CDN Integration with Workspace ONE UEM

VMware Workspace ONE UEM 1909

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

CDN Integration with Workspace ONE UEM

1

A Content Delivery Network (CDN) is a highly distributed platform of servers that responds directly to the end-user requests for the web content. Content delivery network acts as an intermediary between the AirWatch servers and the end-user devices to mitigate the challenges of delivering the content over the Internet. Workspace ONE UEM powered by AirWatch SaaS environments are integrated with Akamai's CDN network and the on-premises customer can take advantage of this functionality by obtaining Akamai's CDN capabilities.

Read through the following sections to learn more about setting up integration between Akamai CDN and Workspace ONE UEM powered by AirWatch.

As an on-premises customer you must first establish the relationship with the CDN provider for hosting. Once this environment is available, you can then proceed to integrate with Workspace ONE UEM. Integrating Workspace ONE UEM with a CDN provider lets end users in different regions download the internal applications from the CDN server closest to them, as opposed to an internal file server that is located remotely.

Benefits of Integrating Workspace ONE UEM with CDN

- Increased download speeds for geographically distributed end users.
- Reduced load for Workspace ONE UEM servers.

Prerequisites for Integrating Workspace ONE UEM with CDN

- Account with the Akamai CDN provider.
- CDN Configuration Tool installer file. To download the installer, go to CDN Configuration Tool.

This chapter includes the following topics:

Workspace ONE UEM and Akamai Integration

The Workspace ONE UEM and Akamai Integration Workflow diagram highlights the communication and interaction between Workspace ONE UEM and Akamai. Workspace ONE UEM and Akamai Integration currently does not support whitelisting of Akamai Edge Server IP Address. That is, if your end-user devices are a part of a network that allows connections to only servers whose IP addresses are whitelisted, then the integration cannot be implemented.

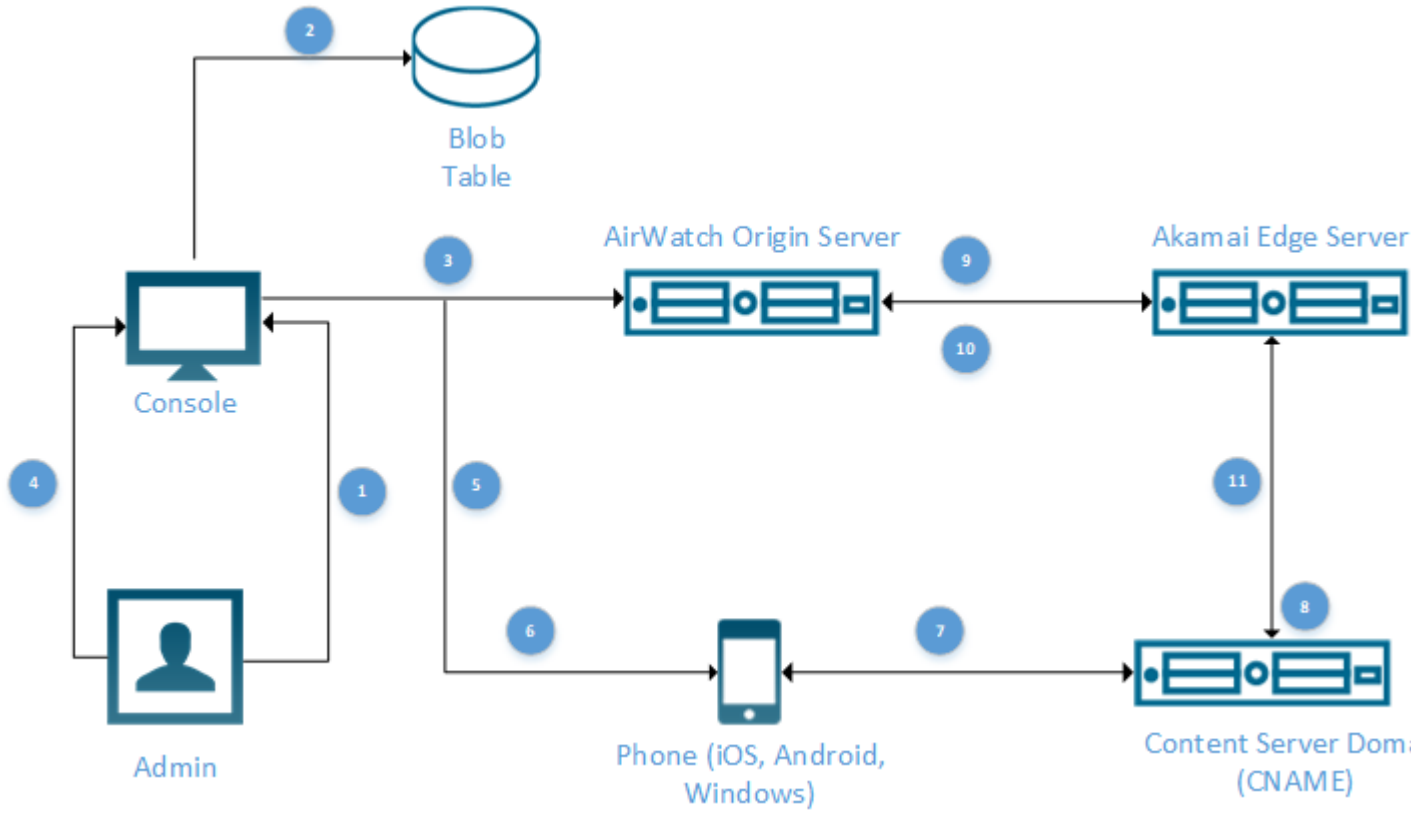
Workspace ONE UEM and Akamai Integration Workflow Components

