

RELEASE NOTES

NETOPS

VERSION 1.3.5



INTRODUCTION

This is a recommended production software release for NetOps Automation Gateway module.

SUPPORTED PRODUCTS

- NetOps - Automation Gateway

KNOWN ISSUES

- Some devices have limited interactions with Automation Gateway's proxying behavior.

To resolve the limitations with these specific devices, the user should use the HTTP settings menu and enable the setting to open HTTP proxy sessions in a new tab.

The Google Chrome browser is recommended when using the sub-tab workaround.

- Does not support the CM8100

CHANGE LOG

Production release: A production release contains new features, enhancements, security fixes and defect fixes.

Patch release: A patch release contains only security fixes or defect fixes for high priority issues.

1.3.5 (April, 2023)

This is a patch release.

Minimum required versions

- Lighthouse: 21.Q4.0
- Operations manager: 20.Q3.0

Features and Enhancements

- Removed the HTTPS redirect behavior based on the “fortigate”, “meraki” and “redirect” strings.

This has been replaced with a new per-device menu option to configure whether HTTP services should open in a new tab.

This menu can also be used to configure the target route for the proxy (with or without opening in a new tab).

1.3.4 (February, 2023)

This is a patch release.

Minimum required versions

- Lighthouse: 21.Q4.0
- Operations manager: 20.Q3.0

Features and Enhancements

- Fixed an issue affecting the startup of the AG proxy when using the new-tab redirect feature

1.3.3 (September, 2022)

This is a patch release.

Minimum required versions

- Lighthouse: 21.Q4.0
- Operations manager: 20.Q3.0

Features and Enhancements

- Accessibility improvements to raise standards of keyboard support
- Minor interface and input changes to improve user experience and flow when accessing parts of the UI

1.3.2 (June, 2022)

This is a production release.

Minimum required versions

- Lighthouse: 21.Q4.0
- Operations Manager: 20.Q3.0

Features and Enhancements

- Improved verbosity of logging for automation gateway
- Added the ability to open found devices in new tabs, containing strings “meraki”, “fortigate”, or “redirect” in the device name - Please refer to known issues for additional information

1.3.1 (April, 2022)

This is a patch release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q3.0

Features and Enhancements

- Improved reliability of Automation Gateway deployment to dependent Lighthouses

1.3.0 (August 2021)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q3.0

Features and Enhancements

- Added support for in-browser remote desktop access to remote hosts using SSH
- Added support for RDP using Network Level Authentication

1.2.0 (July 2021)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q3.0

Note

- In order to deploy NetOps modules using the offline installer, the Lighthouse should have at least 8GB of disk space available.
- After successful deployment of NetOps modules to Lighthouse, the user will need to redeploy modules on the nodes. This can be done by clicking the refresh button for

each module on Configure -> NetOps Modules page.

Features and Enhancements

- Added support for in-browser remote desktop access to remote hosts (RDP & VNC)
- Discovered devices can now be renamed using the more device actions menu
- Discovered devices can be temporarily deleted using the more devices action menu
- Added a rescan devices button to manually trigger device autodiscovery

Defect Fixes

- Fixed issue where logs were too verbose displaying user information

1.1.0 (January, 2021)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q2.0

Features and Enhancements

- Integrated with reworked Lighthouse roles and permissions

1.0.0 (August, 2020)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q2.0

Features and Enhancements

- Automatic discovery of available network services on remote hosts behind OMxxx nodes
- Proxy access to management GUIs on downstream devices via the Lighthouse UI
- Proxy API requests to downstream devices via Lighthouse using secure access tokens