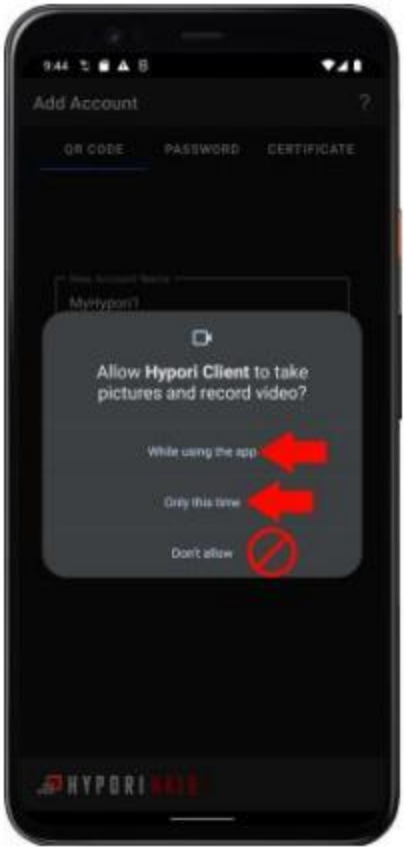
   

3. In the New Account Name field, enter a name for your account, if you want to change the default name.

4. Tap SCAN QR CODE.

   You will see a prompt from your phone or tablet asking permission to allow the Hypori Halo Client access to your physical device's camera.

5. Select either the While using the app or Only this time option.



Tip: To use the QR code setup option, you must have a camera on your phone or tablet, and you must grant the Hypori Halo Client permission to access the camera. If you have already tapped "Don't allow", follow the instructions in Granting Camera Access to the Hypori Halo Client to re-enable the camera.

6. From a second device, open the email titled “Your Hypori account is ready”. You will only need the second device to display the QR code so you can scan it with your phone or tablet.
7. Center the QR code in the camera's view finder.

8. Allow the camera to focus on the QR code. After the image focuses, the camera will automatically scan the QR code and take you to the next screen.
   Your Hypori Halo Client will save your account information and connect you to your virtual workspace.

Configure your Hypori Halo Client using the One-Time Password (OTP) Method

The OTP method of account provisioning is mostly used by users who may have the camera disabled on their physical device. (I.e., the security policies of the organization have resulted in the camera on the physical device being disabled)

Before you begin:

- Make sure you received an enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the credential information needed to complete your account setup.
- Verify that the device is using a supported operating system. The Hypori Halo Client supports Android versions 12, and 13 in the evaluated configuration.
- Install the Hypori Halo Client app on your mobile phone or tablet you will use to access your virtual workspace. You can install the app through the Google Play Store or in some cases through your organization's private mobile app distribution service.

Adding your account using the OTP method:

1. From your phone or tablet's home screen, tap your Hypori Halo Client icon.

If this is the first Hypori Halo account on the physical device, your Hypori Halo Client will prompt you for permission to:

- Access the Camera Tip: This permission is required to complete the QR code setup.
- Access your Location
- Send you Notifications
- Access the Microphone
- Manage your Phone Calls

2. When you see the Hypori Halo splash screen, tap LET'S GO!

3. Tap **Password** under the Add Account banner.
4. In the New Account Name field, enter a name for your account, if you want to change the default name.
5. Populate the remaining fields using the information provided in the "Your Hypori account is ready" email:
    a. Email Address or Login Name
    b. Server Name

c. One-Time Password (OTP)

6. Tap **Next**.

7. Your Hypori Halo Client will save your account information and connect you to your virtual workspace.

Importing a Server CA Certificate

If the certificate chain used for the Hypori server terminates in a well-known root or a corporate-issue CA installed to the device's trust store via alternative means (such as mobile device management), it is not necessary to import the CA certificate. Importing the CA certificate is only necessary when the certificate chain does not terminate in a well-known root CA or a root CA installed via management tools.

1. Obtain the CA file from the administrator (potential file types could include .crt, .cer, .p7c, .p12, or .pem) and download the file to the device.
2. Open the Android Settings application.
3. Using the search function, search for "CA certificate" and select the item titled "Install from device storage".
4. Choose the option to "Install anyway" if a warning screen displays.
5. Navigate the device's file system to find the file downloaded in step 1 and select it.

7.2 iOS Credential Provisioning

iOS provides the Secure Enclave for secure storage of cryptographic keys using the iOS Keychain APIs. Unlike Android, the iOS keychain cannot be shared by non-Apple applications, thus each application can only access their own keys.

