VMware, Inc.

3401 Hillview Ave, Palo Alto, CA 94304, USA, Tel: (877) 486-9273, www.vmware.com

Guidance Supplement

VMware Unified Access Gateway (UAG) 2209

Common Criteria (CC) Evaluated Configuration Guidance

Document Version: 1.0
Document Date: April 24, 2023

VMware, Inc.

3401 Hillview Ave
Palo Alto, CA 94304

United States of America

Phone: +1 (877) 486-9273

http://www.vmware.com

VMware Horizon

https://www.vmware.com/products/horizon.html

VMware Security Response Center

http://www.vmware.com/support/policies/security_response.html

security@vmware.com

REVISION HISTORY

Ver #	Description of changes	Modified by	Date
1.0	Initial release of document	Justin Fisher	April 24, 2023

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Purpose

This document describes the operational guidance and preparative procedures for VMware Unified Access Gateway (UAG). This document defines the necessary steps to configure the Target of Evaluation (TOE) for use and provides guidance for the ongoing secure usage of the TOE.

The evaluated configuration of VMware UAG includes the following VMware Horizon components in its operational environment:

- VMware Horizon Client for Windows
- VMware Horizon Client for Android
- VMware Horizon Connection Server
- VMware Horizon Agent for Linux
- VMware Horizon Agent for Windows

Separate guidance documents exist for each component. Refer to the NIAP Product Compliant List (PCL) at https://www.niap-ccevs.org/Product/PCL.cfm for each product validation and its associated documentation.

1.2 Product Overview

The VMware Unified Access Gateway (UAG) is a virtual network device that is used as a remote access server to allow users on an untrusted network (e.g., a home office or other offsite location) to access enterprise resources on a protected internal network. The product has a variety of uses but the purpose of the TOE as evaluated is for facilitating connectivity between VMware Horizon users and virtual desktops/applications.

The evaluated configuration of VMware UAG is limited to the security functionality claimed in the Security Target; any other functionality that does not relate to the security functional claims are considered to be non-interfering with respect to security. Any product security functionality that is within the scope of the evaluation must be configured in the manner specified in this guidance.

1.3 Document Reference

This document serves as a supplement to the standard VMware documentation set, and as such references (either implicitly or explicitly) the documents referenced in this section.

VMware UAG guidance can be found at the following links:

- Horizon Administration (https://docs.vmware.com/en/VMware-Horizon/2209/horizon-console-administration.pdf)

- Deploying and Configuring VMware Unified Access Gateway (https://docs.vmware.com/en/Unified-Access-Gateway/2209/uag-deploy-config-guide.pdf)

2 INSTALLATION GUIDELINES AND PREPARATIVE PROCEDURES

2.1 Assumptions

The following assumptions are made with regards to the setup, installation, and ongoing operation of this product:

- The UAG is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation.
- The UAG is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing.
- Traffic filtering was outside the scope of this evaluation and is assumed to be provided by appropriately configured network boundary devices.
- The Security Administrator(s) for the UAG are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation.
- The UAG's firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- Administrator credentials are assumed to be stored securely.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
- Administrators for the virtualization system (VS) on which the UAG runs are assumed to be trusted and to act in the best interest of security for the organization.
- The VS on which the UAG runs is assumed to be updated on a regular basis when updates to it are made available.
- It is assumed that the VS provides and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside virtual machines on the same physical platform.
- It is assumed that the virtualization system and virtual machines used by the network device are correctly configured to support necessary functionality.

2.2 Evaluated Configuration

The Target of Evaluation (TOE) is VMware UAG 2209. Specifically, the TOE is a virtual network device that includes its operating system (VMware Photon 3.0) and the software that runs on it. The specific tested version was "Unified Access Gateway (UAG) 2209.2 for vSphere (FIPS)." Ensure that the most recent FIPS version of the product is used.

The evaluated configuration of the TOE expects it to be deployed in a VMware Horizon environment, which consists of one or more VMware Horizon Clients, a VMware Horizon Connection Server, and one or more VMware Horizon Agents. A secondary Horizon Connection Server was also used for the purpose of testing cloud pod communications. In the tested configuration, all components except for the Horizon Clients are virtualized on VMware ESXi 7.0. The diagram below shows the evaluated configuration of VMware Horizon with tested components and interfaces highlighted in blue. VM hypervisors and network boundary/infrastructure devices (e.g., routers, switches, firewalls) are not shown for readability purposes.

Figure 1 shows the TOE in a sample deployment with VMware Horizon components in its operational environment. Note the following:

- Firewalls are not shown between internal and external networks, but it is assumed that the TOE is deployed in a DMZ between them.
- Multiple UAGs may be deployed in a load balancer configuration to ensure resource availability. As the claimed PP does not have availability requirements, only one UAG is deployed in the tested configuration.
- The second Horizon Connection Server that is depicted on the diagram has its own associated Horizon Agents and other external interfaces. These are omitted for simplicity.
- The environment assumes that all components have access to the organization's Certification Authority for issuance and validation of X.509 certificates.

