CDN Integration with Workspace ONE UEM

VMware Workspace ONE UEM 2109

vmware

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

https://docs.vmware.com/

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

Contents

Workspace ONE UEM and Akamai Integration Workflow 1

Workspace ONE UEM powered by AirWatch SaaS environments are integrated with Akamai's Download Delivery CDN network and the on-premises customer can take advantage of this functionality by obtaining Akamai's CDN capabilities. 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.

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

As an on-premises customer, you must first establish a 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 allows the 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.

Hardware, Software, Network, and Generic Requirements

Software Requirements:

1 CDN (Content Delivery Networks) installer. CDN installer can be found here.

2 IIS (Internet Information Services) Server Manager 6 and above.

Hardware Requirements:

1 Windows Server 2012 and above.

2 Minimum of 4 CPU cores and 8 GB RAM.

Network Requirements:

1 Origin Server cannot be on the Device Service or the Console server box.

2 Origin Server must be set up in the same domain as the Console Server box.

3 Port 443 and 80 must be used only for CDN. Ensure that the Origin server is reachable on these ports.

4 Origin Server needs to have a public DNS (Domain Name Servers) so that the Akamai edge server can access the box.

5 Origin Server is possible to set up the DNS to do the routing internally to the proper servers, as necessary.

Note For the Origin Server 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.

Generic Requirements:

1 You must have the Akamai Download Delivery solution account.

2 You must create a secret key (SHA256 Hash Key). this will be used while running the CDN installer and for the Akamai account for Edge Server Identification.

Workspace ONE UEM and Akamai Integration Architecture

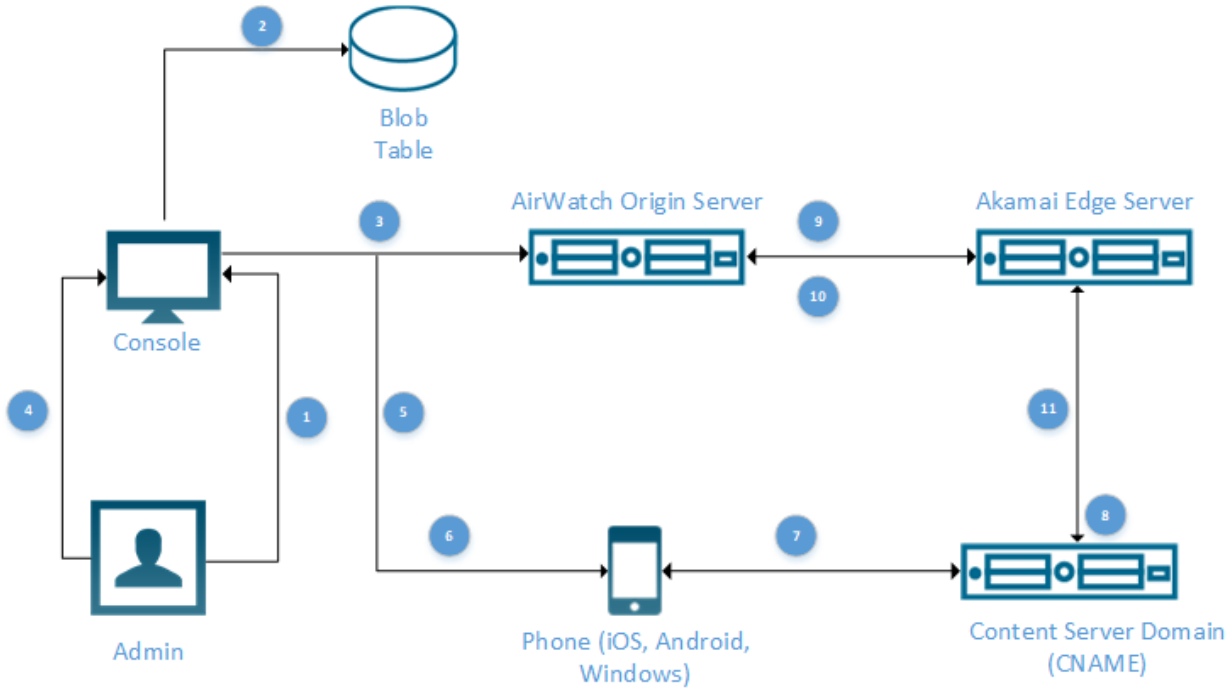
The Workspace ONE UEM and Akamai Integration Workflow highlight the communication and interaction between Workspace ONE UEM and Akamai. Workspace ONE UEM and Akamai Integration support allowlisting of Akamai Edge Server IP Address. That is, if your end-user devices are a part of a network that allows connections to only servers whose IP addresses are allowedlist, then the integration can be implemented with variation in Akamai configuration.