The Hypori Halo Client for iOS supports the following means to get the user's credentials into the iOS keychain for its use:

Configure the Hypori Halo Client Account using a QR Code

Before you begin:

- Make sure you have received the enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the QR code you need to add your account as well as your account information in case you are unable to use the QR code and must use the One-Time Password method.
- It is recommended to use a second device, which has access to your onboarding email, to display the emailed QR code, so you can scan it with your phone or tablet.
- Verify your device is using a supported operating system. (iOS versions 15, and 16)
- Install the Hypori Halo Client app on the mobile phone or tablet you will use to access your virtual workspace. You can install the app through the Apple App Store or in some cases through your organization's private mobile app distribution service.

Add your account using the QR code method:

1. From your phone or tablet's home screen, tap your Hypori Halo Client icon.

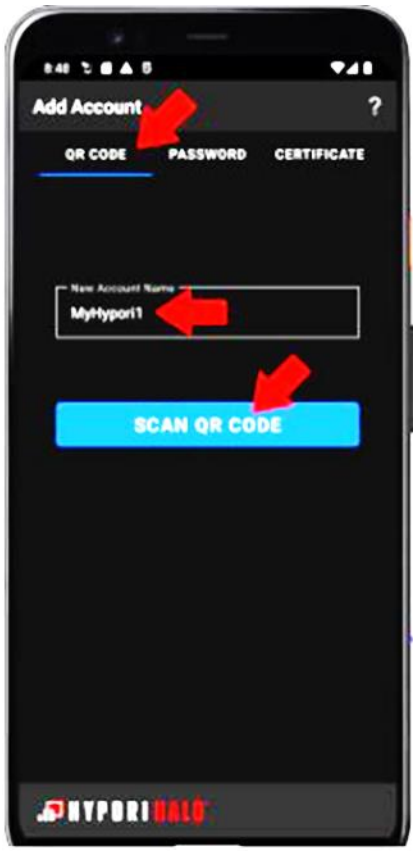
   

   If this is the first Hypori Halo account on the physical device, your Hypori Halo Client will prompt you for permission to:

   - Access the Camera (This permission is required to complete the QR code setup.)
   - Access your Location
   - Send you Notifications
   - Access the Microphone

2. When you see the Hypori Halo splash screen, tap **LET'S GO!**

3. In the Account Name field, enter a name for your account, if you want to change the default name.



4. Tap **SCAN QR CODE**.
5. From a second device, open the email titled "Your Hypori account is ready". You will only need the second device to display the QR code so you can scan it with your phone or tablet.

6. Center the QR code in the camera's view finder.

7. .Allow the camera to focus on the QR code. After the image focuses, the camera will automatically scan the QR code and take you to the next screen.
   The Hypori Halo Client will save your account information and connect you to your virtual workspace.

Configure your Hypori Halo Client using the One-Time Password (OTP) Method

The OTP method of account provisioning is mostly used by users who may have the camera disabled on their physical device. (I.e., the security policies of the organization have resulted in the camera on the physical device being disabled)

Before you begin:

- Make sure you received an enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the credential information needed to complete your account setup.
- Verify your device is using a supported operating system. (iOS versions 15, and 16)
- Install the Hypori Halo Client app on the mobile phone or tablet you will use to access your virtual workspace. You can install the app through the Apple App Store or in some cases through your organization's private mobile app distribution service.

Adding your account using the OTP method:

1. From your phone or tablet's home screen, tap your Hypori Halo Client icon.

   If this is your first account, the Hypori Halo Client will prompt you for permission to:

   - Access the Camera
   - Access your Location
   - Send you Notifications
   - Access the Microphone

2. When you see the Hypori Halo splash screen, tap LET'S GO!

3. Tap Password under the Add Account banner.
4. In the Account Name field, enter a name for your account, if you want to change the default name.
5. Populate the remaining fields using the information provided in the "Your Hypori account is ready" email:

   - Email Address or Login Name

- Server Name
- One-Time Password (OTP)

6. Tap Next.

7. The Hypori Halo Client will save your account information and connect you to your virtual workspace.

Importing a Server CA Certificate

If the certificate chain used for the Hypori server terminates in a well-known root or a corporate-issue CA installed to the device's trust store via alternative means (such as mobile device management), it is not necessary to import the CA certificate. Importing the CA certificate is only necessary when the certificate chain does not terminate in a well-known root CA or a root CA installed via management tools.

1. Utilizing the Safari browser, navigate to a webpage that contains the CA certificate available for download (for iOS, the CA file must be in .crt format).
2. Download the file and select "Allow" when prompted.
3. Proceed to the Settings app and open the item near the top labeled "Profile Downloaded".
4. Select "Install" and enter passcode if prompted. Select "Install" again.
5. Return to the first page of the Settings app. Select "General" and then "About"
6. Scroll all the way to the bottom of the page and select "Certificate Trust Settings".

