



Release Notes for VMware Unified Access Gateway 3.3

Unified Access Gateway | Released on 22 May 2018

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](#)
- [Known Issues](#)
- [Resolved Issues](#)

What's New in This Release

VMware Unified Access Gateway 3.3 provides the following new features and enhancements:

- **Removed dependency on Network Protocol Profile (NPP)** - It is no longer necessary to set up an NPP or an IP Pool to deploy Unified Access Gateway. Instead, the IPv4 netmask, IPv6 prefix, and default gateway are specified when Unified Access Gateway is deployed. This helps with improved vSphere deployment flexibility.
- **Added support for mixed IPv4 and IPv6 clients**- Unified Access Gateway supports more flexible options for IPv4 and IPv6 networking on each network interface card (NIC). IPv6 clients can now connect to IPv4 back-end infrastructure through Unified Access Gateway.
- Large virtual machine sizing option is applicable for Workspace UEM Deployments (AirWatch, VMware Tunnel, Content Gateway, and Web Reverse Proxy).
- Support for device certificate-based authentication for Web Reverse Proxy edge service.
- Separate audit log file introduced for logging all admin-related activities for an easy security audit.
- Upload of trusted SSL certificates of respective back-end servers is added for Horizon, Web Reverse Proxy, and Content Gateway edge services.
- CRL support for client certificate revocation check is added.

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.

Known Issues

- If you use a self-signed certificate on Unified Access Gateway, you may not be able to access the Horizon desktop with Microsoft Edge Browser.
Workaround: Use a valid domain certificate and use port 443 for Blast external url. Do not use port 8443.
- Deployment of Unified Access gateway through HTML 5 UI of vSphere 6.7 fails. Use Flex UI instead to deploy Unified Access Gateway.
- The Enable Windows SSO setting can be used for Horizon RADIUS authentication in cases where the user enters their AD domain username and password for the RADIUS login username and passcode. This setting then allows Unified Access Gateway to skip the normal Windows password prompt which normally happens after successful RADIUS authentication.

If the Horizon Connection Server is configured with a pre-login disclaimer message, this feature does not work. If a pre-login message is configured on Connection Server then the user will be required to enter their domain password in the subsequent prompt.

Workaround: Configure Unified Access Gateway for pass-through authentication and configure RADIUS on the Connection Server. You can also configure a pre-login message on the Connection Server such as "Use the same user name and password for RADIUS and Windows authentication" setting.

Resolved Issues

- Corruption in IP tables after Unified Access Gateway was rebooted.
- Zookeeper logs keep increasing causing high disk utilization and admin UI becomes inaccessible when disk usage is at 100%.
- vIDM proxy pattern issue for Workspace One app on iOS.
- TLS 1.2 could not be toggled on Admin UI.

Copyright © 2022 VMware, Inc. All rights reserved.