Workspace ONE UEM and Akamai Integration Workflow Components

Workspace ONE Origin Server: The Workspace ONE Origin Server is the file server that is configured for storage of all files that will then be cached within the Akamai CDN.

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

Akamai Integration Workflow Diagram



Workflow Number	Description
1	Admin uploads apps to the Workspace ONE UEM console.
2	Adds the application to the AirWatch Database or the File Storage Server.
3	Copies the application files using the configured UNC path and credentials.
4	Publish the application to the end-user devices.
5	Generate the app download URL containing HMAC Token, which is valid for 24hrs, using the salt/ encryption key with SHA256 algorithm.
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 HMAC token received from the device.
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. The communication is authorized by the edge identification key passed in the request header from Edge server.
10	If Edge is in the IP allowlist, the request for the file is processed. If Edge IP is not in the allowlist, then the request for 401/403 is processed.
11	Stream the content to the devices if the token is valid.

This chapter includes the following topics:

Setting up Akamai CDN to integrate with Workspace ONE UEM

Akamai CDN must be configured to communicate with the Workspace ONE origin server and your end-user devices. You can set up various download properties in the Akamai portal as per your business needs by working with your Akamai representative. To learn more about configuring Akamai integration, see Akamai product documentation at https://www.akamai.com

Configure your Origin Server to integrate Workspace ONE UEM with Akamai CDN

The origin server is a physical location from which content is retrieved. It is required in all configurations that retrieve content from an origin. You can set up the Origin Server to integrate Akamai CDN with Workspace ONE UEM.

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

1 Install IIS Server Manager.

2 Once the IIS Server Manager is installed, enable the following server roles under **Web Server (IIS)** > **Web Server** > **Security**.

- Request Filtering
- Window Authentication
- URL Authorization
- IP and Domain Restrictions
- Basic Authentication
- Client Certificate Mapping Authentication
- IIS Client Certificate Mapping Authentication

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

Extension	Content type
.act	application/octet-stream
.afx	application/octet-stream
.agt	application/octet-stream
.apf	application/vnd.android.package-archive
.apk	application/vnd.android.package-archive
.appx	application/vns.ms-appx
.appxbundle	application/octet-stream
.ast	application/octet-stream

.bat	text/plain
.bin	application/octet-stream
.ccp	application/octet-stream
.cfg	application/octet-stream
.cgd	application/octet-stream
.chn	application/octet-stream
.chx	application/octet-stream
.cix	application/octet-stream
.cni	application/octet-stream
.cnm	application/octet-stream
.crd	application/x-mscardfile
.crt	application/x-x509-ca-cert
.dat	application/octet-stream
.db	application/octet-stream
.demconfig	application/octet-stream
.der	application/x-x509-ca-cert
.dmg	application/octet-stream
.dmp	application/octet-stream
.ezp	application/octet-stream
.flg	application/octet-stream
.gif	image/gif
.gnf	application/octet-stream
.Gnu	application/octet-stream
.gst	application/octet-stream
.hsh	application/octet-stream
.inf	application/x-inf
.inx	application/octet-stream
.ipa	application/octet-stream
.json	application/json
.lic	text/plain

.lje	application/octet-stream
.loc	application/octet-stream
.log	text/plain
.lup	application/octet-stream
.map	application/octet-stream
.mpkg	application/octet-stream
.mscript	application/octet-stream
.msi	application/octet-stream
.msp	application/octet-stream
.mst	application/octet-stream
.nix	application/octet-stream
.nms	application/octet-stream
.nst	audio/x-mod
.p12	application/x-pkcs12
.pem	application/x-pem-file
.pfx	application/x-pkcs12
.pho	application/octet-stream
.pkg	application/octet-stream
.plist	text/xml
.png	image/png
.pnm	image/x-portable-anymap
.ppkg	application/octet-stream
.properties	application/octet-stream
.ps1	text/plain
.qd	application/octet-stream
.rgn	application/octet-stream
.set	application/set
.six	application/octet-stream
.snm	application/octet-stream
.sst	application/vnd.ms-pki.certstore

.syn	application/octet-stream
.thn	application/octet-stream
.tmp	application/octet-stream
.tmz	application/octet-stream
.trp	application/octet-stream
.txt	text/plain
.typ	application/octet-stream
.typ2	application/octet-stream
.upl	application/octet-stream
.xap	application/x-silverlight-app
.xbap	application/x-ms-xbap
.xml	text/xml
.yix	application/octet-stream
.ynm	application/octet-stream
.zip	application/zip
.zst	application/zstd

Note

- MIME Types exist in Windows 2012 R2.
- If any of the file type is missing, you can add the extension per your requirement.

