Infoblox

DEPLOYMENT GUIDE

BloxOne Mobile Endpoint

Table of Contents

Introduction

Infoblox BloxOne Mobile Endpoint is a lightweight mobile cloud service for sending queries over an encrypted channel. Mobile Endpoint provides visibility into infected and compromised devices (including Android and iOS), prevents DNS-based data exfiltration and other forms of DNS tunneling, and impedes device communications with botnets and their command-and-control infrastructure.

To enable end users to connect to Infoblox cloud services, you must download and install the Endpoint client on their devices. The client enforces security policies that you apply to the remote networks, regardless of where the end users are and which networks they are connected to.

BloxOne Mobile Endpoint supports IPv4 DNS configurations, thereby protecting all devices, regardless of their network environments. This means roaming clients will be protected in different networking environments. When connected to a network, mobile endpoints can communicate with BloxOne Threat Defense Cloud by using both protocols. Mobile endpoint is able to proxy IPv4 DNS queries and forward them to BloxOne Threat Defense Cloud.

Requirements

The following is a list of prerequisites required to use BloxOne Endpoint with BloxOne Threat Defense.

1. Administrative access to the Infoblox Cloud Services Portal (CSP) (https://csp.infoblox.com).
2. BloxOne Threat Defense License (One of the following):
    - BloxOne Threat Defense - Business Cloud
    - BloxOne Threat Defense - Advanced license
3. Client Operating System (One of the following):
    - Apple:
        - IOS 14.0 or later)
        - iPad (iOS 14.0 or later)
    - Android:
        - Android devices (10.0 and up)
4. BloxOne Mobile Endpoint (EP):
    - Infoblox BloxOne Mobile Endpoint (BloxOne EP) can be downloaded and installed from either the Apple App store or the Google Play store, depending on your device. Use your own mobile endpoint management solution to deploy your mobile endpoint devices. The MDM solution should push your BloxOne Endpoint configuration to the mobile devices before they can be managed/provisioned from the Cloud Services Portal (CSP).
5. Enrollment of BloxOne Mobile Device Management App (if using MDM solution)
    - See **“Enrollment of BloxOne Mobile Device Management App”** section for more information.

Workflow

1. Create a CSP account.
2. Install a Mobile Device Management app.
3. Create an Infoblox Endpoint Group.
4. Enrollment of BloxOne Mobile Device Management app.
5. Configure Mobile Device Management app.
6. Install Mobile Endpoint through MDM.
7. View Mobile endpoint on Devices.
8. Confirm data is being sent and collected via Reporting.

Q&A

Q. Is BloxOne Endpoint supported on any additional MDM's not talked about in this guide?
A. If the Endpoint supports BloxOne to push the config then they are supported

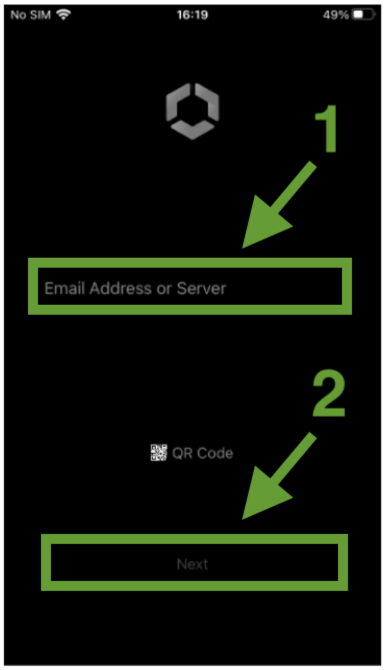
Q. If a user has two containers on their phone (e.g. One for business and one for private use.) will the mobile endpoint affect both containers or only the one container in which it is installed.
A. The mobile endpoint should only affect the one container unless the MDM is set up to push the deployment to both containers.

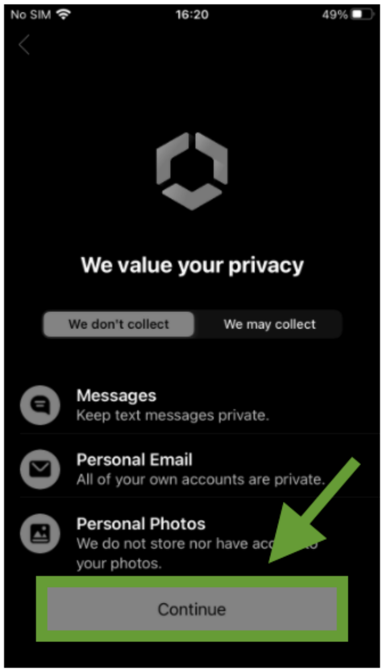
Enrollment of BloxOne Mobile Device Management App

VMware Workspace One

Steps for enrolling BloxOne Mobile app

1. You will need to receive an email from AirWatch (noreply@awmdm.com) with your log-on credentials and the server name for **"Mobile Intelligent Hub Application"**.
2. The BloxOne app will be installed on your device using the MDM application, **"Intelligent Hub"**.
3. Install **"Intelligent Hub"** on your phone. The **"Intelligent Hub"** app is available for your device from the Play/App store.
4. Open the **"Intelligent Hub"** app and provide your email address.
5. Enter your username and password when prompted. Then, tap **Next**. You can change the password using the email you received in Step1, above.



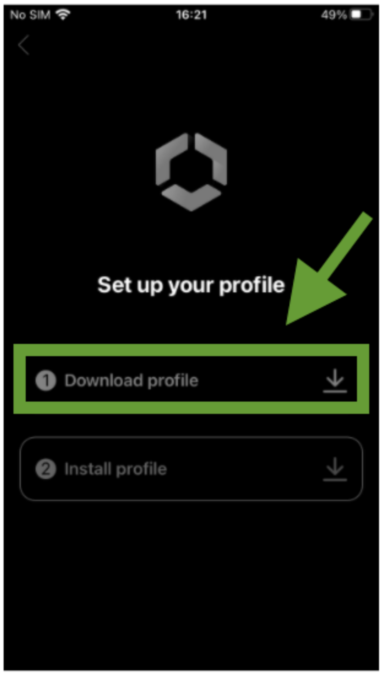


Keep text messages private.

All of your own accounts are private.

We do not store nor have acc to your photos.

6. Set up your profile by tapping **"Download profile".** A browser window will open and a profile will get downloaded to your device.



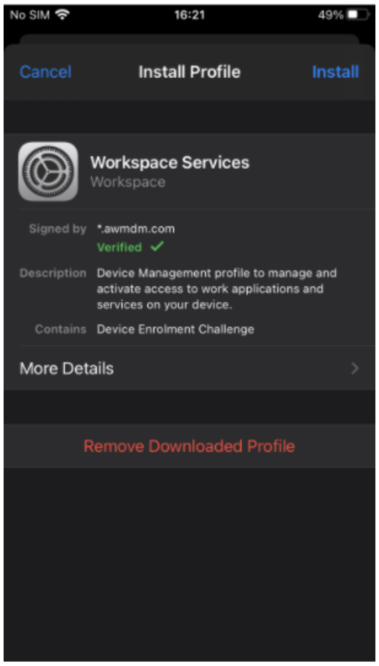
For iOS, perform the following:

A. On the **"Settings"** screen navigate to settings and click on the downloaded profile.

B. Install the profile on your device (**“View Profile”** → **“Install”** → **“Enter passcode”** → **“Install”**).
C. The mobile device is enrolled in the MDM once a profile is installed.

For Android, perform the following:

1. On the **“Settings”** screen navigate to settings and click on the downloaded profile.
2. Install the profile on your device (**“View Profile”** → **“Install”** → **“Enter passcode”** → **“Install”**).
3. Create a work profile by tapping **“Create”.** Proceed with the console.
4. A work profile is created with a set of applications once the connection with MDM is established.



Workspace Services
Workspace

Signed by *.awmdm.com
Verified ✓

Description Device Management profile to manage and activate access to work applications and services on your device.

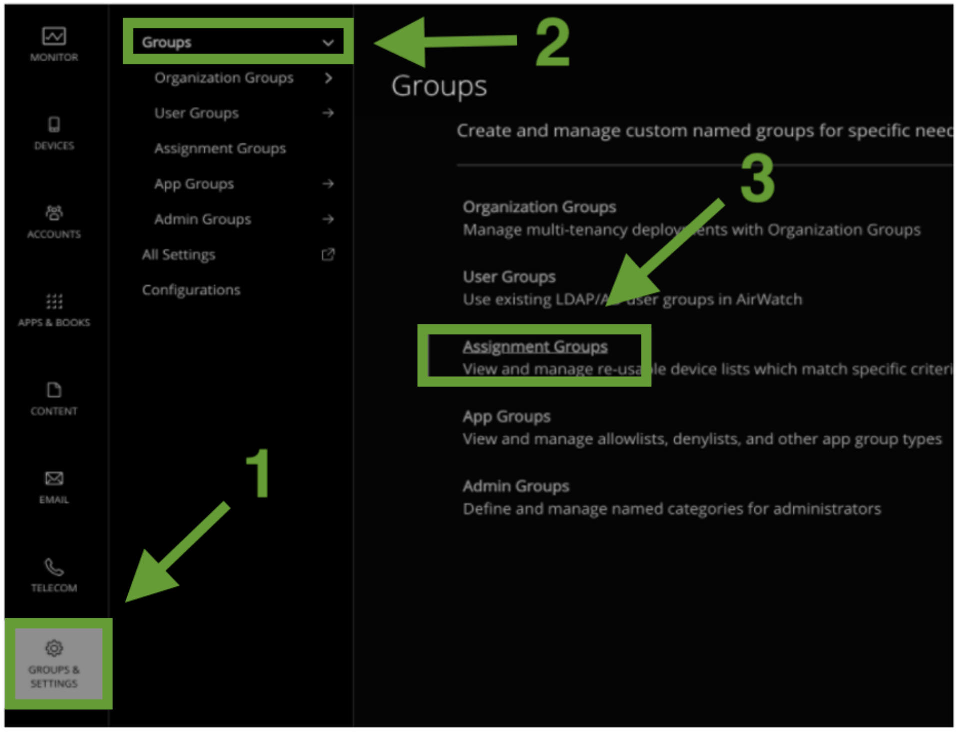
Contains Device Enrolment Challenge

Assignment group

An assignment group must be created so that devices can be grouped together.

In order to create an assignment group, perform the following:

1. Navigate to **“Groups & Settings”** → **“Groups”** → **“Assignment Groups”**.



Groups

Create and manage custom named groups for specific need

Organization Groups
Manage multi-tenancy deployments with Organization Groups

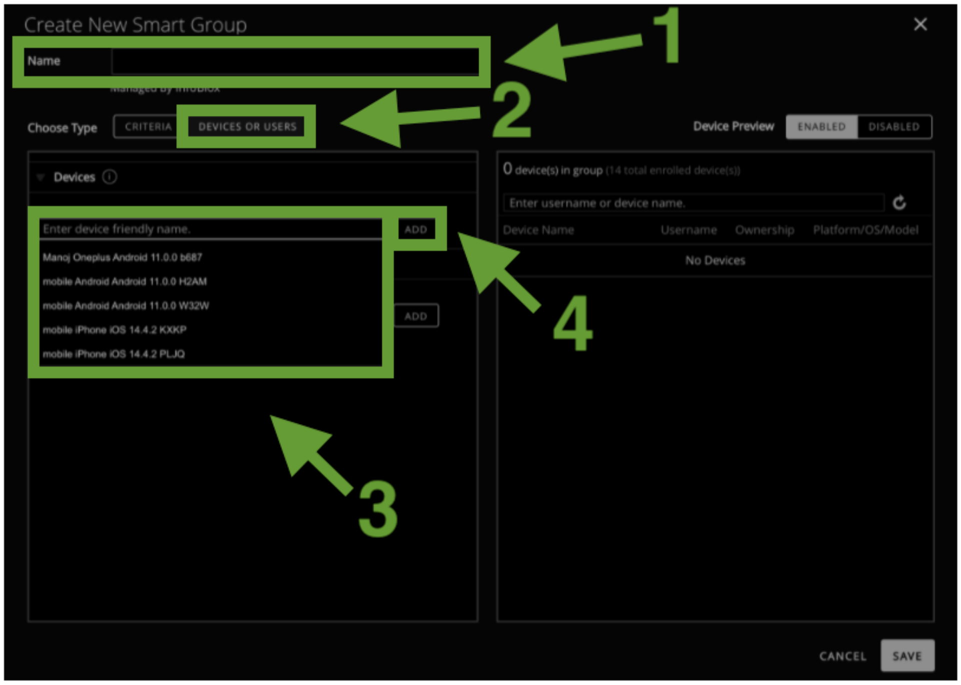
User Groups
Use existing LDAP/AD user groups in AirWatch

Assignment Groups
View and manage re-usable device lists which match specific criteri

App Groups
View and manage allowlists, denylists, and other app group types

Admin Groups
Define and manage named categories for administrators

2. On the **“Create New Smart Group”** screen provide a device name to create a new smart group.
3. Click on **“Devices or Users”**.


Create New Smart Group
Name
Managed by Infoblox
Choose Type
CRITERIA
DEVICES OR USERS
Devices
Enter device friendly name.
ADD
Manoj Oneplus Android 11.0.0 b687
mobile Android Android 11.0.0 H2AM
mobile Android Android 11.0.0 W32W
mobile iPhone iOS 14.4.2 KXKP
mobile iPhone iOS 14.4.2 PLJQ
ADD
Device Preview
ENABLED
DISABLED
0 device(s) in group (14 total enrolled device(s))
Enter username or device name.
Device Name
Username
Ownership
Platform/OS/Model
No Devices
CANCEL
SAVE
1
2
3
4

4. Click on the text box under **“Devices”** and Select the device you want to assign.
5. Click **“ADD”** to add the device to your configuration.

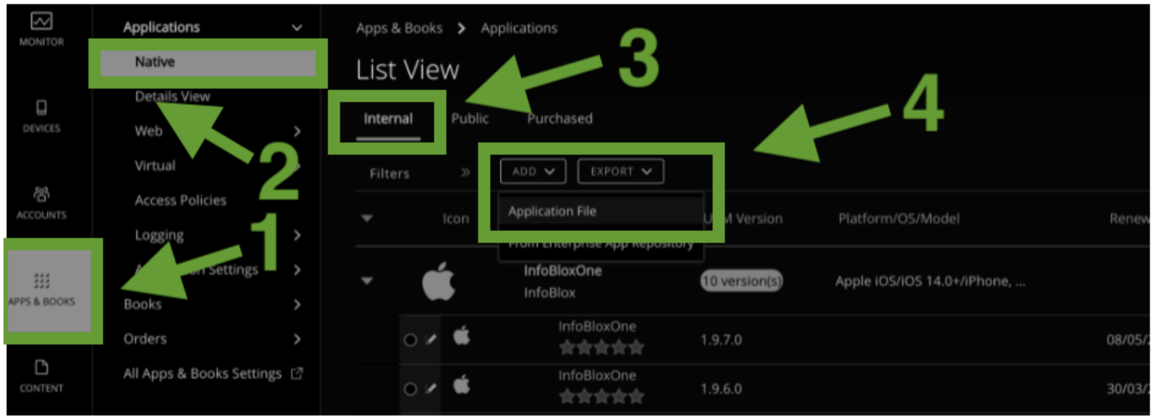
6. Repeat the process from step 4 to add additional devices to your configuration.
7. Click **“Save”** to save your configuration.

Install an Application

Make sure the mobile device is registered with the MDM and an assignment group has been created previously. If this hasn’t happened, return to the beginning of VMware Workspace One in this guide to do so.

Steps to create a new app(IOS)

1. Navigate to **“Apps and Books”** → **“Native”** → **“Internal”**.
2. Click the **“Add”** drop down and click **“Application File”**.

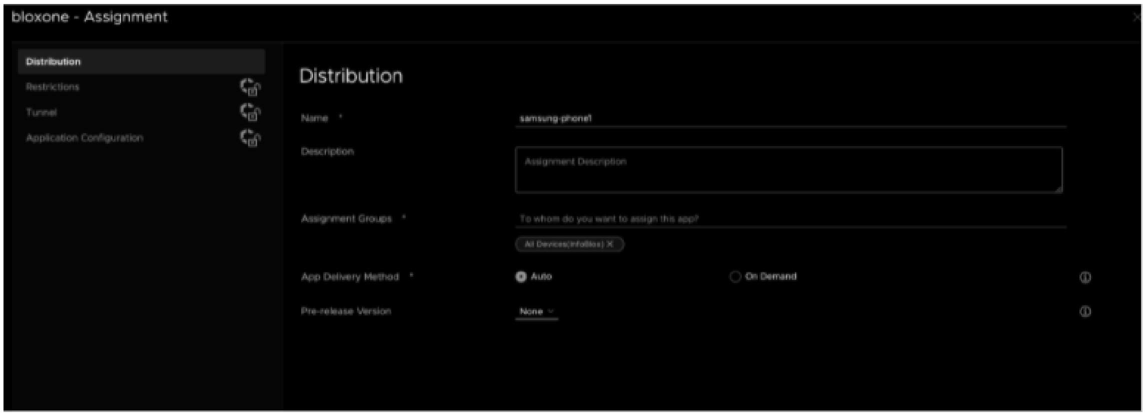


InfoBloxOne InfoBlox 10 version(s) Apple iOS/iOS 14.0+/iPhone, ...

InfoBloxOne 1.9.7.0 08/05/

InfoBloxOne 1.9.6.0 30/03/

3. Upload the provided application file (.ipa) and click **“NEXT”**.
4. when you click **“Save and Assign”**, a new window will open. Carry out the following steps 5 through 9 listed below to create a new app (Apple).
5. A wizard will open, guiding you through the set-up process. On the **“Add Application”** screen, enter the assignment name and select the assignment of choice from the **“Assignment”** text/drop down menu.



Name * samsung-phone1

Description Assignment Description

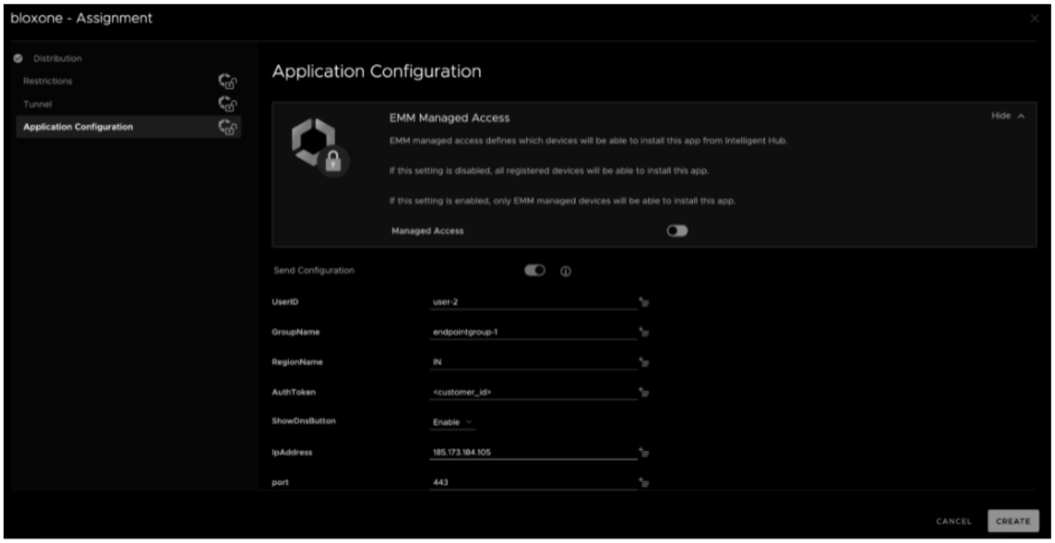
Assignment Groups * To whom do you want to assign this app?

All Devices(Infoblox) ✕

App Delivery Method * ● Auto ○ On Demand

Pre-release Version None

6. On the **“Distribution”** screen, you will see options for restrictions. (eg. If the user should not be able to uninstall the application, then these options can be enabled). Click **“Create”** then select any options and tap **“Create”** again.
7. Apply the app configuration located under the **“Application Configuration”** tab.



Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access

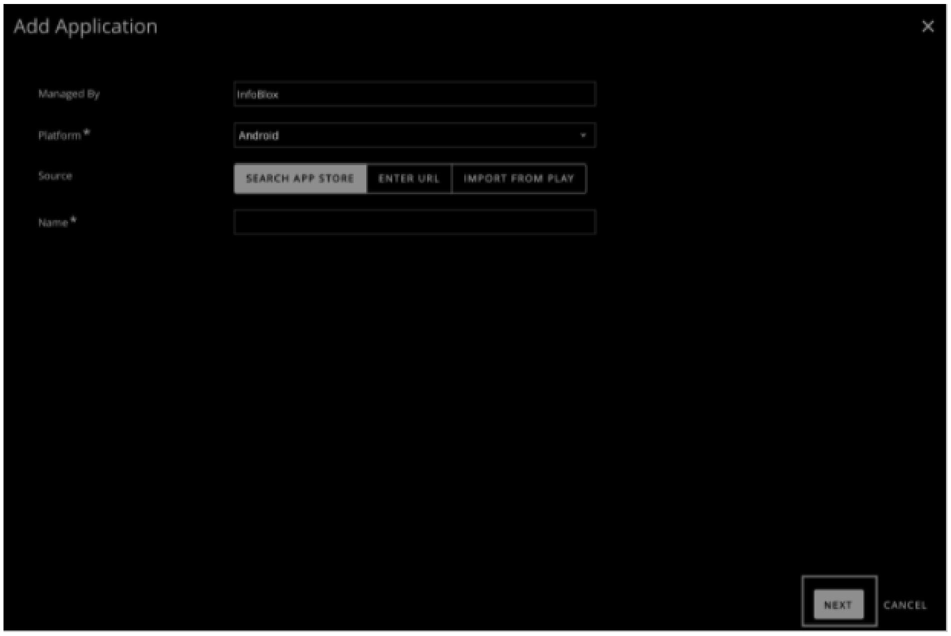
Send Configuration

UserID	user-2
GroupName	endpointgroup-1
RegionName	IN
AuthToken	<customer_id>
ShowDnsButton	Enable
IpAddress	185.173.184.105
port	443

8. click **“Publish”** on the window that displays a list of devices to which the application has been installed.

Steps to create a new app (Android)

1. Navigate to **“Apps and Books”** → **“Native”** → **“Public”**.



Add Application

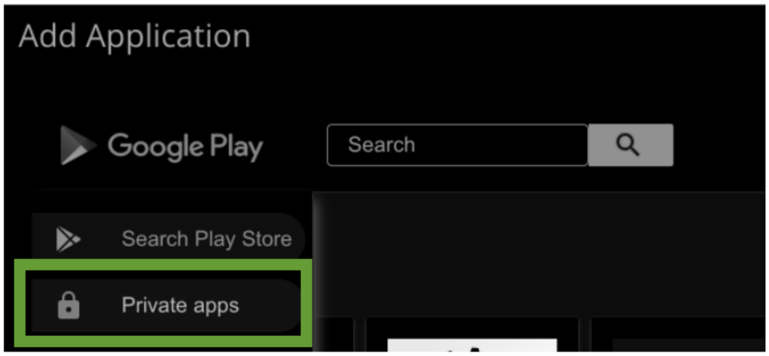
Managed By: InfoBlox

Platform*: Android

Source: SEARCH APP STORE | ENTER URL | IMPORT FROM PLAY

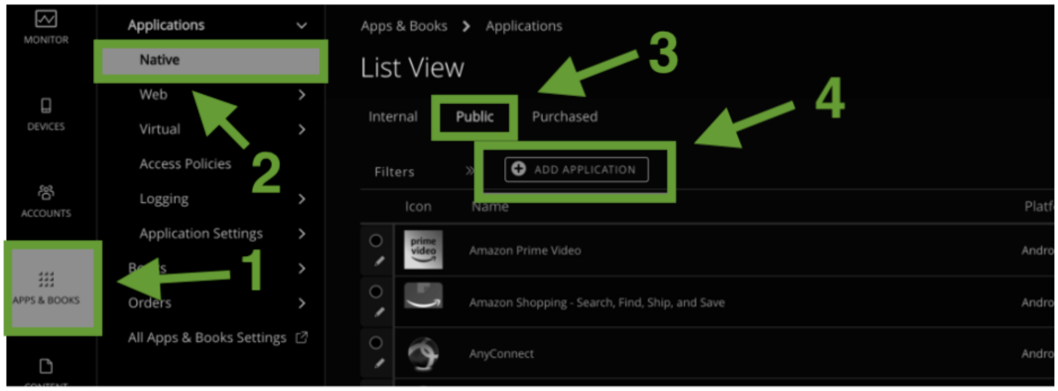
Name*:

2. Click **“ADD APPLICATION”**.

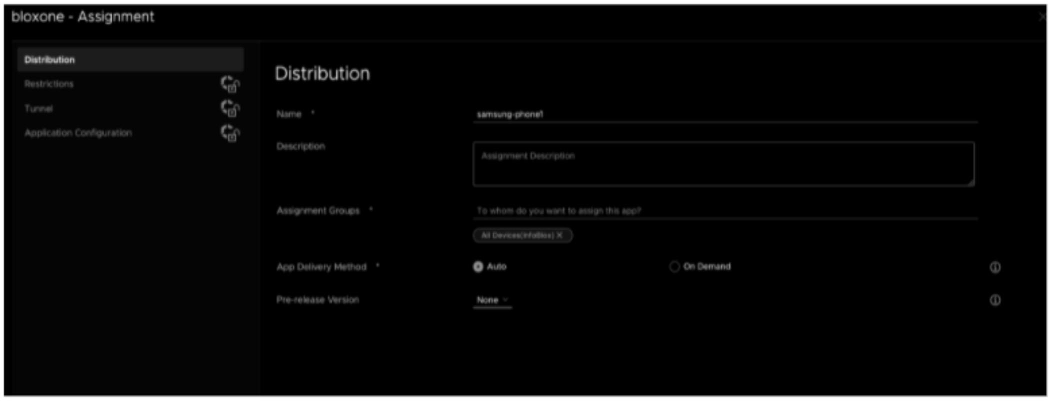


Add Application

3. Select platform and provide the name of the application to be installed then Click **“Next”.**
4. Select **“Private apps”** from the app store window.
5. Tap on the **“Plus”** symbol to upload the provided application file (.apk). then click **“Next”**.



6. A wizard will open, guiding you through the set-up process. On the **“Add Application”** screen, enter the assignment name and select the assignment of choice from the **“Assignment”** text/drop down menu.



Distribution

Name * samsung-phone1

Description: Assignment Description

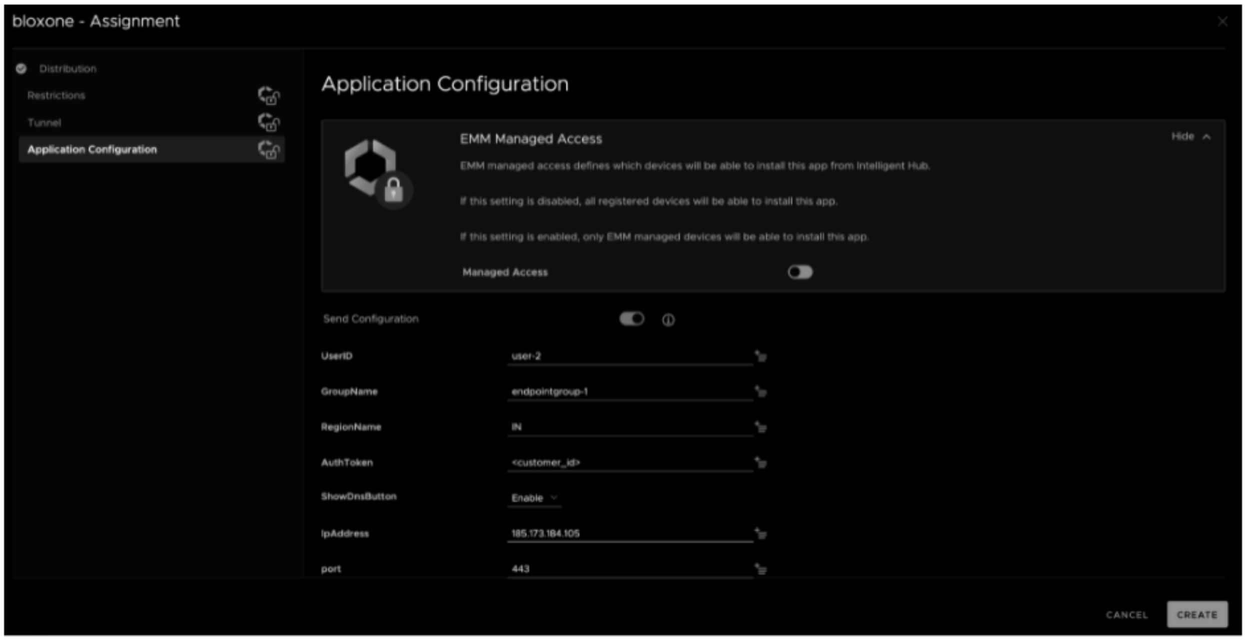
Assignment Groups * To whom do you want to assign this app?

All Devices(Infoblox) ✕

App Delivery Method * ● Auto ○ On Demand

Pre-release Version: None

7. On the **“Distribution”** screen, you will see options for restrictions. (eg. If the user should not be able to uninstall the application, then these options can be enabled). Click **“Create”** then select any options and tap **“Create”** again.
8. Apply the app configuration located under the **“Application Configuration”** tab.



Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access: off

Send Configuration: on

UserID	user-2
GroupName	endpointgroup-1
RegionName	IN
AuthToken	<customer_id>
ShowDnsButton	Enable
IpAddress	185.173.184.105
port	443

9. Click **“Publish”** on the window that displays a list of devices to which the application has been installed.

Steps to install an existing application

If the application is already being used by some users, and the application needs to be added to our device, follow these steps:

1. Navigate to **“Apps and Books”** → **“Native”** → **“Public”**.
2. Click on the edit icon of the application of choice.
3. Click on **“Save & Assign”**. A wizard opens up for an assignment.
4. Click on **“Add assignment”.**
5. Enter the Assignment name and select the assignment of choice from the Assignment text/drop down menu.
6. Select the options as per requirement and click **“save and publish”**.

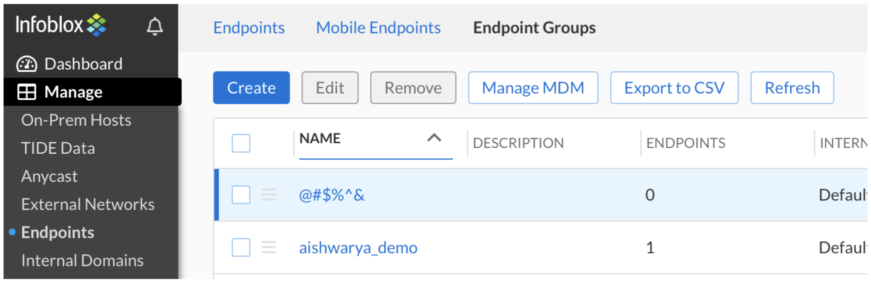
Cisco Meraki

Downloading the MDM Config File from the Cloud Services Portal

The app config file is required to update the configuration in MDM.

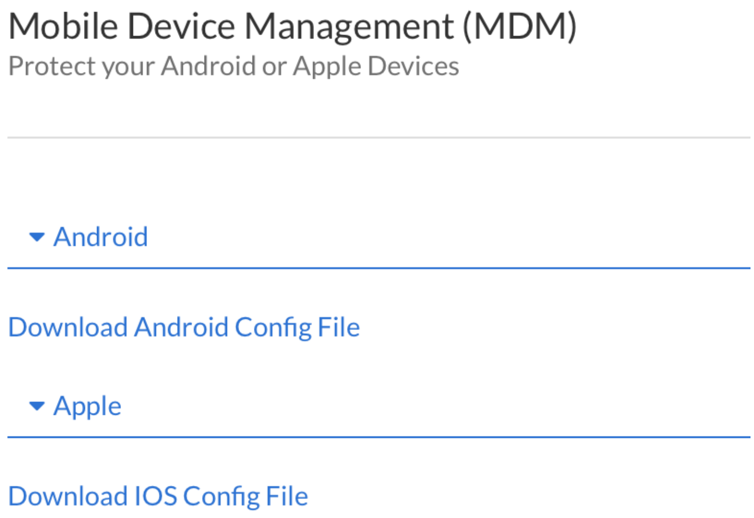
Perform the following steps to download the MDM config file from the Cloud Services Portal:

1. In the Cloud Services Platform, navigate to **“Manage”** → **“Endpoints”** → **“Endpoint Groups”.**
2. Click **“Create”** on the **“Endpoints Groups”** page.



NAME	DESCRIPTION	ENDPOINTS	INTERN
@#$%^&		0	Defaul
aishwarya_demo		1	Defaul

3. In the **“Mobile Device Management (MDM)”** section of the **"Create Endpoint Group”** pane download the config file for your device. For Android devices, click **“Download Android Config File”.** For Apple iOS, click **“Download IOS Config File”.**



Mobile Device Management (MDM)

Protect your Android or Apple Devices

▾ Android

Download Android Config File

▾ Apple

Download IOS Config File

Note: The Mobile Device Management (MDM) app configuration file contains the following parameters:

- **customerId**: Uses the value present in the xml file.
- **groupName**: Specifies the group name in the Cloud Services Portal to which the mobile endpoint has moved to and added. If the group name is not present in the Cloud Services Portal, then It will be added to the **All BloxOne Endpoints** group by default.
- **userId**: The unique name of the mobile device. The configured name will be displayed on the **"Endpoints"** page.
- **allowServiceControl**: By default this value will be **True**. using the toggle , you can change this value to **False** in order to hide it.

In MDM, the app configuration can be added manually or by uploading the .xml file.

Registering Mobile Endpoint to Cisco Meraki Server

To register Mobile Endpoint with Cisco Meraki server, perform the following:

- Install the **"Meraki Systems manager"** app from the play store/app store.

  For Android devices, complete the following:

  1. Copy the enrollment code from the **"System Manager"** portal.

  2. Open the **"Meraki Systems Manager"** app and enter the enrollment code.

  3. Follow the steps as provided and register the Android device to the Cisco Meraki server.

  4. For additional information, see the Cisco Meraki Android *documentation*.

For iOS devices, complete the following:

1. Copy the network ID from the *System Manager* portal.

2. Open the **“Meraki Systems Manager”** app and enter the network ID.

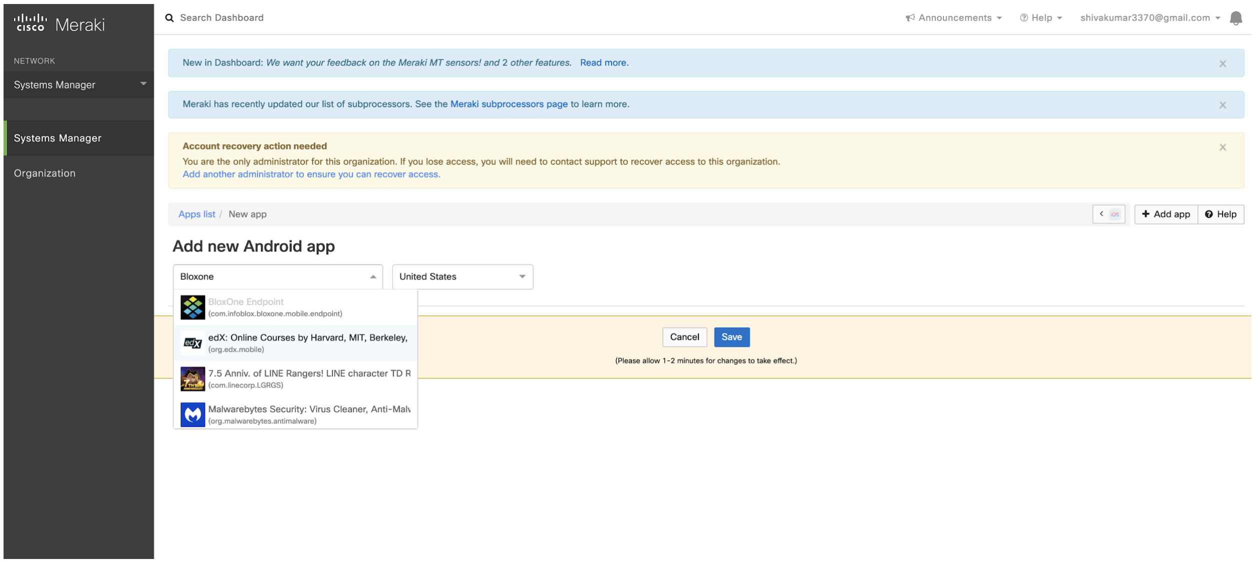
3. Follow the steps as provided and register the iOS device to the Cisco Meraki server.

4. For additional information, see the Cisco Meraki iOS documentation.

Adding the BloxOne App to Cisco Meraki Server

To add BloxOne Mobile Device Management (MDM) to the Cisco Meraki, server, perform the following steps:

1. Navigate to **“System Manager”** → **“Manage”** → **“Apps”** → **“Add App”.**
2. Based on the App platform(iOS/Android) choose the App store or Play store app.
3. In the **“Add new iOS/Android app”**, perform a search for **“BloxOne EP”** and select the app from the returned search results.
4. Select the app from among the search results.
5. Select **“Device Target”** and click **“Save”** making sure **“App”** is listed on the **“Apps List”.**



New in Dashboard: *We want your feedback on the Meraki MT sensors! and 2 other features.* Read more.

Meraki has recently updated our list of subprocessors. See the Meraki subprocessors page to learn more.

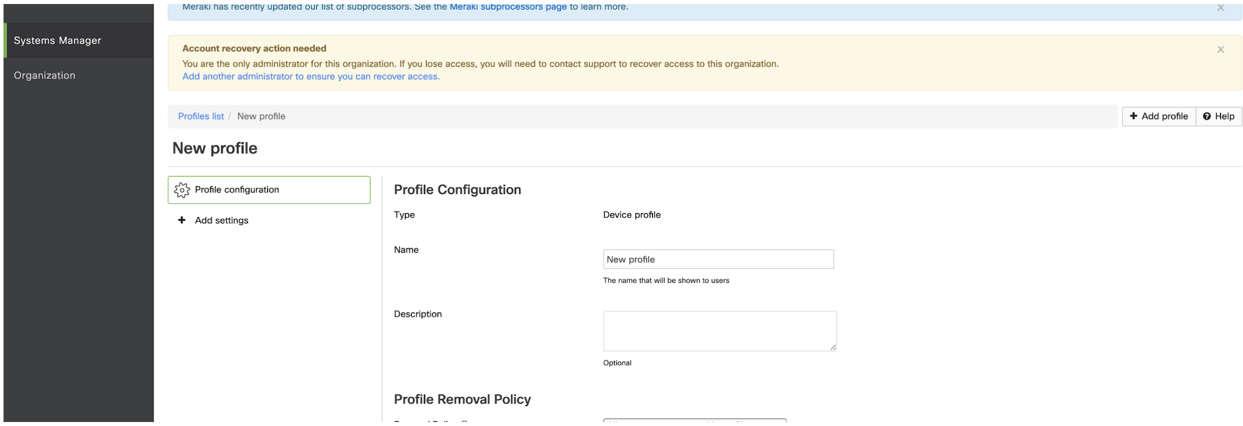
Account recovery action needed
You are the only administrator for this organization. If you lose access, you will need to contact support to recover access to this organization.
Add another administrator to ensure you can recover access.

(Please allow 1-2 minutes for changes to take effect.)

How to Upload and Add the App Configuration to Cisco Meraki Server

To add the app configuration to the MDM configuration, perform the following steps:

1. Navigate to **“System Manager”** → **“Manage”** → **“Settings”.**
2. Click **“+ Add Profile”.**
3. In the name field, provide the new profile name.
4. Click **“+ Add Settings”** to save the profile.



Meraki has recently updated our list of subprocessors. See the Meraki subprocessors page to learn more.

Account recovery action needed

You are the only administrator for this organization. If you lose access, you will need to contact support to recover access to this organization.
Add another administrator to ensure you can recover access.

