



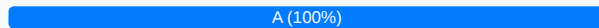
- Expert Verified, Online, **Free**.

As a Workspace ONE administrator, you have been tasked with creating a custom visualization for management that shows device statistics, trust network threats, and application adoption metrics in a single view.
Which feature of Workspace ONE can be used?

- A. Workspace ONE Intelligence Dashboards
- B. Workspace ONE Access Application View
- C. Workspace ONE Intelligence Automations
- D. Workspace ONE UEM Device List View

Suggested Answer: A

Reference:

<https://techzone.vmware.com/resource/workspace-one-intelligence-architecture#workspace-one-uem>*Community vote distribution*

🗨️ 👤 **adeliarona** 2 years, 4 months ago

Selected Answer: A

agree with A

upvoted 1 times

🗨️ 👤 **svx** 2 years, 9 months ago

Selected Answer: A

A is correct -

Just Passed the Exam - All Questions and Answers Valid. Good Luck!

upvoted 1 times

🗨️ 👤 **astroid** 3 years, 2 months ago

A is Correct

upvoted 1 times

Which Workspace ONE UEM feature can assist in sending event log information to a Security Information and Event Management (SIEM) tool?

- A. Syslog Integration
- B. Relay Server Integration
- C. Certificate Authority Integration
- D. File Storage Integration

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **adeliarona** 2 years, 4 months ago

Selected Answer: A

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_Logging/GUID-AWT-SYSLOGOVERVIEW.html
upvoted 1 times

🗨️ 👤 **ColdCut** 2 years, 11 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2102/UEM_Logging/GUID-AWT-SYSLOGOVERVIEW.html#:~:text=Workspace%20ONE%20UEM%20integrates%20with,%2C%20Device%20events%2C%20or%20both.
upvoted 1 times


🗨️ 👤 **astroid** 3 years, 2 months ago

Option A it is
upvoted 1 times



Which two steps would an administrator complete to enable auto-discovery for their Workspace ONE UEM environment? (Choose two.)

- A. Enter the email domain when installing the AirWatch Cloud Connector.
- B. Verify the domain by accepting the link in the email that registered auto-discovery.
- C. Register email domain within Workspace ONE UEM.
- D. Enter the email domain when establishing directory services.
- E. Email auto-discovery@workspaceone.com with the domain the administrator wants to register.

Suggested Answer: BC

  **Kosmas** 3 years ago

BC is the correct answer
upvoted 1 times

  **astroid** 3 years, 2 months ago

B & C are correct
upvoted 2 times

What two features of Hub Services can be enabled without enabling Workspace ONE Access and having the authentication mode set to Workspace ONE UEM?
(Choose two.)

- A. enable SSO for applications
- B. enable People Search
- C. notifications for iOS and Android
- D. Hub Virtual Assistant Chatbot
- E. Hub Catalog layout


Suggested Answer: AB

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-012E7722-FC83-4EF5-8ADD-2457E29720FE.html

Community vote distribution

 CE (100%)

 **willpena** 1 year, 6 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-BEFA3A94-357A-4B9C-AEC6-5B62D2BF3AEE.html

It's C&E


upvoted 1 times

 **crimsonghost** 3 years, 1 month ago

Selected Answer: CE

It's CE

upvoted 1 times

 **vinodhg** 3 years, 2 months ago

Selected Answer: CE

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-012E7722-FC83-4EF5-8ADD-2457E29720FE.html

upvoted 1 times

 **Maksor** 3 years, 2 months ago

Selected Answer: CE

CE is the correct answer

upvoted 1 times

 **Mightybob** 3 years, 3 months ago

Selected Answer: CE

The options detailed in the link below clearly show these as the only options:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-012E7722-FC83-4EF5-8ADD-2457E29720FE.html


And says "...Hub Services can operate with Workspace ONE UEM alone providing a subset of Hub Services features - Catalog for UEM apps, Notification, Self-Service Support, and Custom Tab."

upvoted 3 times

 **JLF_VMW** 3 years, 5 months ago

I agree, CE for me.

upvoted 3 times

 **FoxTMo** 3 years, 6 months ago

CE - The link referenced takes you to a page that even shows these two are the only options.

upvoted 2 times

Where is Hub Services component co-located?

- A. Workspace ONE Intelligence
- B. Workspace ONE Access
- C. Workspace ONE Airlift
- D. Workspace ONE UEM

Suggested Answer: B

🗨️ 👤 **MYJ** 1 year, 8 months ago

Selected Answer: B
upvoted 2 times

🗨️ 👤 **astroid** 3 years, 2 months ago

B is correct
upvoted 3 times

🗨️ 👤 **Xryake** 3 years, 5 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-012E7722-FC83-4EF5-8ADD-2457E29720FE.html
upvoted 1 times

🗨️ 👤 **JLF_VMW** 3 years, 4 months ago

You are correct, B is de answer.
upvoted 1 times

🗨️ 👤 **JLF_VMW** 3 years, 5 months ago

For me is D, WS1 UEM because is where you active the service.
After that, work with WS1 Access
upvoted 1 times

🗨️ 👤 **DanielGP** 3 years, 2 months ago

"The Workspace ONE Hub Services component is co-located with Workspace ONE Access and is dependent on Workspace ONE Access for shared services."

Source: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-1D3018CE-8716-4960-B16B-696D1F2B7E50.html#:~:text=The%20Workspace%20ONE%20Hub%20Services%20component%20is%20co-located,the%20Workspace%20ONE%20Intelligent%20Hub%20app%20on%20devices.

upvoted 4 times

Which two Workspace ONE UEM core components are required for all on-premises environments? (Choose two.)

- A. Device Services
- B. AirWatch Cloud Connector
- C. Unified Access Gateway
- D. Secure Email Gateway
- E. Console Services

Suggested Answer: AB

Reference:

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#scalability>

Community vote distribution

AE (68%)

AB (32%)

 **Ikazimirs** Highly Voted 2 years, 11 months ago

Selected Answer: AE

Just completed the troubleshoot course, and its clearly documented in course material you can run on prem without a cloud connector but the DS and CN server will need to be able to access the local domain (for example in PS integration you can do it without ACC). You will not be able to run the service without a console server
upvoted 7 times

 **ColdCut** 2 years, 11 months ago

Good Job!

upvoted 1 times

 **pablitvs** Most Recent 1 year, 5 months ago

Selected Answer: AE

In a Workspace ONE UEM (Unified Endpoint Management) on-premises environment, the two core components that are typically required for all on-premises environments are:

A. Device Services: Device Services is a core component that manages the device lifecycle, profiles, and policies in Workspace ONE UEM.

E. Console Services: Console Services is the component responsible for hosting the Workspace ONE UEM administrative console, which allows administrators to configure and manage the Workspace ONE UEM environment.

