Release Notes for VMware Unified Access Gateway 3.8

Updated on 02/25/2020

Unified Access Gateway | Released on 12 Dec 2019

Check for additions and updates to these release notes.

What is in the Release Notes

The release notes cover the following topics:

What is New in This Release

VMware Unified Access Gateway 3.8 provides the following new features and enhancements:

- Added support for SAML 2.0 third-party identity provider integration for Horizon user authentication
  This feature can be configured for the Horizon SAML authentication and Active Directory password authentication or for the SAML authentication with Horizon True SSO. This feature is supported for Horizon clients and browser-based HTML Access. Third-party identity providers used can be Okta, Ping Identity, and Microsoft Azure Active Directory
- Added support for the Horizon protocol redirect based on JWT (JSON Web Token) claims.
  This feature is used with the forthcoming Horizon Universal Broker and supports an optimized architecture with Horizon protocol access to desktops and RDS hosted apps that are in a different location to the Horizon broker.
- Added support for setting Host Redirect Mappings.
  - The HTTP Host Redirect capability can be used to simplify Horizon load balancing affinity requirements in certain multi VIP UAG environments. After a load balancer selects a UAG appliance, an HTTP redirect is returned so that the Horizon Client connects directly to the selected UAG appliance without further need for load balancer affinity.
  - `Host Redirect Mappings` text box added to Horizon Settings in the UAG Admin UI.

- Added support in the UAG Admin UI and REST API to include a new field, which provides the countdown in number of days until the date of admin password expiry.
  `Password expires in (days)` is shown in the Account Settings page in the UAG Admin UI.
- Added support for defining allow or deny control for multiple error categories in the OPSWAT endpoint compliance checks for Horizon.
  `Show Allowed Status Codes` field added to the Endpoint Compliance Check Provider Settings page in the UAG Admin UI.

- Added support for OPSWAT endpoint compliance checks with Horizon Client on iOS version 5.3.
  This support is in addition to the existing UAG OPSWAT support for Windows and macOS clients.
- Added support for new customized labels for the RADIUS authentication method user prompts to enhance usability.
  The Horizon RADIUS authentication prompt `User name` and `Passcode` label text can be configured on UAG.
- Added support to display UAG SEG (Secure Email Gateway) Health and Diagnostics from the Admin UI
  Health and Diagnostics screens are provided for SEG under the Edge Service Session Statistics section.
- When SEG is configured with the local SSL certificate, the corresponding certificate thumbprint is displayed under the SEG edge services settings.
- Added support for OCSP configuration through PowerShell
- Added support for JWT audience restriction in Horizon Edge service.
  The JWT audience restriction is a security feature provided by UAG to these Edge services. UAG administrators can restrict the JWT audiences accessing Horizon and backend applications.
- `SAML Audiences` settings added to Horizon and Web Reverse Proxy (with Identity Bridging enabled) Edge services settings in the UAG Admin UI.

For more information about these features, see the Documentation Center

Internationalization

The Unified Access Gateway user interface, online help, and product documentation are available in Japanese, French, German, Spanish, Brazilian Portuguese, Simplified Chinese, Traditional Chinese, and Korean. For the complete documentation, go to the Documentation Center.

Compatibility Notes

For more information about the VMware Product Interoperability Matrix, go to http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

UAG Lifecycle Support policy

For information about the UAG Lifecycle Support policy, go to https://kb.vmware.com/s/article/2147313.

Installation and Upgrade

To download Unified Access Gateway, see the Product Download page.

Resolved Issues

- Validation improvements in applying initial configuration settings by using PowerShell.
- If the hostname for SEG (Secure Email Gateway) in the UAG Admin UI does not resolve, then the service failed.
- Setting up network routes by using the UAG Admin UI method did not work for networks specified when using a number of bits not divisible by 8.
- UAG OPSWAT Device Policy check incorrectly granted access when assessment was pending.
  In UAG 3.8, policies for allow or deny for all error categories are configurable.
- The `.ini` and `JSON` files, downloaded from the UAG Admin UI, did not contain the UAG XL (Extra Large) size deployment information.
- Import of rsyslog settings with the client certification and key was not supported
- Thumbprint in `.ini` file downloaded from UAG contained a colon `(:)` mark. PowerShell does not support colon separation.

- The default self-signed TLS server certificate generated on UAG was not usable by Chrome browsers, Safari browsers, or VMware Horizon clients running on Apple macOS 10.15, iOS 13, and Chrome OS 76. This issue occurred after a change in requirements by Apple.

- An issue about an expired password of the "gateway" user with UAG 3.7 and 3.7.1 has been resolved. This affected the Workspace ONE UEM Edge Services and HA configuration.

  For further details about this issue, see the knowledge base article, https://kb.vmware.com/s/article/76424.

Known Issues

- When UAG is set up for Horizon SAML 2.0 authentication, some versions of the Horizon Client for Windows hide the client UI after the desktop or application opens. This prevents the opening of subsequent desktops or applications. However, the URL used to access Horizon through UAG can specify individual desktops or RDSH Apps.

  Workaround: Administrators can create shortcuts on the Horizon server and push them down to the end points on first connection.

- When Horizon SAML 2.0 is used with Horizon True SSO to avoid the initial AD password prompt, if the session is manually locked or locks due to inactivity, the user must either enter their AD password to unlock the session or close the client and reconnect. The Horizon True SSO unlock mechanism currently depends on Workspace ONE Access.

- UAG RADIUS settings using a local hostname can sometimes fail.

  Workaround: Use a hostname in DNS or an IP address.

- Horizon Smart Card authentication fails if there are non-ASCII characters in the X.509 certificate fields.

  Workaround: Use Smart Card certificates with ASCII characters.

- When an application is launched through a desktop shortcut or command-line interface by using `filePath` or `args` parameters that get encoded, then the application launch fails. This issue occurs when UAG integrates with third-party SAML identity provider.

- When using Horizon SAML IDP authentication with Microsoft ADFS, users receive the `HTTP ERROR 500`.

  The SAML metadata XML file is used for configuring SAML trust on UAG. This file is obtained from Microsoft ADFS. The XML file might contain a `SPSSODesriptor` section. This section is not required for UAG and causes the `HTTP ERROR 500`. The UAG esmanager.log displays the `Error on validating assertion` with a ClassCastException as follows:

  ```
  java.lang.ClassCastException:
  org.opensaml.saml.saml2.metadata.impl.SPSSODescriptorImpl cannot be
  cast to
  org.opensaml.saml.saml2.metadata.IDPSSODescriptor
  ```

  Workaround: Before uploading the identity provider's SAML metadata to UAG, edit the XML file to remove the SPSSODescriptor section. This section starts with "<SPSSODescriptor" and ends with "</SPSSODescriptor>" tags.

Trademarks

Glossary

Help

Feedback