New profile

Profile Configuration

Type: Device profile

Name: New profile

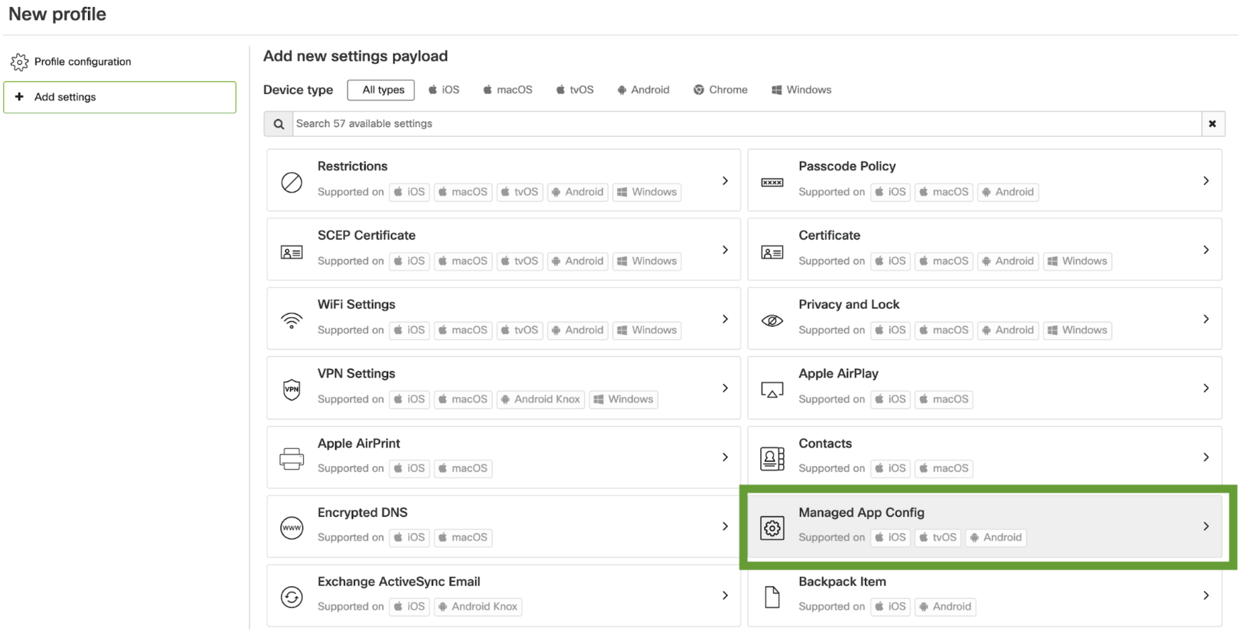
The name that will be shown to users

Description:

Optional

Profile Removal Policy

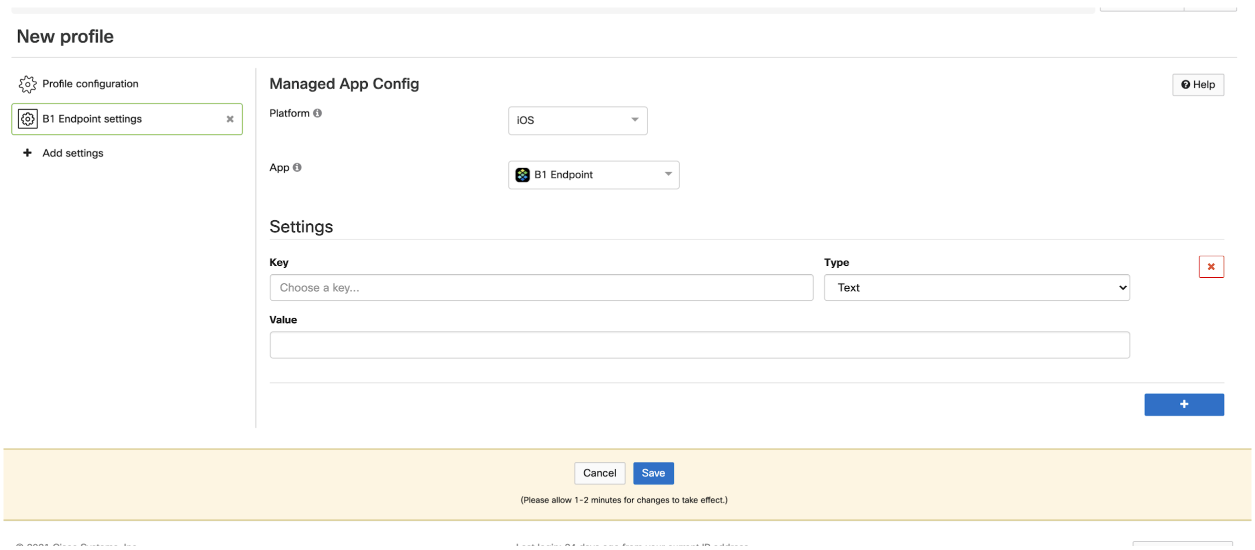
5. In the **"Add new settings payload"** section of the **"New profile"** page, click **"Managed App Config"** to add settings to the configuration.



Restrictions Supported on iOS macOS tvOS Android Windows	Passcode Policy Supported on iOS macOS Android
SCEP Certificate Supported on iOS macOS tvOS Android Windows	Certificate Supported on iOS macOS Android Windows
WiFi Settings Supported on iOS macOS tvOS Android Windows	Privacy and Lock Supported on iOS macOS Android Windows
VPN Settings Supported on iOS macOS Android Knox Windows	Apple AirPlay Supported on iOS macOS
Apple AirPrint Supported on iOS macOS	Contacts Supported on iOS macOS
Encrypted DNS Supported on iOS macOS	Managed App Config Supported on iOS tvOS Android
Exchange ActiveSync Email Supported on iOS Android Knox	Backpack Item Supported on iOS Android

Configuring Cisco Meraki for Android Devices

1. In the **"Managed App Config"** section of the **"New profile"** page select the correct **"App"** and click **"+"**.



New profile

Profile configuration

B1 Endpoint settings

Add settings

Managed App Config

Help

Platform: iOS

App: B1 Endpoint

Settings

Key: Choose a key...

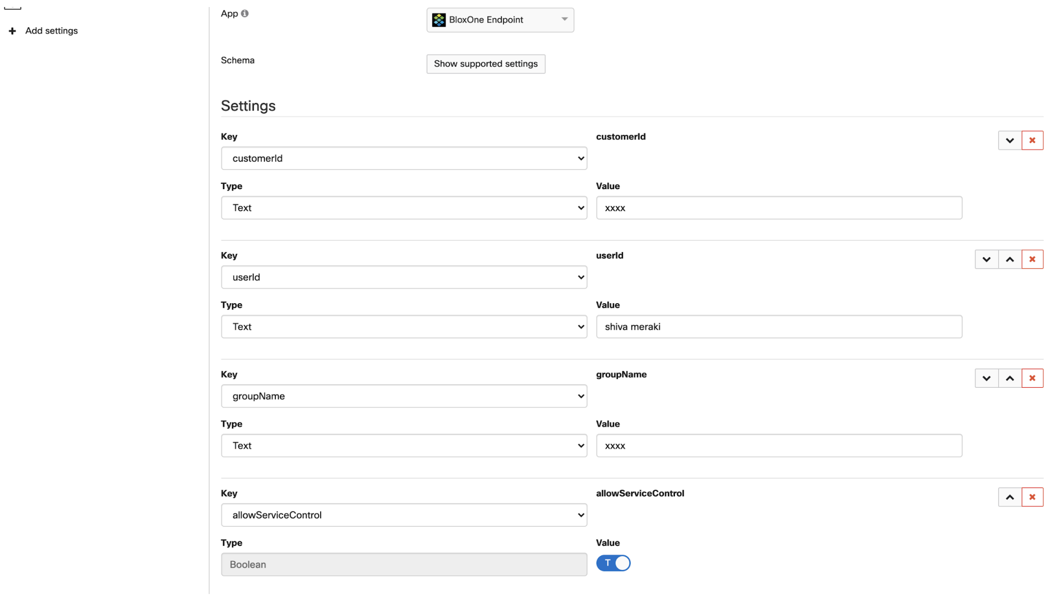
Type: Text

Value:

Cancel Save

(Please allow 1-2 minutes for changes to take effect.)

2. On the **"Settings"** pane, all app configurations will be displayed. Using the app configuration downloaded from the Cloud Services Portal, select each of the app configurations and add the value one-by-one to the in the respective configuration settings values. Configuration values include the following: **"customerId"**, **"userID"**, **"groupName"**, and **"allowServiceControl"**. Click **"Save"** to save your configuration.



Add settings

App: BloxOne Endpoint

Schema: Show supported settings

Settings

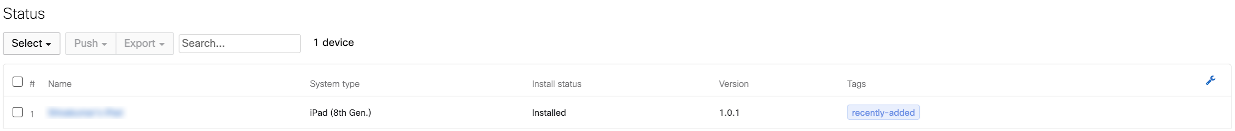
Key: customerId | Type: Text | Value: xxxx

Key: userId | Type: Text | Value: shiva meraki

Key: groupName | Type: Text | Value: xxxx

Key: allowServiceControl | Type: Boolean | Value: T

3. Once the configuration values are added and saved, the new assignment will be pushed to the device. If it is not installed, it can be forcefully pushed from **"System Manager"** → **"Apps"** → **"BloxOne EP"** (scroll down until you see the status and select the device and push).

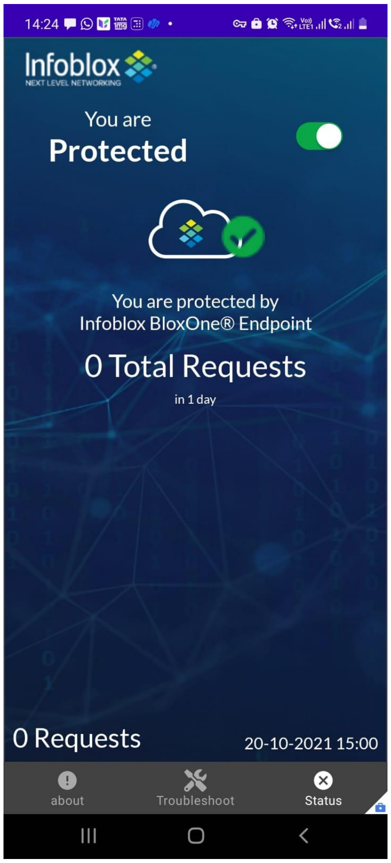


Status

1 device

□ #	Name	System type	Install status	Version	Tags
□ 1	[redacted]	iPad (8th Gen.)	Installed	1.0.1	recently-added

4. BloxOne Endpoint will automatically install on the client devices. Please note that it may take several minutes for the installation to complete.
5. On your Android device, open the **BloxOne EP** app which is located on the work profile screen on Android devices. Accept the VPN acknowledgement. After a few seconds the app will enter into a protected state



You are
Protected

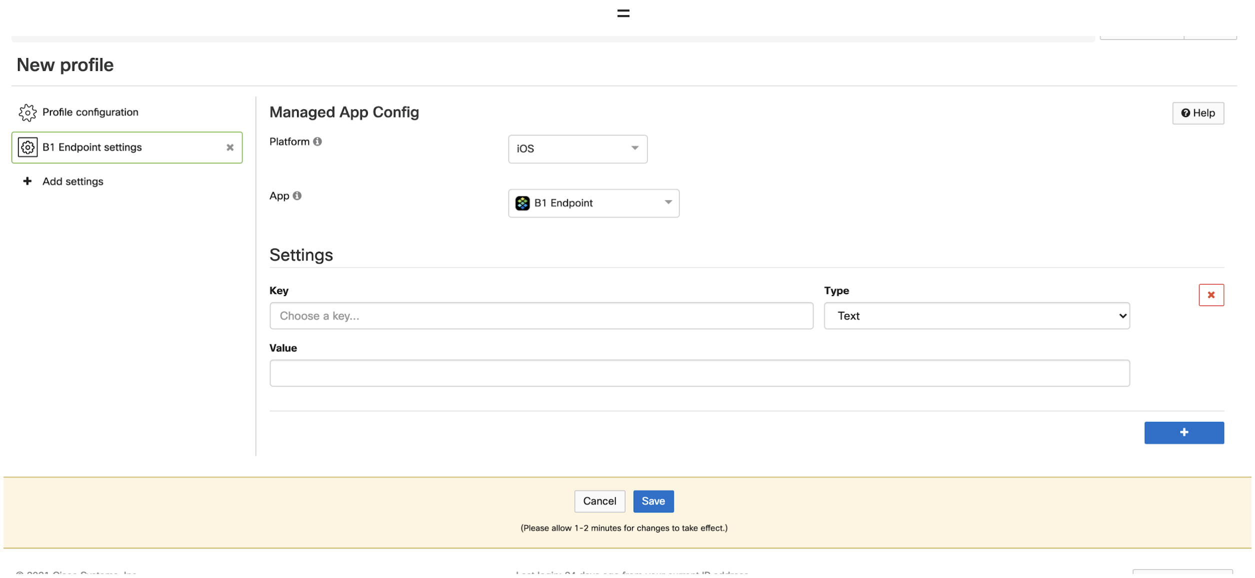
You are protected by
Infoblox BloxOne® Endpoint

0 Total Requests
in 1 day

0 Requests
20-10-2021 15:00

Configuring Cisco Meraki for iOS Devices

1. On the **"New profile"** page in the **"Managed App Config"** section, select **"App"** Add each key and value. Click **"+"** to add to the configuration.
2. Click **"Save"** to save your configuration.


New profile

Profile configuration

B1 Endpoint settings

Add settings

Managed App Config

Help

Platform: iOS

App: B1 Endpoint

Settings

Key: Choose a key...

Type: Text

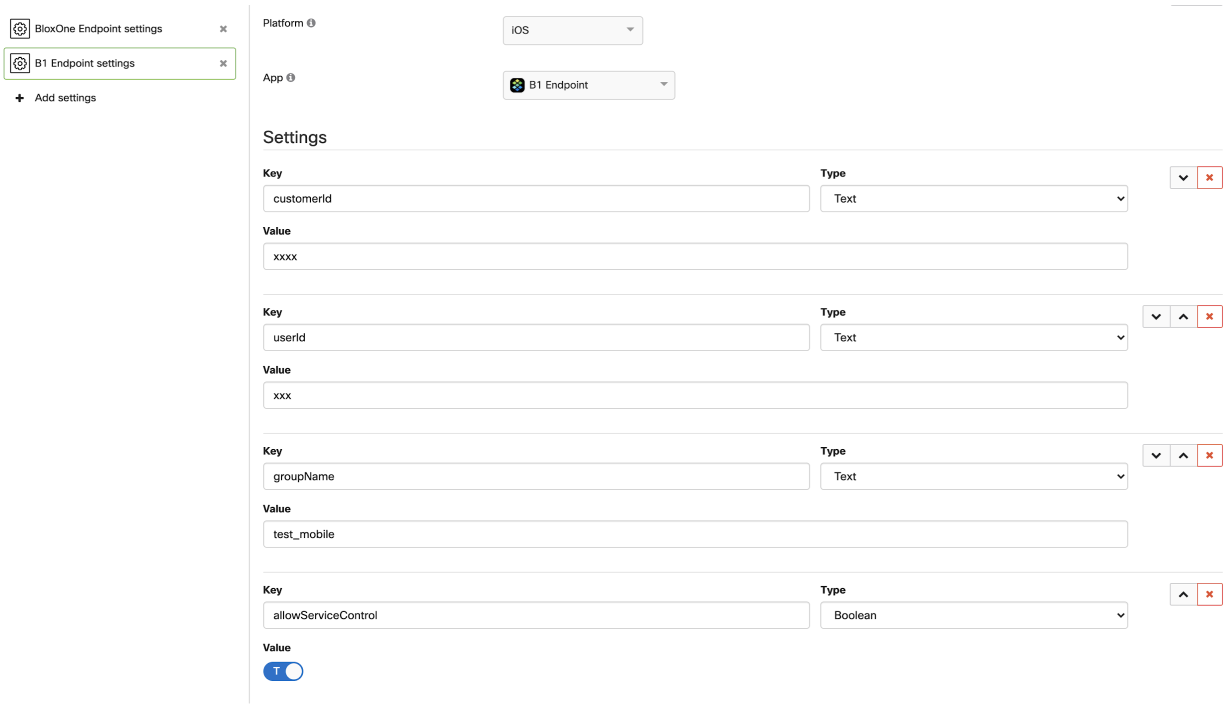
Value:

Cancel

Save

(Please allow 1-2 minutes for changes to take effect.)

3. The BloxOne Endpoint app config will display the following settings: **“customerID”**, **“userID”**, **“groupName”**, and **“showServiceControl”**.


BloxOne Endpoint settings

B1 Endpoint settings

Add settings

Platform: iOS

App: B1 Endpoint

Settings

Key: customerId

Type: Text

Value: xxxx

Key: userId

Type: Text

Value: xxx

Key: groupName

Type: Text

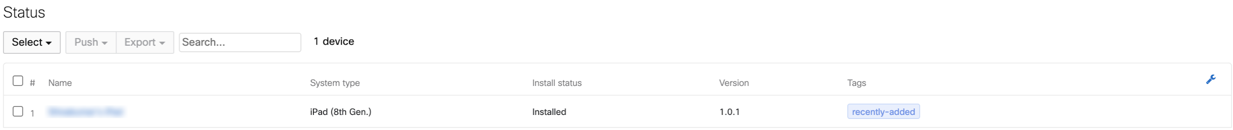
Value: test_mobile

Key: allowServiceControl

Type: Boolean

Value: T

4. Once the configuration has been completed, the new assignment will be pushed to the device. If it is not installed, it can be forcefully pushed from **“System Manager”** → **“Apps”** → **“BloxOne EP”** (scroll down until you see the status and select the device and push).

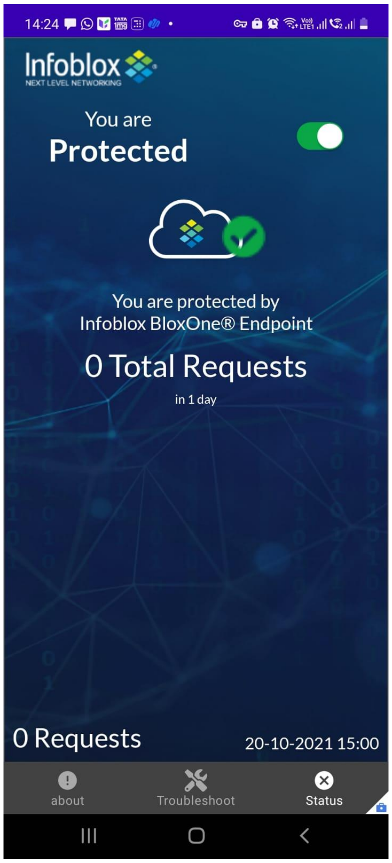


Status

Select ▾ | Push ▾ | Export ▾ | Search... | 1 device

□	#	Name	System type	Install status	Version	Tags
□	1	[redacted]	iPad (8th Gen.)	Installed	1.0.1	recently-added

5. BloxOne Endpoint will automatically install on the client devices. Please note that it may take several minutes for the installation to complete.
6. On your iOS device, open the **“BloxOne EP”** app which is located on the work profile screen and accept the VPN acknowledgement. After a few seconds the app will be in a protected state.



14:24

Infoblox
NEXT LEVEL NETWORKING

You are
Protected

You are protected by
Infoblox BloxOne® Endpoint

0 Total Requests
in 1 day

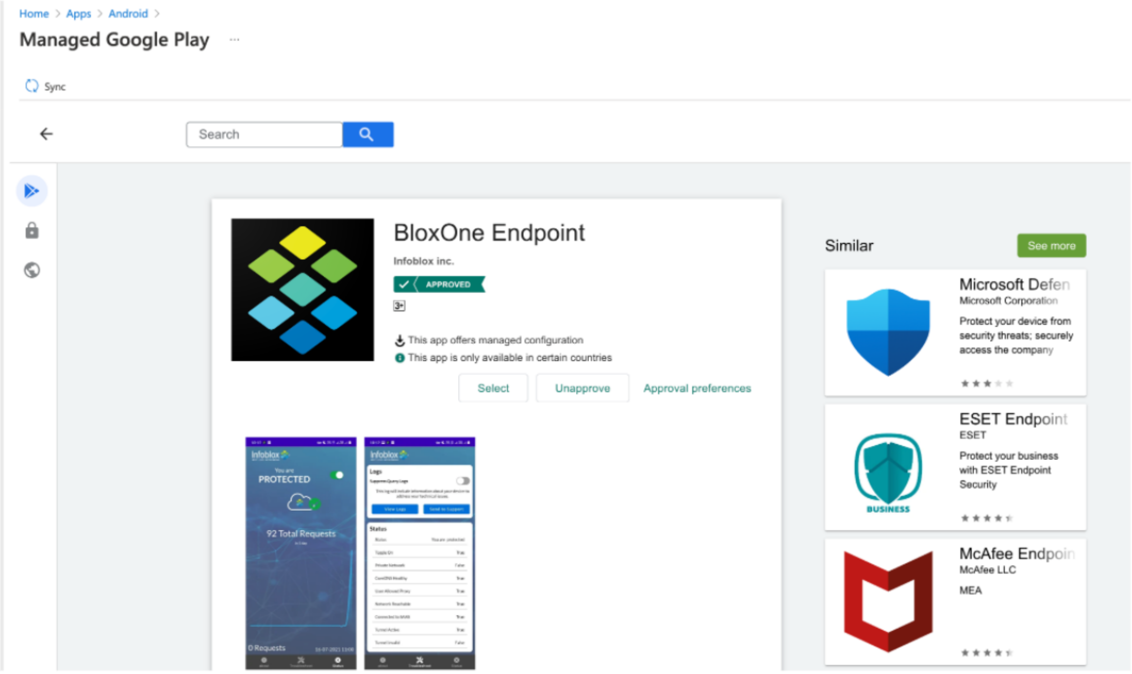
0 Requests 20-10-2021 15:00

Microsoft Intune

Steps for adding the BloxOne app in Microsoft Intune server

To configure Microsoft Intune MDM server for use with Android, perform the following steps:

1. Navigate to **“Home”** → **“Apps”** → **“Android”** → **“Add Managed Google Play”**
2. perform an app search using **“BloxOne”** to find your app.



