



NVIDIA UFM Enterprise Appliance Software User Manual v1.6.2

Table of Contents

| | | |
|----------|--|-----------|
| 1 | Overview | 6 |
| 2 | Software Download | 7 |
| 3 | Document Revision History | 8 |
| 4 | Technical Support | 9 |
| 5 | Release Notes..... | 10 |
| 5.1 | Changes and New Features | 10 |
| 5.2 | Installation Notes | 10 |
| 5.2.1 | Supported NVIDIA Externally Managed Switches | 10 |
| 5.2.2 | Supported NVIDIA Internally Managed Switches | 10 |
| 5.2.3 | UFM GUI Client Requirements..... | 11 |
| 5.3 | Bug Fixes in This Release | 12 |
| 5.4 | Known Issues in This Release | 12 |
| 5.5 | Changes and New Features History | 12 |
| 5.6 | Bug Fixes History..... | 15 |
| 5.7 | Known Issue History | 18 |
| 6 | Introduction..... | 21 |
| 6.1 | Key Features..... | 21 |
| 7 | Getting Started..... | 22 |
| 7.1 | Obtaining the License | 22 |
| 7.2 | Activating the License | 23 |
| 7.3 | Configuring the Appliance for the First Time | 23 |
| 7.3.1 | Configuring the Management Interface..... | 24 |
| 7.3.2 | Configuring the Back-to-Back Interface | 24 |
| 7.3.3 | Configuring the Fabric Interface | 25 |
| 7.4 | Starting UFM | 25 |
| 7.4.1 | Starting UFM Procedure | 25 |
| 7.4.2 | Logging Into UFM Web UI | 26 |
| 8 | High Availability | 27 |
| 8.1 | High-Availability Configuration | 27 |
| 8.1.1 | Configure HA with VIP (Virtual IP)..... | 28 |
| 8.1.2 | Configure HA without VIP (on a Dual Subnet) | 28 |
| 8.2 | High-Availability Cluster Management..... | 29 |

| | | |
|-----------|---|-----------|
| 9 | Authentication, Authorization and Accounting (AAA) | 31 |
| 9.1 | TACACS+ | 31 |
| 9.2 | Configuring TACACS+ and Performing AAA | 32 |
| 9.2.1 | Configuring TACACS+ on UFM Servers | 32 |
| 9.2.2 | Adding TACACS Users on the Server Side | 32 |
| 10 | Command Line Interface (CLI) | 34 |
| 10.1 | CLI Modes | 34 |
| 10.2 | Prompt and Response Conventions | 35 |
| 10.3 | Using "no" Command Form..... | 35 |
| 10.4 | System Management..... | 35 |
| 10.4.1 | Network Interfaces | 35 |
| 10.4.2 | NTP..... | 42 |
| 10.4.3 | Software Management | 43 |
| 10.4.4 | User Management and AAA | 45 |
| 10.4.5 | Chassis Management..... | 49 |
| 10.4.6 | Operating System License | 50 |
| 10.5 | UFM Commands | 52 |
| 10.5.1 | General | 52 |
| 10.5.2 | UFM License | 55 |
| 10.5.3 | UFM Configuration Management..... | 56 |
| 10.5.4 | Data Management..... | 59 |
| 10.5.5 | Management Interface Monitoring | 60 |
| 10.5.6 | UFM Logs | 61 |
| 10.5.7 | UFM Web Client | 64 |
| 10.5.8 | UFM Audit | 67 |
| 10.5.9 | High-Availability..... | 68 |
| 10.5.10 | UFM Multi-Port SM | 70 |
| 10.6 | InfiniBand Commands | 72 |
| 10.6.1 | OpenSM..... | 72 |
| 10.6.2 | HCA Commands..... | 80 |
| 10.6.3 | Partition | 81 |
| 10.6.4 | NVIDIA SHARP..... | 82 |
| 11 | UFM Enterprise Appliance Upgrade | 87 |
| 11.1 | In-Service Upgrade via CLI..... | 88 |

| | | |
|-----------|---|------------|
| 12 | Troubleshooting | 89 |
| 12.1 | Split-Brain Recovery in HA Installation | 89 |
| 13 | Appendixes..... | 90 |
| 13.1 | Appendix - Chassis Health Monitoring | 90 |
| 13.1.1 | Overview | 90 |
| 13.1.2 | Configuration | 90 |
| 13.2 | Appendix - Secure Boot Activation and Deactivation..... | 90 |
| 13.2.1 | Enabling Secure Boot | 91 |
| 13.2.2 | Disable Secure Boot | 99 |
| 13.3 | Appendix - Deploying UFM Appliance from an ISO File..... | 109 |
| 13.3.1 | Deploying UFM Appliance from an ISO File..... | 109 |
| 13.4 | Appendix - UFM Factory Reset | 129 |
| 13.4.1 | UFM Docker Container Factory Reset | 129 |
| 13.4.2 | UFM Factory Reset via CLI | 130 |
| 13.5 | Appendix - Software Components Upgrade | 131 |
| 13.5.1 | Upgrading UFM Enterprise Appliance Operating System | 131 |
| 13.5.2 | Upgrading All UFM-Related Software Components..... | 135 |
| 13.5.3 | Upgrading Specific UFM-Related Software Component | 136 |
| 14 | Document Revision History | 138 |

You can download a PDF version [here](#).

1 Overview

NVIDIA® UFM® Enterprise Appliance is a powerful platform for managing InfiniBand scale-out computing environments. It is based on Ubuntu 18.04 OS, where the UFM Enterprise software is deployed and running as a Docker container. UFM enables data center operators to efficiently monitor and operate the entire fabric, boost application performance and maximize fabric resource utilization.

2 Software Download

To download the UFM software, please visit [NVIDIA's Licensing Portal](#).

If you do not have a valid license, please fill out the [NVIDIA Enterprise Account Registration](#) form to get a UFM evaluation license.

3 Document Revision History

For the list of changes made to this document, refer to [Document Revision History](#).

4 Technical Support

Customers who purchased NVIDIA products directly from NVIDIA are invited to contact us through the following methods:

- E-mail: Enterprisesupport@nvidia.com
- Enterprise Support page: <https://www.nvidia.com/en-us/support/enterprise>

5 Release Notes

NVIDIA UFM Enterprise Appliance is a powerful platform for managing InfiniBand scale-out computing environments. UFM enables data center operators to efficiently monitor and operate the entire fabric, boost application performance and maximize fabric resource utilization.

5.1 Changes and New Features

| Feature | Description |
|----------------|--|
| UFM SM | New routing algorithm for asymmetric QFT topologies |
| UFM Package | Integrated with UFM version 6.15.2-6 |
| UFM HA Package | Integrated with UFM HA version 5.3.1-2 |
| UFM OS | Integrated with UFM OS version 23.11.18-2 |
| MFT Package | Integrated with MFT version mft-4.26.1-3 |
| MLNX_OFED | Integrated with MLNX_OFED version 23.07-0.5.1 |
| Firmware | Integrated with firmware version XX.38.2104 to resolve HCA overheating issue |

For UFM Enterprise Changes and New Features, please refer to the [UFM Enterprise User Manual](#).

5.2 Installation Notes

5.2.1 Supported NVIDIA Externally Managed Switches

| Type | Model | Latest Tested Firmware Version |
|--------------|--|--------------------------------|
| NDR switches | <ul style="list-style-type: none">MQM9790 | 31.2010.6102 |
| HDR switches | <ul style="list-style-type: none">MQM8790 | 27.2010.6102 |
| EDR switches | <ul style="list-style-type: none">SB7790SB7890 | 15.2010.5108 |
| FDR switches | <ul style="list-style-type: none">SX6025SX6015SX6005 | 11.2000.1142 |

5.2.2 Supported NVIDIA Internally Managed Switches

| Type | Model | Latest Tested OS Version |
|--------------|--|--------------------------|
| NDR switches | <ul style="list-style-type: none">MQM9700 | MLNX-OS 3.11.1014 |
| HDR switches | <ul style="list-style-type: none">MQ8700MCS8500TQ8100-HS2FTQ8200-HS2F | MLNX-OS 3.11.1014 |

| Type | Model | Latest Tested OS Version |
|--------------|--|--------------------------|
| EDR switches | <ul style="list-style-type: none"> • SB7700 • SB7780 • SB7800 • CS7500 • CS7510 • CS7520 | MLNX-OS 3.10.5002 |
| FDR switches | <ul style="list-style-type: none"> • SX6012 • SX6018 • SX6036 • SX6506 • SX6512 • SX6518 • SX6536 • SX1012 • SX6710 • SX6720 • SX1700 • SX1710 | MLNX-OS 3.8.1054 |

For supported HCAs per MLNX_OFED version, please refer to MLNX_OFED Release Notes.

5.2.3 UFM GUI Client Requirements

The platform and GUI requirements are detailed in the following tables:

| Platform | Details |
|----------|---|
| Browser | Edge, Internet Explorer, Firefox, Chrome, Opera or Safari |
| Memory | <ul style="list-style-type: none"> • Minimum: 6 GB • Recommended: 16 GB |

5.2.3.1 MFT Package Version

| Platform | Details |
|----------|--|
| MFT | Integrated with MFT version mft-4.26.1-2 |

5.2.3.2 UFM SM Version

| Platform | Type and Version |
|----------|--|
| SM | UFM package includes SM version 5.17.0 |

5.2.3.3 UFM NVIDIA SHARP Software Version

| Platform | Type and Version |
|---|--|
| NVIDIA® Scalable Hierarchical Aggregation and Reduction Protocol (SHARP)™ | UFM package includes NVIDIA SHARP software version 3.5.1 |

5.3 Bug Fixes in This Release

| Ref # | Description |
|-------|-------------------------------|
| | Description: |
| | Keywords: |
| | Discovered in release: |

Refer to UFM Enterprise Software Release Notes for further [Bug Fixes](#).

5.4 Known Issues in This Release

| Ref# | Issue |
|---------|---|
| 3560659 | <p>Description: Modifying the <code>mtu_limit</code> parameter for [MngNetwork] in <code>gv.cfg</code> does not accurately reflect changes upon restarting UFM.</p> <p>Keywords: <code>mtu_limit</code>, MngNetwork, <code>gv.cfg</code>, UFM restart</p> <p>Workaround: UFM needs to be restarted twice in order for the changes to take effect.</p> <p>Discovered in Release: v1.6.0</p> |
| 3729822 | <p>Description: The Logs API temporarily returns an empty response when SM log file contains messages from both previous year (2023) and current year (2024).</p> <p>Keywords: Logs API, Empty response, Logs file</p> <p>Workaround: N/A (issue will be automatically resolved after the problematic SM log file, which include messages from 2023 and 2024 years, will be rotated)</p> <p>Discovered in Release: v1.6.0</p> |

5.5 Changes and New Features History

| Feature | Description |
|---------------------|---|
| Rev 1.6.1 | |
| AAA TACACS+ Support | Added support for AAA TACACS+. For more information, please refer to Authentication, Authorization and Accounting (AAA) . |
| | Added support for three TACACS+ servers for AAA - with fallback or weighted priority. |
| | Added per command authorization AAA TACACS+ support |

| | |
|-----------------------------------|--|
| | Added IPv6 TACACS server support |
| | Added TACACS+ CLI command to allow the TACACS+ functionality. For more information, refer to TACACS+ . |
| CLI Commands | <p>Added the following CLI commands:</p> <ul style="list-style-type: none"> • In Routing: <ul style="list-style-type: none"> • show {ip ipv6} route • show {ip ipv6} default-gateway • In AAA Methods: <ul style="list-style-type: none"> • aaa authentication login default • show aaa • In TACACS+: <ul style="list-style-type: none"> • tacacs-server • tacacs-server host • show tacacs • In Chassis Management: <ul style="list-style-type: none"> • show files system • show resources • In UFM License: <ul style="list-style-type: none"> • ufm license install • ufm license delete • show ufm license • show files ufm-license • In UFM Configuration Management: <ul style="list-style-type: none"> • ufm configuration delete • ufm configuration export • ufm configuration fetch • ufm configuration import • ufm configuration upload • show files ufm-configuration • High-Availability <ul style="list-style-type: none"> • ufm ha configure • In UFM Multi-Port SM: <ul style="list-style-type: none"> • ufm multi-port-sm • show ufm multi-port-sm • ufm additional-fabric-interfaces • show ufm additional-fabric-interfaces • HCA Commands <ul style="list-style-type: none"> • ib hca-vl15-window • show ib hca-vl15-window • In NVIDIA SHARP: <ul style="list-style-type: none"> • ib sharp dump-files-generation enable • ib sharp dynamic-tree-allocation enable • ib sharp dynamic-tree-algorithm • ib sharp ib-qpc-sl <0-15> • ib sharp ib-sat-qpc-sl <0-15> • ib sharp allocation enable |
| Client Certificate Authentication | Added support for pinning SAN with RegEx. |
| UFM Package | Integrated with UFM version 5.3.0-17 |
| UFM HA Package | Integrated with UFM HA version 6.15.0 |
| UFM OS | Integrated with UFM OS version 23.10.18-9 |
| MFT Package | Integrated with MFT version mft-4.26.0-93 |
| MLNX_OFED | Integrated with MLNX_OFED version 23.07-0.5.1 |
| Firmware | Integrated with firmware version XX.38.2104 to resolve HCA overheating issue |

| Rev 1.5.1 | |
|--------------------------------|---|
| UFM Package | Integrated with UFM version 6.14.1 |
| MFT Package | Integrated with MFT version mft-4.25.0-200 |
| Cable and Transceivers Burning | UFM supports second-source cable transceivers burn. |
| Rev 1.5.0 | |
| Command Line Interface (CLI) | Enhanced CLI commands in the following chapters: <ul style="list-style-type: none"> • In-Service Upgrade • IP Management • UFM data reset • UFM HA nodes |
| In-Service Upgrade | Added support for in-service upgrade in HA configuration. For more information, refer to In-Service Upgrade . |
| UFM Factory Reset | Added support for UFM Factory Reset. For more information, refer to Appendix - UFM Factory Reset . |
| UFM Package | Integrated with UFM version 6.14.0 |
| UFM HA Package | Integrated with UFM HA version 5.1.1-6 |
| UFM OS Package | Integrated with UFM OS version 23.07.18-3 |
| MFT Package | Integrated with MFT version mft-4.25.0-63 |
| Rev 1.4.1 | |
| Command Line Interface (CLI) | Enhanced CLI commands in the following chapters: <ul style="list-style-type: none"> • System Management • UFM Commands • InfiniBand Commands |
| UFM Package | Integrated with UFM version 6.13.2 |
| UFM HA Package | Integrated with UFM HA version 5.1.1 Added support for configuring high-availability with dual-link connectivity for improving the high availability robustness |
| UFM OS Package | Integrated with UFM OS version 2.1.11 |
| MFT Package | Integrated with MFT version mft-4.24.0-72 |
| Appliance OS License | Added appliance OS license mechanism to allow accessing the Shell with "root" permissions |
| Rev 1.3.1 | |
| Command Line Interface (CLI) | Added support for Command Line Interface (CLI) for initial configuration of the appliance |
| UFM Initial Settings | Removed the requirement to set the IPoIB address to the main IB interface used by UFM/SM (gv.cfg → fabric_interface). Refer to Configuring the Fabric Interface |
| UFM Package | Integrated with UFM version 6.12.1 |
| UFM HA Package | Integrated with UFM HA version 5.0.1 Improved UFM HA configuration by setting UFM HA nodes using IP addresses only (removed the need of using hostnames and sync interface names) |

| | |
|-----------------------|--|
| UFM Logical Elements | UFM Logical Elements (Environments, Logical Servers, Networks) views are no longer available |
| UFM OS Package | Integrated with UFM HA version 2.1.7 |
| MFT Package | Integrated with MFT version 4.23.0-104 |
| Rev 1.2.0 | |
| NVIDIA SHARP Software | Updated NVIDIA SHARP software version to v3.1.1. |
| UFM Package | Integrated with UFM version 6.11.0 |
| UFM HA Package | Integrated with UFM HA version 4.0.0 |
| UFM Logical Elements | UFM Logical Elements (Environments, Logical Servers, Networks) views are deprecated and will no longer be available starting from UFM v1.3.0(January 2023 release) |
| Rev 1.1.0 | |
| UFM Package | Integrated with UFM version 6.10.0 |
| UFM HA Package | Integrated with UFM HA version 3.0.0 |
| Chassis Health | Added support for chassis health monitoring |
| Rev 1.0.0 | |
| UFM Package | Integrate with UFM version 6.9.0 |
| UFM HA Package | Integrate with UFM HA version 2.0.0 |
| UFM Plugins | Pluggable platform for advanced functionality and third-party plugins. |

5.6 Bug Fixes History

| Ref# | Description |
|---------|---|
| 3672810 | Description: TACACS+ authorization encounter failure when attempting to execute a command with arguments that are exclusively allowed in the configuration file. |
| | Keywords: TACACS+; Per command Authorization |
| | Discovered in release: 1.6.0 |
| 3673626 | Description: Accessing the CLI requires the entry of the sudo password. |
| | Keywords: CLI; Login; Sudo; Password |
| | Discovered in release: 1.6.0 |
| 3629287 | Description: UFM3.x unstable HCA due to overheating of transceiver |
| | Keywords: HCA overheating |
| | Discovered in release: v1.5.0 |
| 3575882 | Description: UFM event is not generated for a switch down |
| | Keywords: UFM Event, Switch Down |
| | Discovered in release: v1.4.1 |
| 3565820 | Description: The UFM start command does not reflect fabric-related issues (such as "no IB interface is running") |

| Ref# | Description |
|---------|--|
| | Keywords: UFM start |
| | Discovered in release: v1.4.3 |
| 3590777 | Description: After upgrading UFM new telemetry data is not being collected and presented in UI Telemetry tab. |
| | Keywords: Telemetry, Coredump |
| | Discovered in release: 1.15.0 |
| 3549795 | Description: Fixed ufm_ha_cluster status to show DRBD sync status. |
| | Keywords: ufm_ha_cluster, DRBD, Sync Status |
| | Discovered in Release: 1.4.1 |
| 3547517 | Description: Fixed UFM logs REST API returning empty result when SM logs exist on the disk. |
| | Keywords: Logs, SM logs, Empty |
| | Discovered in Release: 1.2.0 |
| 3469639 | Description: Fixed REST RDMA server failure every couple of days, causing inability to retrieve ibdiagnet data. |
| | Keywords: REST RDMA, ibdiagnet |
| | Discovered in Release: 1.3.1 |
| 3499668 | Description: Fixed the replacement or overwriting of the IPv4 default gateway when specifying an IPv6 default gateway |
| | Keywords: IPv4, IPv6, Default Gateway, overwrite |
| | Discovered in Release: 1.4.2 |
| 3499983 | Description: Fixed inability to fetch bootstrap certificate when the user is set to "admin" |
| | Keywords: Bootstrap certificate, "admin" |
| | Discovered in Release: 1.4.1 |
| 3486980 | Description: Rectified inability to upload an image or certificate using user admin |
| | Keywords: Image, Certificate, SCP |
| | Discovered in Release: 1.4.0 |
| 3486981 | Description: Rectified inability to add multiple NTP servers. |
| | Keywords: NTP Server |
| | Discovered in Release: 1.4.0 |
| 3468783 | Description: Fixed UFM version update in /etc/ufm-release upon manual upgrade of UFM CLI |
| | Keywords: UFM CLI version, Update |
| | Discovered in Release: 1.4.0 |
| 3410826 | Description: Rectified inability to modify UFM user password |
| | Keywords: User Password, Update, Fail |
| | Discovered in Release: 1.3.1 |

| Ref# | Description |
|---------|--|
| 3461058 | Description: When using the Dynamic Telemetry API to create a new telemetry instance, the log rotation mechanism will not be applied for the newly generated logs of the UFM Telemetry instance |
| | Keywords: Dynamic, Telemetry, Log-rotate |
| | Discovered in Release: 1.4.0 |
| 3383916 | Description: Fixed Client CTRL+C server disruption |
| | Keywords: Client CTRL+C, Server functionality |
| | Discovered in Release: Rest Over RDMA Image 1.0.0-21 |
| 3375414 | Description: Fixed improper functionality of UFM UI Dashboard |
| | Keywords: UI Dashboard |
| | Discovered in Release: 1.2.0 |
| 3342713 | Description: Fixed UFM Health configuration for periodic restarts of the telemetry |
| | Keywords: UFM Health, Telemetry, Periodic restarts |
| | Discovered in Release: 1.2.1 |
| 3459431 | Description: UFM System Dump cannot be extracted from UFM 3.0 Enterprise Appliance host when running in high-availability mode. |
| | Keywords: System Dump, High-Availability |
| | Discovered in Release: 1.3.1 |
| 3461658 | Description: The network fast recovery configuration (<code>/opt/ufm/files/conf/opensm/fast_recovery.conf</code>) is missing when UFM is deployed in Docker Container mode. |
| | Keywords: Network Fast Recovery; Docker Container; Missing Configuration |
| | Discovered in Release: 1.4.0 |
| 3361160 | Description: Resolved the prolonged UFM upgrade time caused by a large historical Telemetry database table |
| | Keywords: Long Upgrade Time, Historical Telemetry, Database File |
| | Discovered in Release: 1.2.0 |
| 3228547 | Description: Client certificate authentication is not working on UFM Docker container after a Docker container restart |
| | Keywords: Client Certificate Authentication, Ubuntu, Docker |
| | Discovered in Release: 1.1.0 |
| 3143391 | Description: UFM agent port 6306 is blocked |
| | Keywords: UFM Agent |
| | Discovered in Release: 1.0.0 |
| 3116018 | Description: ufm-ha-watcher is not working |
| | Keywords: UFM-HA |
| | Discovered in Release: 1.0.0 |

5.7 Known Issue History

| Ref # | Issue |
|---------------------|---|
| 36 99 41 9 | <p>Description: After remanufacturing the UFM Enterprise Appliance from an ISO file as described in Appendix - Deploying UFM Appliance from an ISO File, rebooting or power cycling the host in High-Availability (HA) mode results in the unsuccessful start of the HA services.</p> <p>Workaround: Change the crontab option in UFM Enterprise Appliance via the OS shell <code>#crontab -e</code>:</p> <pre>@reboot /usr/sbin/netplan apply</pre> <p>to:</p> <pre>@reboot sleep 240 && /sbin/ip link set up dev idrac</pre> <p>Keywords: Reboot; HA; Power Cycle</p> <p>Discovered in Release: 1.6.0</p> |
| N/ A | <p>Description: Execution of UFM Fabric Health Report (via UFM Web UI / REST API) will trigger ibdiagnet to use SLRG register, which might cause some of the Switch and HCA's firmware to get stuck and cause the HCA's ports to stay at "Init" state.</p> <p>Keywords: UFM Fabric Health Report; SLRG; Stuckness</p> <p>Discovered in Release: 1.5.0</p> |
| 35 11 41 0 | <p>Description: Collect system dump for DGX host does not work due to missing sshpass utility.</p> <p>Workaround: Install sshpass utility on the DGX .</p> <p>Keywords: System Dump, DGX, sshpass utility</p> |
| 34 32 38 5 | <p>Description: UFM does not support HDR switch configured with hybrid split mode, where some of the ports are split and some are not.</p> <p>Workaround: UFM can properly operate when all or none of the HDR switch ports are configured as split.</p> <p>Keywords: HDR Switch, Ports, Hybrid Split Mode</p> |
| 34 61 65 8 | <p>Description: After the upgrade from UFM Enterprise Appliance v1.4.0 GA to UFM Enterprise Appliance v1.4.1 FUR, the network fast recovery path in <code>opensm.conf</code> is not automatically updated and remains with a null value (<code>fast_recovery_conf_file (null)</code>)</p> <p>Workaround: If you wish to enable the network fast recovery feature in UFM, make sure to set the appropriate path for the current fast recovery configuration file (<code>/opt/ufm/files/conf/opensm/fast_recovery.conf</code>) in the <code>opensm.conf</code> file located at <code>/opt/ufm/files/conf/opensm</code> , before starting UFM.</p> <p>Keywords: Network fast recovery, Missing, Configuration</p> |
| N/ A | <p>Description: Upgrading the UFM Enterprise Appliance SW while upgrading the UFM Enterprise Appliance OS is not supported.</p> <p>Workaround: Do not use the <code>--appliance-sw-upgrade</code> flag while upgrading the UFM Enterprise Appliance OS. Alternatively, upgrade the UFM Enterprise Appliance SW as described in Software Upgrade</p> <p>Keywords: SW Upgrade; OS Upgrade, <code>--appliance-sw-upgrade</code></p> |

| R e f # | Issue |
|---------------------|---|
| 34 73 60 0 | <p>Description: The UFM Enterprise service is enabled while upgrading the UFM Enterprise Appliance SW on HA mode.</p> <p>Workaround: Disable the UFM Enterprise service after the upgrade in HA mode by running the following command:</p> <pre style="border: 1px solid #ccc; padding: 5px;">systemctl disable ufm-enterprise.service</pre> <p>Keywords: SW Upgrade, HA Mode</p> |
| 33 61 16 0 | <p>Description: Upgrading UFM Enterprise Appliance from versions 1.3.0, 1.2.0 and 1.1.0 results in cleanup of UFM historical telemetry database (due to schema change). This means that the new telemetry data will be stored based on the new schema.</p> <p>Workaround: To preserve the historical telemetry database data while upgrading from UFM Enterprise Appliance version 1.3.0, 1.2.0 and 1.1.0, perform the upgrade in two phases. First, upgrade to UFM Enterprise Appliance v1.2.0, and then upgrade to the latest UFM version (UFM v1.3.0 or newer). It is important to note that the upgrade process may take longer depending on the size of the historical telemetry database.</p> <p>Keywords: UFM Historical Telemetry Database, Cleanup, Upgrade</p> |
| 33 46 32 1 | <p>Description: In some cases, when multiport SM is configured in UFM, a failover to the secondary node might be triggered instead of failover to the local available port</p> <p>Workaround: N/A</p> <p>Keywords: Multiport SM, Failover, Secondary port</p> |
| N/ A | <p>Description: Enabling a port for a managed switch fails in case that port is not disabled in a persistent way (this may occur in ports that were disabled in previous versions of UFM Enterprise Appliance v1.3.0)</p> <p>Workaround: Set "persistent_port_operation=false" in <code>gv.cfg</code> to use non-persistent (legacy) disabling or enabling of the port. UFM restart is required.</p> <p>Keywords: Disable, Enable, Port, Persistent</p> |
| 33 46 32 1 | <p>Description: Failover to another port (multi-port SM) will not work as expected in case UFM was deployed as a docker container</p> <p>Workaround: Failover to another port (multi-port SM) works properly on UFM Bare-metal deployments</p> <p>Keywords: Failover to another port, Multi-port SM</p> |
| 34 85 87 | <p>Description: Replacement of defected nodes in the HA cluster does not work when PCS version is 0.9.x</p> <p>Workaround: N/A</p> <p>Keywords: Defected Node, HA Cluster, pcs version</p> |
| 33 36 76 9 | <p>Description: UFM-HA: If the back-to-back interface is disabled or disconnected, the HA cluster will enter a split-brain state, and the "ufm_ha_cluster status" command will stop functioning properly.</p> <p>Workaround: To resolve the issue:</p> <ol style="list-style-type: none"> 1. Connect or enable the back-to-back interface 2. Run <pre style="border: 1px solid #ccc; padding: 5px;">pcs cluster start --all</pre> <ol style="list-style-type: none"> 3. Follow instructions in Split-Brain Recovery in HA Installation. |

| R e f # | Issue |
|------------------|--|
| | Keywords: HA, Back-to-back Interface |
| N/ A | Description: Running UFM software with external UFM-SM is no longer supported |
| | Workaround: N/A |
| | Keywords: External UFM-SM |

6 Introduction

This manual is intended for system administrators responsible for the installation, configuration, management and maintenance of the software and hardware of UFM Enterprise Appliance. NVIDIA® UFM® Enterprise Appliance is a powerful platform for managing InfiniBand scale-out computing environments.

6.1 Key Features

UFM provides a central management console, including the following main features:

- Pluggable platform for advanced functionality and third-party plugins
- Fabric dashboard including congestion detection and analysis
- Advanced real-time health and performance monitoring
- Fabric health reports
- Threshold-based alerts
- Fabric segmentation/isolation
- Quality of Service (QoS)
- Routing optimizations
- Central device management
- Task automation
- Logging
- High availability
- Daily Report: Statistical information of the fabric during the last 24 hours
- Event management
- Client certificate authentication
- Chassis health monitoring

7 Getting Started

The procedures described on this section assume that you have already installed and powered on your UFM Enterprise appliance according to the instructions in the Hardware Installation Guide.

- [Obtaining the License](#)
- [Activating the License](#)
- [Configuring the Appliance for the First Time](#)
- [Starting UFM](#)

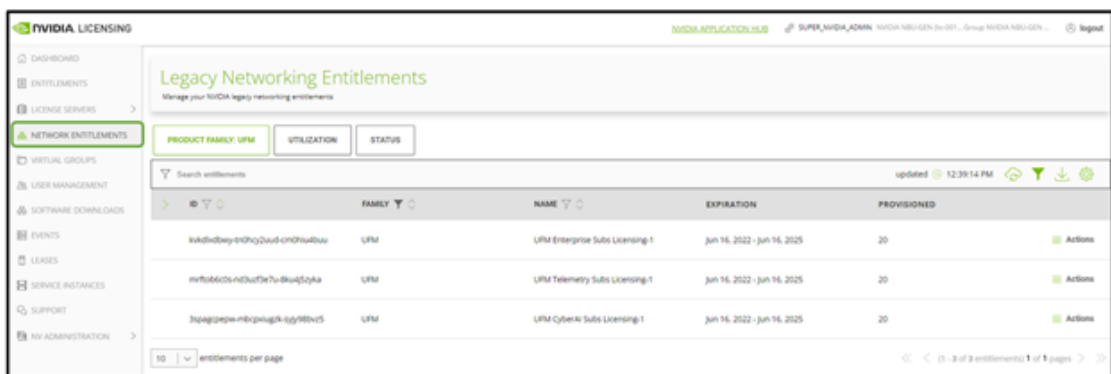
7.1 Obtaining the License

UFM Enterprise Appliance is licensed per managed servers according to the UFM license agreement. When you purchase UFM Enterprise Appliance, you will receive an email with instructions on obtaining your product license. A valid license is a prerequisite for the installation and operation of UFM Enterprise Appliance.

UFM licenses are per managed node and are aggregative. If you install an additional license, the system adds the previous node number and the new node number and manages the sum of the nodes. For example, if you install a license for 10 managed nodes and an additional license for 15 nodes, UFM will be licensed for up to 25 managed nodes.

To obtain the license:

1. Go to NVIDIA's [Licensing and Download Portal](#) and log in as specified in the licensing email you received.
 - If you did not receive your NVIDIA Licensing and Download Portal login information, contact your product reseller.
2. If you purchased UFM directly from NVIDIA and you did not receive the login information, contact enterprisesupport@nvidia.com. Click on the Network Entitlements tab. You'll see a list with the serial licenses of all your software products and software product license information and status.



3. Select the license you want to activate and click on the “Actions” button.
4. In the MAC Address field, enter the MAC address of the delegated license-registered host. If applicable, in the HA MAC Address field, enter your High Availability (HA) server MAC address. If you have more than one NIC installed on a UFM Server, use any of the MAC

addresses.

Manage License File [Close]

Make changes to the license allotment and generate a new file

| ID | NAME | PROVISIONED | EXPIRATION |
|----------------------------------|---------------------------------|-------------|-----------------------------|
| kvkdlxdbwy-tn0hcy2uud-cm0hiu4buu | UFM Enterprise Subs Licensing-1 | 20 | Jun 16, 2022 - Jun 16, 2025 |

minx-ufm-kvkdlxdbwy-tn0hcy2uud-cm0hiu4buu-20220711143558.lic
license file generated Jul 11, 2022 5:37 PM [Download] last downloaded Jul 11, 2022 5:37 PM

MAC Address
24:6e:96:6f:04:6c

Secondary MAC Address (optional)
MAC Address (XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX)

[GENERATE LICENSE FILE] [DOWNLOAD LICENSE FILE]

5. Click on Generate License File to create the license key file for the software.
6. Click on Download License File and save it on your local computer.

If you replace your NIC or UFM server, repeat the process of generating the license to set new MAC addresses. You can only regenerate a license two times. To regenerate the license after that, contact NVIDIA Sales Administration at enterprisesupport@nvidia.com.

7.2 Activating the License

Before starting the UFM software, copy your license file downloaded from NVIDIA's Licensing and Download Portal to the `/opt/ufm/files/licenses` directory.

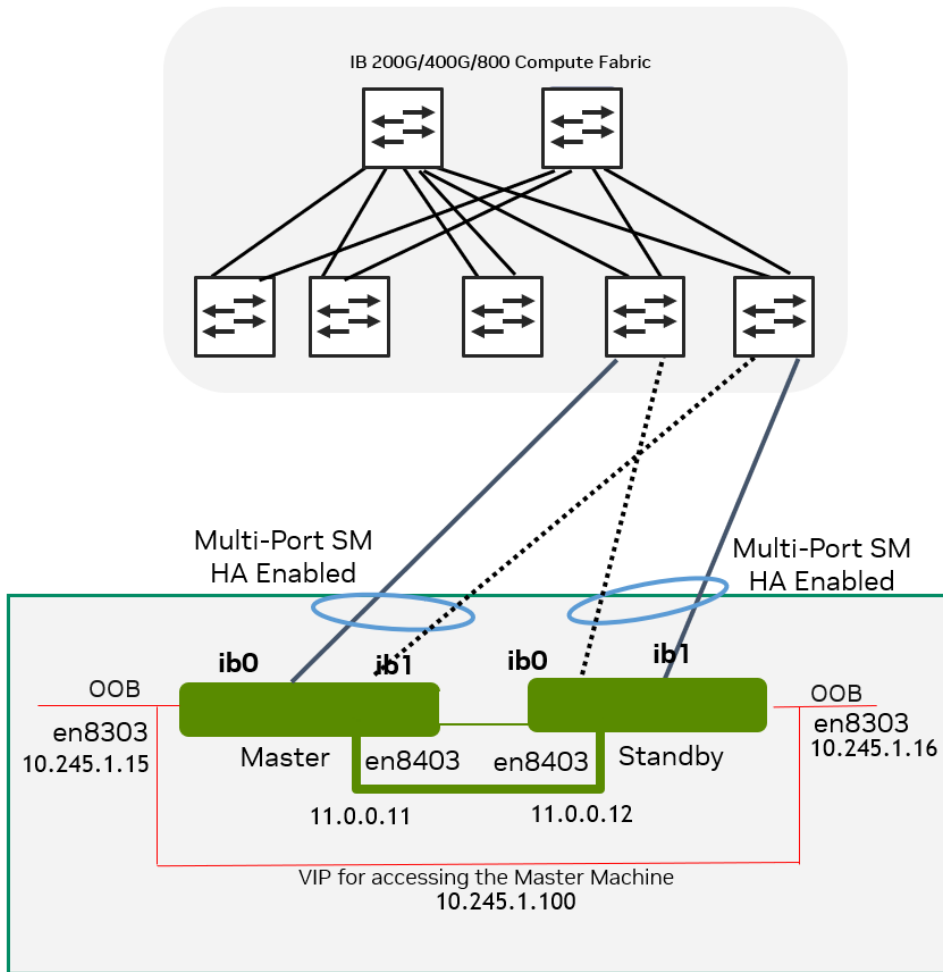
We recommend that you back up the license file.

Your software is now activated.

In a High Availability configuration, the license files are replicated to the standby machine automatically.

7.3 Configuring the Appliance for the First Time

The diagram below describes the connectivity scheme of the UFM High-Availability cluster.



The following are instructions on how to configure the management and fabric (InfiniBand) interfaces in the UFM cluster.