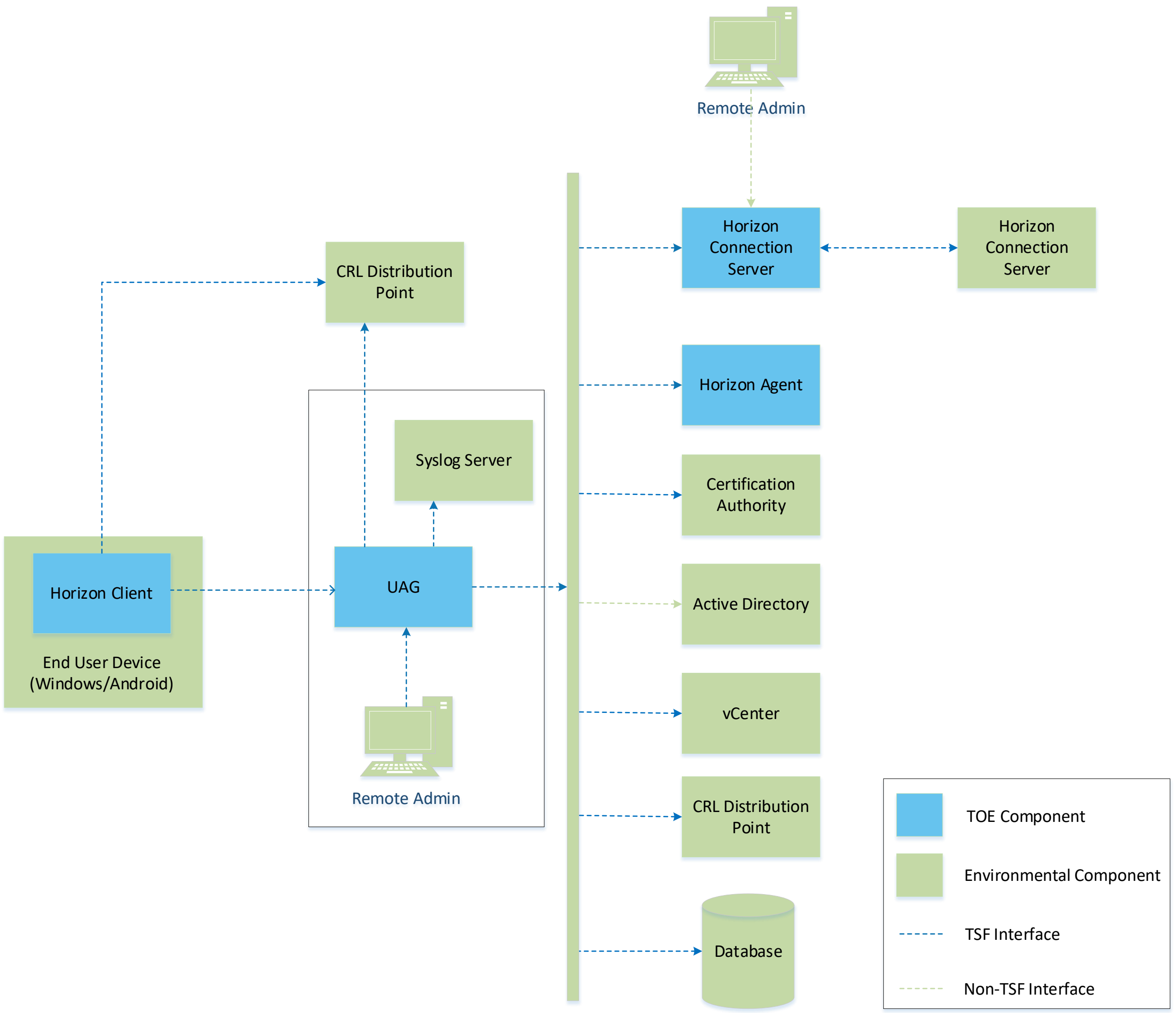

Figure 1: UAG Evaluated Configuration (simultaneously deployed with VMware Horizon components evaluated individually)

The TOE handles inbound requests from the Horizon Client over both mutually-authenticated and one-way TLS. Initial Horizon Client connectivity to the TOE requires mutually-authenticated TLS but once authenticated, subsequent connections do not require re-validation of the client certificate. Inbound management communications and outbound communications, both to the environmental syslog server and to other Horizon components (Connection Server and Agent) use one-way TLS. While the TOE does not provide a certificate to a remote Horizon Agent for authentication, the Horizon Agent does require it to provide a single use authorization token that is issued to the TOE by the Connection Server.

The following network ports must be open for the TOE to function:

- TCP/443 (for inbound session establishment connectivity and Blast protocol connectivity from Horizon Clients)

- TCP/9443 (for inbound remote administration)

Since Horizon consists of multiple components, it is expected that each component is configured in accordance with its own evaluated configuration guidance.

Additionally, the evaluated configuration is defined such that all certificates used within the Horizon deployment are issued by the same Certificate Authority. While not explicitly required for Horizon to function properly, it simplifies administration and reduces the likelihood of misconfiguration leading to error or vulnerability.

2.3 Supporting Environmental Components

The following table lists the external components that are required for the product to function in its evaluated configuration.

Component	Description
VMware Horizon Agent	Used to serve content from a remote host to a VMware Horizon Client.
VMware Horizon Client	End user application that requests content to be served to it by VMware Horizon Agents.
VMware Horizon Connection Server	Used for authentication and authorization of VMware Horizon Client users.
Certificate Authority	Used to manage the generation, issuance, and revocation of X.509 certificates used for authentication and secure communications.
Syslog Server	Used for remote storage of audit data.

The TOE’s operational environment includes the following:

- VMware Horizon components (at least one each of Horizon Client, Horizon Connection Server, and Horizon Agent)
- Remote syslog server
- Platform (hardware and software) on which the TOE is hosted. In the tested configuration, this included the following:
  - VMware ESXi 7.0
  - Dell PowerEdge R740 with Intel Xeon 6230R (Cascade Lake) processor
- Access to a Certification Authority and corresponding revocation checking mechanism is needed to validate presented X.509 certificates.

Note that UAG does not use X.509 certificates for trusted updates and executable code integrity so extendedKeyUsage fields related to these purposes are not used.

- A remote system with a supported web browser for remote administrative access:
  - The tested configuration used Google Chrome 106.0.5249.119

2.4 Installation of the TOE

The Deploying and Configuring VMware Unified Access Gateway document provides specific instructions for installing VMware Unified Access Gateway (UAG) in your environment.

2.5 Obtaining Support

In the event of software failure, customers should engage with VMware Global Support Services to make use of any purchased support contract(s). See the Support Contact Options for more information.

Failure of self-tests:

- BC-FJA failures logged under the "org.bouncycastle.crypto.fips.FipsSelfTestFailedError" message type in various log files in the /opt/vmware/gateway/logs directory.
- OpenSSL failures logged into the syslog-ng.log or bsg.log in the /opt/vmware/gateway/logs directory.
- Failure of boot partition filesystem check will cause UAG to fail to boot entirely and a corresponding error message will be displayed on the local console.

Note that cryptographic interfaces will not function if the associated cryptographic library fails to start, including remote syslog transmission of audit data in the event of an OpenSSL failure; in the event of lack of connectivity the logs should be reviewed on the local console.

Failure of updates: recorded in the package-updates file available in the local console.

In case of any failure, first attempt to restart UAG and then contact VMware support if the issue is not resolved.

VMware also maintains comprehensive guidance for all VMware products in the VMware Knowledge Base, located at https://kb.vmware.com/s/. Consult the Knowledge Base for any issues that are not found in other guidance, as well as any product patches and associated documentation.

2.6 Security Issues and Mitigations

VMware maintains a Security Advisories page at https://www.vmware.com/security/advisories.html. Information regarding security issues and product workarounds or fixes for the issues are posted here as part of the timely security update process. Administrators can also sign up for notifications to be made aware of updated guidance and patches as they are released.

3 Configuring the Common Criteria Evaluated Configuration

3.1 Deployment Overview

Unified Access Gateway is packaged as an Open Virtualization Form package (OVF) and is deployed onto a vSphere ESXi host as a pre-configured virtual appliance. Two versions of the UAG OVF package are available: a standard version and a FIPS version. The Common Criteria evaluated configuration requires the FIPS version. Note that when the FIPS version is used, the UAG is automatically configured into FIPS mode; this is not modifiable.

Note that use of the FIPS version automatically ensures that the VMware OpenSSL FIPS Object Module 2.0.20-vmw and VMware Bouncy Castle FIPS Java API (BC-FJA) 1.0.2.3 on JDK 11 are used for cryptographic operations. No other cryptographic engines are present in the product and the non-FIPS version of the product was not evaluated or tested. Both cryptographic implementations ensure the destruction of plaintext keys in volatile and non-volatile storage in accordance with the key destruction methods claimed in the VMware Unified Access Gateway Security Target; there are no circumstances that cause an exception to this.

Two methods can be used to deploy the UAG appliance on vSphere: the OVF Template Wizard through vSphere, which is discussed in the "Using the OVF Template Wizard to Deploy Unified Access Gateway" section of Deploying and Configuring VMware Unified Access Gateway, or PowerShell, which is discussed in the "Using PowerShell to Deploy Unified Access Gateway" section of Deploying and Configuring VMware Unified Access Gateway.

3.2 Prerequisites

1. The UAG FIPS appliance OVA file.
2. Certificates to upload to UAG in PFX format or private key and certificate chains in PEM format.
    a. For communication with syslog server.
    b. For communication with SAML identity provider configuration.
    c. All the certificates, including the full chain (root, intermediate, and leaf) MUST have only SHA384 based signature.

Note that a self-signed certificate is pre-loaded onto UAG by default; this will be changed to a PKI certificate in the steps listed in section 3.5 below.

