vmware airwatch

VMware AirWatch SaaS Overview

Upgrades and Maintenance Overview

vmware airwatch

Contents

Introduction

The purpose of this document is to provide an overview of the SaaS offering including information regarding the scheduling of software updates for dedicated SaaS environments, the AirWatch and Workspace ONE software update process checklist, and answers to frequently asked questions relative to customers using SaaS environments.

Customers have the option to deploy the AirWatch solution using a Shared SaaS environment or Dedicated SaaS environment. A Shared SaaS environment is one where a customer is deployed in a multi-tenant shared instance with other customers. VMware AirWatch SaaS Operations controls the frequency and timing of promoting software updates, which include upgrades or feature packs. To accomplish this, shared VMs are assigned to the Shared SaaS environment to host the AirWatch application. The database does reside on a shared SQL Cluster, where it contains data for multiple customers which is isolated within the application layer.

Many customers chose to deploy the AirWatch solution using a Dedicated SaaS environment, which provides them direct control over the frequency and timing of promoting software updates, which include upgrades or feature packs. To accomplish this, dedicated VMs are assigned to the Dedicated SaaS environment to host the AirWatch application. The database does reside on a shared SQL Cluster, however the database containing customer data is isolated and not shared.

The VMware AirWatch SaaS Operations team monitors all SaaS environments using both uptime and performance indicators. In regards to performance, in most cases on-the-fly changes can be made to the infrastructure to seamlessly update back end resources to meet the growing needs of customers. In the rare case that a short downtime window for a dedicated environment is needed, the AirWatch Account Representative (Technical Service Manager/Support/etc.) will work directly with the customer and downtime will occur during an agreed upon maintenance window. For more information regarding SaaS Maintenance, refer to the SaaS Maintenance and Support section of this document.

Scheduling an Upgrade

VMware AirWatch SaaS Operations schedules all software updates for Shared SaaS environments, and shall provide at least 5 days advanced notice via email of Upgrades to production environments.

Shared SaaS UAT environments receive daily upgrades during business off-hours without any advanced notification,

- NA Shared UAT upgrades during 1 AM (ET) to 5 AM (ET)
- APAC Shared UAT upgrades during 10 AM (ET) to 2 PM (ET)
- EMEA Shared UAT upgrades during 2 PM (ET) to 6 PM (ET)

All times are noted in Eastern Time Zone, USA

To schedule a software update for your Dedicated AirWatch SaaS environment, please use the Upgrade Scheduler tool available on the myAirWatch support portal. For any queries regarding this tool, please refer to https://support.air-watch.com/articles/115001661768

AirWatch recommends providing a minimum of 5 days advanced notice to ensure your desired maintenance window is available.

With Globally distributed teams, AirWatch offers the following update windows during the business week:

- 1 AM (ET) to 5 AM (ET)
- 5 AM (ET) to 9 AM (ET)
- 10 AM (ET) to 2 PM (ET)
- 2 PM (ET) to 6 PM (ET)

All times are noted in Eastern Time Zone, USA

Note: Upon request, AirWatch may provide after-hours weekend update windows. Such after-hours windows may be subject to additional costs. Contact AirWatch Account Representative for specific options based on your requirements.

For any support related issues, AirWatch offers a 24/7 support available as per the support procedures outlined on the AirWatch website (http://www.air-watch.com/downloads/pricing/support-pricing-na.pdf).

Dedicated SaaS Upgrade Process

Pre Upgrade

- ✓ Confirm access to all active and passive Application and Database Servers
- ✓ Stage Application Files to all active and passive servers

During Upgrade

- ✓ Check ticket systems and confirm the Upgrade details (time, version, etc.)
- ✓ Disable automated monitoring platforms for the environment
- ✓ Enable the Maintenance page for the environment
- ✓ Stop all AirWatch Services and Applications on all the Application Servers
- ✓ Backup all Application Servers and Database
- ✓ Apply Windows Patches on all Application Servers
- ✓ Upgrade all the relevant Application Databases
- ✓ Upgrade the relevant Application Servers
- ✓ Upgrade the relevant Reports Database
- ✓ Run basic tests on All Application Servers
- ✓ Disable any passive Application Servers
- ✓ Remove Maintenance page for environment
- ✓ Expected User Impact during the upgrade includes but is not limited to,
  - Admin users will not be able to log in to the AirWatch Console
  - New device users will not be able to enroll
  - Existing device users will not be able to access the App Catalog or Self Service Portal, as well as some other AirWatch apps like Tunnel and Browser (See notes about the Enterprise components)
  - Existing Content in Content Locker will continue to be accessible, but new content will not be available
  - VMware Identity Manager integration with backend enterprise system is available during the upgrade

