Expand All

2103

Release Notes

Product Documentation

More Information

2012

2009.1

2009

3.10

3.9.1

3.9

3.8

3.7.2

3.7.1

3.7

Release Notes

Release Notes for VMware Unified Access Gateway 3.7

Product Documentation

More Information

Archived Documentation

Release Notes for VMware Unified Access Gateway 3.7

Updated on 11/03/2019

Unified Access Gateway | Released on 17 Sept 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 3.7 provides the following new features and enhancements:

- Syslog consolidation for all the edge services
- Supports Extra Large Unified Access Gateway deployment with 8 CPU cores and 32 GB RAM
- Support for uploading SEG SSL certificate from Admin UI
- Supports dynamic fetch of the JWT signing public key with `HTTPS GET`
- Improvements in the use of Horizon RADIUS support with Windows SSO for multi-domain environments
- Support for Multicast DNS
  DNS host names ending with .local are reserved for Multicast DNS. For more information about Multicast DNS, see the *Deploying and Configuring VMware Unified Access Gateway* documentation.

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

- This version resolves the issue with VMware Tunnel SNMP MIB not being available after reboot.

Known Issues

- Syslog settings server certificate revocation validation is not done in runtime. If the Syslog server certificate is revoked, then the Unified Access Gateway might still connect to the Syslog server even though the certificate on the server is the revoked certificate.

  Workaround: It is recommended that administrators monitor the certificates used for Syslog servers.

- Import of rsyslog settings with the client certification and key is not working as expected.

  Workaround: None

- Error is displayed and the session is marked as expired which adds to session stats as an inactive session.

  Workaround: None

- Thumbprint in INI file downloaded from Unified Access Gateway contains colon mark. PowerShell does not support colon separation. If the INI file with a colon mark is used, then the WRP instance will not be enabled.

  Workaround: None.

- The INI and JSON files do not contain the `Extra Large` size deployment information.

  Workaround: None

- The default self-signed TLS server certificate generated on Unified Access Gateway might not be usable by Chrome browsers, Safari browsers, or VMware Horizon clients running on macOS 10.15, iOS 13, and Chrome OS 76. This problem can happen because the requirements for trusted TLS server certificates have been changed by Apple in these OS versions. The default self-signed certificates do not currently meet these new requirements. If the connection to Horizon from a client is through an intermediate load balancer or proxy that terminates TLS, the new certificate requirements must also be met on those devices.

  Workaround: VMware generally recommends that the default self-signed TLS server certificate on Unified Access Gateway is replaced by a trusted CA-signed certificate for the environment. This recommendation is always a good security practice. In this situation, as long as the trusted CA-signed certificate meets the new Apple requirements, the problem does not occur. An alternative workaround for macOS and iOS Horizon clients is to set the SSL Configuration to not verify server certificates. For more information on the Apple certificate requirements, see https://support.apple.com/en-us/HT210176