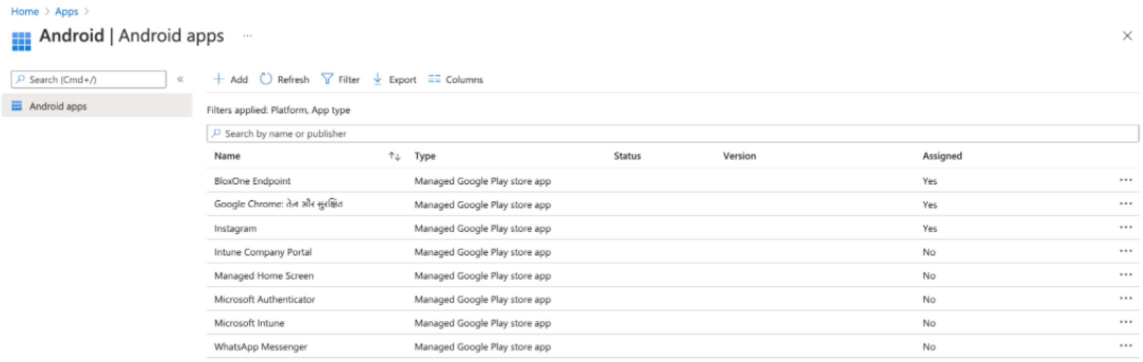
This app offers managed configuration

This app is only available in certain countries

Protect your device from security threats; securely access the company

Protect your business with ESET Endpoint Security

3. Verify the app is listed in the Apps list.



Filters applied: Platform, App type

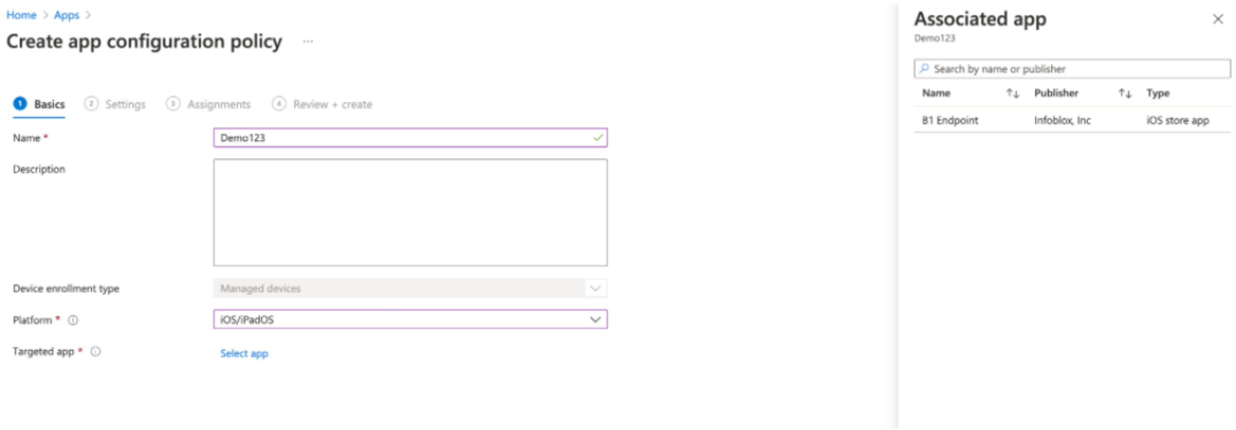
Search by name or publisher

Name	Type	Status	Version	Assigned	
BloxOne Endpoint	Managed Google Play store app			Yes	···
Google Chrome: તેજ ઔર સુરક્ષિત	Managed Google Play store app			Yes	···
Instagram	Managed Google Play store app			Yes	···
Intune Company Portal	Managed Google Play store app			No	···
Managed Home Screen	Managed Google Play store app			No	···
Microsoft Authenticator	Managed Google Play store app			No	···
Microsoft Intune	Managed Google Play store app			No	···
WhatsApp Messenger	Managed Google Play store app			No	···

4. Open the BloxOne app and add the assignments to the app.

MDM App Configuration

App configuration is required to use the BloxOne app.



Home > Apps >

Create app configuration policy ...

1 Basics 2 Settings 3 Assignments 4 Review + create

Name * Demo123

Description

Device enrollment type Managed devices

Platform * iOS/iPadOS

Targeted app * Select app

Associated app

Demo123

Search by name or publisher

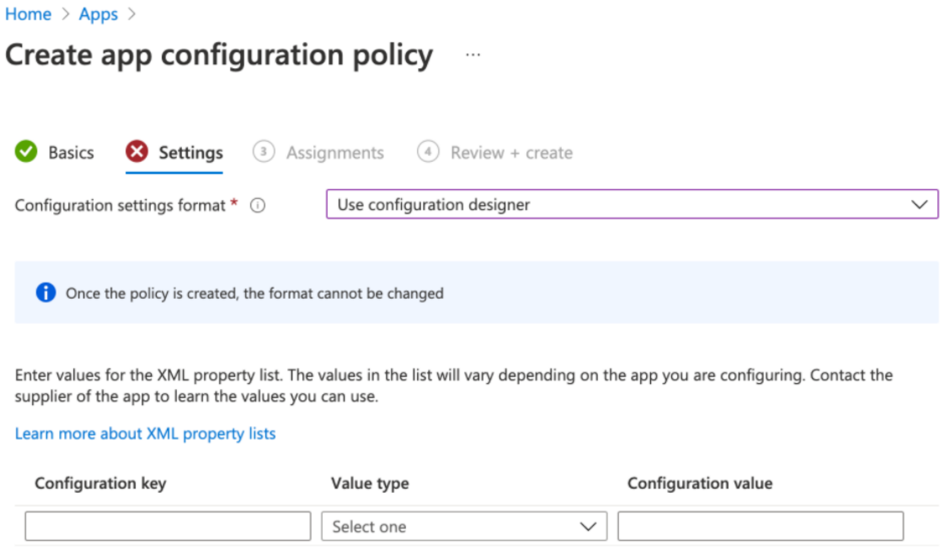
Name	Publisher	Type
B1 Endpoint	Infoblox, Inc	iOS store app

1. Log into the Cloud Services Portal.
2. From the Cloud Services portal, click “**Manage”** → “**Endpoint Groups”** → “**Manage MDM”**.
3. On the **“Manage MDM”** page, the following information can be viewed:
   - **“customerId”** (Use the value present in the xml file)
   - **“groupName”** (Specify the group name in CSP to which endpoint should be moved. If the group name is not present in the CSP, It will be added to the ‘All BloxOne Endpoints’ group).
   - **“userId”** (Name to uniquely identify the mobile device. Configured name will be displayed on the CSP>Endpoints page)On the *Manage MDM* page, the following information can be viewed:
   - **“allowServiceControl”** (By default this value will be ‘True’. Change it to ‘False’ for the toggle button in the app to be hidden).

In MDM, the downloaded app config file can be added manually or by uploading the .xml file.

Perform the following steps to add MDM configuration:

1. Navigate to **“Home”** → **“Apps”** → **“App Configuration Policies”**.
2. Click **“+ Add”** → **“Managed devices”**.
3. Select the device platform (iOS or Android) and select the targeted app.



Home > Apps >

Create app configuration policy ...

✓ Basics ☒ Settings 3 Assignments 4 Review + create

Configuration settings format * Use configuration designer

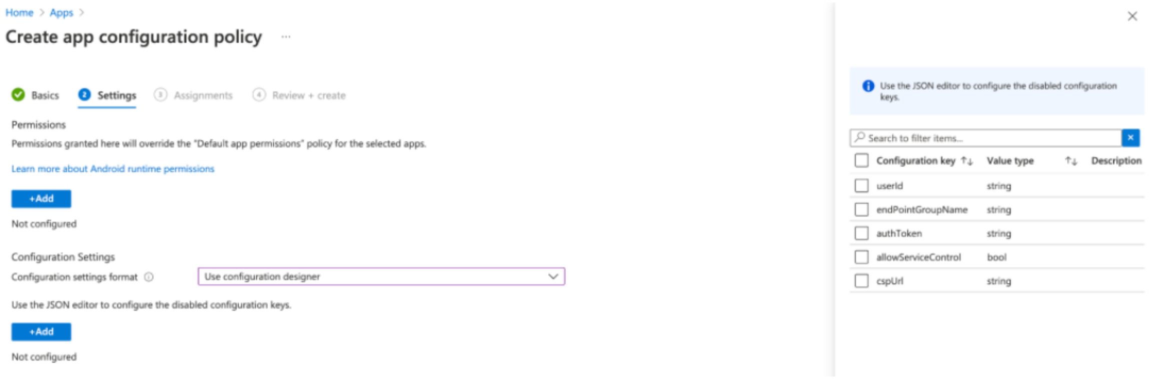
Once the policy is created, the format cannot be changed

Enter values for the XML property list. The values in the list will vary depending on the app you are configuring. Contact the supplier of the app to learn the values you can use.

Learn more about XML property lists

Configuration key	Value type	Configuration value
	Select one	

4. Choose each of the configuration keys and add the respective values to it.



Home > Apps >

Create app configuration policy ...

✓ Basics ② Settings ③ Assignments ④ Review + create

Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

Learn more about Android runtime permissions

+Add

Not configured

Configuration Settings

Configuration settings format: Use configuration designer

Use the JSON editor to configure the disabled configuration keys.

+Add

Not configured

Use the JSON editor to configure the disabled configuration keys.

Search to filter items...

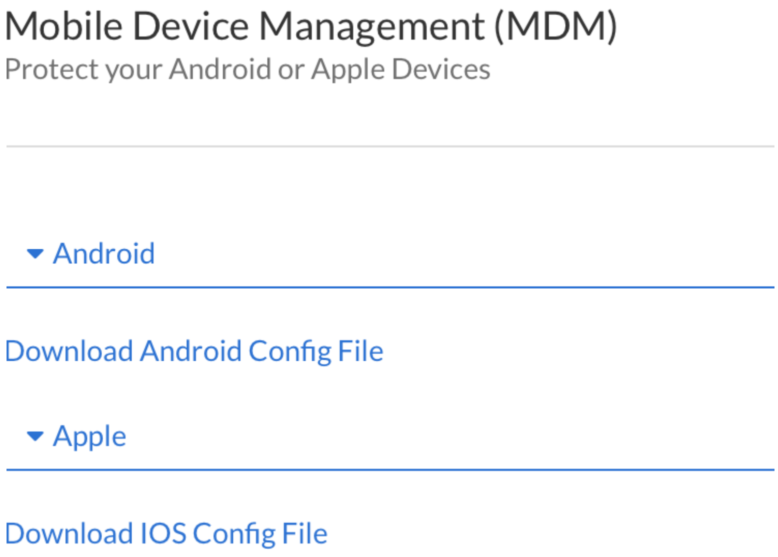
□	Configuration key ↑↓	Value type ↑↓	Description
□	userId	string	
□	endPointGroupName	string	
□	authToken	string	
□	allowServiceControl	bool	
□	cspUrl	string	

5. Go to the device and refresh for the assignments.

Configuring Android

To configure Microsoft Intune MDM server for use with Android, perform the following steps:

1. Add the configuration values to their respective configuration keys.



Mobile Device Management (MDM)

Protect your Android or Apple Devices

▾ Android

Download Android Config File

▾ Apple

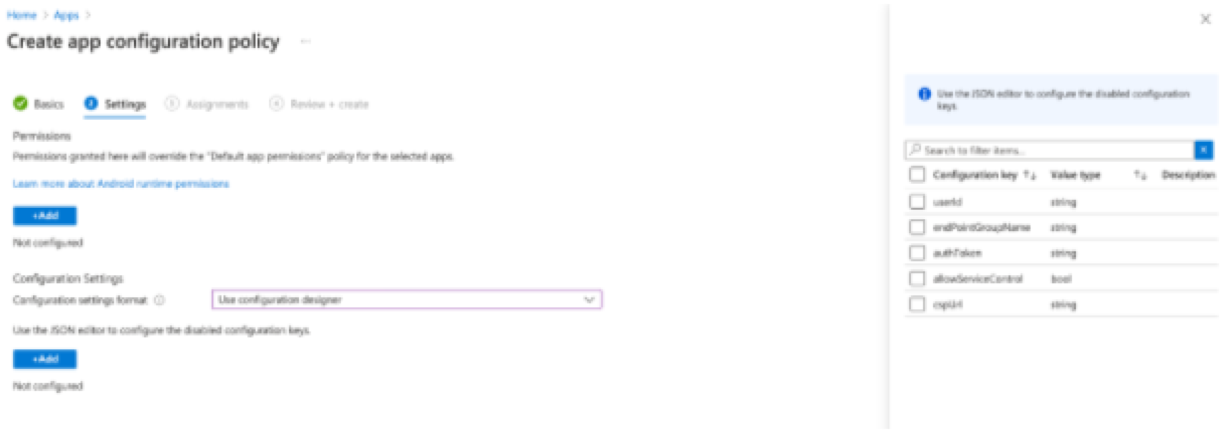
Download IOS Config File

2. Go to the device being configured and refresh to verify the new assignments.

Configuring iOS

To configure Microsoft Intune MDM server for use with iOS, perform the following steps:

1. Add the app config with key and values and create the policy. Note: An XML file can be used or a key/value can be manually entered.



Permissions

Permissions granted here will override the "Default app permissions" policy for the selected apps.

Learn more about Android runtime permissions

Not configured

Configuration Settings

Configuration settings format: Use configuration designer

Use the JSON editor to configure the disabled configuration keys.

Not configured

Use the JSON editor to configure the disabled configuration keys.

	Configuration key	Value type	Description
□	userId	string	
□	endPointGroupName	string	
□	authToken	string	
□	allowServiceControl	bool	
□	cspUrl	string	

2. Go to the device being configured and refresh to verify the new assignments.

MobileIron

To enroll BloxOne Mobile app using MobileIron, do the following:

Prerequisite: The device must be registered with the MobileIron MDM server prior to enrollment.

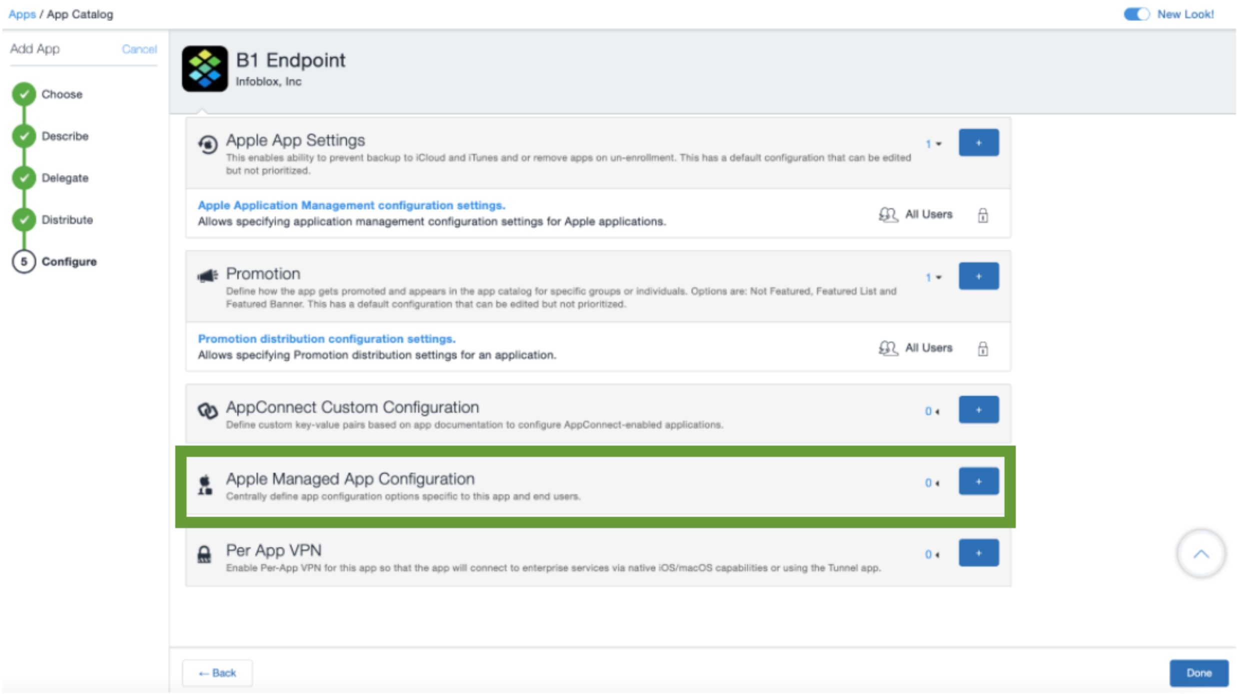
Steps for adding the BloxOne app in MobileIron server

Perform the following steps to add BloxOne Mobile app in Mobiletron server:

1. Navigate to **"Apps"** → **"App Catalog"**,
2. Click **"+ Add"**.
3. Based on your app platform (iOS or Android), choose your app based on your platform (iOS or Android). You can do an app search using **"BloxOne"** to find your app.
4. Configure the BloxOne app as described in the **"MDM App Configuration"** section below.

MDM App Configuration

App configuration is required to use the BloxOne app.



Apple App Settings: This enables ability to prevent backup to iCloud and iTunes and or remove apps on un-enrollment. This has a default configuration that can be edited but not prioritized.

Apple Application Management configuration settings. Allows specifying application management configuration settings for Apple applications.

Promotion: Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritized.

Promotion distribution configuration settings. Allows specifying Promotion distribution settings for an application.

AppConnect Custom Configuration: Define custom key-value pairs based on app documentation to configure AppConnect-enabled applications.

Apple Managed App Configuration: Centrally define app configuration options specific to this app and end users.

Per App VPN: Enable Per-App VPN for this app so that the app will connect to enterprise services via native iOS/macOS capabilities or using the Tunnel app.

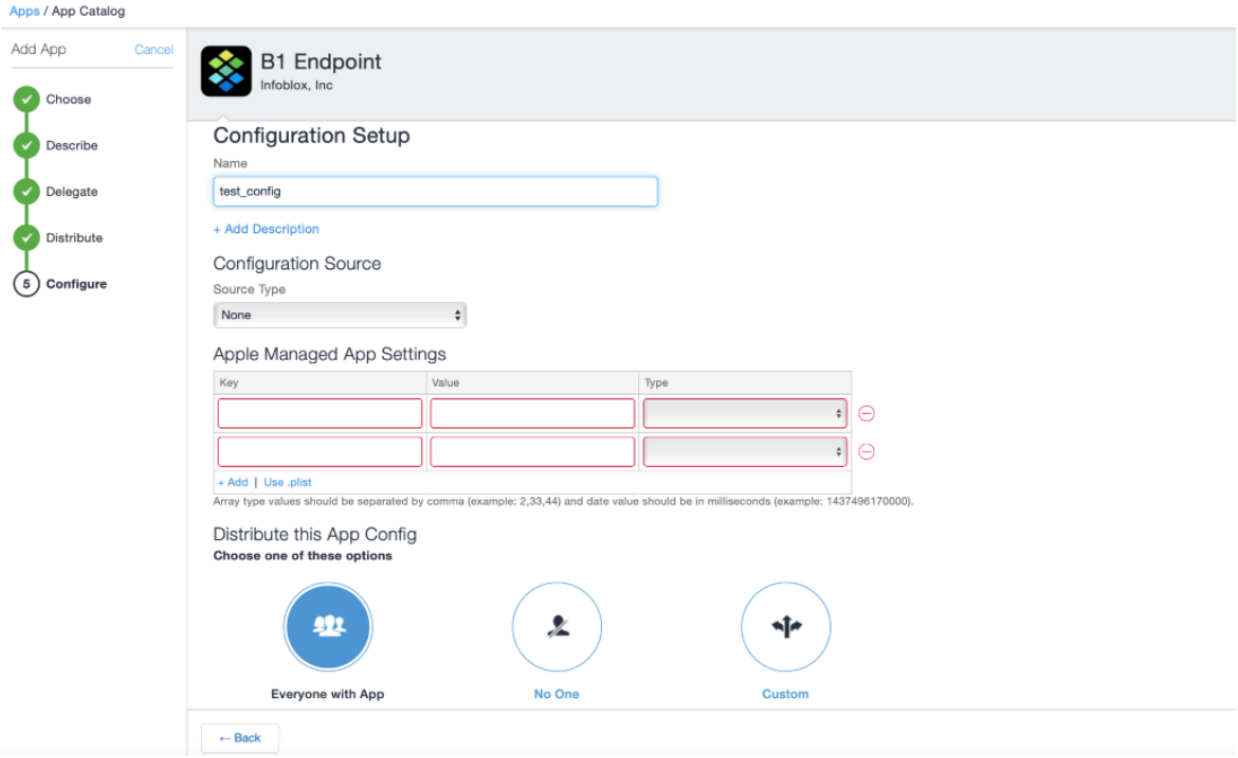
The app configuration file contains the following parameters:

1. Log into the Cloud Services Portal.
2. From the Cloud Services portal, click “**Manage”** → “**Endpoint Groups”** → “**Manage MDM”**.
3. On the **“Manage MDM”** page, the following information can be viewed:
    - ○ **“customerId”** (Use the value present in the xml file)
    - ○ **“groupName”** (Specify the group name in CSP to which endpoint should be moved. If the group name is not present in the CSP, It will be added to the ‘All BloxOne Endpoints’ group).
    - ○ **“userId”** (Name to uniquely identify the mobile device. Configured name will be displayed on the CSP>Endpoints page)On the *Manage MDM* page, the following information can be viewed:
    - ○ **“allowServiceControl”** (By default this value will be ‘True’. Change it to ‘False’ for the toggle button in the app to be hidden).

