Learning AirWatch

Nowadays, organizations are facing a critical challenge of providing reliable, efficient, and secure access to corporate information. With AirWatch by VMware’s Enterprise Mobility Management (EMM) platform, you will be able to set up and deploy access to corporate information securely from mobile devices, allowing security policies and regulations to meet compliance for your business.

This book will guide you through a detailed overview on how to set up AirWatch by VMware, administer the deployment, manage enterprise integrations, and configure security controls and many more options available for effective EMM deployments in enterprises. Each of the components of EMM is explained in the book in a way that you can apply your knowledge in the best possible manner while working with your mobile deployments.

Who this book is written for

If you are a technical professional who wants to dive deeper into the functionality offered by AirWatch or manage the solution, then this book will help you choose the best set of configuration, device management, and monitoring options that you can use to effectively manage your EMM implementation.

What you will learn from this book

- Set up your working environment with the options provided by AirWatch
- Understand the administration console and learn to manage your EMM platform
- Integrate AirWatch by VMware into your corporate infrastructure
- Secure your EMM deployment to meet the security and regulation standards
- Learn to set up and configure Mobile Device Management (MDM) for your mobile devices
- Discover how to set up and deploy Mobile Containerization and the use cases it can be used for
- Deploy Mobile E-mail Management (MEM) to allow you to access e-mails securely
- Configure Mobile Application Management (MAM) and Mobile Browser Management (MBM)

In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 4 'Mobile Security'
- A synopsis of the book’s content
- More information on Learning AirWatch

About the Author

Mark Dunkerley is currently the manager of messaging, mobile, and video services at the Adventist Health System. He was born in Newcastle upon Tyne, England and currently resides in Orlando, Florida. He holds a bachelor's degree of science in business administration and a master's in business administration.

He has worked in the technology field for over 12 years and has experience in several technical areas. He has earned certifications from AirWatch, Microsoft, CompTIA, VMware, AXELOS, Cisco, and EMC.

Mark is currently involved with unified communication and mobility strategies and deployments in his current role. He recently spoke at several conferences for AirWatch and Microsoft and published several case studies. To view more information on the work Mark has done, you can visit his LinkedIn profile at www.linkedin.com/in/markdunkerley.
Learning AirWatch

The ability to become fully dependent on our mobile devices is a reality we are faced with today. With the rapid growth of mobile usage in the consumer space, enterprises are challenged with providing the workforce with the ability to access corporate resources easily and, most importantly, securely. This is where we need to fully understand the bigger picture of mobility and the security implications that come with it. As technical experts, we are not only responsible for installing and providing the solutions to the end users, but we are also fully responsible for understanding the risks associated with providing access to corporate information and the possible leakage of that information. As we are all aware, there is a constant growth of societies worldwide that are constantly looking for ways to penetrate confidential information, and as technical experts, we are tasked with minimizing the risk.

In order to provide the level of security and usability to our users, we need to understand the tools available on the market today. The latest toolset available that encompasses all manageability of mobile devices is currently known as Enterprise Mobility Management (EMM), which was recently known as Mobile Device Management (MDM). MDM is now part of the overall suite of EMM. EMM tools include the ability to manage mobile devices, applications for the device including a catalog, content on the device, secured containers, integration with enterprise tools, full security over all information, and much more.

Throughout this book, you will learn how AirWatch by VMware has provided the toolset needed to manage all the components of EMM, allowing you to deploy a secure and robust mobile environment. As you travel through the chapters, you will gain a thorough understanding of what is involved in EMM and the benefits it can provide to your workforce. Mobility has exploded in the recent years and is growing at an incredible pace, forcing us to implement solutions to meet the needs of the workforce. This book will allow you to view the bigger picture of mobility and provide you with the information that will allow your organization to become ahead of the curve and provide solutions to the users before they start demanding them from you.

The days of providing only e-mail to mobile devices are behind us, and we need to be innovative as technical experts. If your organization hasn't already done so, it needs to start looking at it as mobile services and invest in a mobility team or provide dedicated resources to allow growth in the area. Today, a mobile strategy is critical for your organization, especially with the growth of the younger generation moving into the workforce and their dependency on mobile devices to do everything.
What This Book Covers

Chapter 1, Getting Started, gives an introduction to AirWatch along with providing you with an overview of the different management suite options available. It continues onto the hosting and support options available to the customer as well as the learning and deployment services available. The chapter then shows the devices supported by AirWatch, the different types of ownership supported and a walk-through setting up your environment.

Chapter 2, Administration, covers how you access the Admin Console once you complete the installation of AirWatch. You will then be shown the Getting Started wizard and how it will help with the deployment. Following the Getting Started wizard is an overview of the console before covering all aspects of the console in detail.