4 Create a shared folder named **CDN**. The folder that is configured for the web server must be mapped to a file with both read and write permissions that is available to the Workspace ONE UEM console and the Device Services. As a best practise, create a separate partition E drive from local disk drive and then create the CDN folder under the newly created partition E drive. For example, you can create `E:\CDN`

5 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.

Note

- File extension checkbox is cleared.
- Make sure the filename does not contain the file extension. That is, ensure your file is not created as **`monitor.txt.txt`**.

6 On IIS, right-click **Default Website**. Select **Manage Website**, and select **Advanced Settings**. Change the **Physical Path** to the configured drive for the CDN content. For example, `E:\CDN` .

7 Set up the **Physical Path Credential** to the **service account** or the **local user**.

8 Ensure you have access to a service account or local 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 username and password are used for connecting to the `UNC/SMB` folder and are also entered into the UEM console.

9 Set up the **Physical Path Credentials Logon** to clear text.

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

- Add the application pool user account to the CDN folder of the shared drive.
- Add the following users:
  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).

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

12 Make sure you have installed Application Request Routing (ARR) on IIS. If you have not installed ARR, see Application Request Routing.

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

a Obtain the CDN Configuration Tool installer.

b Run the CDN installation

1. Click **Next** on the **Welcome to Install Shield Wizard**.
2. Enter the SHA256 Authentication key.

   Note The SHA256 key is generated using any string of your choice. You can use any SH256 string generator tool at your disposal. The key used in this step is later used in Akamai account configuration for identifying Edge Servers.

3. Click **Install**.

14 CDN installer must create the URL rewrite. If URL rewrite is not created, perform the following steps:

a Install Application Request Routing https://www.iis.net/downloads/microsoft/application-request-routing. The URL rewrite shows up only after you install the Application Request Routing.

b Run the CDN installer again to install URL Rewrite.

15 Navigate to the CDN folder `E:\CDN`. Right-click the CDN folder and go to **Sharing**. Make a note of the **Network Path** for the UEM console configuration.

16 Perform the following validation:

- Two rules are created for URL Rewrite.
  - `IgnoreMonitorFile` - Ignores the monitor.txt file that is created under the CDN folder.
  - `AkamaiSharedKeyCookie` – Allows Akamai to use the SHA256 key to authenticate into this server.
- Navigate to `localhost/monitor.txt` on the web browser. A random text is entered in the monitor.txt file.

Setting up your Origin server for High Availability and Disaster Recovery

You can configure the Origin Server behind a load balancer to have high availability. You can have the Active-Active mode or Active-Passive mode, but it would be based on the network requirement for your environment. Session persistence is not required as long as the File Optimization feature is enabled on Akamai portal. With the File Optimization, the requests are broken down to ranges eliminating the need for persistence.

This section lists the various configuration that is needed as part of a highly available system. The setup is the same as the single Origin server with a few minor differences. In single Origin Server setup, the Physical Path is set to a CDN folder created in one of the drives of the server. In the high availability setup, the Physical Path is set to the Network Directory. It can be part of any file sharing system if the right permissions are assigned to the user accessing the Network Directory. The service account needs to be the owner of the whole network folder.

When you point to the network file system, the web configuration file is no longer in the local machine. Instead, it resides in the destination file-sharing system. The web configuration file stores the IIS configuration. On the remaining origin servers, go through the setup with the following exceptions:

1 Point the default website to the network path of the file sharecluster instead of the drive on the server.

2 Skip running the CDN installer tool for the URL rewrite setup. This step is only needed on one of the origin servers.

Configure Akamai CDN to integrate with Workspace ONE UEM

Akamai CDN must be configured to communicate with Workspace ONE UEM origin server and your end-user devices. You can set up various download properties in the Akamai portal as per your business needs by working with your Akamai representative. To learn more about configuring Akamai integration, see Akamai product documentation at https://www.akamai.com. However, the following communication properties are required for the distribution from Workspace ONE UEM to work:

1 Create **Property**> **Download delivery** (used by Workspace ONE UEM SaaS) and provide a name to the property. As a best practice, consider using **`Workspace ONE environment`** or the **`datacenter name`**.