In MDM, the downloaded app config file can be added manually or by uploading the .xml file.

How to upload or add the config file for Android

1. From the **“Apps Catalog”** page, select **“Managed Configuration for Android”.**



Configuration Setup

Name: test_config

Configuration Source

Source Type: None

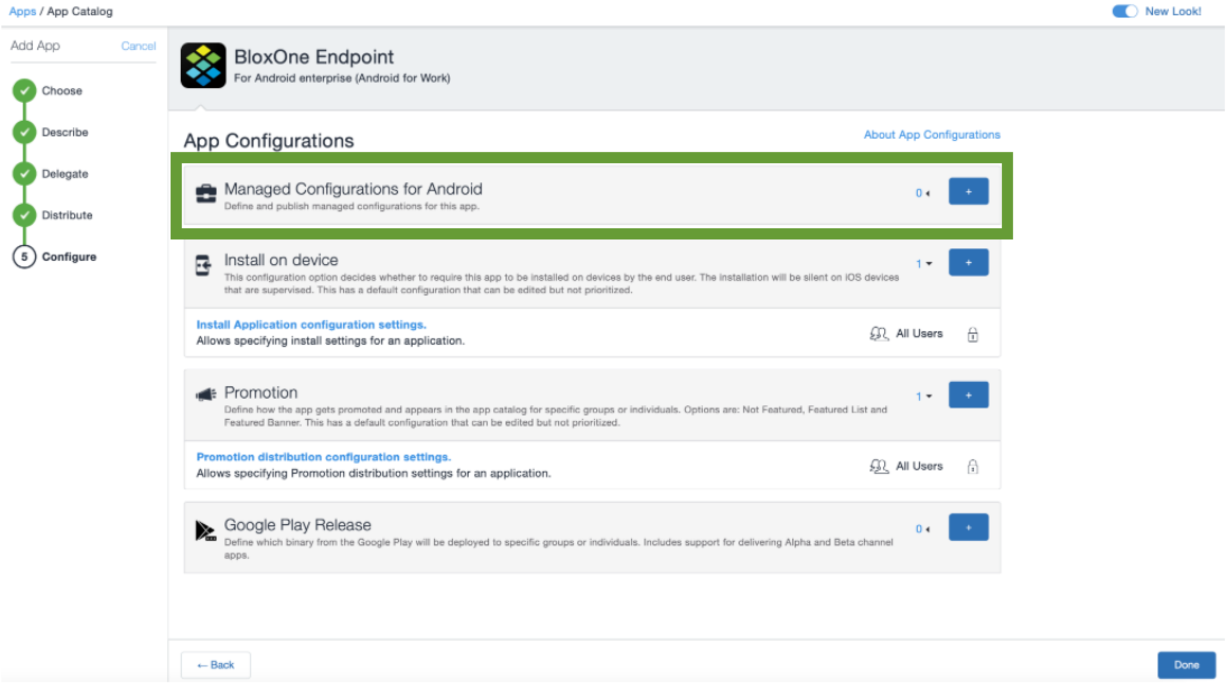
Apple Managed App Settings

Array type values should be separated by comma (example: 2,33,44) and date value should be in milliseconds (example: 1437496170000).

Distribute this App Config

Choose one of these options

2. Add the values to the app config keys section.



App Configurations

Managed Configurations for Android
Define and publish managed configurations for this app.

Install on device
This configuration option decides whether to require this app to be installed on devices by the end user. The installation will be silent on iOS devices that are supervised. This has a default configuration that can be edited but not prioritized.

Install Application configuration settings.
Allows specifying install settings for an application.

Promotion
Define how the app gets promoted and appears in the app catalog for specific groups or individuals. Options are: Not Featured, Featured List and Featured Banner. This has a default configuration that can be edited but not prioritized.

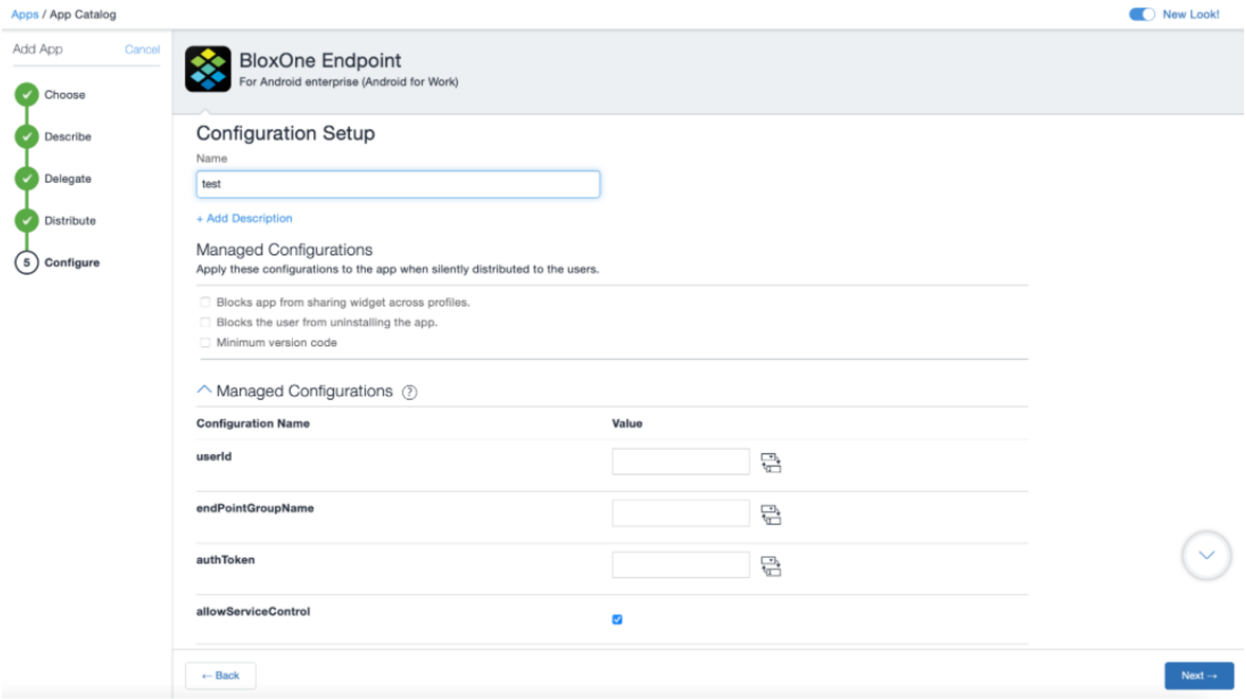
Promotion distribution configuration settings.
Allows specifying Promotion distribution settings for an application.

Google Play Release
Define which binary from the Google Play will be deployed to specific groups or individuals. Includes support for delivering Alpha and Beta channel apps.

3. Click **“Next”** followed by **“Done”** to complete the configuration process.
4. Go to your device and refresh to view the new assignments.

How to upload or add the config file for iOS

1. From the **"Apps Catalog"** page, select **"Apple Managed App Configuration"**.



Apps / App Catalog

New Look!

Add App Cancel

- Choose
- Describe
- Delegate
- Distribute
- 5 Configure

BloxOne Endpoint
For Android enterprise (Android for Work)

Configuration Setup

Name: test

+ Add Description

Managed Configurations
Apply these configurations to the app when silently distributed to the users.

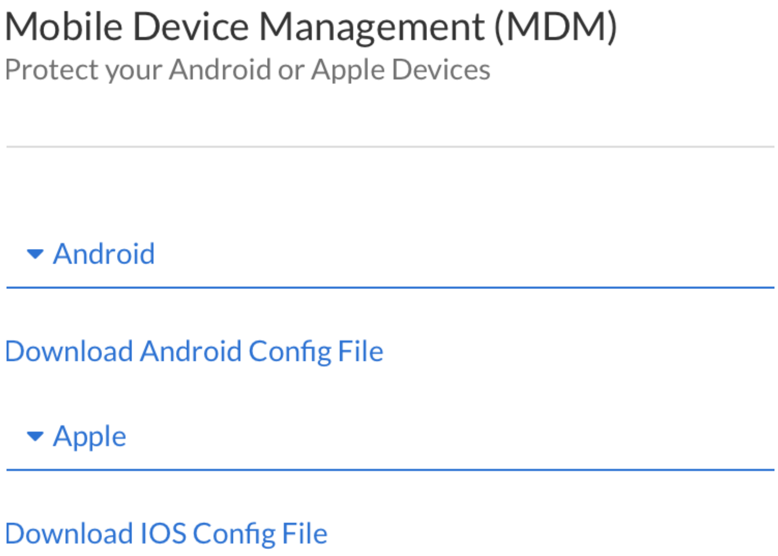
□ Blocks app from sharing widget across profiles.
□ Blocks the user from uninstalling the app.
□ Minimum version code

Managed Configurations

Configuration Name	Value
userId	
endPointGroupName	
authToken	
allowServiceControl	☑

← Back Next →

2. In the Configuration Setup section of the page, import your xml file or manually enter your app configuration information.



Mobile Device Management (MDM)
Protect your Android or Apple Devices

▼ Android

Download Android Config File

▼ Apple

Download IOS Config File

3. Click “**Next”** followed by “**Done”** to complete the configuration process.

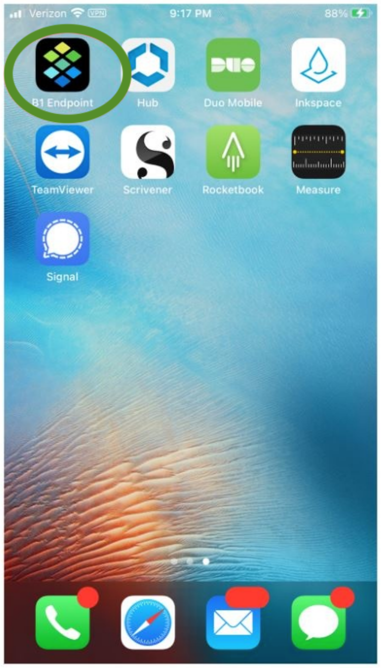
Viewing Mobile Endpoint Devices

Mobile View

To view BloxOne Mobile Endpoint on your device, complete the following:

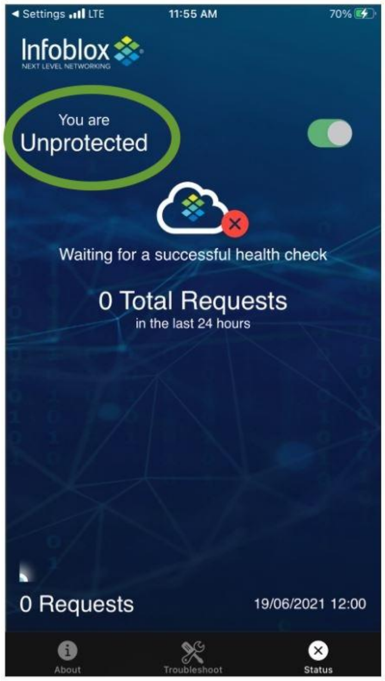
1. **Open BloxOne Mobile Endpoint**

To view BloxOne Mobile Endpoint, tap on the BloxOne Mobile Endpoint icon on the home screen of your device.



2. **BloxOne Endpoint Status**

When you first open the BloxOne Mobile Endpoint application on your device, BloxOne Mobile Endpoint will be turned off by default. You will see the message: “**You are Unprotected**.”



◄ Settings LTE 11:55 AM 70%

You are
Unprotected

Waiting for a successful health check

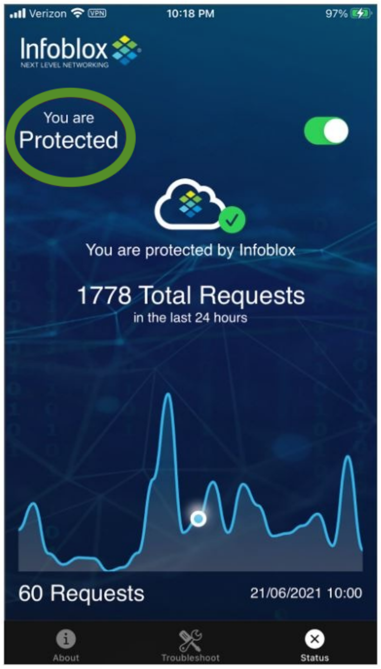
0 Total Requests
in the last 24 hours

0 Requests 19/06/2021 12:00

3. Turning On BloxOne Mobile Endpoint Protection

To turn on Endpoint protection, slide the toggle located in the upper, right-hand quadrant of the BloxOne Mobile Endpoint application screen to the right. BloxOne Mobile Endpoint is now active. You will see BloxOne Mobile Endpoint status change from unprotected to protected status with the following message: **"You are Protected"**.

Health check is performed through Cloud Services Portal and DNS. If it is not possible to achieve a successful health check, then the mobile endpoint will default to an unprotected state until such time a successful health check can be performed.



You are
Protected

You are protected by Infoblox

1778 Total Requests
in the last 24 hours

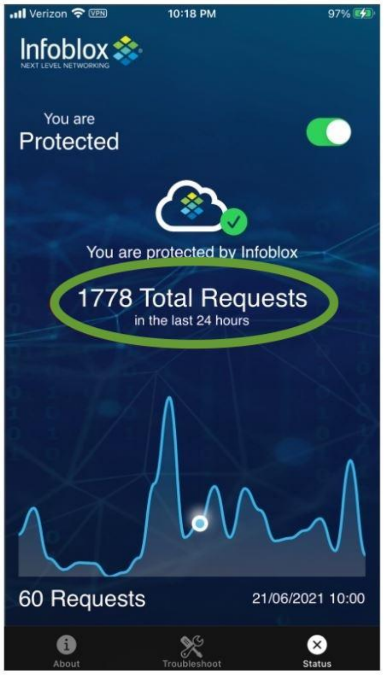
60 Requests 21/06/2021 10:00

4. **Viewing Total Requests**

The total number of requests received in the past 24 hours is displayed in the center of the screen. The graph located at the bottom of the screen displays the number of requests received on an hourly basis for the past 24 hours.

5. **Viewing Hourly Requests**

Dragging the circle item across the graph line allows you to view the number of requests received during any selected one hour period within the past 24 hours.



You are Protected

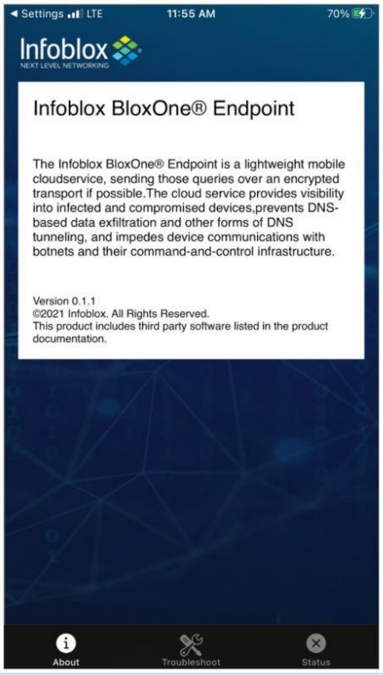
You are protected by Infoblox

1778 Total Requests
in the last 24 hours

60 Requests 21/06/2021 10:00

6. About

The **“About screen”** displays information about the installed BloxOne Mobile Endpoint application.



Infoblox BloxOne® Endpoint

The Infoblox BloxOne® Endpoint is a lightweight mobile cloudservice, sending those queries over an encrypted transport if possible.The cloud service provides visibility into infected and compromised devices,prevents DNS-based data exfiltration and other forms of DNS tunneling, and impedes device communications with botnets and their command-and-control infrastructure.

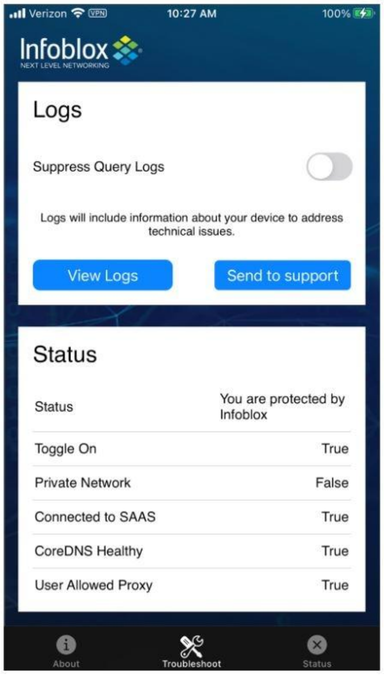
Version 0.1.1
©2021 Infoblox. All Rights Reserved.
This product includes third party software listed in the product documentation.

7. Logs/Status

The **“Logs/Status”** screen allows you to view mobile endpoint logs and mobile endpoint status. The following information can be viewed on the **“Logs/Status”** screen:

- **View Logs**: Tapping **“View Logs”** displays endpoint logs. You can view configuration, application, and query logs.
- **Send to suppor**t: Tapping **“Send to support”** opens a screen where endpoint logs can be sent to support.

Status: The status screen displays the current status for BloxOne Mobile Endpoint.



Logs

Suppress Query Logs ○

Logs will include information about your device to address technical issues.