Chapter 3, Enterprise Integration, provides an overview of the enterprise integrations available, then covers core enterprise integrations. The chapter continues onto covering AirWatch Cloud Connector and how to install it as part of your deployment. Once AirWatch Cloud Connector is installed, you will learn how to integrate with the core enterprise systems. The chapter will then finish off with an overview of Mobile Application Gateway, Secure Email Gateway, and other available enterprise integrations.

Chapter 4, Mobile Security, gives an overview of mobile security today and covers the more popular compliances you can expect the need to adhere to. You will then be shown the security controls available within AirWatch before being shown how to implement the controls to secure your mobile fleet.

Chapter 5, Mobile Device Management, provides an overview of Mobile Device Management and then describes the different device ownership types for the admin to understand. You will then be shown what the organization and smart groups are along with how to set them up and configure them. After organization and smart groups, you will learn how to create and publish a profile and what is needed before you enroll your device. You will then learn how to enroll a device, manage your device through the Self Service Portal while finishing off, and un-enroll a device.

Chapter 6, Workspace Management, shows an overview of workspace management and goes into detail about bring your own device and why workspace management is a good fit for it. You will then go over organization groups and smart groups again for workspace management before configuring the workspace options. Next, you will go through the pre-enrollment steps before enrolling a device into workspace management. The chapter then finishes off with managing workspace on the device, how to use the Self Service Portal to manage your device and un-enrolling the device from AirWatch.
Chapter 7, Mobile Email Management, gives an overview of Mobile Email Management and the importance of protecting e-mail. You will then learn the supported deployments within AirWatch before covering how to integrate with the Secure Email Gateway, PowerShell, and Direct Google. The chapter then covers the security configurations available with AirWatch and then demonstrates how to set up and configure an e-mail profile. The chapter then finishes off with managing and removing e-mail.

Chapter 8, Mobile Content Management, provides an overview of Mobile Content Management and the importance of protecting content. The next section will cover Mobile Application Gateway for proxy and content before covering the security configurations available. Next, you will learn how to configure content management and then be shown how to access the configured content before learning how to manage and remove the content from a mobile device.

Chapter 9, Mobile Application and Mobile Browser Management, covers Mobile Application Management by providing an overview before showing how to set up and configure Mobile Application Gateway per-app VPN. You will then learn the different application types and how to deploy applications and manage them. The second part of the chapter covers Mobile Browser Management with an overview of what it is before finishing off with the configuration and deployment of browser management.

Chapter 10, Multiuser and Laptop Management, demonstrates what Multiuser Device Management is by providing an overview to the admin before showing how to configure and deploy multiuser devices into the environment. The second part of the chapter covers laptop management, giving an overview of what it is. You will then learn how to configure and deploy laptop management into the environment.

Appendix, The Future of Mobility, gives an overview of where mobility has come from, what we are seeing it being used for today and an overview of what we could potentially see in the future with mobile devices.
Before you get started with the deployment of your mobile devices, you need to fully understand the risks associated with Mobility and what you can do to best secure the devices for your users. With the ever-growing threat of cyber-crime and the continued increase of data leakage, we need to provide the best possible security available. At the same time, we also need to be conscious of the usability of the mobile solution. If we secure something to a level that makes the solution unusable, the users will circumvent the controls and find other ways to get what they need. This in turn creates more risk to the environment. With this, we need to ensure that the mobile solution being provided is secure, meets regulations, and is also a solution that allows the users to easily use and adopt.

We will first go into an overview of Mobile Security to better understand the vulnerabilities and risks associated with it. We will then take a look at the industry compliances that we need to adhere to today and what to use as technology professionals.

The following section will show us how AirWatch has put Security at the core of its solutions to help us meet the compliance and regulations we are faced with today. Moving beyond this, we will look at how to configure and enforce the security controls within your EMM deployment to better protect your corporate information and users.

The following will be covered in this chapter:

- Security overview
- Industry compliances
- Security with AirWatch
- Securing your devices
Mobile Security

Security overview

We are living in a world where the consumer is driving the technology and the enterprises are trying to catch up with them. With the release of iPhone in 2007, there has been an incredible growth in the use of smart devices and this only continues to grow. The trend has also shifted to the adoption of tablet devices with the release of iPad in 2010. Since then, users are carrying around multiple different mobile devices. Because of this, users demand to be able to access and do everything from their smart devices. The big concern, as we all know, is how to provide this access to the users securely and ensure that the data isn't being leaked.

Over the years, the laptop and desktop markets have matured steadily with the growth of management tools to update the devices and the ability to enforce security policies and firewall rules and ensure that the antivirus is installed and up to date. With the rapid growth of mobile devices, we have been faced with the challenge of efficiently managing and securing these devices. Not only are we faced with managing and securing the devices owned by the enterprise, but also with providing the ability for users to access corporate information on personal mobile devices. This creates a whole new challenge for enterprises as there are multiple risks and challenges associated with this.

