

GlobalSign Integration Guide

GlobalSign Enterprise PKI (EPKI) and
AirWatch Enterprise MDM



Table of Contents

Table of Contents	2
Introduction	3
GlobalSign Enterprise PKI (EPKI)	3
Partner Product Information	3
Managed PKI Architecture	3
Setup Overview	4
GlobalSign EPKI Account Setup	4
Adding GlobalSign as a Certificate Authority (CA)	7
Assigning a Certificate Template	8
Creating an Operating System (OS) Profile	9
Distributing Profiles to a Device(s)	11
Certificate Revocation	12
EPKI License Expiration	13
About GlobalSign	13
GlobalSign Contact Information	13

Introduction

This technical integration guide describes how to integrate the AirWatch Enterprise MDM platform with GlobalSign's managed Enterprise PKI (EPKI) service to automatically provision digital certificates for mobile devices from the GlobalSign SaaS CA. Digital certificates provide a secure and cost effective method to authenticate corporate and Bring Your Own Device (BYOD) devices accessing enterprise resources. Before being able to issue certificates from your GlobalSign EPKI Account, there are setup steps involving both the AirWatch MDM and GlobalSign's EPKI consoles that need to be completed. The following guide will walk you through these steps.

GlobalSign Enterprise PKI (EPKI)

The GlobalSign managed Enterprise PKI (EPKI) is a cloud-based PKI service allowing organizations an easy method to issue and manage digital certificates to corporate users. The EPKI web portal and associated API, provide administrators an easy-to-use solution to simplify PKI deployments and eliminate the need to host their own Certificate Authority. EPKI provides enterprises the necessary tools to maintain full control of their PKI requirements without the complexities and overhead cost of running an in-house CA. Further, with integration into AirWatch MDM version 8.0+, organizations can automatically provision digital certificates directly from the AirWatch MDM console.

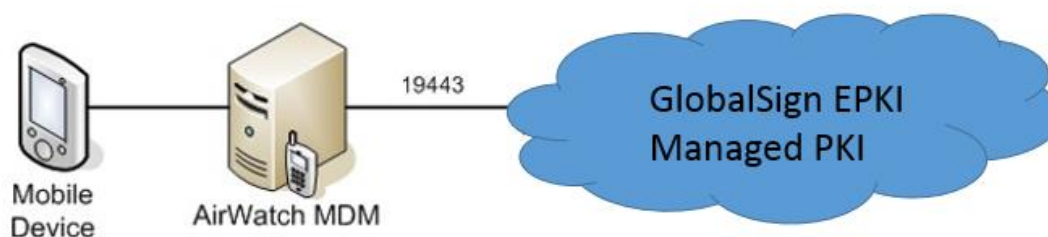
For more information about EPKI, see <https://www.globalsign.com/en/enterprise-pki/>

Partner Product Information

Partner Name	AirWatch
Website	www.airwatch.com
Product Name	AirWatch Enterprise MDM v.8.0
Product Description	<p>AirWatch® Mobile Device Management enables businesses to address challenges associated with mobility by providing a simplified, efficient way to view and manage all devices from the central admin console. Our solution enables you to enroll devices in your enterprise environment quickly, configure and update device settings over-the-air, and secure mobile devices. With AirWatch, you can manage a diverse fleet of Android, Apple iOS, BlackBerry, Mac OS, Symbian, Windows Mobile, Windows PC/RT and Windows Phone devices from a single management console.</p> <p>Read more at: http://www.air-watch.com/solutions/mobile-device-managment/</p>

Managed PKI Architecture

The following diagram shows a simple architecture, illustrating an integration with AirWatch MDM and the GlobalSign EPKI and Managed Services PKI. *Note, all ports shown are the default ports.*



Setup Overview

In order to establish the connection between AirWatch MDM and your GlobalSign EPKI account you will need to complete the following steps, outlined in this guide:

- [Setup a GlobalSign EPKI Account](#)
- In the AirWatch MDM Platform:
 - [Select GlobalSign as a Certificate Authority](#)
 - [Assign GlobalSign to a Certificate Template](#)
 - [Create an operating system \(OS\) profile](#)
 - [Distribute the profile to a device](#)

To start the setup process please proceed to the first step: [GlobalSign EPKI Account Setup](#).

