INTRUSION SHIELD ANDROID ENDPOINT USER MANUAL

INTRUSION 101 E. Park Blvd. Suite 1200, Plano, TX 75074

Table of Contents

INTRODUCTION 3

INSTALLATION 3

UI DASHBOARD 4

SHIELD FILTERING 5

UI MAIN MENU 7

BLOCKED AND ALLOWED SITES 8

CLIENT – ACTIVE DIRECTORY IDENTITY ENROLLMENT AND USAGE 8

ADDING ACTIVE DIRECTORY ACCOUNT ON ANDROID DEVICE 11

SUPPORT 12

Introduction

The Shield Endpoint Android **Client**

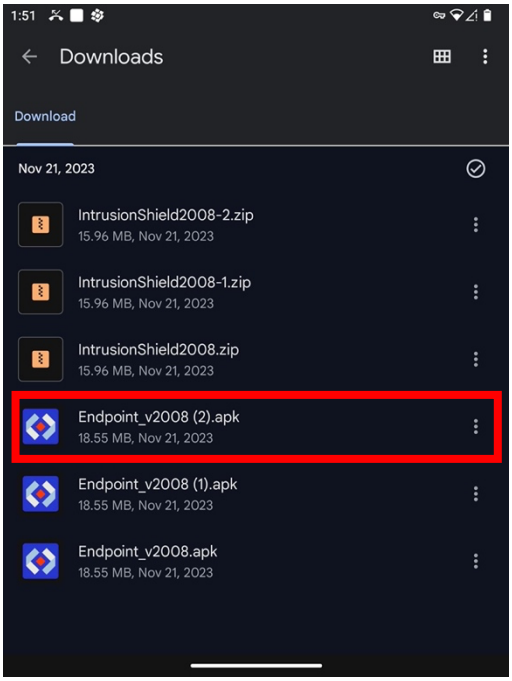
- Filters malicious traffic to and from the device, including applications and browser
- Provide access to services based on the registered identity on the device
- Allows users to manage an allowlist

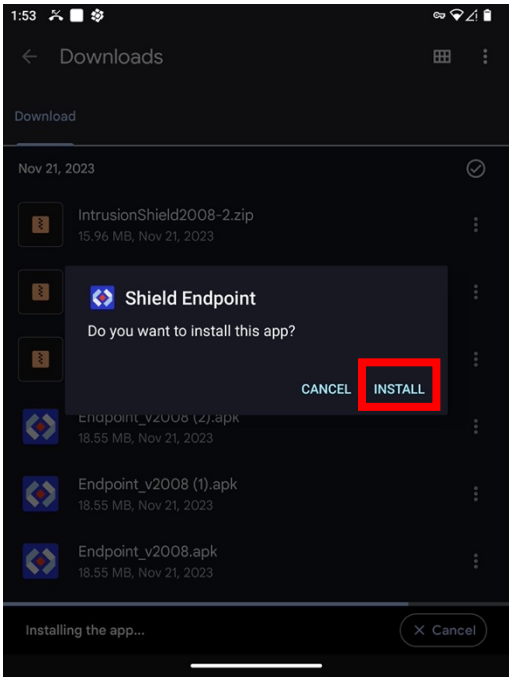
Installation

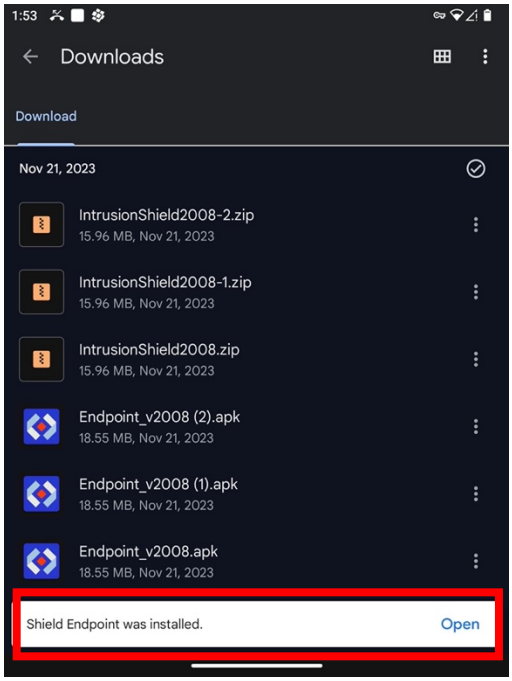
APK

Shield Endpoint for Android is installable from an APK file. Ask your administrator for the latest installation APK if you do not have access to it.

From your Android file browser, tap on the install file to begin. It should only take a few seconds for the installation to complete.