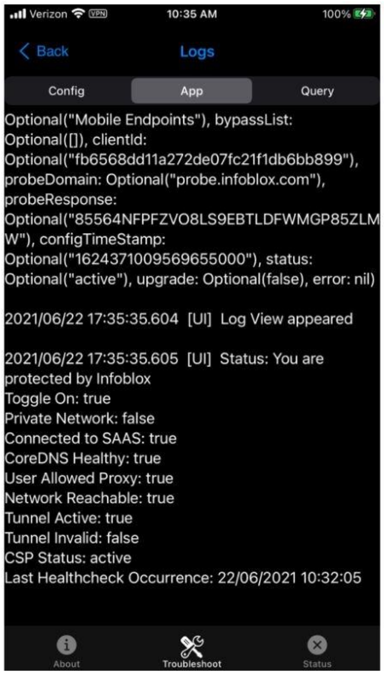
Status

Status	You are protected by Infoblox
Toggle On	True
Private Network	False
Connected to SAAS	True
CoreDNS Healthy	True
User Allowed Proxy	True

8. Logs (Example)

The **“Logs screen”** displays data for the three following log types:

- Config
- App
- Query



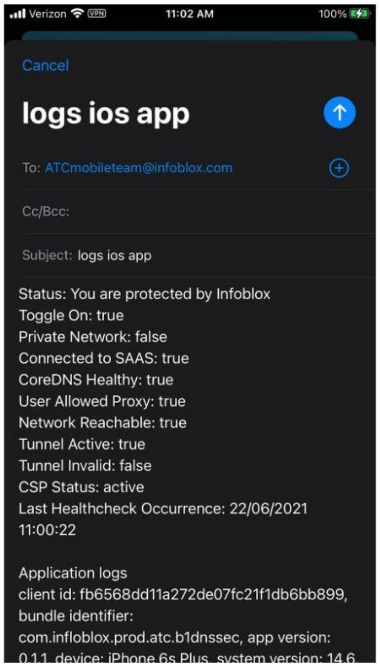
```
Optional("Mobile Endpoints"), bypassList:
Optional([]), clientId:
Optional("fb6568dd11a272de07fc21f1db6bb899"),
probeDomain: Optional("probe.infoblox.com"),
probeResponse:
Optional("85564NFPFZVO8LS9EBTLDFWMGP85ZLM
W"), configTimeStamp:
Optional("1624371009569655000"), status:
Optional("active"), upgrade: Optional(false), error: nil)

2021/06/22 17:35:35.604  [UI]  Log View appeared

2021/06/22 17:35:35.605  [UI]  Status: You are
protected by Infoblox
Toggle On: true
Private Network: false
Connected to SAAS: true
CoreDNS Healthy: true
User Allowed Proxy: true
Network Reachable: true
Tunnel Active: true
Tunnel Invalid: false
CSP Status: active
Last Healthcheck Occurrence: 22/06/2021 10:32:05
```

9. Support

The **"Support"** screen displays the log report ready to be sent to the BloxOne Mobile Endpoint support team.



logs ios app

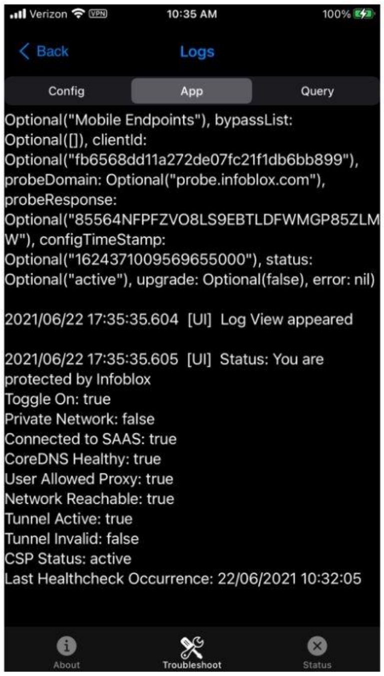
To: ATCmobileteam@infoblox.com

Cc/Bcc:

Subject: logs ios app

```
Status: You are protected by Infoblox
Toggle On: true
Private Network: false
Connected to SAAS: true
CoreDNS Healthy: true
User Allowed Proxy: true
Network Reachable: true
Tunnel Active: true
Tunnel Invalid: false
CSP Status: active
Last Healthcheck Occurrence: 22/06/2021
11:00:22

Application logs
client id: fb6568dd11a272de07fc21f1db6bb899,
bundle identifier:
com.infloblox.prod.atc.b1dnssec, app version:
0.1.1, device: iPhone 6s Plus, system version: 14.6,
```



```
Optional("Mobile Endpoints"), bypassList:
Optional([]), clientId:
Optional("fb6568dd11a272de07fc21f1db6bb899"),
probeDomain: Optional("probe.infoblox.com"),
probeResponse:
Optional("85564NFPFZVO8LS9EBTLDFWMGP85ZLM
W"), configTimeStamp:
Optional("1624371009569655000"), status:
Optional("active"), upgrade: Optional(false), error: nil)

2021/06/22 17:35:35.604  [UI]  Log View appeared

2021/06/22 17:35:35.605  [UI]  Status: You are
protected by Infoblox
Toggle On: true
Private Network: false
Connected to SAAS: true
CoreDNS Healthy: true
User Allowed Proxy: true
Network Reachable: true
Tunnel Active: true
Tunnel Invalid: false
CSP Status: active
Last Healthcheck Occurrence: 22/06/2021 10:32:05
```

Infoblox Cloud Service Portal View

Devices

To view BloxOne Mobile Endpoint in the Cloud Services Platform, complete the following:

On the **“Mobile Endpoints”** page, the Cloud Services Portal displays the list of mobile devices, including devices on which BloxOne Mobile Endpoint has been installed. You can view detailed information about these devices and their current status. By default, this list includes all devices that are active, inactive, or disabled. By default, the Cloud Services Portal displays the first page of endpoint devices.

To view information about mobile devices, complete the following:

1. From the Cloud Services Portal, click **“Manage”** → **“Endpoints”**.
2. On the **“Mobile Endpoints”** page, the Cloud Services Portal displays the following for each device on which Endpoint is installed:
    - **Active**: The device is currently online and active.
    - **Inactive**: The device is currently offline and inactive.
    - **Disabled**: The device has been disabled.
    - **DEVICE NAME**: The name of the device.
    - **USER NAME**: The user name that is used to log in to this device.
    - **ENDPOINT GROUP**: The BloxOne Group to which the device belongs.
    - **MAC ADDRESS**: The MAC address for the device.
    - **ENDPOINT VERSION**: The BloxOne Endpoint version that is installed on the device.
    - **OS VERSION**: The OS version that is currently running on the device.
    - **LAST SEEN**: The timestamp when the device was last seen on the network.
    - **LAST IP ADDRESS**: The list of IP addresses that have been associated with this device.
    - **STATUS**: The current status of the device.

On the **“Mobile Endpoints”** page, you can select a mobile device and click the **“Endpoint Status”** tab to enable or disable the mobile device.

To enable or disable a mobile device, select the mobile device and click ≡ → to **“enable”** or **“disable”** it. To remove a mobile device, select the mobile device. Note that the selected mobile device must be disabled prior to its removal. Click ≡ → **“Remove”** to delete the mobile device. You can also select the respective mobile device and click the **“Remove”** button to delete it.

You can also perform the following on the **“Mobile Endpoints”** page:

- Select a mobile endpoint device and click “**Move”** to move it to a different endpoint group.
- Click “**Export to CSV”** to download a list of BloxOne Mobile Endpoints.
- Click the **“Refresh”** button to update data on this page. Active filters will be preserved when refreshing the records.
- Click ≡▾ to select the columns you want to display or use the arrow keys to reorder the columns.
- Select an endpoint to view additional details in the right panel. You can collapse the right panel by clicking ⓘ.
- Enter the value that you want to search in the **“Search”** text box. The Cloud Services Portal displays the list of records that match the keyword in the text box.

- Click ▼ and then ⊕ to filter data by the available values.
- **Column Sorting**: All columns on the page can be sorted by clicking the label in the column header. When the sorting order is changed, the page view will default back to the first page of records.
- **Page Size Control**: Select the number of records to view per page by clicking the view option (25, 50, 100) on the bottom-left of the screen.
- **Page View**: Select what page of records to view by clicking the page option (Page 1, 2, . . .) located on the bottom-right of the screen.

Groups

To view BloxOne Mobile Endpoint Groups in the Cloud Services Platform, complete the following:

On the **“Endpoint Groups”** page, the Cloud Services Portal displays the list of all endpoint groups residing on your network. An Endpoints Group is a defined group of endpoints containing any number of endpoints (minimum of one endpoint). You can view detailed information about an endpoint group along with the current status of each endpoint that is a member of the endpoint group. By default, the Cloud Services Portal displays the name of the endpoint group, including the number of endpoints residing within an endpoint group, any internal domains lists and associated security policies, and if bypass mode has been enabled or applied to an endpoint group.

To view information about Endpoint devices, navigate to the “**Manage”** → “**Endpoint Groups”** page which displays the list of Endpoint groups you have created.

To view information about Endpoint groups, complete the following:

1. From the Cloud Services Portal, click **“Manage”** → **“Endpoints”**.
2. On the **“Endpoints”** page, click the **“Endpoint Groups”** tab.
3. Cloud Services Portal displays the following for each Endpoint group:
    - **NAME** : The name of the endpoint group.
    - **DESCRIPTION:** The description about the group.
    - **ENDPOINTS**: The total number of endpoints in the group.
    - **INTERNAL DOMAINS LIST**: The internal domains list contains domains served by local DNS servers that you want to reach without interruptions.
    - **ASSOCIATED POLICY**: The name of the security policy with which the group is associated.
    - **BYPASS MODE**: Bypass mode must be enabled on the group level so that the bypass configuration can be used. The bypass mode setting is inherited whenever a new endpoint group is created. The user can change the settings at a group level. The group level setting will override the setting established at the default endpoint group setting.
    - **STATUS**: The current status for the endpoint group.; Enabled, Disabled, or Inactive,
    - **PERIOD OF INACTIVITY**: The length of time the endpoint has been inactive (0-180 days).

On the **“Viewing Endpoint Groups”** page, you can click **“Manage MDM”** to display the **“Mobile Device Management (MDM)”** page. On the **“Mobile Device Management (MDM)”** page, you can download the configuration file for Android or Apple iOS devices.

You can also perform the following on the *Endpoint* page:

- Select an endpoint group and click ≡ → **“Edit”** to modify endpoint group information. You can also select the respective endpoint group and click the **“Edit”** button to modify it.

- Select an endpoint group and click ≡ → **“Remove”** to delete the endpoint group. You can also select the respective endpoint group and click the **“Remove”** button to delete it.
- Select an endpoint device and click **“Move”** to move it to a different endpoint group.
- Click **“Export to CSV”** to download a list of BloxOne Endpoint groups.
- Click the **“Refresh”** button to update data on this page. Active filters will be preserved when refreshing the records.
- Click ≡▾ to select the columns you want to display or use the arrow keys to reorder the columns.
- Select an endpoint group to view additional details in the right panel. You can collapse the right panel by clicking ⓘ .
- Enter the value that you want to search in the **“Search”** text box. The Cloud Services Portal displays the list of records that match the keyword in the text box.
- Click ▼ and then ⊕ to filter data by the available values.
- **Column Sorting**: All columns on the page can be sorted by clicking the label in the column header. When the sorting order is changed, the page view will default back to the first page of records.
- **Page Size Control**: Select the number of records to view per page by clicking the view option (25, 50, 100) on the bottom-left of the screen.
- **Page View**: Select what page of records to view by clicking the page option (Page 1, 2, . . .) located on the bottom-right of the screen.

Reporting

To view BloxOne Mobile Endpoint Reports in the Cloud Services Platform, complete the following:

You can view the DNS Hits section of the *DNS Activity Report* to see BloxOne Mobile Endpoint activity. To view the DNS Hits section of the *DNS Activity Report*, navigate to the **“Reports”** section in the Cloud Services Portal (**“Reports”** → **“DNS Activity”** → **“DNS”**)

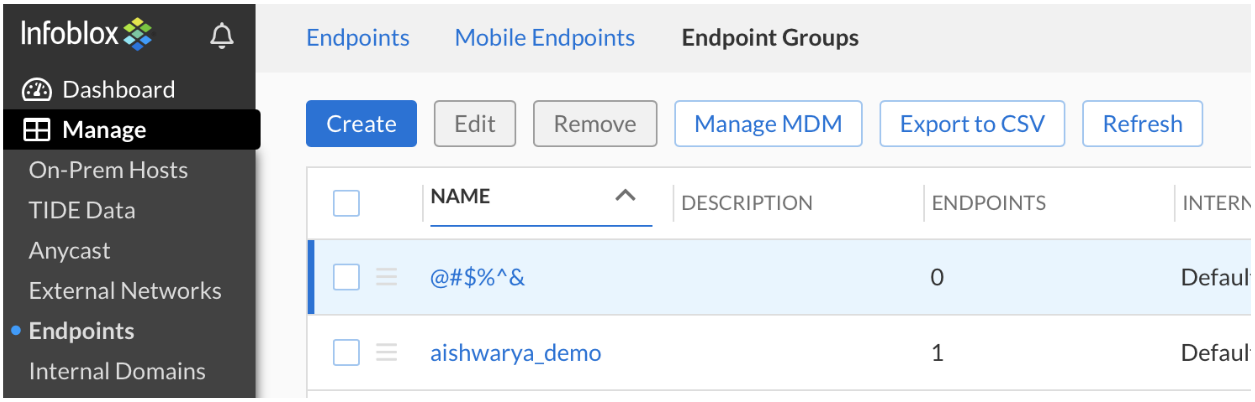
For additional information on the DNS Activity Report, see the DNS Activity Report.

VMware Workspace One (AirWatch)

Downloading the MDM Config File from the Cloud Services Portal

To download the BloxOne Mobile app from the Cloud Services Portal, complete the following steps.

1. Download the app config file from the Cloud Services Portal. (**“Manage”** → **“Endpoints”** → **“Endpoint Groups”** → **“Manage MDM”**). An app config file is available for both Android and iOS devices. The app config file is required for updating the application configuration in MDM.

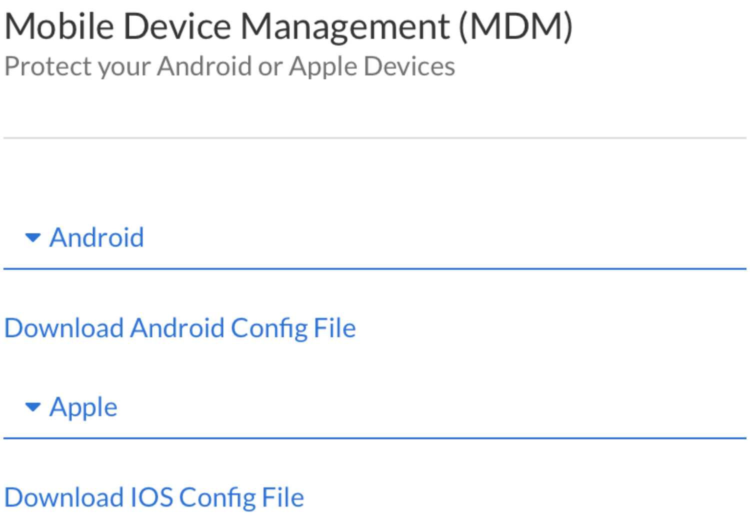


NAME	DESCRIPTION	ENDPOINTS	INTERN
@#$%^&		0	Defaul
aishwarya_demo		1	Defaul

2. On the **“Mobile Device Management (MDM)”** screen, download the config file for your device. For Android devices, click **“Download Android Config File”**. For iOS devices click **“Download iOS Config File”**.

The config file contains the following parameters. Edit and update each parameter as instructed:

- **customerId**: Use the value present in the .xml file.
- **groupName**: Specify the group name in the Cloud Services Portal to which the endpoint should be moved. If the endpoint group name is not present in the Cloud Services Portal, it will be added to the **All BloxOne Endpoints** group.
- **userId**: Choose a name that uniquely identifies the mobile device. The configured name will be displayed on the *Endpoints* page.
- **allowServiceControl**: By default this value will be **“True”**. Change this value to **“False”** if you want the toggle button in the BloxOne app to be hidden.


Mobile Device Management (MDM)

Protect your Android or Apple Devices

Registering Mobile Endpoint to VMWare Workspace One Server

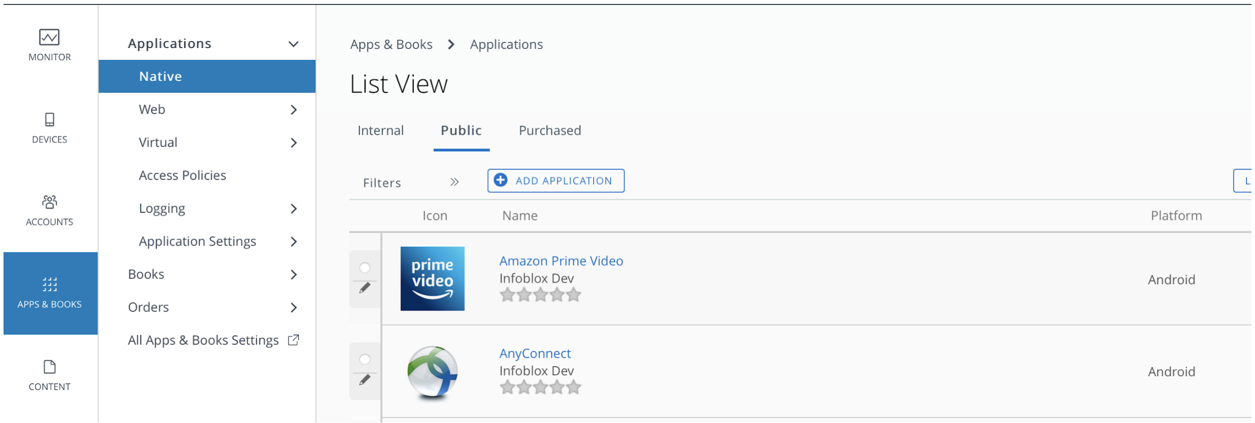
To register a mobile endpoint with the VMWare Workspace One server, complete the following steps.

1. Install the **"Intelligent Hub"** app from the play store/app store. For additional information, see Downloading and Enrolling of BloxOne Mobile Endpoint on Your Device.
2. Login to **"Intelligent Hub"** using the credentials provided by your admin. For additional information, see Enrollment of BloxOne Mobile using Workspace One MDM.
3. Follow the steps provided to register your device to the Workspace One server.

Installing the BloxOne App in Workspace One Server on an Android Device

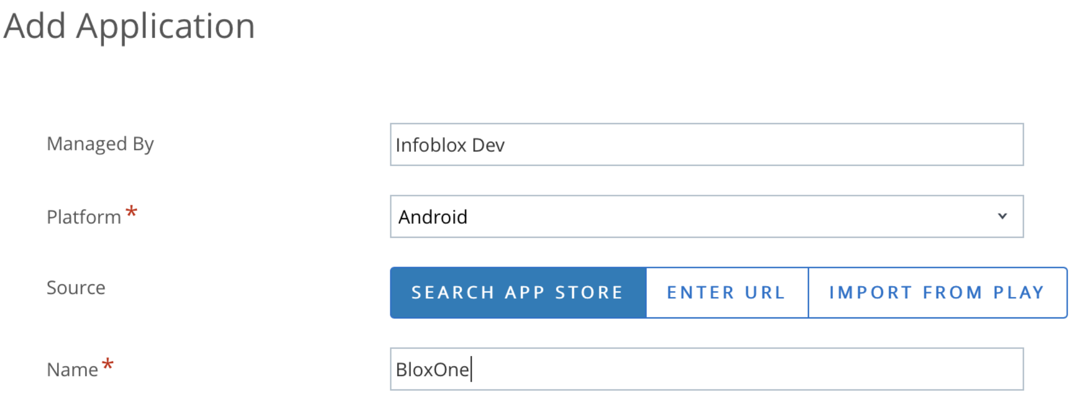
To install on an Android device, complete the following: steps

1. Login to the Workspace One UEM console.
2. Navigate to **"Apps & Books"** → **"Applications"** → **"Native"** → **"Public"**.
3. Click **"+ Add Application"**.



Icon	Name	Platform
	Amazon Prime Video Infoblox Dev	Android
	AnyConnect Infoblox Dev	Android

4. Select platform as Android. Search for BloxOne EP and click **"Next"**.



Add Application

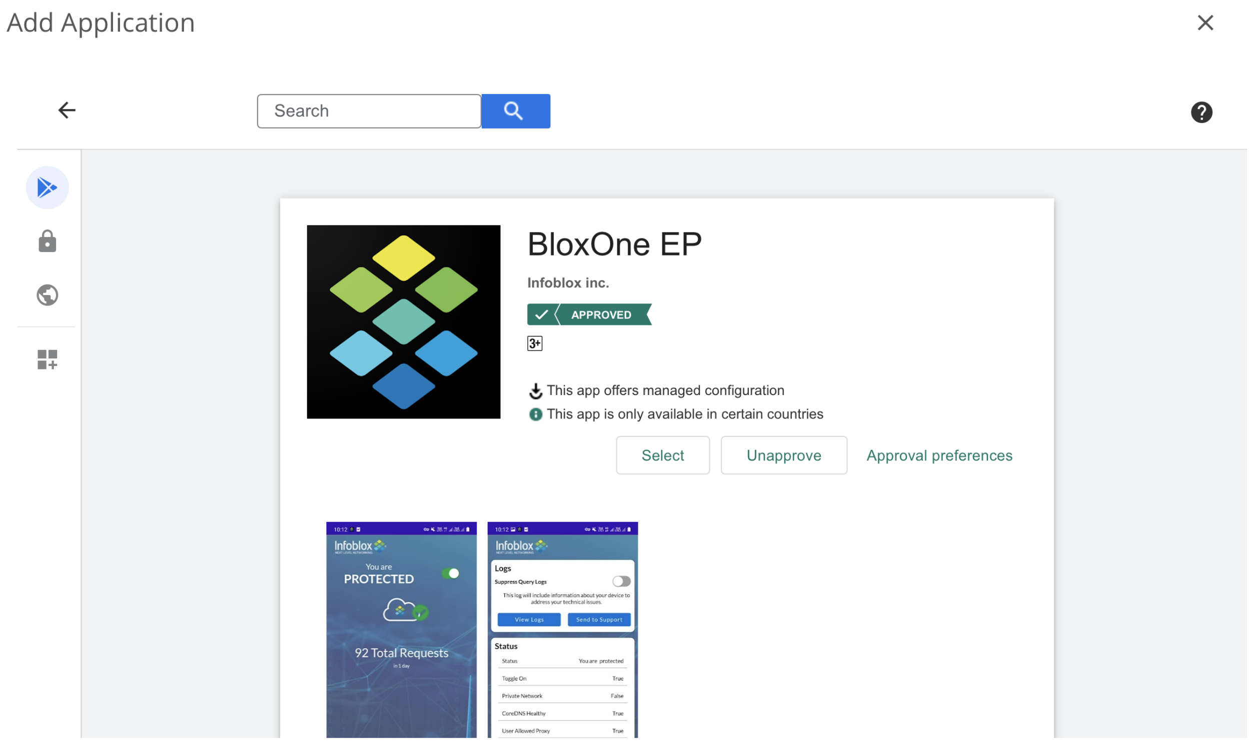
Managed By: Infoblox Dev

Platform *: Android

Source: SEARCH APP STORE | ENTER URL | IMPORT FROM PLAY

Name *: BloxOne

5. Click **“Approve”** and **“Select”**.



Add Application

BloxOne EP

Infoblox inc.