7.3.1 Configuring the Management Interface

The NVIDIA UFM Enterprise Appliance has multiple Ethernet management interfaces. The primary management interface is eno8303. The MAC address for eno8303 is available on the pull tab and can be configured in the DHCP server. To use the remote management controller with DHCP, the free-range IP allocation must be enabled on the DHCP server.

The appliance supports a direct connection via a serial port.

For instructions on how to configure the management interface, please refer to [Configuring the Appliance](#).

7.3.2 Configuring the Back-to-Back Interface

This interface should be used as the primary interface when configuring HA.

When operating in HA configuration, directly connect (back-to-back - without a management switch in the middle) the Master node to the Standby node. To do so, utilize the Ethernet management interface eno8403, as shown in the above diagram.

For your convenience, you may use the CLI command [interface](#) to set a static IP address for eno8403.

Example:

```
interface eno8403 ip address 11.0.0.11 /24
```

7.3.3 Configuring the Fabric Interface

As of UFM Enterprise Appliance v1.3.0 (UFM Enterprise v6.12.0), configuring the fabric interface is optional.

The NVIDIA UFM Enterprise Appliance has multiple InfiniBand interfaces. The primary interface is ib0.

Configure a static IPoIB with Network service (create the file /etc/network/interfaces.d/ifcfg-ib0 and run ifup ib0).

Example of ifcfg-ib0 file definition:

```
auto ib0
iface ib0 inet static
address 10.0.0.12
netmask 255.255.255.0
broadcast 10.0.0.255
```

For your convenience, you may use the CLI command [interface](#) to set a static IP address for ib0.

Example:

```
interface ib0 ip address 192.168.1.11 /24
```

For more details on how to configure the UFM Enterprise, please refer to [UFM Enterprise Initial Configuration](#).

7.4 Starting UFM

7.4.1 Starting UFM Procedure

1. Start the UFM Enterprise service. Run:

```
# systemctl start ufm-enterprise.service
```

2. Wait 1 minute for the service to come up.
3. Ensure the service health. Run:

```
# ufm_enterprise_sanity.sh
Checking Service...
```

```
Done
Checking Images...
Done
Checking Containers...
Done
Checking ufm REST server...
Done
Sanity tests completed successfully!
```

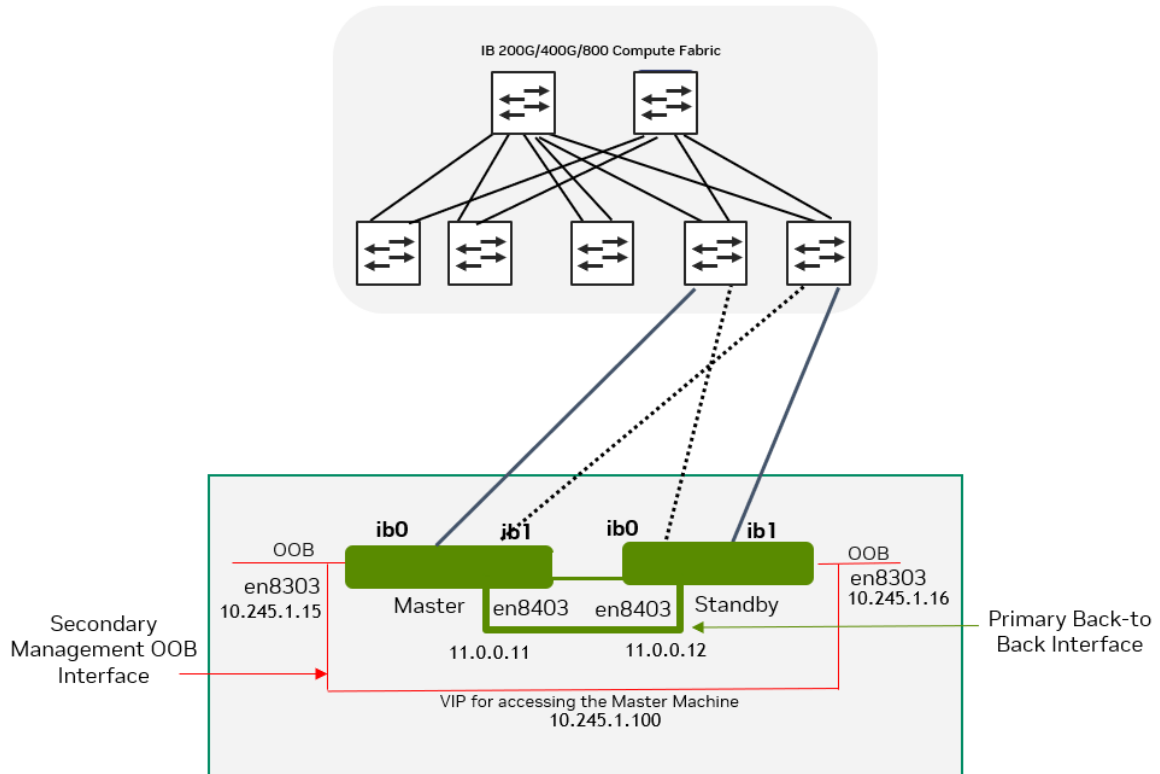
7.4.2 Logging Into UFM Web UI

To open UFM WEB UI, open the following URL in your browser: [https://\[SERVER_IP\]/ufm/](https://[SERVER_IP]/ufm/) and type the default credentials.

8 High Availability

UFM HA supports High-Availability on the host level for UFM Enterprise appliances. The solution is based on a pacemaker to monitor services, and on DRBD to sync file-system states.

The diagram below describes the connectivity scheme of the UFM High-Availability cluster.



8.1 High-Availability Configuration

UFM HA should be configured on two appliances, master and standby.

High-availability should be configured first on on the standby node. When completed, it should be configured on the master node.

Command Usage:

```
# ufm_ha_cluster config --help
Usage: ufm_ha_cluster config [<options>]

The config command configures ha add-on for ufm server.
```

Options:

| Option | Description |
|-------------------------------------|---|
| -r --role <node role> | Node role (master or standby) - Mandatory |
| -e --peer-primary-ip <ip address> | Peer node primary ip address - Mandatory |

| Option | Description |
|--|--|
| -l --local-primary-ip <ip address> | Local node primary ip address - Mandatory |
| -E --peer-secondary-ip <ip address> | Peer node secondary ip address - Mandatory |
| -L --local-secondary-ip <ip address> | Local node secondary ip address - Mandatory |
| -i --virtual-ip <virtual-ip> OR -N --no-vip | Cluster virtual IP <u>OR</u> Do not create virtual IP resource - Mutual exclusive with virtual-IP option One of the two options is mandatory |
| -p --hacluster-pwd <pwd> | hacluster user password - Mandatory |
| -f --ha-config-file <file path> | HA configuration file - The default is ufm-ha.conf |

8.1.1 Configure HA with VIP (Virtual IP)

1. [On Standby Server] Run the following command to configure Standby Server:

```
ufm_ha_cluster config -r standby \
--local-primary-ip <local back-to-back IP> \
--peer-primary-ip <peer back-to-back IP> \
--local-secondary-ip <local management IP> \
--peer-secondary-ip <peer management IP> \
--virtual-ip <virtual management IP used for accessing the master node> \
--hacluster-pwd <password>
```

2. [On Master Server] Run the following command to configure Master Server:

```
ufm_ha_cluster config -r master \
--local-primary-ip <local back-to-back IP> \
--peer-primary-ip <peer back-to-back IP> \
--local-secondary-ip <local management IP> \
--peer-secondary-ip <peer management IP> \
--virtual-ip <virtual management IP used for accessing the master node> \
--hacluster-pwd <password>
```

Alternatively, you can run the CLI command [ufm ha configure](#).

You must wait until after configuration for DRBD sync to finish before starting the UFM cluster. To check the DRBD sync status, run:

```
ufm_ha_cluster status
```

8.1.2 Configure HA without VIP (on a Dual Subnet)

Please change the variables in the commands below based on your setup.

1. [On Standby Server] Run the following command to configure Standby Server:

```
ufm_ha_cluster config -r standby \
--local-primary-ip <local back-to-back IP> \
```

```
--peer-primary-ip <peer back-to-back IP> \  
--local-secondary-ip <local management IP> \  
--peer-secondary-ip <peer management IP> \  
--hacluster-pwd <password> \  
--no-vip
```

2. [On Master Server] Run the following command to configure Master Server:

```
ufm_ha_cluster config -r master \  
--local-primary-ip <local back-to-back IP> \  
--peer-primary-ip <peer back-to-back IP> \  
--local-secondary-ip <local management IP> \  
--peer-secondary-ip <peer management IP> \  
--hacluster-pwd <password> \  
--no-vip
```

Alternatively, you can run the CLI command [ufm ha configure dual-subnet](#).

You must wait until after configuration for DRBD sync to finish before starting the UFM cluster. To check the DRBD sync status, run:

```
ufm_ha_cluster status
```

8.2 High-Availability Cluster Management

- To manage the HA cluster, use the *ufm_ha_cluster* tool.

ufm_ha_cluster Usage

```
# ufm_ha_cluster --help  
=====   
UFM-HA version: 5.3.0-17  
-----   
Usage: ufm_ha_cluster [-h|--help] <command> [<options>]  
This script manages UFM HA cluster.
```

Options:

```
OPTIONS:  
-h|--help          Show this message  
  
COMMANDS:  
version           HA cluster version  
config            Configure HA cluster  
cleanup           Remove HA configurations  
status            Check HA cluster status  
failover          Master node failover  
takeover          Standby node takeover  
start             Start HA services  
stop              Stop HA services  
detach            etach the standby from cluster  
attach            Attach a new standby to cluster  
enable-maintain   Enable maintenance to cluster  
disable-maintain  Disable maintenance to cluster  
reset             Reset DRBD connectivity from split-brain  
is-master         check if the current node is a master  
is-running        check if ufm services are running  
is-ha             Check if running in HA mode
```

- For further information on each command, run:

```
ufm_ha_cluster <command> --help
```

- To check UFM HA cluster status, run:

```
ufm_ha_cluster status
```

- To start the UFM HA cluster, run:

```
ufm_ha_cluster start
```

- To stop the UFM HA cluster, run:

```
ufm_ha_cluster stop
```

- Execute the failover command on the master appliance to become the standby appliance.

Run:

```
ufm_ha_cluster failover
```

- Execute the takeover command on the standby machine to become the master appliance.

Run:

```
ufm_ha_cluster takeover
```

For additional information on configuring UFM HA, please refer to [Installing UFM Server Software for High Availability](#). Since the UFM HA package and related components (i.e. pacemaker and DRBD) are already deployed, follow instructions from step 6 (Configure HA from the main server) and onward.

9 Authentication, Authorization and Accounting (AAA)

AAA is a term describing a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing the system. The UFM Enterprise Appliance switch supports Terminal Access Controller Access Control device Plus (TACACS+) protocol.

- Authentication - authentication provides the initial method of identifying each individual user, typically by entering a valid username and password before access is granted. The AAA server compares a user's authentication credentials with the user credentials stored in a database. If the credentials match, the user is granted access to the network or devices. If the credentials do not match, authentication fails and network access is denied.
- Authorization - following the authentication, a user must gain authorization for performing certain tasks. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for different types of access or activity.
- Accounting - the last level is accounting, which measures the resources a user consumes during access. This includes the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information, and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Authentication, authorization, and accounting services are often provided by a dedicated AAA server, a program that performs these functions.

9.1 TACACS+

TACACS (Terminal Access Controller Access Control System), widely used in network environments, is a client/server protocol that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. TACACS implements the TACACS Client and provides the AAA (Authentication, Authorization and Accounting) functionalities.

TACACS is used for several reasons:

- Facilitates centralized user administration
- Uses TCP for transport to ensure reliable delivery
- Supports inbound authentication, outbound authentication and change password request for the authentication service
- Provides some level of protection against an active attacker

For the list of TACACAS+ CLI commands, please refer to [TACACAS+](#).

9.2 Configuring TACACS+ and Performing AAA

Note: TACACS+ should be configured on two appliances, master and standby.

9.2.1 Configuring TACACS+ on UFM Servers

- Add TACACS server with a key. Run:

```
ufmapl (config) # tacacs-server host 10.209.102.86 key testkey123
```

- [Optional] Review the added server configuration. Run:

```
ufmapl (config) # show tacacs
```

Example:

```
swx-ufm3-06 (config) # show tacacs  
TACACS+ defaults:  
  Timeout      :1  
TACACS+ servers:  
  10.209.102.86:49:  
  Key          : *****
```

- Enable TACACS authentication. Run:

```
ufmapl (config) # aaa authentication login default local tacacs+
```

- [Optional] Review the Authentication and Accounting methods. Run:

```
ufmapl (config) # show aaa
```

Example:

```
swx-ufm3-06 (config) # show aaa  
AAA authorization:  
  Map Order: remote-only  
  
Authentication method(s)L  
  local  
  tacacs+  
  
Accounting method(s)L  
  tacacs+
```

9.2.2 Adding TACACS Users on the Server Side

The predefined "root" and "admin" users are local users, therefore, they can not be defined as remote TACACS+ users.

A simple configuration file is provided below:

```
accounting file = /var/log/tac_plus.acct  
key = testkey123  
user = testuser1 {
```



```

global = cleartext testpass1
service = exec { priv-lvl=15 }
cmd = help { permit .* }
cmd = enable { permit .* }
cmd = configure { permit terminal }
cmd = show {
    permit ufm.*
    deny .*
}
}

user = testuser2 {
global = cleartext testpass2
service = exec { priv-lvl=15 }
cmd = help { permit .* }
cmd = enable { permit .* }
cmd = configure { permit terminal }
cmd = ufm {
    permit "logging .*"
    deny .*
}
cmd = no {
    permit "ufm logging .*"
    deny .*
}
cmd = show { permit .* }
}

user = testuser3 {
default service = permit
global = cleartext testpass3
service = exec { priv-lvl=15 }
}

```

From the above configuration example

- There are 3 TACACS users named `testuser1`, `testuser2` and `testuser3` with respective passwords of `testuser1`, `testuser2` and `testuser3`.
- The secret of the tacacs server is `testkey123`, assuming that this server is running at an IP address of 10.209.102.86. This information is used to register a TACACS server using the `tacacs-host` command in UFMCLI.
- `testuser1` can only execute the `show ufm` commands. Executing any other command is not allowed.
- `testuser2` can execute all show commands and can configure only the `[no] ufm logging` commands.
- `testuser3` can execute all commands since the default service is permit.

10 Command Line Interface (CLI)

UFM Enterprise Appliance is equipped with an industry-standard command line interface (CLI). The CLI is accessed through SSH session or directly through the console port, following login with username (admin) and credentials (admin). Following the initial login, the user is asked to set a new password.

This section explains how to use the CLI of UFM Enterprise Appliance.

Ignored Commands

To support backward compatibility with automation for initial configuration, the following commands are being ignored (they do not output error):

1. `cli default auto-logout 1`
2. `no cli default paging enable`
3. `no cli default progress enable`
4. `no cli default prompt confirm-reload`
5. `no telnet-server enable`
6. `no interface <ifname> dhcp`
7. `no interface <ifname> ipv6 enable`
8. `no interface <ifname> shutdown`
9. `write memory`

10.1 CLI Modes

The CLI has the following modes, and each mode makes available a different set of commands for execution. The different CLI configuration modes are:

| Mode/Context | Description |
|-----------------------------|--|
| standard | When the CLI is launched, it begins in Standard mode. This is the most restrictive mode and only has commands to query a restricted set of state information. Users cannot take any actions that directly affect the system, nor can they change any configuration. |
| enable | The "enable" command moves the user to Enable mode. This mode offers commands to view all state information and take actions like rebooting the system, but it does not allow any configuration to be changed. Its commands are a superset of those in Standard mode. To return to Standard mode, enter "exit". |
| config | The "configure terminal" command moves the user from Enable mode to Config mode. This mode has a full unrestricted set of commands to view anything, take any action, or change any configuration. Its commands are a superset of those in Enable mode. To return to Enable mode, enter "exit". Note that moving directly from/to Standard mode to/from Config mode is impossible. |
| config interface management | Configuration mode for management interfaces |

10.2 Prompt and Response Conventions

The prompt always begins with the hostname of the system. What follows depends on what command mode the user is in. To demonstrate by example, assuming the machine name is "ufm-enterprise-app", the prompts for each of the modes are:

```
ufm-enterprise-app >           (Standard mode)
ufm-enterprise-app #           (Enable mode)
ufm-enterprise-app (config) #   (Config mode)
```

The following session shows how to move between command modes:

```
ufm-enterprise-app >           (You start in Standard mode)
ufm-enterprise-app > enable     (Move to Enable mode)
ufm-enterprise-app #           (You are in Enable mode)
ufm-enterprise-app # configure terminal (Move to Config mode)
ufm-enterprise-app (config) #   (You are in Config mode)
ufm-enterprise-app (config) # exit (Exit Config mode)
ufm-enterprise-app #           (You are back in Enable mode)
ufm-enterprise-app # exit       (Exit Enable mode)
ufm-enterprise-app >           (You are back in Standard mode)
```

Commands entered do not print any response and simply show the command prompt after you press <Enter>.

10.3 Using "no" Command Form

Several config commands feature a "no" form whose purpose is to reset a parameter value to its inherited or default value, or to disable a configuration.

10.4 System Management

10.4.1 Network Interfaces

This section describes the commands that configure and monitor the network interface.

10.4.1.1 Interface

10.4.1.1.1 interface

| | | |
|--------------------|--|---------------------------------------|
| | interface <eno8303 eno8403 eno12399np0 eno12409np1 ib0 ib1 ib2 ib3> Enters a network interface context. | |
| Syntax Description | eno8303 | Management port 0 (out of band) |
| | eno8403 | Management port 1 (out of band) |
| | eno12399np0 | Management port 2 (out of band) |
| | eno12409np1 | Management port 3 (out of band) |
| | ib0 | InfiniBand interface 0 |
| | ib1 | InfiniBand interface 1 |
| | ib2 | InfiniBand interface 2 (UFM 3.0 only) |

| | | |
|--------------------|--|---------------------------------------|
| | ib3 | InfiniBand interface 3 (UFM 3.0 only) |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.3.0 | |
| Example | <pre>ufmapl (config) # interface eno8303 ufmapl (config interface eno8303) #</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.1.1.2 show interfaces

| | | |
|--------------------|--|--|
| | show interfaces [eno8303 eno8403 eno12399np0 eno12409np1 ib0 ib1 ib2 ib3] Displays information about the network interfaces. | |
| Syntax Description | eno8303 | Management port 0 (out of band) |
| | eno8403 | Management port 1 (out of band) |
| | eno12399np0 | Management port 2 (out of band) |
| | eno12409np1 | Management port 3 (out of band) |
| | ib0 | InfiniBand interface 0 |
| | ib1 | InfiniBand interface 1 |
| | ib2 | InfiniBand interface 2 (UFM 3.0 only) |
| | ib3 | InfiniBand interface 3 (UFM 3.0 only) |
| Default | N/A | |
| Configuration Mode | enable | |
| History | 1.6.0 | Updated example and added command syntax |
| | 1.4.1 | First release |

| | |
|------------------|---|
| Example | <pre> swx-ufm3-06 # show interfaces eno8303 Interface eno8303 status: Comment : Admin up : yes Link up : yes DHCP running : yes IP address : 10.209.36.101 Netmask : 255.255.252.0 IPv6 enabled : yes Autoconf enabled : N/A Autoconf route : N/A Autoconf privacy : N/A DHCPv6 running : yes IPv6 addresses : 2 IPv6 address: fcfc:fcfc:209:36:b27b:25ff:fee9:30c8/64 fe80::b27b:25ff:fee9:30c8/64 Speed : 1000Mb/s (auto) Duplex : Full (auto) Interface type : ethernet Interface source : physical MTU : 1500 HW address : b0:7b:25:e9:30:c8 Rx: 6109552397 bytes 45457113 packets 36881549 mcast packets 295 discards 0 errors 0 overruns 0 frame Tx: 242521186 bytes 1211397 packets 0 discards 0 errors N/A overruns 0 carrier 1211397 collisions 1000 queue len </pre> |
| Related Commands | interface <ifname> ip address <IP address> <netmask> |
| Notes | |

10.4.1.1.3 ip address

| | | |
|--------------------|---|---------------------------|
| | ip address <IP address> <netmask> Sets the IP address and netmask of this interface. | |
| Syntax Description | IP address | IPv4 address |
| | netmask | Subnet mask of IP address |
| Default | N/A | |
| Configuration Mode | config interface | |
| History | 1.3.0 | |
| Example | <pre> ufmapl (config interface eno8303) # ip address 10.10.10.10 255.255.255.0 </pre> | |
| Related Commands | interface | |
| Notes | The command sequence is important. The <code>ip address</code> command should be used first during automation since it clears both default-gateway and name-server settings | |

10.4.1.1.4 ipv6 address

| | | |
|--------------------|---|---|
| | ipv6 address <IPv6 address>/<netmask> Configures static IPv6 address and netmask to this interface, static option is possible. | |
| Syntax Description | IPv6 address/netmask | Configures a static IPv6 address and netmask. Format example: 2001:db8:1234::5678/64. |
| Default | N/A | |
| Configuration Mode | config interface management | |
| History | 1.3.0 | |
| Example | <pre>ufmapl (config interface eno8303)# ipv6 address fe80::202:c9ff:fe5e:a5d8/6</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.1.2 Hostname

10.4.1.2.1 hostname

| | | |
|--------------------|---|--------|
| | hostname <hostname> Sets a static system hostname. | |
| Syntax Description | hostname | String |
| Default | | |
| Configuration Mode | config | |
| History | 1.3.0 | |
| Example | <pre>ufmapl(config) # hostname ufmapl-hostname</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.1.2.2 ip name-server

| | | |
|--------------------|---|--------------|
| | ip name-server <no ip name-server> no ip name-server Configures DNS servers to be used. The no form of the command clears the name server. | |
| Syntax Description | IPv4 address | IPv4 address |
| | IPv6 address | IPv6 address |
| Default | No server name | |
| Configuration Mode | config | |

| | | |
|------------------|---|--|
| History | 1.4.2 | Updated command description and added the a no form of the command |
| | 1.3.0 | First release |
| Example | ufmap1 (config)# ip name-server 9.9.9.9 | |
| Related Commands | N/A | |
| Notes | The command sequence is important. The <code>ip name-server</code> command should be used during automation, after running the <code>ip address</code> and the <code>ip default-gateway</code> commands | |

10.4.1.2.3 {ip | ipv6} host

| | | |
|--------------------|---|----------------------|
| | <pre>{ip ipv6} host <hostname> <ip-address></pre> <pre>no {ip ipv6} host <hostname> <ip-address></pre> Sets the static domain name. The no form of the command clears the domain name. | |
| Syntax Description | hostname | String |
| | ip-address | IPv4 or IPv6 address |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.5.0 | |
| Example | <pre>ufmap1 (config)# ip host test-host 1.2.3.4</pre> <pre>ufmap1 (config)# ipv6 host my-ipv6-host 2001::8f9</pre> | |
| Related Commands | show hosts | |
| Notes | | |

10.4.1.2.4 show hosts

| | |
|--------------------|---|
| | <pre>show hosts</pre> Displays hostname, DNS configuration, and static host mappings. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Any configuration mode |
| History | 1.4.0 |

| | |
|------------------|---|
| Example | <pre> ufmapl (config) # show hosts Hostname: swx-ufm3-02 Name servers: 10.211.0.124 (on eno8303) 10.211.0.121 (on eno8303) 10.7.77.135 (on eno8303) Domain names: mtr.labs.mlnx (on eno8303) Static IPv4 host mappings: 127.0.0.1 --> localhost Static IPv6 host mappings: ::1 --> localhost ::1 --> ip6-localhost ::1 --> ip6-loopback ff02::1 --> ip6-allnodes ff02::2 --> ip6-allrouters </pre> |
| Related Commands | N/A |
| Noes | N/A |

10.4.1.3 Routing

10.4.1.3.1 ip default-gateway

| | | |
|--------------------|--|---|
| | <code>ip default-gateway <address></code> <code>no ip default-gateway <address></code> Configures a static default route. The no form of the command removes the static route. | |
| Syntax Description | address | gateway IPv4 or IPv6 address |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.2 | Updated syntax description and added a no form of the command |
| | 1.3.0 | First release |
| Example | ufmapl (config)# ip default-gateway 10.209.36.1 | |
| Related Commands | N/A | |
| Notes | The command sequence is important. The <code>ip default-gateway</code> command should be used during automation, after running the <code>ip address</code> command as it requires a static IP setting | |

10.4.1.3.2 ipv6 default-gateway

| | | |
|--------------------|---|----------------------|
| | <code>ipv6 default-gateway <address></code> <code>no ipv6 default-gateway <address></code> Configures a static default route. The no form of the command removes the static route. | |
| Syntax Description | address | gateway IPv6 address |

| | |
|--------------------|--|
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.2 |
| Example | ufmapl (config)# ip default-gateway ::1 |
| Related Commands | N/A |
| Notes | The command sequence is important. The <code>ip default-gateway</code> command should be used during automation, after running the <code>ip address</code> command as it requires a static IP setting |

10.4.1.3.3 show {ip | ipv6} route

| | | |
|--------------------|--|---|
| | show {ip ipv6} route [static] Displays the routing table in the system. | |
| Syntax Description | static | Filters the table with the static route entries |
| Default | N/A | |
| Configuration Mode | Enable | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # show ip route Destination Mask Gateway Interface Source default 0.0.0.0 10.209.36.1 eno8303 dhcp 10.209.36.0 255.255.252.0 0.0.0.0 eno8303 interface 10.209.36.1 255.255.255.255 0.0.0.0 eno8303 dhcp 169.254.1.0 255.255.255.0 0.0.0.0 idrac interface 172.17.0.0 255.255.0.0 0.0.0.0 docker0 interface</pre> | |
| Related Commands | {ip ipv6} route | |
| Notes | | |

10.4.1.3.4 show {ip | ipv6} default-gateway

| | | |
|--------------------|--|--|
| | show {ip ipv6} default-gateway [static] Displays the default gateway. | |
| Syntax Description | static | Displays the static configuration of the default gateway |
| Default | N/A | |
| Configuration Mode | Enable | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # show ip default-gateway Active default gateways: 10.209.36.1 (interface: eno8303)</pre> | |
| Related Commands | {ip ipv6} default-gateway | |

| | |
|-------|--|
| Notes | |
|-------|--|

10.4.2 NTP

10.4.2.1 ntp enable

| | | |
|--------------------|---|--|
| | ntp enable Enables NTP. | |
| Syntax Description | N/A | |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.3.0 | |
| Example | <pre>ufmap1 (config) # ntp enable</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.2.2 ntp server

| | | |
|--------------------|--|--|
| | ntp server <address> no ntp server <address> Configures an NTP server The no form of the command removes NTP server | |
| Syntax Description | address | IPv4 or IPv6 address |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.2 | Updated the command description and added a no form of the command |
| | 1.3.0 | First release |
| Example | <pre>ufmap1 (config) # ntp server 10.10.10.10</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.2.3 ntp peer

| | | |
|--------------------|--|----------------------|
| | ntp peer <address> no ntp peer <address> Configures an NTP peer The no form of the command removes the NTP peer | |
| Syntax Description | address | IPv4 or IPv6 address |

| | | |
|--------------------|---|----------------------------------|
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.2 | Added the no form of the command |
| | 1.3.0 | First release |
| Example | <pre>ufmapl (config) # ntp peer 11.11.11.11</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.3 Software Management

10.4.3.1 image fetch

| | | |
|--------------------|--|--|
| | image fetch <URL> Downloads a system image from a remote host. | |
| Syntax Description | URL | HTTPS, SCP and SFTP are supported Example: scp://username[:password]@hostname/path/filename |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.5.0 | |
| Example | <pre>ufmapl (config) # image fetch scp://root:123456@192.168.10.125/tmp/ ufm-appliance-1.5.0-6-omu.tar 100.0% [#####] #####</pre> | |
| Related Commands | show images | |
| Notes | <ul style="list-style-type: none"> The image format must be as follows: ufm-appliance-<version>-omu.tar Please delete the previously available image, prior to fetching the new image See section UFM Enterprise Appliance In-Service Upgrade | |

10.4.3.2 image install

| | | |
|--------------------|--|--------------------------|
| | image install <image-name> Installs an image file. | |
| Syntax Description | image name | Specifies the image name |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.5.0 | |

| | |
|--------------------------------|--|
| <p>Example</p> | <pre>ufmapl (config) # image install ufm-appliance-1.5.0-6-omu.tar Verifying image... Extracting image... Installing image... 20230809-07_24_52: UFM-OS UPGRADE to version 23.07.18-3 STARTED 20230809-07_24_52: UFM_OS_UPGRADE [STARTED] WARNING!!! /tmp/ufm_os_upgrade_ml2ah98f/ufm-appliance-1.5.0-4-omu/ufm-os-upgrade.sh will require a restart upon completion. OFED drivers, kernel and kernel models will not work properly until the server is rebooted!!! In case of a change to the secureboot certificate , a message will be prompted to the screen to indicate that an action is needed when restarting. 20230809-07_24_52: HighAvailability is detected, node role is: stand-by 20230809-07_24_53: Check if ufm-enterprise.service is running 20230809-07_24_53: ufm-enterprise.service is not running, continue with the upgrade 20230809-07_24_53: Extracting ISO... 20230809-07_24_53: CERTIFICATE-VALIDATION [PASSED] 20230809-07_24_54: HA-STANDBY-MODE-ACTIVATE [PASSED] 20230809-07_24_54: Backup HA cluster config to /var/tmp/ ufm_os_upgrade_23_07_18-3/pcs_config_backup_23.07.18-3.tar.bz2 20230809-07_24_55: HA-PREPARATION [PASSED] 20230809-07_24_55: A newer kernel version is detected: 4.15.0-213- generic, installing 20230809-07_25_22: KERNEL-UPGRADE [PASSED] 20230809-07_25_22: Preparing MOFED repo 20230809-07_25_24: MOFED-PREPARATION [PASSED] 20230809-07_25_24: Upgrading UFM-APPLIANCE SW 20230809-07_27_01: Upgrading UFM-APPLIANCE SW finished 20230809-07_27_01: APPLIANCE-UPGRADE [PASSED] 20230809-07_27_01: HA-PACKAGES-UPGRADE [SKIPPED] 20230809-07_27_01: Upgrading telemetry packages... 20230809-07_27_01: TELEMETRY-REQUIREMENTS-UPGRADE [PASSED] 20230809-07_27_06: updating firmware 20230809-07_27_19: FW-UPGRADE [PASSED] 20230809-07_27_19: Upgrading packages... 20230809-07_28_15: PACKAGES-UPGRADE [PASSED] 20230809-07_28_15: Upgrading collection tools... 20230809-07_28_15: Updating FW rules 20230809-07_28_20: FIREWALL-PORTS [PASSED] 20230809-07_28_20: UFMCLI tar is copied to /opt/ufm-os-firstboot to run on next-boot. 20230809-07_28_20: UFMCLI-PREPERATION [PASSED] 20230809-07_28_20: HA-STANDBY-MODE-DEACTIVATE [PASSED] 20230809-07_28_20: UFM-OS-UPGRADE [PASSED] 20230809-07_28_20: UPGRADE finished, kernel modules, OFED and new kernel wont function properly until reboot is performed. 20230809-07_28_20: Please reboot the server. Please check log file for more details: /var/log/ ufm_os_upgrade_23.07.18-3.log Upgrade steps status information: /var/log/ ufm_os_upgrade_23.07.18-3_status.log.</pre> |
| <p>Related Commands</p> | <p>show images</p> |
| <p>Notes</p> | <ul style="list-style-type: none"> • The image should be installed on the standby node only. Installation on the master node is not allowed. • Once the installation is complete, perform system reboot using the command: <pre>reload</pre> |

10.4.3.3 image delete

| | | |
|---------------------------|--|---------------------------------|
| | <p>image delete <image-name> Deletes the specified image file from the hard drive.</p> | |
| <p>Syntax Description</p> | <p>image-name</p> | <p>Specifies the image name</p> |
| <p>Default</p> | <p>N/A</p> | |
| <p>Configuration Mode</p> | <p>config</p> | |

| | |
|------------------|---|
| History | 1.5.0 |
| Example | <pre>ufmapl (config) # image delete ufm-appliance-1.5.0-6-omu.tar</pre> |
| Related Commands | show images |
| Notes | |

10.4.3.4 show images

| | |
|--------------------|--|
| | show image Displays information about the system images and boot parameters. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Any configuration mode |
| History | 1.5.0 |
| Example | <pre>ufmapl (config) # show images Installed images: Partition 1: version: ufm_appliance UFMAPL_1.4.3.1_UFM_6.13.2.5 2023-06-13 08:42:27 x86_64 Images available to be installed: 1: Image : ufm-appliance-1.5.0-6-omu.tar</pre> |
| Related Commands | image delete image fetch image install |
| Notes | |

10.4.4 User Management and AAA

10.4.4.1 User Accounts

10.4.4.1.1 username

| | |
|--------------------|--|
| | username root disable no username root disable Disable logging into root account The no form of the command reenables login into root account |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.1 |
| Example | <pre>ufmapl (config) # username root disable</pre> |

| | |
|------------------|-----|
| Related Commands | N/A |
| Notes | N/A |

10.4.4.1.2 username admin password

| | | |
|--------------------|--|---|
| | username admin password <password> Changes the "admin" user password. | |
| Syntax Description | password | Specifies a password for the user in string form. |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.2 | |
| Example | <pre>ufmapl (config) # username admin password 123456</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.4.4.2 AAA Methods

10.4.4.2.1 aaa authentication login default

| | | |
|--------------------|--|---|
| | aaa authentication login default <auth method> [<auth method>] Sets a sequence of authentication methods. Up to two methods can be configured. | |
| Syntax Description | auth-method | Possible values: <ul style="list-style-type: none"> • local • tacacs+ |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # aaa authentication login default local tacacs+</pre> | |
| Related Commands | show aaa | |
| Notes | Setting tacacs+ as one of the authentication methods enables tacacs. Setting no tacacs+ and only local in the authentication methods disables tacacs. | |

10.4.4.2.2 show aaa

| | |
|--------------------|---|
| | show aaa Displays the AAA configuration. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre> ufmapl [mgmt-sa] (config) # show aaa AAA authorization: Map Order: remote-only Authentication method(s): local tacacs+ Accounting method(s): tacacs+ </pre> |
| Related Commands | aaa authentication login default |
| Notes | |

10.4.4.3 TACACS+

10.4.4.3.1 tacacs-server

| | | |
|--------------------|---|--|
| | tacacs-server {key <secret> timeout <seconds>} no tacacs-server {key timeout} Sets global TACACS+ server attributes. The no form of the command resets the attributes to default values. | |
| Syntax Description | key | Set a secret key (shared hidden text string) known to the system and to the TACACS+ server |
| | timeout | Timeout in seconds (1-60) |
| Default | 1 second | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre> ufmapl (config) # tacacs-server key testkey </pre> | |
| Related Commands | show tacacs tacacs-server host | |
| Notes | Each TACACS+ server can override the global secret parameter using the command "tacacs-server host" | |

10.4.4.3.2 tacacs-server host

| | | |
|--------------------|--|--|
| | tacacs-server host <ip-address> {auth-port <port> key <secret>} no tacacs-server host <ip-address> {auth-port <port>} Configures TACACS+ server attributes. The no form of the command removes the TACACS+ server. | |
| Syntax Description | ip-address | TACACS+ server IP address |
| | auth-port | TACACS+ server UDP port number |
| | key | Set a secret key (shared hidden text string) known to the system and to the TACACS+ server |
| Default | Default TCP port is 49 | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # tacacs-server key testkey</pre> | |
| Related Commands | show tacacs tacacs-server | |
| Notes | <ul style="list-style-type: none"> TACACS+ servers are tried in the order they are configured If the user does not specify a parameter for this configured TACACS+ server, the configuration will be taken from the global TACACS+ server configuration. Refer to "tacacs-server" command. | |