While components like the AirWatch Cloud Connector (B), Unified Access Gateway (C), and Secure Email Gateway (D) can be important for specific use cases or configurations, they are not always required for all on-premises environments. The specific components needed may vary based on your organization's requirements and setup.

upvoted 1 times

 **Joaquino** 1 year, 10 months ago

Selected Answer: AE

A&E, ACC is only required if you want communication with your Back-End, which is not mandatory.

upvoted 1 times

 **Skysurfer69** 2 years, 2 months ago

Selected Answer: AE

Only AE is correct in this scenario

upvoted 1 times

 **salei** 2 years, 6 months ago

Selected Answer: AE

Workspace ONE UEM consists of many services that come together to provide a single cohesive application. The term "core component" refers to the service or software required for the platform to function at its most basic ability:

- Workspace ONE UEM console server
- Workspace ONE UEM device services
- Workspace ONE UEM database
- AirWatch Cloud Messaging (AWCM) service

The AirWatch Cloud Messaging (AWCM) service works with AirWatch Cloud Connector to integrate Workspace ONE UEM with your back-end enterprise systems. BUT it's not mandatory
upvoted 2 times

🗨️ 👤 **AllenHuang** 2 years, 8 months ago

Selected Answer: AE

Admin Console & Device Service
upvoted 1 times

🗨️ 👤 **UEM_Kenobi** 2 years, 10 months ago

It seems to be: A & E

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#on-premises-architecture>

Syncing with internal resources such as Active Directory or a Certificate Authority can be achieved directly from the core components (Device Services and Admin Console) or using an AirWatch Cloud Connector.

The implementation is separated into the three main components:

- Workspace ONE UEM Admin Console
- Workspace ONE UEM Device Services
- AirWatch Cloud Connector

upvoted 1 times

🗨️ 👤 **ColdCut** 2 years, 11 months ago

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#on-premises-architecture>

upvoted 1 times

🗨️ 👤 **FumerLaMoquette** 3 years ago

Selected Answer: AE

Cloud connector is not necessary if all accounts are local to WS1 UEM.
upvoted 1 times

🗨️ 👤 **LaVoz** 3 years ago

Selected Answer: AB

On-Premises Architecture:

The implementation is separated into the three main components:

Workspace ONE UEM Admin Console
Workspace ONE UEM Device Services
AirWatch Cloud Connector

Reference: <https://techzone.vmware.com/resource/workspace-one-uem-architecture#on-premises-architecture>

upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 1 month ago

Selected Answer: AB

AWCC is required for on-prem.

The implementation is separated into the three main components:

Workspace ONE UEM Admin Console
Workspace ONE UEM Device Services
AirWatch Cloud Connector

The AirWatch Cloud Messaging Service can be installed as part of the Workspace ONE UEM Device Services server, and the API Endpoint is installed as part of the Admin Console server. Depending on the scale of the environment, these can also be deployed on separate servers.

In addition to the components already described for this cloud-based architecture, there are additional components required for an on-premises deployment.

upvoted 2 times

🗨️ 👤 **Ikazimirs** 2 years, 11 months ago

you my friend confusing ACC with AWCM - different components.

upvoted 3 times

🗨️ 👤 **Joaquinoo** 1 year, 10 months ago

Agree, AWCM != ACC

upvoted 1 times

🗨️ 👤 **crimsonghost** 3 years, 1 month ago

It's A&E. ACC is not required on-prem

upvoted 1 times

🗨️ 👤 **astroid** 3 years, 2 months ago

Selected Answer: AE

AE is the correct answer, the rest are optional components

upvoted 1 times

🗨️ 👤 **PetterV** 3 years, 2 months ago

I would say A+E. We don't use ACC in our on-prem environment

upvoted 1 times

🗨️ 👤 **Mightybob** 3 years, 3 months ago

Selected Answer: AB

Per reference architecture, the diagram for on-prem architecture shows that Devices Services and AirWatch Cloud Connector are required:

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#on-premises-architecture>

upvoted 4 times

🗨️ 👤 **Joaquinoo** 1 year, 10 months ago

It is only required if you want communication with your Back-End, which is not mandatory.

upvoted 1 times

🗨️ 👤 **nfu21593** 3 years, 3 months ago

Selected Answer: AE

CC is no requirement

upvoted 2 times

An administrator would like to track these details for all Windows desktops managed by Workspace ONE UEM:

- ⇒ driver details for a mouse driver
- ⇒ warranty information for OS
- ⇒ registry value of internal apps

Which Workspace ONE UEM utility can the administrator use?

- A. Create LGPO and assign to Windows devices.
- B. Create sensors and assign to Windows devices.
- C. Create an OEM update profile and assign to Windows devices.
- D. Create Application Control profile and assign to Windows devices.

Suggested Answer: B

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskSensors.html

🗨️ 👤 **MYJ** 1 year, 8 months ago

Selected Answer: B

upvoted 1 times

🗨️ 👤 **astroid** 3 years, 2 months ago

Sensors can execute a PowerShell command and capture these details

upvoted 3 times

When using Workspace ONE 20.x and higher, which three ways can an administrator using UEM automatically move devices into specified organization groups?

(Choose three.)

- A. user group mappings
- B. device type mappings
- C. location based mappings
- D. IP-based mappings
- E. device ownership mappings

Suggested Answer: ACE

Community vote distribution

ADE (100%)

🗨️ **adeliarona** 2 years, 4 months ago

Selected Answer: ADE

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2203/UEM_Managing_Devices/GUID-DeviceAssignments.html

upvoted 3 times

🗨️ **AnnPrz** 2 years, 10 months ago

Does anyone know the right answer for this question?

upvoted 1 times

🗨️ **Rams4u** 3 years ago

Selected Answer: ADE

A D E-check link - https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/UEM_Managing_Devices/GUID-AWT-ENABLEDEVICEASSIGNMENTS.html

upvoted 4 times

🗨️ **ATRider** 3 years, 1 month ago

A colleague of mine is an expert with long years of experience in WS1 in large environments. He says: ACE is right here.

upvoted 1 times

🗨️ **astroid** 3 years, 2 months ago

With my experience, I can say that there is only one type of mapping that is User Group mapping to move devices automatically to an OG. So question should be wrong

upvoted 1 times

🗨️ **unknownexpert** 3 years, 2 months ago

You can have device assignment based in User Groups, Device Custom Attribute (I think it includes location) and IP Range. For the same Group ID you can only select on type.

upvoted 1 times

🗨️ **ATRider** 3 years, 2 months ago

what is now correct here???

upvoted 1 times

🗨️ **exode** 3 years, 3 months ago

Device Assignments enable you to move devices across organization groups (OG) and user names based on the network Internet protocol (IP) address range or custom attributes. I

upvoted 1 times



🗨️ **Mightybob** 3 years, 3 months ago

Selected Answer: ADE

According to documentation (link below) you can do Device Assignments, User Group Assignments and IP Range Assignments.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/WS1_UEM_Managing_Devices.pdf

upvoted 2 times

  **astroid** 3 years, 2 months ago

Assignments are different from OG mapping

upvoted 1 times

What product from Workspace ONE needs to be enabled to provide administrators a flexible method for alerting and informing end-users?

- A. AirWatch Cloud Connector
- B. Workspace ONE Intelligence
- C. Workspace ONE Hub Services
- D. VMware Tunnel

Suggested Answer: C



Reference:

https://techzone.vmware.com/automating-notifications-workspace-one-operational-tutorial#_1267872

  **MYJ** 1 year, 8 months ago

Correct Answer : C

upvoted 1 times

  **astroid** 3 years, 2 months ago

Answer CORrect. C

upvoted 2 times

What component of the Hub Services can be integrated with Physical Access Control Systems to allow the Workspace ONE Intelligent app on mobile devices to act as digital badge?