AirWatch Origin Server: The AirWatch Origin Server is the file server that is configured for storage of all files to be cached within the Akamai CDN on a pull model.

Content Domain Server : The Content Domain Server is the domain mapping to the configured Akamai Edge Server using the CNAME **DNS plus *.edgekey.net**.

Akamai Edge Server: The Akamai Edge Server is responsible for caching and distributing files based on the geographic location. The server also authenticates the resources that end users try to access. If the connection to the CDN provider fails, then the content is instead pushed from the AirWatch Device Services server, as it might be if CDN integration was not configured.

Akamai Integration Workflow Diagram



Workflow Number	Description
1	Admin uploads apps to the Workspace ONE UEM console.
2	Add the application to the AirWatch Database or the File Storage Server.
3	Copy the application files using the configured UNC path and credentials.
4	Publish the application to the end-user devices.
5	Generate the token URL for the application using HMACSHA256.
6	Send the generated content download URL to the device.
7	Request content from the content server that points to the Akamai Edge server.
8	Forward the request to the edge server with the valid token for expiration.
9	Verify if the content is available in cache. Pull the content from the Origin Server if the content is not in the cache or if the content has changed.
10	If Edge is in the IP whitelist, request for the file is processed. If Edge IP is not in the whitelist, then request for 401/403 is processed.
11	Stream the content to the devices if the token is valid.

Configure Akamai to Integrate with Workspace ONE UEM

To integrate Workspace ONE UEM With Akamai CDN, you might have to first set up Akamai for use in a production environment.

To learn more about configuring Akamai integration, see Akamai product documentation at https://www.akamai.com.

To configure Akamai to integrate with Workspace ONE UEM, complete the following settings:

1 At the time of configuration, select **AirWatch** as your client name.

2 After you set up properties that control Akamai's edge server traffic, add behaviors to the property as per your requirements. Currently, Workspace ONE UEM requires you to configure the following two behaviors:

   a **Edge Server Identification**: Include a known cookie value that can be verified at the origin server before serving requests back to the edge server.

Setting	Description
	AW-AUTH-KEY.
Cookie Value	Use a hash generator to create the hash key generated value. CDN server uses the key to connect to the origin server. Retain a copy of the hash key for use while installing the origin server.
Cookie Domain	Enter the Origin Server URL. For example, enter origin.acme.com.

b **Advanced Override**: Use the Advanced Override option to specify the parameter to use for tokens that are passed to the URL. Also, specify the expected shared-secret/salt that is used to generate the HMAC token when validating the file requests to the edge server. Advanced Override is only available by request from Akamai Support, and requires an extra fee. This feature is required to enter the Token key in the Console configuration.

Configure Origin Server

The origin server is the file server configured for storage of all files to be cached with your CDN provider on a pull model.

To set up the Origin Server, complete the following steps:

1 Install the Web Server Role (IIS). he Internet. It is possible to set up the DNS to do routing internally to the proper servers as necessary. For storage, multiply the average file size by the average number of files, then multiply by two to avoid full disk issues that prevent the caching of files.

Enable the following features:

a Request Filtering

b Window Authentication

c URL Authorization

d IP and Domain Restrictions

2 Install URL Rewrite IIS from the Microsoft website.

3 Add the following extensions to **Default Website MIME Types**.

Extension	Content Type
.app	application/vnd.android.package-archive
.appx	application/vns.ms-appx
.appxbundle	application/octet-stream
.ipa	application/octet-stream
.lic	text/plain (For BSP)
.msi*	.msi* application/octet-stream
.msp	application/octet-stream
.mst	application/octet-stream
.pkg	application/octet-stream
.xap*	application/x-silverlight-app
.xbap*	application/x-ms-xbap
.ppkg	application/octet-stream
.dmg	application/octet-stream
.mpkg	application/octet-stream

Extension	Content Type
.plist	text/xml
.apk	application/vnd.android.package-archive

Note MIME Types already exist in Windows 2012 R2.