10.4.4.3.3 show tacacs

| | |
|--------------------|---|
| | show tacacs Displays TACACS+ configurations. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # show tacacs TACACS+ defaults: Timeout : 1 TACACS+ servers: 10.209.36.156:49: Key : ***** 1.2.3.4:49: Key : *****</pre> |
| Related Commands | tacacs-server tacacs-server host |
| Notes | |

10.4.5 Chassis Management

10.4.5.1 show resources

| | |
|--------------------|--|
| | show resources Displays system resources. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Any configuration mode |
| History | 1.6.0 |
| Example | <pre> ufmapl (config) # show resources Total Used Free Physical 65400 MB 2719 MB 60585 MB Swap 16252 MB 0 MB 16252 MB Number of CPUs: 64 CPU load averages: 0.16 / 0.08 / 0.04 CPU 1 Utilization: 0% Peak Utilization Last Hour: 0% at 2023-11-05 09:45:01 Avg. Utilization Last Hour: 0% CPU 2 Utilization: 5% Peak Utilization Last Hour: 19% at 2023-11-05 09:45:01 Avg. Utilization Last Hour: 7% ... CPU 64 Utilization: 0% Peak Utilization Last Hour: 1% at 2023-11-05 09:45:01 Avg. Utilization Last Hour: 1% </pre> |
| Related Commands | |
| Notes | |

10.4.5.2 show version

| | | | | | |
|--------------------|--|-------|------------------------|-------|---------------|
| | show version Displays version information for the currently running system image. | | | | |
| Syntax Description | N/A | | | | |
| Default | N/A | | | | |
| Configuration Mode | Any configuration mode | | | | |
| History | <table border="1"> <tr> <td>1.4.2</td> <td>Updated command output</td> </tr> <tr> <td>1.4.0</td> <td>First release</td> </tr> </table> | 1.4.2 | Updated command output | 1.4.0 | First release |
| 1.4.2 | Updated command output | | | | |
| 1.4.0 | First release | | | | |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # show version Product name: ufm_appliance Product release: UFMAPL_1.4.2.2_UFM_6.13.1.1 Build date: 2023-06-04 10:31:42 Version summary: ufm_appliance UFMAPL_1.4.2.2_UFM_6.13.1.1 2023-06-04 10:31:42 x86_64 UFM OS: 2.1.11 UFM CHASSIS HEALTH: 1.0.0-3 UFM HA: 5.1.1-4 UFM CLI: 1.2.0-8 Uptime: 3h 54m CPU load averages: 0.21 / 0.14 / 0.06 Number of CPUs: 64 System memory: 2463 MB used / 58693 MB free / 65400 MB total Swap: 0 MB used / 16252 MB free / 16252 MB total</pre> |
| Related Commands | N/A |
| Notes | N/A |

10.4.5.3 show files system

| | | |
|--------------------|--|---|
| | show files system [detail] Displays usage information of the file systems on the system. | |
| Syntax Description | detail | Displays more detailed information on file-system |
| Default | N/A | |
| Configuration Mode | Any configuration mode | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # show files system Statistics for /var filesystem: Space Total 1649517 MB Space Used 23438 MB Space Free 1626079 MB Space Available 1542216 MB Space Percent Free 98% Inodes Percent Free 99% Statistics for /opt/ufm/files filesystem: Space Total 150105 MB Space Used 294 MB Space Free 149811 MB Space Available 142116 MB Space Percent Free 99% Inodes Percent Free 99%</pre> | |
| Related Commands | | |
| Notes | | |

10.4.6 Operating System License

The following CLI commands relate to the operating system license. For UFM License CLI commands, please refer to [UFM License](#).

license install

| | | |
|--------------------|--|--|
| | license install <url> Installs a UFM appliance OS license file from a remote host. | |
| Syntax Description | url | https, sftp are supported. Example: sftp://username:password@hostname/path/filename |

| | | |
|--------------------|---|--|
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.1 | First release |
| | 1.4.3 | Added the first note in the "Notes" row. |
| Example | <pre>ufmapl (config) # license install sftp://root:root/tmp/nvidia-ufm-os-restricted-3922145848058.lic</pre> | |
| Related Commands | license delete show license | |
| Notes | <ul style="list-style-type: none"> • The license installation is used to access the SHELL in cases where the root account is disabled. For UFM Enterprise license installation, please refer to Activating the UFM Enterprise License. • The license format must be as follow: *.lic • The license installation overrides the existing license, if present. • To generate UFM appliance OS license, the management interface MAC address (eno8303) should be provided to NVIDIA by running the "show interfaces" command. | |

10.4.6.1 license delete

| | |
|--------------------|--|
| | license delete Deletes a UFM appliance OS license file from the hard drive. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.1 |
| Example | <pre>ufmapl (config) # license delete</pre> |
| Related Commands | license install show license |
| Notes | N/A |

10.4.6.2 show license

| | |
|--------------------|--|
| | show license Displays UFM appliance OS license information. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.1 |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # show license Customer ID: NVIDIA RND TESTING SN: 194042963524002 Type: Subscription Status: Valid MAC address: b0:7b:25:e9:79:a2</pre> |
| Related Commands | <pre>license install license delete</pre> |
| Notes | N/A |

10.4.6.3 `_shell`

| | |
|--------------------|--|
| | <p><code>_shell</code> Runs a UNIX command shell such as bash. This shell command replaces the CLI; when the user exits the shell, they will be returned to the CLI.</p> |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.1 |
| Example | <pre>ufmapl # _shell root@ufmapl:~#</pre> |
| Related Commands | <pre>license install license delete show license</pre> |
| Notes | N/A |

10.5 UFM Commands

10.5.1 General

10.5.1.1 `ufm start`

| | |
|--------------------|--|
| | <pre>ufm start no ufm start</pre> <p>Starts UFM. The no form of the command stops UFM.</p> |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.1 |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # ufm start</pre> |
| Related Commands | show ufm status |
| Notes | |

10.5.1.2 show ufm status

| | | |
|--------------------|--|------------------------|
| | show ufm status Displays the status of UFM. The outcome of the command varies according to the working mode. | |
| Syntax Description | N/A | |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.2 | Updated command output |
| | 1.4.0 | First release |

Example

```

ufmapl (config) # show ufm status

Cluster name: ufmcluster
WARNING: corosync and pacemaker node names do not match (IPs used in setup?)
Stack: corosync
Current DC: swx-ufm3-02 (version 1.1.18-2b07d5c5a9) - partition with quorum
Last updated: Thu Jun 1 19:06:57 2023
Last change: Thu Jun 1 19:06:11 2023 by root via crm_resource on swx-ufm3-02

2 nodes configured
5 resources configured

Online: [ swx-ufm3-01 swx-ufm3-02 ]
Full list of resources:

Master/Slave Set: ha_data_drbd_master [ha_data_drbd]
Masters: [ swx-ufm3-01 ]
Slaves: [ swx-ufm3-02 ]
Resource Group: ufmcluster-grp
  ha_data_file_system (ocf::heartbeat:Filesystem): Started swx-ufm3-01
  ufm-ha-watcher (systemd:ufm-ha-watcher): Started swx-ufm3-01
  ufm-enterprise (systemd:ufm-enterprise): Started swx-ufm3-01

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
DRBD_RESOURCE: ha_data
DRBD_CONNECTIVITY: Connected
DISK_STATE: UpToDate
DRBD_ROLE: Primary
PEER_DISK_STATE: UpToDate
PEER_DRBD_ROLE: Secondary
DRBD Sync Status:
version: 8.4.10 (api:1/proto:86-101)
srcversion: 7C5B8378BE913D722F67EFD
0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate C r-----
 ns:9044 nr:159762612 dw:159771656 dr:2813 al:48 bm:0 lo:0 pe:0 ua:0 ap:0
 ep:1 wo:d oos:0

=====
=====
UFM Main Processes
=====
=====
ModelMain Process is : [ Running ]
Opensm Process is : [ Running ]
Unhealthy Ports Process is : [ Running ]
Daily Report Process is : [ Running ]
UFM Health Process is : [ Running ]
UFM Telemetry Process is : [ Running ]
UFM Running
=====
HA Summary
=====
Local
=====
Primary IP 11.0.0.11
Secondary IP 10.209.44.115
DRBD Running Primary
DRBD State ConnectionState = Connected - DiskState = UpToDate
=====
Peer
=====
Primary IP 11.0.0.12
Secondary IP 10.209.44.116
DRBD Running Secondary
DRBD State ConnectionState = Connected - DiskState = UpToDate
=====
swx-ufm3-01 (config) #

```

Related Commands

N/A

Notes

- The output example above is taken from a high-availability setup
 - If working in HA mode, you will receive information on the HA status
- The process status can be one of the below:
- Running - the process is running
 - Stopped - the process is not running

10.5.2 UFM License

10.5.2.1 ufm license install

| | | |
|--------------------|--|---|
| | ufm license install <url> Installs a UFM license file from a remote host. | |
| Syntax Description | url | https, scp and sftp are supported. Example: scp://username[:password]@hostname/path/filename , usb:/path/filename . |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm license install scp://root:123456@10.209.1.21/ tmp/volt-ufm-advanced.lic</pre> | |
| Related Commands | ufm license delete show ufm license | |
| Notes | <ul style="list-style-type: none"> The license format must be as follow: volt-ufm-*.lic, mlnx-ufm-*.lic or nvidia-ufm-*.lic Duplicate license are not permitted. You must delete the previous license before installing the new one. | |

10.5.2.2 ufm license delete

| | | |
|--------------------|--|----------------------|
| | ufm license delete <filename> Deletes a UFM license file from the hard drive. | |
| Syntax Description | filename | UFM license filename |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm license delete volt-ufm-advanced.lic</pre> | |
| Related Commands | ufm license install show ufm license | |
| Notes | | |

10.5.2.3 show ufm license

| | | |
|--------------------|---|--|
| | show ufm license Displays UFM license information. | |
| Syntax Description | N/A | |

| | |
|--------------------|--|
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre> ufmapl (config) # show ufm license ----- Customer ID SN swName Type MAC Address Exp. Date Limit Functionality Status ----- 495760397 123456778 UFM Evaluation NA 2090-11-21 1024 Advanced Valid ----- </pre> |
| Related Commands | ufm license install ufm license delete |
| Notes | |

10.5.2.4 show files ufm-license

| | |
|--------------------|---|
| | show files ufm-license Displays a list of UFM license files |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre> ufmapl (config) # show files ufm-license nvidia-ufm-advanced.lic </pre> |
| Related Commands | ufm license delete |
| Notes | |

10.5.3 UFM Configuration Management

10.5.3.1 ufm configuration delete

| | | |
|--------------------|--|------------------------|
| | ufm configuration delete <zip-file> Deletes a configuration zip file from the hard drive. | |
| Syntax Description | zip-file | Zip filename to delete |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre> ufmapl (config) # ufm configuration delete ufm-config-20121128-180857.zip </pre> | |

| | |
|------------------|---|
| Related Commands | ufm configuration upload ufm configuration import ufm configuration export ufm configuration fetch |
| Notes | |

10.5.3.2 ufm configuration export

| | | |
|--------------------|--|---|
| | ufm configuration export [<zip-file>] Exports UFM configuration to a file (a zip archive). | |
| Syntax Description | zip-file | UFM configuration of exporting the zip file |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm configuration export</pre> | |
| Related Commands | ufm configuration upload ufm configuration import ufm configuration delete ufm configuration fetch | |
| Notes | If no zip file is provided, a zip archive is created with the name: ufm-config-<date>-<time>.zip (e.g. ufm-config-20130327-153314.zip) | |

10.5.3.3 ufm configuration fetch

| | | |
|--------------------|--|--|
| | ufm configuration fetch <url> Downloads UFM configuration files from a remote host or a USB device. | |
| Syntax Description | url | The URL path from where the configuration file can be downloaded. https, scp and sftp are supported. Example: scp://username[:password]@hostname/path/filename |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm configuration fetch usb:/ufmapp/ufmconf1.zip</pre> | |
| Related Commands | ufm configuration upload ufm configuration import ufm configuration export ufm configuration delete | |
| Notes | | |

10.5.3.4 ufm configuration import

| | | |
|--------------------|---|---|
| | ufm configuration import <zip-file> [upgrade] Imports UFM configuration from a file (a zip archive). | |
| Syntax Description | zip-file | Zip filename from which to import |
| | upgrade | Imports UFM-SDN Appliance configuration from a previous version and upgrades it to the latest one |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm configuration import ufm-config-20121128-180857.zip</pre> | |
| Related Commands | ufm configuration upload ufm configuration export ufm configuration delete ufm configuration fetch | |
| Notes | | |

10.5.3.5 ufm configuration upload

| | | |
|--------------------|--|--|
| | ufm configuration upload <filename> <url> Uploads UFM configuration to a remote host or a USB device (a zip archive). | |
| Syntax Description | filename | The UFM configuration of uploading the file name |
| | url | The URL path from where the configuration file can be uploaded. Supported formats: https, scp and sftp. Example: scp://username[:password]@hostname/path/filename |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>ufmapl (config) # ufm configuration upload ufm-config-20121128-180857.zip scp://mlnx:123456@172.30.3.201/tmp</pre> | |
| Related Commands | ufm configuration export ufm configuration import ufm configuration delete | |
| Notes | | |

10.5.3.6 show files ufm-configuration

| | |
|--------------------|---|
| | show files ufm-configuration Displays a list of UFM configuration zip archives. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # show files ufm-configuration ufm-config-20231105-102019.zip</pre> |
| Related Commands | |
| Notes | |

10.5.4 Data Management

10.5.4.1 ufm data reset

| | |
|--------------------|---|
| | ufm data reset Resets the UFM data (both the configuration and the database data). |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.5.0 |
| Example | <pre>ufmapl (config) # ufm data reset This command resets UFM data (configuration and database) and consequently deletes installed web client related certificates. Are you sure you wish to proceed? [yes/no] yes UFM reset to factory defaults finished successfully.</pre> |
| Related Commands | N/A |
| Notes | This command is available in standalone mode only. For resetting UFM in HA mode, refer to no ufm ha . |

10.5.5 Management Interface Monitoring

10.5.5.1 ufm mgmt-interface monitor enable

| | | |
|--------------------|---|--|
| | ufm mgmt-interface monitor enable no ufm mgmt-interface monitor enable Enables monitoring of the management interface. The no form of the command disables monitoring of the management interface. | |
| Syntax Description | N/A | |
| Default | Disabled | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm mgmt-interface monitor enable</pre> | |
| Related Commands | ufm mgmt-interface monitor interval ufm mgmt-interface show ufm mgmt-interface | |
| Notes | | |

10.5.5.2 ufm mgmt-interface monitor interval

| | | |
|--------------------|--|--|
| | ufm mgmt-interface monitor interval <time> Configures the management interface monitoring interval. | |
| Syntax Description | time | The management interface monitoring interval. Range: 5-180 seconds. |
| Default | 10 seconds | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm mgmt-interface monitor interval 15</pre> | |
| Related Commands | ufm mgmt-interface monitor enable ufm mgmt-interface show ufm mgmt-interface | |
| Notes | | |

10.5.5.3 ufm mgmt-interface

| | | |
|--------------------|--|--|
| | ufm mgmt-interface <interface> Configures the management interface to be monitored. | |
| Syntax Description | interface | Management interface to be monitored (e.g. eno8303, eno8403) |
| Default | eno8303 | |

| | |
|--------------------|---|
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ufm mgmt-interface eth0</pre> |
| Related Commands | ufm mgmt-interface monitor enable ufm mgmt-interface monitor interval show ufm mgmt-interface |
| Notes | N/A |

10.5.5.4 show ufm mgmt-interface

| | |
|--------------------|--|
| | show ufm mgmt-interface Displays the management interface settings. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ufm mgmt-interface Management interface monitoring: Interface name: eno8303 Enabled: Yes Monitoring interval: 10 seconds</pre> |
| Related Commands | ufm mgmt-interface monitor enable ufm mgmt-interface monitor interval ufm mgmt-interface |
| Notes | |

10.5.6 UFM Logs

10.5.6.1 show ufm logging

| | |
|--------------------|---|
| | show ufm logging Displays logging configuration. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.4.0 |

| | |
|------------------|--|
| Example | <pre> ufmapl (config) # show ufm logging Number of archived log files to keep: 15 Log rotation size threshold: 100M Ufm-log level: WARNING Syslog: Enabled: No Server: Local Level: WARNING Ufm-log enabled: No Ufm-events enabled: No swx-ufm3-01 (config) # </pre> |
| Related Commands | |
| Notes | |

10.5.6.2 ufm logging syslog enable

| | |
|--------------------|---|
| | <pre> ufm logging syslog enable no ufm logging syslog enable </pre> <p>Enable sending UFM logs to syslog. The no form of the command disables sending UFM logs to syslog.</p> |
| Syntax Description | N/A |
| Default | Disabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre> ufmapl (config) # ufm logging syslog enable </pre> |
| Related Commands | |
| Notes | This change takes effect after UFM restart. |

10.5.6.3 ufm logging syslog

| | |
|--------------------|--|
| | <pre> ufm logging syslog <host:port> no ufm logging syslog </pre> <p>Sends UFM logs to a remote syslog server. The no form of the command sends UFM logs to the local syslog server.</p> |
| Syntax Description | port Remote syslog hostname and port |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre> ufmapl (config) # ufm logging syslog 172.30.36.120:514 </pre> |
| Related Commands | |
| Notes | This change takes effect after UFM restart. |

10.5.6.4 ufm logging syslog ufm-log enable

| | | |
|--------------------|--|--|
| | ufm logging syslog ufm-log enable no ufm logging syslog ufm-log enable Send UFM log messages to a syslog server The no form of the command disables sending UFM log messages to a syslog server | |
| Syntax Description | N/A | |
| Default | Disabled | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm logging syslog enable</pre> | |
| Related Commands | | |
| Notes | This change takes effect after UFM restart. | |

10.5.6.5 ufm logging syslog ufm-events enable

| | | |
|--------------------|---|--|
| | ufm logging syslog ufm-events enable no ufm logging syslog ufm-events enable Send UFM event log messages to a syslog server. The no form disables the ability to log UFM event messages to syslog server | |
| Syntax Description | N/A | |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm logging syslog ufm-events enable</pre> | |
| Related Commands | | |
| Notes | This change takes effect after UFM restart. | |

10.5.6.6 ufm logging level

| | | |
|--------------------|---|---|
| | ufm logging level <log-level> Sets the severity level of certain log messages. | |
| Syntax Description | log-level | <ul style="list-style-type: none"> • CRITICAL - critical conditions • DEBUG - debug-level messages • ERROR - error conditions • INFO - informational messages • WARNING - warning conditions |
| Default | WARNING | |
| Configuration Mode | config | |
| History | 1.6 | |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # ufm logging level WARNING</pre> |
| Related Commands | |
| Notes | |

10.5.7 UFM Web Client

10.5.7.1 ufm web-client mode

| | | |
|--------------------|--|---|
| | ufm web-client mode <http https-client-authentication> Configures Access mode to the UFM web clients. | |
| Syntax Description | https | HTTPS access |
| | https-client-authentication | HTTPS access with client authentication |
| Default | https | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm web-client mode https-client-authen</pre> | |
| Related Commands | show ufm web-client ufm web-client client-authentication ufm web-client associate-user | |
| Notes | | |

10.5.7.2 ufm web-client associate-user

| | | |
|--------------------|---|---|
| | ufm web-client associate-user <san> <username> no ufm web-client associate-user <san> <username> Associates client certificate subject alternative name with a UFM user. The no form of the command disassociates client certificate subject alternative name from a UFM user. | |
| Syntax Description | san | Client certificate subject alternative name |
| | username | UFM username |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm web-client associate-user ufm.mellanoxhpc.net admin</pre> | |

| | |
|------------------|--|
| Related Commands | show ufm web-client ufm web-client mode ufm web-client client-authentication |
| Notes | |

10.5.7.3 show ufm web-client

| | |
|--------------------|---|
| | show ufm web-client Displays UFM web client settings. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre> ufmapl (config) # show ufm web-client Mode: HTTPS Client authentication: Yes Bootstrap certificate file: Present CA certificate file: Present Server certificate file: Present Server certificate hostname: ufm.mellanoxhpc.net User Associations: SAN: ufm.mellanoxhpc.net User: ufmsysadmin Certificate Auto-refresh: Enabled: Yes CA certificate URL: https://mellanox.com/cacert Server certificate URL: https://mellanox.com/servercerts Server certificate thumbprint: 2268BDD79DF7FD9C818EB97F315AE0F35D223A15 Last checked: 2019-04-20 20:57:21 Last update: 2019-04-20 20:57:21 </pre> |
| Related Commands | ufm web-client mode ufm web-client client-authentication ufm web-client associate-user |
| Notes | |

10.5.7.4 ufm web-client client-authentication cert-refresh enable

| | |
|--------------------|--|
| | ufm web-client client-authentication cert-refresh enable no ufm web-client client-authentication cert-refresh enable Enables UFM web client certificates auto-refresh. The no form of the command disables the feature. |
| Syntax Description | N/A |
| Default | Disabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre> ufmapl (config) # ufm web-client client-authentication cert-refresh enable </pre> |
| Related Commands | show ufm web-client |

| | |
|-------|--|
| Notes | |
|-------|--|

10.5.7.5 ufm web-client client-authentication cert-refresh ca-cert

| | | |
|--------------------|---|--|
| | ufm web-client client-authentication cert-refresh ca-cert <download-url> no ufm web-client client-authentication cert-refresh ca-cert <download-url> Sets the download URL for root/intermediate certificate. The no form of the command clears the root/intermediate certificate auto-refresh settings. | |
| Syntax Description | download-url | Download URL for root/intermediate certificate |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.5 | |
| Example | <pre>ufmapl (config) # ufm web-client client-authentication cert-refresh ca-cert "https://mellanox.com/cacerts"</pre> | |
| Related Commands | show ufm web-client | |
| Notes | | |

10.5.7.6 ufm web-client client-authentication cert-refresh server-cert

| | | |
|--------------------|---|---|
| | ufm web-client client-authentication cert-refresh server-cert <url> <thumbprint> no ufm web-client client-authentication cert-refresh server-cert <url> <thumbprint> Sets the download URL for server and bootstrap certificates. The no form of the command clears the server and bootstrap certificates auto-refresh settings. | |
| Syntax Description | url | https and sftp are supported. Example: sftp://username[:password]@hostname/path/filename . |
| | thumbprint | Server certificate thumbprint |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ufm web-client client-authentication cert-refresh server-cert "https://mellanox.com/servercerts" 2268BDD79DF7FD9C818EB97F315AE0F35D223A15</pre> | |
| Related Commands | show ufm web-client | |
| Notes | | |

10.5.7.7 ufm web-client client-authentication cert-refresh run-now

| | |
|--------------------|--|
| | ufm web-client client-authentication cert-refresh run-now Refreshes the server and root/intermediate certificates manually. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ufm web-client client-authentication cert-refresh run-now</pre> |
| Related Commands | show ufm web-client |
| Notes | |

10.5.8 UFM Audit

10.5.8.1 ufm track-conf-changes enable

| | |
|--------------------|---|
| | ufm track-conf-changes enable no ufm track-conf-changes enable Enables UFM configuration changes tracking The no form of the command disables UFM configuration changes tracking |
| Syntax Description | N/A |
| Default | Enabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ufm track-conf-changes enable</pre> |
| Related Commands | show ufm track-conf-changes |
| Notes | |

10.5.8.2 show ufm track-conf-changes

| | |
|--------------------|---|
| | show ufm track-conf-changes Displays UFM configuration changes tracking settings |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |

| | |
|------------------|---|
| Example | <pre>ufmapl (config) # show ufm Track UFM configuration changes: No</pre> |
| Related Commands | <code>ufm track-conf-changes enable</code> <code>no ufm track-conf-changes enable</code> |
| Notes | |

10.5.9 High-Availability

10.5.9.1 ufm ha

| | | |
|--------------------|---|---|
| | <code>ufm ha [failover takeover]</code> Performs High Availability failover/takeover operations. | |
| Syntax Description | <code>failover</code> | Failover can be performed only on master (active) machine |
| | <code>takeover</code> | Takeover can be performed only on slave (standby) machine |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.1 | |
| Example | <pre>ufmapl (config) # ufm ha takeover</pre> | |
| Related Commands | | |
| Notes | | |

10.5.9.2 ufm ha configure

| | | |
|--------------------|---|---|
| | <code>ufm ha configure <standby master> <local primary IP> <peer primary IP> <local secondary IP> <peer secondary IP> <virtual ip> <hacluster-pwd></code> <code>no ufm ha</code> Applies HA configuration. The no form of the command reverts the appliance to a standalone configuration. | |
| Syntax Description | <code>node-role</code> | Master or standby |
| | <code>local-primary-ip</code> | Local node primary IP address |
| | <code>peer-primary-ip</code> | Peer node primary IP address |
| | <code>local-secondary-ip</code> | Local node secondary IP address |
| | <code>peer-secondary-ip</code> | Peer node secondary IP address |
| | <code>virtual ip</code> | Virtual IP used for accessing the active (master) machine |
| | <code>hacluster-pwd</code> | hacluster user password |

| | |
|--------------------|---|
| Default | N/A |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>swx-ufm3-01 (config) # ufm ha configure standby 11.0.0.12 11.0.0.11 10.209.44.12 10.209.44.11 10.209.44.111 123456</pre> |
| Related Commands | |
| Notes | <ol style="list-style-type: none"> 1. The local and peer primary interfaces should be connected directly back-to-back 2. The command must be ran first on standby node and only then on the master node |

10.5.9.3 ufm ha configure dual-subnet

| | | |
|--------------------|--|---------------------------------|
| | <p>ufm ha configure dual-subnet <standby master> <local primary IP> <peer primary IP> <local secondary IP> <peer secondary IP> <hacluster-pwd> no ufm ha Applies HA configuration for dual-subnet. The no form of the command reverts the appliance to a standalone configuration.</p> | |
| Syntax Description | node-role | Master or standby |
| | local-primary-ip | Local node primary IP address |
| | peer-primary-ip | Peer node primary IP address |
| | local-secondary-ip | Local node secondary IP address |
| | peer-secondary-ip | Peer node secondary IP address |
| | hacluster-pwd | hacluster user password |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>swx-ufm3-01 (config) # ufm ha configure dual-subnet standby 11.0.0.12 11.0.0.11 10.209.44.12 10.209.44.11 123456</pre> | |
| Related Commands | | |
| Notes | <ol style="list-style-type: none"> 1. The local and peer primary interfaces should be connected directly back-to-back 2. The command must be ran first on standby node and only then on the master node | |

10.5.9.4 ufm ha-nodes

| | | |
|--------------------|--|---|
| | <code>ufm ha-nodes <master hostname> <standby hostname></code> <code>no ufm ha-nodes</code> Sets the HA nodes information in UFM configuration. The no form of the commands clears the HA nodes information from the UFM configuration. | |
| Syntax Description | master hostname | The originally set master node hostname. |
| | standby hostname | The originally set standby node hostname. |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.5.0 | |
| Example | <pre>ufmapl (config) # ufm ha-nodes ufm-host-01 ufm-host-02</pre> | |
| Related Commands | show ufm ha-nodes | |
| Notes | | |

10.5.9.5 show ufm ha-nodes

| | |
|--------------------|--|
| | <code>show ufm ha-nodes</code> Shows the UFM HA configuration that is set in UFM. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.5.0 |
| Example | <pre>ufmapl (config) # show ufm ha-nodes 08c0eb030098609a:11.0.0.12:1,08c0eb0300986042:11.0.0.11:2</pre> |
| Related Commands | ufm ha-nodes |
| Notes | N/A |

10.5.10 UFM Multi-Port SM

10.5.10.1 ufm multi-port-sm

| | |
|--------------------|---|
| | <code>ufm multi-port-sm enable</code> <code>ufm multi-port-sm ha-enable</code> <code>no ufm multi-port-sm enable</code> Enables configuring OpenSM with multiple GUIDs. The no form of the command disables configuring OpenSM with multiple GUIDs. |
| Syntax Description | enable - enables configuring OpenSM with multiple GUIDs ha-enable - enables multi-port SM with high availability |

| | |
|--------------------|--|
| Default | Disabled |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufm (config) # ufm multi-port-sm enable</pre> |
| Related Commands | show ufm multi-port-sm |
| Notes | |

10.5.10.2 show ufm multi-port-sm

| | |
|--------------------|---|
| | show ufm multi-port-sm Displays whether configuring OpenSM with multiple GUIDs is enabled. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufm (config) # show ufm multi-port-sm Enable</pre> |
| Related Commands | ufm multi-port-sm enable |
| Notes | |

10.5.10.3 ufm additional-fabric-interfaces

| | |
|--------------------|---|
| | ufm additional-fabric-interfaces no ufm additional-fabric-interfaces Sets additional fabric interfaces for OpenSM. Clears the additional fabric interfaces list. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufm (config) #ufmapl (config) # ufm additional-fabric-interfaces ib1</pre> |
| Related Commands | ufm multi-port-sm enable |
| Notes | |

10.5.10.4 show ufm additional-fabric-interfaces

| | |
|--------------------|--|
| | <code>show ufm additional-fabric-interfaces</code> Displays the additional fabric interfaces list used by OpenSM. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufm (config) # show ufm additional-fabric-interfaces ib1</pre> |
| Related Commands | <code>ufm multi-port-sm enable</code> |
| Notes | |

10.6 InfiniBand Commands

10.6.1 OpenSM

10.6.1.1 ib sm configuration import

| | |
|--------------------|---|
| | <code>ib sm configuration import [partition-conf-user-ext] <url></code> Imports the Subnet Manager configuration. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.1 |
| Example | <pre>ufmapl (config) # ib sm configuration import partition-config-user-ext sftp://admin:123456@192.168.1.12/tmp/partitions.conf.user_ext</pre> |
| Related Commands | <code>show ib sm configuration import</code> |
| Notes | N/A |

10.6.1.2 show ib sm allow-both-pkeys

| | |
|--------------------|---|
| | <code>show ib sm allow-both-pkeys</code> Displays if both full and limited memberships on the same partition are enabled or not. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.4.0 |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # show ib sm allow-both-pkeys disable</pre> |
| Related Commands | ib sm allow-both-pkeys |
| Notes | N/A |

10.6.1.3 ib sm allow-both-pkeys

| | |
|--------------------|--|
| | ib sm allow-both-pkeys no ib sm allow-both-pkeys Enables having both a full and limited membership on the same partition. The no form of the command disables having both full and limited memberships on the same partition. |
| Syntax Description | N/A |
| Default | Disabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm allow-both-pkeys</pre> |
| Related Commands | show ib sm allow-both-pkey ib partition management defmember |
| Notes | N/A |

10.6.1.4 show ib sm keep-pkey-indexes

| | |
|--------------------|--|
| | show ib sm keep-pkey-indexes Displays whether PKey indexes belonging to the historical PKeys configured on the port are preserved or not. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm keep-pkey-indexes enable</pre> |
| Related Commands | ib sm keep-pkey-indexes |
| Notes | N/A |

10.6.1.5 ib sm keep-pkey-indexes

| | |
|--------------------|---|
| | <p>ib sm keep-pkey-indexes no ib sm keep-pkey-indexes Preserves PKey indexes belonging to the historical PKeys configured on the port when generating PKey tables for a certain port. The no form of the command calculates PKey indexes belonging to the historical PKeys configured on the port.</p> |
| Syntax Description | N/A |
| Default | Enabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # no ib sm keep-pkey-indexes</pre> |
| Related Commands | <p>show ib sm keep-pkey-indexes ib sm allow-both-pkeys</p> |
| Notes | N/A |

10.6.1.6 show ib sm virtualization

| | |
|--------------------|--|
| | <p>show ib sm virtualization Displays virtualization support.</p> |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm virtualization enable</pre> |
| Related Commands | <p>ib sm virtualization enable ib sm virtualization ignore</p> |
| Notes | N/A |

10.6.1.7 ib sm virtualization enable

| | |
|--------------------|---|
| | <p>ib sm virtualization enable no ib sm virtualization enable Enables virtualization on all supported ports (default). The no form of the command disables virtualization on all supporting ports.</p> |
| Syntax Description | N/A |
| Default | Enabled |

| | |
|--------------------|--|
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm virtualization enable</pre> |
| Related Commands | show ib sm virtualization |
| Notes | It is not possible to modify the virtualization support in case OpenSM or UFM are running. |

10.6.1.8 ib sm virtualization ignore

| | |
|--------------------|--|
| | ib sm virtualization ignore No virtualization support. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm virtualization ignore</pre> |
| Related Commands | show ib sm virtualization |
| Notes | It is not possible to modify the virtualization support in case OpenSM or UFM are running. |

10.6.1.9 show ib sm root-guid

| | |
|--------------------|--|
| | show ib sm root-guid Displays all configured root GUIDs for the SM. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm root-guid 0x0002c903006ad830 0x0002c903006ae120 0x0002c903006af520</pre> |
| Related Commands | ib sm root-guid |
| Notes | N/A |

10.6.1.10 ib sm root-guid

| | | |
|--------------------|---|---|
| | ib sm root-guid <guid> no ib sm root-guid <guid> Adds a root GUID for the SM. The no form of the command removes the GUID from the SM. | |
| Syntax Description | guid | The root GUID number in hexadecimal notation For example: 0x0002c903006ad830 |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ib sm root-guid 0x0002c903006ad830</pre> | |
| Related Commands | show ib sm root-guid | |
| Notes | The list of root GUIDs are relevant when the routing algorithm is up-down or fat-tree. | |

10.6.1.11 show ib sm routing-engines

| | | |
|--------------------|--|--|
| | show ib sm routing-engines Displays number of CPUs configured to use for parallel calculations. | |
| Syntax Description | N/A | |
| Default | N/A | |
| Configuration Mode | enable | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # show ib sm routing-engines ar_updn</pre> | |
| Related Commands | ib sm routing-engines | |
| Notes | N/A | |

10.6.1.12 ib sm routing-engines

| | | |
|--------------------|---|---|
| | ib sm routing-engines <engine> Configures number of CPUs to use for parallel calculations. | |
| Syntax Description | engine | Multiple routing engines can be specified separated by space. Supported engines: ar-dor, ar-ftree, ar-torus, ar-updn, chain, dfp, dfp2, dor, file, ftree, minhop, pqft, torus-2QoS, updn) |
| Default | 1 | |
| Configuration Mode | config | |
| History | 1.4.0 | |

| | |
|------------------|--|
| Example | <pre>ufmapl (config) # ib sm routing-engines ar-updn</pre> |
| Related Commands | show ib sm routing-engines |
| Notes | N/A |

10.6.1.13 show ib sm ar-sl-mask

| | |
|--------------------|---|
| | show ib sm ar-sl-mask Displays the adaptive routing SL mask. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm ar-sl-mask 0xffff</pre> |
| Related Commands | ib sm ar-sl-mask |
| Notes | N/A |

10.6.1.14 ib sm ar-sl-mask

| | | |
|--------------------|---|----------------------|
| | ib sm ar-sl-mask <mask> no ib sm ar-sl-mask Configures the adaptive routing SL mask. The no form of the command rests the mask value to default. | |
| Syntax Description | mask | Range: 0x0000-0xffff |
| Default | 0xffff | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ib sm ar-sl-mask 0xfffe</pre> | |
| Related Commands | show ib sm ar-sl-mask | |
| Notes | N/A | |

10.6.1.15 show ib sm configuration import

| | |
|--------------------|--|
| | show ib sm configuration import Displays imported subnet manager configuration files. |
| Syntax Description | N/A |
| Default | N/A |

| | |
|--------------------|---|
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm configuration import partitions.conf.user_ext ----</pre> |
| Related Commands | ib sm configuration import |
| Notes | N/A |