3.3 Deploying UAG Using OVF Template Wizard

To deploy the UAG OVA through vSphere, follow the steps outlined in the "Using the OVF Template Wizard to Deploy Unified Access Gateway" section of Deploying and Configuring VMware Unified Access Gateway.

Note that the passwords for the console root admin and Web UI admin will be set interactively during this process.

The OVF deployment options listed below must be specified for UAG to be in its evaluated configuration.

Enable SSH: `disable`

> In the evaluated configuration, the SSH interface is disabled; all console access is locally through vSphere and all remote access is through the Admin UI.

SecureRandom Source: `/dev/random`

> This specifies where the secure random bit generator source used by Java process is obtained. By default, the parameter is configured to use the non-FIPS mode value. This parameter needs to be configured to use the FIPS mode value.

Password policy minimum length: `n`

> The minimum length of the root (console) password. The evaluated configuration requires this parameter to be between `8` and `64`.

Session idle timeout for OS user in seconds: `n`

> The evaluated configuration requires a local administrator session to be terminated after some period of inactivity. This parameter must be non-zero for the evaluated configuration.

Password policy for maximum failed attempts: `0`

> The local console interface does not lock out so that a recovery mechanism exists for the case where the remote admin is locked out.

Password policy for unlock time in seconds on maximum failed attempts: `0`

> The local console is not locked out, so this setting is not applicable.

Admin password policy for minimum length: `n`

> The minimum length of the Admin UI password. The evaluated configuration requires this parameter to be between `8` and `64`.

Admin session idle timeout in minutes: `n`

> The evaluated configuration requires a remote administrator session to be terminated after some period of inactivity. This parameter must be non-zero for the evaluated configuration.

Admin password policy for maximum failed attempts: `n`

Admin password policy for unlock time in minutes on maximum failed attempts: `n`

> The evaluated configuration requires the TOE to prevent an administrator from logging into the system after a specified number of successive unsuccessful authentication attempts have occurred. The first value specifies the number of unsuccessful login attempts and must be a value between `1` and `100` (default is `3`). The second value specifies the lockout period, in

minutes, and must be non-zero. The second value has an allowable range of `1` to `9999` and is `5` by default.

Login Shell Banner Text: `<text>`

Sets the banner text for the local console to the value specified by `<text>`.

3.4 Deploying UAG using PowerShell

The following is a summary of the steps needed to deploy UAG using PowerShell. For more detailed instructions, reference the "Using PowerShell to Deploy Unified Access Gateway" section of Deploying and Configuring VMware Unified Access Gateway.

Note that UAG will prompt for the passwords for the console root admin and Web UI admin when the .ini is uploaded through PowerShell.

3.4.1 Procedures

1. Download the Unified Access Gateway OVA from https://my.vmware.com/ to your Windows machine.
2. Download the `uagdeploy-XXX.zip` file and extract it into a folder on the Windows machine. The ZIP files are available at the VMware Download page for Unified Access Gateway.
3. Open a PowerShell command window-and change the directory to the location of the script extracted above.
4. Create a INI configuration file for the Unified Access Gateway virtual appliance.

3.4.2 PowerShell Required Configuration Parameters

The following sections define parameters that are specific to the Common Criteria evaluation and must be configured to set the UAG in the evaluated configuration.

3.4.2.1 Miscellaneous Parameters

```
secureRandomSource=/dev/random
```

The `secureRandomSource` parameter specifies where the secure random bit generator source used by Java process is obtained. By default, the parameter is configured to use the non-FIPS mode value. This parameter needs to be configured to use the FIPS mode value.

```
sshLoginBannerText=<text>
```

Sets the banner text for the local console to the value specified by `<text>`.

3.4.2.2 Administrator Password Management Policies

UAG supports two administrator login accounts: root and admin. The root login is used for local console access. The admin account is used for Web UI access. Each account must be configured with the parameters listed below.

Note that the console root password is only defined during initial configuration; this password cannot be changed unless UAG is reinstalled.

The Web UI admin password can be changed during operation using one of the following mechanisms:

- Through the Web UI: navigate to **Manual Configuration** > **Advanced Settings** > **Account Settings**, select admin from the dropdown list, and specify Reset Password. UAG will prompt for the old password followed by the desired new password.
- Through the console (e.g., if the admin password has been lost): use the **adminpwd** command with no arguments to specify the desired new password.

Separate from the minimum password length, best practices for secure passwords should be followed. Specifically, passwords should contain at least one each of uppercase letter, lowercase letter, number, and special character in the set of [! @ # $ % ^ & * ( )], and should not contain any common dictionary words.

3.4.2.2.1 Root Account Parameters

`passwordPolicyMinLen=n`

The minimum length of the root password. The evaluated configuration requires this parameter to be between `8` and `64`.

`rootSessionIdleTimeoutSeconds=n`

The evaluated configuration requires a local administrator session to be terminated after some period of inactivity. This parameter must be non-zero for the evaluated configuration. Allowed configuration value is between `30` and `3600` seconds, with a default value of `300`.

`passwordPolicyFailedLockout=0`

The evaluated configuration requires that the local console interface not lock out so that a recovery mechanism is always available in the event that the remote interface experiences a denial of service due to excessive failed authentication attempts. Therefore, this parameter **must** be set to `0`.

`passwordPolicyUnlockTime=n/a`

This setting has no significance when `passwordPolicyFailedLockout` is set to `0`, as is required by the above note.

3.4.2.2.2 Admin Account Parameters

`adminPasswordPolicyMinLen=n`

The minimum length of the admin password. The evaluated configuration requires this parameter to be between `8` and `64`.

`adminSessionIdleTimeoutMinutes=n`

The evaluated configuration requires a remote administrator session to be terminated after some period of inactivity. This parameter must be non-zero for the evaluated configuration. Allowed configuration value is between `1` and `1440` minutes, with a default value of `10`.

`adminPasswordPolicyFailedLockoutCount=n`

`adminPasswordPolicyUnlockTime=n`

The evaluated configuration requires the TOE to prevent an administrator from logging into the system after a specified number of successive unsuccessful authentication attempts have occurred. `adminPasswordPolicyFailedLockoutCount` specifies the number of unsuccessful login attempts and must be a value between `1` and `100`. `adminPasswordPolicyUnlockTime` specifies the lockout period, in minutes, and must be non-zero.

3.4.3 Run PowerShell Completion

1. To make sure that the script execution is not restricted type the following command.

   ```
   set-executionpolicy -scope currentuser unrestricted
   ```

2. Run the command to start the deployment. If you do not specify the `.ini` file, the script defaults to `uag.ini` in the same folder.
3. Enter the credentials when prompted and complete the script.
4. The UAG appliance is deployed and available for production.

3.5 Obtain and Upload the TLS Server Certificate

The next step is to generate the CSR for TLS certificates and bind signed certificates for UAG admin and public interfaces.

NOTE: Ensure that all the certificates in the chain have SHA-384 signatures.

Any mismatch of signature algorithms in the certificates and the TLS configurations under System Settings might result in TLS handshake failures and loss of access to the server.

1. Log in to the UAG OS console.
2. Edit `/opt/vmware/certutil/uagcertutil.conf` and update the configuration values as necessary. Specifically, the Common Name, Organization, Organizational Unit, and Country values in the CSR can be modified here by altering the CN, O, OU, and C lines under the [req_distinguished_name] parameter block.

Note: the identifier for the UAG must be a DNS name in the SAN attribute; IP addresses are not supported.

