



FAMOC & Cisco Umbrella integration guide



www.famoc.com

PUBLISHED BY

Famoc Software Limited
Atrium Business Centre
The Atrium, Blackpool Park
Cork, Ireland

Copyright© 2008-2021 by Famoc Software Limited

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of the publisher. Famoc™ and FAMOC™ are either registered trademarks or trademarks of Famoc Software Limited. This publication may contain the trademarks and service marks of third parties and such trademarks and service marks are the property of their respective owners.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS AND SERVICES IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS AND SERVICES. THE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT AND SERVICES ARE SET FORTH IN THE Famoc TERMS AND CONDITIONS AND ARE INCORPORATED HEREIN BY THIS REFERENCE.



Table of Contents

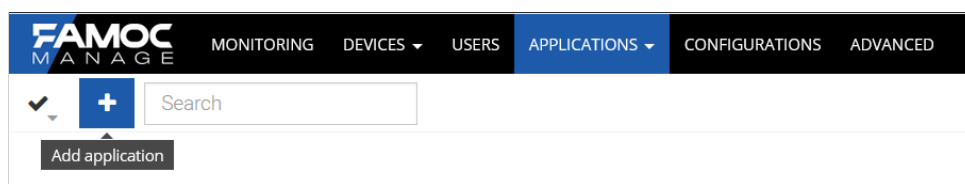
What is Cisco Umbrella	4
Adding Cisco AnyConnect to FAMOC	4
AnyConnect configuration in FAMOC manage	5
Device operations	7
Additional possibilities	7

1 What is Cisco Umbrella

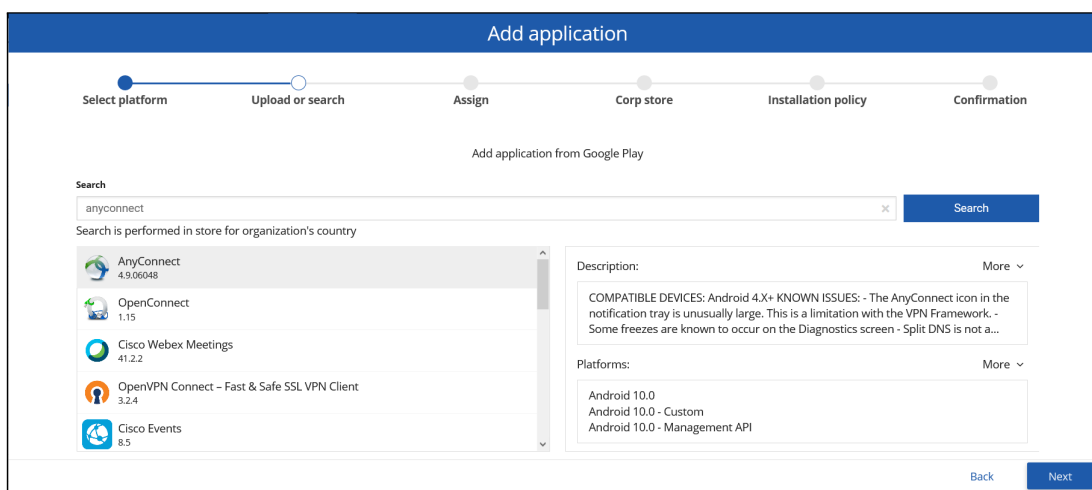
Cisco Umbrella is a network solution that monitors network traffic at the DNS level. All network traffic from a managed device can pass through the Umbrella engines and there it is analyzed whether it is free for malware, phishing etc. Cisco Umbrella uses the Internet infrastructure to block access to dangerous places on the network and prevents connection being established, ensuring security regardless of the customer's location. Umbrella redirects DNS queries from our devices to a secure DNS service that updates the knowledge about the network state in real time.