4 Navigate to the CDN content storage location.

5 Create a shared folder named **CDN**. The folder that is configured for the web server must be mapped to a file with both read, write permission that is available to the Workspace ONE UEM console and Device Services.

6 In the **CDN** folder, create a file named **monitor.txt**. Enter some random text into the document so that you can validate the connection at a later stage. For more information, see Validate Workspace ONE UEM Integration with CDN .

7 Set up the user account credentials for accessing the CDN using a UNC/SMB path. The UNC/SMB path is used during the configuration of the UEM console. The user name and password are used for connecting to the **UNC/SMB** folder and are also entered into the UEM console.

8 Configure the security setup for accessing the folder from the IIS website.

   a Add the application pool user account to the **CDN**folder of the shared drive.

   b Add the following usernts:

      1 ISUR (All but Full control)

      2 IIS_IUSRS (All but Full control)

      3 NetworkService (Full Control)

      4 UNC/SMB Service Account (All but Full control)

9 Under **Application Pools**, right-click **DefaultAppPool** and select **Advanced Settings**. Set the App Pool Identity to **NetworkService**.

10 Right-click **Default Website**, select **Manage Website**, and select **Advanced Settings**.

11 Change the **Physical Path** to the configured drive for the CDN content.

12 After Akamai is configured, you can set up the request filtering for the cookie that is used for authentication of the URL.

   a Obtain the CDN Configuration Tool installer.

   b Run the CDN installation and enter the secret key (SHA256 Hash Key) that is configured with your Akamai account for Edge Server Identification. For more information on setting up Edge Server Identification, see Configure Akamai to Integrate with Workspace ONE UEM .

13 Make a note of the **Network Path** for the UEM console configuration.

Configure Akamai in Workspace ONE UEM Console

You can configure Akamai CDN in Workspace ONE UEM console . The values that you enter in this page can be retrieved by logging in to your CDN provider portal and locating the values. If you are an on-premises customer who requires additional assistance, contact Workspace ONE UEM Support.

Before You Begin:

- For more information, see Configure Origin Server.
- **Current Setting** – Select whether to **Inherit** or **Override** the displayed settings. Inherit means use the settings of the parent OG if the current organization group, Override enables the settings for editing so you can modify the current OG settings directly.

Complete the Akamai configuration in the UEM console:

1 In the UEM console, ensure that you are in the Global OG.

2 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > CDN**.

3 Complete the Akamai configuration settings:

Setting	Description
Enabled	Select **Enabled** to route all the application downloads through the CDN for all the devices that are the managed at the current organization group. Select **Disabled** to route all the application downloads through Workspace ONE UEM server.
Directory	Enter the server name and the directory. The Directory name is the **Network Path** that is used while configuring the origin server. See Configure Origin Server.
User name	Enter a dedicated Service Account user name that is placed on the Origin Server side.
Password	Enter the dedicated Service Account password that is placed on the Origin Server side.
Content Server	Enter the DNS of the CNAME that is as per the data center (for example, CDN.acme.com).
Token Parameter	For Akamai, it is the token as per the Advanced Override.
Salt Value	Enter the token that your CDN provides. For Akamai, it is done by enabling the Advanced Override code.
Destination	Enter the destination name of the CDN.

Child Permission – Select the available behavior of child organization groups that exist below the currently selected organization group. Inherit only means child OGs are only allowed to inherit these settings. Override only means they override the settings, and Inherit or Override means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

Test Connection – Select this button to test the connection between Workspace ONE UEM and Akamai. A status message is displayed to confirm the connection.

Disable CDN System Settings for the Child Organization Group

If the child organization group has devices with IP whitelisting and restricts the application downloads to be routed through the CDN, you can disable the CDN routing. To disable CDN System Settings for the Child Organization Group, navigate to the child organization, select **Override**, and disable **Allow App downloads through CDN**. u choose to override the settings, you can only disable **Allow App downloads through CDN**. However, the system restricts you from editing the **Child Permission**.

Validate Workspace ONE UEM Integration with CDN

You can validate Workspace ONE UEM integration with CDN.

Complete the following steps to validate Workspace ONE UEM integration with CDN:

1 In a web browser, navigate to your CDN DNS. For example, CDN.acme.com/monitor.txt), which results in an error. The reason is because the connection to the Origin server from the CDN requires authentication.

2 In a web browser, navigate to your Origin DNS. For example, origin.acme.com/monitor.txt), which succeeds. Accessing the origin server directly only works for the **monitor.txt** file, which is used to validate the connection.