- A. Hub Employee Self-service
- B. Hub Passport
- C. Hub Catalog
- D. Hub Access

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **crimsonghost** 3 years, 1 month ago

B is correct but it was never released under this name. As Mightybob said - it's called Digital Badge.

upvoted 3 times

🗨️ **Maksor** 3 years, 2 months ago

B is correct. <https://en.prnasia.com/releases/apac/vmware-enriches-digital-workspace-solutions-to-meet-evolving-business-continuity-needs-276551.shtml>

upvoted 2 times

🗨️ **Mightybob** 3 years, 3 months ago

Selected Answer: B

I can't find any official documentation that calls it a "Hub Passport", only this article from an external source -

<https://www.zdnet.com/article/vmware-updates-workspace-one-with-capabilities-for-new-hires/#:~:text=The%20Intelligent%20Hub%20will%20offer,employee's%20identity%20and%20access%20allowances.>

The proper name is called a "Digital Badge Service" per this official documentation - https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-662F8F84-F589-469F-A99C-53CC8B6EFB60.html

Be mindful of this name just in case.

upvoted 3 times

🗨️ **SShamz** 3 years, 4 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-662F8F84-F589-469F-A99C-53CC8B6EFB60.html

upvoted 3 times

Which administrative console is used to change to an organization logo (branding) in the Intelligent Hub Catalog?

- A. Workspace ONE Access
- B. Workspace ONE Hub Services
- C. Workspace ONE
- D. Workspace ONE UEM

Suggested Answer: B

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-DD632B89-7457-4764-B14F-48AAFAAC8113.html

Community vote distribution

B (67%)

D (33%)

🗨️ 👤 **ColdCut** 2 years, 11 months ago

Correct Answer B as per - You can use your organization's logo in the Workspace ONE Intelligent Hub app and portal pages instead of the default Workspace ONE logo. You can customize the product name that displays in the web browser tab, and change accent, font and background colors.

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-DD632B89-7457-4764-B14F-48AAFAAC8113.html

upvoted 1 times

🗨️ 👤 **dominic1koch** 2 years, 12 months ago

Selected Answer: B

I can verify B as correct answer: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-DD632B89-7457-4764-B14F-48AAFAAC8113.html

upvoted 2 times

🗨️ 👤 **FumerLaMoquette** 3 years ago

I mean.. This question could be more specific. Hub services exists within WS1 access..

upvoted 2 times

🗨️ 👤 **DanielGP** 3 years, 1 month ago

Seems to be "HUB SERVICES", as per this official VMware link:

Customizing the Workspace ONE Intelligent Hub App Layout

24/05/2021

You can modify the Branding settings in Hub Services to add your company LOGO and change the colors that display in the Workspace ONE Intelligent Hub app or Hub portal in the browser.

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-3F44B63B-E429-4965-9298-97CAC885D0CB.html

upvoted 1 times

🗨️ 👤 **nfu21593** 3 years, 3 months ago

Selected Answer: D

It speaking about catalog so logo can be change form W1 UEM

upvoted 1 times

🗨️ 👤 **Maksor** 3 years, 2 months ago

That's for branding the admin console, not the Hub catalog. Also see Question #25

upvoted 1 times

Which is true about Workspace ONE compatibility when deploying content across different device types?


- A. Content cannot be distributed to iOS devices.
- B. Content cannot be distributed by Workspace ONE.
- C. Content can be distributed to devices types including iOS, Android, Windows, and MacOS.
- D. Content can be distributed to devices types including iOS, Android, and Windows.

Suggested Answer: D

Community vote distribution

D (50%)

C (50%)

 **pablitvs** 1 year, 5 months ago

Selected Answer: C

The statement that is true about Workspace ONE compatibility when deploying content across different device types is:

C. Content can be distributed to device types, including iOS, Android, Windows, and MacOS.


Workspace ONE supports content distribution to a wide range of device types, including iOS, Android, Windows, and MacOS. This allows organizations to manage and distribute content to a diverse set of devices in their environment.

upvoted 1 times

 **jmnugent** 1 year, 7 months ago

This seems like a bit of a misleading (or poorly constructed) question. Especially because the word "content" is lowercase in the Question,.. but in the Answer-choices it's Capitalized (are they referring specifically to the "Content" app ?.. of just to the general concept of "pushing content" to various OSes ?.. because you absolutely can push content (PDF's, etc) down to OSes like macOS,. I've done it. But that doesn't seem to be what they are referring to here. Especially frustrating as others have mentioned that the "Content" app comes and goes (availability) on various OSes. ;\

upvoted 1 times

 **Trainee** 1 year, 10 months ago

The correct answer is not listed... it should be iOS an Android only.

In earlier days there was a windows content application but that one is stopt because most customers always use the "explorer.exe" application to see there files on windows devices.

So in this case the correct answer should be iOS, Android AND windows. (Answer D)

<https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2212/MCM/GUID-WorkspaceONEContent.html>

upvoted 2 times

 **Joaquino** 1 year, 10 months ago

Selected Answer: C

I think it's the C. In the Official WS1_MCM_Doc.pdf says it clearly:

Platform Requirements:

iOS 7.2 and later

Android 3.2 and later

Windows 7

Windows 8

Windows 10

10.9 Mavericks and later (Mavericks = OS X = MacOS)

(<https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/MCM/GUID-AWT-CL-PLAT-MATRIX.html>)

upvoted 1 times

 **AllenHuang** 2 years, 8 months ago

In the New version

Only Android & iOS

<https://docs.vmware.com/tw/VMware-Workspace-ONE-UEM/services/MCM/GUID-WorkspaceONEContent.html>

upvoted 3 times

🗨️ 👤 **Kal_dd** 2 years, 9 months ago

Selected Answer: C

I think it is C

upvoted 1 times

🗨️ 👤 **Oishikee** 2 years, 9 months ago

Should be C. I work in VMware and when the hub app is installed in the macOS device it can deploy apps, profiles etc. to it.

upvoted 1 times

🗨️ 👤 **LaVoz** 3 years ago

Selected Answer: D

Only iOS, Android and Win 10 platforms are supported:

<https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/MCM/GUID-AWT-CL-PLAT-MATRIX.html>

upvoted 3 times

🗨️ 👤 **kaow** 3 years, 1 month ago

Selected Answer: C

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/macOS_Platform/GUID-AWT-APPSSCLSYNCFORMAC.html

upvoted 1 times

🗨️ 👤 **exode** 3 years, 3 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/macOS_Platform/GUID-AWT-APPSSCLSYNCFORMAC.html

upvoted 1 times

🗨️ 👤 **JLF_VMW** 3 years, 3 months ago

I think is C, because you can install HUB in MacOS and share content:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-28049087-F7AC-47D1-BD72-199A1D94B0ED.html#:~:text=The%20Intelligent%20Hub-

[based%20enrollment%20process%20secures%20a%20connection,management%20and%20access%20to%20the%20relevant%20device](https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-28049087-F7AC-47D1-BD72-199A1D94B0ED.html#:~:text=The%20Intelligent%20Hub-based%20enrollment%20process%20secures%20a%20connection,management%20and%20access%20to%20the%20relevant%20device)

upvoted 2 times

🗨️ 👤 **JLF_VMW** 3 years, 3 months ago

more information: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_Assist/GUID-AWT-RMV4-SUPPORTEDPLATFORMS.html

[SUPPORTEDPLATFORMS.html](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_Assist/GUID-AWT-RMV4-SUPPORTEDPLATFORMS.html)

upvoted 1 times

🗨️ 👤 **Mightybob** 3 years, 3 months ago

Selected Answer: D

Content has been available for iPhone and Android for some time and is now available for Windows

(https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskAppOverview.html)

[uemWindeskAppOverview.html](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskAppOverview.html))

NOTE: It is not available for MacOS

upvoted 1 times

A Workspace ONE UEM administrator is migrating collections, applications, and policies from SCCM to Workspace ONE. When using AirLift, which three of the following must the administrator allow AirLift to access on the ConfigMgr server? (Choose three.)