10.6.1.16 ib sm partition-config-merge

| | |
|--------------------|--|
| | ib sm partition-config-merge Merges the partitions.conf.user_ext into the partitions.conf and starts the heavy sweep on the SM. To use after importing the specific file or importing all configuration files. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm partition-config-merge</pre> |
| Related Commands | ib sm configuration import partition-config-user-ext |
| Notes | The SM must be running for this command to work. |

10.6.1.17 ib sm sharp enable

| | |
|--------------------|---|
| | ib sm sharp enable no ib sm sharp enable Enables NVIDIA® Scalable Hierarchical Aggregation and Reduction Protocol (SHARP)™ on all supporting switches. The no form disables NVIDIA SHARP on all supporting switches. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm sharp enable</pre> |

| | |
|------------------|--|
| Related Commands | show ib sm sharp |
| Notes | It is not possible to modify the NVIDIA SHARP support parameter in case OpenSM is running. |

10.6.1.18 ib sm sharp ignore

| | |
|--------------------|---|
| | <p>ib sm sharp ignore No NVIDIA SHARP support. This command does not change the current switch configuration. If NVIDIA SHARP is enabled on the switch, it will remain enabled. If it is disabled on the switch, it will remain disabled.</p> |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sm sharp ignore</pre> |
| Related Commands | show ib sm sharp |
| Notes | It is not possible to modify the NVIDIA SHARP support parameter in case OpenSM is running. |

10.6.1.19 show ib sm sharp

| | |
|--------------------|--|
| | <p>show ib sm sharp Displays NVIDIA SHARP support.</p> |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib sm sharp ignore</pre> |
| Related Commands | <p>ib sm sharp enable ib sm sharp ignore</p> |
| Notes | N/A |

10.6.2 HCA Commands

10.6.2.1 ib hca-vl15-window

| | | |
|--------------------|--|----------------------|
| | ib hca-vl15-window <value> no ib hca-vl15-window Sets the HCA VL15 port receive buffer size. The no form of the command resets this parameter to its default. | |
| Syntax Description | value | 1,2,4,8,16,32,64,128 |
| Default | 1 | |
| Configuration Mode | config | |
| History | 1.6.0 | |
| Example | <pre>UFM-APL (config) # ib hca-vl15-window 6</pre> | |
| Related Commands | show ib hca-vl15-window | |
| Notes | UFM system must be rebooted to apply the new configuration | |

10.6.2.2 show ib hca-vl15-window

| | |
|--------------------|--|
| | show ib hca-vl15-window Displays the configured HCA VL15 port receive buffer size. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | Enable |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # show ib hca-vl15-window /dev/mst/mt4123_pciconf0: Running configuration: default /dev/mst/mt4123_pciconf1: Running configuration: default</pre> |
| Related Commands | ib hca-vl15-window |
| Notes | The example shows an instance where the system has not been rebooted after implementing new configuration |

10.6.3 Partition

10.6.3.1 ib partition management defmember

| | | |
|--------------------|--|--|
| | ib partition management defmember <type> no ib partition management defmember Sets the default membership for the management IB partition (default PKEY). The no form of the command resets the parameter to its default value. | |
| Syntax Description | type | <ul style="list-style-type: none"> • full - full membership • limited - limited membership |
| Default | Full membership | |
| Configuration Mode | config | |
| History | 1.4.0 | |
| Example | <pre>ufmapl (config) # ib partition management defmember limited</pre> | |
| Related Commands | show ib partition | |
| Notes | <ul style="list-style-type: none"> • The defmember setting controls the ability of end nodes to communicate over the management partition • It is not possible to modify the defmember in case OpenSM or UFM are running | |

10.6.3.2 show ib partition

| | |
|--------------------|---|
| | show ib partition Displays partition information. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | enable |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # show ib partition management: Default membership: full</pre> |
| Related Commands | ib partition management defmember |
| Notes | N/A |

10.6.4 NVIDIA SHARP

10.6.4.1 ib sharp enable

| | |
|--------------------|---|
| | <code>ib sharp enable</code> <code>no ib sharp enable</code> Enables NVIDIA® Scalable Hierarchical Aggregation and Reduction Protocol (SHARP)™. The no form of the command disables NVIDIA SHARP. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sharp enable</pre> |
| Related Commands | <code>show ib sharp</code> |
| Notes | N/A |

10.6.4.2 ib sharp allocation enable

| | |
|--------------------|--|
| | <code>ib sharp allocation enable</code> <code>no ib sharp allocation enable</code> Enables NVIDIA SHARP allocation reservation. The no form of the command disables NVIDIA SHARP allocation reservation. |
| Syntax Description | N/A |
| Default | N/A |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp allocation enable</pre> |
| Related Commands | <code>show ib sharp</code> |
| Notes | |

10.6.4.3 ib sharp smx-protocol

| | |
|--------------------|--|
| | <code>ib sharp smx-protocol {sockets ucx}</code> <code>no ib sharp smx-protocol</code> Configures network protocol to be used by SMX. The no form of the command restores the network protocol to default. |
| Syntax Description | N/A |
| Default | sockets |
| Configuration Mode | config |

| | |
|------------------|--|
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sharp smx-protocol ucx</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.4 ib sharp topology-api enable

| | |
|--------------------|---|
| | ib sharp topology-api enable no ib sharp topology-api enable Enables the SHARP topology API. The no form of the command disables the SHARP topology API. |
| Syntax Description | N/A |
| Default | Disabled |
| Configuration Mode | config |
| History | 1.4.0 |
| Example | <pre>ufmapl (config) # ib sharp topology-api enable</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.5 show ib sharp

| | | |
|--------------------|---|--|
| | show ib sharp Displays the configuration of NVIDIA SHARP Aggregation Manager. | |
| Syntax Description | N/A | |
| Default | N/A | |
| Configuration Mode | config | |
| History | 1.6.0 | Updated the output to reflect the new settings |
| | 1.4.0 | First release |
| Example | <pre>ufmapl (config) # show ib sharp Enabled: No Allocation: No SMX protocol: sockets Topology API: No Dump files generation: Yes Dynamic tree allocation: No Dynamic tree algorithm: 0 IB QPC SL: 0 IB SAT QPC SL: 1</pre> | |
| Related Commands | N/A | |
| Notes | N/A | |

10.6.4.6 ib sharp dump-files-generation enable

| | |
|--------------------|---|
| | ib sharp dump-files-generation enable no ib sharp dump-files-generation enable Enables dumping SHARP's internal state to files The no form of the command disables dumping SHARP's internal state to files |
| Syntax Description | N/A |
| Default | Disable |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp dump-files-generation enable</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.7 ib sharp dynamic-tree-allocation enable

| | |
|--------------------|---|
| | ib sharp dynamic-tree-allocation enable no ib sharp dynamic-tree-allocation enable Enables dynamically allocated trees for each SHARP job The no form of the command disables dynamically allocated trees for each SHARP job |
| Syntax Description | N/A |
| Default | Enable |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp dynamic-tree-allocation enable</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.8 ib sharp dynamic-tree-algorithm

| | |
|--------------------|---|
| | ib sharp dynamic-tree-algorithm <0-1> no ib sharp dynamic-tree-algorithm Sets which algorithm should be used by the dynamic tree mechanism The no form of the command restores the algorithm used by the dynamic tree mechanism to default |
| Syntax Description | N/A |
| Default | 0 |
| Configuration Mode | config |

| | |
|------------------|--|
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp dynamic-tree-algorithm</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.9 ib sharp ib-qpc-sl <0-15>

| | |
|--------------------|--|
| | <p>ib sharp ib-qpc-sl <0-15> no ib sharp ib-qpc-sl Set the IB QP context SL for SHARP data path communication The no form of the command restores the IB QP context SL for SHARP data path communication to default</p> |
| Syntax Description | N/A |
| Default | 0 |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp ib-qpc-sl 1</pre> |
| Related Commands | show ib sharp |
| Notes | N/A |

10.6.4.10 ib sharp ib-sat-qpc-sl <0-15>

| | |
|--------------------|---|
| | <p>ib sharp ib-sat-qpc-sl <0-15> no ib sharp ib-sat-qpc-sl Sets the IB QP context SL for SHARP streaming data path communication The no form of the command restores the IB QP context SL for SHARP streaming data path communication to default</p> |
| Syntax Description | N/A |
| Default | 1 |
| Configuration Mode | config |
| History | 1.6.0 |
| Example | <pre>ufmapl (config) # ib sharp ib-sat-qpc-sl 1</pre> |
| Related Commands | show ib sharp |

| | |
|-------|-----|
| Notes | N/A |
|-------|-----|

11 UFM Enterprise Appliance Upgrade

This is the recommended upgrade procedure, which involves upgrading all UFM Enterprise appliance software components and operating system. For additional upgrade procedures of specific software components, please refer to [Appendix - Software Components Upgrade](#).

As of UFM Enterprise Appliance version 1.5.0, upgrading the appliance on HA supports an in-service upgrade, meaning UFM can continue running during the steps of the upgrade, and there is no need to stop UFM before the upgrade.

The upgrade is performed on both Master and Standby nodes.

To upgrade the UFM Enterprise Appliance software:

1. On the standby server, extract the OMU image to the /tmp folder:

```
tar -xzf ufm-appliance-<version>-omu.tar -C /tmp
```

2. On the standby server, access the installation folder and upgrade script:

```
standby# cd /tmp/ufm-appliance-<version>-omu
```

3. Run the UFM upgrade script on the standby server:

```
./ufm-os-upgrade.sh --appliance-sw-upgrade --yes --reboot
```

4. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:

" UFM-OS-FIRSTBOOT-FAILURE " - if installation is failed.

" UFM-OS-FIRSTBOOT-SUCCESS " - if installation succeeded.

Example:

```
root@ufm-ai03:~#  
root@ufm-ai03:~#  
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):  
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

To manually check the status, run `systemctl status ufm-os-firstboot.service`. If it is already finished, an error message is prompted stating that there is no such service. In that case, the log `/var/log/ufm-os-firstboot.log` can be checked instead.

```
systemctl status ufm-os-firstboot.service
```

Example:

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot  
Unit ufm-os-firstboot.service could not be found.  
root@ufm-ai03:~#
```

Do NOT proceed to the next step before ensuring that the `systemctl status ufm-os-firstboot.service` service has been completed.

5. After the completion of the upgrade script, the UFM code is upgraded, while the UFM data remains unchanged. The automatic upgrade of UFM data will take place during the next UFM startup. To initiate this process, execute a failover from the Master node (or perform a takeover from the Standby node).

```
master# ufm_ha_cluster failover
```

The upgrade script logs the data to `/var/log/ufm_os_upgrade_<UFM-OS version>.log` and outputs simultaneously it to the screen. In case of an issue, UFM data can be restored to factory default. For more information, refer to [Appendix - UFM Factory Reset](#).

6. Once UFM is operational on the upgraded node (formerly the standby node), proceed to replicate steps 1 to 3 on the non-upgraded node (previously the master node).

11.1 In-Service Upgrade via CLI

Alternatively, in-service upgrade can be performed via the CLI. The upgrade is performed on both Master and Standby nodes.

Follow the below instructions:

1. On the Standby node, fetch the new image from a remote server. Run:

```
ufmapl (config) # image fetch <download URL>
```

2. On the Standby node, install the new image. Run:

```
ufmapl (config) # image install <image name>
```

3. Reload the Standby UFM Enterprise Appliance. Run:

```
ufmapl (config) # reload
```

4. After the completion of the upgrade on the Standby node, the UFM code is upgraded, while the UFM data remains unchanged. The automatic upgrade of UFM data will take place during the next UFM startup. To initiate this process, execute a failover from the Master node. Once the Standby node is up and running, perform a failover on the Master node. Run:

```
ufmapl (config) # ufm ha failover
```

5. Once UFM is operational on the upgraded node (formerly the standby node), proceed to replicate steps 1 to 3 on the non-upgraded node (previously the Master node).

12 Troubleshooting

12.1 Split-Brain Recovery in HA Installation

The split-brain problem is a DRBD synchronization issue (HA status shows `DUnknown` in the DRBD disk state), which occurs when both HA nodes are rebooted. For example, in cases of electricity shut-down. To recover, please follow the below steps:

- Step 1: Run the following command to clear the cluster failure.

```
pcs resource cleanup
```

If the split-brain issue is not resolved, perform the below steps.

- Step 2: Manually choose a node where data modifications will be discarded. It is called the split-brain victim. Choose wisely; all modifications will be lost! When in doubt, run a backup of the victim's data before you continue. When running a Pacemaker cluster, you can enable maintenance mode. If the split-brain victim is in the Primary role, bring down all applications using this resource. Now switch the victim to the Secondary role:

```
victim# drbdadm secondary ha_data
```

- Step 3: Disconnect the resource if it's in connection state `WFCConnection`:

```
victim# drbdadm disconnect ha_data
```

- Step 4: Force discard of all modifications on the split-brain victim:

```
victim# drbdadm connect --discard-my-data ha_data
```

- Step 5: Resync starts automatically if the survivor is in a `WFCConnection` network state. If the split-brain survivor is still in a `Standalone` connection state, reconnect it:

```
survivor# drbdadm connect ha_data
```

Now the resynchronization from the survivor (`SyncSource`) to the victim (`SyncTarget`) starts immediately. There is no full sync initiated, but all modifications on the victim will be overwritten by the survivor's data, and modifications on the survivor will be applied to the victim.

13 Appendixes

13.1 Appendix - Chassis Health Monitoring

13.1.1 Overview

Chassis Health Monitoring enables monitoring hardware alerts via `rsyslog` and generating external events in UFM. The alerts are written to `/var/log/syslog`.

Monitoring hardware health status is essential for failure prevention and maintenance. The Chassis Health Monitoring service is run as a Docker container.

13.1.2 Configuration

1. Generate UFM token authentication. Run:

```
POST https://<UFM server IP>/ufmRest/app/tokens
```

2. Set the UFM server hostname and authentication token in `/opt/ufm/chassis_health/chassis_health.conf`:

```
[connection]
# UFM server hostname. In case of HA, it should be the VIP
hostname =

[authentication]
# UFM server user credentials
token =
```

3. Restart the Chassis Health Monitoring service for changes to take effect. Run:

```
systemctl restart ufm-chassis-health.service
```

Once the service runs, the status can be viewed via `systemctl` (`systemctl status ufm-chassis-health.service`) and `/var/log/chassis_health_fluentd_console.log` file.

13.2 Appendix - Secure Boot Activation and Deactivation

- [13.2.1 Enabling Secure Boot](#)
 - [13.2.1.1 Add NVIDIA Certificate to MOK DB](#)
 - [13.2.1.2 Enable Secure Boot](#)
- [13.2.2 Disable Secure Boot](#)
 - [13.2.2.1 Disable Secure Boot in the BIOS](#)
 - [13.2.2.2 Remove the NVIDIA Certificate from MOK db](#)

This section provides instructions on how to enable/disable the Secure Boot feature in UFM Enterprise Appliance.

13.2.1 Enabling Secure Boot

The NVIDIA public certificate needs to be imported to the Machine Owner Key DB (MOK DB) before enabling secure boot. To do so, follow the below steps:

13.2.1.1 Add NVIDIA Certificate to MOK DB

1. Download NVIDIA certificate [mlnx_signing_key_pub.der](#) to a temporary folder.
checksums:

MD5: c3ce3dcad0f38b02a9cbb991ce1bc7f4

sha256: ff7fe8c650e936079a8add2900b190f9e7f3806e5ad42e48c2b88408a6ce70aa

```
cd /tmp
wget http://www.mellanox.com/downloads/ofed/mlnx_signing_key_pub.der
ls -ltrh ./mlnx_signing_key_pub.der
```

Example:

```
root@ubuntu:/tmp# ls -ltrh mlnx_signing_key_pub.der
-rw-r--r-- 1 root root 1.5K Feb 23 2017 mlnx_signing_key_pub.der
```

2. Import the mlnx_signing_key_pub.der to MOK DB using mok-util:

```
cd /tmp
mokutil --import ./mlnx_signing_key_pub.der --root-pw
```

The certificate is in the enrolled queue at this point. Upon the next server reboot, a 10 second prompt appears at the start of the boot process to confirm the certificate addition. It is important to confirm the certificate addition at this stage. Failure to do so requires you to repeat the procedure.

To be able to interact with the prompt, a console connection is needed either from the serial port or from the web console available via Remote Management.

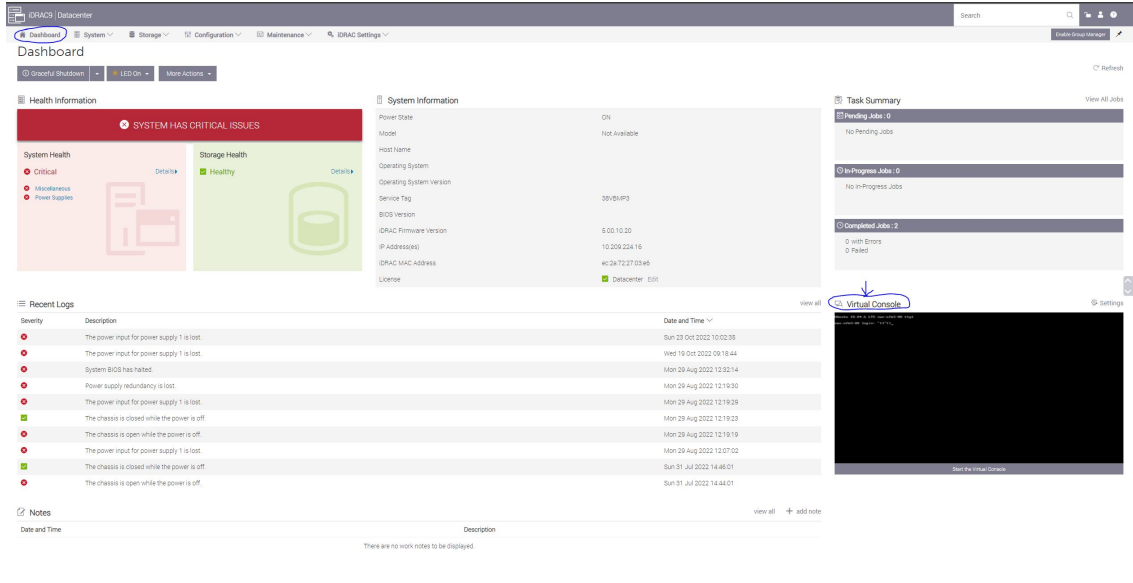
Verify the certificate in the enrolled queue:

```
mokutil --list-new
```

```
root@ubuntu:~# mokutil --list-new
[key 1]
SHA1 Fingerprint: dc:cd:44:95:92:2f:95:9f:28:49:7b:64:94:41:d8:bd:64:60:6d:69
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    ba:b0:f5:cd:23:24:a0:ed
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: O=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
```

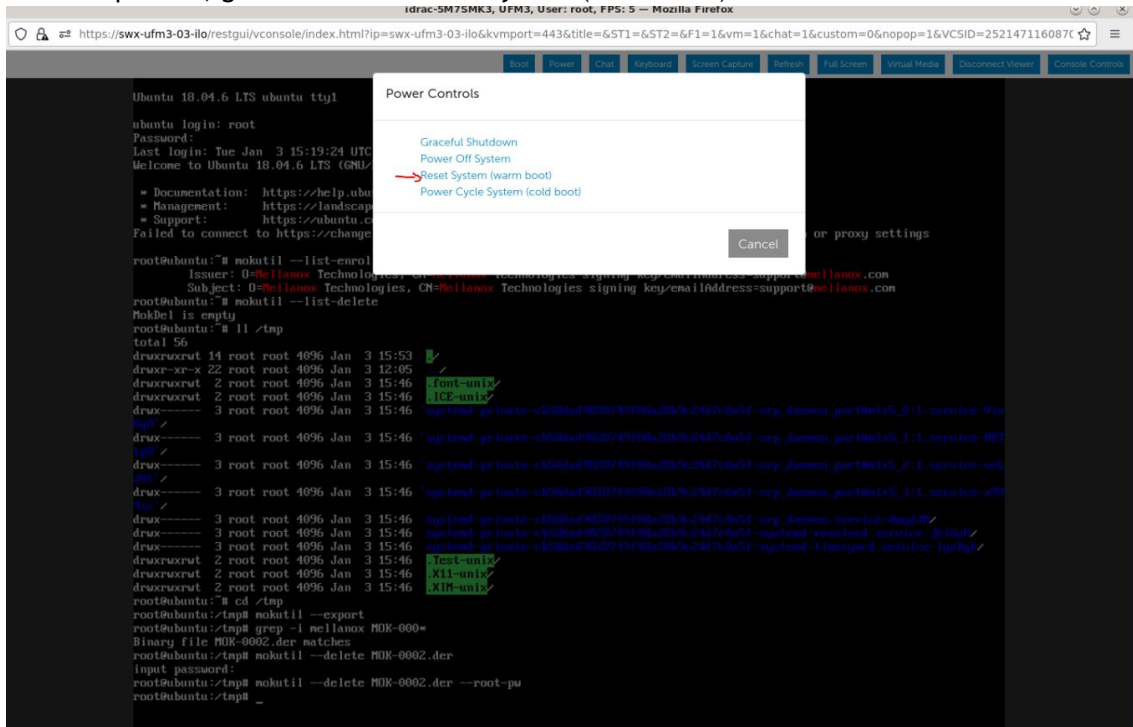
3. Login to Remote Management via <https://<iDRAC-ip address>>

4. To open the virtual web console, click on "Dashboard" → "Virtual Console"



5. Power cycle the server (at boot startup a 10 second prompt appears to verify the certificate addition)

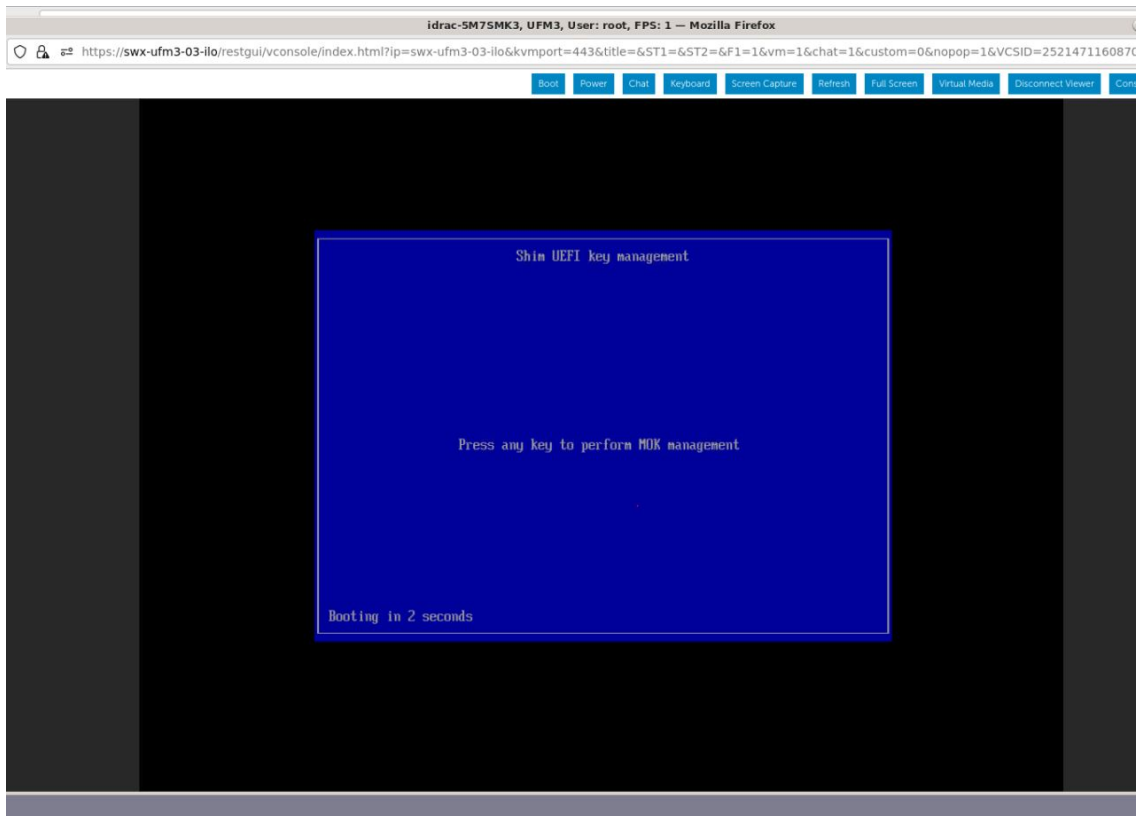
On the top menu, go to "Power" → "Reset System (warm boot)"



The server will now reboot.

6. At boot startup, a confirmation prompt appears to verify certificate addition. The prompt closes after 10 seconds, so if missed, the certificate addition procedure needs to be done again.

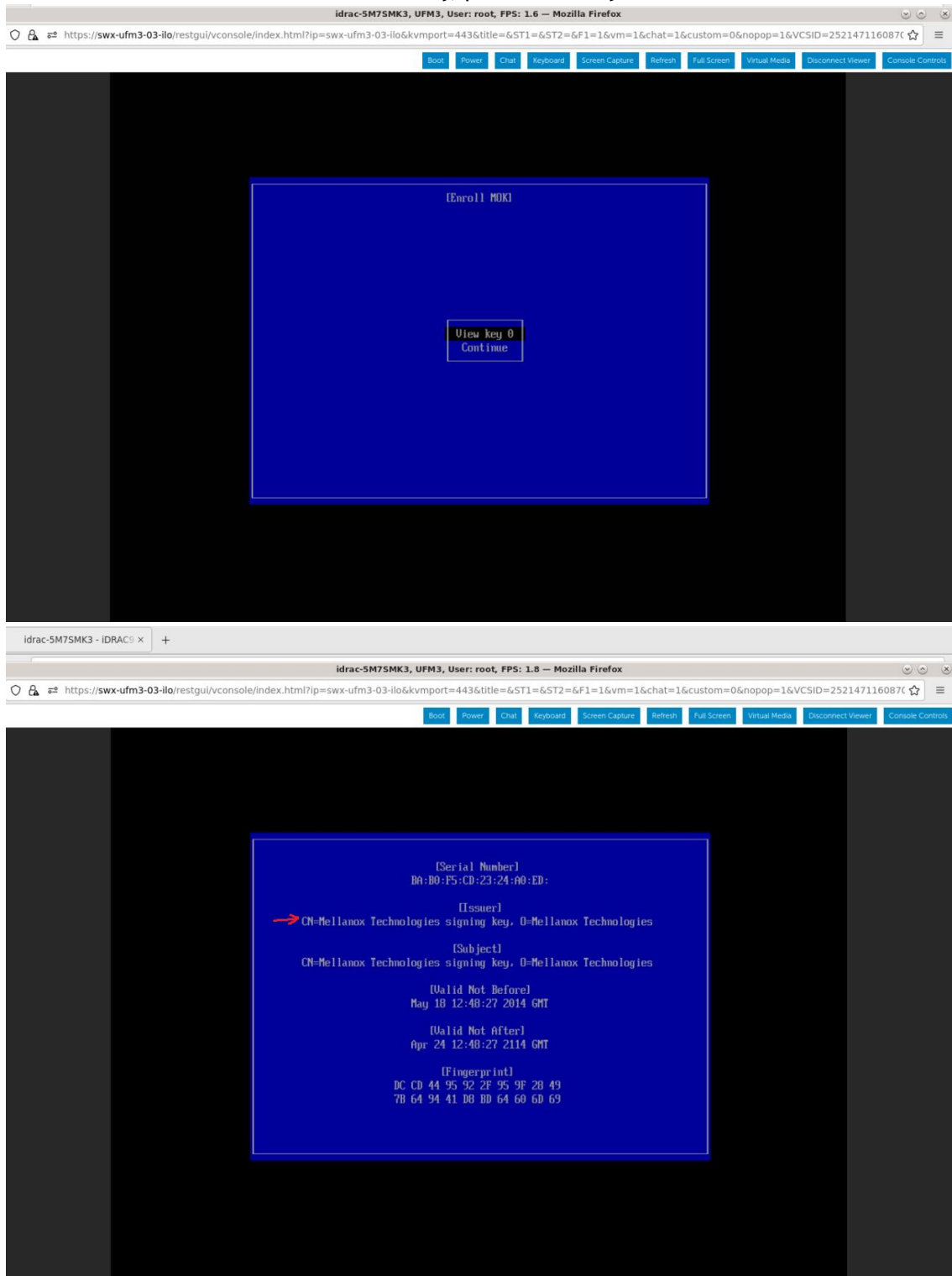
When the prompt appears, press any key to interact.



7. Navigate to "Delete MOK"

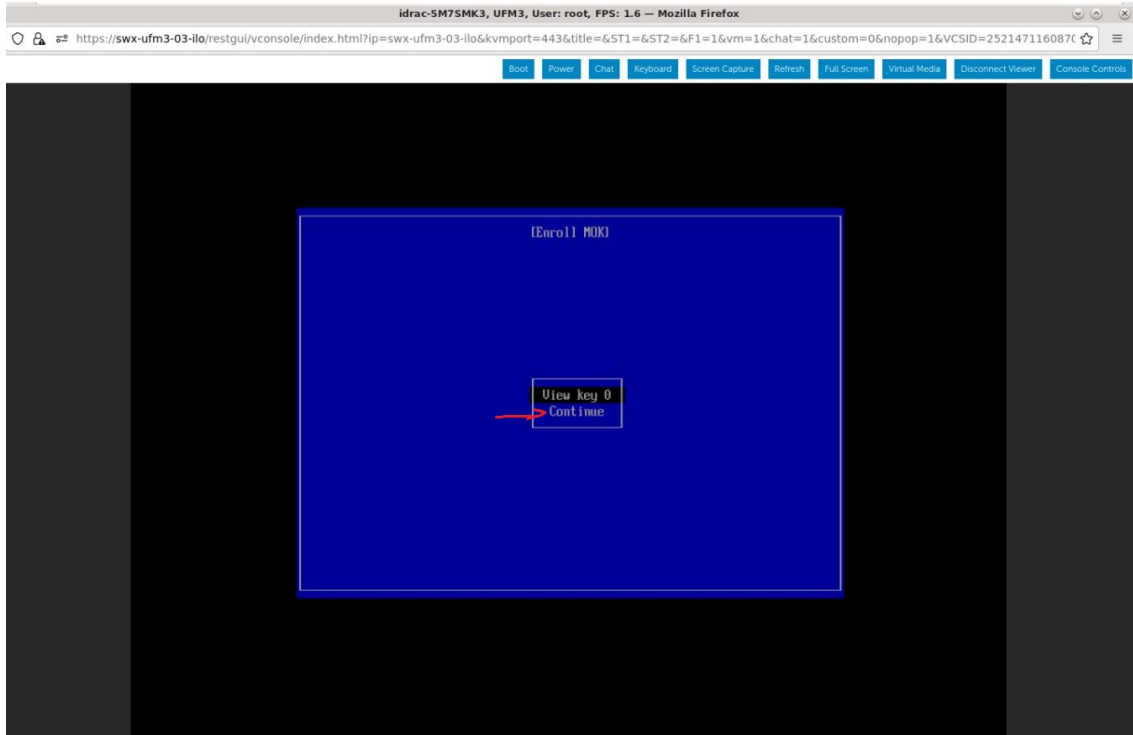


8. View the certificate to be enrolled. To verify, press "View key0".

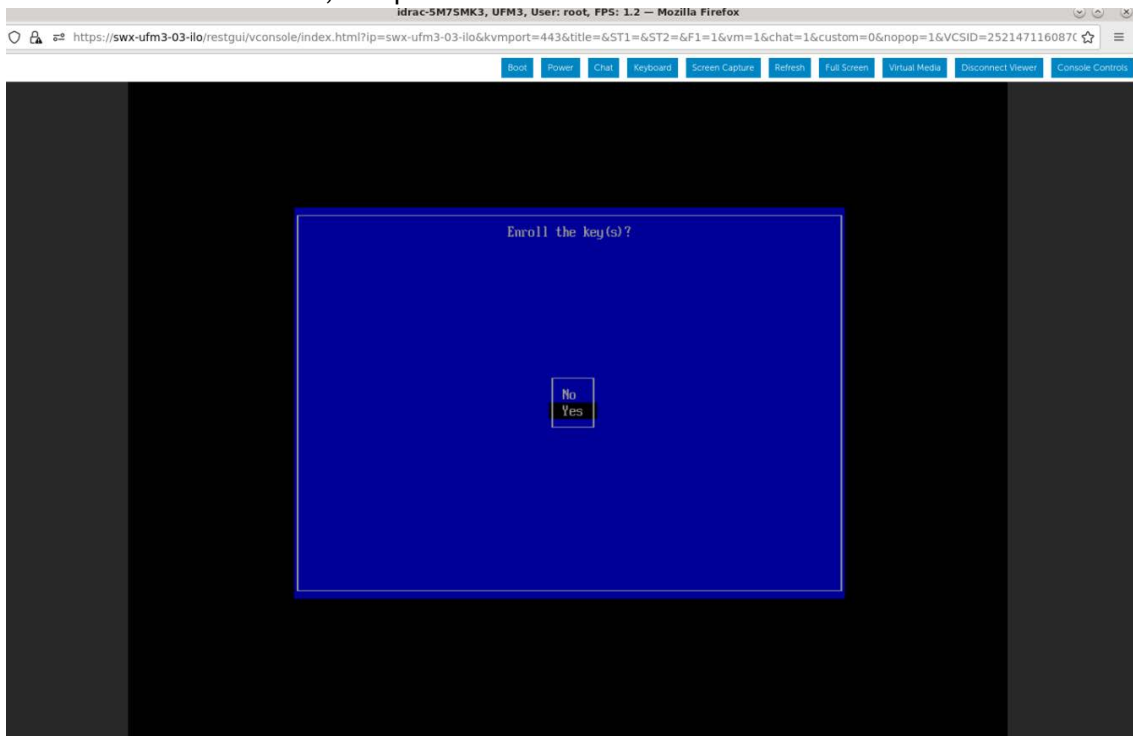


Press "Enter" to exit the view.

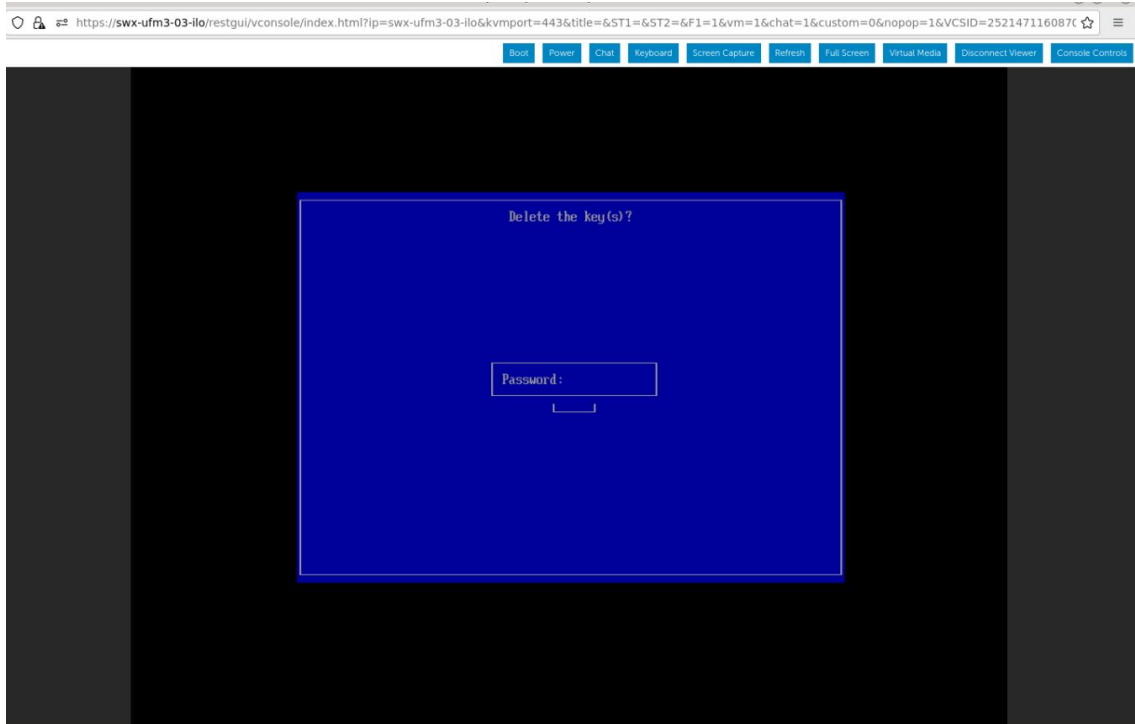
9. Select "Continue" from the menu and press Enter.