As we look to secure the mobile devices, we need to understand how the users are accessing the information and the risks associated with it. An everyday user may not fully understand the risks associated with the information they are accessing and may not realize how vulnerable their device is. To them, they are just doing their job as efficiently as possible. As technical experts, it is our job to understand the risks associated with using mobile devices and enforce the controls available as best as possible.

There are multiple ways in which data breaches can occur, some of the more common are:

- Intentional loss of data where a user steals data from within organization
- Cybercrime whether it be a virus, malware, hacking a device, physical theft by access and so on
- Accidental loss of data where a user unintentionally misplaces data for others to view or outside of the organization
As we look at each of the possible breaches, we need to be able to add controls as best as possible to secure the corporate data. The following is a list of some ways in which we should already be enforcing security within the corporate networks to help prevent data breach:

- **Access Controls**
  - Password/PIN enforcement, certificates, smart cards, biometric/retina

- **Encryption**
  - Data at rest and in transit, at disk level and file level

- **Network**
  - Firewalls, proxies, secure gateways, intrusion detection, VPNs

- **Software**
  - Virus/malware/spyware scanners, software and system updates/patches/fixes, firewalls, remote wipe/disable

- **Auditing and logging**

- **Compliance and policies**

As you deploy your enterprise mobile solution, you need to ensure that you enforce security controls you currently have in place onto your mobile devices and that you are at minimum meeting your policies and compliances. As you build the security requirements for your mobile devices, it is highly recommended that you work closely with your security and compliance teams. For example, I currently work in the health care industry and I have a good understanding of the compliances being enforced to our organization, but I'm not an expert and don't get to see the constant updates and changes to the requirements we need to meet. This is where your security and compliance teams will provide that added knowledge to help you fully understand and build a more secure mobile deployment.

It is important that you work to provide a secure environment for your users and your organization. There are more and more data breaches happening each day with data of millions of users/customers/patients getting into the wrong hands. The cost of this leakage is substantial to the organization, not only in the cost of dollars, but more importantly to the reputation of your organization. We live in a world where trust is critical, and if we can't maintain the trust with our customers because of data leakage, our business will struggle to survive. It is our job as technical professionals to understand and ensure that we are doing all we can to help protect the information within the organization.
Industry compliances

The following is a list of some of the larger industry segments that your organization most likely falls within:

- Health care
- Government
- Education
- Construction
- Technology
- Retail
- Financial
- Hospitality
- Transportation
- Energy/utilities/natural resources

In today's world with technology, your organization will most likely have to comply with some of the standards and regulations that fall within your industry. The compliance will also differ from each country, and it's important that you understand and comply with each of these compliances if they apply to your organization, as severe penalties will occur. As mentioned already, it is extremely important that you work closely with your security and compliance teams, as they will be educated with the latest and most up-to-date compliances that apply to your organization.

The following are some of the more common and known compliances you may be familiar with that can potentially affect your mobile deployment. We won't be able to list and describe all known compliances, but this will give you an idea of the security you will have to adhere to.

- **Payment Card Industry Security Standards Council (PCI)** establishes compliance to help protect customer information from debit/credit card usage. For more information, visit https://www.pcisecuritystandards.org/.

- **The Health Insurance Portability and Accountability Act (HIPAA)** enforces compliance to help protect the privacy of the patient's health information. For more information, visit http://www.hhs.gov/ocr/privacy/.


These compliances are those that fall within industries in the USA.

One point to note is that it shouldn't matter what industry you are in when looking at security controls and enforcement. If you don't have strict compliances to adhere to, you will have information in your organization that needs to be protected. Whether it is an employee’s personal information or proprietary information for your organization, you should always look to enforce the best security controls possible to help prevent the leakage of information outside your organization.

Security with AirWatch

AirWatch has put security at the core of its Enterprise Mobility Management solution. From earlier discussions in the chapter, it is evident that security is not an option but rather a requirement. Your security controls should be fully enabled and in place before you start deploying your devices.

Although the focus of the security is built around the devices, we also need to ensure that Admin Console and the infrastructure used to provide your mobile deployment is also secure. For the most part, you are most likely to already have these controls in place as AirWatch will not be your first deployment of an application and infrastructure. As an overview though, here are the items that will help ensure that you are providing a better service with your AirWatch infrastructure and deployment:

• **Physical access**
  - Ensure that your infrastructure is secure and contains limited access
Mobile Security

- Make sure that there is auditing and logging of who has access
- Ensure that there are multiple layers of access to get to the infrastructure

- Network considerations
  - Ensure that the infrastructure is behind firewalls, proxies, or Intrusion Prevention Systems (IPS)
  - Use DMZ where applicable
  - Ensure that network access is limited to the infrastructure via ACLs/VLANs
  - Only allow access to ports/services that are required
  - Plan and deploy redundancy for High Availability (HA)
  - Plan and deploy scalability for reliability

