AirWatch Securing Mobile Devices with Certificates

Know who is accessing and what is being accessed on your network
## Contents

### Overview
Digital Certificates in the Enterprise

### Empowering Mobile Security with Certificates
Certificate-based Email Authentication
Certificate-based Wi-Fi Authentication
Certificate-based Virtual Private Network (VPN) Authentication
Email Encryption and Message Signing with S/MIME
In-App Encryption and Authentication

### Certificate Management with AirWatch
Supported PKI
Issuing Digital Certificates
Managing Digital Certificates
Renewing Digital Certificates
Revoking Digital Certificates
Overview

As the availability of sensitive corporate content become increasingly mobile, the possibilities of unauthorized access and other malicious threats become larger and larger.

Even if you protect your corporate email, Wi-Fi, and VPN with strong passwords, you are leaving your infrastructure vulnerable to brute force, dictionary attacks, and even employee error. If you take these threats seriously, then it’s time to consider securing your corporation with digital certificates.

Certificates offer a level of stability, security, and authentication that passwords just can’t compete with. AirWatch’s Mobile Certificate Management solves this problem by ensuring security throughout a device’s full life cycle.

Digital Certificates in the Enterprise

For enterprises, content security is top priority. Safeguarding your company’s resources online can get complicated, especially when hackers don’t sign a non-disclosure agreement.

In the mobile landscape, digital certificates do more than act as a security gate for internal content. These certificates allow complete confidence in virtual interaction and discretion by providing:

- **Cross-Platform Scalability**: Digital certificates can be leveraged to protect data across many different mobile platforms. Digital certificates can be used to securely transfer same message via either email or instant messaging. The extensibility of certificate security allows organizations to avoid implementing multiple inferior single point security solutions that ultimately leave data vulnerable as it moves from point to point.

- **Multifunctionality**: Once a user or device receives a certificate, it can be utilized across many different platforms for a variety of purposes.
  - **Encryption**: Certificates can be used to encrypt digital information regardless of the platform. For example, the S/MIME standard leverages certificates for email encryption, while the HTTPS protocol utilizes SSL to provide web page encryption.
  - **Message Signing**: Enterprises in need of digital message signatures can leverage certificates in order to prove message integrity and show that the message originates from an authenticated sender and was not altered by any malicious third party. S/MIME can also provide email message signing to ensure recipients that the sender is exactly who they say they are.
  - **Authentication**: Lastly, because digital certificates contain identifying information about both the user and the device that has been certified by a trusted source, certificates provide secure authentication into a number of systems such as email, Wi-Fi, and VPNs.

- **High Security**: Digital certificates are much more secure than traditional passwords because they are not susceptible to common password cracking methods such as brute force or dictionary attacks.
Empowering Mobile Security with Certificates

Mobile devices are becoming ubiquitous in the enterprise at a faster pace. Security conscious organizations and enterprises are increasingly looking for authentication strategies to handle how devices access their network and sensitive information, and they are commonly finding digital certificates as the answer. With AirWatch, these organizations can breeze through the technical challenges of deploying and managing certificates so that they can focus on the true matter at hand: mobile security.

Certificate-based Email Authentication

Accessing enterprise email on-the-go is key to maintaining a steady workflow, and mobile devices allow users to tap directly into corporate email servers anywhere. Users can call on everything from their complete list of contacts and calendar information without lugging a laptop or plugging directly into the company’s network. However, this ease-of-access also opens potential for exposure of sensitive material to uninvited viewers.

Corporate emails typically involve private information that isn’t intended for outside parties. Proprietary company information, confidential customer communication, and sensitive business details are all discussed on a daily basis via email. If an unwanted user cracks into a company email account, any and every message in that account is open for viewing. The intruder is now free to leak sensitive company information, whether it be your “secret formula,” future prospects, or weak points.

By implementing certificate-based email, you remove the chance for intrusion by establishing unique certificates for users and devices that render common dictionary attacks and brute force attempts useless. They also eliminate the need for users to manually enter their username and password for authentication, and they are silently updated for security purposes once a year instead of monthly. That means that IT administrators get the security that they need, and all of the end-users get the ease of access that they want.
Certificate-based Wi-Fi Authentication

Wi-Fi networks often provide a faster and more stable connection than cellular networks, but your wireless network requires just as much security as the devices accessing enterprise information. Unwanted users who access an unprotected or password-protected network can take control of the network itself and alter system settings. Those same users can then lock you out of your own network, view sensitive data, and commandeer devices on the network.

Certificates bolster secure connections between devices and Wi-Fi network by providing greater security than a simple Wi-Fi password. Not only does certificate authentication prevent common Wi-Fi cracking techniques, but it also allows each end-user to authenticate with their own unique digital certificate. This provides visibility into when and where each individual user is accessing Wi-Fi, and the ability to remove or revoke an individual user’s network access without compromising the access of others. From the end-user’s perspective this also means that they will never have to manually enter or remember a password to get connected to corporate Wi-Fi anymore. Even when certificates are updated every year or two, the transition is seamless to the end-user.

Certificate-based Virtual Private Network (VPN) Authentication

Password-protected VPN connections are just as susceptible to bypass and cracking techniques as Wi-Fi networks. Similarly, leveraging certificates for VPN offer all of the benefits that certificate-based Wi-Fi offer, plus more. By using certificates with your corporate VPN, it becomes possible to implement VPN On-Demand: a seamless solution that automatically enables and disabled VPN access as end-users access intranet sites from their mobile device.