GlobalSign EPKI Account Setup

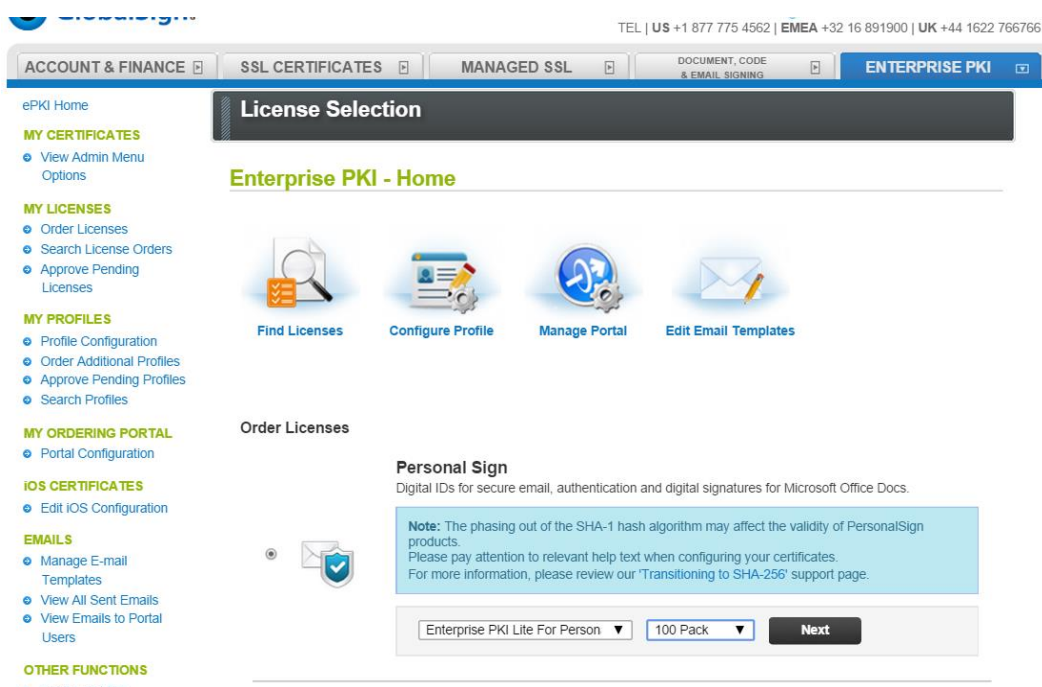
The following steps will walk you through obtaining the information from your GlobalSign Enterprise PKI (EPKI) account, establishing a pre-vetted organization profile, and ordering a certificate license pack, which you will need to integrate with your AirWatch MDM. If you do not already have an EPKI account please visit the following page to request a quote: <https://www.globalsign.com/en/enterprise-pki/>.

You will need the following information from your GlobalSign EPKI Account:

- **Login Credentials:** Your GlobalSign account number, in the following format “**PARXXXXXX_user name**”. You will need to remember both your EPKI account number and password when configuring your AirWatch MDM.

Next, complete the following steps to order your **EPKI Certificate License Pack**:

1. **Login** to your EPKI Account.
2. Click the **ENTERPRISE PKI** tab.
3. Click **Order Licenses** on the left-hand menu.
4. Select the **Enterprise PKI Lite for Personal Digital ID** license pack appropriate for the number of users /devices you are planning to manage with your AirWatch MDM.