Post Upgrade

- ✓ Perform any additional configuration needed for the environment (varies on the version in question)
- ✓ Perform basic tests for verifying core AirWatch Functionality, such as:
  - Device Enrollment
  - Basic MDM Commands
- ✓ Re-Enable automated monitoring platforms for the environment

Rollback Plan

- ✓ Restore active and passive Application Server backups
- ✓ Restore database on the Database Server backup
- ✓ Run basic server tests on each Application Server
- ✓ Perform basic tests for verifying core AirWatch Functionality, such as:
  - Device Enrollment
  - Basic MDM Commands
- ✓ Re-Enable automated monitoring platforms for the environment

Note: Workspace one customers will have the VMware Identity Manager components upgraded alongside the upgrade of core AirWatch systems

Frequently Asked Questions

What is the difference between a Shared vs. Dedicated SaaS Environment?

The table below highlights the key differences between Shared and Dedicated SaaS deployment models

Features	Shared SaaS	Dedicated SaaS
Custom URL for your Environment	✓ (Setup as Redirects)	✓* (Set up as CNAME record)
Lock down AirWatch Console URL by IP range		✓
Migration between SaaS and on premises	✓ (Requires re-enrollment)	✓ (No end-user action needed)
Upgrades to latest AirWatch version	✓ (Environments upgraded on quarterly release cycle)	✓ (Customer approval required to upgrade environment)
Testing available in a Shared UAT environment	✓	✓
Feature Pack updates for the current AirWatch version	✓ (Applied at regular intervals)	✓ (Applied at regular intervals and customer approval is required)
Rollback options		✓ (Within 24 hours with customer approval)
Device count recommendation	20,000 or less	Greater than 20,000
Dedicated VMware Identity Manager		✓ (Greater than 3,000 users)

*Does not apply to dedicated VMware Identity Manager endpoints

What are the AirWatch SaaS IP ranges?

For SaaS customers who need to whitelist outbound communication, please refer to the following AirWatch Knowledge Base article for a list of up-to-date IP ranges AirWatch currently owns: https://support.air-watch.com/articles/115001662168

Will I get notified when the upgrade is complete?

For Dedicated SaaS environments, notifications will be provided. When you schedule the upgrade via myAirWatch support portal, a support ticket is automatically created to track progress. This ticket will be updated when the upgrade begins and completes, which will also send email notifications.

Will new features be setup as part of the upgrade process?

The upgrade process focuses on maintaining functionality present prior to the upgrade, and no set configurations on the console will be altered. If you wish to setup a new feature, it is recommended to refer to the AirWatch Administrator and User Guides, along with the AirWatch Knowledge Base. Additionally, AirWatch offers a number of Professional Services options for assisting implementing new features. Please contact your Account Representative for specific options based on your requirements.

Where can I find more information about the new version of AirWatch?

For more information such as release notes or administrator guides, please refer to the AirWatch Knowledge Base.

Will I have to do anything prior to the upgrade?

It is highly recommended that clients:

- Review their support and relevant end-user documentation with every upgrade
- Notify their AirWatch Administrators and End-Users of the planned outage for the AirWatch upgrade, and advise them of the implications
- Avoid scheduling conflicts so that other related activities (such as device roll out or application deployments) do not overlap with the upgrade process

Will I have to do anything or test anything when the upgrade is completed?

As part of the update process, AirWatch validates that core functionality is maintained post update. It is highly recommended that clients review their support and relevant end-user documentation with every update in addition to validating any functionality deemed critical for their end-users.

Can I test the new version ahead of time?

Contact AirWatch Account Representative for specific options based on your requirements.

Can AirWatch setup a test environment in the cloud for me?

Contact AirWatch Account Representative for specific options based on your requirements.

What can I use a test environment in the cloud for?

User Acceptance testing (UAT) environments are ideally used for:

- Testing of the critical customer end-user workflows ahead of a new version upgrade
- Creation and testing of new end-user workflows before deployment into production environment
- Testing new application functionality and application code fixes ahead of a new version upgrade
- Updating customer end-user documentation ahead of a new version upgrade

UAT environments are not intended to support any load or penetration testing

Customers are requested to contact their AirWatch Account Representative for specific options based on your requirements

How many devices can I register in a test environment?

For a Shared UAT environment, customer deployments are limited to 25 devices

For a Dedicated UAT environment, customers are recommended to deploy no more than 50-100 devices

Who do I contact in case of any issues post update?