7. In the list underneath “Enable Full Trust for Root Certificates”, toggle the selector on for the root CA that was downloaded.

7.3 Windows Credential Provisioning

Windows securely stores a CA certificate for the server certificates in the platform’s Windows Certificate Store during installation. (The user need not install a CA certificate when the CA is a platform trusted CA.) All TLS communications require the entire certificate path (in order of leaf, intermediates, and finally the root) to be provided by the server to successfully validate the server’s certificate chain. The TOE builds its certificate chain by recursively retrieving certificates published in the Authority Information Access CA Issuers field of the presented certificate until a trusted root is found or the chain is exhausted. Leaf and intermediate certificates used with the TOE must contain the CA Issuers field and the URI contained within must point to the CA that issued the certificate containing this extension, as specified in section 4.2.2.1 of RFC 5280.

Configure your Hypori Halo Client Account using a QR Code

Before you begin:

- Make sure you have received the enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the QR code you need to add your account as well as your account information in case you are unable to use the QR code and must use either the One-Time Password or Manual Entry methods.
- It is recommended to use a second device, which has access to your onboarding email, to display the emailed QR code, so you can scan it with your phone or tablet.
- Verify your device is using a supported operating system. (Windows 10 and 11)
- Install the Hypori Halo Client app on the Windows workstation, laptop or tablet you will use to access your virtual workspace. You can install the app through the Microsoft Store or in some cases through your organization's private mobile app distribution service.

Add your account using the QR code method:

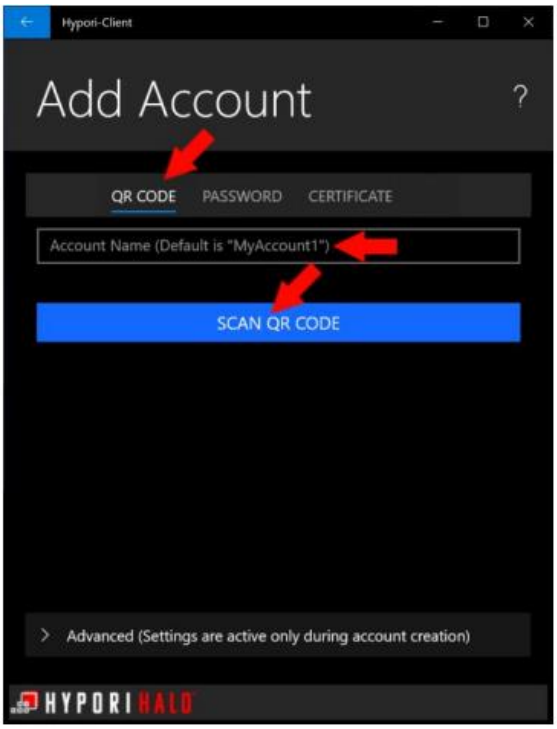
1. Using either the Windows Start menu or the tile, launch your Hypori Halo Client.

   If this is the first Hypori Halo account on the physical device, the Hypori Halo Client will prompt you for permission to:

   - Access the Camera
   - Access the Microphone
2. When you see the Hypori Halo splash screen, click **LET'S GO!**

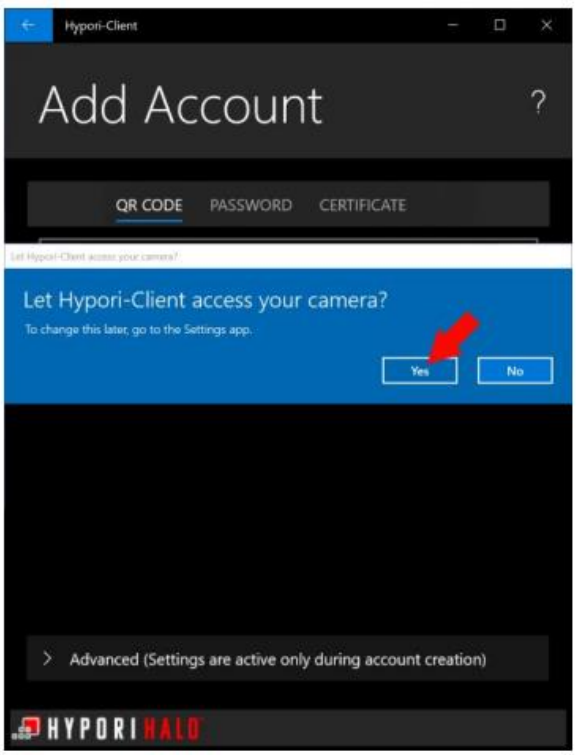
3. In the Account Name field, enter a name for your account, if you want to change the default name.