Next, complete the steps in the EPKI Administrator guide to register for a **pre-vetted organization profile**:

<https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>

Note: the default EPKI service utilizes a shared issuing CA, issued from a GlobalSign publically trusted root. Therefore GlobalSign recommends utilizing the “lock base DN” feature in order to reserve an Organization and OU combination that will be restricted to the account. Dedicated private issuing CAs, either self-signed or issued from a GlobalSign trusted root, are available. Please contact your GlobalSign EPKI product specialist for details.

At the completion of the Organization Profile registration, a GlobalSign vetting agent will begin the identity verification process of your organization. **This may take up to three (3) business days.** After the Profile has been approved, a Profile number with the following format type will be available to use. Here’s an example:

Certificate Profile Details >> Confirm Details

Certificate Profile Details

These details will be vetted and included as the certified identity within your issued Certificate. Make sure the details entered are correct - we will vet the details you include. To assist you, some details will be pre-populated from previous pages or from your GCC account details, you may overwrite these if needed.

Note. Within the form below you have the ability to define the certificates DistinguishedName (DN). One optional element is a freeform Organizational Unit (OU) description. The OU field allows you to enter a value that suits your business needs with a description such as “Marketing Team Building 5” for example. It is not mandatory to enter this but please note that if you choose to ‘Lock a unique OU’ then this means that the description you have chosen cannot be used again and is unique to this profile. An example of where you might choose to do this is for client authentication situations where each certificate needs one or two fixed unique strings to allow access such as ‘O’ and ‘OU’.

Organization <small>Required</small>	ABC Inc.
Organizational Unit <small>Optional unless locked as unique</small>	Mobile users
	<input checked="" type="checkbox"/> Lock a unique OU
Locality <small>Optional</small>	Portsmouth
State or Province <small>Optional</small>	NH
Country <small>Required</small>	United States - US
Hash Algorithm	<div><input checked="" type="radio"/> SHA-256 (Recommended) SHA-256 certificates provide the highest level of security, but may not be compatible with older environments e.g. WinXP SP2. To ensure application compatibility, we strongly encourage testing PKI-dependent components before using SHA-256 certificates.</div> <div><input type="radio"/> SHA-1</div>

Next

After your pre-vetted profile has been established, you will need to complete the following steps to make sure your EPKI Account is ready to be integrated with your AirWatch MDM:

1. In your EPKI account, click **Profile Configuration** on the left-hand menu.
2. In the **API IP Address Range** field, enter the IP address (range) of the server hosting your AirWatch MDM.

MY CERTIFICATES

- Order Certificates
- Order Certificate BULK
- Search Certificates
- PKCS#12 Bulk Registration and Pickup
- Search PKCS#12 Bulk Order History
- Approve Pending Certificates

MY LICENSES

- Order Licenses
- Search License Orders
- Approve Pending Licenses

MY PROFILES

- Profile Configuration
- Order Additional Profiles
- Approve Pending Profiles
- Search Profiles

MY ORDERING PORTAL

- Portal Configuration

IOS CERTIFICATES

- Edit IOS Configuration

EMAILS

- Manage E-mail Templates
- View All Sent Emails
- View Emails to Portal Users

OTHER FUNCTIONS

- Configure LDIF

RESOURCES

- ePKI Admin Auth Guide
- ePKI Administrator Guide

Profile Configuration

Profile ID	MP201211011148
Organization	GMO GlobalSign Inc.
Organization Unit	
URL	https://system.globalsign.com/cr/public/certificate/order.do?p=141c441dbf39bade5fe7546066c40687227c9ace
URL(PKCS12 Option)	https://system.globalsign.com/cr/public/certificate/order.do?p=816247bb98ed6dade2bd16901ff1ca6537cd0b84
User Permission	Configure