With AirWatch, these capabilities even extend into proprietary SSL-VPN apps such as Cisco AnyConnect, Junos Pulse, and the F5 BIG-IP Edge Client so that end-users can automatically receive and utilize their VPN certificate and proprietary VPN application. Once again, this equates to unprecedented security for your IT administrators and unprecedented ease of use for your end users.
Email Encryption and Message Signing with S/MIME
When it comes to corporate email, certificates can go even further than secure authentication. By leveraging the Secure/Multipurpose Internet Mail Extensions (S/MIME) standard, certificates can be used for both email encryption and email message signing as well. With email encryption, only the sender and intended receiver of a message are able to see and understand a message. This prevents any third parties from reading through sensitive corporate messages as they are transferred across the wire. With message signing, users can certify their mail with a digital signature from their trusted certificate. This means that email recipients can be certain that the sender of a message is indeed who they say they are.

In-App Encryption and Authentication
Also, by empowering your internally developed applications with the AirWatch SDK, AirWatch is able to deploy digital certificates to individual applications. Whereas certificates deployed to a device can be used for device-wide functions such as Wi-Fi or VPN authentication, certificates deployed within an application can be used for application functions like app data encryption or web service authentication. For example, the Secure Content Locker leverages in-app certificates to encrypt and decrypt corporate content on a device so that it can only be accessed within the Secure Content Locker itself. Empower and secure your internal applications with your corporate PKI with AirWatch.
Certificate Management with AirWatch

Deploying digital certificates to mobile devices is the most effective way of protecting your internal content, however it also requires a great deal of footwork to properly set up and maintain. AirWatch simplifies the normally costly and labor-intensive establishment to provide the most comprehensive Mobile Certificate Management solution in the industry. The AirWatch solution not only ensures safe and secure certificate management but also automates the management process throughout the entire certificate life cycle.

Supported PKI

AirWatch facilitates simplified certificate management for a variety of Certificate Authorities, including both on-premise and cloud-based CAs. AirWatch offers support to an ever-expanding list of CA types to make sure that you can meet your unique project requirements:

Each CA’s native API is supported (for example, DCOM integration for Microsoft ADCS), as well as SCEP (Simple Certificate Enrollment Protocol) if it is supported by the CA. The choice of how to integrate with a CA is dependent upon your unique network setup and security requirements.
Issuing Digital Certificates

AirWatch’s complete certificate lifecycle management starts with automatic certificate issuing to mobile devices. No longer will your end users and IT personnel have to worry about the cumbersome process of manually deploying a certificate to a device. As soon as a device begins the enrollment process AirWatch will seamlessly interact with your corporate certificate authority to deploy a unique digital certificate to each corporate user’s device. Even more, AirWatch will not only deliver the certificate, but it will also tell the device how to use it by seamlessly fetching corporate email, accessing enterprise Wi-Fi, or enabling VPN On-Demand. That said, each time an end-user enrolls in AirWatch, they will automatically request, receive, and utilize a digital certificate without ever even knowing what a digital certificate is in the first place.

Additionally, AirWatch has even made it very easy for administrators to take advantage of certificate deployment from the Admin Console. Configuring AirWatch to issue digital certificates is as simple as:

1. Establishing a connection between AirWatch and your Certificate Authority
2. Configuring the certificate template that AirWatch will fetch from the CA for mobile devices
3. Deploying and utilizing the certificate in a profile

Managing Digital Certificates

Once issued, AirWatch helps you manage the digital certificates seamlessly through the Certificate page in the Admin Console. From here administrators are able to view and sort certificates by issuing CA, expiration date, status, and device. AirWatch gives you authority to manage these certificates for your Enterprise.

![Certificates](image)

*Having all information available in one place makes managing your certificates easier than ever.*

But the Certificate Dashboard doesn’t only provide a summary of deployed certificates—it also provides the ability to immediately renew or revoke certificates individually or in bulk with the click of a button. Easily locate and revoke all digital certificates from a deactivated user/device, or even renew/rotate all Wi-Fi authentication certs well in advance of a compliance driven expiration date.
Renewing Digital Certificates

Next, as certificates gradually approach their expiration date, AirWatch will automatically renew them well in advance. Although on-demand renewal on the Certificate Dashboard does have many benefits under circumstances, automating this process can only yield better results for your corporate IT.

By simply checking a box and specifying a renew period from the Admin Console, administrators will never have to manually renew certificates again – saving help desk hours, operational costs, and any possibilities of human error.

Revoking Digital Certificates

Lastly, revoking digital certificates is just as easy as issuance, management, and renewal. In the event that an employee leaves the company without notice, an administrator can immediately revoke all corporate certificates, content, apps, and profiles on his device so that no further activity can be done under the company’s identity. No internal material can be accessed with the ex-employee’s device or login information.

In addition to revoking a certificate from a device, select CA types (listed below) offer advanced certificate revocation in which AirWatch adds a certificate to a CA’s certificate revocation list (CRL). By doing so, any attempts from an unauthorized user to manually obtain their devices certificate can be prevented, as the certificate itself is now invalid directly on the CA.

With AirWatch’s streamlined certificate revocation process, denying access to internal content is as easy as flipping a switch. Most importantly, it only takes a moment to implement, which is vital to keeping your content and identity safe.