RELEASE NOTES

NETOPS

VERSION 2.3.3

INTRODUCTION

This is a recommended production software release for NetOps IP Access module.

SUPPORTED PRODUCTS

- NetOps - IP Access

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.

2.3.3 (April, 2023)

This is a patch release.

Minimum required versions

- Lighthouse: 21.Q4.0 (or 22.Q1 for CM8100 support)
- Operations manager: 20.Q3.0
- Console Server: 4.5.0

Features and Enhancements

- Resolved an issue affecting access to LAN and WAN zones that had previously been renamed

2.3.2 (September, 2022)

This is a patch release.

Minimum required versions

- Lighthouse: 21.Q4.0 (or 22.Q1 for CM8100 support)
- Operations manager: 20.Q3.0
- Console Server: 4.5.0

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
- Aligned module naming convention from *Software Defined Infrastructure* to *IP Access*

2.3.1 (June, 2022)

This is a production release.

Minimum required versions

- Lighthouse: 21.Q4.0 (or 22.Q1 for CM8100 support)
- Operations Manager: 20.Q3.0
- Console Server: 4.5.0

Features and Enhancements

- Support for CM8100 (requires Lighthouse 22.Q1.0)

Defect Fixes

- Improved the handling of invalid usernames when configuring SDI
- Security enhancements

2.3.0 (July, 2021)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q3.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

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

- Support for Lighthouse 21.Q2.
- Network Access Policies implemented to support user permissions for Zone access with User groups
- Togglable functionality between old Zones and new Network Access Policies for OM devices
- Eth2 support for Opengear devices

Defect Fixes

- Fixed issue where secondary lighthouses had SDI action buttons enabled
- Fixed issue where SDI doesn’t handle edge case of same node id reused without restart

2.2.0 (January, 2021)

This is a production release.

Minimum required versions

- Lighthouse: 20.Q4.0
- Operations Manager: 20.Q2.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

Features

- Integrated with reworked Lighthouse roles and permissions

2.1.0 (May, 2020)

This is a production release.

Minimum required versions

- Lighthouse: 2020.Q2.0

- Operations Manager: 2020.Q2.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

Features and Enhancements

- Add IP Access support for Operations Manager nodes
- Add IP Access support for Lighthouse Multiple Instance feature
- Changed behaviour to no longer automatically sync NetOps Modules on applying a license
- Improve performance of certificate operations

2.0.2 (March, 2020)

This is a patch release.

Minimum required versions

- Lighthouse: 2020.Q1.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

Defect Fixes

- Fix race condition when deploying multiple NetOps modules in succession

2.0.1 (February, 2020)

This is a patch release.

Minimum required versions

- Lighthouse: 2020.Q1.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

Defect Fixes

- Fix ‘Push WAN routes’ advanced option

2.0.0 (February, 2020)

This is a production release.

Minimum required versions

- Lighthouse: 2020.Q1.0
- Console Server: acm700x-4.5.0, acm7004-5-4.5.0, im72xx-4.5.0

Features and Enhancements

- Certificates are now managed independently and may be exported as OpenVPN client configs
- Any OpenVPN client config may connect to any authorized node by adding :node-name to the username during authentication, e.g. adal:acm7004-5
- VPN client traffic is now masqueraded behind the node’s remote IP address and no longer requires a remote subnet IP
- Connected clients can access multiple remote subnets behind the node (this behavior is configurable under Advanced Options)
- When the SDI module is activated, nodes are now automatically enabled for IP

Access
- New UI framework with faster deployment

1.1.2 (October, 2019)

This is a patch release.

Minimum required versions

- Lighthouse: 2019.Q4.0 (bundles SD Infrastructure 1.1.2 by default)
- Console Server: acm700x-4.4.1, acm7004-5-4.4.1, im72xx-4.4.1

Defect Fixes

- Fixed an issue which caused pages not to load in Lighthouse 2019.Q4.0

1.1.1 (July, 2019)

This is a patch release.

Minimum required versions

- Lighthouse: 2019.Q2.0

Defect Fixes

- Fix regression in previous version, allow multiple clients to connect to a single node

1.1.0 (July, 2019)

This is a production release.

Minimum required versions

- Lighthouse: 2019.Q2.2

Features and Enhancements

- Add the name of the node to the downloaded client configuration filename
- Multi-client configuration add/delete, support generating client configurations for multiple nodes at once
- Client configurations are visible to Node Users with corresponding node permissions (requires Lighthouse LH 2019.Q3.0 or later)
- Forward IP Access OpenVPN log to Lighthouse syslog
- Filter out unsupported third party nodes
- Support IP Access to devices on IM72xx-2-24E switch interface (eth2 instead of eth1)

1.0.1 (April, 2019)

This is a patch release.

Minimum required versions

- Lighthouse: 2019.Q2.0

Defect Fixes

- Fix CONFIGURE > IP Access > Enable Nodes state persistence across module upgrades

1.0.0 (April, 2019)

This is a production release.

Minimum required versions

- Lighthouse: 2019.Q2.0

Features

- Centralized IP Access using OpenVPN, to devices on arbitrary Management LAN networks behind IM72xx and ACM7xxx nodes
- Client IP auto assignment from the second-to-top /29 subnet
- Central syslog messages of IP Access configuration and connection events
- Automated client configuration generation
- Web UI management of client configurations
- Two factor client authentication via per-node revokable x.509 certificates and username/password
- Enable/Disable IP Access bridge mode using node Connection Manager
- Support multiple concurrent client connections to nodes