- Application considerations
  - Limit access to Admin Console to only those who need it
  - Integrate with your current directory to provide better security controls around access
  - Build roles and allow admin access to the needed function
  - Limit Global Admin access to only a few users
  - Keep application up to date with the latest patches/fixes
  - Always enforce encryption for greater security
  - Use certificates to provide secure access

- Logical considerations
  - Enforce complex password policies
  - Ensure that the server OS is always up to date with the latest patches
  - Use server OS Firewall
  - Ensure that the antivirus/anti-spam/anti-malware software is running and always up to date

- Compliance and policies
  - Ensure that auditing and logging is enabled
  - Ensure that you are meeting all compliance and policies and update any that are outdated
  - User agreements during enrollment or for application usage
• Other considerations
  ° Build in High Availability and Disaster Recovery
  ° Back up and protect data

Now that Admin Console and the infrastructure controls are in place, we can look at the security considerations for the mobile devices. With AirWatch, the following security controls are a focus with the mobile devices that will allow you to meet your security compliances and policies.

**Device security**

It is extremely important that we put all the controls available in place with the device as this is where all of the information will be accessed. If the device gets compromised or stolen and there is no security controls in place, all data that is accessible or stored on the device will be compromised. There are multiple controls in place to help protect the mobile devices being used to access your corporate information. With AirWatch, the following security controls can be enforced for the device:

• Use of the Mobile Device Management (MDM) agent to manage devices
• Device encryption enforcement to protect all data
• Device wipe or remote lock in the event a device is stolen
• PIN enforcement to prevent unauthorized access to the device
• Device restrictions on applications, device settings, browser usage and so on
• Enforce the minimum OS version in the event of vulnerabilities
• Enforce specific models for reduced management and vulnerabilities within specific devices
• Geofencing configuration to prevent information leaving specific boundaries
• Jailbroken/rooted detection to prevent access to corporate data
• Enforce installation of Security apps to detect viruses/malware on devices
Mobile Security

Workspace security
Workspace provides you with the ability to deploy a virtualized encrypted work area to the user's devices. This is something that will most likely better fit your BYOD deployment as you don't need to manage the device using an MDM agent. AirWatch Workspace is deployed at the OS layer, which creates a lot more flexibility for your deployment. With AirWatch, the following security controls can be enforced using Workspace:

- AirWatch Workspace is secured with FIPS 140-2 compliant encryption mechanisms
- Workspace allows compromised detection to prevent access to corporate content
- Workspace allows enterprise-wipe of all corporate data not affecting personal content
- Enable Data Loss Prevention (DLP) policies such as copy/paste prevention
- Password protect Workspace and not the device

User security
In order to ensure the best user security, it is recommended that you integrate with your enterprise directory. This will allow you to provide the same level access to your users that you do today using the current policies and compliances you have in place with your current user accounts. You will also create a more secure environment by allowing your directory to own the enablement and termination of your users, preventing duplication of work and possible error of accounts not being correctly disabled in AirWatch. With AirWatch, the following security controls can be enforced for the users:

- Integration to your enterprise directory to provide the following security:
  - Current Directory policies should already be in compliant to meet security requirements
  - User accounts enabled and disabled will automatically allow enrollment/un-enrollment
  - Access can be provided based on user groups already in place
- Integration with certificate services can provide multifactor authentication
- Access to specific content/features can be limited based on the enrollment group
Content security

There are multiple controls available with AirWatch to ensure your content is secure and within compliance. Content can span an array of different entities including applications, e-mail, documents, images, and so forth. It is critical that the content on the user's devices is secure and access to it isn't gained by anyone who shouldn't. With AirWatch, the following security controls can be enforced to better help protect the content:

- AirWatch's SCL provides full security with FIPS-140 compliant 256-bit SSL encryption
- Access to content can be controlled based on location and time
- Policies can prevent content from leaving the SCL and being copied or moved to other locations

E-mail security

Protecting your e-mail and attachments is also a critical part of an organization's security policies. AirWatch provides multiple options to help secure your e-mail depending on how strict your policies and compliances are. With AirWatch, the following security controls can be enforced to better help protect your corporate e-mail:

- E-mail access can be limited based on enrollment of MDM or Workspace and policies enforced by them
- You can prevent copy/paste of an e-mail and e-mails from being forwarded
- E-mail can be deployed and managed via a native profile or a secure e-mail client
- Enterprise or device wipe can be performed to remove e-mail
- Only approved users can be configured to access e-mails
- Attachment control can be enforced with the use of SCL
Network security
You can integrate AirWatch with your existing network security policies by allowing and denying devices based on compliances from AirWatch. This allows you to only permit trusted and secure devices enrolled with AirWatch access to your internal network resources. If devices fall out of compliance with AirWatch, your network can detect and immediately remove access. With AirWatch and your network, the following security controls can be enforced to better help protect your organization:

- Integrate AirWatch to your Network Infrastructure devices via APIs to view device information
- Allow/deny access to Network based on compliances enforced in AirWatch
- Control access to Network based on enrollment of users
- Integrate with certificate authorities to approve and allow Network Access to internal resources
- Allow access to corporate network by use of an approved VPN
- Allow access to an internal application through the use of App Tunneling

Application security
There are multiple ways to ensure the protection of your apps to help meet your security requirements and compliances that have been put in place. For corporate-owned devices, you will be able to fully manage the application being accessed and used but there are some considerations with BYOD. Depending on the app and how it's being made available will depend on how much you can secure it. If vendors release an application that is available in the public app store, you will need to work with them to see what security controls they have in place with their app that can be integrated with AirWatch. With AirWatch, the following security controls can be enforced to better help protect your applications:

- Application installation can be granted or restricted using whitelisting or blacklisting
- Some native applications can be restricted on devices
- Applications can be deployed to only specific enrollment groups
- Access to applications can be disabled if devices don't meet your MDM or workspace policies
- Additional security features can be added to applications using the AirWatch Software Development Kit (SDK)
- Additional security features can be added to applications using AirWatch App Wrapping
Certificate security

There are a number of integrations available with certificates that will provide an additional layer of security to your mobile deployment. By leveraging certificates within AirWatch, you will be able to provide additional security to the following initiatives:

- E-mail authentication with certificates
- Wi-Fi access and authentication with certificates
- Certificate Integration for VPN authentication
- Certificates to encrypt e-mails and message signing with S/SMIME
- In-app encryption and authentication with certificates

The compliance engine

AirWatch has an extremely powerful compliance engine that will help you enforce the policies and security required within your organization. Compliance engine allows you to continuously monitor and detect devices that are out of compliance. If devices are out of compliance, you are able to apply multiple different actions to ensure that the device is put back into compliance or to simply enterprise wipe or device wipe if needed. With AirWatch, the following compliances can be enforced to help protect your corporate information:

- Application List (contains or does not contain a specific identifier, contains blacklisted or whitelisted app(s), does not contain required apps or does not contain a specific version)
- Cell data usage meets or exceeds a specific percentage
- Cell message usage meets or exceeds a specific percentage
- Cell voice usage meets or exceeds a specific percentage
- Device is compromised or is not compromised
- Device last seen within a specific amount of hours or days
- Encryption is not enabled
- Expiry of the interactive certificate profile within a specific amount of days
- Laptop encryption is not enabled
- Last compromised scan not within a specific amount of hours or days
- MHD terms of use acceptance not within a specific amount of hours or days
- The model is or is not a specific version
Mobile Security

- The OS version (is the same, is not the same, is greater than a specific version, is greater than or equal to a specific version, is less than or equal to a specific version)
- The passcode is not present
- The device is roaming
- The SIM card change has been detected

Securing your devices
Now that we have a better idea on the security available with AirWatch, you will need to configure your environment to enforce the security controls discussed within this chapter to your devices. During this section, we will navigate through where you can configure the components that have been reviewed to better secure the mobile devices being managed.

Passcode and encryption
One of the most important security settings for your devices is the passcode and encryption. For your MDM-enrolled devices, you are going to want to enforce a device-level password and encryption to protect the information on the device. Depending on the manufacturer, the enabling of encryption may be a little different. For the iOS and Android, you can configure the passcode and encryption in the following way:

- For iOS password and encryption enforcement, perform the following steps:
  1. Log in to the Admin Console.
  2. Navigate to Devices | Profiles | List View.
  3. Click on Add and then on Apple iOS.
  4. In the General section fill out all the information required and assign it to the smart groups the policy will apply to.
  5. Click on Passcode and then on Configure. Enter the required passcode on the device.

We will go into the profile creation in more detail within Chapter 5, Mobile Device Management. This chapter will simply demonstrate where to configure the security features to better protect your devices.
6. Fill out the passcode requirements based on your security requirements.

7. Click on **Save & Publish** to enforce the policy.

Have a look at the following screenshot:

<table>
<thead>
<tr>
<th>Passcode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require passcode on device</td>
</tr>
<tr>
<td>Allow Simple Value</td>
</tr>
<tr>
<td>Require Alphanumeric Value</td>
</tr>
<tr>
<td>Minimum Passcode Length</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
</tr>
<tr>
<td>Maximum Passcode Age (days)</td>
</tr>
<tr>
<td>Auto-Lock</td>
</tr>
<tr>
<td>Passcode History</td>
</tr>
<tr>
<td>Grace period for device lock (min)</td>
</tr>
<tr>
<td>Maximum Number of Failed Attempts</td>
</tr>
</tbody>
</table>

iOS devices are encrypted by default, so you don't need to enforce encryption through the profile, but you will need to enforce a passcode in order to effectively prevent access to data on the device. Also, the National Institute of Standards and Technology (NIST) granted iOS 6 with the FIPS 140-2 certification. It is recommended that you configure your iOS profiles to require at least iOS 6 for additional security.