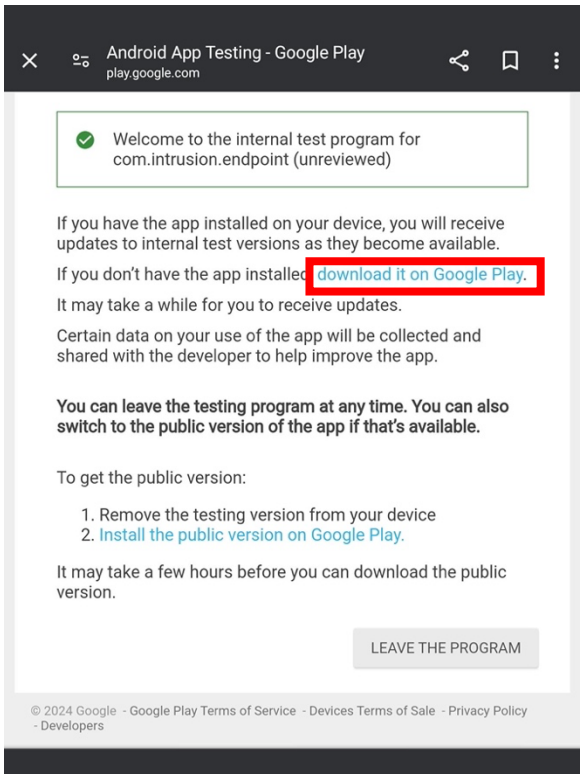


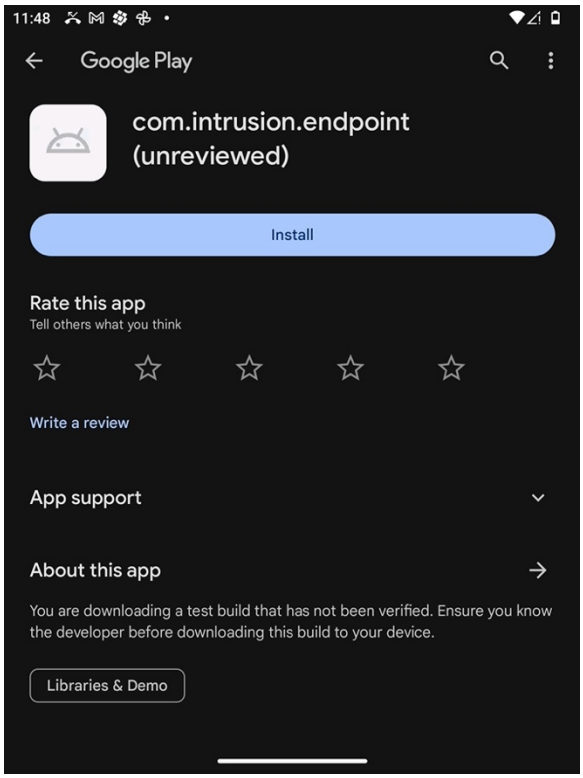




Google Play Store

Android Endpoint is also available as download through the Google play store. You will first receive a link to become part of the internal test team. Follow the link, and you will see this screen. Click on “download it on Google Play.” You will be redirected to the Google Play store and be prompted to install the app.

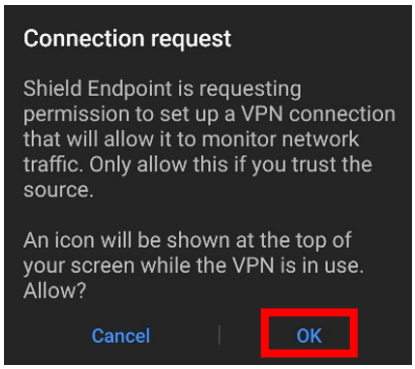




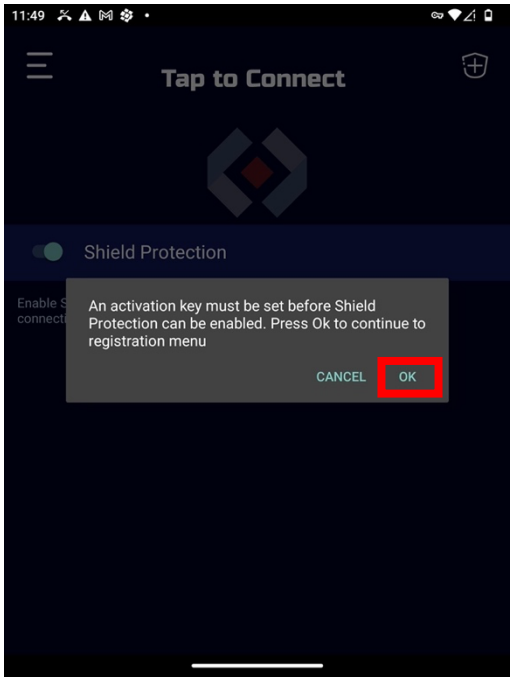
UI Dashboard

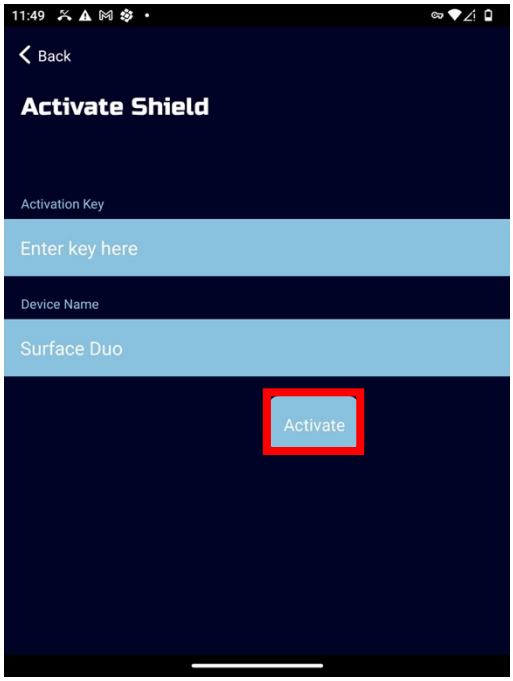
After installation, open the Shield Endpoint from your app list.