3. Run the command "`uagcertutil --newcsr`" to generate new keypair and CSR.
4. Copy the generated CSR to external CA and get a signed certificate chain.
5. Copy the signed certificate back to UAG.
6. Edit the above configuration file and update the file path for signed certificate.
7. Run the command "`uagcertutil --bind`" to configure admin (Web UI)/esmanager (Horizon Client connections) TLS servers with the above certificate.
8. The utility supports configuring same certificate for admin as well as esmanager. However, if required, above steps can be repeated to configure different certificates for both admin and esmanager.

3.6 Verifying Successful Deployment

To verify successful deployment, log onto the UAG using the Web UI.

1. When the appliance is powered on, verify that administrators can connect to the appliance by opening a browser and entering the following URL:
   https://*FQDN-of-UAG-appliance*:9443/admin

   In this URL, *FQDN-of-UAG-appliance* is the DNS-resolvable fully qualified domain name of the UAG appliance.

2. The VMware UAG login page will appear.

3. Enter the admin name and admin password configured during deployment. The password characters will be automatically obscured (a bullet ('•') will be displayed in place of each character). Select **Login**.

4. A page will be displayed giving the options to Import Settings or Configure Manually.

   Additionally, the UAG appliance version will be displayed at the top of the page. Verify the latest update to the proper TOE version is used (e.g. 2209.2 if that is the most recent version available). Also, under the version number (FIPS) should be displayed because the evaluated configuration of the TOE must be in FIPS mode. If the version number is incorrect or if (FIPS) is not displayed, return to section 3.1 for redeployment.

   The top right of the page displays an icon identifying the username (admin). Next to the icon is a pulldown menu. To logout of your remote session, select the pulldown menu and select **Logout**. The login page will appear if **Logout** is selected.

3.7 Enabling Time Sync

As a virtual network device, the TOE obtains its time data from the virtualization system on which it is deployed using the VMware Tools periodic time synchronization interface.

1. Select the **Advanced Settings > System Configuration** gearbox icon.

2. Slide the **Time Sync With Host** parameter right to enable.

Note that the time sync occurs every minute so a delay of up to one minute can occur between a time update on the host and that update being applied to UAG.

4 Operational Procedures for Administrators

This section describes additional steps, clarifications, and exclusions that might not be documented in the public documentation for this product. The assumption is that the TOE and its environment have already been successfully deployed, working and accessible before these next steps are performed.

4.1 Logging Into and Out of UAG

To log into UAG using the console, activate the VM image in ESXi. You will be presented with the option to log in or to specify the time zone. Choose the option to log in and specify the local root administrator password. The login banner is displayed on this screen. Once authenticated, log out using the **exit** command.

To log into UAG using the Web UI, navigate to the URL on which the Web UI is hosted (port 9443 on the DNS name of the host), acknowledge the login banner, and then enter the web admin credentials on the login page. Once authenticated, log out using the pulldown menu and selecting **Logout**.

4.2 Unlocking Remote Administrator Account

If the remote administrator account is locked due to excessive failed authentication attempts, access will be restored automatically after the configured lockout period has expired. Alternatively, to force the account to be unlocked, log in to the local console and issue the command `supervisorctl restart admin`.

4.3 Configuring TLS Parameters

For both client and server, the default configuration of the application supports a more permissive set of TLS connection settings, so it is necessary to configure a restriction of this in order for the product to be in its evaluated configuration. Note that the supported cryptographic algorithms and key strengths are configured implicitly by defining the supported TLS cipher suites.

1. Select the **Advanced Settings** > **System Configuration** gearbox icon.

4.3.1 Step 1: Configure the TLS Server Cipher Suites

The UAG evaluated configuration supports only one TLS server cipher suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. This parameter must be configured by an administrator because the UAG default server cipher suites in FIPS mode include a larger group of cipher suites.

Note: this restricted configuration is defined for the purpose of Commercial Solutions for Classified (CSfC) conformance. No other configuration is necessary for UAG to conform to the required CSfC claims for TLS Protected Server.

To configure the TLS server cipher suites using the Web UI:

1. Enter `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` in the **TLS Server Cipher Suites** parameter.

4.3.2 Step 2: Configure the TLS Client Cipher Suites

The UAG evaluated configuration supports the following cipher suites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

Note: UAG has two separate cryptographic engines—OpenSSL and Bouncy Castle BC-FJA. OpenSSL only supports the TLS_ECDHE cipher suites listed above while BC-FJA supports all six. Only one configuration setting is used because the FIPS version of UAG automatically restricts OpenSSL from using the TLS_DHE cipher suites.

This can be configured using the Web UI by modifying the **TLS Client Cipher Suites** option. This parameter must be configured by an administrator because the UAG default client cipher suites in FIPS mode include a larger group of cipher suites.

To configure the TLS client cipher suites using the Web UI:

1. Enter `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384` in the **TLS Client Cipher Suites** parameter.
   The option requires comma-separated values (no spaces).

4.3.3 Step 3: Enabling TLS 1.2 Only

The UAG evaluated configuration requires TLS 1.2 for both client and server and rejects all other TLS versions. The FIPS version of UAG supports this by default and does not allow other TLS versions to be configured.

4.3.4 Step 4: Setting the SSL Provider

UAG enables an administrator to configure TLS Named Groups and TLS Signature Schemes. To support modification of these parameters, the UAG's **SSL Provider** parameter must be set to `JDK` (the default value is `OPENSSL`). This option must be set to `JDK` for the evaluated configuration.

To configure **SSL Provider** using the Web UI:

1. Select the **Advanced Settings** > **System Configuration** gearbox icon.
2. Select `JDK` from the pulldown menu of the **SSL Provider** parameter.
3. Select **Save**.

4.3.5 Step 5: Setting the TLS Named Groups

The UAG allows an administrator to configure the desired named groups (elliptic curves) from a list of supported named groups used for key exchange during SSL handshake. The evaluated configuration requires an administrator to configure the **TLS Named Groups**. The **SSL Provider** option must be set to `JDK` to enable this option.

To configure **TLS Named Groups** using the Web UI:

1. Select the **Advanced Settings** > **System Configuration** gearbox icon.
2. Enter `secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192` in the **TLS Named Groups** parameter.
3. Select **Save**.

Any changes to this option result in the UAG services getting restarted. Ongoing UAG session are not retained during the restart.

4.3.6 Step 6: Set the TLS Signature Schemes

The UAG allows an administrator to configure the supported TLS signature algorithms used for key validation during SSL handshake. The evaluated configuration requires an administrator to configure the **TLS Signature Schemes**. The **SSL Provider** option must be set to `JDK` to enable this option.

To configure **TLS Signature Schemes** using the Web UI:

1. Select the **Advanced Settings** > **System Configuration** gearbox icon.
2. Enter `rsa_pkcs1_sha384` in the **TLS Signature Schemes** parameter.
   The option allows comma-separated values (no spaces).
3. Select **Save**.

Any changes to this option result in the UAG services getting restarted. Ongoing UAG session are not retained during the restart.

4.4 Configuring the Warning Banner

The evaluated configuration requires UAG to display an advisory notice and consent warning message regarding use of the TOE before any logon attempt.

To configure the warning banner for the Web UI using the Web UI:

1. Select the **Advanced Settings** > **System Configuration** gearbox icon.

2. Enter the admin disclaimer text you would like displayed in the **Admin Disclaimer Text** field.

To configure the warning banner for the local console, the Login Shell Banner Text or `sshLoginBannerText` parameter is used for OVF and PowerShell deployments, respectively. The console banner text can only be configured during initial setup.

