Release Notes for VMware Unified Access Gateway 3.6

Unified Access Gateway | Released on 02 July 2019

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

- What's New in This Release
- Internationalization
- Compatibility Notes
- Installation and Upgrade
- Resolved Issues

What's New in This Release

VMware Unified Access Gateway 3.6 provides the following new features and enhancements:

- Secure Email Gateway (SEG) integration with Unified Access Gateway
- Unified Access Gateway support for RADIUS authorization restriction based on the class attribute
- Support public keys for validation of JSON web tokens.
- NTP servers for network time protocol synchronization.
- Simple Network Management Protocol (SNMP) support to collect system statistics, memory, and VMware Tunnel server MIB information by Unified Access Gateway.
- REST API and Admin UI support to add, modify, and delete static routes.

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.

Installation and Upgrade

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

Resolved Issues

- Web Reverse Proxy health check fails with an error.
- When multiple Web Reverse Proxy is given in an INI file, some Web Reverse Proxy does not work in a Unified Access Gateway deployed in Amazon AWS.
- In a PowerShell deployment, an exported JSON file contains random data foridpMediaType although IDP metadata is not uploaded.
- Unified Access Gateway marks the session as unauthenticated while unlocking response processing in Horizon deployment.
- Unified Access Gateway does not retain the query parameters in the location header after rewriting operation.
- Unified Access Gateway fails to update API monitor statistics.
- When accessing Admin UI of Unified Access Gateway in the Microsoft Internet Explorer, the browser attempts to access an external URL to get the browser language.
- Quiesce mode is not applied on a deployed instance of Unified Access Gateway when request payload has 'quiesceMode' set to true.
- Horizon Pass-through Authentication: Any error message given as a response to<get-configuration> is not recognized by the client.
- Unified Access Gateway PowerShell deployment fails if PEM certificate"Bag Attributes" contains a single-quote character.
- High Availability configuration is wiped off from haproxy.conf configuration file on restart triggered by the certificate.
- Bypass High Availability for UDP XML API and UDP WebSocket connections.

Known Issues

- Thumbprint in the INI file downloaded from Unified Access Gateway contains a colon (:) punctuation mark.

  Workaround: None

- DNS search field does not allow the use of custom TLD (top-level domain). For example, .local

  Workaround: Run vami_set_dns command manually

```
    vami_set_dns -s “DNSSEARCH” “DNSADDR”
    ```

    DNSSEARCH : Space separated DNS Search Address

    DNSADDR : Space separated DNS Address

- PowerShell deployment fails to configure Horizon and Web Reverse Proxy if a thumbprint is set to a certain format.

  Workaround: None

- If the Secure Email Gateway container is unable to connect to API server to fetch MEM Configuration, then the container fails to start while setting up Secure Email Gateway. An original error message indicating the reason for failure is not displayed in Appliance Agent logs.

  Workaround: Analyze Secure Email Gateway logs. The log files`installer-script.log` and `v2-seg-installer.log` are available in the folder/**var**/**log**/**vmware**/**docker**/**seg**.

- Static Deployment with multi-NIC does not create a static route for eth0.

  Workaround: Use `routes0=0.0.0.0/0 a.b.c.d` in a multi NIC deployment to force the default gateway to be on eth0.