For Shared SaaS environments, please engage via support.air-watch.com. Support procedures outlined at: http://www.air-watch.com/downloads/pricing/support-pricing-na.pdf

Similarly for Dedicated SaaS environments, when the upgrade is completed, the email alert will invite you to engage with Support for any issues.

Is there a roll back plan to restore to the previous version in case the upgrade goes wrong?

For Shared SaaS environments, AirWatch Operations will initiate a roll back should there be any issues encountered post update. For Dedicated SaaS environments, customers can request a roll back within 24 hours of the upgrade starting. Following the standard support procedures, please engage with Support to initiate a roll back.

What is the impact to devices and end-users during the upgrade?

The impact to end users is minimal – primary impact is outlined below:

- Existing profiles, policies and applications deployed to devices will still function on the device
- Email will continue to sync as normal
- Users will not be able to enroll new devices
- The App Catalog will be unavailable, so users will not be able to install internal applications. Public applications can be downloaded directly from the device's native Application store. Non-sToken VPP users will not be able to join the VPP program to download VPP apps.
- The Self Service portal will be unavailable
- Content Locker will allow users to view content that has already been downloaded to the device (Security policies allowing) but users will not be able to download new content
- AirWatch Browser will continue to work normally for users that have previously signed in (Security policies allowing) but will not function if the configuration is set to use AirWatch Tunnel
- AirWatch Inbox / VMware Boxer will continue to function
- AirWatch Tunnel will be unavailable
- Any AirWatch Administrator users will be unable to login to the AirWatch Console
- For the Shared SaaS VMware Identity Manager customers, there should be no impact to incoming authentication requests
- For On-Premise VMware Identity Manager instances, there should be no impact to incoming authentication requests
- For Dedicated SaaS VMware Identity Manager, the infrastructure will be upgraded along with the AirWatch upgrade process so no integration with backend enterprise system is available during the environment upgrade

Secure Email Gateway (SEG)

The Secure Email Gateway is an optional component that may be installed on your environment based on your email technology and management requirements. If the Secure Email Gateway is installed in your environment, refer to the FAQ below:

Do I need to upgrade the SEG?

Although it is not a requirement, it is recommended to upgrade the SEG infrastructure as part of the MDM server upgrade process. In general, backwards compatibility is maintained for up to a three major release version difference, however, the SEG is designed to work most efficiently when aligned with the same version as the AirWatch Application servers.

What is the impact to the SEG during the AirWatch environment Upgrade?

Compliance and blocking policies are cached locally on the SEG server. During an upgrade of the AirWatch environment, this cache is maintained and email infrastructure is secured.

What is the impact to the SEG during a SEG Server Upgrade?

The SEG server goes into failover mode during an upgrade. In failover mode, the compliance and blocking rules cached on the server are cleared. By default, the SEG is configured to fail open, so email on both compliance and non-compliant devices will continue to sync. This can also be configured to fail closed if required.

Should I make additional considerations if I have multiple SEG servers?

If multiple SEG servers are available in a highly available architecture behind a load balancer, the SEG servers can be taken out of the pool one by one and upgraded individually to maintain the integrity of the compliance and blocking rules protecting your email infrastructure.

AirWatch Cloud Connector (ACC) – For AirWatch versions 9.0 and lower

The AirWatch Cloud Connector Server is an optional component that may be installed on your environment based on your needs to securely integrate with backend enterprise systems such as Active Directory or Exchange from the AirWatch SaaS environment. If the AirWatch Cloud Connection Server is installed in your environment, refer to the FAQ below:

Do I need to upgrade the ACC?

Although it is not a requirement, it is recommended to upgrade the ACC infrastructure as part of the AirWatch environment upgrade process. The ACC can be configured to auto upgrade itself upon detecting the new version on the Application servers. In general, backwards compatibility is maintained for up to a three major release version difference; however the ACC is only supported for version 6.4 or higher, and is designed to work most efficiently and support available features when aligned with the same version as the AirWatch Application servers.

What is the impact to the ACC during the AirWatch environment Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. During an upgrade of the Application server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

What is the impact to the ACC during an ACC Server Upgrade?

No integration with backend enterprise system is available during the ACC Server upgrade. During an upgrade of the ACC server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

VMware Enterprise Systems Connector – For AirWatch versions 9.1 and higher

The VMware Enterprise Systems Connector is an optional component that may be installed on your environment based on your needs to leverage VMWare Identity Manager and or securely integrate with backend enterprise systems such as Active Directory or Exchange from the AirWatch SaaS environment. If the AirWatch Cloud Connection Server is installed in your environment, refer to the FAQ below:

Do I need to upgrade the VMware Enterprise Systems Connector?