Note that even though SSH is not used in the evaluated configuration, the banner text used for the SSH interface is the same as that used for the local console interface, so this parameter is applicable to the evaluated configuration of UAG despite having 'ssh' in its name.

4.5 Configuring X.509 Client Authentication

First, obtain the root certificate and any intermediate certificates from the CAs that signed the Horizon Client certificates that will be presented to UAG.

Then, perform the following steps in the Admin UI:

1. Select **Configure Manually**.
2. Select the **General Settings** > **Authentication Settings** slider and then the **X.509 Certificate** gearbox.
3. Slide the Enable X.509 Certificate slider to on.
4. Upload the trusted Root CA and intermediate CA certificates of the client certificates.
5. Enable certificate revocation check using the toggle button.
6. Configure CRL based certificate revocation check - either a URL can be configured to fetch CRL or can be configured to read the details from certificate chain itself.
7. Enter Save.

Client certificates will be validated against the CAs placed in the trust store using this manner. The reference identifier of the certificate is automatically validated using the value in the CN field; SAN is not used as the basis for reference identifier checking and no configuration is needed for this behavior.

4.6 Configuring SAML

UAG authenticates Horizon Client users via mutual TLS authentication and passes access request to Connection Server via SAML assertion. To enable this, the SAML Identity Provider and SAML Service Provider parameters must be configured.

To configure the SAML settings follow the following sections:

1. Select **Advanced Setting > SAML Setting** gearbox icon.
2. Expand **SAML Identity Provider Settings**.
3. Select **Provide Certificate**.
4. Upload the **Private Key** and **Certificate Chain** (signed with RSA+SHA384 algorithm) by selecting **Select** next to each field.

For more information refer to the "Generate Unified Access Gateway SAML Metadata" section of Deploying and Configuring VMware Unified Access Gateway.

5. Select **Save**.
6. Download the generated identity provider setting XML by providing the external hostname of UAG.
7. Select **Download**.
8. Update the environmental Connection Server with the downloaded Identity Provider settings. For more details, reference the "Configure SAML Authentication to Work with True SSO" section of Horizon Administration.
9. Expand the **SAML Service Provider Settings**.
10. Paste the SAML **Metadata XML** content and enter a **Service Provider Name**.

    For more information refer to the "Copy Service Provider SAML Metadata to Unified Access Gateway" section of Deploying and Configuring VMware Unified Access Gateway.
11. Select Save.

4.7 Enabling Advanced X.509 Settings

To ensure proper handling of X.509 certificates, several advanced settings must be configured.

The UAG must be configured to validate certificates for expiration, identity, revocation, and extended key usage values. For server certificates, this is done in the following manner:

To configure **Extended Server Certificate Validation** using the Web UI:

1. Select the **Advanced Settings > System Configuration** gearbox icon.
2. Set **Extended Server Certificate Validation** to be enabled.
3. Select **Save**.

As of UAG 2209, the following two parameters are implemented using a feature flag (`<FeatureFlag>`) and hence need to be explicitly enabled during or post deployment.

1. SyslogCrlCheck – used to ensure that revocation checking is performed for syslog server certificates

2. ClientCertEkuCheck – used to ensure that extendedKeyUsage is checked for client certificates

To verify if a feature flag is enabled post deployment, run below curl command:

```
curl -X 'GET' \
   -k \
   -u admin \
   "https://uag-
host:9443/rest/v1/config/feature?featureName=<FeatureFlag>' \
   -H 'accept: application/json'
```

To enable feature flags during PowerShell based deployment, use the following configuration in the .ini file.

```
[General]
enableAdvancedFeatures=FeatureFlag1,FeatureFlag2,…
```

To enable a feature flag post deployment, use the below curl command.

```
curl -X 'PUT' \
    -k \
    -u admin \
    'https://uag-host:9443/rest/v1/config/feature' \
    -H 'accept: application/json' \
    -d '{
    "featureName": "<FeatureFlag>",
    "enabled": true,
    "environment": "PRODUCTION"
} '
```

4.8 Configuring Edge Services

1. Log in to the UAG Admin UI.
2. Click **Select** under the **Configure Manually** section.
3. At the top of the screen, slide the **Edge Service Settings** in the **General Settings** section to on.
4. Select the **Horizon Settings** gearbox icon.
5. Slide the **Enable Horizon** parameter right to enabled.
   Enter the Connection Server URL in the **Connection Server URL** parameter in the form of *https://FQDN-of-ConnectionServer:443*.
6. Under Auth Methods, select **X.509 Certificate**.
7. Select the pull-down menu of **the Minimum SHA Hash Size** parameter and select `SHA-384`.
8. Slide the **Enable Blast** parameter right to enable.
9. Enter the Blast External URL by entering the UAG/LB public hostname with port 443 in the form of *https://FQDN-of-UAG:443* in the **Blast External URL** parameter field.
10. Click **More.**
11. Under **SAML SP**, enter the name of the SAML service provider

12. Under **Trusted Certificates**, add any root and intermediate CA certificates needed to trust the certificates presented by Horizon Connection Server and Horizon Agents.
13. If necessary, modify the **Host Entries** field for name resolution of Horizon Connection Server and Horizon Agents.
14. Click **Save**.

4.9 Recovering Broken Connections

In the case that UAG goes offline or otherwise becomes unavailable to external systems, the UAG will automatically re-establish connectivity to the environmental Horizon Connection Server and syslog server. Any admin sessions need to be manually re-established in such cases. Horizon Clients will periodically attempt to re-connect until connectivity is re-established, but the session will be terminated so the remote user must re-authenticate.

Note that for any case where UAG needs to validate an X.509 certificate to establish a remote connection, a certificate whose revocation status is unavailable is automatically rejected. It is therefore necessary to ensure that any presented certificate's source of revocation information (i.e., CRL) is available when a connection is being made.

5 AUDITING, SYSLOG, AND UPDATES

The section describes:

- How to configure the log level
- How to configure a syslog server
- Sample log files for security-relevant events
- How to apply package updates

5.1 Configuring Auditing Using the Web UI

The following section describes UAG's audit mechanism and includes instructions for configuring UAG's audit handling to be consistent with its evaluated configuration.

5.1.1 Logged Events

Events are logged:

- when an administrator logs into the UAG Web UI,
- when an administrator performs configuration changes,
- when an administrator logs out of the Web UI,
- any login failure,
- when a session is created at user login, and
- when a session is destroyed after user logout.

5.1.2 Log Retention Requirements

The log files are configured by default to use a certain amount of space which is smaller than the total disk size in the aggregate. The logs for UAG are rotated by default. You must use syslog to preserve these log entries. See Collecting Logs from the Unified Access Gateway Appliance in Deploying and Configuring VMware Unified Access Gateway.

Audit records are stored in several different log files. With respect to the TSF, the admin.log, audit.log, and esmanager.log files contain records of security-relevant events. No remote administrative commands exist to modify or delete log files; only the local root admin is authorized to interact with these files. A Security Administrator is therefore authorized to manually delete audit records only if they are authenticated to the TOE via the local console. This is done using the **rm** command on the log file to be deleted. Each of the log files are rotated such that the exhaustion of storage for one file causes it to be archived with active auditing moving to the next file in the rotation. Once all files are filled in this manner, subsequent rotations will overwrite the oldest stored record. By default, each of the log files have a maximum file size of 10 MB and store five separate files in the rotation. In the evaluated configuration, all log files are configured to transmit log data to a remote syslog server over TLS; this occurs in real-time, simultaneously with the audit records that are written locally. In the event of a syslog outage, there is no buffering mechanism that allows for synchronization between local and remote logs.