- For Android password and encryption enforcement, perform the following steps:
  1. Log in to the Admin Console.
  2. Click on **Devices | Profiles | List View**.
  3. Click on **Add** and then on **Android**.
4. In the **General** section, fill out all the information required and assign it to the smart groups the policy will apply to.

5. Click on **Passcode** and then on **Configure**.

6. Fill out the passcode requirements based on your security requirements and enable storage and SD card encryption.

7. Click on **Save & Publish** to enforce the policy.

Have a look at the following screenshot:

As you can see with the Android profile, you need to enforce encryption on the devices as they don't have it enabled by default. This is similar on some of the other device types in which you will need to enforce and configure encryption.
Setting up a passcode for Windows 8 devices is very similar to setting up the iOS passcode profile.

If you aren't going to be using MDM for your deployment and you will be using workspace or apps that don't require MDM, you will want to require a passcode for access and ensure that encryption is enforced, which is by default on AirWatch native applications.

- **Require Passcode on Workspace/Apps**
  1. Log in to Admin Console.
  2. Click on **Groups & Settings** and then on **All Settings**.
  3. Click on **Apps | Settings And Policies | Security Policies**.
  4. Select the type of **Passcode Mode** to enable a passcode and fill out the passcode requirements based on your security requirements.
  5. Click on **Save** to save the settings.

Have a look at the following screenshot:

![Apps / Settings And Policies / Security Policies](image)
If you don't already have a password policy for mobile devices and workspace, you will need to work with your security and compliance team to create one. It is recommended that you don't simply use the current password policy you use for your enterprise directory for your mobile devices and workspace. Enforcing long complex passwords on a mobile device or workspace creates extreme difficulty and frustration and you have to evaluate the risk of possibly allowing a PIN. The PIN is only used for the mobile device and workspace and not used for any other enterprise access. The hacker would physically need access to the device in order to compromise and gain control, so the risk to use a PIN can be looked at as low. To add additional security to the device, configure a maximum number of failed attempts on the passcode to force a device wipe or enterprise-wipe on workspace after the specified number of incorrect attempts.

Certificate integration
To deploy certificates to your devices in AirWatch, you will need to ensure that you have set up your integration to your CA and configure the template AirWatch will use to deploy the certificates as covered in Chapter 3, Enterprise Integration. Once you have your CA and template set up, you can deploy certificates using AirWatch profiles. We will demonstrate how to configure a profile using the credentials payload (you can also configure SCEP) in AirWatch using the following instructions:

1. Log in to the Admin Console.
2. Click on Devices | Profiles | List View.
3. Click on Add and then on the platform to deploy the certificate (I will use iOS).
4. In the General section, fill out all of the information required and assign it to the smart groups the policy will apply to.
5. Click on Credentials and then on Configure.
6. Select one of the following credential sources:
   - Upload to import an individual certificate to the device
   - Defined Certificate Authority to select your integrated CA and certificate template
   - User Certificate for S/MIME
7. Click on Save & Publish to enforce the policy.
Have a look at the following screenshot:

![Credentials](image)

Now that you have configured the devices to use certificates, you can start leveraging them for multiple initiatives. One example I have just worked on is the integration of certificates with our enterprise Cisco ISE deployment. We are leveraging the AirWatch CA integration to install certificates from our internal CA with customized attributes in the certificate. ISE is then being configured to look for devices with the certificates we have deployed with the customized attributes. Once ISE has validated the device has the correct certificate, it will automatically onboard the device to the internal network to allow connection to all resources. This allows us to better manage our corporate assets as we have full control and management over them and what is installed.

For additional security, you can also manage, view, and revoke certificates from Admin Console. Simply navigate to Devices | Certificates | List View to see all deployed certificates in your environment.

There are way too many certificate integrations to cover in this book, let alone this chapter. To learn more on all the certificate options and integration in AirWatch, log in to the myAirWatch portal, go to Resources, click on Home on the left, and then click on Certificate Management to view all certificate management guides.

**Enterprise and device wipe**

Another great security feature within AirWatch is the ability to enterprise or device wipe an enrolled device. The difference between an enterprise-wipe and a device wipe is that an enterprise wipe will remove only the data that has been deployed as part of the enrollment. This will be most valuable in BYOD deployments, where you don't want to device wipe a user's personal device since legality issues may arise. A device wipe on the other hand is the ability to reset the device back to default and remove all data. This is most useful with corporate-owned assets and stolen devices.
Mobile Security

The following steps demonstrate how to enterprise or device wipe an asset as an admin:

1. Log in to Admin Console.
2. Click on **Devices | List View**.
3. On the main screen, search for the device to be wiped.
4. Click on the device name under the **General Info** column.
5. In the top-right corner, click on More. Here, you will see the **Enterprise Wipe** and **Device Wipe** options.
6. Click on the action you would like to take with the device.

