Unified Access Gateway Security Guide

Unified Access Gateway 2207

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

Copyright © 2022 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About this book - Unified Access Gateway Security Guide 1

This document serves as a guide for Unified Access Gateway administrators to understand the security practices.

This chapter includes the following topics:

Introduction

Unified Access Gateway is a VMware hardened Linux based virtual security appliance designed to protect remote user access to end-user computing resources such as virtual desktops and applications. It is designed to operate with the following VMware solutions:

- Desktop and App Virtualization with Horizon 7/8 and Horizon Cloud
- Workspace ONE Access
- Workspace ONE UEM
  - Per-App Tunnel
  - Content Gateway
  - Secure Email Gateway

A virtual appliance is a pre-configured software solution that makes it possible to combine the hardened Linux configuration with the application gateway and the security software so that it can be managed as a singe appliance. Unified Access Gateway is delivered as a single image file that is pre-hardened and tested overall by VMware. All configuration settings can be pushed during deployment so that Unified Access Gateway is "production-ready on first boot" and using automated deployment, and take less than 2 minutes. There is no need to separately configure or harden the appliance after it is deployed. This functionality eliminates the need to separately manage the operating system and install application packages. It also means that there are no incompatibility issues that might be encountered by combining different application code versions with different operating system components and Java versions. Overall, all components of a released appliance image are tested by VMware prior to release.

There is a full version of Unified Access Gateway and a limited FIPS version. Deployment of Unified Access Gateway is supported on:

- vSphere (ESXi and vCenter)

  Note vCenter is mandatory for ESXi deployment.

- Amazon AWS EC2 (Xen and KVM)
- Microsoft Azure
- Hyper-V (for Workspace ONE UEM only)
- Google Compute Engine (GCE in Google Cloud).

The same Unified Access Gateway appliance (standard or FIPS version) is used for all solutions, hypervisors, and VMware Cloud services such as Horizon Cloud.

Virtual Appliance Operating System

Consistent with many other modern VMware virtual appliances, Unified Access Gateway uses the Photon operating system. Photon OS, is an open-source minimalist Linux operating system from VMware. The latest Unified Access Gateway versions use Photon 3.0.

Console access is supported to allow an administrator to log on as the root user. This is available through the virtualisation platform such as vCenter Console link and access can be restricted through a comprehensive Role-Based Access Control (RBAC) facility on vCenter to ensure only authorized administrators can gain access. SSH access to Unified Access Gateway is normally deactivated but can be activated using a password or the SSH key controls.

Product Updates

This section covers about the various updates that are released for Unified Access Gateway.

Every new version of Unified Access Gateway uses updated Photon, Java, and other components with all recent security updates applied. VMware strongly recommends you to stay up-to-date with Unified Access Gateway versions to take advantage of security updates and other improvements.

Note Release Notes describes the product updates and published for every release in the Unified Access Gateway Documentation page. For more information about the release updates, see *Release Notes* on VMware Docs.

Standard Releases

Currently, new versions of Unified Access Gateway are released every quarter (approximately 4 times in a year). New releases include functional updates, security updates, improvements, bug fixes, and updates to OS package versions.

Version numbering of Unified Access Gateway uses a simple YYMM format indicating the year and month of release. For example, version 2207 indicates it was released in July 2022.

Maintenance Releases

VMware might also release an interim maintenance version to address a critical security vulnerability that applies to Unified Access Gateway, or to address a critical defect.

Version numbering of Unified Access Gateway maintenance releases uses the YYMM format with a dot (.) and an incrementing number. For example, maintenance releases might be 2207.1, 2207.2, meaning it is a maintenance release for Unified Access Gateway 2207.

Critical OS Patch Updates

VMware might authorize the update of one or more OS packages to rectify a critical vulnerability that affects a specific version of Unified Access Gateway and for which no viable workaround is available.

Configure Automatic Check

Starting with Unified Access Gateway version 2009, a new capability is available for the administrator to configure an automatic check for any authorized package updates. By default, this capability is deactivated. Administrator can activate this capability for dynamic package download and update at next boot time. Either set to check and apply required updates once at next boot time, or configure to check and apply required updates at every boot. For more information about these settings, see Configure Unified Access Gateway to Automatically Apply Authorized OS Updates section in the Deploying and Configuring VMware Unified Access Gateway Guide on VMware Docs. This allows the administrator to schedule this update for a time that would not involve disruption of the running services. Authorized updates are rare and only made available for Photon and application packages that would address critical security or stability issues that apply in the context of the particular Unified Access Gateway version.

Note This feature is rarely used. Non critical updates and updates that are not required on Unified Access Gateway are not available for dynamic download but instead batched and released as part of the quarterly Unified Access Gateway releases or the next maintenance release.

Security Settings for Unified Access Gateway

This section covers the security settings configured for Unified Access Gateway.