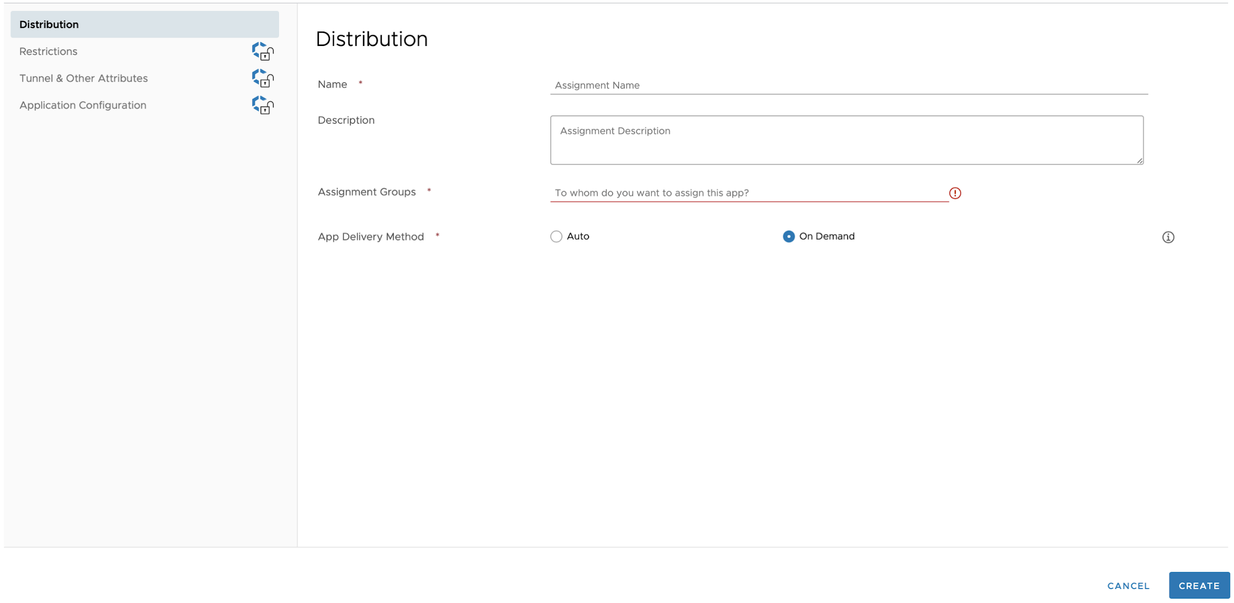
APPROVED

3+

This app offers managed configuration

This app is only available in certain countries

6. Click **“Save and Assign”**. The app assignment distribution window will open.
7. In the Distribution window, provide information for the following fields: **Name**, **Description, Assignment Groups,** and **App Delivery** method. For App Delivery method, select **“On Demand”**.
8. Click **“Create”**.



Distribution

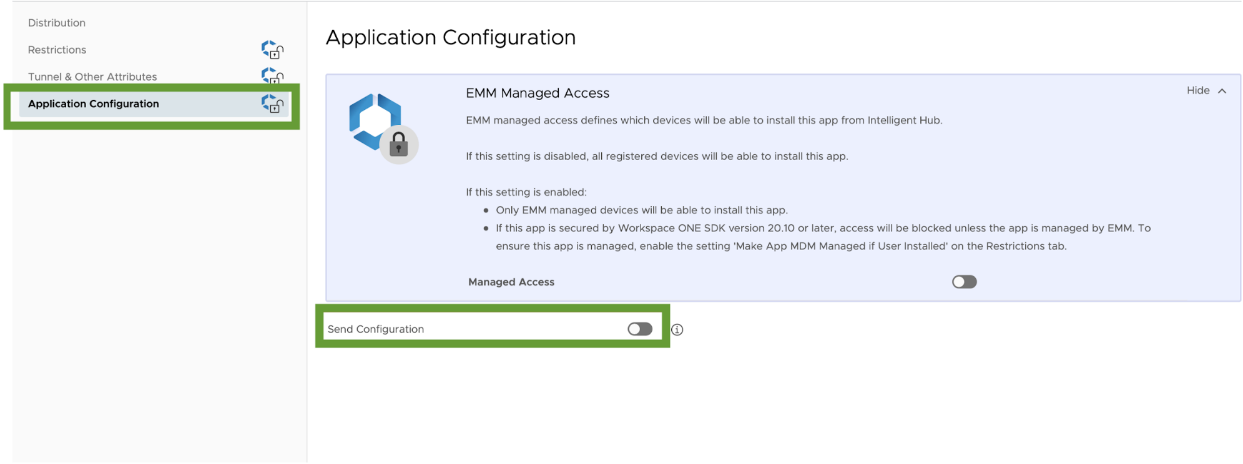
Name * Assignment Name

Description Assignment Description

Assignment Groups * To whom do you want to assign this app?

App Delivery Method * ○ Auto ● On Demand

9. Navigate to the Application Configuration page and toggle the **“Send Configuration”** button to the ON position.



Distribution
Restrictions
Tunnel & Other Attributes
Application Configuration

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

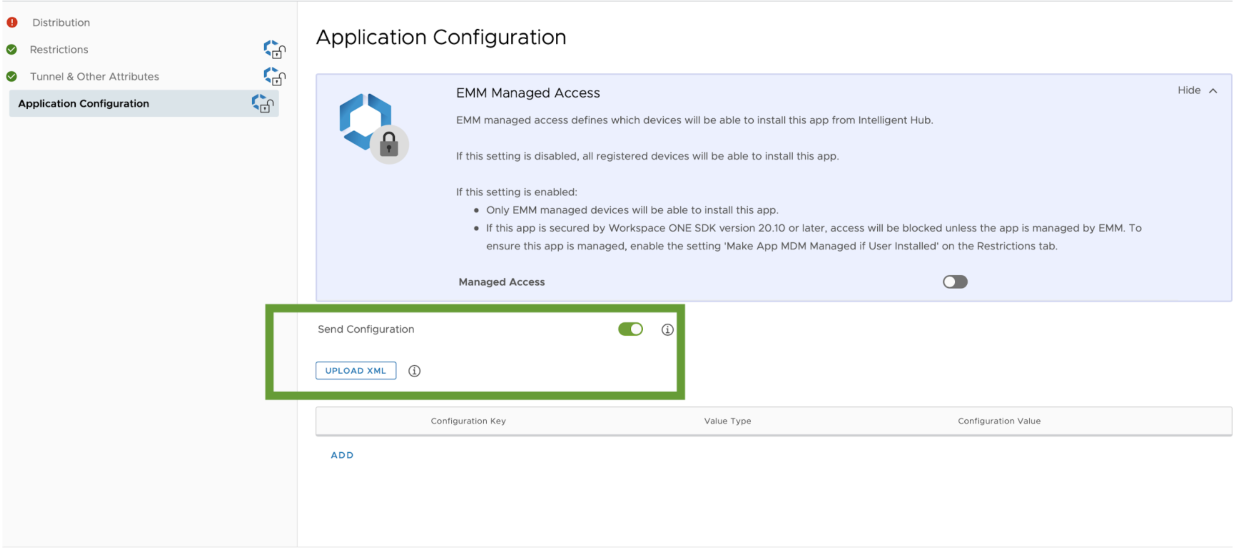
If this setting is enabled:

- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access

Send Configuration

10. Upload the configuration file previously downloaded from the Cloud Services Portal.
11. Click **“UPLOAD XML”** and select the file to be uploaded.



Distribution
Restrictions
Tunnel & Other Attributes
Application Configuration

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled:

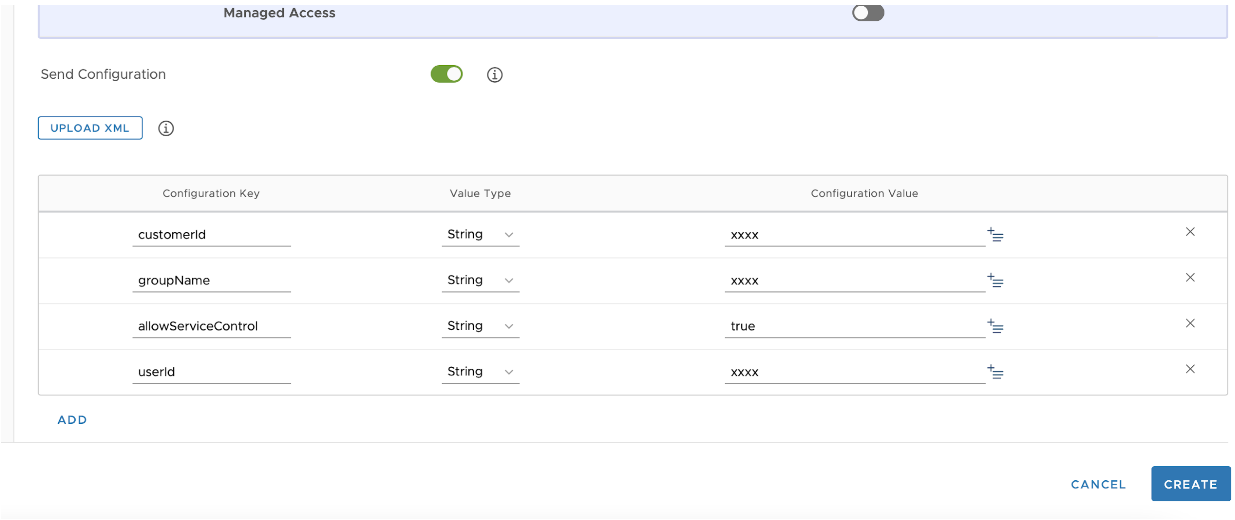
- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access

Send Configuration

Configuration Key	Value Type	Configuration Value

12. Click **“CREATE”** to create the configuration.

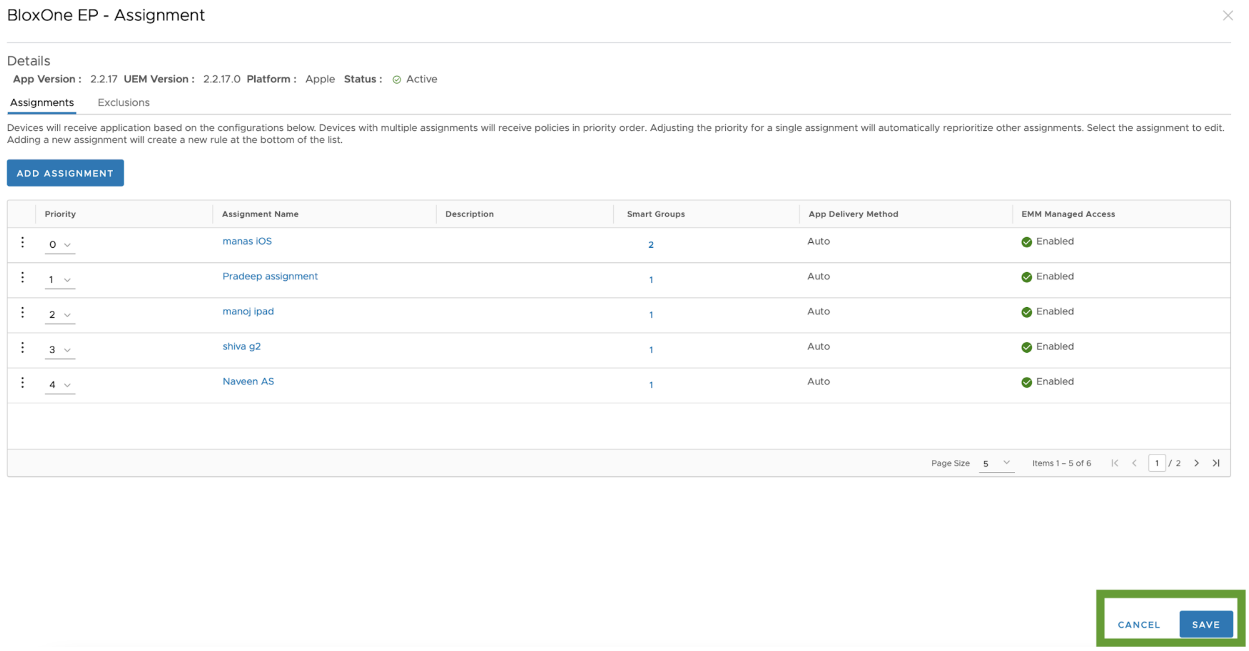


Managed Access

Send Configuration

Configuration Key	Value Type	Configuration Value
customerId	String	xxxx
groupName	String	xxxx
allowServiceControl	String	true
userId	String	xxxx

13. Click **"SAVE"** to save the created configuration.



BloxOne EP - Assignment

Details

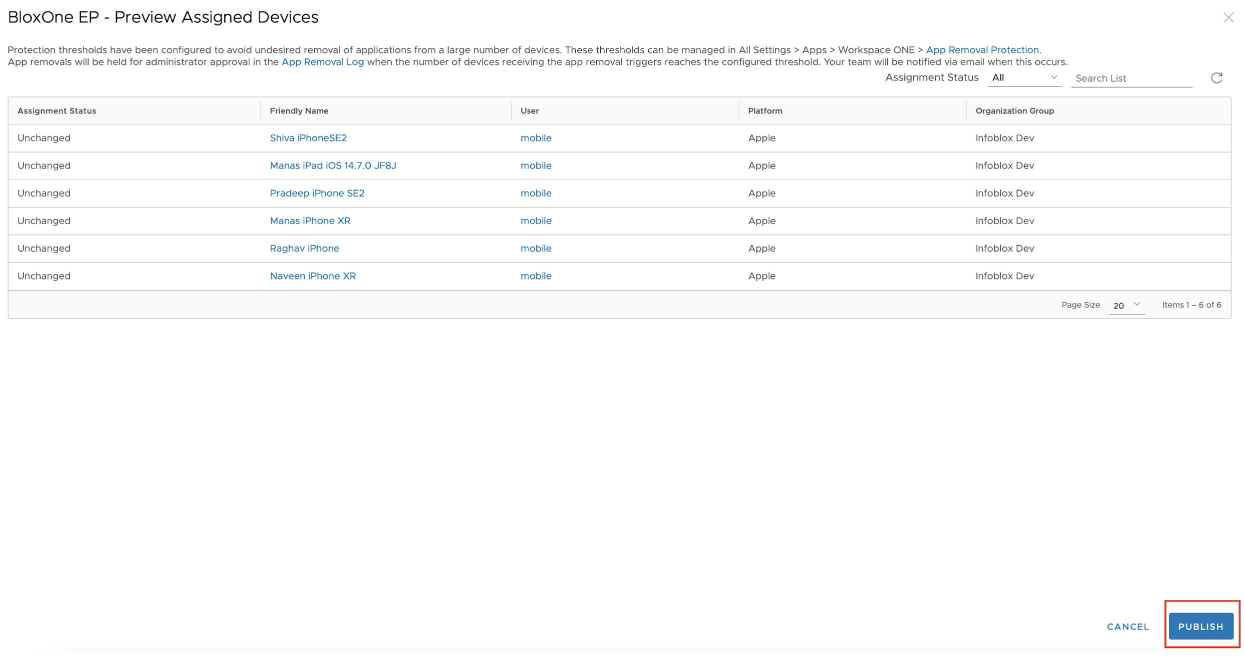
App Version : 2.2.17 **UEM Version :** 2.2.17.0 **Platform :** Apple **Status :** Active

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically reprioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

Priority	Assignment Name	Description	Smart Groups	App Delivery Method	EMM Managed Access
0	manas iOS		2	Auto	Enabled
1	Pradeep assignment		1	Auto	Enabled
2	manoj ipad		1	Auto	Enabled
3	shiva g2		1	Auto	Enabled
4	Naveen AS		1	Auto	Enabled

Page Size 5 Items 1 – 5 of 6 1 / 2

14. Click **"PUBLISH"** to finalize the configuration creation process.



BloxOne EP - Preview Assigned Devices

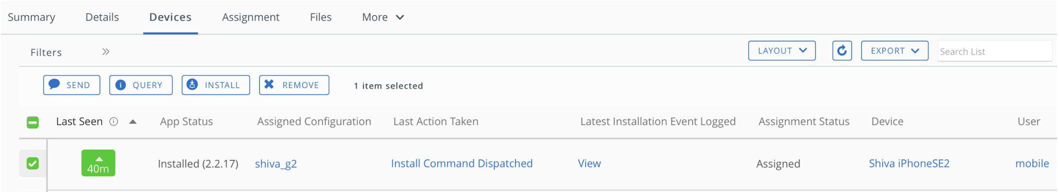
Protection thresholds have been configured to avoid undesired removal of applications from a large number of devices. These thresholds can be managed in All Settings > Apps > Workspace ONE > App Removal Protection.
App removals will be held for administrator approval in the App Removal Log when the number of devices receiving the app removal triggers reaches the configured threshold. Your team will be notified via email when this occurs.

Assignment Status All

Assignment Status	Friendly Name	User	Platform	Organization Group
Unchanged	Shiva iPhoneSE2	mobile	Apple	Infoblox Dev
Unchanged	Manas iPad iOS 14.7.0 JF8J	mobile	Apple	Infoblox Dev
Unchanged	Pradeep iPhone SE2	mobile	Apple	Infoblox Dev
Unchanged	Manas iPhone XR	mobile	Apple	Infoblox Dev
Unchanged	Raghav iPhone	mobile	Apple	Infoblox Dev
Unchanged	Naveen iPhone XR	mobile	Apple	Infoblox Dev

Page Size 20 Items 1 – 6 of 6

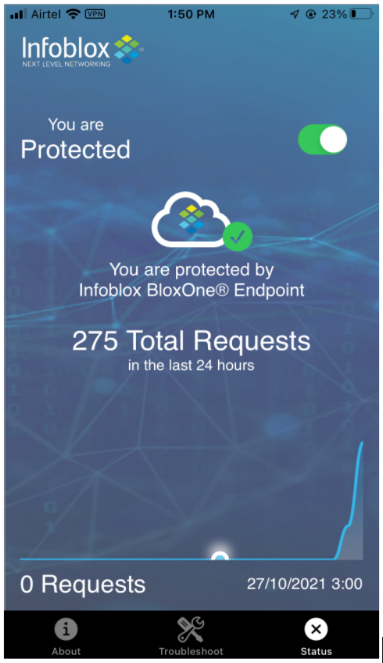
15. The newly created and published assignment will be pushed to the device. If it is not pushed from this page, then it can also be published by navigating to **“Devices”** → **“select the device”** → **“click Install”.**



1 item selected

	Last Seen	App Status	Assigned Configuration	Last Action Taken	Latest Installation Event Logged	Assignment Status	Device	User
☑	40m	Installed (2.2.17)	shiva_g2	Install Command Dispatched	View	Assigned	Shiva iPhoneSE2	mobile

16. Endpoint is automatically installed on the client devices. It might take a few minutes for the installation to complete.
17. Open the BloxOne EP on your iOS device and accept the VPN acknowledgement. After a few seconds the app will be in a protected state.



You are
Protected

You are protected by
Infoblox BloxOne® Endpoint

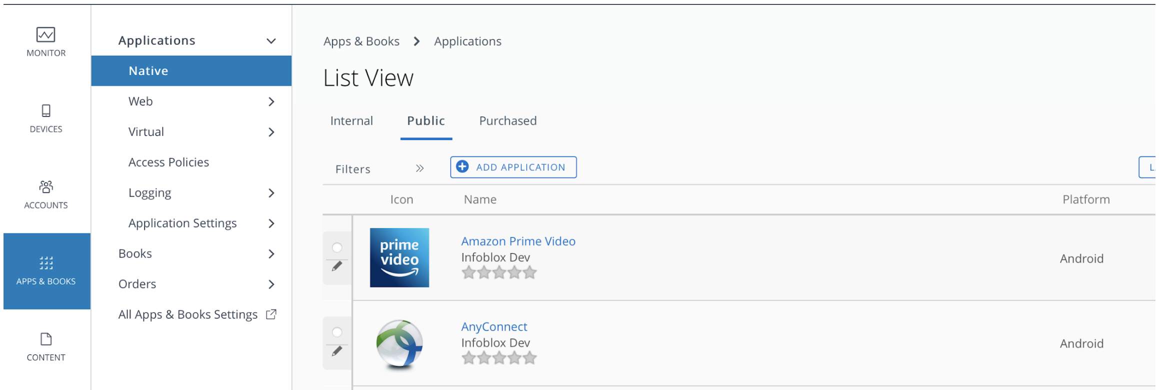
275 Total Requests
in the last 24 hours

0 Requests 27/10/2021 3:00

Installing the BloxOne App in Workspace One Server on an Apple iOS Device

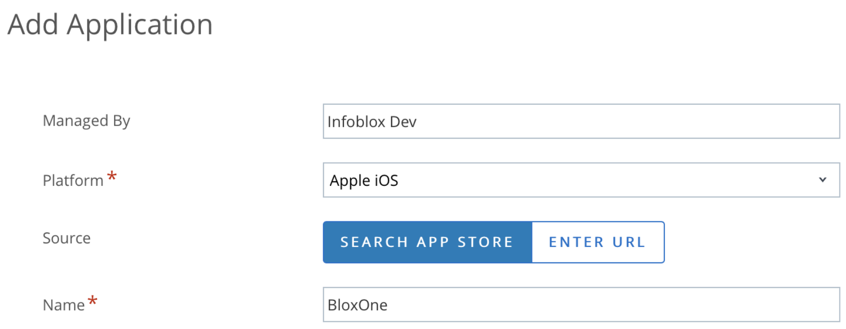
To install on an iOS device, complete the following steps:

1. Login to the Workspace One UEM console.
2. Navigate to **“Apps & Books”** → **“Applications”** → **“Native”** → **“Public”.**
3. Click **“+ Add Application”**.