Here is a screenshot for your reference:

![Enterprise Wipe and Device Wipe options](image)

There is also a way for the user to enterprise or device wipe their device from AirWatch Self Service Portal. This allows the user to be more proactive and not have to wait for the IT group to wipe the device in the event it has been stolen. To wipe your own device, navigate to your environment's URL with `/mydevice` added to the end, for example, `myenvironment.awmdm.com/mydevice`. Log in with your e-mail or group ID, then click on **Next**, enter your username and password, and click on **Login**. Then, select your device and click on **Enterprise Wipe** or **Device Wipe** and then on click on **OK**.

You may not see the option to device wipe because the device you are trying to wipe may be assigned to the employee-owned profile, which may be configured to not allow this. If you were requested to device wipe someone's device and it's on the employee-owned profile, you can simply change the device ownership to **Corporate-Dedicated** then device wipe.
Autodisable accounts

If you have integrated with your enterprise directory, which is recommended, you will want to ensure that the user accounts are being automatically disabled or removed from AirWatch based on the status within your enterprise directory. This allows one place to manage your accounts and allows the current process to continue without needing to manually disable the accounts in AirWatch. To ensure accounts are being automatically disabled and removed from groups, which will force un-enrollment in AirWatch and remove corporate data, you need to complete the following:

1. Log in to the Admin Console.
2. Click on Groups & Settings and then on All Settings.
4. Click on User in the main screen and then on Show Advanced. Check Automatically Set Disabled Users to Inactive and then click on Save.
5. Click on Group on the main screen and then on Show Advanced. Check Auto Sync Default and Auto Merge Default and then click on Save.

If you don't assign groups to your profiles, you don't need to have the groups auto sync and merge. You will just need to ensure that the account is set to automatically disable.

6. If you are leveraging groups in your profiles, you will also need to configure the group to automatically sync:
   1. Navigate to Accounts | User Groups and click on the group you would like to configure to auto sync.
   2. Check Auto Sync with Directory and Auto Merge Changes and then click on Save.
Geofencing and time schedules

Geofencing and time schedules allow you to better control where users can access your corporate information and apply time as to when they can access your corporate data. For Geofencing, you may need to require that your corporate information does not leave the state your organization resides in or the country you work in. With a Geofence profile, access to the corporate data will not be allowed if the device falls outside the scope of the defined area. For time schedules, this allows you to configure devices to only allow access during the specified time. For example, you may have employees who are working on an hourly basis and are not allowed to check their e-mail out of hours. You can prevent this by assigning a time schedule that will prevent them from accessing e-mail outside of work hours. To set up Geofencing and time schedules, you first need to define them:

1. Log in to Admin Console.
2. Navigate to Devices | Profiles | Settings.
3. Click on Geofencing to define the areas access is permitted.
4. Click on Time Schedules to create the time during which access is permitted.

Once you have defined the geofence area and time schedule, you can apply them to your profiles:

1. Log in to Admin Console.
2. Click on Devices | Profiles | List View.
3. Click Add and click on the platform to deploy geofence and time schedule (I will use iOS).
4. In the General section, fill out all the information required and assign it to the smart groups the policy will apply to.
5. Towards the bottom, click on Enable Geofencing and install only on devices inside selected areas. Select the created Geofence area.
6. Towards the bottom, click on Enable Scheduling and install only during selected time periods. Select the created Time Schedule.
7. Click on Save & Publish to enforce the policy.
Workspace security

There are multiple options to ensure that when you deploy workspace to the users, your corporate information is fully protected. You will want to ensure that there is a passcode enforced as described in the Passcode and Encryption section, Compromised Detection is enabled, and the Data Loss Prevention settings are configured. To enable or disable the configurations in workspace, complete the following:

1. Log in to Admin Console.
2. Click on Groups & Settings and then on All Settings.
4. Configure the security settings based on your corporate policy and then click on Save.

Here is a screenshot for your reference:
Terms of use

For legal and compliance, you may be required to have users agree to the services that they are using. In AirWatch, you can force the users to agree to terms of use during enrollment, during an application installation, or for access to the console. If the user doesn't agree to the terms, they won't be able to use the service. To apply terms of use in your environment, complete the following steps:

1. Log in to Admin Console.
2. Navigate to Accounts | Terms of Use | Add Terms Of Use.
3. Select Console, Enrollment, or Application.
4. Fill out the options and add your terms and click on Save.