- A. Port 443 or specified TLS port if Secure Connection is configured
- B. WinRM port (typically 5985)
- C. Port 3268 or the specified Global Catalog port
- D. Port 389 for Active Directory
- E. Interactive Login Permissions

Suggested Answer: ABE


Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_AirLift_Configuration.pdf

(7)

Community vote distribution

ABE (100%)

 **LaVoz** Highly Voted 3 years ago

Selected Answer: ABE

You must allow Workspace ONE AirLift the following access to the ConfigMgr server:

- WinRM port (typically 5985)
- Port 443 or the specified TLS port if Secure Connection is configured.
- Interactive Log in Permissions - Ensure that AD user account settings or security policy settings do not deny local log in.

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2111/AirLift_Configuration/GUID-AWT-INTRO-AIRLIFT.html

upvoted 5 times

Which protocol does Workspace ONE use to communicate with third party Identity Providers?

- A. SAML
- B. Kerberos
- C. RADIUS
- D. OAuth

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ **MYJ** 1 year, 8 months ago

Selected Answer: A
upvoted 1 times

🗨️ **Kal_dd** 2 years, 9 months ago

Selected Answer: A

A is correct
upvoted 2 times

🗨️ **ColdCut** 2 years, 11 months ago

Add and Configure a SAML Third-Party Identity Provider Instance in Workspace ONE Access
upvoted 2 times

🗨️ **ColdCut** 2 years, 11 months ago

You can configure a third-party identity provider to manage user identity and authentication for single sign-on to Workspace ONE.
upvoted 1 times

🗨️ **LaVoz** 3 years ago

Selected Answer: A

"Workspace ONE Access supports identity providers that are compatible with the SAML 2.0 and OpenID Connect 1.0 protocols".

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/21.08/ws1_access_authentication_cloud/GUID-0A7E40E1-9D7C-4B9B-8A0F-EB17D6889BC5.html

upvoted 3 times


Which three Workspace ONE Edge Services are included in Unified Access Gateway? (Choose three.)

- A. AirWatch Cloud Connector
- B. Content Gateway
- C. Secure Email Gateway
- D. Workspace ONE Intelligence Connector
- E. VMware Tunnel

Suggested Answer: BCE

Community vote distribution

BCE (100%)

 **pablitvs** 1 year, 5 months ago

Selected Answer: BCE

Workspace ONE Unified Access Gateway (UAG) includes the following three Workspace ONE Edge Services:

B. Content Gateway: Content Gateway provides secure access to content repositories and enables features like content filtering and DLP (Data Loss Prevention).

C. Secure Email Gateway: Secure Email Gateway is responsible for securing email communication on mobile devices, ensuring that emails are encrypted and protected.

E. VMware Tunnel: VMware Tunnel provides secure access to internal resources and applications behind the corporate firewall. It establishes a secure tunnel for mobile devices to access these resources without exposing them to the public internet.

The AirWatch Cloud Connector (A) and Workspace ONE Intelligence Connector (D) are separate components and not included within the Unified Access Gateway. They serve different purposes within the Workspace ONE ecosystem.

upvoted 1 times

 **ColdCut** 2 years, 11 months ago

BCE - <https://docs.vmware.com/en/Unified-Access-Gateway/index.html>

VMware Tunnel

Tunnel is a modern VPN replacement providing full device and per application modes to enable remote access to any type of user. Unified Access Gateway appliance serves as the on-premises option for Zero Trust Network Access (ZTNA) leveraging the Workspace ONE Tunnel app. VMware's ZTNA solution is also available as a hosted SaaS service as part of VMware's Secure Access Service Edge.

Additional use cases for Workspace ONE

Unified Access Gateway serves as a secure black box for deploying other Workspace ONE components including Content Gateway and Secure Email Gateway. These gateways can be used in conjunction with the Workspace ONE Content app, Workspace ONE Boxer app, and other native and third party mail clients.

upvoted 2 times


An administrator is tasked with determining the root cause for a recent outage where devices were not able to authenticate. An investigation revealed a single AirWatch Cloud Connector (ACC) server that had a disk error which caused it to be completely unresponsive. Which VMware resiliency recommendation would have prevented this outage?

- A. High Availability
- B. Disaster Recovery
- C. Cloud Hosted ACC
- D. Restart ACC

Suggested Answer: A

Community vote distribution

A (100%)

 **pablitvs** 1 year, 5 months ago


Selected Answer: A

he VMware resiliency recommendation that would have prevented the outage described is:

A. High Availability (HA)


High Availability ensures that there are redundant components or servers in place to take over in case of a failure. In this scenario, having a High Availability setup for the AirWatch Cloud Connector (ACC) server would have prevented the outage caused by the single ACC server's disk error. If one server fails, the other can take over, ensuring continuity of service.

upvoted 1 times

 **MYJ** 1 year, 8 months ago

Correct Answer: A

upvoted 1 times

 **ColdCut** 2 years, 11 months ago

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/it-outcomes-hari-datasheet.pdf>

upvoted 3 times

Which of the following authentication methods is needed to be enabled/configured for an administrator to leverage Day Zero Onboarding?

- A. Token Auth Adapter
- B. Workspace ONE UEM External Access Token
- C. FIDO2
- D. Certificate-based authentication
- E. Verify (Intelligent Hub)

Suggested Answer: A

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-1DB5A54E-2F72-4629-97C8-F456BBDB7F5E.html

Community vote distributionA (100%)

🗨️ **salei** 2 years, 7 months ago

Answer is A - see this link [https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-7F95F539-47AE-489E-8DE3-80346B834C68.html?](https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-7F95F539-47AE-489E-8DE3-80346B834C68.html?hWord=N4IghgNiBclAoCcCmAHMyAEARMBPDAWkkggPYYDyAdgEYnoAmAlpQOYbMYDqJCA1gM5oAxkgoA5AKIYAgkJH9+IAL5A)

[hWord=N4IghgNiBclAoCcCmAHMyAEARMBPDAWkkggPYYDyAdgEYnoAmAlpQOYbMYDqJCA1gM5oAxkgoA5AKIYAgkJH9+IAL5A](https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-7F95F539-47AE-489E-8DE3-80346B834C68.html?hWord=N4IghgNiBclAoCcCmAHMyAEARMBPDAWkkggPYYDyAdgEYnoAmAlpQOYbMYDqJCA1gM5oAxkgoA5AKIYAgkJH9+IAL5A)

upvoted 2 times

🗨️ **Mightybob** 3 years, 3 months ago

Selected Answer: A

Article below confirms that Token Auth Adapter needs to be configured for this feature to occur:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-51B88155-B9AA-4B78-A6E6-7F59D74F9CED.html

upvoted 1 times

🗨️ **SShamz** 3 years, 4 months ago



https://docs.vmware.com/en/VMware-Workspace-ONE/services/VMware_Workspace_ONEHub_onboarding_pre-hires/GUID-51B88155-B9AA-4B78-A6E6-7F59D74F9CED.html

upvoted 1 times

When configuring a Certificate Authority in Workspace ONE, which three protocols are supported? (Choose three.)