Icon	Name	Platform
	Amazon Prime Video Infoblox Dev	Android
	AnyConnect Infoblox Dev	Android

4. Select platform as iOS Search for **“BloxOne EP”** and click on **“Next”.**



Add Application

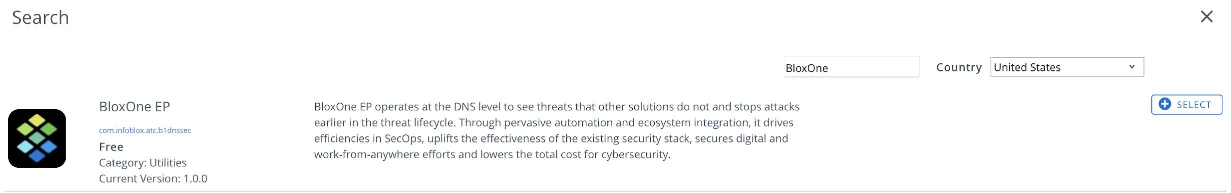
Managed By: Infoblox Dev

Platform*: Apple iOS

Source: SEARCH APP STORE | ENTER URL

Name*: BloxOne

4. Once the application is listed, click **"Select".**



Search

BloxOne | Country: United States

BloxOne EP

com.infoblox.atc.b1dnssec

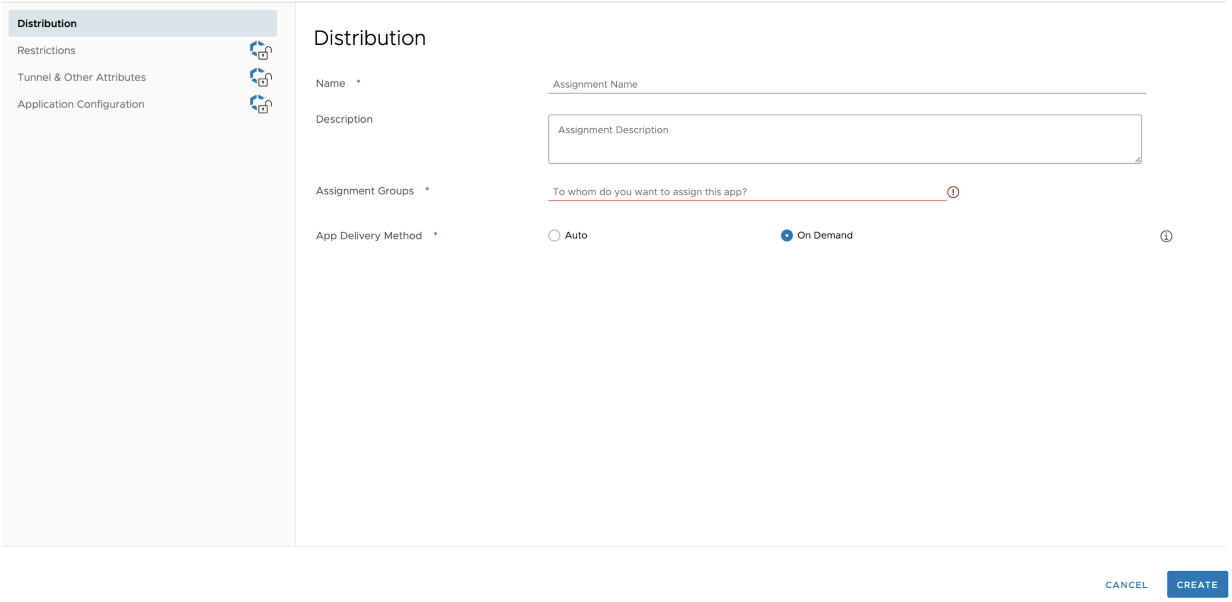
Free

Category: Utilities

Current Version: 1.0.0

BloxOne EP operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integration, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts and lowers the total cost for cybersecurity.

5. Click **"Save and Assign"**. The app assignment distribution window will open.
6. In the Distribution window, provide information for the following fields: **Name**, **Description, Assignment Groups,** and **App Delivery** method. For App Delivery method, select **"On Demand"**.
7. Click **"Create"**.



Distribution

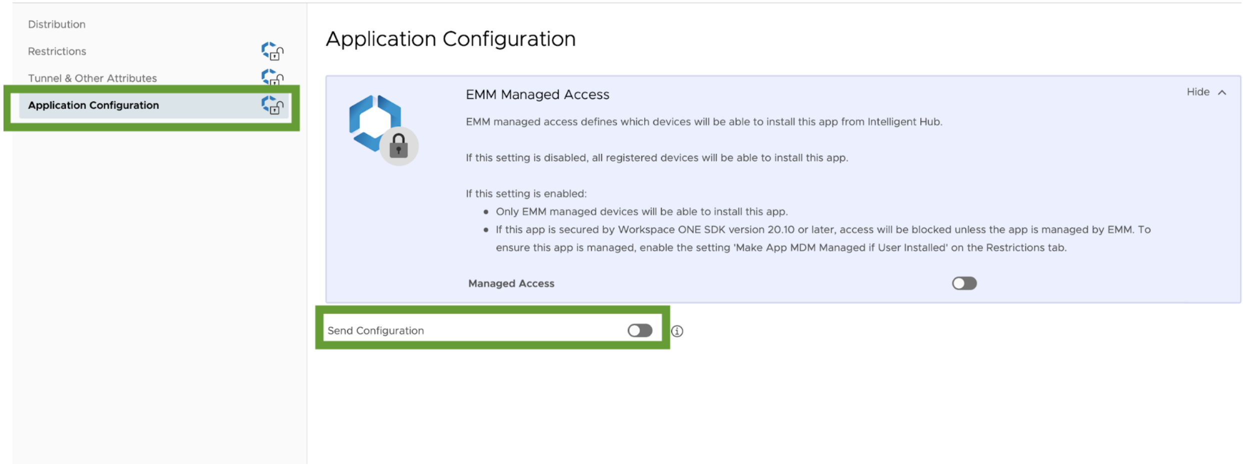
Name *: Assignment Name

Description: Assignment Description

Assignment Groups *: To whom do you want to assign this app?

App Delivery Method *: ○ Auto ● On Demand

8. Navigate to the Application Configuration page and toggle the **"Send Configuration"** button to the ON position.



Distribution
Restrictions
Tunnel & Other Attributes
Application Configuration

Application Configuration

EMM Managed Access

Hide

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

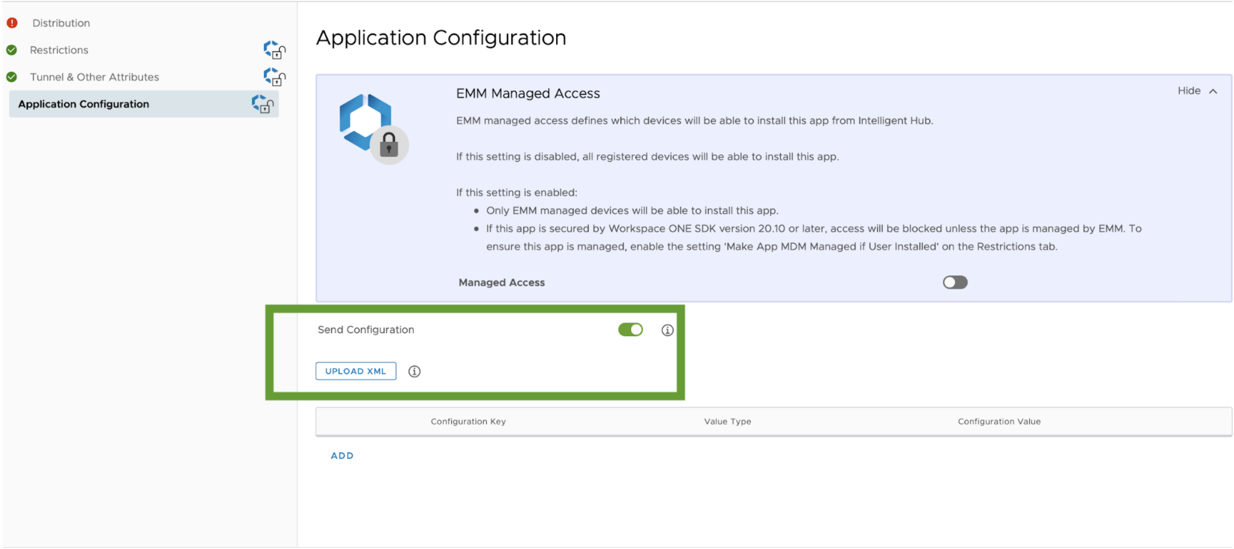
If this setting is enabled:

- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access

Send Configuration

9. Upload the configuration file previously downloaded from the Cloud Services Portal.
10. Click **"UPLOAD XML"** and select the file to be uploaded.



Distribution
Restrictions
Tunnel & Other Attributes
Application Configuration

Application Configuration

EMM Managed Access

Hide

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled:

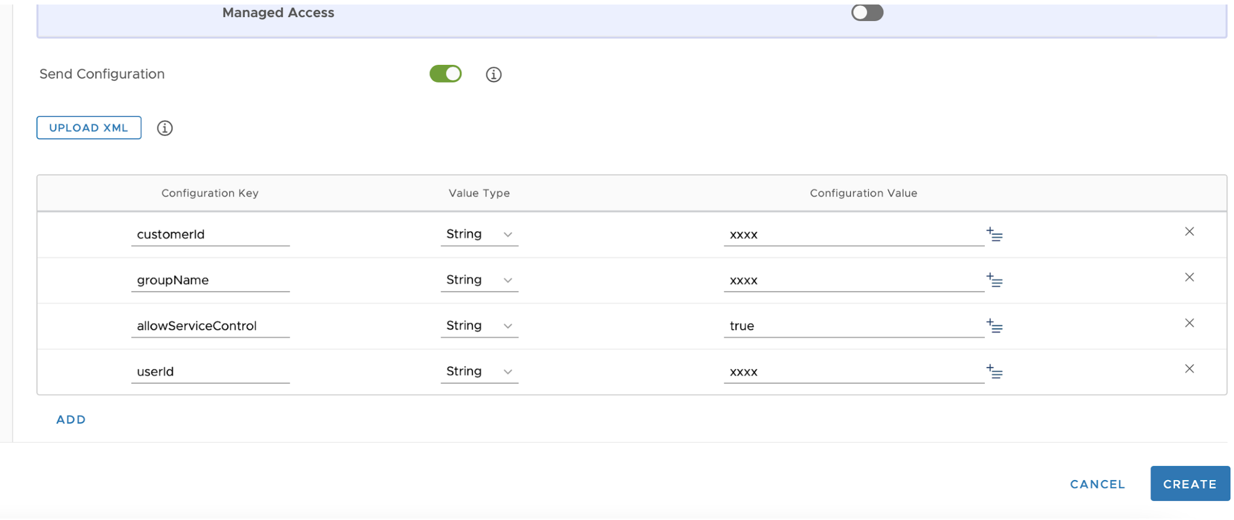
- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access

Send Configuration

Configuration Key	Value Type	Configuration Value

11. Click **"CREATE"** to create the configuration.

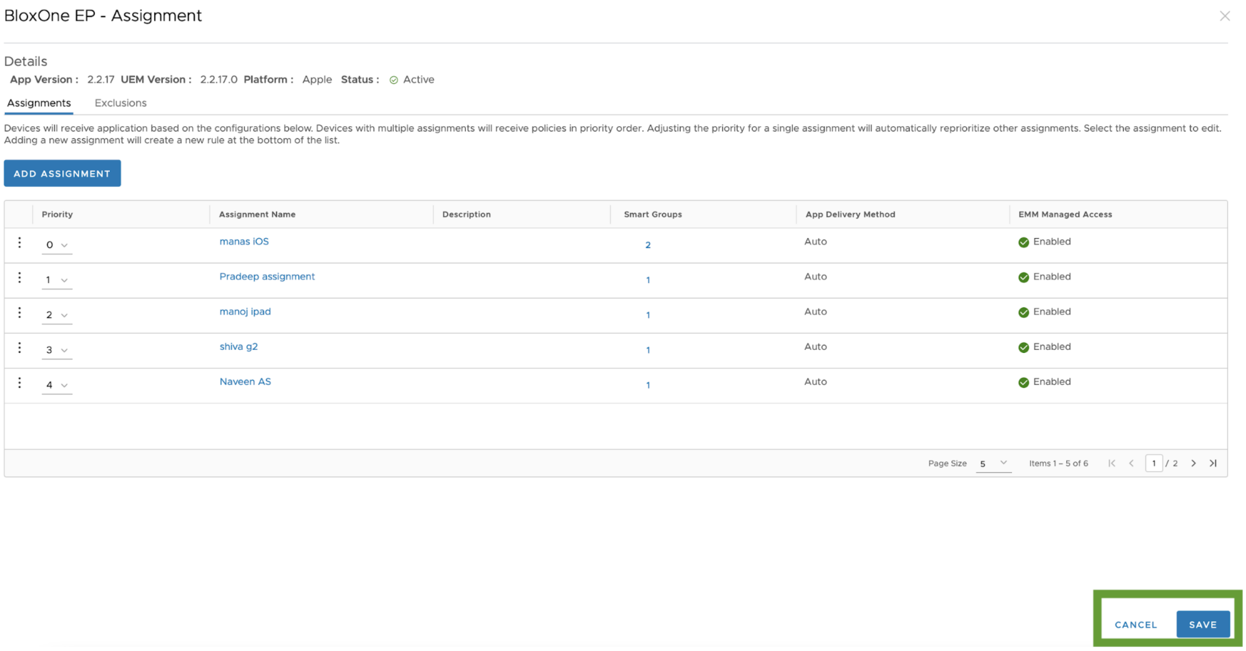


Managed Access

Send Configuration

Configuration Key	Value Type	Configuration Value
customerId	String	xxxx
groupName	String	xxxx
allowServiceControl	String	true
userId	String	xxxx

12. Click **"SAVE"** to save the created configuration.



BloxOne EP - Assignment

Details

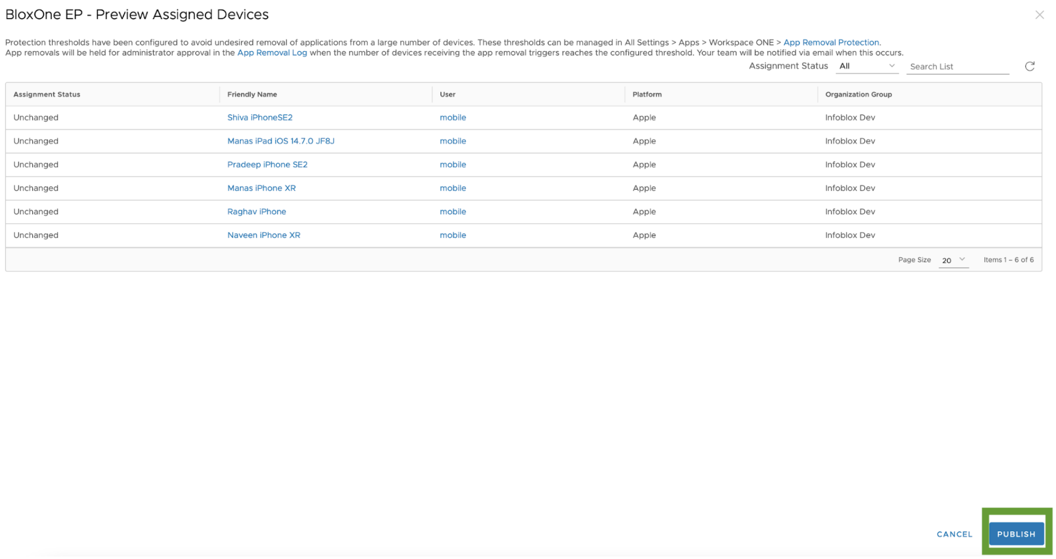
App Version : 2.2.17 **UEM Version :** 2.2.17.0 **Platform :** Apple **Status :** Active

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically reprioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

Priority	Assignment Name	Description	Smart Groups	App Delivery Method	EMM Managed Access
0	manas iOS		2	Auto	Enabled
1	Pradeep assignment		1	Auto	Enabled
2	manoj ipad		1	Auto	Enabled
3	shiva g2		1	Auto	Enabled
4	Naveen AS		1	Auto	Enabled

Page Size 5 Items 1 – 5 of 6 1 / 2

13. Click **"PUBLISH"** to finalize the configuration creation process.



BloxOne EP - Preview Assigned Devices

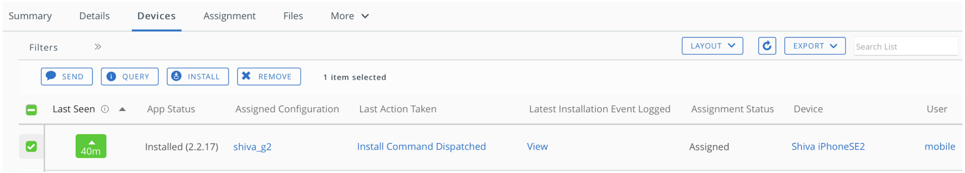
Protection thresholds have been configured to avoid undesired removal of applications from a large number of devices. These thresholds can be managed in All Settings > Apps > Workspace ONE > App Removal Protection.
App removals will be held for administrator approval in the App Removal Log when the number of devices receiving the app removal triggers reaches the configured threshold. Your team will be notified via email when this occurs.

Assignment Status: All

Assignment Status	Friendly Name	User	Platform	Organization Group
Unchanged	Shiva iPhoneSE2	mobile	Apple	Infoblox Dev
Unchanged	Manas iPad iOS 14.7.0 JF8J	mobile	Apple	Infoblox Dev
Unchanged	Pradeep iPhone SE2	mobile	Apple	Infoblox Dev
Unchanged	Manas iPhone XR	mobile	Apple	Infoblox Dev
Unchanged	Raghav iPhone	mobile	Apple	Infoblox Dev
Unchanged	Naveen iPhone XR	mobile	Apple	Infoblox Dev

Page Size 20 Items 1 – 6 of 6

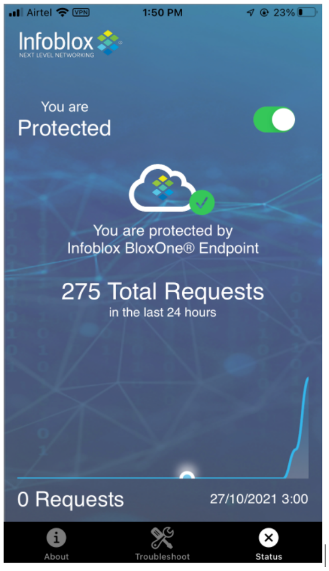
14. The newly created and published assignment will be pushed to the device. If it is not pushed from this page, then it can also be published by navigating to **“Devices”** → **“select the device”** → **“click Install”.**



1 item selected

Last Seen	App Status	Assigned Configuration	Last Action Taken	Latest Installation Event Logged	Assignment Status	Device	User
40m	Installed (2.2.17)	shiva_g2	Install Command Dispatched	View	Assigned	Shiva iPhoneSE2	mobile

15. Endpoint is automatically installed on the client devices. It might take a few minutes for the installation to complete.
16. Open the BloxOne EP on your iOS device and accept the VPN acknowledgement. After a few seconds the app will be in a protected state.



You are
Protected

You are protected by
Infoblox BloxOne® Endpoint

275 Total Requests
in the last 24 hours

0 Requests 27/10/2021 3:00

References

BloxOne Admin Guide:

https://docs.infoblox.com/

BloxOne Threat Defense Endpoint User Guide:

https://www.infoblox.com/wp-content/uploads/infoblox-deployment-guide-accessing-bloxone-threat-defense-using-bloxone-endpoint.pdf

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).