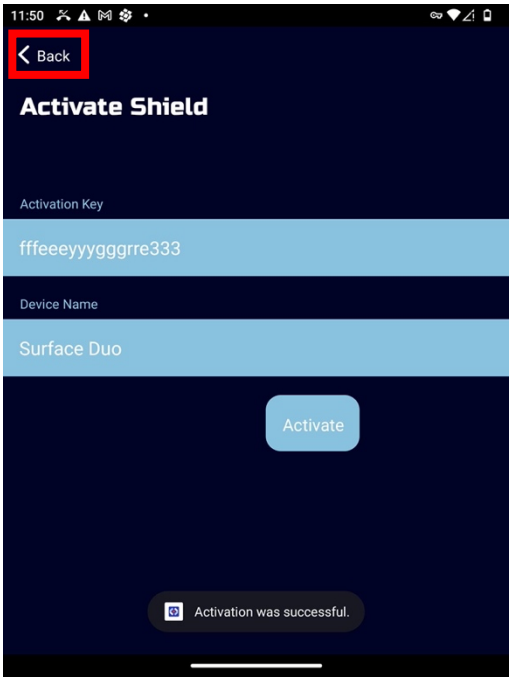
The central Shield icon is the one-click master control of the Shield Endpoint for Android. When tapping on the Shield icon for the first time, the Android system will ask about allowing a VPN connection. Select OK to proceed.



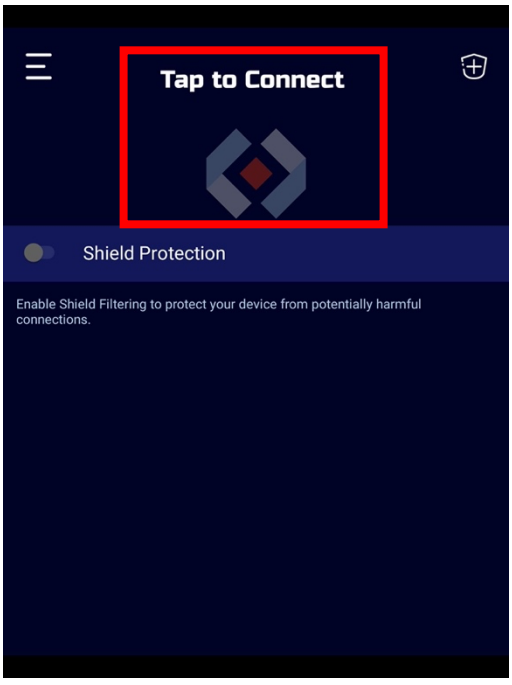
When attempting to connect the first time, you will see a popup prompting you to activate the device. Select OK to proceed. You will be redirected to the activation screen. Enter the activation key given to you by your administrator. Select Activate to proceed, then select the back button to navigate back to the home screen.

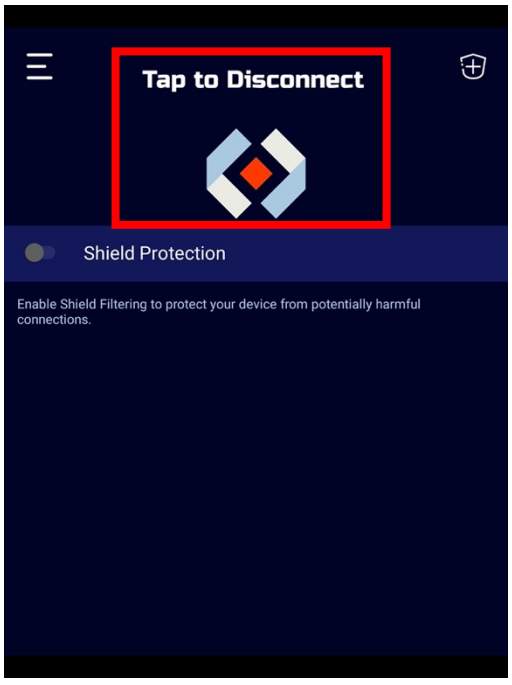






When the Shield icon is grayed out, the Shield filtering and any registered identities are all inactive. When the Shield icon is in color, the Shield filtering and identities are activated. Note that while the master control for the Shield Endpoint may be activated, the individual controls for filtering and identities may be enabled or disabled in other parts of the app.