Hash Algorithm	<input checked="" type="radio"/> SHA-256 (Recommended) SHA-256 certificates provide the highest level of security, but may not be compatible with older environments e.g. WinXP SP2. To ensure application compatibility, we strongly encourage testing PKI-dependent components before using SHA-256 certificates.
	<input type="radio"/> SHA-1
Encrypting File System	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
MS SmartCard Logon	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Renewal Type	<input checked="" type="radio"/> Manual <input type="radio"/> Auto <input type="radio"/> Quick
Non Exportable Option <small>Limited to only Internet Explorer.</small>	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
OCSP Option	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
API IP Address range <small>IP Address is limited to only at the time of API e.g) *.*.*.* e.g) 211.11.149.249,211.11.149.250</small>	<input type="text" value="<ENTER IP ADDRESS HERE>"/>

Back

Next

Next you will need to **disable** the EPKI system generated emails because the AirWatch MDM service will automatically provision certificates from EPKI, so the emails are not needed:

3. Click **Manage Email Templates**.

The following steps should be completed for the following email types:

- Enrollment (invite)
- Renewal reminders (all)

4. Click **Disable**.

5. Click **Next**

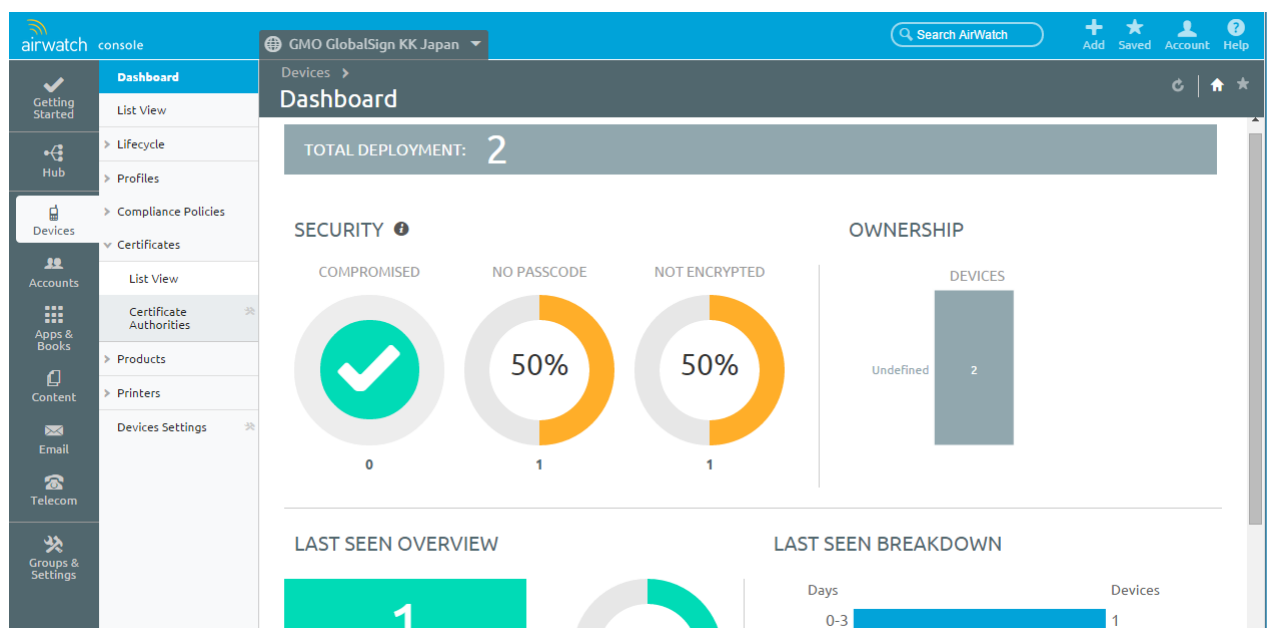
6. Click **Complete**.

Your EPKI Account is now prepared for the integration with your AirWatch MDM. Please continue to step two: [Adding GlobalSign as a Certificate Authority \(CA\)](#).

Adding GlobalSign as a Certificate Authority (CA)

With your EPKI Account activated, you can now configure AirWatch to associate certificate provisioning to mobile devices with the GlobalSign CA.