10. Select "Yes" from the menu, and press Enter.



11. A password prompt appears, then, enter the OS Root user credentials.



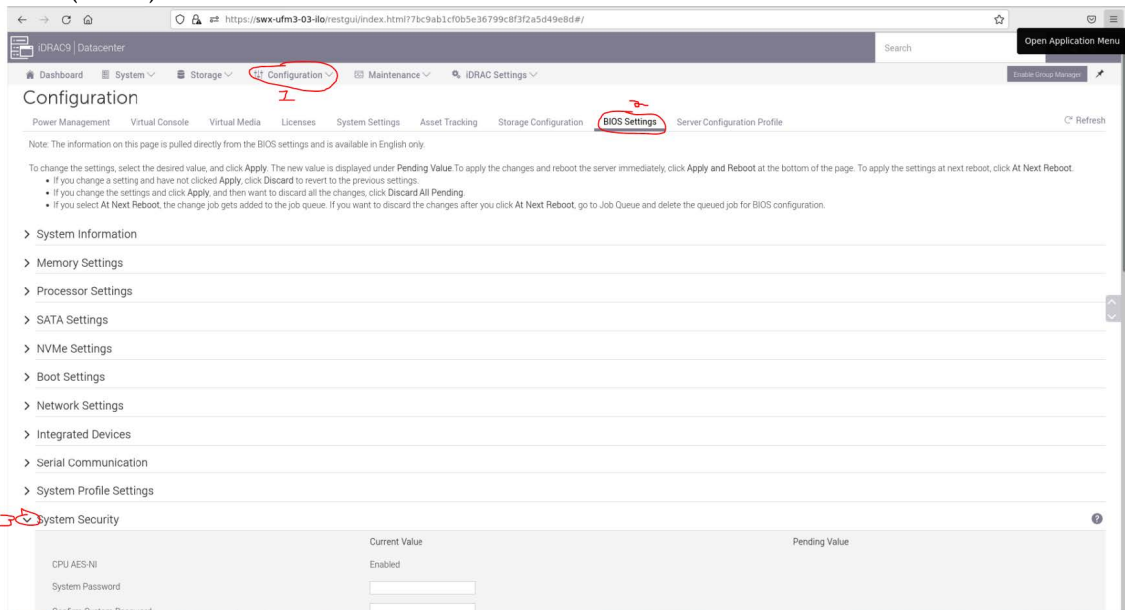
12. Select "Reboot" and press Enter. After the reboot is completed, the certificate is removed.



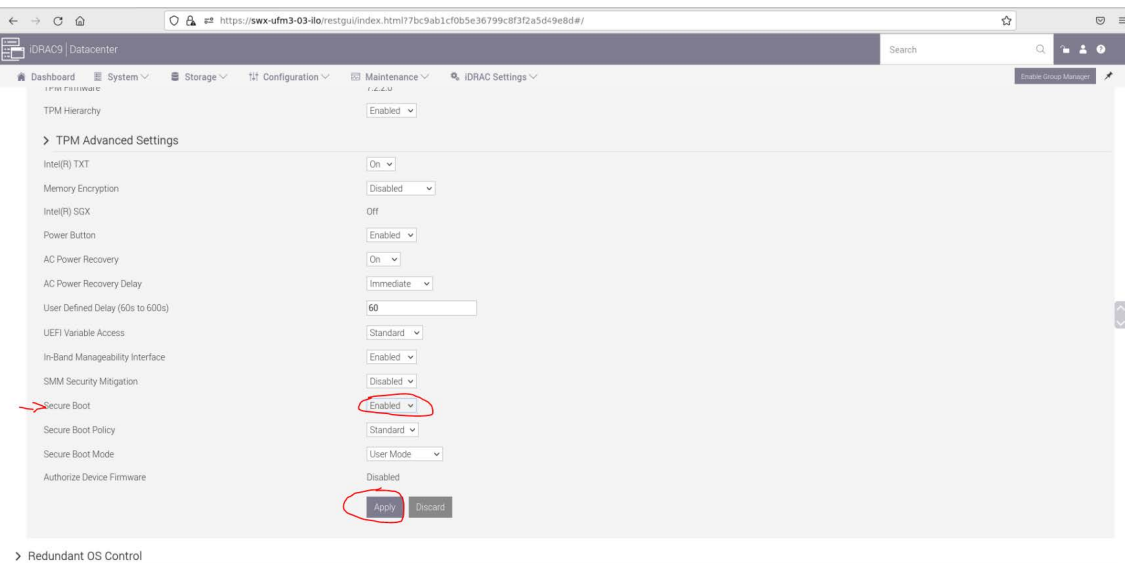
13.2.1.2 Enable Secure Boot

1. Login to Remote Management available via <https://<iDRAC-ip address>>

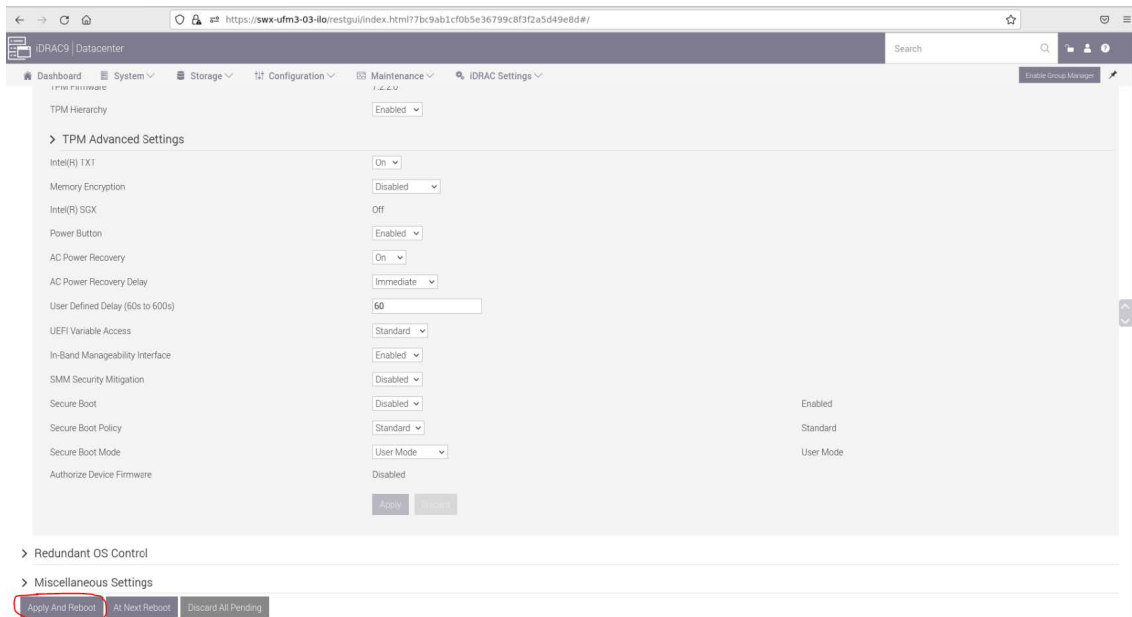
2. Navigate to "Configuration" → "BIOS Settings" → "System Security" and press the drop down menu (arrow).



3. Scroll down to "Secure Boot" and select "Enabled" from the drop menu. Click the "Apply" button.



4. Scroll to the bottom of the page and click on "Apply And Reboot" button, this will reboot the server and perform the configuration



5. An Information Popup is prompted. Click on the "Job Queue" button (can also be navigated from "Maintenance" → "Job Queue").



6. Wait for the Jobs to finish and reach 100%

| ID | Job | Status |
|------------------|---|-------------------------|
| RID_727855969221 | Reboot: Graceful OS shutdown with powercycle on timeout | Reboot Completed (100%) |
| JID_727855968621 | Configure: BIOS Setup: 1-1 | Completed (100%) |
| JID_714091551187 | Export: Server Configuration Profile | Completed (100%) |
| JID_703615455555 | Configure: Import Server Configuration Profile | Completed (100%) |
| JID_703615395967 | Firmware Update: OEM ID Module | Completed (100%) |
| RID_625592058437 | Reboot: Graceful OS shutdown with powercycle on timeout | Reboot Completed (100%) |
| JID_625592057947 | Configure: BIOS Setup: 1-1 | Completed (100%) |
| JID_612763094152 | Firmware Update: OEM ID Module | Completed (100%) |
| RID_612740933938 | Reboot: Graceful OS shutdown with powercycle on timeout | Reboot Completed (100%) |
| JID_612740933147 | Configure: BIOS Setup: 1-1 | Completed (100%) |
| JID_606568609010 | Export: Server Configuration Profile | Completed (100%) |
| IRI_606568480301 | Configure: Import Server Configuration Profile | Failed (100%) |

7. Validate that secure boot is enabled and active (from the terminal).

```
mokutil --sb-state
root@ubuntu:~# mokutil --sb-state
SecureBoot enabled

mokutil --list-enrolled | grep -i mellanox
root@ubuntu:~# mokutil --list-enrolled | grep -i mellanox
Issuer: O=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
Subject: O=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
```

13.2.2 Disable Secure Boot

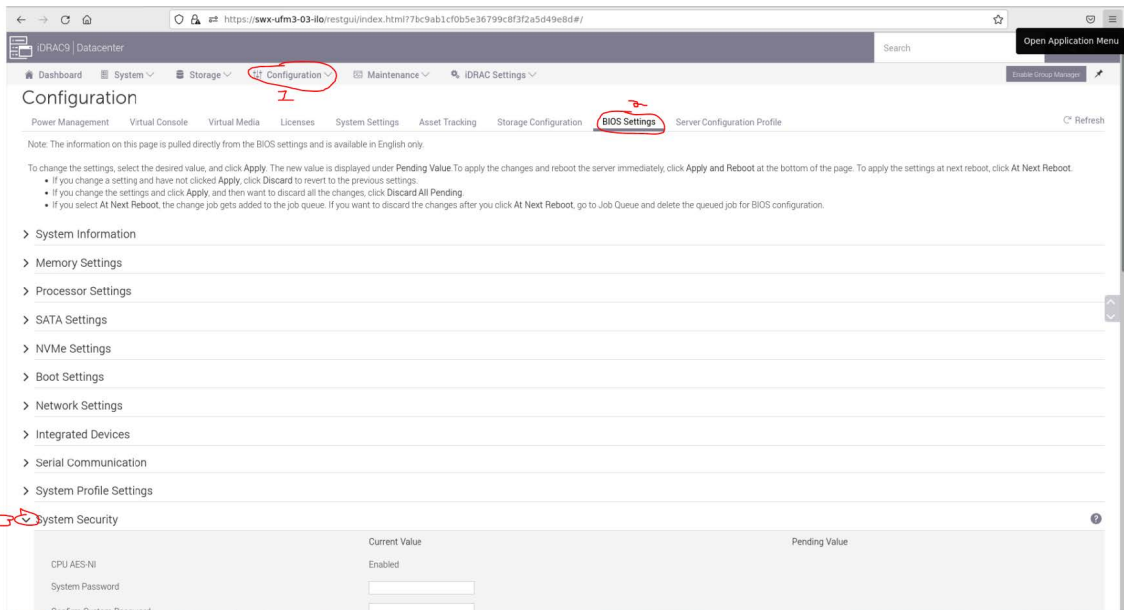
Disabling secure boot is not recommended and may cause security issues.

Secure Boot needs to be disabled prior to removing the NVIDIA public certificate.

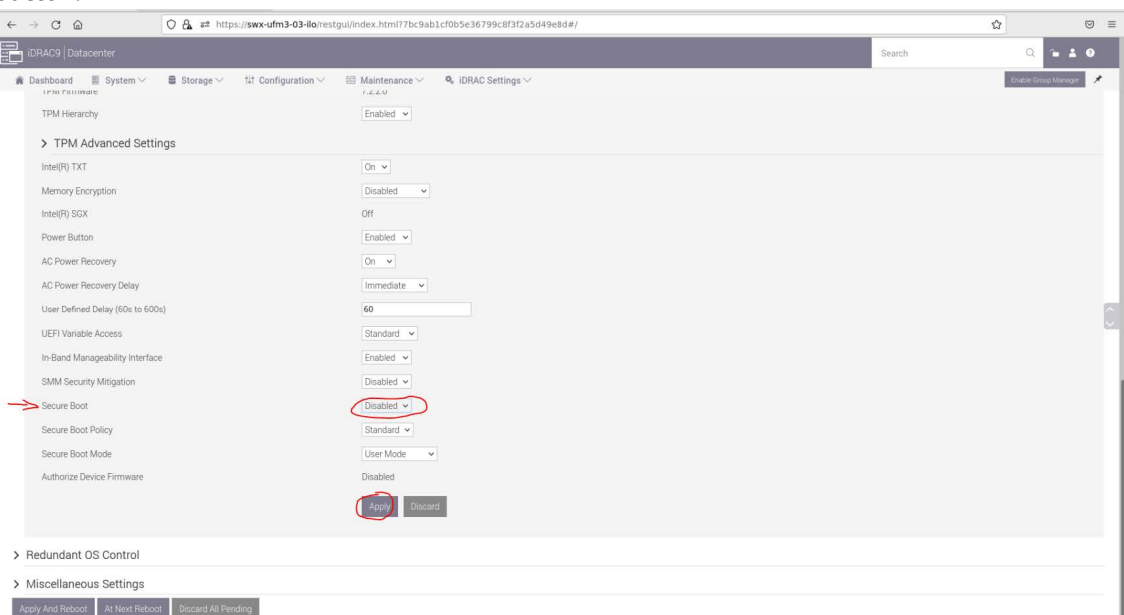
The removal of the certificate is optional and can be skipped if secure boot should be re-enabled at some point in the future.

13.2.2.1 Disable Secure Boot in the BIOS

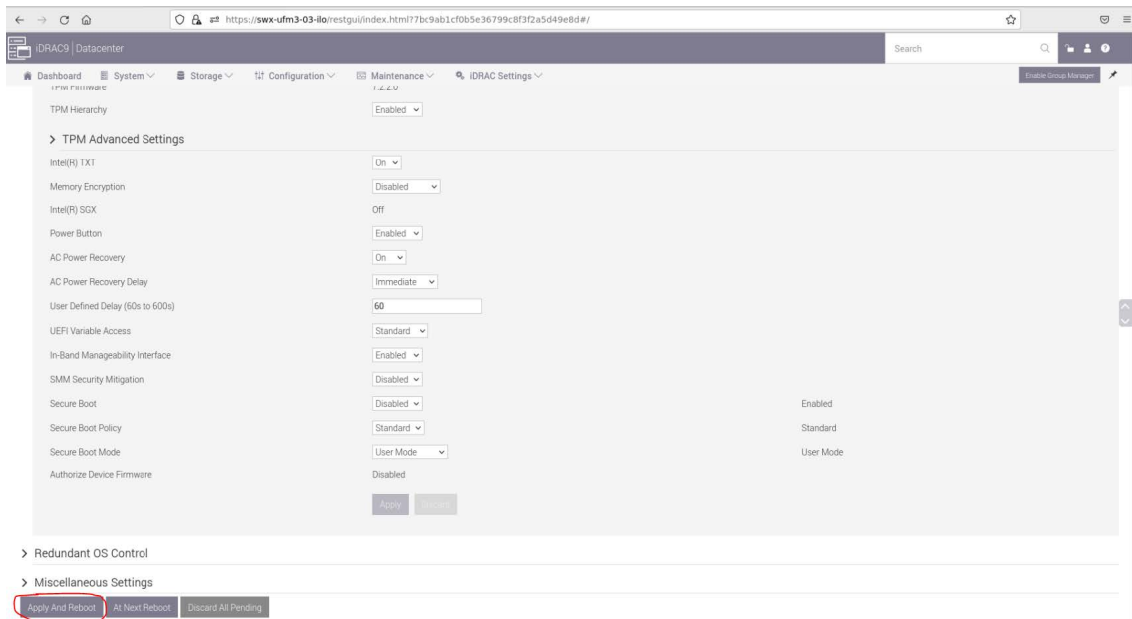
1. Login to Remote Management (<https://<iDRAC-ip address>>)
2. Navigate to "Configuration" → "BIOS Settings" → "System Security" and press the drop menu (arrow).



3. Scroll down to "Secure Boot" and select "Disabled" from the drop menu, and click the "Apply" button.



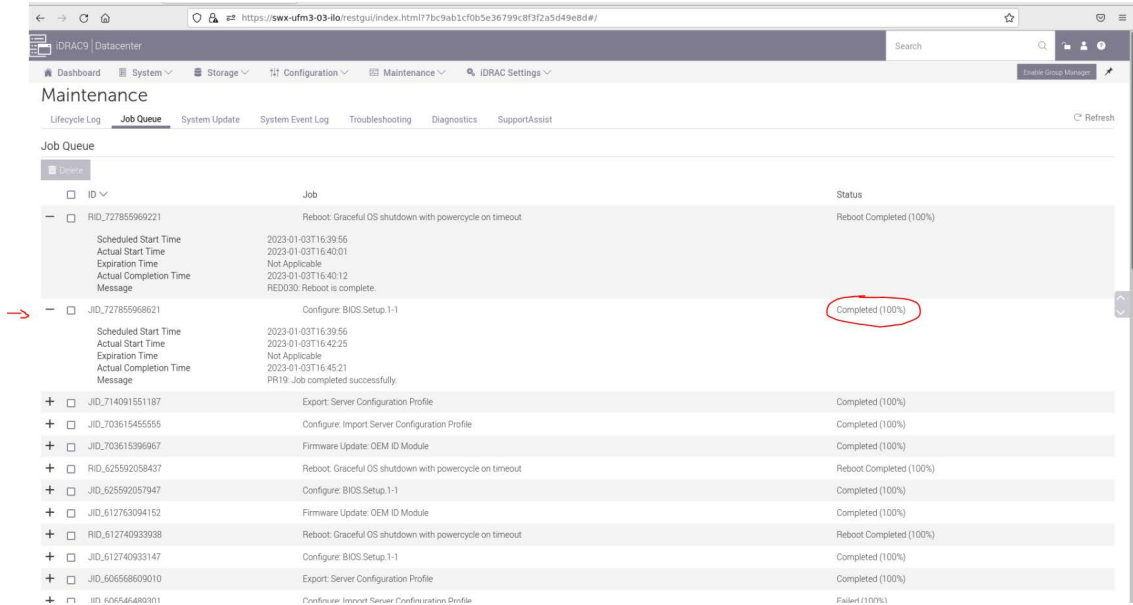
4. Scroll to the bottom of the page and click on the "Apply And Reboot" button; this will reboot the server and perform the configuration.



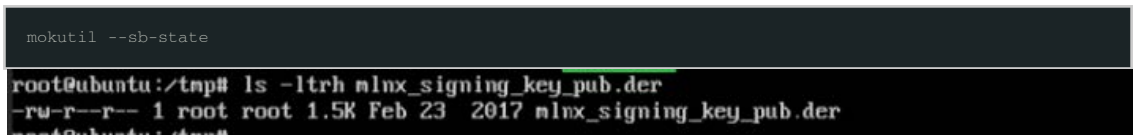
5. An Information Popup is prompted. Click on the "Job Queue" button (can also be navigated from "Maintenance" → "Job Queue").



6. Wait for the completion of the jobs (reach 100%).



7. Validate that secure boot is Disabled (from the terminal).



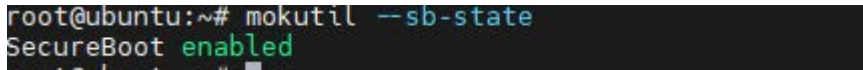
13.2.2.2 Remove the NVIDIA Certificate from MOK db

Perform this step if you want to entirely remove NVIDIA's certificate from MOK DB. This step is optional and is not required to disable secure boot. Skip this if you wish to enable secure boot at a later time.

1. Login as root to the UFM server.
2. Check current enrolled certificates.

```
mokutil --list-enrolled
```

Search for "Issuer: O=Mellanox Technologies.." and note the key ID above the start of this certificate:



3. Download the [mlnx_signing_key_pub.der](#) to a temporary folder (the DER certificate file must be present to be deleted). If the certificate is not available, it can be exported.

```
cd /tmp
wget http://www.mellanox.com/downloads/ofed/mlnx_signing_key_pub.der
```

Or export from current keys (all the keys are named MOK-000X.der) and search the NVIDIA certificate.

```
cd /tmp
mokutil --export
grep "Mellanox" MOK-0*
```

```
root@ubuntu:~# mokutil --list-enrolled | grep -i mellanox
Issuer: 0=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
Subject: 0=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
```

Validate the certificate:

```
openssl x509 -inform der -in MOK-0002.der -noout -issuer
```

```
root@ubuntu:/tmp# openssl x509 -inform der -in MOK-0002.der -noout -issuer
issuer=0 = Mellanox Technologies, CN = Mellanox Technologies signing key, emailAddress = support@mellanox.com
```

4. Remove the certificate from the MOK db. The below example lists MOK-0002.der, the naming convention might be different.

```
mokutil --delete ./MOK-0002.der --root-pw
```

The above can be validated by running

```
mokutil --list-delete
```

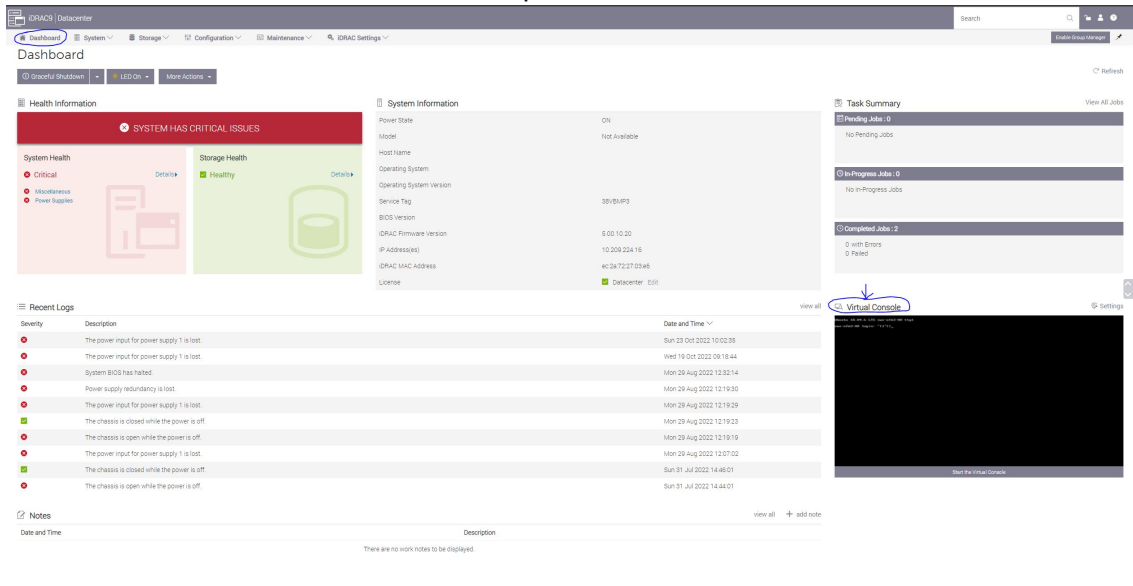
```
root@ubuntu:/tmp# mokutil --list-delete
[key 1]
SHA1 Fingerprint: dc:cd:44:95:92:2f:95:9f:28:49:7b:64:94:41:d8:bd:64:60:6d:69
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      ba:b0:f5:cd:23:24:a0:ed
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: 0=Mellanox Technologies, CN=Mellanox Technologies signing key/emailAddress=support@mellanox.com
    Validity
```

The certificate is in the enrolled queue at this point. Upon the next server reboot, a 10 second prompt appears at the start of the boot process to confirm the certificate addition. It is important to confirm the certificate addition at this stage. Failure to do so requires you to repeat the procedure.

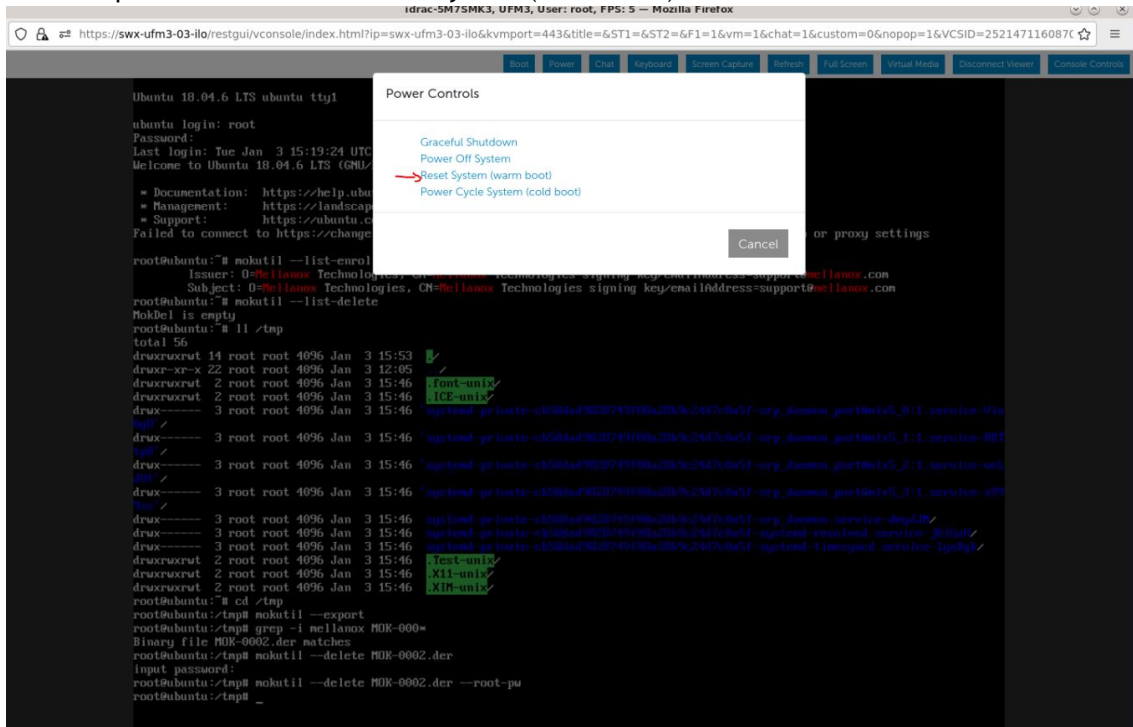
To be able to interact with the prompt, a console connection is needed either from the serial port or from the web console available via Remote Management.

5. Login to Remote Management (<https://<iDRAC-ip address>>)

6. click on "Dashboard" → "Virtual Console" to open the virtual web console.

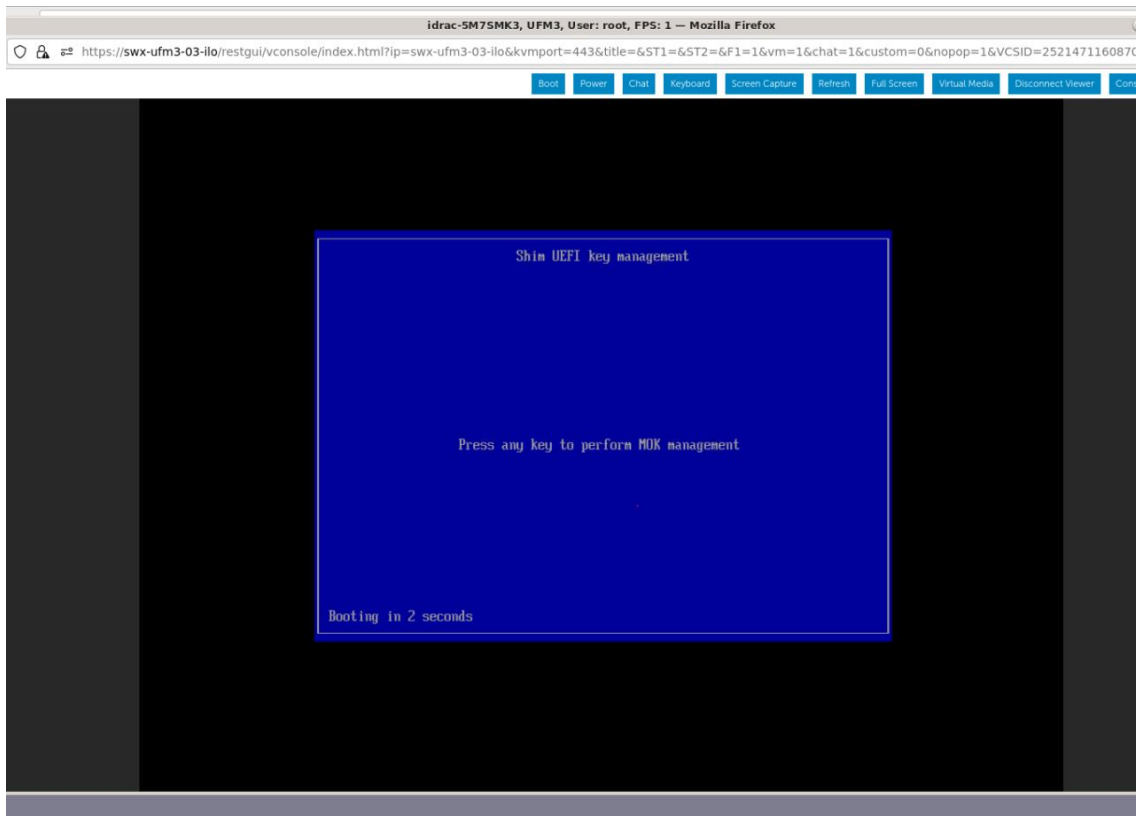


7. Power cycle the server (at boot startup, a 10 second prompt appears to verify the certificate deletion).
 On the top menu: "Power" → "Reset System (warm boot)".

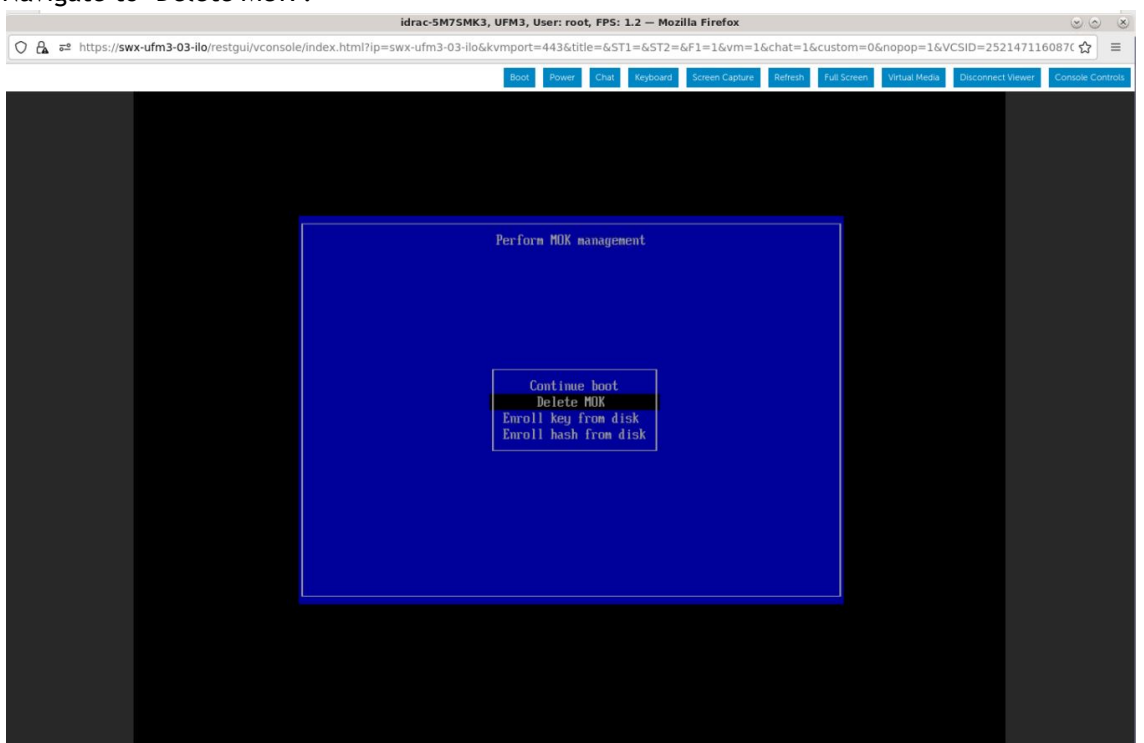


The server now performs reboot.

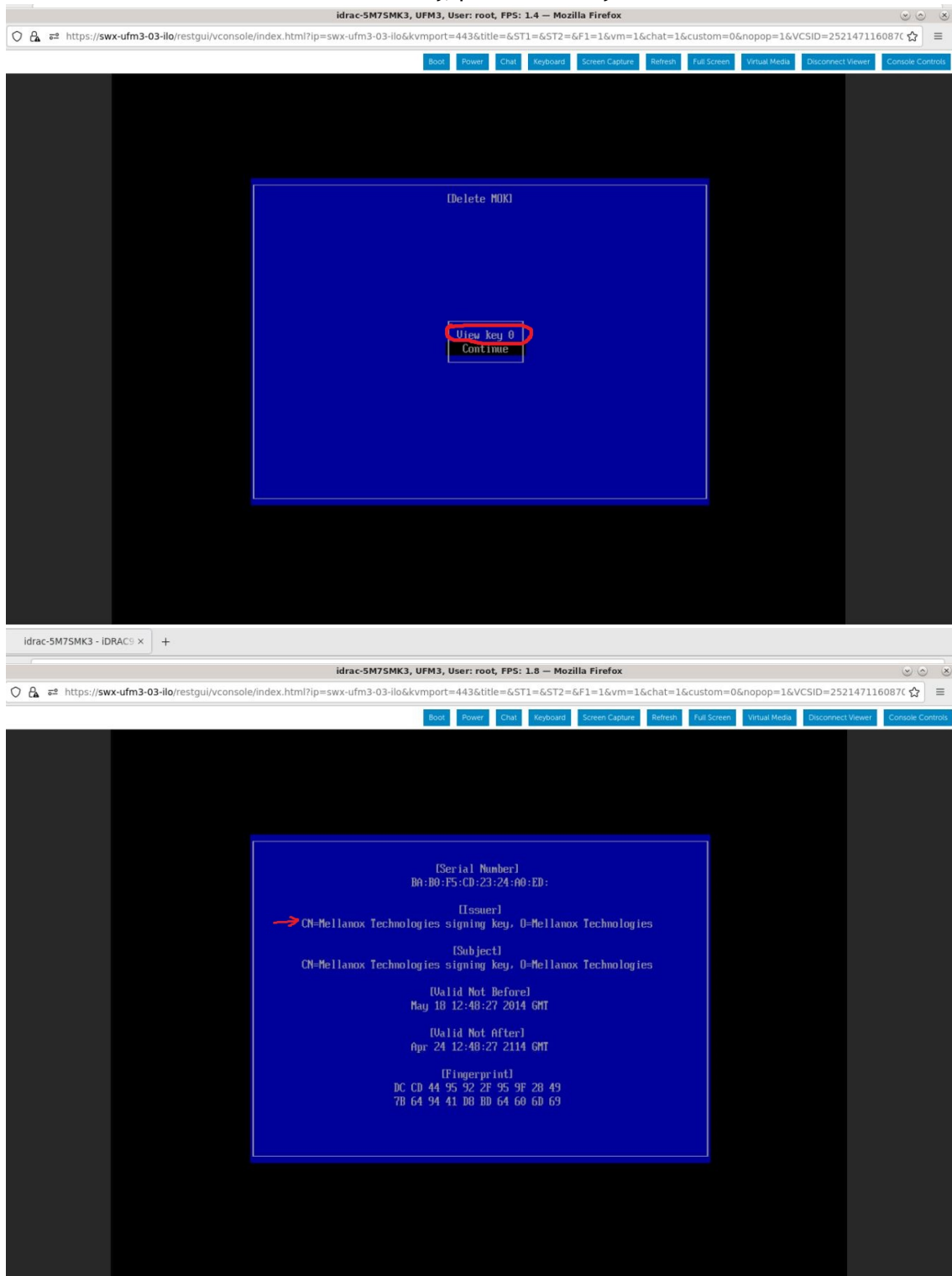
8. Once the startup procedure begins, a confirmation prompt appears to verify certificate deletion. The prompt closes after 10 seconds, if missed, the certificate deletion procedure needs to be repeated.
 Once the prompt appears, press any key to interact.