- A. ADCS
- B. SCEP
- C. EST
- D. PKI
- E. CMP



Suggested Answer: *ABD*

  **ColdCut** 2 years, 11 months ago

public key infrastructure (PKI)



https://en.wikipedia.org/wiki/Public_key_infrastructure

upvoted 1 times

  **ColdCut** 2 years, 11 months ago


SCEP - https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/Certificate_Authority_Integrations/GUID-EF7C4D44-9480-4AD1-91E3-EA4F02448F5A.html

upvoted 1 times

  **ColdCut** 2 years, 11 months ago



https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2105/Certificate_Authority_Integrations/GUID-Certificate_Authority_Integrations_intro.html

upvoted 1 times

  **unknownexpert** 3 years, 2 months ago

UEM Console confirms ADCS, SCEP and PKI options under Configurations > Certificate Authorities.

upvoted 3 times

  **SShamz** 3 years, 4 months ago


https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2005/WS1_Certificate_Authority_Integrations.pdf

upvoted 1 times

Which feature of Workspace ONE UEM can be configured to allow reports to run on a schedule and have them delivered to a subset of administrators?

- A. Windows Scheduled Tasks
- B. Report Subscriptions
- C. Timed Report Execution
- D. SQL Server Reporting Services

Suggested Answer: *B*

 **SShamz** 3 years, 4 months ago

<https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2102/ReportsAnalytics/GUID-AWT-SUBSCRIBENEWREPORTS.html>
upvoted 2 times

A customer has decided to use VMware Workspace ONE as their primary SAAS solution for endpoint management. The customer's security team requires all infrastructure to support High Availability (HA).

Which two components of Workspace ONE will need to be maintained by the customer? (Choose two.)

- A. AirWatch Cloud Connector
- B. Workspace ONE Database
- C. Console Services Servers
- D. Unified Access Gateway
- E. Device Services Server

Suggested Answer: AD

Community vote distribution

AD (88%)

13%

🗳️ 👤 **Joaquino** 1 year, 10 months ago

Selected Answer: AD

For SaaS deployments, only ACC and UAG need to be maintained.

upvoted 2 times

🗳️ 👤 **AllenHuang** 2 years, 8 months ago

Selected Answer: AD

SaaS, So Only ACC & UAG

upvoted 3 times

🗳️ 👤 **ColdCut** 2 years, 9 months ago

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#on-premises-architecture>

The implementation is separated into the three main components:

Workspace ONE UEM Admin Console

Workspace ONE UEM Device Services

AirWatch Cloud Connector

upvoted 1 times

🗳️ 👤 **Joaquino** 1 year, 10 months ago

That is On-Premises UEM architecture. The question asks for SaaS. So A&D are the correct answers.

upvoted 1 times

🗳️ 👤 **svx** 2 years, 9 months ago

Selected Answer: AD

SaaS deployments would have the console, device and database services in the "cloud" - A company will still have to maintain the Connector and Unified Access Gateway services to reach the companies own network.

upvoted 2 times

🗳️ 👤 **MightyMo** 2 years, 11 months ago

Selected Answer: AE

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#scalability>

upvoted 1 times

🗳️ 👤 **Joaquino** 1 year, 10 months ago

On a SaaS deployment, Device Services are cloud based.

upvoted 1 times

A company has BYOD iOS devices and would like to give them access to internal sites in VMware Web without requiring full device management.

Which VMware best practice configuration is needed to enable this?

- A. Configure Tunnel for VMware Tunnel in the SDK settings.
- B. Configure Tunnel for VMware Tunnel Proxy in the SDK settings.
- C. Configure a VPN Profile for VMware Tunnel.
- D. Configure a VPN Profile for VMware Tunnel Proxy.

Suggested Answer: C

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_UEM_Managing_Devices.pdf

Community vote distribution

A (100%)

🗉 👤 **Trainee** 1 year, 10 months ago

Answer A,

Keyword in this one is IOS devices.

"Stand-alone" tunnel is (for now) not for IOS devices.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Tunnel_Linux/GUID-AWT-TUNNEL-KEYCONCEPTS.html#setting-up-a-load-balancer-for-backend-tunnel-servers-7

upvoted 2 times

🗉 👤 **MRC26** 1 year, 11 months ago

Selected Answer: A

VMware Web cannot be based on classic profiles nor on the VMware Tunnel application which needs system control. You therefore go through the WS1 SDK to push the configuration directly into the application without going through the system. And it's not the B because the Proxy Tunnel is end of life.

Answer from my former

upvoted 3 times

🗉 👤 **ColdCut** 2 years, 11 months ago

Enrollment Considerations, BYOD

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/UEM_Managing_Devices/GUID-AWT-ENROLLMENT-CONSIDERATIONSBYOD.html

upvoted 1 times

🗉 👤 **ColdCut** 2 years, 11 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2011/macOS_Platform/GUID-AWT-MACPROFILEVPN.html

upvoted 2 times

Which three are features of the Workspace ONE Content Gateway service? (Choose three.)

- A. Encrypted communications using SSL/TLS.
- B. Secure access to internal repositories.
- C. Provides health status on external repositories.
- D. Support for most corporate file servers.
- E. Provides email notification for Exchange mail.


Suggested Answer: BCD

Reference:

https://techzone.vmware.com/configuring-edge-services-vmware-unified-access-gateway-vmware-workspace-one-operational-tutorial#_984128


Community vote distribution

ABD (100%)

 **JLF_VMW** Highly Voted 3 years, 5 months ago

Is ABD, from manual of WS1 course.

upvoted 6 times

 **Skysurfer69** Most Recent 2 years, 2 months ago

Selected Answer: ABD

ABD That is all

upvoted 1 times

 **born2winu2** 2 years, 8 months ago

ABC

The Content Gateway provides a secure and effective method for end users to access internal repositories. Using Content Gateway with VMware Workspace ONE® Content (formerly Content Locker) provides levels of access to your corporate content. End users can remotely access their documentation, financial documents, board books, and more, directly from content repositories or internal file shares. As files are added or updated within your existing content repository, the changes immediately display in Workspace ONE Content. Users are granted access to their approved files and folders based on the existing access control lists defined in your internal repository.

Workspace ONE Content not only provides access to on-premises content repositories, but also enables users to have access to multiple cloud repositories.

upvoted 1 times

 **AllenHuang** 2 years, 8 months ago

Selected Answer: ABD

Can't check external repositories

upvoted 2 times

 **svx** 2 years, 9 months ago

Selected Answer: ABD

A, B, D -

Why in the world would email or health have anything to do with this? :)

upvoted 2 times

 **ColdCut** 2 years, 11 months ago

ABD -

A. Encrypted communications using SSL/TLS. Most Voted

The default port for Content Gateway is 443 as TLS Port Sharing is enabled by default on Unified Access Gateway. When TLS Port Sharing is disabled, Content Gateway listens on port 10443.

These ports are secured with a public third-party SSL certificate, which includes the subject name of the server host name.

B. Secure access to internal repositories. Most Voted

The Content Gateway provides a secure and effective method for end users to access internal repositories.