The following table lists the TLS configuration for the main Unified Access Gateway HTTP Port 443 on the standard (non-FIPS) Unified Access Gateway. The FIPS version of Unified Access Gateway uses more limited set of ciphers and TLS versions. The TLS settings are configured in System Settings and are applicable to the Horizon Edge service and the Web Reverse Proxy Edge service.

Note TLS settings for VMware Tunnel, Content Gateway, and Secure Email Gateway Edge services are configured separately in Workspace ONE UEM Console.

Table 1-1. TLS Configuration for Unified Access Gateway HTTP Port 443

TLS Versions	TLS Ciphers	TLS Elliptic Curves/Named Groups	TLS Server Certificates
Unified Access Gateway supports the following TLS versions on the HTTPS 443 interface. - `TLS 1.3` - `TLS 1.2` - `TLS 1.1` - `TLS 1.0` The default is for support of `TLS 1.3` and `TLS 1.2` only. VMware recommends to activate other versions only if required.	Unified Access Gateway supports the following default TLS ciphers on the HTTPS 443 interface. The cipher list is configurable. **TLS 1.3** - `TLS_AES_128_GCM_SHA256` - `TLS_AES_256_GCM_SHA384` - `TLS_CHACHA20_POLY1305_SHA256` **TLS 1.2** - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` - `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256` - `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`	`P-256 (secp256r1)` (256 bits) `P-384 (secp384r1)` (384 bits) `P-521 (secp521r1)` (521 bits) `X25519` (253 bits)	By default, Unified Access Gateway will generate self signed SSL server certificates. VMware strongly recommends to replace with trusted Certificate Authority (CA) signed certificates appropriate for the production environment. The trusted CA signed certificates can be specified during deployment of Unified Access Gateway.

SSH

By default, root console access to Unified Access Gateway using the SSH protocol is deactivated. You can activate SSH access using the password access or the SSH keys or both. If required, it can be limited to access on individual NICs.

By restricting SSH access to specific NICs, it is also possible to use a jumpbox and ensure limited access to that jumpbox.

Compliance

Security Technical Implementation Guides (STIGs)

Unified Access Gateway supports configuration settings to allow Unified Access Gateway to comply with the Photon 3 DISA STIG. For this compliance, the FIPS version of Unified Access Gateway must be used and specific configuration settings are applied at deploy time. For more information about the configuration settings, see *DISA STIG OS Compliance Guidelines for Unified Access Gateway* in the *Deploying and Configuring VMware Unified Access Gateway Guide* at VMware Docs.

FedRAMP Compliance

The Federal Risk and Management Program (FedRAMP) is a cyber security risk management program for the use of cloud products and services used by U.S. federal agencies. FedRAMP uses the National Institute of Standards and Technology's (NIST) guidelines and procedures to provide standardized security requirements for cloud services. Specifically, FedRAMP leverages NIST's Special Publication [SP] 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations series, the baselines and test cases.

VMware is seeking FedRAMP compliance and certification of Unified Access Gateway with Horizon on Azure GovCloud. This requires specific configuration. For more information about the configuration settings, see *FedRAMP Guidelines for Unified Access Gateway* in the *Deploying and Configuring VMware Unified Access Gateway Guide* at VMware Docs.

Frequently Asked Questions (FAQs) about Security

This section covers security related questions and answers for VMware Unified Access Gateway.

Can I install third party agents and/or Anti-virus software on Unified Access Gateway?

No. Antivirus software or third party agents are not required on a Unified Access Gateway appliance and the use of such software is not supported and it applies to all VMware branded virtual appliances. For more information, see https://kb.vmware.com/s/article/80767 and https://kb.vmware.com/s/article/2090839.

Is Unified Access Gateway impacted by CVE-XXX-XXXX?

Unified Access Gateway leverages industry leading code scanning, software composition analysis and vulnerability scanning tools, and monitors industry feeds for newly identified potential vulnerabilities. If vulnerabilities are detected, they are addressed per the VMware Security Response Policy.

If required, customers can be notified according to responsible disclosure practices through a VMware Security Advisory (VMSA). You can subscribe to be notified about newly published advisories at https://www.vmware.com/security/advisories.html. You are encouraged to apply product updates regularly to benefit from the latest security, reliability, and feature improvements.

For more information about Unified Access Gateway releases, see Product Updates.

It is inevitable that after VMware virtual appliances such as Unified Access Gateway are released by VMware, Photon security updates will become available between release dates. The severity of these security updates is generic and mostly do not affect the security of Unified Access Gateway itself. This might be because Unified Access Gateway does not use the affected component or because the vulnerability is in a function of the component that Unified Access Gateway does not support. Performing dynamic unauthorized updates of these Photon components might destabilize the appliance and might introduce a new vulnerability that cannot be detected in the testing prior to release.

All VMware appliances are thoroughly tested and qualified based on the components and versions included with the original release. Updating or changing any components on a virtual appliance may therefore result in unexpected behavior of the system and hence unauthorized updates are not supported.