9. Navigate to "Delete MOK".



10. View the certificate to be deleted. To verify, press "View key0".

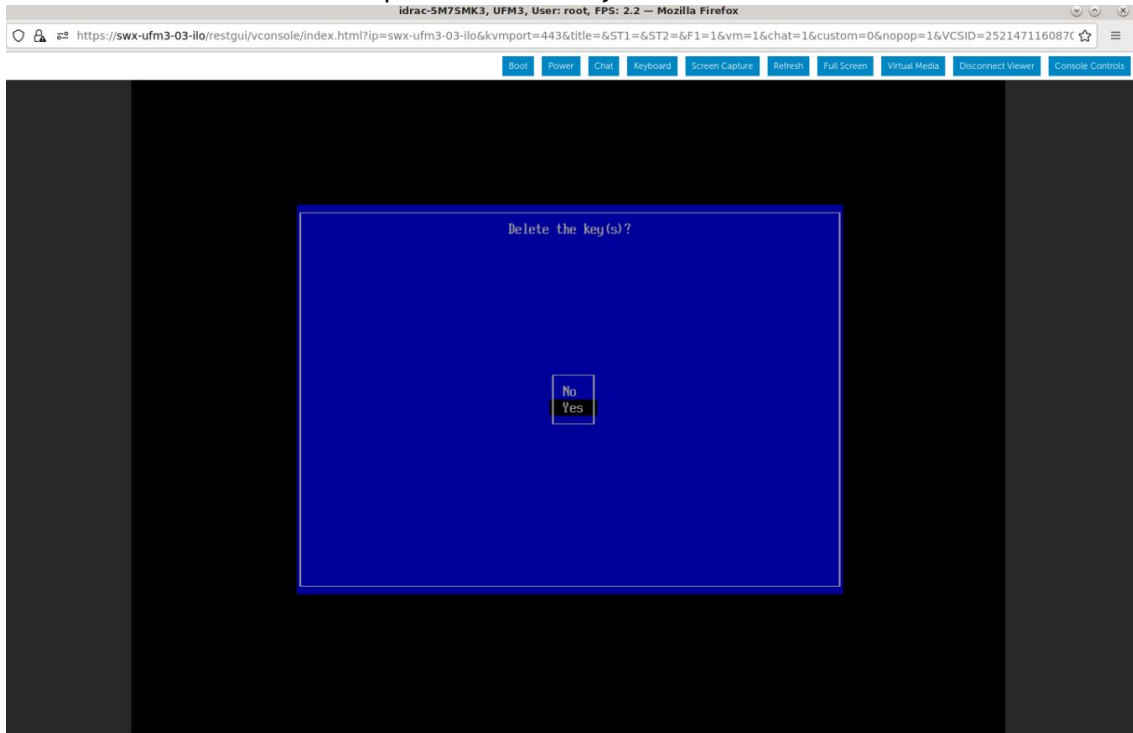


Press "Enter" to exit the view.

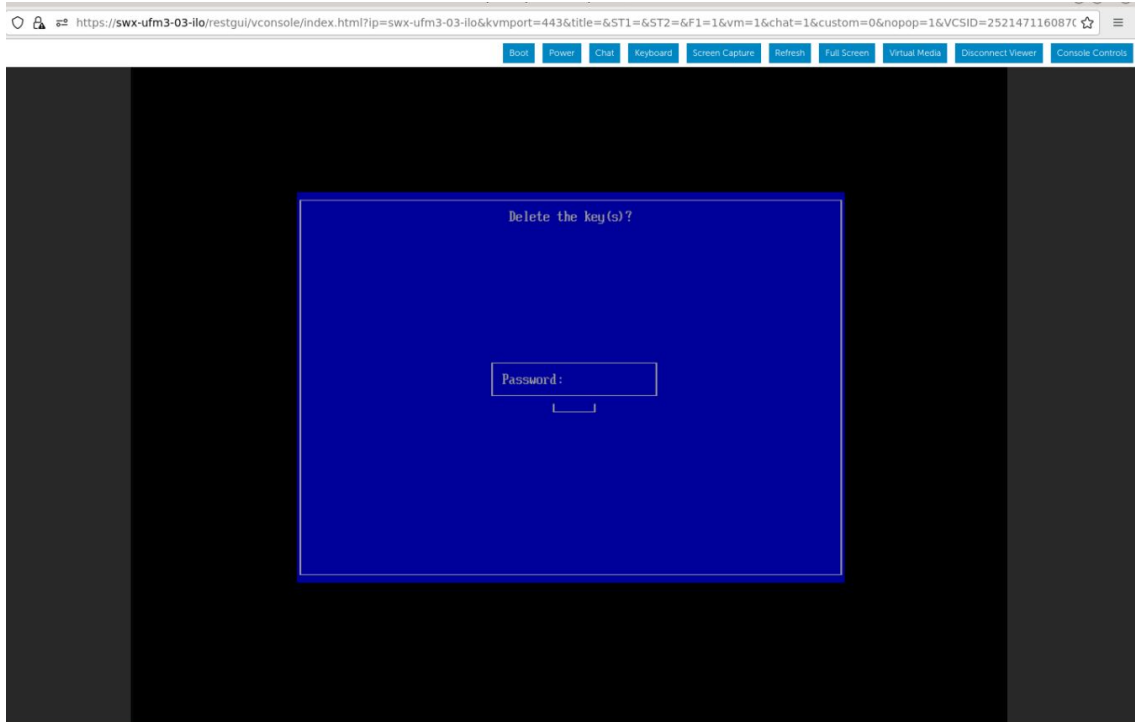
11. Select "Continue" from the menu and press the Enter key.



12. Select "Yes" from the menu and press the Enter key.



13. Once a password prompt appears, enter the OS root user credential.



14. Select "Reboot" from the menu and press Enter. Upon reboot completion, the certificate is removed.



13.3 Appendix - Deploying UFM Appliance from an ISO File

This section provides a step-by-step guide for deploying UFM Enterprise Appliance from an ISO file.

The ISO installation is set to use interface "eno8303" via a DHCP as default; if DHCP is unavailable, the installer will request manual intervention to set the IP address manually on "eno8303" or to skip the IP settings altogether.

If IP settings are skipped, they can be set manually after the installation. Refer to [Getting Started](#).

If a different interface should be used, skip the IP settings when prompted.

13.3.1 Deploying UFM Appliance from an ISO File

Extract the `ufm-appliance-<version>-omu.tar` to a temporary directory.

```
Extract TAR file
```

```
tar xzf /path/to/tar.tar -C /tmp
```

An ISO file and an upgrade script will be present inside the directory.

```
Extract TAR file
```

```
ls -ltrh /tmp/ufm-appliance-<version>/
```

Follow the following steps based on the desired method of installation.

13.3.1.1 Virtual Media via Management Port

1. Open a web browser and navigate to `https://<IDRAC-ILO-address>`
2. On the Dashboard pane, click on the virtual console icon on the bottom right corner of the screen.

DRAC5 | Datacenter

Dashboard | System | Storage | Configuration | Maintenance | DRAC Settings

Dashboard

Graceful Shutdown | LED On | More Actions

Health Information

SYSTEM HAS CRITICAL ISSUES

System Health

● Critical

- Absence
- Power Supply

Storage Health

● Healthy

System Information

| | |
|--------------------------|-------------------|
| Power State | On |
| Model | Not Available |
| Host Name | |
| Operating System | |
| Operating System Version | |
| Service Tag | 38184P3 |
| BCS Version | |
| DRAC Firmware Version | 8.00.10.00 |
| IP Address(es) | 10.209.224.19 |
| DRAC MAC Address | 6c:5a:72:27:036d |
| License | Datacenter - Full |

Task Summary

View All Jobs

Ready Jobs: 0
No Pending Jobs

In-Progress Jobs: 0
No In-Progress Jobs

Completed Jobs: 12
0 With Errors
0 Failed

Recent Logs

| Severity | Description | Date and Time |
|--------------------------------------|---|--------------------------|
| ● | The power input for power supply 1 is lost. | Sun 28 Oct 2022 10:02:36 |
| ● | The power input for power supply 1 is lost. | Wed 19 Oct 2022 09:18:44 |
| ● | System BCS has halted. | Mon 29 Aug 2022 12:32:14 |
| ● | Power supply redundancy is lost. | Mon 29 Aug 2022 12:19:30 |
| ● | The power input for power supply 1 is lost. | Mon 29 Aug 2022 12:19:29 |
| ● | The chassis is closed while the power is off. | Mon 29 Aug 2022 12:19:23 |
| ● | The chassis is open while the power is off. | Mon 29 Aug 2022 12:19:19 |
| ● | The power input for power supply 1 is lost. | Mon 29 Aug 2022 12:07:02 |
| ● | The chassis is closed while the power is off. | Sun 31 Jul 2022 14:48:01 |
| ● | The chassis is open while the power is off. | Sun 31 Jul 2022 14:44:01 |

Notes

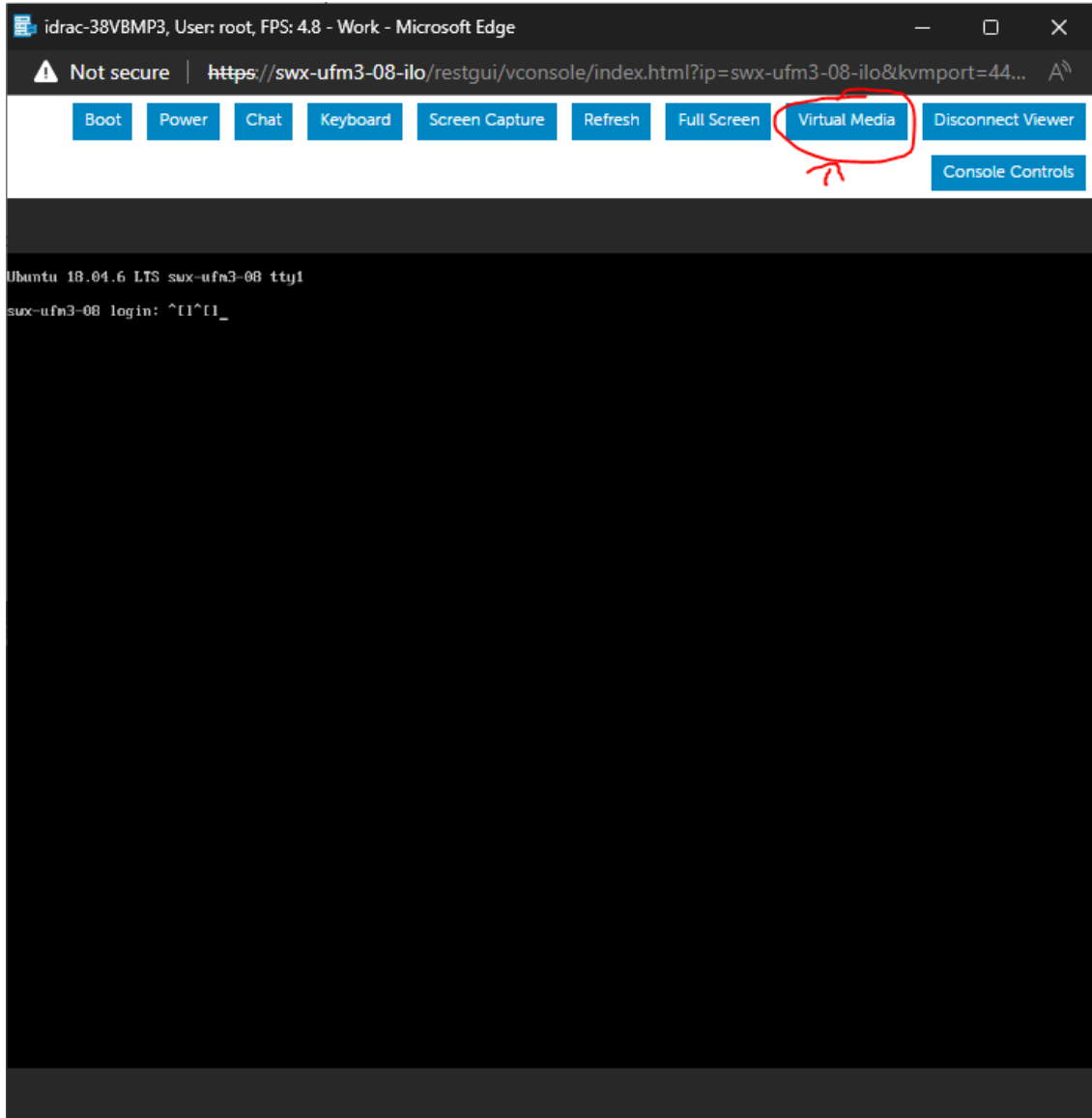
view all + add note

| Date and Time | Description |
|--|-------------|
| There are no work notes to be displayed. | |

Virtual Console

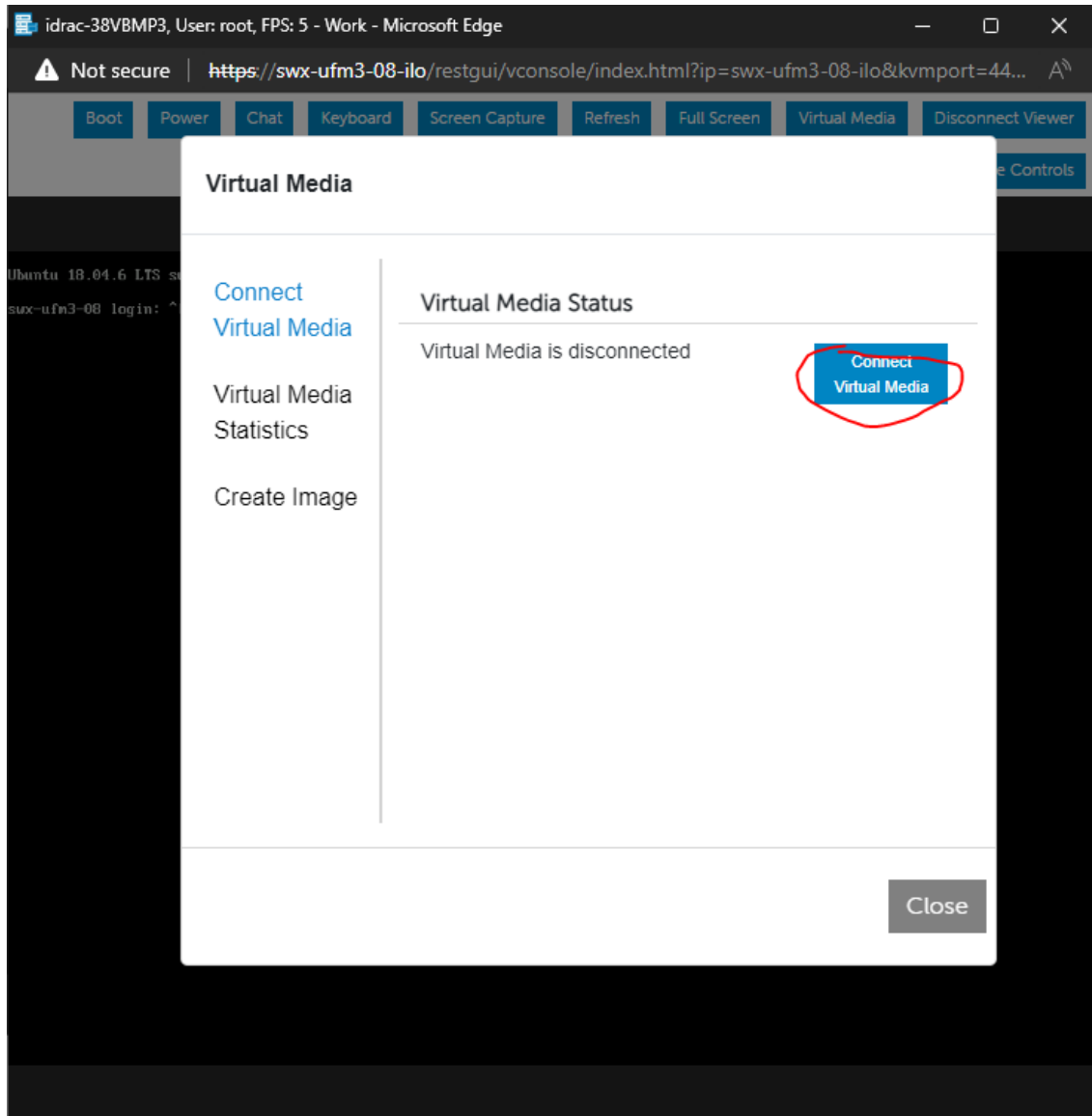
view all Settings

3. A new virtual console window will pop out, on the top right corner, click on the virtual media.



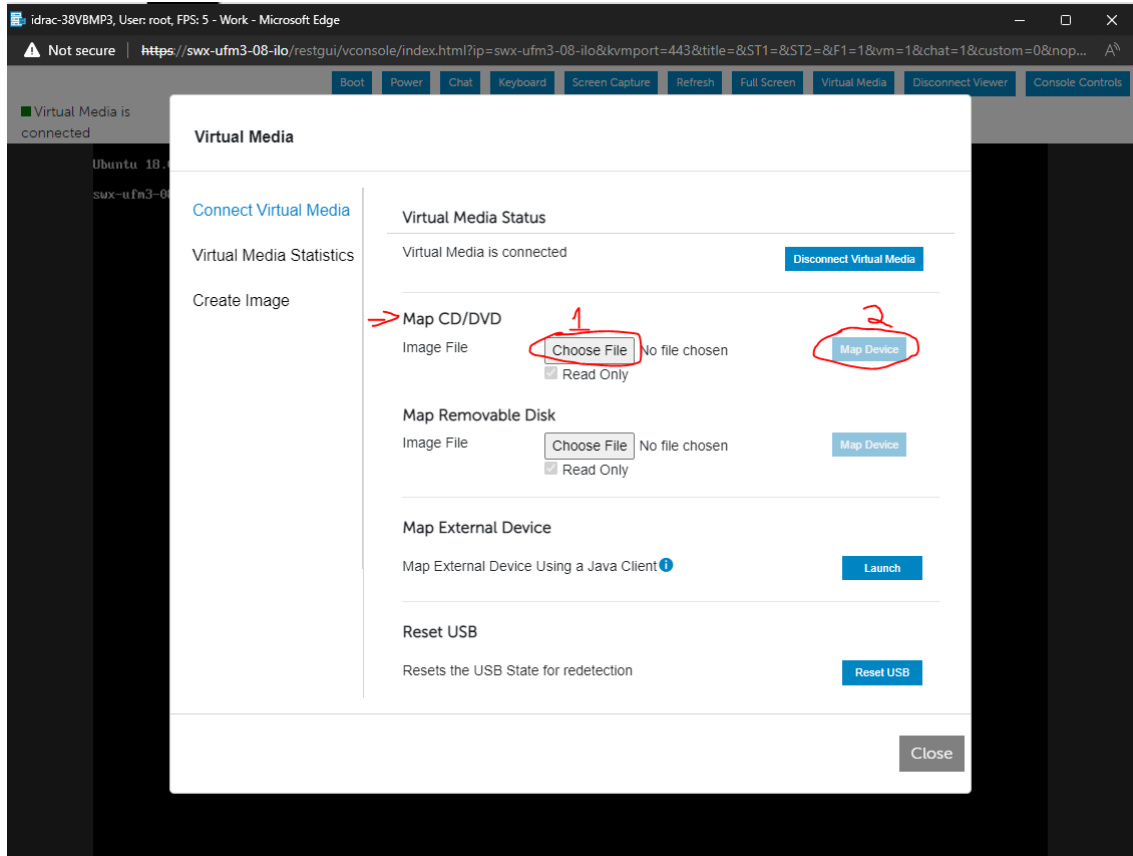
A new console window will appear

4. Click on the "Connect Media" button.

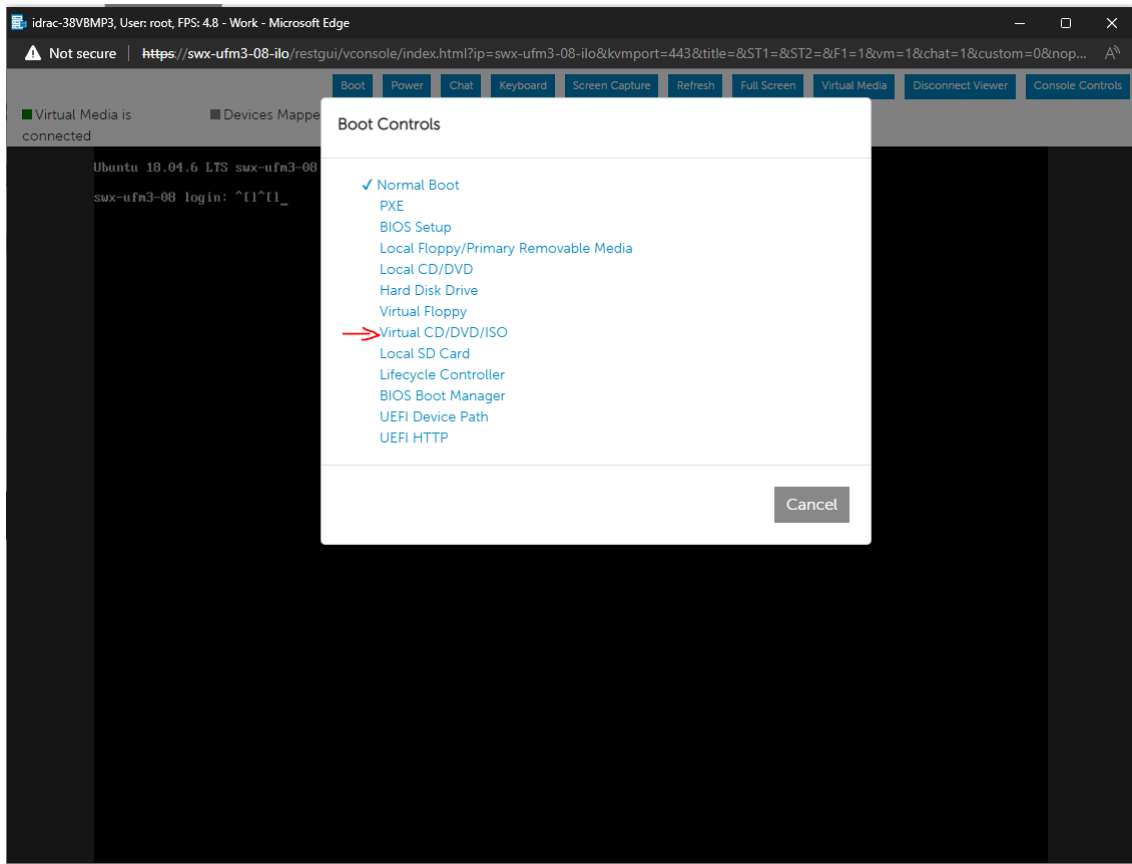


5. Under the "Map CD/DVD" section, click on "Choose file" and select the `ufm-appliance-<version>.iso` file extracted from the tar archive previously extracted and click on the

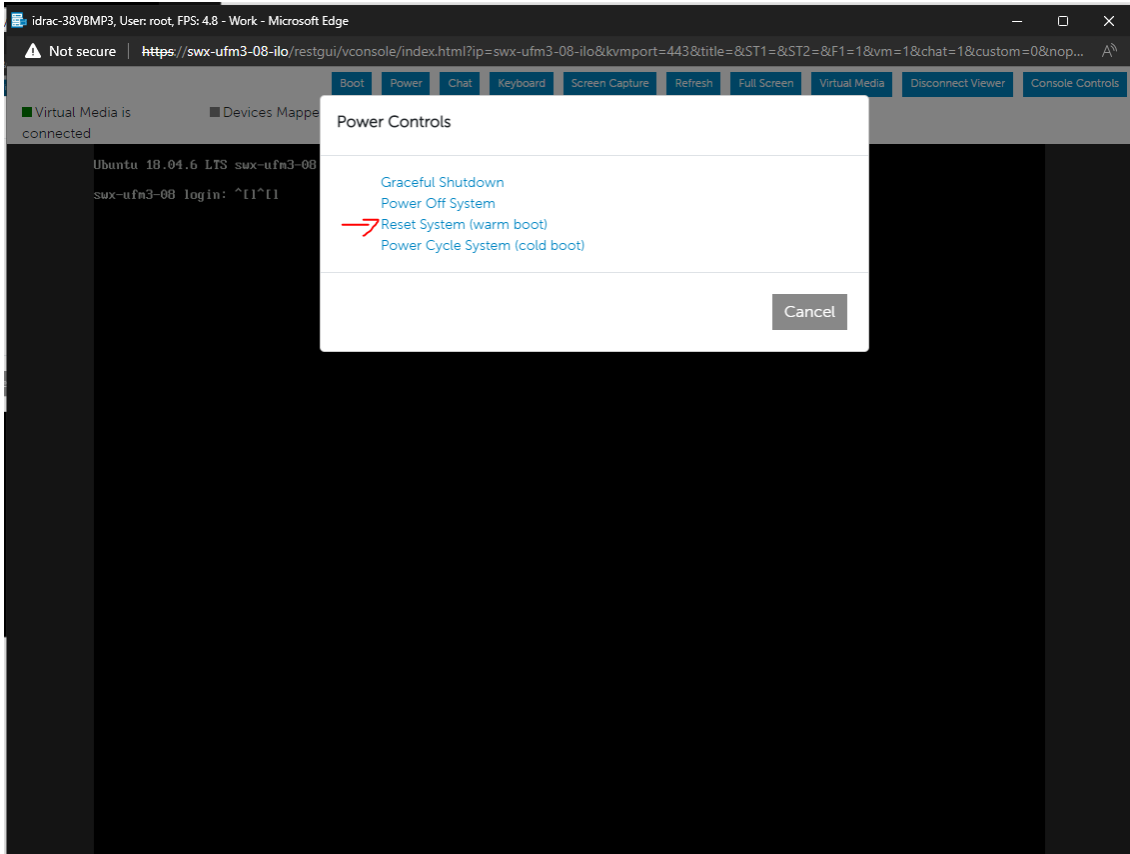
"Map Device" button. Then, "Close".



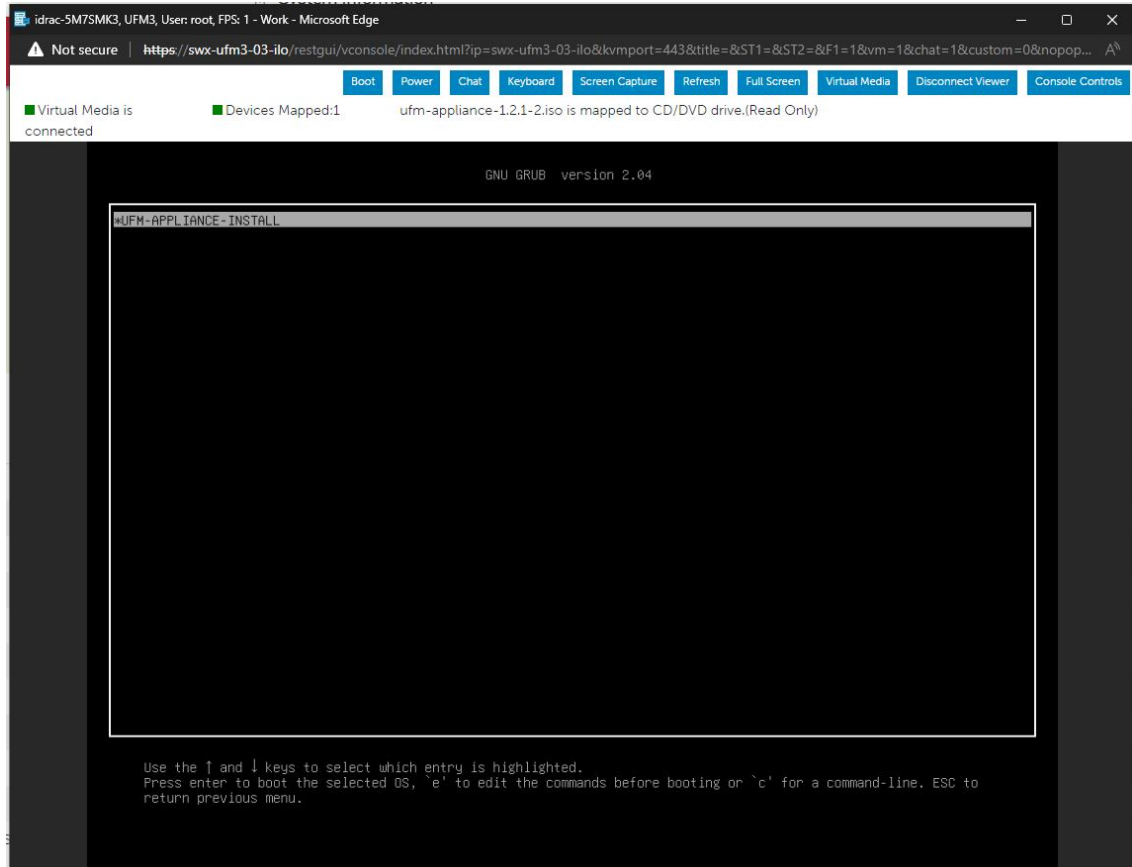
6. Click on the "Boot" menu button on the top left, on the opened menu choose "Virtual CD/DVD/ISO".



7. Click on the "Power" menu button and select "Reset System (warm boot)" entry.



8. At this point an automatic installation should start.



Installation will auto start after 30 seconds, press the enter key to start it immediately.

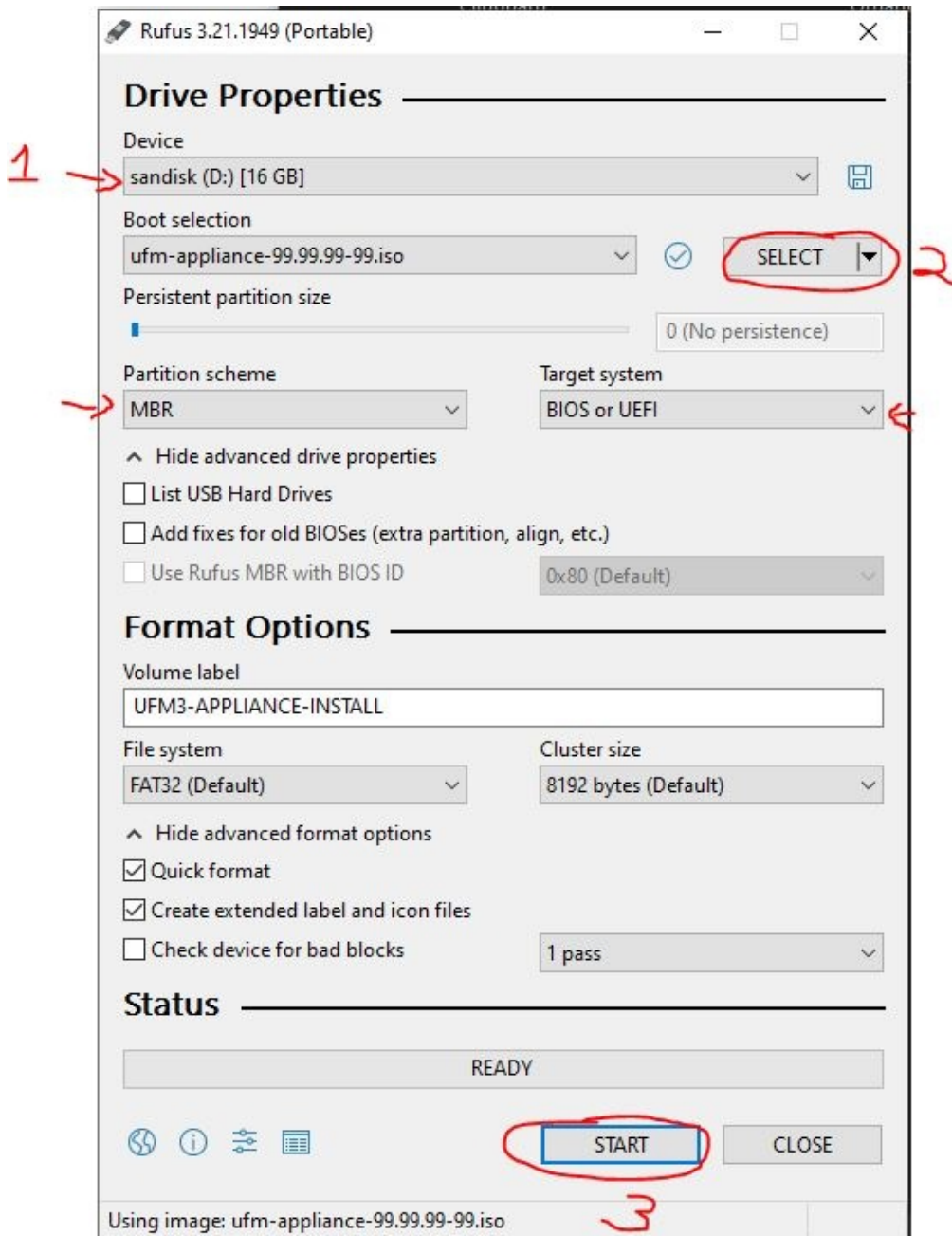
9. Proceed to [Finalizing the Installation](#).