D. Support for most corporate file servers. Most Voted

Workspace ONE UEM supports integration with various corporate file servers. The syncing method support and requirement of the Content Gateway component vary by repository type.

upvoted 1 times

  **Rams4u** 3 years ago

Selected Answer: ABD

ABD is right

upvoted 1 times

  **FumerLaMoquette** 3 years ago

Selected Answer: ABD

CG has nothing to do with exchange. And it doesn't provide health status of remote repo.

upvoted 1 times

  **Mightybob** 3 years, 3 months ago

Selected Answer: ABD

Using the link below, I think ABD are more appropriate answers.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_Content_Gateway.pdf

upvoted 4 times

Which is used to authenticate and encrypt traffic from individual applications on compliant devices to internal resources?

- A. VMware Tunnel
- B. Device Compliance
- C. Workspace ONE Intelligence
- D. Email Notification Service

Suggested Answer: A

Community vote distribution

A (100%)

🗉 👤 **UEM_Kenobi** 2 years, 8 months ago

<https://techzone.vmware.com/resource/workspace-one-uem-architecture#vmware-tunnel>

VMware Tunnel leverages unique certificates deployed from Workspace ONE UEM to authenticate and encrypt traffic from the mobile device to resources on the internal network.

upvoted 1 times

🗉 👤 **thiagobassan** 2 years, 8 months ago

Selected Answer: A

simples

upvoted 1 times

🗉 👤 **ColdCut** 2 years, 11 months ago

VMware Tunnel

[https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2008/Tunnel_Windows/GUID-AWT-WINDOWS-INTRO.html?](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2008/Tunnel_Windows/GUID-AWT-WINDOWS-INTRO.html?hWord=N4IghgNiBclGoFkDuYBOBTABAFQK4Dt90oBfIA)

[hWord=N4IghgNiBclGoFkDuYBOBTABAFQK4Dt90oBfIA](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2008/Tunnel_Windows/GUID-AWT-WINDOWS-INTRO.html?hWord=N4IghgNiBclGoFkDuYBOBTABAFQK4Dt90oBfIA)

upvoted 1 times

🗉 👤 **Rams4u** 3 years ago

Selected Answer: A

A is right

upvoted 1 times

Which three options are supported by Workspace ONE Access? (Choose three.)

- A. Configuring Per-App VPN.
- B. Configuring conditional access.
- C. Configuring network segmentation.
- D. Configuring Mobile SSO.
- E. Configuring unified application catalog.
- F. Configuring encryption.

Suggested Answer: BDE

Community vote distribution

BDE (100%)


 **Mightybob** Highly Voted 3 years, 3 months ago

Selected Answer: BDE

Confirming BDE as per this document:

https://techzone.vmware.com/quick-start-tutorial-series-cloud-based-vmware-workspace-one#_1016928

upvoted 7 times

 **ColdCut** Most Recent 2 years, 11 months ago

<https://techzone.vmware.com/search?q=%20Workspace%20ONE%20conditional%20Access>

upvoted 1 times

 **cvs** 3 years ago

Thank you Mightybob.

upvoted 2 times

An administrator would like to customize their admin consoles default branding to include the company logo and reflect the company's text color and background.

How would the administrator accomplish this task?

- A. Navigate to UEM Console, All Settings, System, Branding. Click Branding and edit the settings in the Branding page as appropriate.
- B. Navigate to the Configurations tab on the console. Click Branding. Edit the settings in the Branding page as appropriate.
- C. Navigate to the Hub Service console Home page. Click Branding. Edit the settings in the Branding page as appropriate.
- D. Navigate to UEM Console, All Settings, Hub Services. Click Branding and edit the settings in the Branding page as appropriate.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **pablitvs** 1 year, 5 months ago

Selected Answer: A

To customize the admin console's default branding in Workspace ONE, the administrator should:

A. Navigate to UEM Console, All Settings, System, Branding. Click Branding and edit the settings in the Branding page as appropriate.

This is the correct path and location for customizing the branding of the admin console in Workspace ONE. It allows you to customize the company logo, text color, and background to reflect your organization's branding preferences.

upvoted 1 times

🗨️ 👤 **Joaquino** 1 year, 10 months ago

Selected Answer: A

A is right. Checked on the Admin Console itself. C&D of course not, "Admin Console's Branding" nothing to do with Hub Services.

upvoted 2 times

Which two statements are true about Content Gateway and Tunnel on Unified Access Gateway? (Choose two.)

- A. Both can be configured with the same hostname on port 8443.
- B. Both can be configured with the same hostname on different ports.
- C. Both can be configured on port 8443 with different hostnames.
- D. Both can be configured with the same hostname on port 443.
- E. Both can be configured on port 443 with different hostnames.

Suggested Answer: BE

Community vote distribution

BE (100%)

🗨️ 👤 **pablitvs** 1 year, 5 months ago

Selected Answer: BE

The two statements that are true about Content Gateway and Tunnel on Unified Access Gateway are:

B. Both can be configured with the same hostname on different ports: You can configure Content Gateway and Tunnel to use the same hostname but on different ports. For example, you can have Content Gateway on port 8443 and Tunnel on a different port like 8444 or any other port you choose.

E. Both can be configured on port 443 with different hostnames: You can configure Content Gateway and Tunnel on the same port (e.g., port 443) but with different hostnames. This allows you to use different hostnames to access Content Gateway and Tunnel services while they share the same port.

These configurations provide flexibility in how you set up and access Content Gateway and Tunnel on Unified Access Gateway, allowing you to tailor them to your specific requirements.

upvoted 1 times

🗨️ 👤 **unknownexpert** 3 years, 2 months ago

Content Gateway only supports inbound 443 because that is what iOS or Android use. The tunnel is more flexible.

<https://techzone.vmware.com/configuring-edge-services-vmware-unified-access-gateway-vmware-workspace-one-operational-tutorial#architecture>

upvoted 1 times

🗨️ 👤 **unknownexpert** 3 years, 2 months ago

Answers BE are correct

upvoted 1 times

🗨️ 👤 **nfu21593** 3 years, 3 months ago

- B on 100%

But both service we can configure on 443 and 8443

upvoted 2 times

Refer to the Exhibit.

iOS Add Compliance Policy

1 Rules 2 Actions 3 Assignment 4 Summary

Immediately perform the following actions Mark as Not Compliant

Notify Send Push Notification to Device Default template

After 1 Days Perform the following actions: Repeat Mark as Not Compliant

Notify Send Email to User CC: admin@company.com | Default template

After 1 Days Perform the following actions: Repeat Mark as Not Compliant

Application Block/Remove All Managed Apps

+ Add Escalation

An administrator has set up an iOS compliance policy for unwanted apps.

Which of the following is the expected behavior when Workspace ONE UEM receives the app sample indicating the presence of the unwanted app?

- A. After 1 day, end user will receive the push notification.
- B. The concerned device will be marked as Non-compliant immediately.
- C. The concerned device will be unenrolled.
- D. After 2 days, all managed apps will be blocked/removed from the concerned device.

Suggested Answer: D

 **lelouch1977** 2 years, 9 months ago

D - 1 + 1 = 2

upvoted 2 times

Which two configuration steps must be performed when managing iOS devices? (Choose two.)

- A. Obtain an Apple Server Certificate.
- B. Obtain an Apple ID.
- C. Obtain an APNS certificate.
- D. Obtain an Apple Developer ID.
- E. Obtain an iCloud Account.