Although it is not a requirement, it is recommended to upgrade the VMware Enterprise Systems Connector infrastructure as part of the AirWatch environment upgrade process. In general, backwards compatibility is maintained for up to a three major release version difference; however the VMware Enterprise Systems Connector is only supported for version 9.1 or higher, and is designed to work most efficiently and support available features when aligned with the same version as the AirWatch Application servers.

What is the impact to the VMware Enterprise Systems Connector during the AirWatch environment Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. During an upgrade of the Application server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

What is the impact to the VMware Enterprise Systems Connector during a VMware Enterprise Systems Connector Server Upgrade?

No integration with backend enterprise system is available during the VMware Enterprise Systems Connector Server upgrade. During an upgrade of the VMware Enterprise Systems Connector server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

Enterprise Integration Service (EIS)

The Enterprise Integration Server is an optional component that may be installed on your environment based on your needs to securely integrate with backend enterprise systems such as Active Directory or Exchange from the AirWatch SaaS environment. If the Enterprise Integration Service is installed in your environment, refer to the FAQ below:

Do I need to upgrade the EIS?

Although it is not a requirement, it is recommended to upgrade the EIS infrastructure as part of the AirWatch environment upgrade process. In general, backwards compatibility is maintained for up to a three major release version difference, however, the Application is designed to work most efficiently and support available features when aligned with the same version as the Application servers.

What is the impact to the EIS during the AirWatch environment Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. During an upgrade of the Application server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

What is the impact to the EIS during an EIS Server Upgrade?

No integration with backend enterprise system is available during the EIS Server upgrade. During an upgrade of the EIS server, existing email compliance and blocking policies for PowerShell integration stay in effect and no new policies are implemented via MDM.

Content Gateway (CG)

The Content Gateway Server is an optional component that may be installed on your environment based on your needs to securely integrate with backend Content directories and systems. If CG is installed in your environment, refer to the FAQ below:

Do I need to upgrade the CG?

Although it is not a requirement, it is recommended to upgrade the CG infrastructure as part of the AirWatch environment upgrade process. In general, backwards compatibility is maintained for up to a three major release version difference, however, the Application is designed to work most efficiently and support available features when aligned with the same version as the Application servers.

What is the impact to the CG during the AirWatch environment Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. Any content normally available in Content Locker via CG will be unavailable.

What is the impact to the CG during a CG Server Upgrade?

No integration with backend enterprise system is available during the CG Server upgrade. Any content normally available in Content Locker via CG will be unavailable.

VMware Tunnel

The VMware Tunnel Server is an optional component that may be installed on your environment based on your needs to securely integrate with backend web and network systems. If Tunnel is installed in your environment, refer to the FAQ below:

Do I need to upgrade the Tunnel?

Although it is not a requirement, it is recommended to upgrade the Tunnel infrastructure as part of the AirWatch environment upgrade process. In general, backwards compatibility is maintained for up to a three major release version difference, however, the Application is designed to work most efficiently and support available features when aligned with the same version as the Application servers.

What is the impact to the Tunnel during the AirWatch environment Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. AirWatch Tunnel application will not function.

What is the impact to the Tunnel during a Tunnel Server Upgrade?

No integration with backend enterprise system is available during the AirWatch environment upgrade. AirWatch Tunnel application will not function.

SaaS Maintenance and Support

The VMware AirWatch SaaS Operations team monitors all SaaS environments using both uptime and performance indicators. In regards to performance, in most cases on-the-fly changes can be made to the infrastructure to seamlessly update back end resources to meet the growing needs of customers and perform routine maintenance activities. Such changes are implemented in accordance with established Change Management procedures which would include communications to customers a minimum of 5 business days lead time.

VMware AirWatch Monthly maintenance schedule is published to the myAirWatch support portal on an annual basis and can be found below:
https://resources.air-watch.com/save/m5mqfn7shddk67pfvmcp/en

For more information regarding the standard maintenance windows please refer to the myAirWatch support portal.

In the rare case that an unplanned downtime window is needed for a Dedicated SaaS environment, changes are deployed following Change Management emergency procedures where the AirWatch Account representative will work directly with the customer and downtime will occur during an agreed upon maintenance window as best possible.

SaaS Access Policies

AirWatch Global Support Teams are responsible for supporting and assisting customers for all SaaS environments, including:

- Application Support Engineers – Engineers with access to all SaaS environments for troubleshooting purposes
- Database Support Engineers – Engineers with access to AirWatch Application Databases for troubleshooting purposes
- VMware AirWatch SaaS Operations Engineers – Engineers with access to all SaaS environments and limited read only access to AirWatch Application Databases for troubleshooting purposes