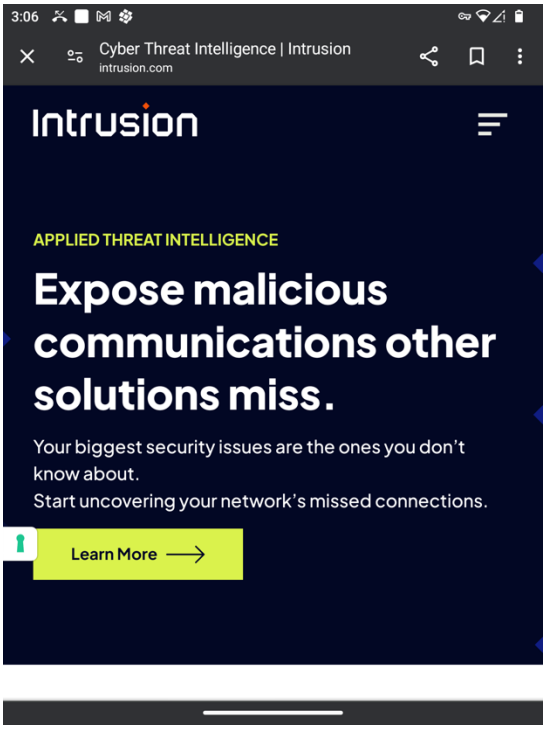


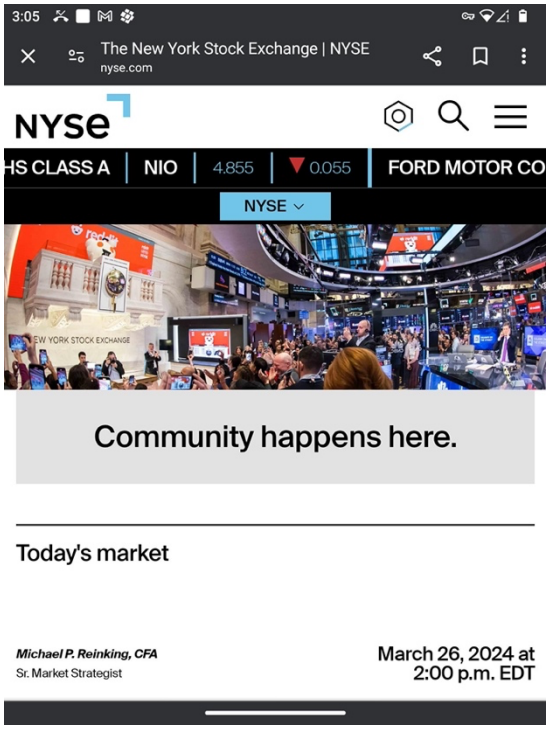


Shield Filtering

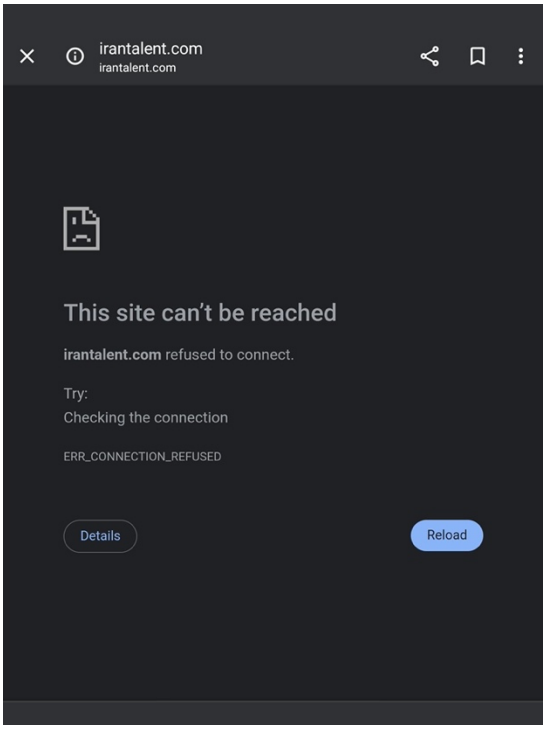
When Shield filtering is active, web browsing is filtered through Intrusion Shield rules.

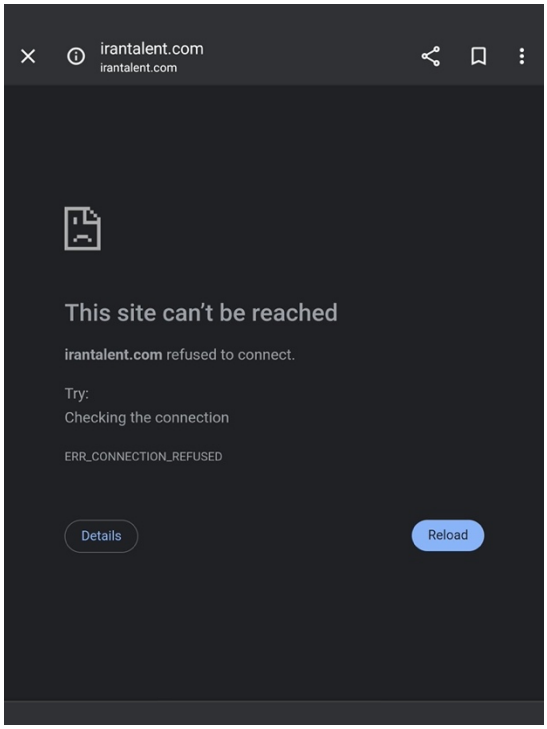
Connections to trusted sites will be allowed.





Connections to untrusted sites will be refused.