The compliance engine

Now that you have all the security configured in place, you need to ensure that the device is in compliance with your policies. AirWatch has an extremely powerful compliance engine that not only detects devices out of compliance, but allows you to take actions against the noncompliant devices. As seen earlier in the chapter, there are multiple rules that can be applied to your devices. The most notable ones you will want to enable first is Compromised Status, Encryption, and Passcode detection. There are too many rules to demonstrate within this chapter for all the configurations, so we will demonstrate one to give you an idea on how to configure the rest. We will configure Compromised Status, as this is the only way to detect jailbroken/rooted devices for MDM profiles. To configure your compliance policy, complete the following steps:

1. Log in to Admin Console.
2. Navigate to Devices | Compliance Policies | List View and then click on Add.
3. In the dropdown, select Compromised Status and click on Compromised.
4. Click the + sign to add additional rules or click on Next.
5. Next is the actions you choose; you have the following choices:
   - Application to block/remove an app or all apps
   - Command to enterprise wipe or request a check-in
   - E-mail to block e-mail
   - Notify to send an e-mail, an SMS, or a push notification to the device
   - Profile to block/remove a profile or all profiles or install a compliance policy
6. For this example, we will notify the user by sending them an e-mail (you can create custom templates to use) that they have 24 hours to resolve the compliance issue or we will remove all profiles. Click on Next.

Here is a screenshot for your reference:

![Screenshot of AirWatch policy setup]

7. In the assignment screen, you will select the platform to apply the policy to. If you like, specify the Model, Operating System and Ownership Type then select Managed By. Select which smart groups to apply the policy to. Click on Next.

8. The Summary screen is where you specify the name and description of the policy and view how many devices are compliant and noncompliant to which the policy will apply. Click on Finish And Activate to apply the policy.

9. Build as many policies as you need to enforce compliance on the devices.

Other security controls

Other security controls within AirWatch include the ability to leverage third-party applications, more specifically, third-party applications that help with security to better protect your enrolled devices from viruses and malware. One example of this integration would be with Lacoon Mobile Security that helps protect your mobile devices from advanced mobile threats. With AirWatch, you can deploy the Lacoon mobile agent to your enrolled devices for added protection. In the event a user removes the agent, you can set up your compliance engine to remove AirWatch profiles to ensure safety of corporate information.
Additional security can be added to the devices through Restrictions. To add restrictions to your managed devices, log in to Admin Console and perform the following steps:

1. Navigate to **Devices | Profiles | List View**.
2. Click on **Add** and then on the platform to deploy restrictions.
3. In the **General** section, fill out all the information required and assign it to the smart groups the policy will apply to.
4. Click on **Restrictions** and deselect what shouldn't be available to the users.
5. Click on **Save & Publish** to enforce the policy.

Restrictions can include device, applications, security, media, and some others depending on the device type.

Outside of certificate integrations, you also need to secure your Admin Console access using an SSL. This would have been part of your deployment and should have already been complete. Other SSL usages will be with the MAG and the SEG, which will require you to use SSLs to encrypt all communication. The MAG and SEG configurations will be covered in more detail in *Chapter 7, Mobile E-mail Management*, and *Chapter 8, Mobile Content Management*.

Additional security controls within the profiles include configuring a Global HTTP Proxy, content filters, and VPN to allow access to internal resources (not all these options may be available for all device types). To configure these options, log in to Admin Console and perform the following steps:

1. Navigate to **Devices | Profiles | List View**.
2. Click on **Add** and then on the platform to deploy restrictions.
3. In the **General** section, fill out all the information required and assign it to the smart groups the policy will apply to.
4. Select the additional security controls (payloads) you would like to apply from the left-hand side of the screen.

It is extremely important that you maintain the AirWatch logs for auditing and logging purposes. It is recommended to export these logs to an external enterprise logging system to allow them to be centrally monitored along with all your other enterprise system logs. This will allow your Security team to monitor unauthorized access and any abnormal behavior within the AirWatch environment. To configure integration with your enterprise logging, log in to Admin Console.

1. Click on **Groups & Settings** and then on **All Settings**.
2. Navigate to **System | Enterprise Integration | Syslog** and configure your external logging server with AirWatch.
Summary

This chapter demonstrates the importance of security in the enterprise environment and how we must fully understand the risks associated with mobility. It is our job as professionals to ensure that we apply the required security controls to help us meet the organization's policies and regulations.

In this chapter, we first looked at mobile security at a high level to get a better understanding of the ways data can be breached and the ways in which we can help prevent the data from being breached. We then moved into looking at the different industries and listed some examples of industry compliances you may have to adhere to as part of your mobile strategy.

The next section showed us the security options available within AirWatch and how they can help us secure the mobile devices being enrolled. To finish the chapter, we demonstrated how to configure AirWatch to enforce the security controls and to ensure they aren't removed. Now that we have everything set up from the console to enterprise integrations, we can move to the next chapter, which will allow us to start building the profiles to allow mobile devices to be enrolled in the environment.
Where to buy this book

You can buy Learning AirWatch from the Packt Publishing website.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

Click here for ordering and shipping details.