1. **Log in to the AirWatch Service** using your AirWatch administrator account.
2. Select **Devices > Certificates > Certificate Authorities**.



3. Click the **+Add** button.
4. Select GlobalSign as the **Authority Type** from the dropdown menu.

5. Add **https://system.globalsign.com/cr/ws/GasOrderService** as the server URL.
6. Enter your GlobalSign EPKI account username (PARxxxxx.username) and Password.
7. Click **Save**.

Certificate Authority - Add / Edit ✕

Name*

Description

Authority Type*

GlobalSign ▼

Server URL*

Username*

Password*

☐ Show Characters

Save

Save and Add Another Template

Test Connection

Cancel

You have now successfully associated your GlobalSign EPKI Account with your AirWatch MDM. Please continue to step three: [Assigning a Certificate Template](#).

Assigning a Certificate Template

The certificate template will now establish a connection between your AirWatch MDM and the certificate profile ID and product code that you established in your EPKI Account. If you have not ordered a certificate license pack or are not sure of your EPKI profile ID, required for the following steps, please view the [GlobalSign EPKI Account Setup](#) section of this guide.

1. Select **Devices > Certificates > Certificate Authorities > Request Templates**
2. Click **+Add**.
3. Enter a name and description for the user.
4. Select the GlobalSign Certificate Authority previously established.
5. Enter your **EPKI Profile ID** from your EPKI Account profile.
Note, the Profile ID will follow this format: MP2015XXXXXXXX.
6. Enter the product code **EPKIPSPersonal**.
7. Enter the **validity period** associated with the EPKI license pack you purchased.
8. Enter the **Common Name** (e.g. First and Last name of the user) in the Subject Name field.
Note, as you are the Local Registration Authority for your pre-vetted organization, you are obligated to verify the identity of the user you are registering using the terms found in the EPKI Service Agreement accepted at service sign up.
<https://www.globalsign.com/en/repository/globalsign-epki-service-agreement.pdf>
9. Click **Save**.

Certificate Template - Add / Edit ✕

Name*

Description

Certificate Authority* GlobalSign Test CA ▼

Profile ID*

Product Code*

Validity Period (in years)* 1 ▼

Subject Name* CN=

Automatic Certificate Renewal ☐ ⓘ

Enable Certificate Revocation ☐ ⓘ

Save
Save and Add Another Template
Cancel

Insert Lookup

This Field Supports Lookup Values

Name	Description
{EmailDomain}	User Email Domain
{EmailUserName}	User Email Username
{EmailAddress}	User Email Address
{EnrollmentUser}	Username
{EnrollmentUserId}	User ID

Now that you have successfully created a Certificate Authority and Certificate Template you will need to create an operating system profile. Please proceed to step four [Creating an Operating System \(OS\) Profile](#).

Creating an Operating System (OS) Profile


The final step is creating a profile based on the OS of the devices you are looking to manage. The profile will assign the CA to the device(s).

1. Click **Devices > Profiles > List View**
2. Click **+Add**


3. Click on **the icon of the device OS** you would like to manage.

Add Profile


Select a platform to start:




Android




Apple iOS




Apple Mac OS X




Apple TV




BlackBerry




BlackBerry 10




Symbian




Windows Mobile




Windows Phone




Windows Phone 8



Windows 8 / RT



Windows PC



Chromebook

Cancel

- Complete the **General form information**. Note, the only required field is the Name of the profile.

Add a New Apple iOS Profile

General

Passcode
Restrictions
Wi-Fi
VPN
Email
Exchange ActiveSync
LDAP
CalDAV
Subscribed Calendars
CardDAV
Web Clips
Credentials
SCEP
Global HTTP Proxy
Single App Mode
Content Filter
Managed Domains

General

Name*
Required Field

Version

Description
Description

Deployment

Assignment Type

Allow Removal

Managed By

Assigned Smart Groups

Exclusions

Additional Assignment Criteria

☐ Enable Geofencing and install only on devices inside selected areas
☐ Enable Scheduling and install only during selected time periods

Removal Date

Agent Required

- In the left-hand menu, click **Credentials**.
- Click **Configure**.
- From the Credential Source dropdown select **Defined Certificate Authority**.