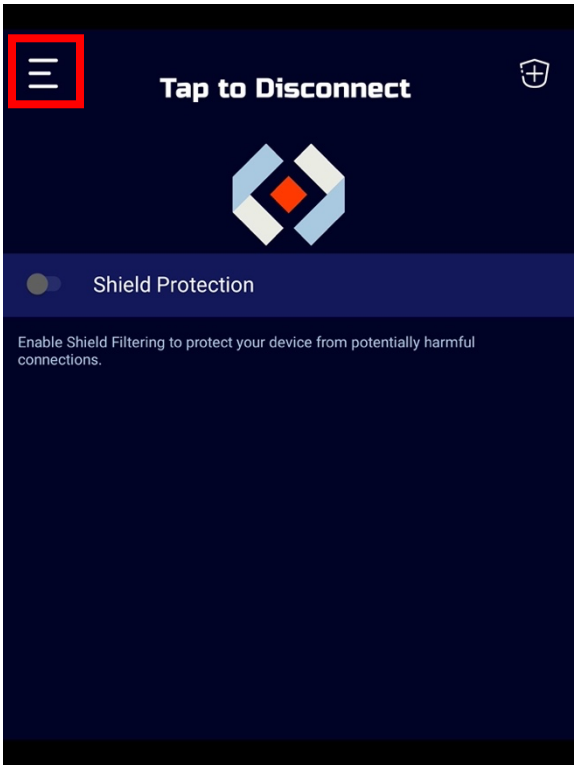


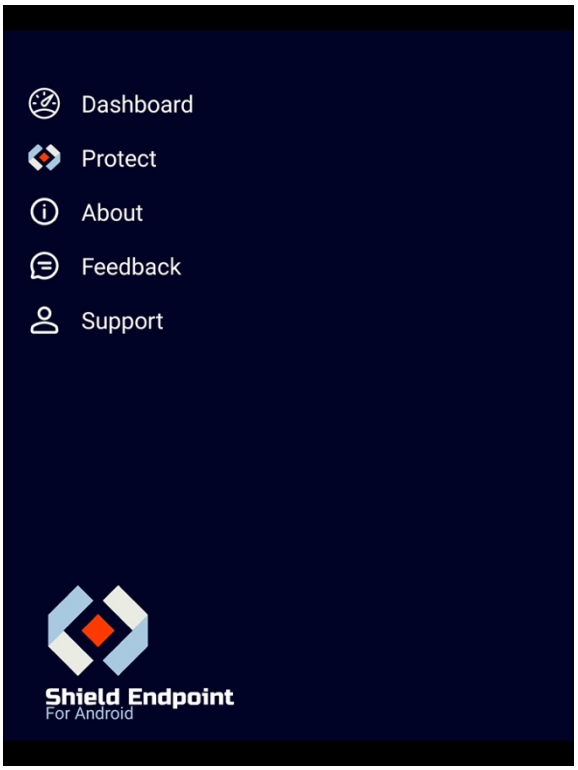


UI Main Menu

Tap on the Main Menu on the top left to access more controls.

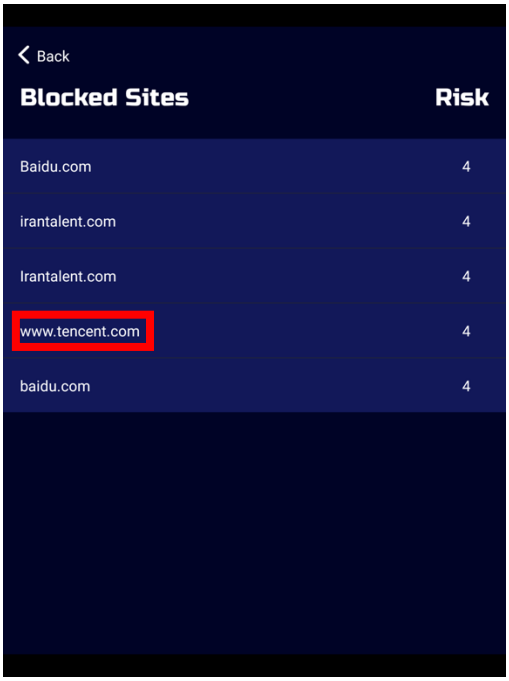
- Protect - Select this to have more granular control over how Shield filtering works on your device.
    - Shield Status - Enable or Disable this to control Shield filtering without affecting the access granted to registered identities
    - Allowed Sites - List of sites allowed by the user after it was blocked by Shield
    - Blocked Sites - List of sites blocked by Shield. The user may choose to allow any from this screen
- About - View information about Shield Endpoint for Android including product information, Privacy Policy, and app version number
- Feedback - Send feedback to developers@intrusion.com
- Support - Access the Intrusion support website