Consistent with other VMware-branded virtual appliances, VMware does not support any modifications or customizations to the underlying operating system and packages included in a VMware-branded Virtual Appliance. This includes adding, updating, or removing of packages, and utilizing custom scripts within the operating system of the appliance. For more information about VMware's policy for virtual appliances, see https://kb.vmware.com/s/article/2090839.

If a security vulnerability is identified by VMware, by a customer or by anyone else, there is a defined policy for reporting this and for VMware's response based on the severity as it applies to the particular product. For more information, see Security Response Policy.

A critical security vulnerability in a Photon component that is not used by Unified Access Gateway or does not apply to any functionality of Unified Access Gateway has no security significance and is therefore not critical in the context of Unified Access Gateway.

If a critical security vulnerability is determined to affect Unified Access Gateway, then VMware might release a patched version of the appliance in addition to providing the update in the next quarterly release. This can be for a critical issue that does apply to Unified Access Gateway for which there is no workaround. VMware publish security advisories from time to time to communicate such vulnerabilities.

How frequently does VMware release new Unified Access Gateway versions?

For more information, see Product Updates.

When are Photon package updates applied to Unified Access Gateway?

Every planned release of Unified Access Gateway contains up-to-date Photon and Java versions determined at the time the virtual appliance is built. Usually this is around 2 weeks prior to the General Availability (GA) date to give an opportunity for final cross functional team and security qualification to ensure the package version combinations work correctly together. Photon packages are updated even if the update was to address a vulnerability that does not apply to Unified Access Gateway.

Is there a mechanism with Unified Access Gateway to automatically download and apply critical Photon vulnerability updates?

Yes. This feature was added with version 2009. Occasionally, VMware might authorize the update of one or more OS packages to rectify a critical vulnerability that affects a specific version of Unified Access Gateway and for which no viable workaround is available. Starting from Unified Access Gateway version 2009 a new capability is available for the administrator to configure an automatic check for any authorized package updates. For more information, see *Configure Automatic Check* section in Product Updates.

If a scanner reports an out-of-date Photon package, does this mean Unified Access Gateway is vulnerable?

A scan report can sometimes indicate a vulnerability, but most times a report about a newer version of package being available is not applicable to Unified Access Gateway. This might be because the corrective action to mitigate the vulnerability has already been applied or the vulnerability is in a component not used or activated by Unified Access Gateway. Vulnerability scanners can be prone to false positives even if they are properly configured and kept up-to-date.

If there is a “false positive” vulnerability scan report, would applying the package update for that package make Unified Access Gateway more secure?

Applying the package update in these cases would make no difference as Unified Access Gateway is not vulnerable with "false positives" anyway. VMware does not support applying package updates to VMware branded virtual appliances. Updating or changing any components might result in unexpected behavior of the system.

Why does VMware not support customer modification/update of Photon packages on VMware branded virtual appliances?

- It could result in unexpected behavior of the system because of incompatibilities with other software on the appliance and backward compatibility issues with configuration.
- Updating a package could introduce a new security vulnerability that would not be detected during security testing prior to the original appliance release.
- For the "false positives", applying a package version update will make no security improvement.

The tests performed by VMware are on the set of components that make up the virtual appliance image exactly as originally released.

If I am concerned about a scanner vulnerability report, can I request information about it from VMware?

Most scanners work by identifying which product and version is running in the network and comparing that information to a list of publicly known vulnerabilities. Vulnerability scanners can be prone to false positives even if they are properly configured and kept up-to-date. A support request can be raised by a customer and VMware support along with VMware Security Response Center (vSRC) will respond and explain why the update does not apply to the particular appliance.

Does VMware regularly run scans on Unified Access Gateway appliances internally?

Yes. The VMware Security Development Lifecycle includes regular and automatic scans of appliances so that early analysis can be performed by VMware.

How often are Photon package versions updated?

Several Photon kernel and package updates are released every month. In most cases, these are not released for Unified Access Gateway and are batched up for release in the next planned Unified Access Gateway release.

If a critical Photon package or Unified Access Gateway software security vulnerability is identified that affects Unified Access Gateway, how can I get to know about it?

Customers can subscribe to VMware security advisories which are published to inform customers of action they must take to protect products against known vulnerabilities that affect VMware products.

What is VMware's response if a Unified Access Gateway critical vulnerability is identified? Should I wait for the next planned version release?

VMware publishes the security response policy which defines response times for security vulnerabilities identified. The response time is based on the severity as it applies to a particular product. For example, a critical security vulnerability detected in Unified Access Gateway requires VMware to begin work on a fix or corrective action immediately. VMware will provide the fix or corrective action to customers in the shortest commercially reasonable time. A fix is delivered as a patch image release and the customer must upgrade to that version as soon as possible. Do not wait for the next planned release of Unified Access Gateway. In this case, VMware also publishes a security advisory and might also make the update available as an automatic update. See Security Response Policy.