2 Adding Cisco AnyConnect to FAMOC

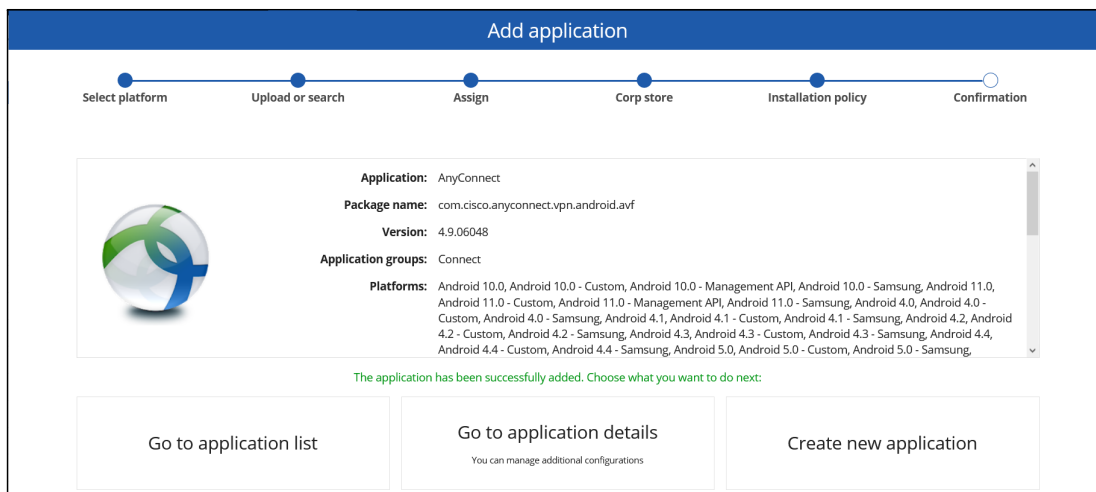
AnyConnect can be added to FAMOC just like any other application. Simply go to the APPLICATIONS tab and click + button to add a new app.



Then select the platform - Android. Select the option to add an application from the Google Play Store. Enter AnyConnect in the search field, select the appropriate application from the list, and click Next.



Then continue with the steps up to the confirmation screen.



2.1 AnyConnect configuration in FAMOC manage

To properly configure the Umbrella service in FAMOC manage, you will need values such as Organization ID and Umbrella Registration Token.

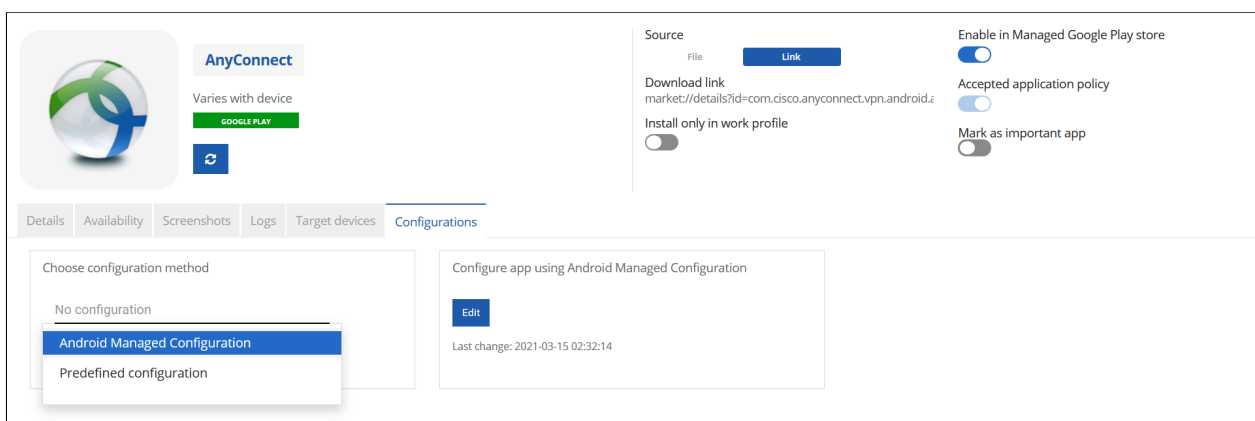
To get them, log in to the Umbrella portal, then in the Deployments> Core Identities> Mobile Devices tab, click Manage MDMS and download the Android config file.

The process is described in detail at the link below.

<https://docs.umbrella.com/deployment-umbrella/docs/android-configuration-download>

Once we have added the AnyConnect application to FAMOC manage and we know the Organization ID and Umbrella Registration Token, we can proceed to configuration.

In the APPLICATIONS tab, search for AnyConnect and go to the application details. Then open the Configurations tab. We choose the Android Managed Configurations method.