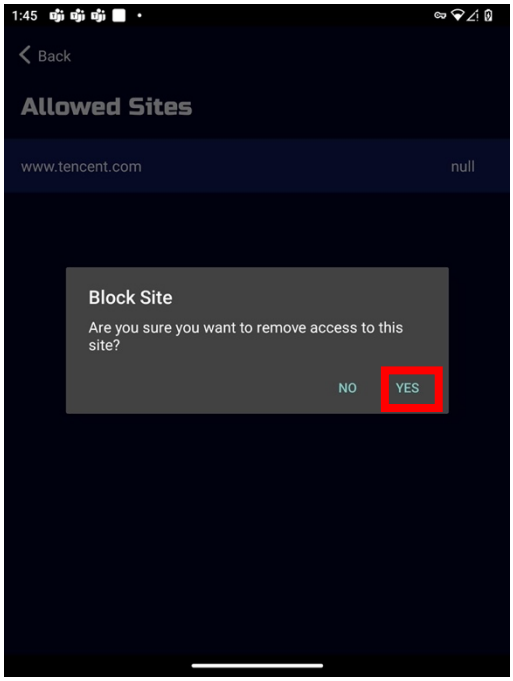


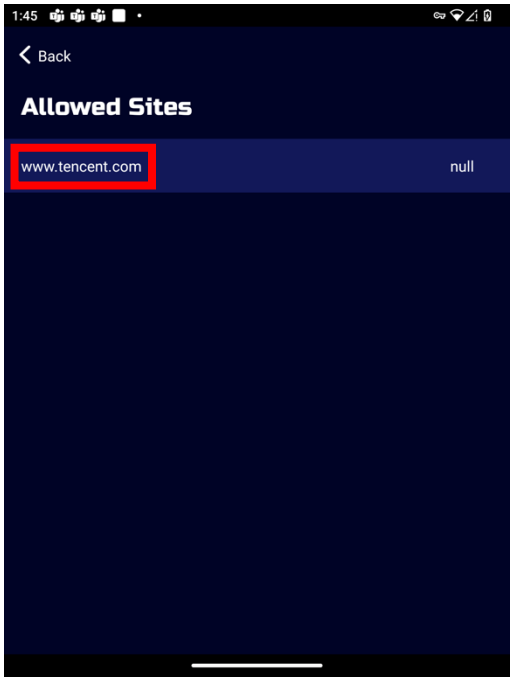


Blocked and Allowed Sites

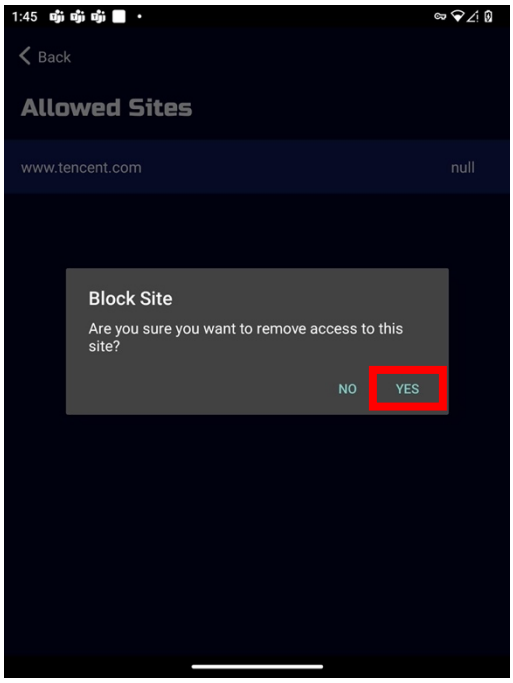
From Main Menu -> Protect -> Blocked Sites, review sites blocked by Shield Endpoint.
Tap on an entry on the Blocked Sites screen, then select Yes to remove it from the Blocked Sites screen and add it to the Allowed Sites screen.







In this example, when www.tencent.com is allowed, the user may access it even if Shield filtering is active. To begin blocking the site again, tap on its entry and choose Block Site.

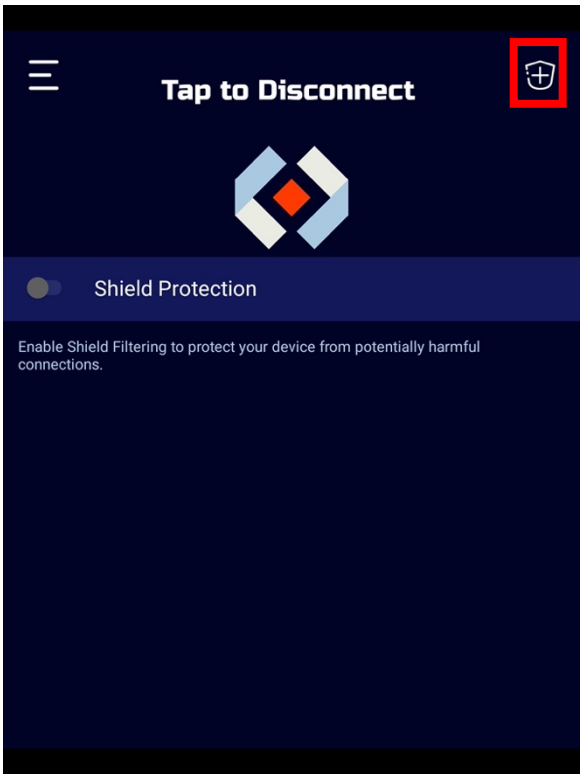


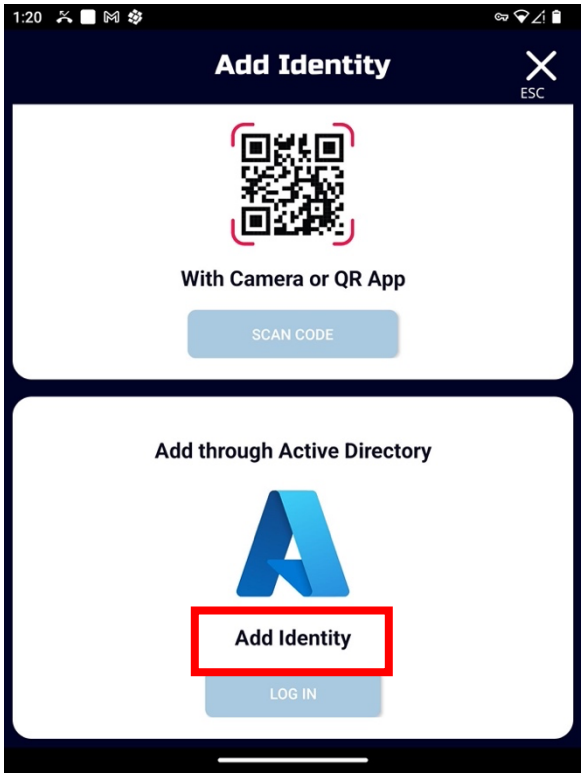
Client – Active Directory Identity Enrollment and Usage

An *Identity* on the Shield Endpoint allows your device to access internal services. This uses Zero-Trust tunneling that allows traffic to flow to and from only trusted services and endpoints. For a guide on provisioning endpoints and services, please review the Shield Endpoint Admin Manual.