4. Click **SCAN QR CODE**.

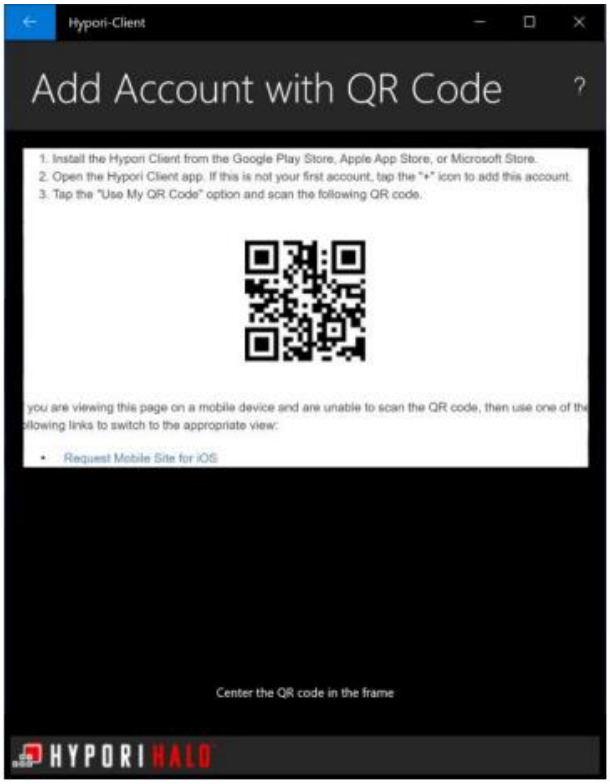
   You will see a prompt from your PC or tablet asking permission to allow the Hypori Halo Client access to your physical device's camera.

5. Select either the **While using the app** or **Only this time** option.



6. From a second device, open the email titled "Your Hypori account is ready". You will only need the second device to display the QR code so you can scan it with your phone or tablet.

7. Center the QR code in the camera's view finder.



8. Allow the camera to focus on the QR code. After the image focuses, the camera will automatically scan the QR code and take you to the next screen.
   The Hypori Halo Client will save the account information and connect you to your virtual workspace.

Before you begin:

- Make sure you received an enrollment email from your Hypori Halo administrator titled "Your Hypori account is ready". This email contains the credential information needed to complete your account setup.
- Verify your device is using a supported operating system. (Windows 10 and 11)
- Install the Hypori Halo Client app on your Windows workstation, laptop or tablet you will use to access your virtual workspace. You can install the app through the Microsoft Store or in some cases through your organization's private mobile app distribution service.

Adding your account using the OTP method:

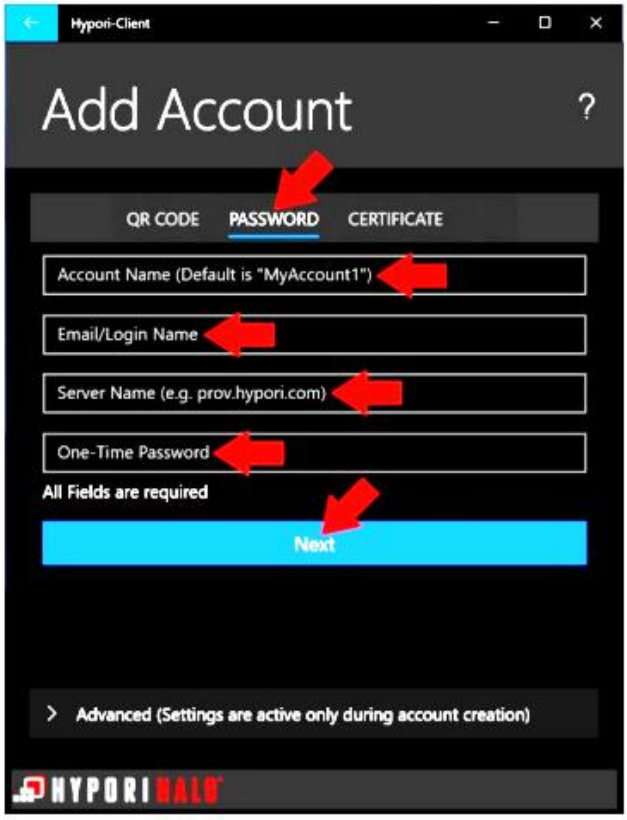
1. Using either the Windows Start menu or the tile, launch your Hypori Halo Client.