5.1.3 Syslog Event Format

UAG categorizes syslog events into two categories: Audit Events and all other types of events. Audit Events are recorded locally to audit.log and all other events are recorded to admin.log and esmanager.log. All log files follow a certain format. The following tables list the log formats and field descriptions:

Table 1: Audit/System Syslog Event Contents

Event Category	Log Format
Audit Events	`<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <session id> <log message>`
Other Events	`<timestamp> <UAG hostname> <app name> <thread id> <log level> <file name> <function name> <line no.> <client IP> <username> <session type> <session id> <log message>`

Table 2: Description of the Syslog Audit Fields

Field	Description
`<timestamp>`	Indicates the time at which the event was generated and logged in the syslog server.
`<UAG hostname>`	Hostname of the Unified Access Gateway appliance.
`<app name>`	Application that generates the event. Note Depending on the log file, the values of this field are as follows: UAG-AUDIT, UAG-ADMIN, and UAG-ESMANAGER.
`<thread id>`	ID of the thread in which the event gets generated.
`<log level>`	Type of information collected in the log message. For more information about logging levels, refer to “Collecting Logs from the Unified Access Gateway Appliance” in Deploying and Configuring VMware Unified Access Gateway.
`<file name>`	Name of the file from which the log is generated.
`<function name>`	Name of the function in that file from which the log is generated.
`<line no.>`	Line number in the file where this log event is generated.
`<client IP>`	IP address of the component (such as Horizon Client, load balancer, and so on) that sends a request to Unified Access Gateway appliance.
`<session type>`	Edge service for which the session is created. In the evaluated configuration, this will only be Horizon.

Field	Description
`<session id>`	Unique identifier of the session.
`<log message>`	Provides a summary about what has occurred in the event

5.1.4 Configuring Log Level Settings

You can configure log levels for the entire UAG appliance or only for specific UAG components such as the Horizon edge service (and sub-components) and admin UI. The log levels that can be generated are ERROR, WARN, INFO, DEBUG, and TRACE. A description of the type of information that the log levels collect follows.

Table 3: Syslog log levels

Parameter	Description
`ERROR`	The ERROR level designates error events that might still allow the service to continue running.
`WARN`	The WARNING level designates potentially harmful situations but are usually recoverable or can be ignored.
`INFO`	The INFO level designates information messages that highlight the progress of the service.
`DEBUG`	Designates events that might generally be useful to debug problems, to view or manipulate the internal state of the appliance, and to test the deployment scenario in the environment. DEBUG is required to generate all auditable events for the evaluated configuration.
`TRACE`	Indicates information such as collection of Unified Access Gateway statistics, details of requests sent from Unified Access Gateway to backend servers and so on. This level must only be applied during trouble shooting as this level can reduce performance due to the production of verbose log messages.

The evaluated configuration requires the log level to be set to DEBUG level so that all required auditable events are generated.

To configure **Log Level Settings** using the Web UI:

1. Login to the UAG system.
2. Select **Configure Manually**.
3. Select the **Support Settings** > **Log Level Settings** gearbox icon.
4. Select the pulldown menu of the **Log Level Settings** option.
5. Select `All` to indicate that the configured log level is applied to the entire UAG appliance.
6. Select the pulldown menu to the second parameter.
7. Select `DEBUG` to set the log level.
8. Click the ‘+’ icon next to the log level dropdown.
9. Select **Save**.

5.2 Logging to External Server

5.2.1 Configuring Syslog Server Settings

The following section summarizes how to configure an external syslog server for remote audit storage. Refer to "Configure Syslog Server Settings" in Deploying and Configuring VMware Unified Access Gateway for additional information.

Note the syslog server certificate must have the extendedKeyUsage marked as a critical extension.

Note: CRL-based revocation checking must be enabled as well; this is done through the steps outlined in "Enabling Advanced X.509 Settings" above.

To enable

1. From the admin UI Configure Manually section, select.
2. Under **Advanced Setting**, click the gearbox icon next to **Syslog Server Settings.**
3. In the **Syslog Server Settings** window, select **Add Syslog Entry**.
4. Enter the following values in the parameters.

Table 4: Advanced Settings > Syslog Server Settings > Add Syslog Entry Page

Parameter	Description
Category	The evaluated configuration requires the Category to `All Events`.
Protocol	The evaluated configuration requires the Protocol to be set to `TLS`.
Syslog URL	The syslog server used for logging UAG events. This value can be an URL, host name or an IP address.

5. Select **Add**.

Table 5: Advanced Settings > Syslog Server Settings Page

Parameter	Description
TLS Syslog Client Certificate	An optional parameter to upload a valid syslog client certificate in the PEM format.
TLS Syslog Client Certificate Key	An optional parameter to upload a valid syslog client certificate key in the PEM format.
Syslog Include System Messages	Turn on this toggle to enable system services such as haproxy, cron, ssh, kernel, and system to send system messages to the syslog server. By default, the toggle is turned off. This setting is not required to be enabled for the evaluated configuration.

6. Select **Save**.

5.3 UAG Generated Audit Events

The following tables provide examples of the audit records generated for the SFRs defined in the Security Target to use as a reference.

Table 6: Sample Audit Record Contents

Requirement	Auditable Events	Example Audit Record
FAU_GEN.1	None.	N/A
FAU_GEN.2	None.	N/A
FAU_STG_EXT.1	None.	N/A
FCS_CKM.1	None.	N/A
FCS_CKM.2	None.	N/A
FCS_CKM.4	None.	N/A
FCS_COP.1/ DataEncryption	None.	N/A
FCS_COP.1/SigGen	None.	N/A
FCS_COP.1/Hash	None.	N/A
FCS_COP.1/ KeyedHash	None.	N/A
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	2023-04-27T19:44:22-04:00 uag2209-2 uag-esmanager: [nioEventLoopGroup-33-1]WARN utils.SyslogManager[operationComplete: 383][][][][] - UAGW00070: Unable to connect to connectionserver.vmware.leidos.ate:443, reason=io.netty.channel.AbstractChannel$AnnotatedNoRouteToHostException: No route to host: connectionserver.vmware.leidos.ate/172.16.23.122:443 retryCount:3, channel:[id: 0x16069dcc]
FCS_RBG_EXT.1	None	N/A
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	2023-04-06T19:38:35-04:00 uag2209-2 uag-esmanager: [nioEventLoopGroup-15-1]ERROR utils.SyslogManager[exceptionCaught: 356][][][][] - UAGE00225: Exception caught while communication to backend on channel: [id: 0x4c15ac24, L:0.0.0.0/0.0.0.0:8128], reason: javax.net.ssl.SSLHandshakeException: Certificate is rejected due to revocation status
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	2023-04-27T19:44:22-04:00 uag2209-2 uag-esmanager: [nioEventLoopGroup-33-1]WARN utils.SyslogManager[operationComplete: 383][][][][] - UAGW00070: Unable to connect to connectionserver.vmware.leidos.ate:443, reason=io.netty.channel.AbstractChannel$AnnotatedNoRouteToHostException: No route to host: connectionserver.vmware.leidos.ate/172.16.23.122:443 retryCount:3, channel:[id: 0x16069dcc]