8. Select the GlobalSign CA from the Certificate Authority Drop=down menu.

iOS Add a New Apple iOS Profile

General

Passcode

Restrictions

Wi-Fi

VPN

Email

Exchange ActiveSync

LDAP

CalDAV

Subscribed Calendars

CardDAV

Web Clips

Credentials 1

SCEP

Global HTTP Proxy

Credentials

Credential Source: Defined Certificate Authority

Certificate Authority: Select Certificate Authority

Certificate Template: Select Certificate Authority

Save & Publish Cancel

9. Click **Save & Publish**.

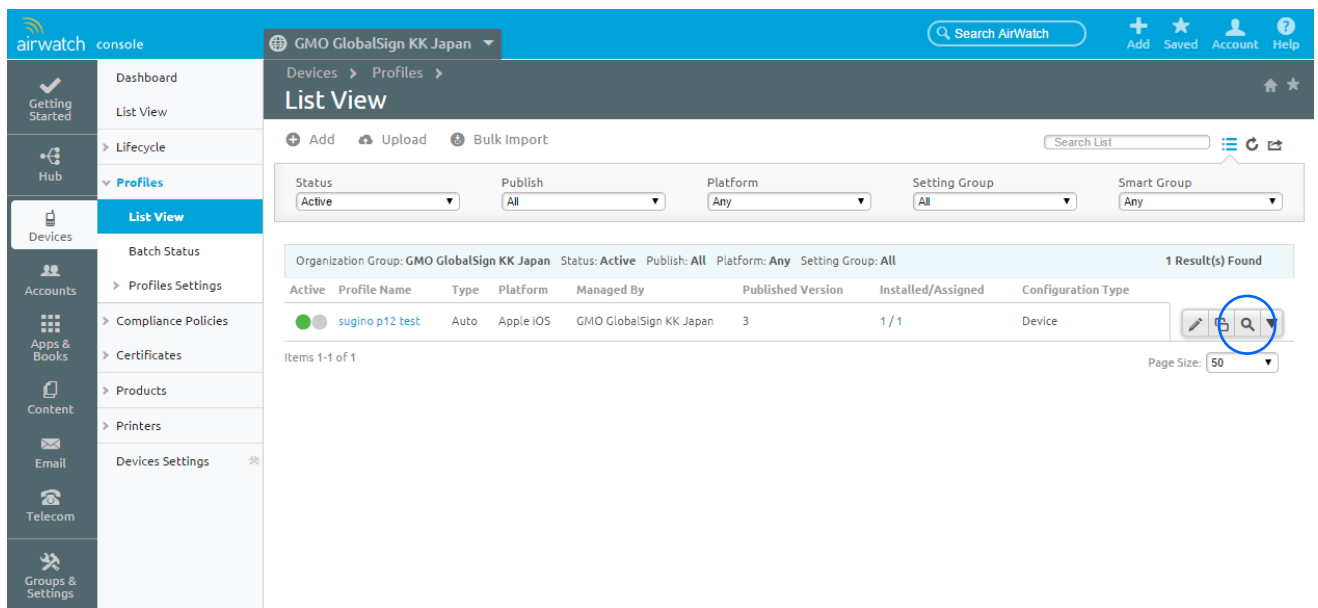
The integration between your AirWatch MDM and GlobalSign EPKI account is now complete. To understand how the AirWatch device profiles are distributed to devices please proceed to the next section, [Distributing Profiles to a Device\(s\)](#).