   If this is your first account, the Hypori Halo Client will prompt you for permission to:

   - Access the Camera
   - Access the Microphone

2. When you see the Hypori Halo splash screen, click LET'S GO!

3. Tap Password under the Add Account banner.
4. In the Account Name field, enter a name for your account, if you want to change the default name.
5. Populate the remaining fields using the information provided in the "Your Hypori account is ready" email:
    - Email Address or Login Name
    - Server Name
    - One-Time Password (OTP)
6. Click Next.



7. The Hypori Halo Client will save your account information and connect you to your virtual workspace.

Importing a Server CA Certificate

If the certificate chain used for the Hypori server terminates in a well-known root or a corporate-issue CA installed to the device's trust store via alternative means (such as mobile device management), it is not necessary to import the CA certificate. Importing the CA certificate is only necessary when the certificate chain does not terminate in a well-known root CA or a root CA installed via management tools.

1. Obtain the CA file from the administrator (potential file types could include .crt, .cer, .p7c, .p12, or .pem) and download the file to the device.
2. Double-click the file and then click "Install certificate…" near the bottom of the window.
3. The Certificate Import Wizard launches. Select Local Machine in the Store Location. Click allow on the security prompt.
4. Click the button to "Place all certificates in the following store". Click "Browse" and select "Trusted Root Certification Authorities".
5. Click "Next" and review the settings. Click "Finish" if correct.

8 Reference Identifier for TLS

As part of setting up a new account on the Hypori Client, a user may receive enrollment instructions from the Hypori administrator. These instructions may come in the form of a web page or email and contain a link to the Hypori User Provisioning service. The user is provided with a QR code or a One-Time Password (OTP). The provisioning service provides the server hostname, port, and the user's client certificate to the Hypori Client and it generates and installs the client certificate for the account as described in section 7.

The hostname of the server and the client certificate association provided by the provisioning server (or manually provided by the user or administrator) is saved as an account. The account represents the linkage between the user of the client and the particular Hypori server. The server certificate returned when connecting to the Hypori server includes the reference identifier associated with its DNS name and is validated against the hostname as required by the protection profile. The reference identifier in the client certificate is chosen by the administrator from one of several fields in the certificate during server configuration. When the client certificate is presented to the Hypori server, it is validated and the reference identifier is extracted and used to authenticate the user. See the *User Authentication Configurations* section inside chapter 5 of the *Hypori Administrator's Guide – Hypori Halo version 1.18* for how to configure and how to choose the reference identifier used to look up users in the directory server.

9 Verify Version of the Hypori Client

To verify the version of the Hypori Client, open the Hypori Client, but do not connect to the Virtual Device. On the Hypori Client Accounts screen, select the ellipses menu and click on ‘About’. The About screen will display the version number, build information and copyright.

10 Commercial Solutions for Classified (CSfC) Conformance

No configuration is necessary to comply with the CSfC, the restrictions are supported out of the box by default.

The Hypori Halo Clients rely on platform provided cryptography. The following TLS ciphersuites are supported by each platform. For CSfC purposes, Hypori will only use the two ciphersuites cited at the end of this section. These are a subset of ciphersuites CSfC allows and therefore doesn't pose any compatibility issues.

Android

The Hypori Halo Client (Android) was tested on Android 12 and Android 13 platforms.

Android 12

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11239

Google Pixel Phones on Android 12.0

Validation Report Number: CCEVS-VR-VID11239-2022

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

Android 13

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11342

Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 13- Spring

Validation Report Number: CCEVS-VR-VID11342-2023

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

iOS

The Hypori Halo Client (iOS) was tested on the iOS v15.7.7 and iOS 16.5.1(C) platforms.

iOS 15

https://www.niap-ccevs.org/Product/Maint.cfm?AMID=1542&PID=11237

Apple iOS 15: iPhones, Update from v15.1.0 to v15.7.1

Validation Report Number: CCEVS-VR-VID11237-2022

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

iOS 16

https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11349

Apple iOS 16: iPhones

Validation Report Number: CCEVS-VR-VID11349-2023

The NIAP evaluation was completed using Apple iOS Version 16.3.

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

Windows

The Hypori Halo Client (Windows) was tested on Windows 10 Enterprise Version 21H2 and Windows 11 Enterprise Version 21H2.

Windows 10

Windows 10 Enterprise Version 21H2

https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2023.1010

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289.

Windows 11

Windows 11 Enterprise Version 21H2

https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2023.1010

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

CSfC

In order to meet CSfC conformance, the Hypori Halo Clients are limited by default to the paired Hypori Server ciphersuites identified below:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.