FCS_TLSS_EXT.2	Failure to establish a TLS Session.	2023-05-05T14:16:10-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag-esmanager: [nioEventLoopGroup-20-2]INFO utils.SyslogManager[write: 199][172.16.23.57][][][943c-***-3d5a-***-2c4f-***-d0f6] - Created session : 943c-***-3d5a-***-2c4f-***-d0f6 2023-05-05T14:16:13-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag-esmanager: [jersey-client-async-executor-8]WARN utils.SyslogManager[logErrorMessage: 326][][][][] - UAGW00095: Auth method(s) failed and no more auth method. Hence sending error response 2023-05-05T14:16:13-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag-esmanager: [jersey-client-async-executor-8]INFO utils.SyslogManager[logMessage: 194][172.16.23.57][][Horizon][943c-***-3d5a-***-2c4f-***-d0f6] - Authentication failed for user null with error Unable to determine revocation status, check failed. Please check if your Certificate Revocation List URL is correct and reachable.. Auth type: CERTIFICATE-AUTH
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	2023-04-07T14:42:42-04:00 uag2209-2 uag-audit: [qtp646757254-28]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_FAILED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=test1: REASON=Incorrect Password. 0 attempts are remaining. 2023-04-07T14:42:43-04:00 uag2209-2 uag-audit: [qtp646757254-54]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_FAILED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=test1: REASON=test1 account is locked. Please try after 5 mins
FIA_PMG_EXT.1	None.	N/A
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Successful authentication (REMOTE) 2023-05-04T18:03:04-04:00 uag2209_short uag-audit: [qtp767764251-54]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_SUCCESS: SOURCE_IP_ADDR=172.16.1.50: USERNAME=cctester (CONSOLE) 2023-05-08T14:50:17-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[12914]: pam_unix(login:session): session opened for user root by root(uid=0) Unsuccessful authentication (REMOTE) 2023-05-04T18:02:31-04:00 uag2209_short uag-audit: [qtp767764251-54]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_FAILED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: REASON=Incorrect Password. 2 attempts are remaining (CONSOLE 2023-05-08T14:51:46-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[23129]: pam_unix(login:auth): authentication

		failure; logname=root uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=root 2023-05-08T14:51:51-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[23129]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failure
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Successful user login (REMOTE) 2023-05-04T18:03:04-04:00 uag2209_short uag-audit: [qtp767764251-54]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_SUCCESS: SOURCE_IP_ADDR=172.16.1.50: USERNAME=cctester (CONSOLE) 2023-05-08T14:50:17-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[12914]: pam_unix(login:session): session opened for user root by root(uid=0) Unsuccessful user login (REMOTE) 2023-05-04T18:02:31-04:00 uag2209_short uag-audit: [qtp767764251-54]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_FAILED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: REASON=Incorrect Password. 2 attempts are remaining (CONSOLE 2023-05-08T14:51:46-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[23129]: pam_unix(login:auth): authentication failure; logname=root uid=0 euid=0 tty=/dev/tty1 ruser= rhost= user=root 2023-05-08T14:51:51-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc login[23129]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failure
FIA_UAU.7	None.	N/A
FIA_X509_EXT.1 /Rev	Unsuccessful attempt to validate a certificate.	2023-04-06T19:38:35-04:00 uag2209-2 uag-esmanager: [nioEventLoopGroup-15-1]ERROR utils.SyslogManager[exceptionCaught: 356][][][][] - UAGE00225: Exception caught while communication to backend on channel: [id: 0x4c15ac24, L:0.0.0.0/0.0.0.0:8128], reason: javax.net.ssl.SSLHandshakeException: Certificate is rejected due to revocation status
	Any addition, replacement, or removal of trust anchors in the TOE's trust store.	(Trust anchor addition) 2023-04-07T20:45:48-04:00 uag2209-2 uag-audit: [qtp646757254-26]INFO utils.SyslogAuditManager[logAuditLog: 469] - CONFIG_CHANGE: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: CHANGE=Syslog CA Certificate details: #012[Subject:CN=VMware-Horizon-Int-CA-T1-CRL-384; Issuer:CN=VMware-Horizon-Root-CA-384; SN:2195994904820209359; Expiry:2032-04-28 13:02:00;

		SHA256Thumbprint:2e11b5f512109cffe395aa409a4093aabbeaaf5c1417c86aeb25490b0d7bb97d]#012[Subject:CN=VMware-Horizon-Int-CA-T1-CRL-384; Issuer:CN=VMware-Horizon-Root-CA-384; SN:2195994904820209359; Expiry:2032-04-28 13:02:00; SHA256Thumbprint:2e11b5f512109cffe395aa409a4093aabbeaaf5c1417c86aeb25490b0d7bb97d]]
FIA_X509_EXT.2	None.	N/A
FIA_X509_EXT.3	None.	N/A
FMT_MOF.1/Function	None.	N/A
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	2023-04-03T13:00:32-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Applying any package updates available 2023-04-03T13:00:33-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Fetching update info from location : https://172.16.23.140/uag/22.09.2/updates-fips.json
FMT_MTD.1/CoreData	None.	N/A
FMT_MTD.1/CryptoKeys	None.	N/A
FMT_SMF.1	All management activities of TSF data.	Refer to Table 7 below.
FMT_SMR.2	None.	N/A
FPT_APW_EXT.1	None.	N/A
FPT_SKP_EXT.1	None.	N/A
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process.	2023-04-07T20:49:17-04:00 uag2209-2 [2023-04-07T20: 49:16.377Z] [debug] [timeSync] [453] TimeSync_PLLUpdate : off 0 freq -1529946 maxerr 0 esterr 0 status 1 const 4 precision 1 tolerance 32768000 tick 10000
FPT_TST_EXT.1	None.	N/A
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	2023-04-03T13:00:32-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Applying any package updates available 2023-04-03T13:00:33-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Fetching update info from location : https://172.16.23.140/uag/22.09.2/updates-fips.json 2023-04-03T13:00:33-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Received updates json. Refresh tdnf metadata cache before package update

		2023-04-03T13:00:33-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Package for update: consul-1.9.15-8.ph3.x86_64 2023-04-03T13:00:40-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Updated package: consul-1.9.15-8.ph3.x86_64 2023-04-03T13:00:40-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Updated 1 packages 2023-04-03T13:00:41-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc uag_pkgupdate: Rebooting as there is an update
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	2023-04-07T20:37:10-04:00 uag2209_short login[3529]: pam_unix(login:session): session opened for user root by root(uid=0) 2023-04-07T20:37:40-04:00 uag2209_short login[3529]: pam_unix(login:session): session closed for user root
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	2023-05-04T18:02:52-04:00 uag2209_short uag-audit: [qtp767764251-53]INFO utils.SyslogAuditManager[logSessionAuditLog: 487] - SESSION_DESTROYED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: INFO=HttpSession@1804276350, Active session count for this user is 0
FTA_SSL.4	The termination of an interactive session.	2023-04-24T19:55:16-04:00 uag2209-2 systemd-logind[449]: Session c24 logged out. Waiting for processes to exit. 2023-04-24T19:55:16-04:00 uag2209-2 systemd-logind[449]: Removed session c24.
FTP_ITC.1	None.	N/A
FTP_TRP.1/Admin	Termination of the trusted channel.	2023-04-12T20:11:02-04:00 uag-d06250c4-5516-44fa-b881-f852bb9cb7bc syslog-ng[4065]: Syslog connection broken; fd='33', server='AF_INET(172.16.0.25:65144)', time_reopen='60'

Table 7: FAU_GEN.1 and FMT_SMF.1 Auditable Events

Admin Action	**Example Audit Record**
Ability to configure the access banner.	2023-04-07T20:45:02-04:00 uag2209-2 uag-admin: [qtp646757254-60]INFO utils.SyslogManager[save: 56] - SETTINGS:CONFIG_CHANGED:allowedHostHeaderValues:(null->) - tlsSyslogServerSettings:(null->[]) - sshPublicKeys:(null->[]) - ntpServers:(null->) - adminDisclaimerText:(This is a consent and warning message.->This is a new warning message.) - dnsSearch:(null->) - fallBackNtpServers:(null->) -
Ability to configure the session inactivity time before session termination or locking.	This is done during install. No logs are generated.