13.3.1.2 Physical USB

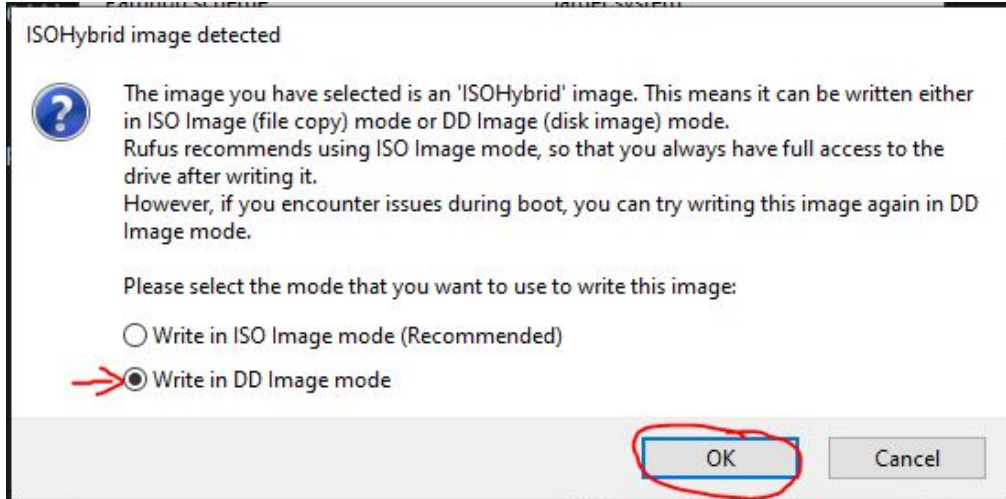
13.3.1.2.1 Burn ISO to USB

13.3.1.2.1.1 Windows

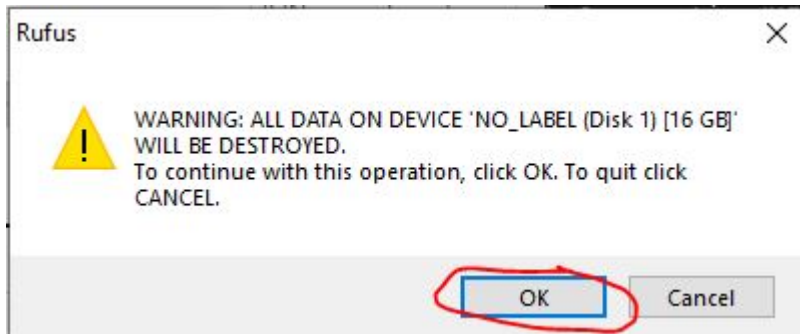
1. Download and open Rufus (Rufus).
2. Select the USB device from the drop down menu under "Devices".
Click on "SELECT" and select `ufm-appliance-<version>.iso`
Validate that the "Partition Scheme" is MBR and "Target System" is "BIOS or UEFI", as seen in the screenshot below.
Click "START".



3. An "ISOHybrid image detected" prompt will pop up, choose "Write in DD mode" and click "OK".



4. Another message will appear stating that all data on the USB device will be lost, click "OK and continue".



5. Wait for Rufus to finish.

13.3.1.2.1.2 Linux

1. Identify the USB drive:

Do not run the following commands on a hard drive device, but only on the USB. The USB drive in the below command is mapped to sdb.

```
root@ubuntu18:~# ls -ltrh /dev/disk/by-id/usb*  
lrwxrwxrwx 1 root root 9 Jan 2 13:44 /dev/disk/by-id/usb-SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:  
0 -> ../../sdb  
lrwxrwxrwx 1 root root 10 Jan 2 13:44 /dev/disk/by-id/usb-SanDisk_Cruzer_Glide_3.0_4C530000040724111091-0:  
0-part1 -> ../../sdb1
```

2. Copy the `ufm-appliance-<version>.iso` to the USB using the following dd command:

Do NOT run the following commands on a hard drive device but only on the USB. The USB drive in the below command is mapped to `/dev/sdb`.

```
dd if=/path/to/ufm-appliance-<version>.iso of=/dev/sdb bs=4M status=progress oflag=sync
```

3. Verify that the USB is bootable:

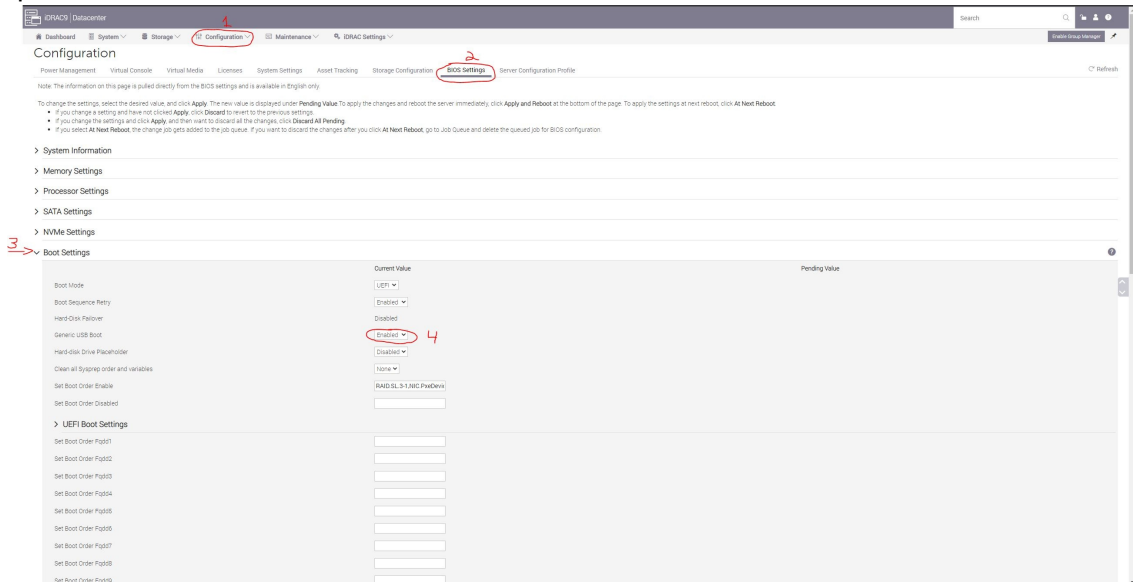
```
root@ubuntu18:~# fdisk -l /dev/sdb
Disk /dev/sdb: 14.9 GiB, 16005464064 bytes, 31260672 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x594ec03e

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1  *        64 15679439 15679376   7.5G 17 Hidden HPFS/NTFS
```

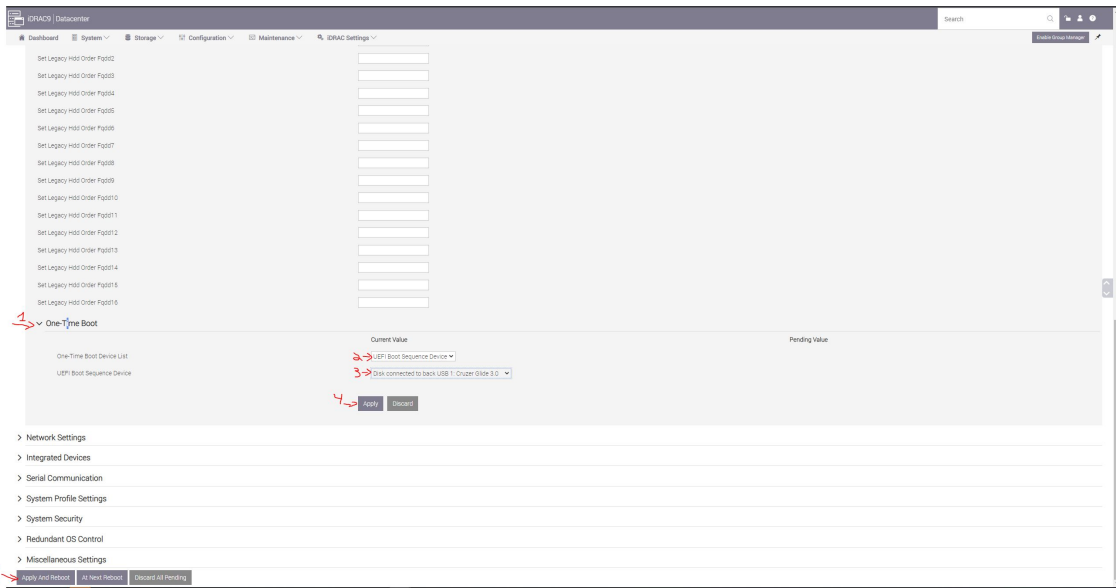
4. Unplug the USB.

13.3.1.2.2 Manufacture UFM Appliance via the USB

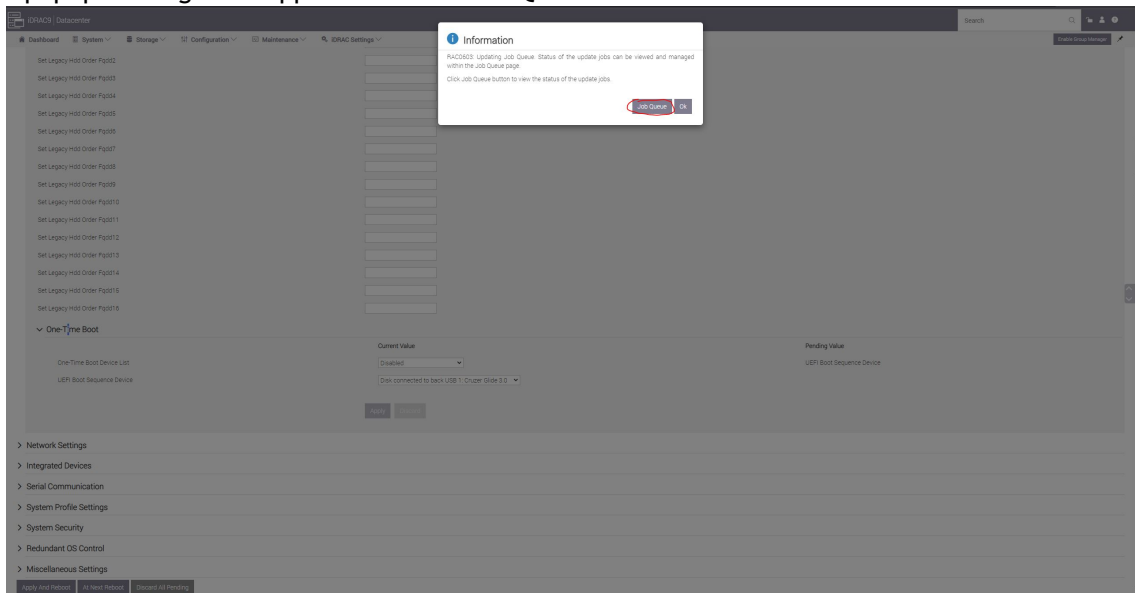
1. Plugin the USB device to the back panel (Front panel USB is disabled).
2. Open a web browser and navigate to <https://<IDRAC-ILO-address>>.
3. Navigate to "Configuration" → "BIOS Settings" → "Boot Settings" and set "Generic USB boot" option to enabled.



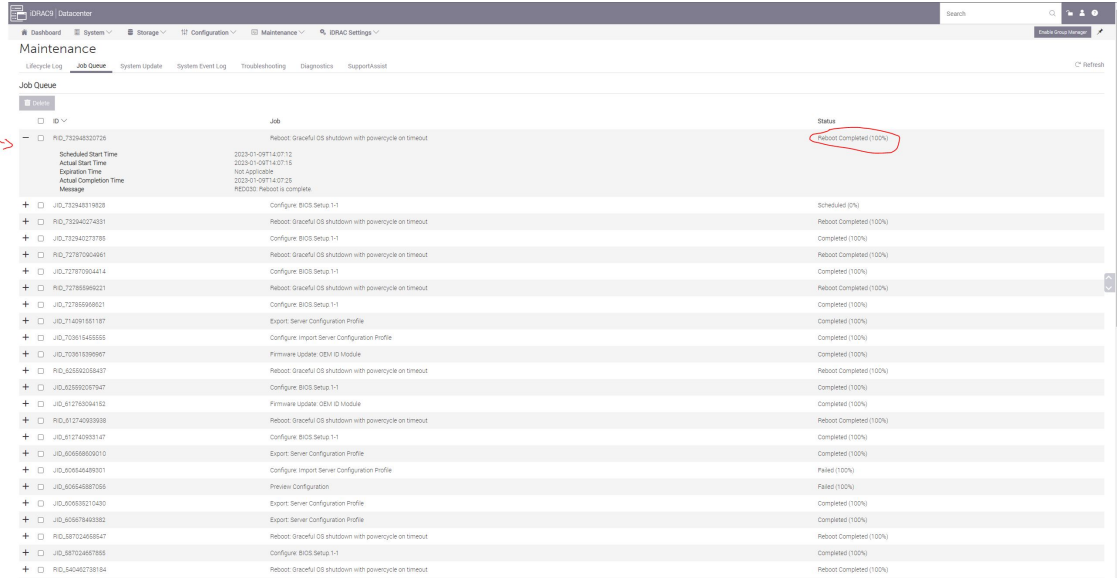
4. On the same pane, scroll down to "One-Time Boot" → "One-Tome Boot Device List" select "UEFI Boot Sequence Device".
In "UEFI Boot Sequence Device", select the connected USB device and click apply.
On the bottom of the page click on "Apply And Reboot" button.



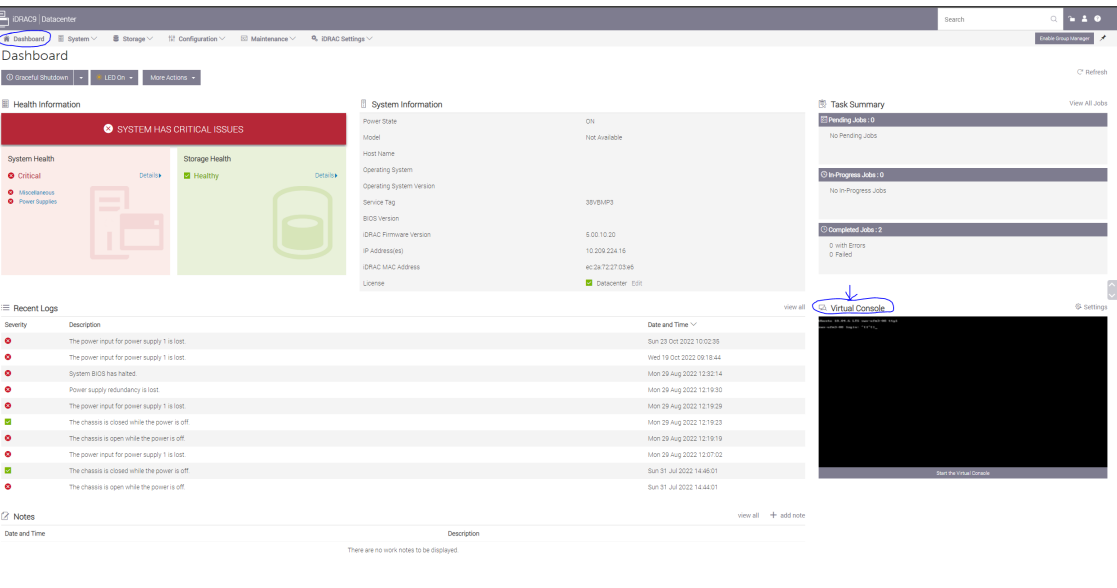
5. A popup message will appear click on "Job Queue" button.



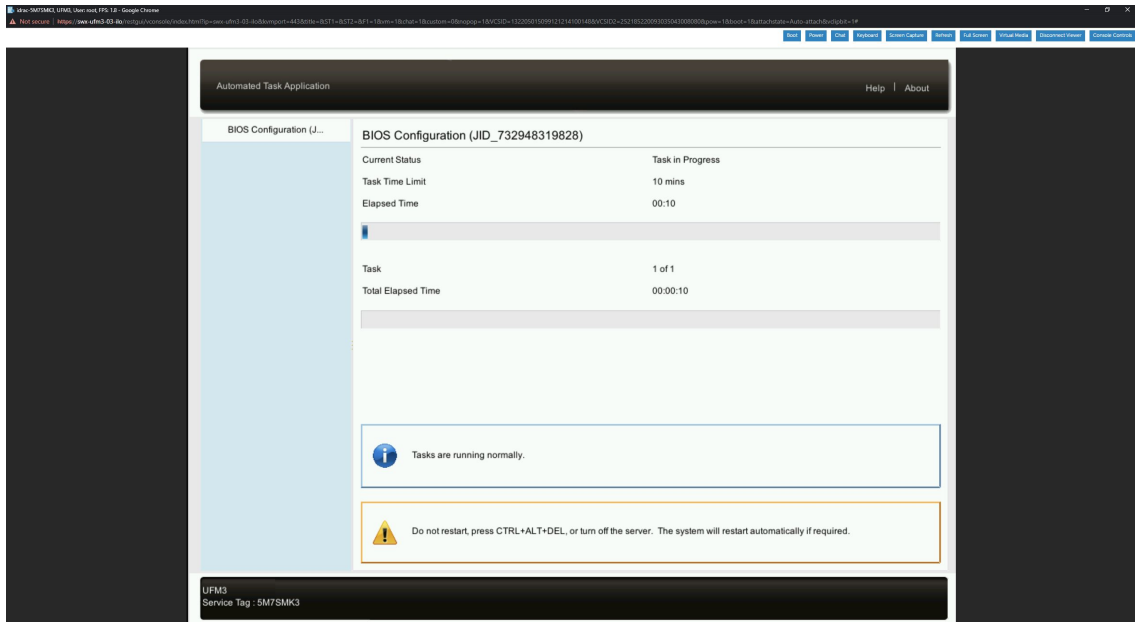
6. A "Job Queue" pane will open to monitor the progress of the created job.



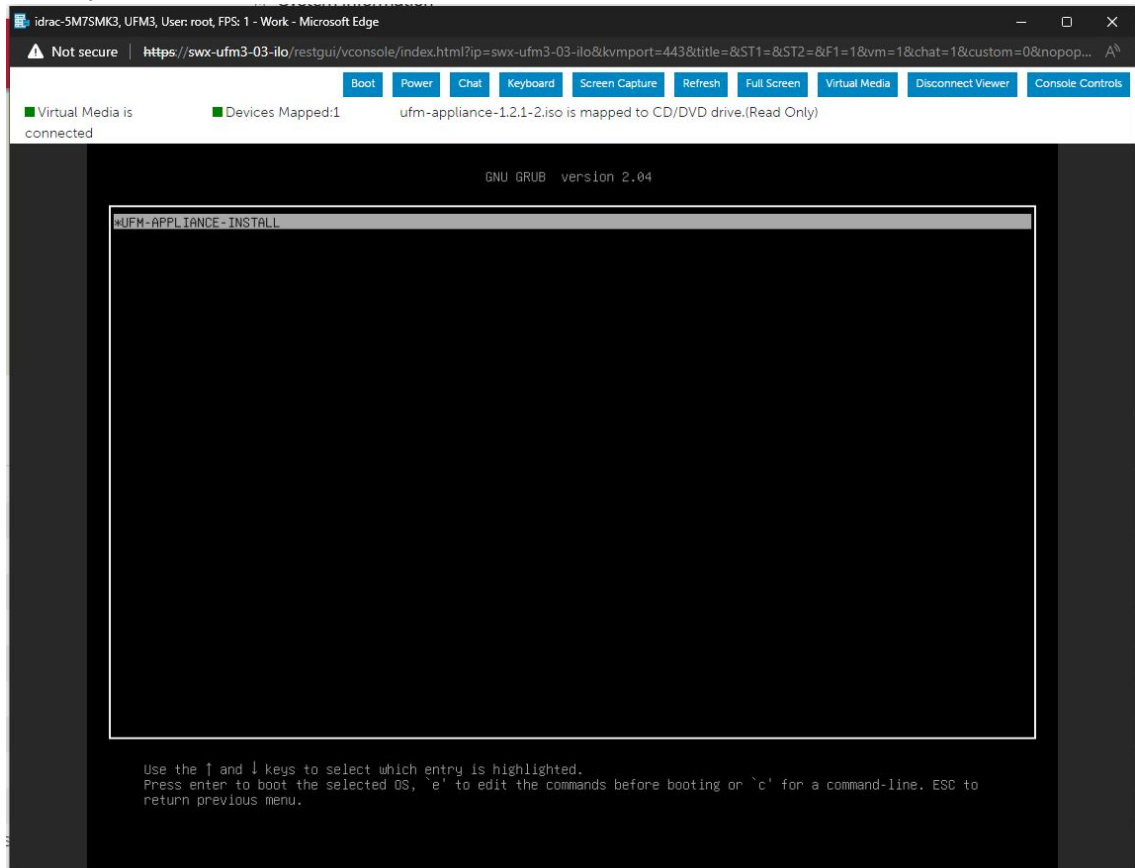
7. Navigate to the Dashboard pane, click on the virtual console icon on the bottom right corner of the screen.



A new console window will appear that shows the progress of restarting the node to USB.



8. At this point an automatic installation should start.



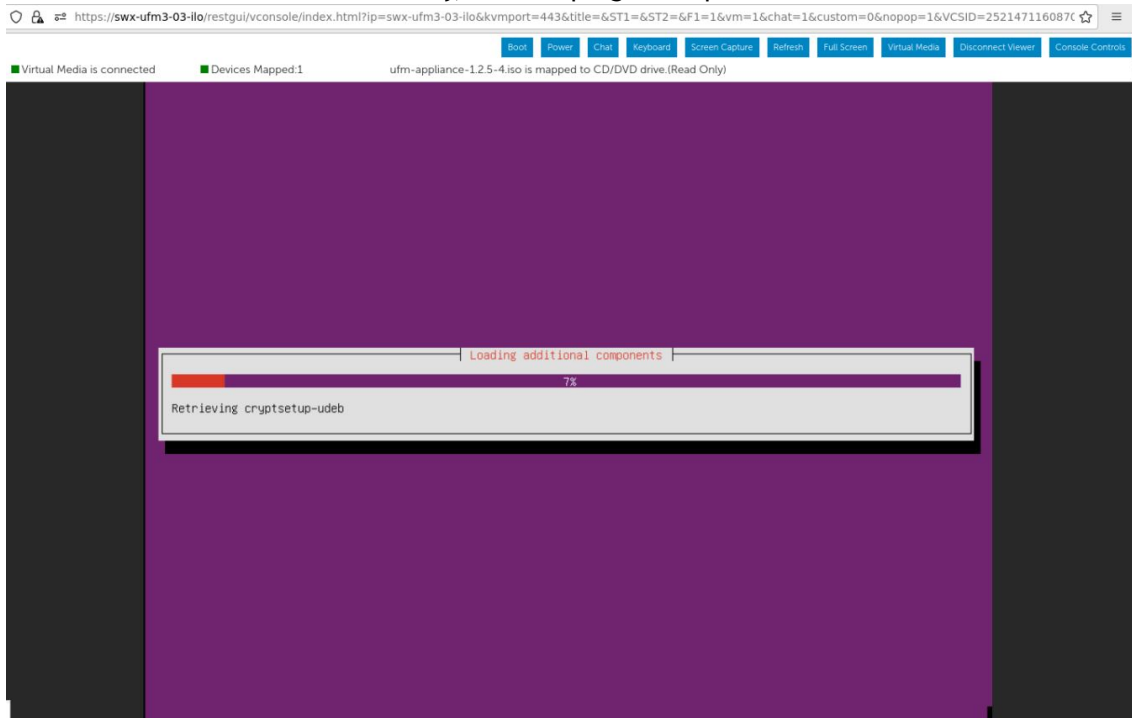
The installation will auto start after 30 seconds, press the enter key to start it immediately.

9. Proceed to the following section to proceed with the installation.

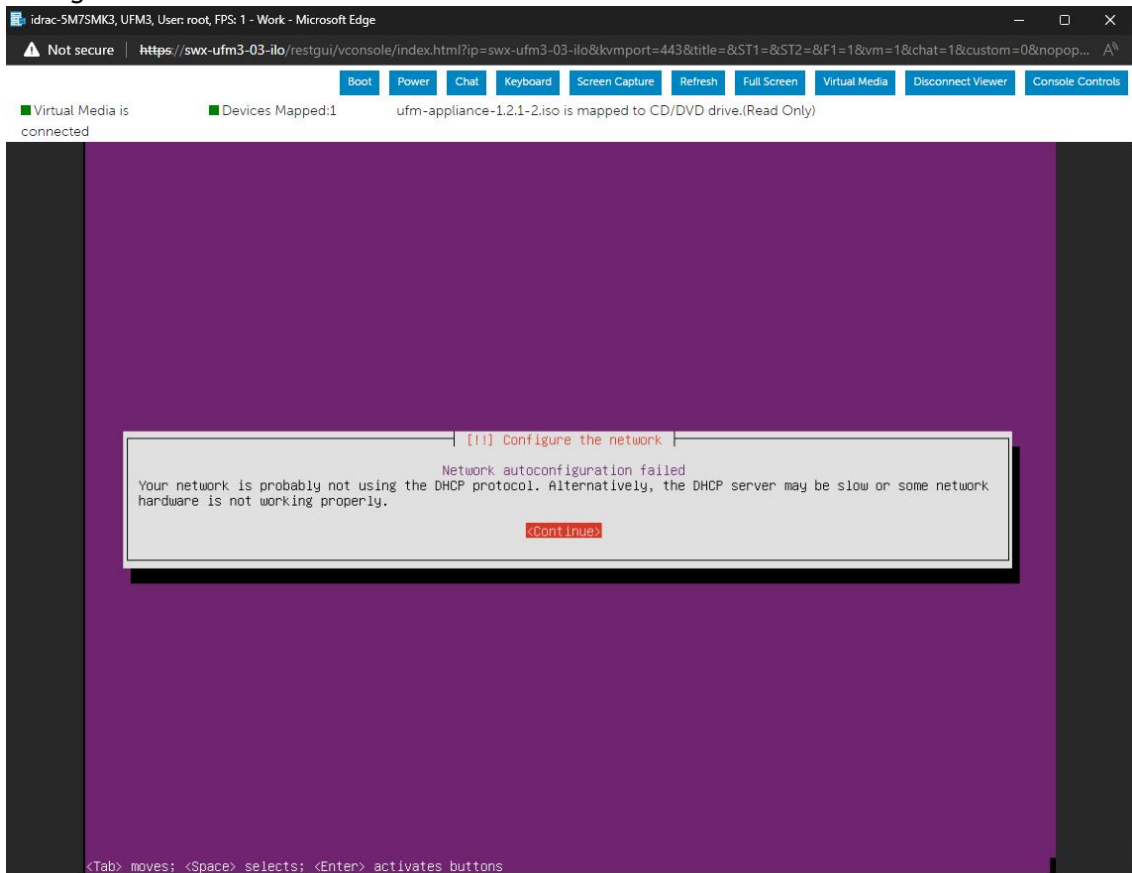
13.3.1.3 Finalizing the Installation

Installation may take 20-90 minutes and depends on the chosen media; with USB it takes around 20 minutes and via the virtual media take around 90 minutes (this may vary and depends on network speed).

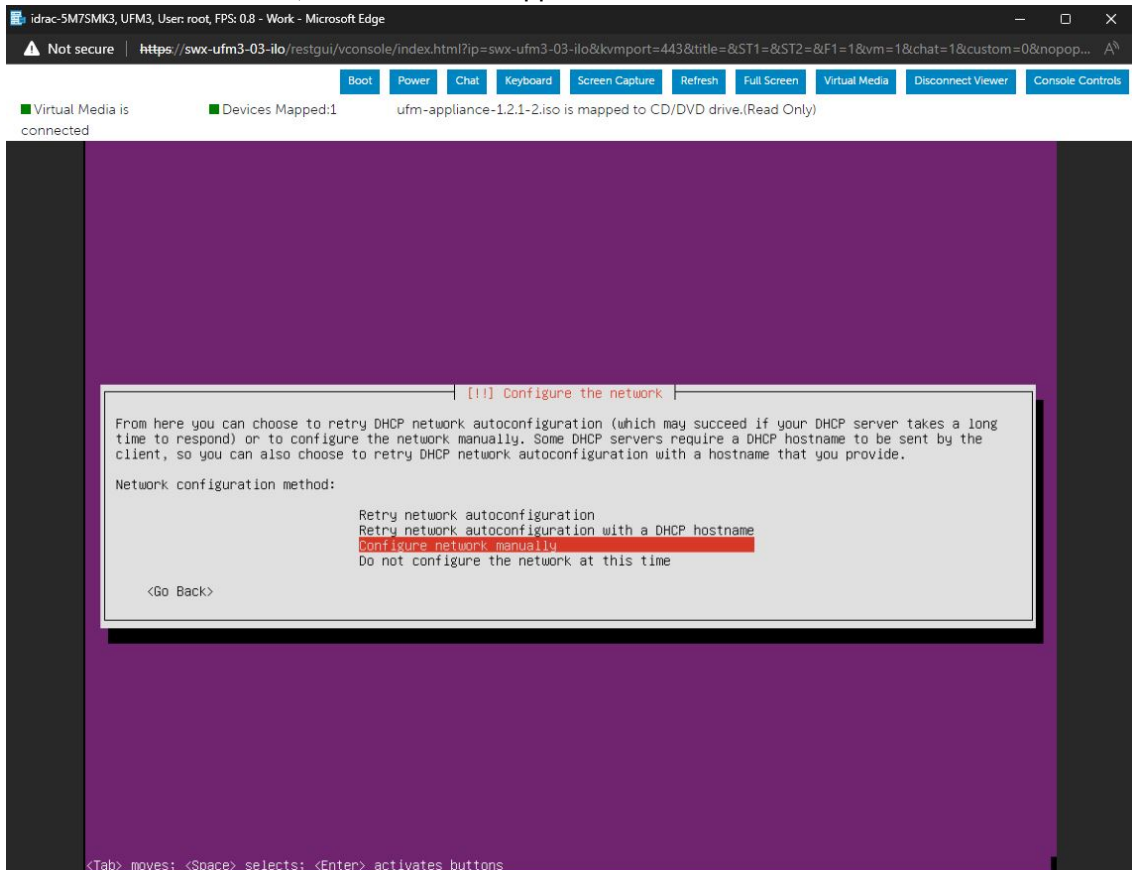
1. Installation should start automatically, and the progress is presented on the screen.



2. In case a DHCP is not available or not configured, a prompt will pop up with notification stating that DHCP cannot be set.

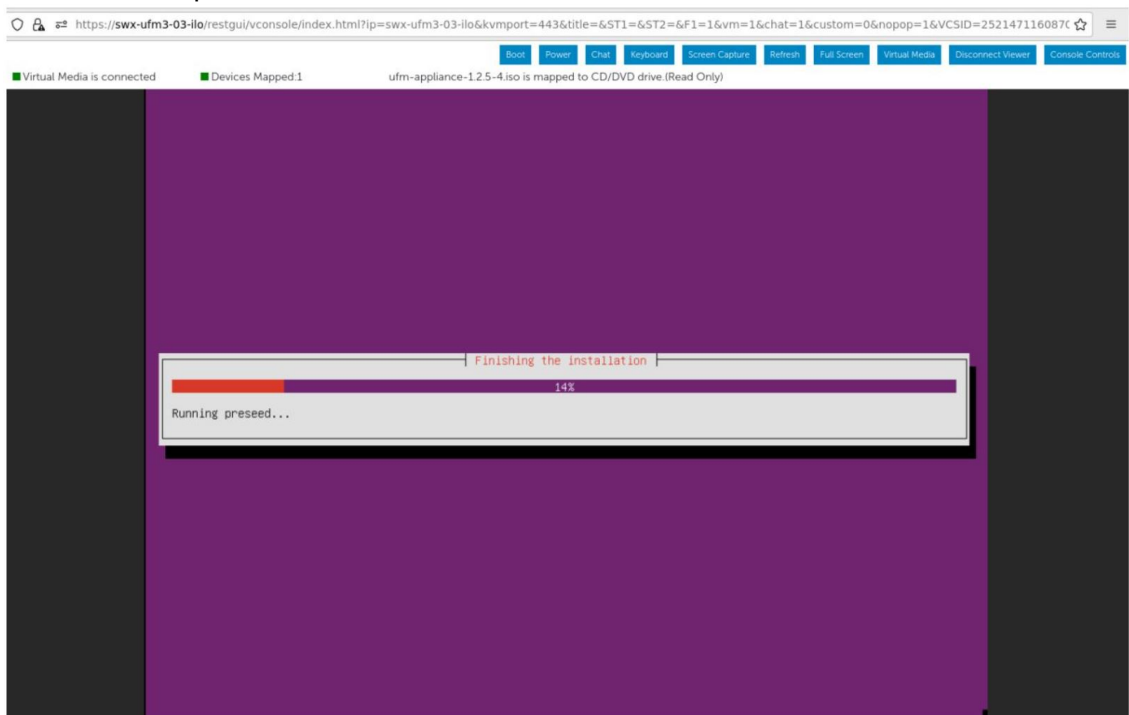


3. Press "Enter" to continue, a sub menu will appear.



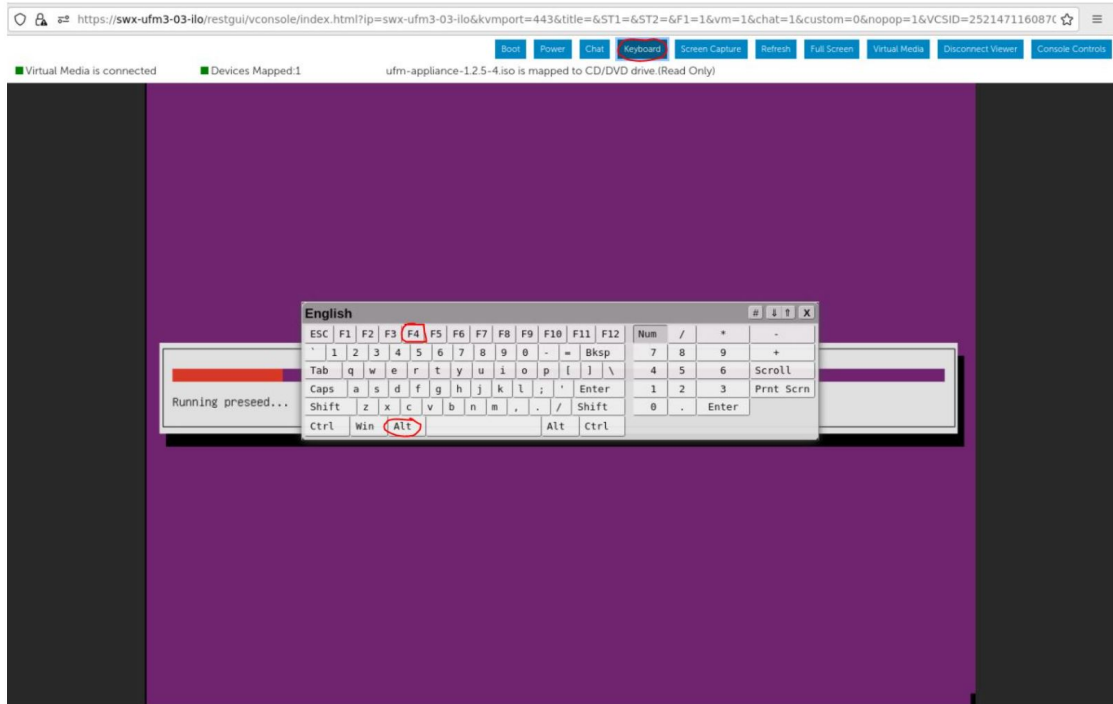
You can choose the preferred option and follow the instructions on the screen by configuring it manually, or skip network configuration and add them at a later point.