Click Edit. The fields of interest are Umbrella Organization Id and Umbrella Registration Token. Open the Android configuration file downloaded from the Umbrella portal and copy the

appropriate values from the file to the managed configuration.

organizationID - Umbrella Organization Id

regToken - Umbrella Registration Token

The above values should be written in the following format:

```
{"organizationInfo": {"Value": {"organizationID": "<orgid>", "regToken": "<reg token>"}}}
```

The screenshot shows the 'Android Managed Configuration' page. On the left, there is a sidebar with 'All parameters', 'Main parameters', and 'VPN Connection List'. The main area has a search bar and a list of parameters. The parameters are as follows:

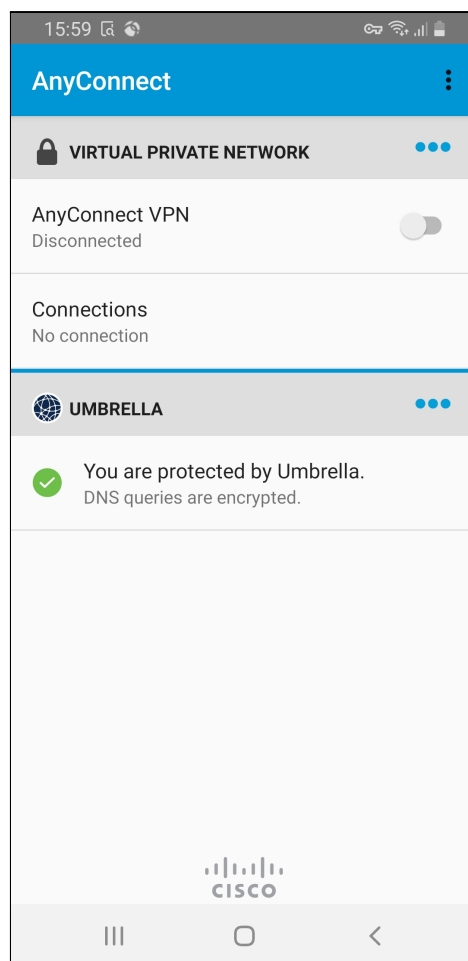
Parameter	Data source	Value
Device Identifier ⓘ	Fill manually	
Report Hardware Identifiers (MAC address and IM... ⓘ)	On	
Allow users to save credentials ⓘ	Off	
Accept SEULA for Users ⓘ	Off	
VPN Connection List ⓘ		
Umbrella Organization Id ⓘ	Fill manually	
Umbrella Registration Token ⓘ	Fill manually	
Umbrella VA FQDNs list ⓘ	Fill manually	
Umbrella Domain list ⓘ	Fill manually	
Administrator Email Address ⓘ	Fill manually	

Then we save the configuration. From now on, the AnyConnect application will install on devices with the parameters set by us.

3 Device operations

After installing the AnyConnect app on your device, launch it. We will receive a notification about the connection request, confirm our consent by clicking OK.

If the process was successful, the application will display the following message about active Umbrella protection:



4 Additional possibilities

Since the AnyConnect app is essentially a VPN client, we can force it to run continuously on the device with the Always on VPN configuration.

In the CONFIGURATIONS tab, we add a new configuration. I choose the Android platform and then the VPN configuration type.

New configuration

Platform Configuration type Basic data Corp store Installation policy Configuration parameters Summary

Select the type of the configuration you want to add.

Configuration types from category: **VPN**

- ☒ Always on VPN settings Android 11.0, Android 11.0 - Samsung, Android 10.0...
- ☐ Generic VPN configuration for Samsung devices Android 11.0 - Samsung, Android 10.0 - Samsung, Android 9.0 - Samsung...
- ☐ Strongswan VPN Android 11.0, Android 11.0 - Samsung, Android 11.0 - Custom...
- ☐ VPN Cisco AnyConnect configuration Android 11.0, Android 11.0 - Samsung, Android 11.0 - Custom...
- ☐ VPN configuration (available for Samsung Devices) Android 11.0 - Samsung, Android 10.0 - Samsung, Android 9.0 - Samsung...

Back Next

We go through the steps of creating a configuration. The name of the package to be entered is: **com.cisco.anyconnect.vpn.android.avf** (be careful not to close the device's connection with the FAMOC manage server in this way).

Then we can decide to disallow the connection to the network without an active VPN connection.

New configuration

Platform Configuration type Basic data Corp store Installation policy Configuration parameters Summary

Set the desired parameters for the configuration.

Configuration type: Always on VPN settings Configuration name: Umbrella Always On

Search

All parameters

Main parameters

VPN package name Value com.cisco.anyconnect.vpn.android.avf

Internet connection when VPN is not connected Allow Disallow

We confirm our choice and finish creating the configuration. We can now apply it to the device manually or add it as part of the policy.

When applied to the device, the connection to the Cisco Umbrella will be permanent, you do not need to manually call it, and the user will not turn it off by accident.