Admin Action	Example Audit Record
Ability to configure the authentication failure parameters for FIA_AFL.1.	This is done during install. No logs are generated.
Ability to configure audit behaviour (e.g., modify the behaviour of the transmission of audit data to an external IT entity).	2023-04-07T20:48:21-04:00 uag2209-2 uag-audit: [qtp646757254-61]INFO utils.SyslogAuditManager[logAuditLog: 469] - CONFIG_CHANGE: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: CHANGE=syslogServerSettings:([SyslogServerSettings(syslogCategory=ALL, sysLogType=UDP, syslogUrl=syslog1.leidos.ate, mqttTopic=null, syslogServerCACertPem=null, tlsSyslogServerSettings=null, tlsMqttServerSettings=null), SyslogServerSettings(syslogCategory=ALL, sysLogType=UDP, syslogUrl=syslog2.ate.com, mqttTopic=null, syslogServerCACertPem=null, tlsSyslogServerSettings=null, tlsMqttServerSettings=null), SyslogServerSettings(syslogCategory=ALL, sysLogType=TLS, syslogUrl=null, mqttTopic=null, syslogServerCACertPem=-----BEGIN CERTIFICATE----- (truncated for space)
Ability to manage the cryptographic keys.	2023-04-07T20:45:48-04:00 uag2209-2 uag-audit: [qtp646757254-26]INFO utils.SyslogAuditManager[logAuditLog: 469] - CONFIG_CHANGE: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: CHANGE=Syslog CA Certificate details: #012[Subject:CN=VMware-Horizon-Int-CA-T1-CRL-384; Issuer:CN=VMware-Horizon-Root-CA-384; SN:2195994904820209359; Expiry:2032-04-28 13:02:00; SHA256Thumbprint:2e11b5f512109cffe395aa409a4093aabbeaaf5c1417c86aeb25490b0d7bb97d]#012[Subject:CN=VMware-Horizon-Int-CA-T1-CRL-384; Issuer:CN=VMware-Horizon-Root-CA-384; SN:2195994904820209359; Expiry:2032-04-28 13:02:00; SHA256Thumbprint:2e11b5f512109cffe395aa409a4093aabbeaaf5c1417c86aeb25490b0d7bb97d]
Ability to manage the TOE's trust store and designate X.509v3 certificates as trust anchors.	2023-04-07T20:49:33-04:00 uag2209-2 uag-admin: [qtp646757254-61]INFO utils.SyslogManager[uploadCaCert: 313] - UPLOADING CA CERT PEM: -----BEGIN CERTIFICATE----- [certificate data] #012 with name: certificate-auth
Ability to import X.509v3 certificates to the TOE's trust store.	2023-04-07T20:49:33-04:00 uag2209-2 uag-admin: [qtp646757254-61]INFO utils.SyslogManager[uploadCaCert: 313] - UPLOADING CA CERT PEM: -----BEGIN CERTIFICATE----- [certificate data] #012 with name: certificate-auth
Ability to reset passwords.	2023-05-08T18:50:38-04:00 uag2209-2 uag-audit: [qtp401862395-27]INFO utils.SyslogAuditManager[logAuditLog: 469] - LOGIN_PASSWORD_CHANGED: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: CHANGE=Admin password changed for user: test1
Ability to re-enable an Administrator account.	2023-05-08T18:48:56-04:00 uag2209-2 uag-audit: [qtp401862395-27]INFO utils.SyslogAuditManager[logAuditLog: 469] - CONFIG_CHANGE: SOURCE_IP_ADDR=172.16.1.50: USERNAME=admin: CHANGE=enabled:(false->true)
Ability to configure password policy.	This is done during install. No logs are generated.

Admin Action	Example Audit Record
Ability to configure the access banner.	2023-04-07T20:45:02-04:00 uag2209-2 uag-admin: [qtp646757254-60]INFO utils.SyslogManager[save: 56] - SETTINGS:CONFIG_CHANGED:allowedHostHeaderValues:(null->) - tlsSyslogServerSettings:(null->[]) - sshPublicKeys:(null->[]) - ntpServers:(null->) - adminDisclaimerText:(This is a consent and warning message.->This is a new warning message.) - dnsSearch:(null->) - fallBackNtpServers:(null->) -

5.4 Performing UAG Package Updates

Occasionally, VMware might authorize the update of one or more software packages to rectify a critical vulnerability that affects a specific version of UAG and for which no viable workaround is available. You can configure the UAG to fetch and apply these packages. To see what packages are currently installed on UAG, including the package versions, run "tdnf list installed" on the local console.

To apply package updates to UAG, it is necessary to configure a file server in your environment that the UAG has network access to on the trusted network (i.e. not in a DMZ). Software packages are uploaded by VMware to https://packages.vmware.com and are applied through the following steps:

1. When an update is available (e.g., in response to a VMware security advisory), go to packages.vmware.com and download the updates-fips.json file for UAG and any associated packages.
2. Once the packages have been downloaded, it is necessary to verify their integrity using a SHA-256 checksum (e.g., linux sha256sum command). The SHA-256 hash of each package must be compared against the published value in the JSON file.
3. Once the hash has been validated, place the JSON file and all associated packages on the file server.

Once the packages are placed on the file server, it is necessary to configure UAG to query this server for package updates. This is done through the following steps in the Web UI:

1. From the admin UI Configure Manually section, select.
2. Select the **Advanced Settings > Appliance Updates Settings** gearbox icon.
3. Enter the following values for the parameters described below.

Table 8: Advanced Settings > Appliance Updates Settings

Step/Parameter	Description
Apply Update Scheme	Set to `Apply updates on next boot.`

Step/Parameter	Description
	The default value is `Don't apply updates`. This is the value that should be set when no updates are available. When it is set to `Apply updates on next boot`, the setting will automatically be restored to the default value. Do not set this value to `Apply updates on every boot`. Automatic updates are not claimed for the evaluated configuration of UAG.
OS Updates URL	Enter the location of the file server from which the Photon OS packages are fetched and applied to the UAG.
Appliance Updates URL	Enter the location of the file server from which the UAG authorized OS packages list is fetched and applied to the UAG.
Trusted Certificates	Load any trusted root or intermediate certificates necessary to establish connectivity to the file server. Note that the evaluated configuration does not require a trusted channel to the file server since the Security Administrator is required to manually verify the integrity of updates prior to installation and the source of the update server is within the trusted network.

The update process is then initiated by rebooting UAG; updates are applied during the boot process so UAG's security functionality is unavailable as this occurs. The success or failure of the update can be determined through a review of the audit log; specifically, package-updates.log on the local console displays this information, or the syslog server can be reviewed for the relevant events (see section 5.3 above).