Suggested Answer: BC

 **jmnugent** 1 year, 7 months ago

This is kind of a poorly worded question. I can see what they are implying here (that, at a minimum, you need an AppleID in order to register an APNS token), so I understand, but the wording of the question is a bit tricky and misleading.


upvoted 1 times

 **ColdCut** 2 years, 11 months ago

APNS certificate

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_ConsoleBasics/GUID-AWT-APNSCERTS.html

upvoted 2 times

 **ColdCut** 2 years, 11 months ago

BC-

[https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2102/UEM_Installation/GUID-AWT-NEXTSTEPSKEY.html?](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2102/UEM_Installation/GUID-AWT-NEXTSTEPSKEY.html?hWord=N4IghgNiBcIIIAcEQKYAICSAREBfIA)

[hWord=N4IghgNiBcIIIAcEQKYAICSAREBfIA](https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2102/UEM_Installation/GUID-AWT-NEXTSTEPSKEY.html?hWord=N4IghgNiBcIIIAcEQKYAICSAREBfIA)

-You may also need to create a corporate Apple ID.

-If your deployment includes Apple iOS devices, you must generate an APNs certificate on behalf of your company.

upvoted 2 times



Which of the following is a prerequisite to deploy VMware Unified Access Gateway OVF?

- A. VMware vSphere
- B. VMware Workstation
- C. VMware Fusion
- D. VMware Horizon

Suggested Answer: A

Reference:

<https://docs.vmware.com/en/Unified-Access-Gateway/3.5/com.vmware.uag-35-deploy-config.doc/GUID-13DCCA35-8620-4F4C-8FBC-6916396221AD.html>

  **MYJ** 1 year, 8 months ago

Correct Answer: A

upvoted 1 times

  **lelouch1977** 2 years, 9 months ago

A - need to have vSphere to deploy

upvoted 1 times

DRAG DROP -

Drag and drop the device operating system on the left into the box associated with its third party messaging solution.

Select and Place:

iOS

APNS

Android

WNS

Windows

FCM

Suggested Answer:	iOS	iOS	APNS
	Android	Windows	WNS
	Windows	Android	FCM

 **radekw1996** 1 year, 7 months ago

iOS - APNS (Apple Push Notification service)

Android - FCM (Firebase Cloud Messaging)

Windows - WNS (Windows Push Notification Services)

upvoted 1 times

Which three can be used to enforce conditional access in Workspace ONE? (Choose three.)

- A. device ownership type
- B. device enrollment method
- C. device platform
- D. application specific
- E. network range
- F. user-based role

Suggested Answer: ABC

Community vote distribution

CDE (63%)

CEF (38%)

🗳️ 👤 **JLF_VMW** Highly Voted 3 years, 5 months ago

Is CDE, <https://blogs.vmware.com/euc/2021/01/vmware-workspace-one-delivers-improved-multi-factor-authentication.html#:~:text=%20Workspace%20ONE%20can%20make%20conditional%20access%20decisions,access%3F%20Internal%20And%20page%20562%20of%20manual%20WS1>
And page 562 of manual WS1

upvoted 10 times

🗳️ 👤 **astroid** 3 years, 2 months ago

According to the above link it is CDEF

1. Who is the user? Contractor, executive, team manager, IT staff etc.
2. Where are they connecting from? Inside the corporate network or from home?
3. What device are they coming from? What OS, is it managed, unmanaged, etc.?
4. What app are they trying to access? Internal, external, high security, etc.?

upvoted 1 times

🗳️ 👤 **DanielGP** 3 years, 2 months ago

CDE is correct.

"13-36 Conditional Access

With Workspace ONE Access, you can enforce conditional access based on the network range, platform, and application-specific authentication criteria.

upvoted 1 times

🗳️ 👤 **Maksor** 3 years, 2 months ago

You are correct, it's CDE

upvoted 1 times

🗳️ 👤 **Skysurfer69** Most Recent 2 years, 2 months ago

Selected Answer: CDE

This question refers specifically to the options for conditional access in Workspace ONE Access in that case the correct answer is CDE

upvoted 2 times

🗳️ 👤 **salei** 2 years, 6 months ago

Selected Answer: CDE

2-39 Conditional Access

With Workspace ONE Access, you can enforce conditional access based on the network range, platform, and application-specific authentication criteria.

upvoted 1 times

🗳️ 👤 **Kal_dd** 2 years, 9 months ago

Selected Answer: CDE

As per vmware explanation

upvoted 1 times

🗳️ 👤 **MightyMo** 2 years, 11 months ago

Selected Answer: CDE

<https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-Access-deploymentguide/GUID-61066072-5A9D-4CDE-A58F-291FEF79C202.html>

upvoted 1 times

🗨️ 👤 **ColdCut** 2 years, 11 months ago

CEF Correct answer

C. device platform - device type

E. network range - network range

F. user-based role - user group

<https://www.youtube.com/watch?v=h5Xlu5K6Pes&t=71s>

The authentication policy you create determines which authentication method Workspace ONE Access implements, based on the network range, device type, and user group.

<https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-Access-deploymentguide/GUID-61066072-5A9D-4CDE-A58F-291FEF79C202.html>

upvoted 1 times

🗨️ 👤 **ColdCut** 2 years, 11 months ago

The authentication policy you create determines which authentication method Workspace ONE Access implements, based on the network range, device type, and user group.

upvoted 1 times

🗨️ 👤 **FumerLaMoquette** 3 years ago

Selected Answer: CEF

In Conditional access policies, you can only filter based on device type, user group, and network range. Then you apply this network policy to an application. So in my opinion, D is the odd one out (from CDEF).

upvoted 2 times

🗨️ 👤 **FumerLaMoquette** 3 years ago

Actually, I retract. I just noticed it says user based role. You cannot assign policies based on user role. User group, yes.

upvoted 2 times

🗨️ 👤 **LaVoz** 3 years ago

Selected Answer: CEF

<https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-Access-deploymentguide/GUID-61066072-5A9D-4CDE-A58F-291FEF79C202.html>

upvoted 1 times

🗨️ 👤 **LaVoz** 3 years ago

This is a tricky question, it could be CDE.

upvoted 1 times

A customer intends to implement Android device management in their environment.

Which three enrollment options would result in an end-user experience in which a dedicated container is created on the device for only business applications and contents? (Choose three.)

- A. Knox Container
- B. Device Enrollment Program (DEP)
- C. Work Managed Device
- D. Legacy enrolled
- E. Corporate Owned Personally Enabled (COPE)
- F. Work Profile

Suggested Answer: CEF

Community vote distribution

CEF (100%)

AllenHuang 2 years, 8 months ago

Selected Answer: CEF

I Agree CEF

upvoted 2 times

astroid 3 years, 2 months ago

A - Knox is for Samsung devices

B - DEP is for iOS devices

D - Legacy method adds all the managed applications in a container with a badge but this method is no more supported. So I will choose CEF.

upvoted 4 times

Mightybob 3 years, 3 months ago

Selected Answer: CEF

CEF are correct. Here is supporting documentation:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Android_Platform/GUID-AndroidEnrollmentEnrollmentConcept.html

upvoted 4 times

Which Security Assertion Markup Language (SAML) configuration item is a pre-requisite to creating a third party identity provider in Workspace ONE Access?

- A. SAML AuthN Request
- B. SAML Metadata
- C. SAML Assertion
- D. SAML AuthN Context

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **salei** 2 years, 6 months ago

Selected Answer: B

Add and Configure a SAML Third-Party Identity Provider Instance in Workspace ONE Access

When you add and configure new SAML identity provider instances for your Workspace ONE Access deployment, you can provide high availability, support additional user authentication methods, and add flexibility in the way you manage the user authentication process based on user IP address ranges.