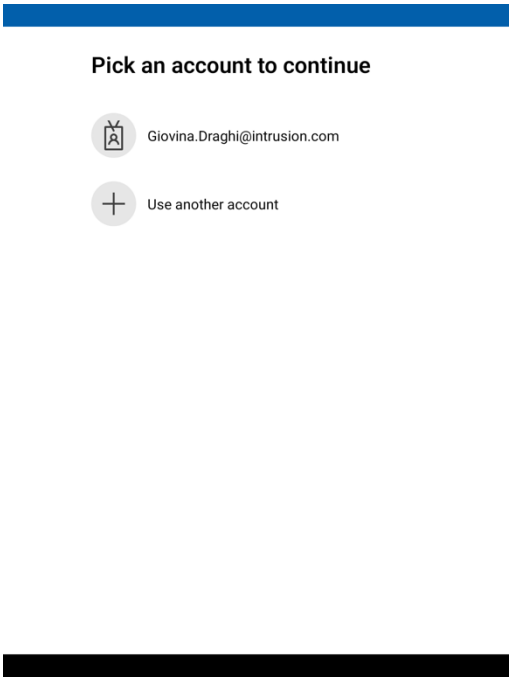
Note That this section assumes that you already have an Entra ID work account on your Android Device. If you do not have an Entra ID account on your Android device, or run into issues with the enrollment steps in this section, see the next section "Adding Entra ID Account on Android Device"

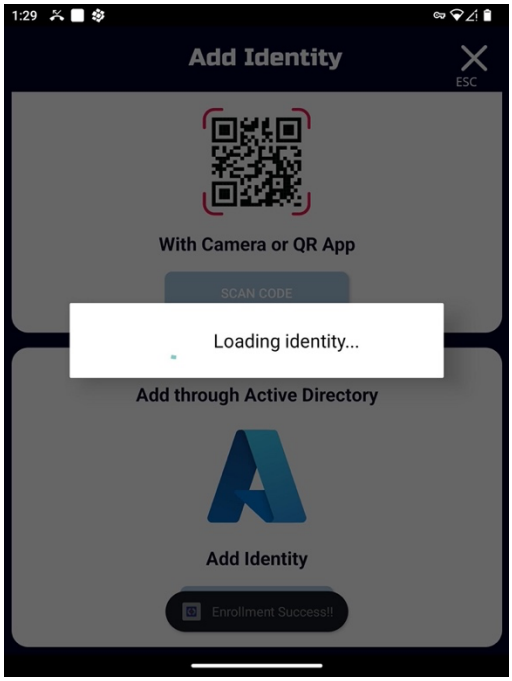
1. To start, tap on ADD IDENTITY symbol on the top left of the dashboard. Scroll down to the last option and choose LOG IN.

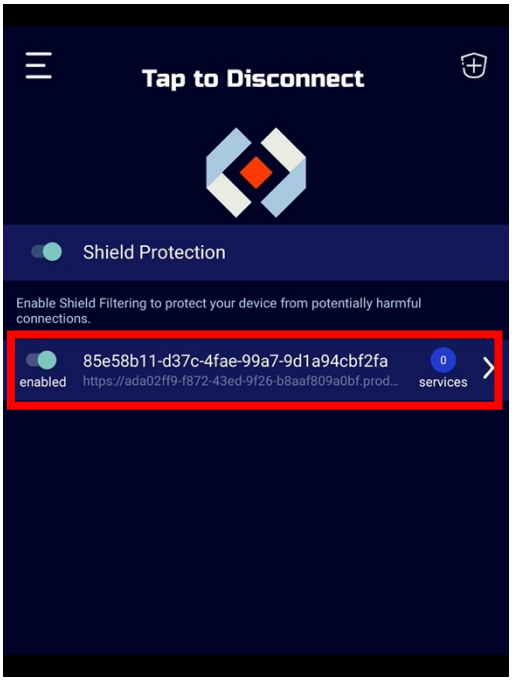




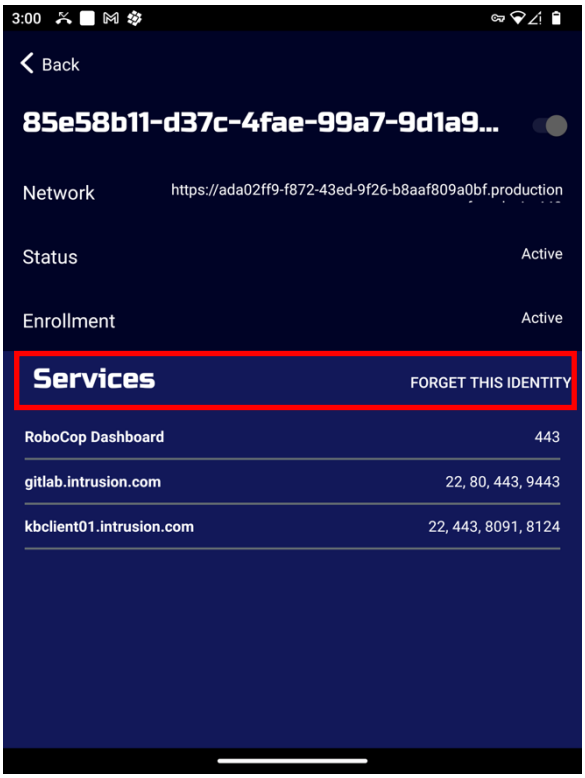
2. If your administrator has configured your Entra ID, choose your Entra ID account and authenticate if needed. If your Entra ID account has been configured correctly by your admin, then an Identity will be successfully added.