Distributing Profiles to a Device(s)

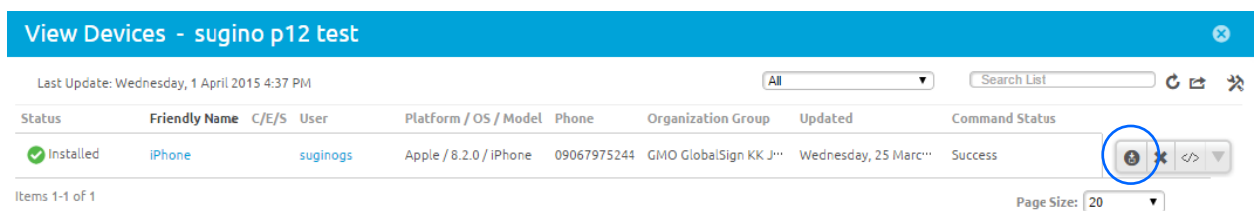
The integration is now complete and you have created certificate templates as well as profiles for the specific OS of the devices you are managing using your AirWatch MDM. The following steps explain how you can now assign profiles to those devices:

1. Click **Devices > Profiles > List View**

- Click the **Search icon** (circled in blue) to the right of the profile you are looking to distribute.



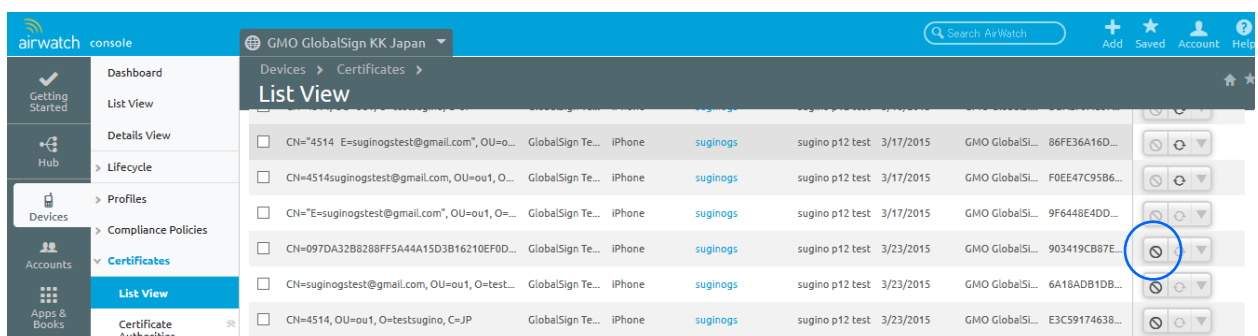
- The devices included in the group will be listed.
- Click the **Install Profile icon** (circled in blue) to the right of the device you would like to apply the profile to.



The certificate and profile are distributed to the device at the same time. Please continue to review the remaining sections of this guide to understand how you can also [revoke certificates](#) through the AirWatch MDM interface and how to handle [certificate license expirations](#).

Certificate Revocation

You will be able to revoke certificates by viewing the certificate list from **Devices > Certificates > View list**. Simply click the **Cancel icon** (circled in blue) to revoke the certificate.



EPKI License Expiration

You will see the following error, pictured below, should you attempt to provision a certificate against an expired EPKI license. To resolve the issue, login to your EPKI account, and order additional certificate licences.

Last Update: Wednesday, 18 March 2015 4:54 PM

All Search List

s	Friendly Name	C/E/S	User	Platform / OS / Model	Phone	Organization Group	Updated	Command
nstall Failed	8		ykawatsura	Apple / 8.1.2 / iPad		GMO GlobalSign KK Japan	Wednesday, 18 March 2015 3:1...	Error

Errors

Error Code	Date/Time	Description
	3/18/2015 2:16:27 AM	Server Error: Not found License

About GlobalSign

GlobalSign was one of the first Certificate Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc. group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital ID Solutions, internal PKI and Microsoft Certificate Service root signing. Our trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, and member of the Online Trust Alliance, CAB Forum and Anti-Phishing Working Group, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign Contact Information

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	GlobalSign EU Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	GlobalSign UK Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	GlobalSign DE Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	GlobalSign NL Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com