Prerequisites

Complete the following tasks before adding the third-party identity provider instance.

Verify that the third-party instances are SAML 2.0 compliant and that the Workspace ONE Access service can reach the third-party instance.

Coordinate the integration with the third-party identity provider. Depending on the identity provider, you might need to configure both settings in unison.

Obtain the appropriate third-party metadata information to add when you configure the identity provider in the Workspace ONE Access console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

upvoted 1 times

An administrator is preparing to setup email management for Office 365 in UEM.
Which is VMware's recommended email deployment model for this scenario?

- A. VPN
- B. Proxy
- C. Indirect
- D. Direct

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ **MYJ** 1 year, 8 months ago

Selected Answer: D

answer is D

upvoted 1 times

🗨️ **Trainee** 1 year, 10 months ago

Based on M365, the answer is D (direct).

See: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2212/WS1_MEM_Guide/GUID-AWT-EMAILDEPLOYMENTTYPES.html

upvoted 2 times

🗨️ **Mightybob** 3 years, 3 months ago

I believe it to be D because according to the document on page 6 (linked below) Direct mode is for Office 365. Interestingly Proxy mode doesn't reference Office 365.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_MEM_Doc.pdf

upvoted 2 times

🗨️ **mafe** 3 years, 4 months ago

On page 13 of the WS1_MEM_Doc.pdf it says: "Use the Secure Email GatewaySecure Email Gateway (SEG) for all on-premises email

infrastructures with deployments of more than 100,000 devices. For deployments of less than 100,000 devices, using PowerShell is another option for your email management. Refer to the Secure Email Gateway vs. PowerShell Decision Matrix"

I agree with answer D, because most deployments will have less than 1000,000 devices.

upvoted 2 times

🗨️ **JLF_VMW** 3 years, 5 months ago

I have some doubts in this one, because can be D or B:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1_MEM_Doc.pdf

upvoted 1 times

Which type of design is a diagram that includes network zones, network components, server locations, and hardware recommendations?

- A. Physical
- B. Logical
- C. Theoretical
- D. Conceptual

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **MYJ** 1 year, 8 months ago

Selected Answer: A

Answer is: A

upvoted 1 times

🗨️ 👤 **Trainee** 1 year, 10 months ago

Answer is: A

Physical desig, see "part 3" of this link:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-workspace-one-design-handbook-technical-whitepaper.pdf>

upvoted 2 times

🗨️ 👤 **wikwi** 1 year, 9 months ago

Nice doc paul

upvoted 1 times

🗨️ 👤 **Joaquino** 1 year, 10 months ago

Selected Answer: A

Why? Just, why? I mean yeah, it has to do with WSONE, but it has to do with everything!

upvoted 2 times

Which three features within Hub Services can an administrator leverage when Workspace ONE Access is configured and integrated with Workspace ONE UEM?


(Choose three.)

- A. Email Notification
- B. Mobile Flows
- C. AirLift
- D. Virtual Assistant
- E. People

Suggested Answer: BCE

Community vote distribution

BDE (100%)

 **EUCGuy** 1 year, 4 months ago

Selected Answer: BDE

Email Notification available in UEM without the need to Access, While AirLift is useful for easing the transition to modern management of Windows 10 devices, it's not a Hub Services feature.

upvoted 1 times

 **Skysurfer69** 2 years, 2 months ago

Selected Answer: BDE

Airlift has nothing to do with Hub Services as far as configurations are concerned.

upvoted 2 times

 **ColdCut** 2 years, 11 months ago

BDE - https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-709B42DE-D3B8-476C-B751-4BB21110FD48.html

upvoted 2 times

 **tut123** 3 years, 3 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-012E7722-FC83-4EF5-8ADD-2457E29720FE.html

Its BDE

upvoted 3 times

 **lismi** 3 years, 5 months ago

Its B D and E

Under Hub Services / System Settings you can configure Mobile Flow URL

upvoted 4 times

 **Tom_tank** 3 years, 5 months ago

yes, B,D and E

When Workspace ONE Access is integrated with Workspace ONE UEM, you can create a fully digital workspace experiences for users with additional Hub Services features including the People service, Notifications through Workspace ONE mobile flows, and a Hub virtual assistant chatbot.

upvoted 1 times

 **JLF_VMW** 3 years, 5 months ago

Is ADE, Hub features:

• Hub Catalog • Notifications • People Search • Employee Self-Service support • Hub Virtual Assistant

upvoted 1 times

An administrator is concerned with data loss on Workspace ONE managed endpoints.


Which three configurations should be enabled to further improve the device security posture? (Choose three.)


- A. Configure compliance policies to monitor rooted and jailbroken devices.
- B. Configure compliance policies to monitor Roaming Cell Data Usage.
- C. Enable device-level data encryption.
- D. Enable SMTP integration.
- E. Enable verbose logging.
- F. Enable Data Loss Prevention policies.

Suggested Answer: ACF

Community vote distribution

ACF (100%)



 **Aldox3** 1 year, 7 months ago

Selected Answer: ACF

ACF - Correct Answer

upvoted 1 times

An organization has purchased a SaaS Workspace ONE solution and wants to implement these:

- ⇒ integration with back-end resources like Active Directory from Microsoft to sync users and groups
- ⇒ Kerberos authentication
- ⇒ integration with Virtual Desktops and Applications from services (Horizon 7, Horizon Cloud, or Citrix)
- ⇒ third party integration with RSA SecureID, RADIUS for authentication

Which Workspace ONE component is required?

- A. VMware AirWatch Cloud Connector
- B. VMware Workspace ONE Access Connector
- C. VMware Workspace ONE Assist
- D. VMware Workspace Unified Access Gateway

Suggested Answer: B

Community vote distribution

B (100%)

🗉 👤 **Mightybob** 3 years, 3 months ago

Selected Answer: B

Answer is B according to the link below:


https://docs.vmware.com/en/VMware-Workspace-ONE-Access/21.08/ws1_access_connector_install/GUID-271C47F6-856C-40F0-97AB-A8AD95025F9C.html

upvoted 3 times

A customer is managing only iOS devices using Workspace ONE. They would like to begin managing Android devices. What would be the first step an administrator needs to complete to begin managing Android Devices?

- A. Download and deploy Workspace ONE Unified Access Gateway.
- B. Complete Android EMM registration from Workspace One Console.
- C. Download and deploy Workspace ONE Access Connectors for Android devices.
- D. Configure a Workspace ONE AirLift Server-side Connector.

Suggested Answer: B

 **Trainee** 1 year, 10 months ago

Answer B

See: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2212/Android_Platform/GUID-AndroidRegistrationRegisterAndroidwithWorkspaceONE.html

upvoted 2 times

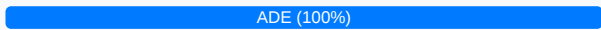
For federal clients, FIPS 140-2 and AES 256-bit encryption are applied to which three areas? (Choose three.)

- A. data in use
- B. data in flying
- C. data in pace
- D. data in rest
- E. data in transit

Suggested Answer: ADE

Community vote distribution

ADE (100%)



 **radekw1996** 1 year, 7 months ago

Selected Answer: ADE

<https://www.encryptionconsulting.com/education-center/what-is-fips/>
upvoted 1 times