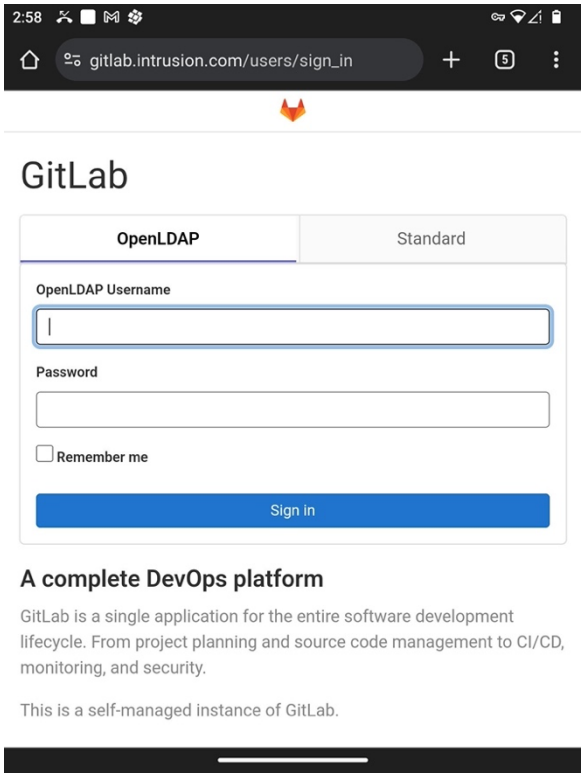






3. Tap on the Identity on the dashboard to see its details. Services available to you at the bottom of the screen are provisioned by your administrator. Tap on an entry to connect to the service through the browser.

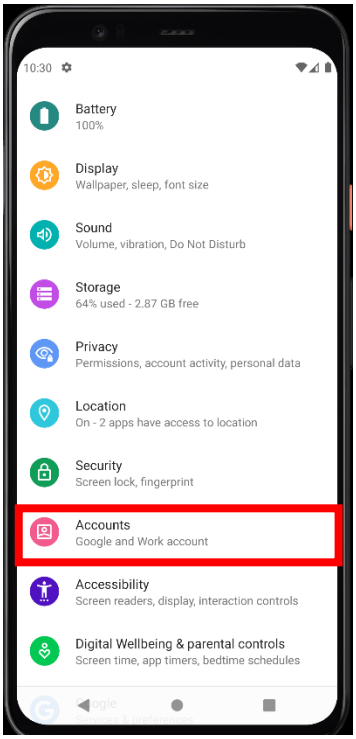


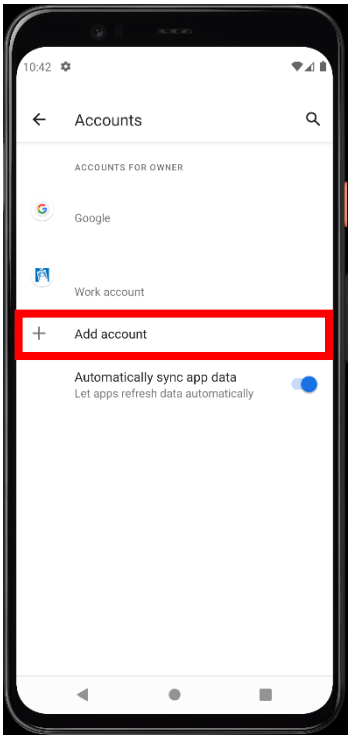


Adding Active Directory Account on Android Device

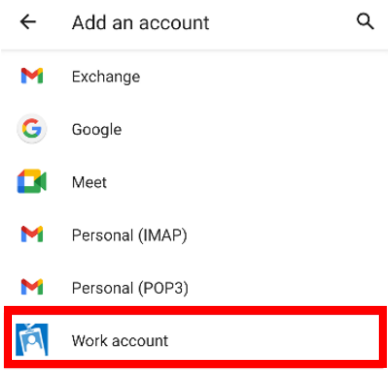
1. On your Android device, make sure both the Shield Endpoint and Microsoft Authenticator are installed.

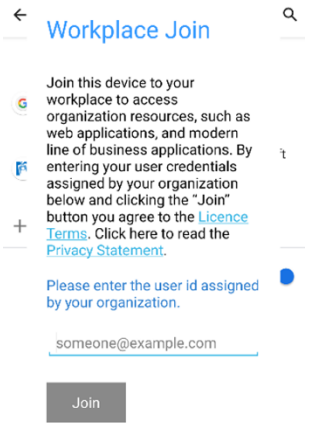
2. Go to device Settings -> Search for Accounts -> Add an account.



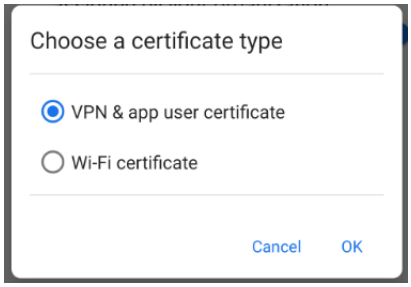


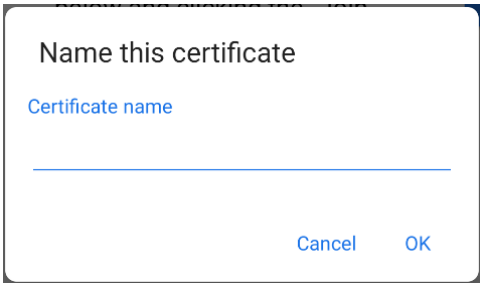
3. Select 'Work Account'. In the following menu, log in with your user account. You will be prompted to log in to the account.
    a. The 'Work Account' option only shows up when Microsoft Authenticator is installed. This is the only way to reliably register a device in Entra ID. The account will automatically be added to Authenticator when doing this.
    b. It is recommended to use an admin account, or at least an account with permissions to consent to external apps on behalf of your organization.





4. You will be asked to choose a certificate type, just leave it at the default as it is not used. You can choose whatever name you want, as this is also not used.





5. Hit Ok once you are done. You should now have a work account listed.

Once the device has been registered, the Entra ID integration will pick it up in 15 - 60 minutes, depending on the sync frequency set by your admin.

Support

If you have any questions or would like to make any feature suggestions, please reach out to our customer support team.
Support@intrusion.com
1-888-637-7770 and use option 3.