4. The installation procedure should continue.

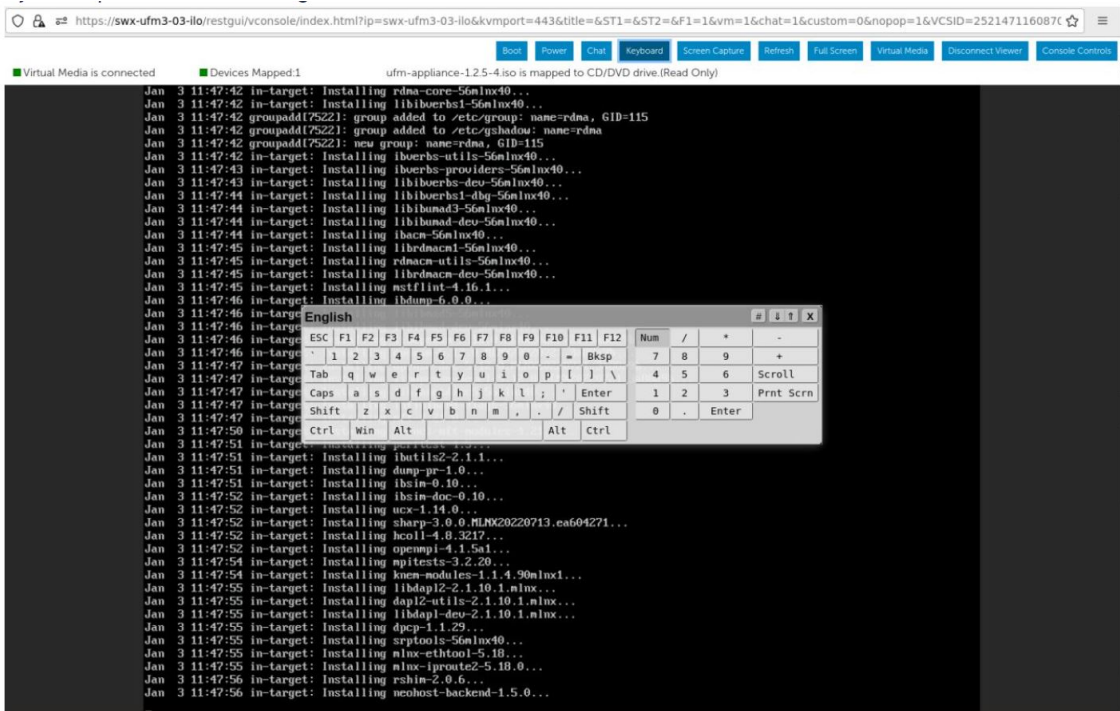


The installer may seem stuck when the status bar gets to "Running preseed" (14-16 %) - it takes a while to pass this, the script runs in the background and the progress can be seen by switching to tty4 (optional) by opening the virtual keyboard.

This should be done on the virtual keyboard, otherwise it will close the installation window. The installation window can be opened by pressing "ALT+F4" on the virtual keyboard.



tty4 will open and the install log will show current status.



To return to the progress screen, click on "ALT+F1" on the virtual keyboard.

5. The server will automatically reboot when the installation procedure is completed.
6. At this point, the login screen will appear

The installation procedure is not finished yet. At this point, an automatic service will install additional SW (including the UFM Enterprise Appliance).

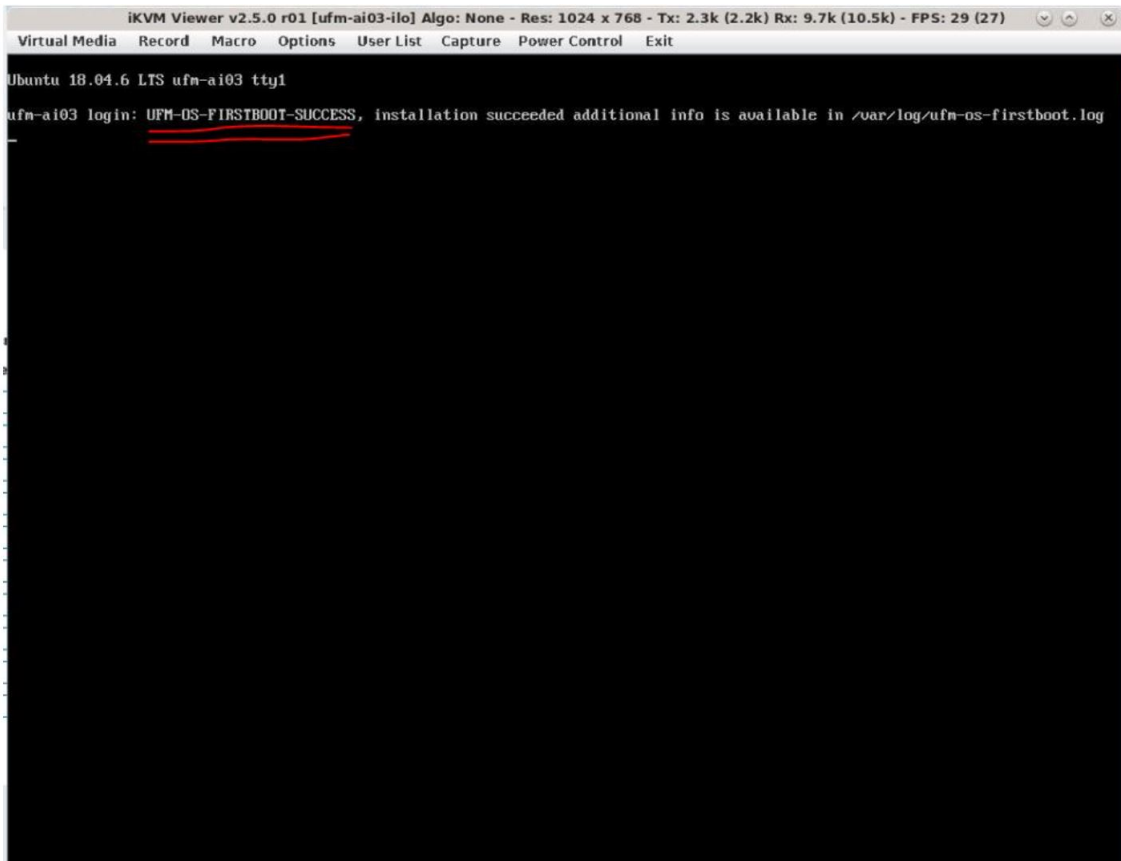
Upon installation completion, a message will appear on any attached terminal stating UFM-OS-FIRSTBOOT-SUCCESS for successful installation, or UFM-OS-FIRSTBOOT-FAILED for failed installation.

A log can be checked in `/var/log/ufm-os-firstboot.log`.

The below is an example from an attached ssh session:

```
root@ufm-ai03:~#
root@ufm-ai03:~#
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

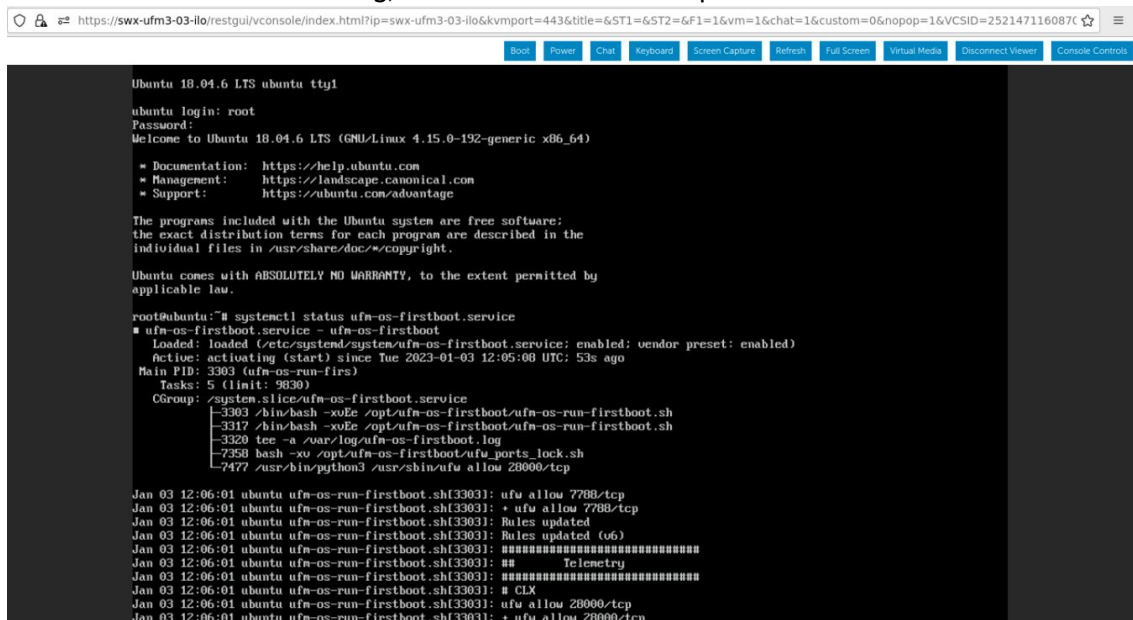
Example from the console web screen:



To manually check if the installation procedure has completed or is still running:

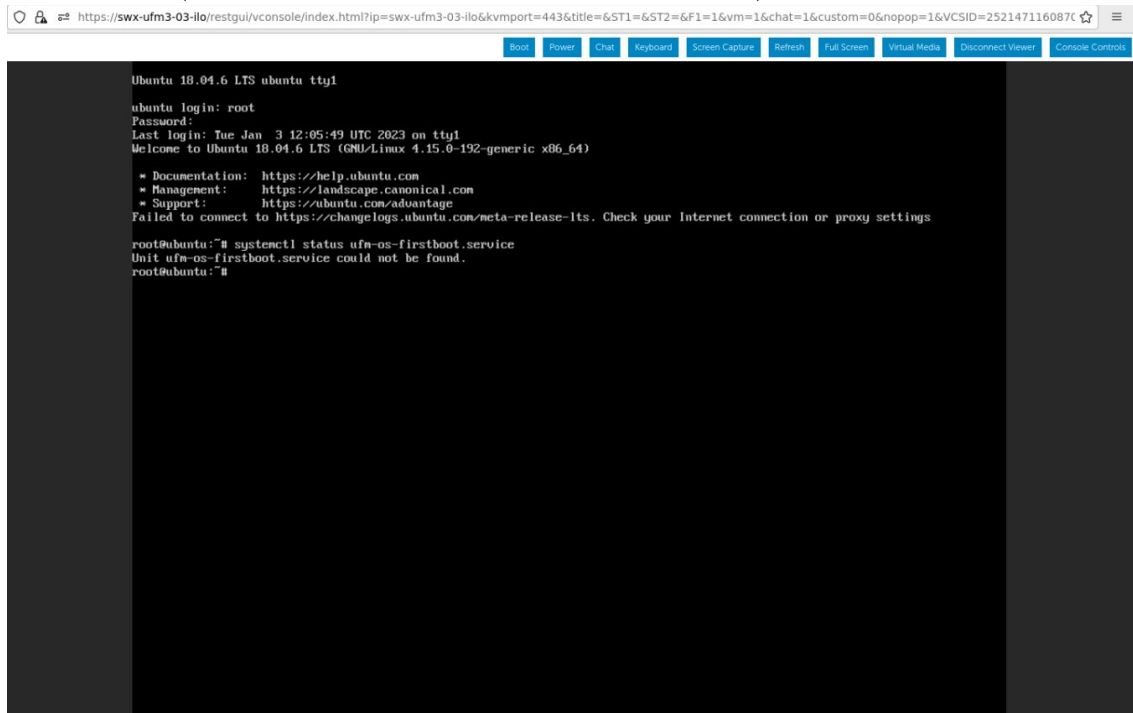
```
systemctl status ufm-os-firstboot.service
```

If the installation is still running, the below status will be presented:



If the installation is completed, an error message stating that `ufm-os-firstboot.service`

does not exist (as it is deleted when the installation is finished).



7. The installation is now finished and the UFM Enterprise Appliance can be started. If the network configuration step is skipped in previous steps, it can now be configured.

13.4 Appendix - UFM Factory Reset

This section provides a comprehensive guide on resetting UFM to its original factory settings.

WARNING!!! this operation will remove all user data and configuration and will restore UFM to its factory defaults.

The UFM Factory-Reset will exclusively revert UFM to its original factory settings, leaving HA configurations unaffected. To remove HA, it is essential to execute `ufm_ha_cluster cleanup` before initiating the factory reset.

13.4.1 UFM Docker Container Factory Reset

To reset UFM to its factory defaults when using UFM on a Docker container, follow these steps.

1. Ensure that UFM is not up and running. If UFM is running, stop it.
For Stand-alone (SA) installations:

```
systemctl stop ufm-enterprise
# validate that ufm is not running
systemctl status ufm-enterprise
```

For High-Availability setups (perform the following on the master node only):

```
ufm_ha_cluster stop
# validate that ufm is not running
ufm_ha_cluster status
```

2. Run `mellanox/ufm-enterprise` Docker Container with the following flags:

WARNING: This operation will erase all user data and configurations, resetting UFM to its factory defaults.

CAUTION: This step does not require user confirmation, meaning UFM will be restored to factory defaults immediately once initiated.

```
docker run -it --name=ufm_installer --rm \
-v /var/run/docker.sock:/var/run/docker.sock \
-v /tmp:/tmp \
-v /opt/ufm/files:/opt/ufm/shared_config_files/ \
mellanox/ufm-enterprise:latest \
--factory-reset
```

| Flag | Type | Description |
|--|-----------|---|
| <code>--name=ufm_installer</code> | Mandatory | The container name must be called <code>ufm_installer</code> . |
| <code>-v /var/run/docker.sock:/var/run/docker.sock</code> | Mandatory | The docker socket must be mounted on the docker container. |
| <code>-v /tmp:/tmp</code> | Optional | Logs of the operation can be viewed in <code>/tmp</code> on the host in case it is mounted. |
| <code>-v /opt/ufm/files:/opt/ufm/shared_config_ufm/</code> | Mandatory | For the factory reset to persist, it is essential to have the <code>/opt/ufm/files</code> directory mounted from the host. TBD: eylon - naming convention of the <code>/opt/ufm/files/</code> |
| <code>mellanox/ufm-enterprise:latest</code> | Mandatory | The docker image name. |
| <code>--factory-reset</code> | Mandatory | This action will signal the UFM container to initiate the factory reset process. |

13.4.2 UFM Factory Reset via CLI

13.4.2.1 UFM Factory Reset in HA Configuration

The UFM Factory-Reset will exclusively revert UFM to its original factory settings, including the HA configurations.

1. On the Master node, stop the UFM cluster. Run:

```
ufmapl (config) # no ufm start
```

2. On both Master and Standby nodes, reset the UFM cluster configuration to factory settings. Run:

```
ufmapl (config) # no ufm ha
```

After the factory reset procedure is completed, both UFM nodes are configured as Standalone mode.

13.4.2.2 UFM Factory Reset in Standalone Configuration

The UFM Factory-Reset will exclusively revert UFM to its original factory settings.

1. Stop the UFM service. Run:

```
ufmapl (config) # no ufm start
```

2. Reset the UFM data to factory settings. Run:

```
ufmapl (config) # ufm data reset
```

13.5 Appendix - Software Components Upgrade

It is recommended to upgrade all UFM Enterprise appliance software components as listed in [UFM Enterprise Appliance Upgrade](#).

This section includes optional instructions on how to upgrade [specific](#) software components.

- [Upgrading UFM Enterprise Appliance Operating System](#): Involves UFM Enterprise appliance [operating system upgrade only](#).
- [Upgrading All UFM-Related Software Components](#): Involves [all UFM-related software components](#), including UFM Enterprise, Docker Container and UFM HA. The upgrade is done on all software components at once.
- [Upgrading Specific UFM-Related Software Component](#): Involves upgrading [specific UFM-related software components](#) separately.

13.5.1 Upgrading UFM Enterprise Appliance Operating System

This section provides a step-by-step guide for UFM Enterprise Appliance Operating System upgrade.

Each UFM Enterprise Appliance software has an additional tar file with a `-omu.tar` suffix (OMU stands for OS Manufacture and Upgrade). This tar file can be used to re-manufacture the server and to upgrade the operating system/software on the server.

13.5.1.1 Extracting the Software

1. Copy the OMU tar file to a temporary directory on the server.

```
UFM-APPLIANCE - ufm-appliance<version>-<revision>-omu.tar
```

2. Extract the contents of the tar file to /tmp.

```
tar vxf ./ufm-appliance-<version>-<revision>-omu.tar -C /tmp/
```

3. Change to the extracted directory.

```
cd /tmp/ufm-appliance-<version>-<revision>-omu
```

4. An upgrade script and an ISO file are included in the extracted directory.

```
ls -l ./# ls -l ./
./ufm-os-upgrade.sh
ufm-appliance-<version>-<revision>.iso
```

The following flags are available in the upgrade script help.

```
# ufm-os-upgrade.sh --help
ufm-os-upgrade.sh will upgrade and install OS packages.

IMPORTANT!!! a reboot is mandatory after the finalization of this script,
kernel and kernel models will not work properly until the server is rebooted.

Additional SW installations will be automatically invoked after reboot,
a message will pop on all open terminals with the installation status:
"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.
"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.

Additional info will be available in "/var/log/ufm_os_upgrade_@@UFM-OS-VERSION@@.log" log file.
Upgrade steps status information can be viewed in "/var/log/ufm_os_upgrade_@@UFM-OS-VERSION@@_status.log"
log file.

Syntax: ufm-os-upgrade.sh [options]

options
-d,--debug          debug info will be visible on the screen.

-r,--reboot         Automatically reboot the server when upgrade is finished.
                   P.S. if secure boot is enabled and a new certificate is enrolled
                   the server will not automatically reboot even if this flag is set.

-y,--yes            Will not prompt for user acknowledgements, use with CAUTION user prompts will be
                   assumed as answered yes.

-h,--help          print this help message.
```

IMPORTANT!!! System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server at the end of the upgrade. Note that some kernel modules may not work properly until server reboot is performed.

13.5.1.2 Standalone Mode Upgrade

1. Stop UFM service by running the following command:

```
systemctl stop ufm-enterprise.service
```

2. Run the upgrade script.

System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server.

The `--appliance-sw-upgrade` flag CAN NOT !!! be supplied to upgrade the UFM Enterprise Appliance SW.

The `-y` flag can be supplied to skip user questions (the flag does not automatically reboot the server on its own. For auto reboot, combine with the `-r` flag)

Once a secure boot certificate is updated/installed, the script will not auto reboot even if `-y` and `-r` flags are provided. That is because the addition of certificates require manual user intervention at boot (after the upgrade).

There is a 10 seconds window to press any button when prompted during the boot procedure and insert the server root password in order to import the certificate. Further details are available in [Appendix - Secure Boot Activation and Deactivation](#).

In the following example the server will auto reboot when upgrade is finished.

```
./ufm-os-upgrade.sh -y -r
```

3. In case a secure-boot certificate is installed/upgraded, the following warning is presented:

```
WARNING!!!
The secure boot certificate have been renewed, to enroll the newly installed certificate:
[1] reboot the server
[2] upon boot a BIOS screen will pop out notifying a new certificate have been enrolled
    if secure boot is disabled discard it and continue with the boot process
[3] There is a 10 seconds window to apply the new certificate (if missed please refer to the manual on how to update the certificate manually)
[4] follow the instructions on the screen, the password will be the root user password
if secure boot is not enabled please discard this message.
```

In that case the server does not reboot automatically, a manual configuration is required at boot (a 10 second prompt appears during the boot. For more information, refer to [Appendix - Secure Boot Activation and Deactivation](#).

To continue with the upgrade procedure, manually reboot the server from as instructed in [Appendix - Secure Boot Activation and Deactivation](#).

4. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:

" UFM-OS-FIRSTBOOT-FAILURE " - if installation is failed.

" UFM-OS-FIRSTBOOT-SUCCESS " - if installation succeeded.

Example:

```
root@ufm-ai03:~#
root@ufm-ai03:~#
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

To manually check the status, run `systemctl status ufm-os-firstboot.service`. If it is already finished, an error message is prompted stating that there is no such service. In that case, the log `/var/log/ufm-os-firstboot.log` can be checked instead.

```
systemctl status ufm-os-firstboot.service
```

Example:

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot
Unit ufm-os-firstboot.service could not be found.
root@ufm-ai03:~#
```

13.5.1.3 High-Availability Mode Upgrade

Upgrade on HA should be done first on the stand-by node and after that on the master node, each node upgrade is similar to the SA instructions.

In case the Standby node is unavailable, the upgrade can be run on the Master node only, however, some additional steps will be required after the appliance is upgraded.

In case a secure boot certificate needs to be updated/installed, the script will stop execution and request the user to install the secure-boot certificate, secure-boot does not have to be active (although it is highly recommended), but the certificate must be installed/updated by the user before proceeding to the upgrade.

The upgrade script will verify that the certificate is up to date and will stop execution if it needs to be installed/updated (this happens at the start of the script)

1. [On the stand-by Node]: Copy and extract the OMU tar file to a temporary directory.
2. [On the stand-by Node]: Run the upgrade script.

System reboot is mandatory once the upgrade procedure is completed. The `-r` flag can be used to automatically reboot the server.

The `-y` flag CAN NOT !!! be supplied to upgrade the UFM Enterprise Appliance SW.

The `-y` flag can be supplied to skip user questions (the flag does not automatically reboot the server on its own. For auto reboot, combine with the `-r` flag).

In the following example the server auto reboots once the upgrade procedure is completed:

```
cd /tmp/ufm-appliance-<version>-<revision>-omu
./ufm-os-upgrade.sh -y -r
```

3. If `-r` flag was not provided reboot the server when the script will finish (a question will show on the screen that will ask to reboot if No was answered a manual reboot is required) to manually reboot the server:

```
reboot now
```

4. After the reboot procedure is complete, a systemd service (`ufm-os-firstboot.service`) runs the remainder of the upgrade procedure. Once completed, a message is prompted to all open terminals including the status:

"UFM-OS-FIRSTBOOT-FAILURE" - if installation is failed.

"UFM-OS-FIRSTBOOT-SUCCESS" - if installation succeeded.

Example:

```
root@ufm-ai03:~#
root@ufm-ai03:~#
Broadcast message from root@ufm-ai03 (somewhere) (Fri Dec 30 18:47:32 2022):
UFM-OS-FIRSTBOOT-SUCCESS, installation succeeded additional info is available in /var/log/ufm-os-firstboot.log
```

To manually check the status, run `systemctl status ufm-os-firstboot.service`. If it is already finished, an error message is prompted stating that there is no such service. In that case, the log `/var/log/ufm-os-firstboot.log` can be checked instead.

```
systemctl status ufm-os-firstboot.service
```

Example:

```
root@ufm-ai03:~# systemctl status ufm-os-firstboot
Unit ufm-os-firstboot.service could not be found.
root@ufm-ai03:~#
```

5. After the stand-by node have finished the upgrade check the HA cluster status

```
ufm_ha_cluster status

root@swx-ufm3-11:~# ufm_ha_cluster status
Cluster name: ufmcluster
WARNING: corosync and pacemaker node names do not match (IPs used in setup?)
Stack: corosync
Current DC: swx-ufm3-11 (version 1.1.18-2b07d5c5a9) - partition with quorum
Last updated: Thu Mar 16 18:45:19 2023
Last change: Mon Feb 27 12:40:22 2023 by root via crm_resource on swx-ufm3-11

2 nodes configured
5 resources configured

Online: [ swx-ufm3-09 swx-ufm3-11 ]

Full list of resources:

Master/Slave Set: ha_data_drbd_master [ha_data_drbd]
Masters: [ swx-ufm3-09 ]
Slaves: [ swx-ufm3-11 ]
Resource Group: ufmcluster-grp
  ha_data_file_system (ocf::heartbeat:Filesystem): Started swx-ufm3-09
  ufm-ha-watcher (systemd:ufm-ha-watcher): Started swx-ufm3-09
  ufm-enterprise (systemd:ufm-enterprise): Started swx-ufm3-09

Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
DRBD_RESOURCE: ha_data
DRBD_CONNECTIVITY: Connected
DISK_STATE: UpToDate
DRBD_ROLE: Secondary
PEER_DISK_STATE: UpToDate
PEER_DRBD_ROLE: Primary
```

All the nodes in the cluster should be online and the current node should remain a stand-by (Secondary in DRBD_ROLE)

6. [On the Master Node]: Fail-over the UFM to the stand-by node (upgraded node will become master and current node will become stand-by).

```
ufm_ha_cluster failover
```

wait for all the resource of UFM are up and running on the upgraded node.

7. repeat the procedure on the un-upgraded node (which is now acting as stand-by).

13.5.2 Upgrading All UFM-Related Software Components

The installation process consists of replacing the containers/packages with the new version and upgrading the UFM data.

1. Copy the tarball file of UFM Enterprise Appliance software to the /tmp folder.
2. Connect to the UFM Enterprise Appliance via SSH.
3. Stop the UFM service/cluster before upgrading.

In SA mode, run:

```
#systemctl stop ufm-enterprise.service
```

In HA mode, run:

```
# ufm_ha_cluster stop
```

4. Extract the tarball file and run the installer for the upgrade. Run:

```
# cd /tmp
# tar xvf ufm-appliance-sw-<version>.tar
# cd ufm-appliance-sw-<version>
# ./install.sh
```

Installer Options:

```
-q|--quiet          Upgrade UFM without prompt
```

In HA mode, this step should be performed on both servers.

5. After the upgrade, start the UFM service/cluster.
In SA mode, run:

```
# systemctl start ufm-enterprise.service
```

In HA mode, run:

```
# ufm_ha_cluster start
```

6. Wait one minute for the service to come up.
7. Ensure the service health. Run:

```
# ufm_enterprise_sanity.sh
Checking Service...
Done
Checking Images...
Done
Checking Containers...
Done
Checking ufm REST server...
Done
Sanity tests completed successfully!
```

13.5.3 Upgrading Specific UFM-Related Software Component

13.5.3.1 Upgrading UFM Docker in SA Mode

Stop the UFM service before upgrading. Run:

```
systemctl stop ufm-enterprise.service
```

For detailed information on upgrading the UFM docker in standalone mode, please refer to [Upgrading UFM on Docker Container](#).

13.5.3.2 Upgrading UFM Docker in HA Mode

Stop the UFM cluster before upgrading. Run:

```
ufm_ha_cluster stop
```


For detailed information on upgrading the UFM docker in high availability mode, please refer to [Upgrading UFM on Docker Container](#).

13.5.3.3 Upgrading UFM HA Package

1. Stop the UFM cluster before upgrading. Run:

```
ufm_ha_cluster stop
```

2. Download the UFM-HA package on both servers using the following command:

```
https://www.mellanox.com/downloads/UFM/ufm_ha_5.3.0-17.tgz
```

3. On both servers, extract the downloaded UFM-HA package under /tmp/
4. On both servers, go to the extracted directory /tmp/ufm_ha_XXX and run the installation script:

```
./install.sh --upgrade
```

5. After the upgrade, start the UFM HA Cluster. Run:

```
ufm_ha_cluster start
```

13.5.3.4 Upgrading UFM Enterprise Appliance CLI Package

1. Copy the tarball of the UFM CLI package to the /tmp folder.
2. Extract the tarball file and run the installer. Example:

```
# cd /tmp
# tar xvf ufmcli_<version>.tgz
# cd ufmcli_<version>
# ./install.sh
Creating the UFM3 CLI repository file /etc/apt/sources.list.d/ufmcli.list
Refreshing the UFM3 CLI packages information...
Installing the UFM3 CLI package...
Removing the UFM3 CLI local repository /etc/apt/sources.list.d/ufmcli.list
Done.
```

3. Once the upgrade procedure is completed, connect to the UFM Enterprise Appliance via SSH with admin. Run:

```
ssh admin@<hostname>
```

14 Document Revision History

| Revision | Date | Description |
|----------|-------------------|---|
| 1.6.2 | January 4, 2024 | Updated the following section: <ul style="list-style-type: none">• Changes and New Features• Known Issues in This Release |
| 1.6.1 | December 12, 2023 | Updated the following sections: <ul style="list-style-type: none">• Installation Notes• Bug Fixes in This Release• Known Issues in This Release |
| 1.6.0 | December 12, 2023 | Updated Known Issues in This Release |
| | November 21, 2023 | Added instructions on Configuring TACACS+ and Performing AAA and Adding TACACS Users on the Server Side |

| Revision | Date | Description |
|----------|------------------|---|
| | November 5, 2023 | <p>Updated the following sections:</p> <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release • UFM Enterprise Appliance Upgrade - Added an important note • Configuring the Appliance for the First Time - Added a diagram to reflect the connectivity of the UFM High-Availability cluster and instructions on how to configure the back-to-back Interface • High Availability - Added the HA configuration instructions <p>Added Appendix - Software Components Upgrade</p> <p>Updated the following CLI Commands:</p> <ul style="list-style-type: none"> • show interfaces - Updated the output and added optional argument interface name • show ib sharp - Updated the output to reflect the new settings <p>Added the following CLI commands:</p> <ul style="list-style-type: none"> • In Routing: <ul style="list-style-type: none"> • show {ip ipv6} route • show {ip ipv6} default-gateway • In AAA Methods: <ul style="list-style-type: none"> • aaa authentication login default • show aaa • In TACACAS+: <ul style="list-style-type: none"> • tacacs-server • tacacs-server host • show tacacs • In Chassis Management: <ul style="list-style-type: none"> • show files system • show resources • In UFM License: <ul style="list-style-type: none"> • ufm license install • ufm license delete • show ufm license • show files ufm-license • In UFM Configuration Management: <ul style="list-style-type: none"> • ufm configuration delete • ufm configuration export • ufm configuration fetch • ufm configuration import • ufm configuration upload • show files ufm-configuration • High-Availability <ul style="list-style-type: none"> • ufm ha configure • In UFM Multi-Port SM: <ul style="list-style-type: none"> • ufm multi-port-sm • show ufm multi-port-sm • ufm additional-fabric-interfaces • show ufm additional-fabric-interfaces • HCA Commands <ul style="list-style-type: none"> • ib hca-vl15-window • show ib hca-vl15-window • In NVIDIA SHARP: <ul style="list-style-type: none"> • ib sharp dump-files-generation enable |

| Revision | Date | Description |
|----------|-----------------|---|
| | | <ul style="list-style-type: none"> • ib sharp dynamic-tree-allocation enable • ib sharp dynamic-tree-algorithm • ib sharp ib-qpc-sl <0-15> • ib sharp ib-sat-qpc-sl <0-15> • ib sharp allocation enable |
| 1.5.1 | August 31, 2023 | Updated the following sections: <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release • license install - Added note #1 |
| 1.5.0 | August 10, 2023 | Updated the following sections: <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release • Troubleshooting - Added step 1 and rearranged the remainder of the steps. Added the following sections: <ul style="list-style-type: none"> • UFM Enterprise Appliance In-Service Upgrade • Appendix - UFM Factory Reset Added the following CLI commands: <ul style="list-style-type: none"> • image fetch • image install • image delete • show images • ufm data reset • {ip ipv6} host • ufm ha-nodes • show ufm ha-nodes |
| | August 24, 2023 | Added step 4 to UFM Enterprise Appliance In-Service Upgrade |
| 1.4.3 | June 20, 2023 | Updated the following sections: <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release |
| 1.4.2 | June 5, 2023 | Updated the following sections: <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release Updated the following CLI commands: <ul style="list-style-type: none"> • ip name-server • show version • ntp server • ntp peer • ip default-gateway Added the following command: <ul style="list-style-type: none"> • ipv6 default-gateway • username admin password • ib sm configuration import |

| Revision | Date | Description |
|----------|--------------|---|
| 1.4.1 | May 18, 2023 | <p>Updated the following sections:</p> <ul style="list-style-type: none"> • Changes and New Features • Bug Fixes in This Release • Known Issues in This Release <p>Added the following CLI Commands:</p> <ul style="list-style-type: none"> • High-Availability <ul style="list-style-type: none"> • ufm ha • General <ul style="list-style-type: none"> • ufm start • Network Interfaces <ul style="list-style-type: none"> • show interfaces • License <ul style="list-style-type: none"> • license install • license delete • show license • _shell • User Management <ul style="list-style-type: none"> • username |

| Revision | Date | Description |
|----------|-------------|--|
| 1.4.0 | May 5, 2023 | <p>Updated the following sections:</p> <ul style="list-style-type: none"> • Changes and New Features • Installation Notes • Bug Fixes in This Release • Known Issues in This Release • High Availability • UFM Enterprise Appliance Upgrade <p>Added the following sections:</p> <ul style="list-style-type: none"> • Appendix - Software Components Upgrade <p>Added the following CLI Commands:</p> <ul style="list-style-type: none"> • General <ul style="list-style-type: none"> • show ufm status • System Management <ul style="list-style-type: none"> • show hosts • show version • OpenSM: <ul style="list-style-type: none"> • show ib sm allow-both-pkeys • ib sm allow-both-pkeys • show ib sm keep-pkey-indexes • ib sm keep-pkey-indexes • show ib sm virtualization • ib sm virtualization enable • ib sm virtualization ignore • show ib sm root-guid • ib sm root-guid • show ib sm routing-engines • ib sm routing-engines • show ib sm ar-sl-mask • ib sm ar-sl-mask • show ib sm configuration import • ib sm partition-config-merge • Partition: <ul style="list-style-type: none"> • show ib partition • ib partition management defmember • SHARP Aggregation Manager <ul style="list-style-type: none"> • ib sharp enable • ib sharp smx-protocol • ib sharp topology-api enable • show ib sharp • SHARP Configuration in OpenSM <ul style="list-style-type: none"> • ib sm sharp enable • ib sm sharp ignore • show ib sm sharp • High-Availability <ul style="list-style-type: none"> • ufm ha configure dual-subnet • Management Interface Monitoring <ul style="list-style-type: none"> • show ufm mgmt-interface • ufm mgmt-interface monitor interval • ufm mgmt-interface • ufm mgmt-interface monitor enable • UFM Logs: <ul style="list-style-type: none"> • show ufm logging • ufm logging syslog enable • ufm logging syslog • ufm logging syslog enable • ufm logging syslog ufm-events enable • ufm logging level • UFM Web Client: <ul style="list-style-type: none"> • ufm web-client mode |

| Revision | Date | Description |
|----------|--------------|--|
| | | <ul style="list-style-type: none"> ufm web-client associate-user show ufm web-client ufm web-client client-authentication cert-refresh enable ufm web-client client-authentication cert-refresh ca-cert ufm web-client client-authentication cert-refresh server-cert ufm web-client client-authentication cert-refresh run-now <u>UFM Audit</u>: <ul style="list-style-type: none"> ufm track-conf-changes enable show ufm track-conf-changes |
| | May 15, 2023 | Added Upgrading UFM Enterprise Appliance CLI Package |
| 1.3.1 | Feb 19, 2023 | Updated <ul style="list-style-type: none"> Changes and New Features Bug Fixes in This Release Known Issues in This Release |
| | Mar 16, 2023 | Updated Changes and New Features - Added MFT package integration details |
| 1.3.0 | Feb 6, 2023 | Updated the following sections: <ul style="list-style-type: none"> Installation Notes Changes and New Features Bug Fixes in This Release Known Issues in This Release Added a note under Configuring the Fabric Interface Added the following sections: <ul style="list-style-type: none"> Command Line Interface (CLI) Appendix - Secure Boot Activation and Deactivation Appendix - Deploying UFM Appliance from an ISO File |
| | Feb 6, 2023 | <ul style="list-style-type: none"> Added Troubleshooting Updated Known Issues in This Release |
| 1.2.1 | Dec 1, 2022 | Updated the following sections: <ul style="list-style-type: none"> Changes and New Features Installation Notes |
| | Dec 19, 2022 | Updated <ul style="list-style-type: none"> Changes and New Features |
| 1.2.0 | Nov 21, 2022 | Updated the following sections: <ul style="list-style-type: none"> Release Notes UFM Enterprise Appliance Upgrade Added the following section: <ul style="list-style-type: none"> Appendix - Chassis Health Monitoring |
| 1.1.0 | Jul 31, 2022 | Updated the following sections: <ul style="list-style-type: none"> Release Notes Added the following section: <ul style="list-style-type: none"> Introduction Getting Started High Availability UFM Enterprise Appliance Upgrade |

| Revision | Date | Description |
|----------|--------------|--|
| | Oct 23, 2022 | Update the following sections: <ul style="list-style-type: none"><li data-bbox="874 286 1278 320">• UFM Enterprise Appliance Upgrade<li data-bbox="874 320 1043 353">• Starting UFM |

Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. Neither NVIDIA Corporation nor any of its direct or indirect subsidiaries and affiliates (collectively: "NVIDIA") make any representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice. Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer ("Terms of Sale"). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer's own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer's sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer's product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

Trademarks

NVIDIA, the NVIDIA logo, and Mellanox are trademarks and/or registered trademarks of NVIDIA Corporation and/or



Mellanox Technologies Ltd. in the U.S. and in other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

Copyright

© 2024 NVIDIA Corporation & affiliates. All Rights Reserved.