2 Add the property hostname. The property hostname is used for the configuration in the Workspace ONE UEM console in the next section.

3 A certificate is required to bind with the hostname created. The certificate can be Akamai issued certificate or a third-party party issued certificate. For more support, reach out to Akamai.

4 After you set up the 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:

- **Origin Server**: Include the origin server hostname that is publicly available.

Settings	Description
Origin Type	Your Origin
Origin Server Hostname	This is the public-facing hostname for the origin server
Forward Host Header	Origin Hostname
Cache key hostname	Origin Hostname
HTTP Port	80
HTTPS Port	443

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

Settings	Description
Cookie Name	AW-AUTH-KEY.
Cookie Value	Use the SHA256 Authentication Key generated in step 9 of the previous, origin server setup section to create the hash key generated value. CDN server uses the key to connect to the origin server.
Cookie Domain	Enter the Origin Server URL. For example, enter **`origin.acme.com`**. The address must match the origin server hostname and is case sensitive.

- **Auth Token 2.0 verification**: 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 the Akamai Support and may require additional fees. You need this feature to enter the Token key in the console configuration.

Settings	Description
Token Location	Query String
Token Name	This is the same token parameter in Workspace ONE UEM console under **Groups & Settings** > **All Settings** > **System** > **Enterprise Integration** > **CDN** > **Akamai**. This is case sensitive.
Encryption Key	Click the button on the right side to generate the key. This key will be used in the configuring Workspace ONE UEM console. Encryption equals **`Salt Value`**.
Action	Verify and Deny

Configure Akamai CDN in the Workspace ONE UEM Console

You can configure Akamai CDN in Workspace ONE UEM console. During the configuration, the values that you enter in the configuration page is retrieved by logging in to your CDN provider portal and locating the values. Before You Begin, ensure you finished your origin server setup and Akamai portal configuration.

Complete the Akamai configuration in the Workspace ONE UEM console:

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

Note CDN configuration can be set up only at **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 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. **Note** If your origin server has the high-avaiblity setup, enter the path to the file share cluster here.
User name	Enter a Service Account username that has read/write permissions on the origin server directory.
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).

Setting	Description
Token Parameter	For Akamai, it is the token as per the Advanced Override.
Salt Value	Enter the token that your CDN provides. This is Encryption key in Akamai settings. For Akamai, it is done by enabling Advanced Override code.
Destination	Enter the destination name of the CDN.

4 After you save the configuration, click **Test Connection** to validate CDN setup end-to-end based on your settings. The validation uploads a dummy file to the origin server, checks if file saves and tries to download it from Akamai using the CDN download URL.

Validate Your Workspace ONE UEM Integration with Akamai CDN

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

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

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

Akamai CDN Servers Per Data Center

	CDN URL
US02	https://cdnus02.awmdm.com/
US02 IP	https://cdnus02ip.awmdm.com
US04	https://cdnus04.awmdm.com
US04 IP	https://cdnus04ip.awmdm.com
US04UAT	https://cdnus04uat.awmdm.com
US06	https://cdnus06.awfed.com
US08	https://cdnus08.awmdm.com
US08 IP	https://cdnus08ip.awmdm.com
US09	https://cdnus09.awmdm.com
US09 IP	https://cdnus09ip.awmdm.com
DE01	https://cdnde01.awmdm.com
DE01 IP	https://cdnde01ip.awmdm.com
AU01	https://cdnau01.awmdm.com

AU01 IP	https://cdnau01ip.awmdm.com
JP02	https://cdnjp02.awmdm.com
JP02 IP	https://cdnjp02ip.awmdm.com
UK01	https://cdnuk01.awmdm.com
UK01 IP	https://cdnuk01ip.awmdm.com
IN02	https://cdnin02.awmdm.com
IN02 IP	https://cdnin02ip.awmdm.com
CA04	https://cdnca04.awmdm.com
CA01	https://cdnca01.awmdm.com
CA01 IP	https://cdnca01ip.awmdm.com
SG01	https://cdnsg01.awmdm.com
SG01 IP	https://cdnsg01ip.awmdm.com
HK02	https://cdnhk02.awmdm.com
HK02 IP	https://cdnhk02ip.awmdm.com
US00	https://cdnus00.awpreprod.com