Migrating from NIMS to OMS 17.5.1.0

User Guide

1 Dec 2018

Table of Contents

1

Chapter 1: Migrating NIMS to OMS

Before migrating to OMS

OMS was developed to meet the distinct needs of network professionals with Apex, Observer, OI, and Probe installations. OMS manages an extensive menu of essential tasks and delegates specific IT jobs on a tiered authorization basis to appropriately credentialed network team members. TLS-based communication security safeguards sensitive user data while in transit.

What can you do more efficiently with OMS?

- Authenticate IT staff for the entire Observer Platform from one central location
- Integrate with third-party authentication servers including AD, RADIUS, TACACS+, and more
- Authorize user access according to clearance credentials or asset group
- Audit user access and activity related to company-sensitive data
- Manage user passwords and permissions
- Define access rights by user, user group, or asset group
- Automatically license new Observer Platform components connecting to the network
- Easily and efficiently administer software upgrades across the Observer Platform

Purpose of this migration guide

The purpose of this user guide is to help you migrate from NIMS to OMS. This guide is for making the transition only.

Full documentation for features and general use of OMS is located at Observer Management Server Documentation.

Name changes from NIMS to OMS

Some of the vocabulary used for the terms and features of NIMS have changed in OMS. We recommend reviewing these changes during the first launch of OMS.

Old name	New name
Network Instruments Management Server (NIMS)	Observer Management Server (OMS)
Entity	Asset
Entity Group	Asset Group
User Group Permissions	Authorization Policy
Auto-Upgrade	Upgrade Policy
Primary-Secondary Server Configuration	Failover

What is needed for migration

To successfully migrate from NIMS to OMS, you must have or know some items before beginning the migration. Do not uninstall NIMS. Your configuration settings will migrate from NIMS to OMS.

Table 1. What to collect before migrating from NIMS to OMS

What to have or know	Purpose for having or knowing
Version 17 license information for OMS	During the first launch of OMS, you will need to provide your version 17 identification and license numbers.
Version 17 installation file for OMS	This file is necessary for installing OMS.
The user name and password to OMS is: **admin** / **admin**	The first login to OMS requires this user name and password. No other login credentials are accepted. This user name and password must be used for configuring user access.
Only if you use Active Directory authentication in NIMS, you will need the information from the section: For Active Directory users only (page 9)	Active Directory authentication will *not* operate as intended after migration. It must be reconfigured with new settings after your migration. The process is straightforward and documented in this migration guide.
User group permissions have been consolidated for ease-of-use, so you will need the information	Because the user group permissions have changed (they are now called authorization policies), you should familiarize yourself with what permissions are available in OMS.

What to have or know from the section: Authorization list (page 7)	**Purpose for having or knowing**
Backup of existing NIMS files and configuration	It is recommended to back up your NIMS installation. In NIMS, choose **File** > **Export Configuration**. Also, copy `C:\Program Files\Network Instruments Management Server` to secure, removable media.

What migrates from NIMS to OMS

Nearly every NIMS setting will successfully migrate to OMS. The details of these migrated settings are provided.

Authentication	Authentication settings for RADIUS, TACACS+, Active Directory, and the local NIMS list, are migrated. Active Directory settings currently experience a glitch after migration, and it must be fixed manually. The settings migrated for all authentication settings include, but are not limited to, IP addresses and ports, authentication choices, shared secrets, and bindings. RADIUS only migrates one primary and one secondary server —not the optional primary and secondary accounting servers. Cache timers for authentication will not be migrated for any authentication scheme.
Auto-upgrade	Auto-upgrade settings used in NIMS are migrated. The settings include transfer and installation schedules, maximum concurrent transfers, speed limit for transfers, and if auto-upgrade is enabled or disabled. These settings will migrate to the Global Upgrade Policy in OMS.
Auto-upgrade (per entity)	Any unique auto-upgrade settings on entities and entity groups are migrated. The settings include transfer and installation schedules, maximum concurrent transfers, speed limit for transfers, and if auto-upgrade is enabled or disabled per entity. Any unique auto-upgrade settings for an entity or entity groups will be given an automatically generated upgrade policy named *ConversionGeneratedPolicy* with a number appended to the name. The generated name can be manually renamed.
Email Notification Settings	Configuration details for forwarding log events and alarms as emails will be migrated. This includes the mail server and port, any authentication credentials, encryption choice, and email display name. If you actively use email for sending log events and alarm notification in NIMS, this will continue in OMS uninterrupted.
Entities	The following entities migrate: Observer, Probe, GigaStor, OI, Observer Reporting Server. The data migrated is primarily, but not limited to, each entity's IP address, probe name (if known), and probe ID (if known). If the probe name and ID are not currently known in NIMS, they will later be resolved by OMS when connected.
Entity Groups	If you used entity groups in NIMS, an optional feature, these migrate to OMS. The relationships between your entities and their entity groups will remain. Entity group names will remain the same after migration.
Failover / Redundancy	The primary-secondary configuration of NIMS will migrate. This includes the choice to use failover functionality (for example, enabled versus disabled), the IP address of the other NIMS server, and the designation if a NIMS system is the primary or not.
Licenses	Licenses for versions 15 and 16 products will be migrated. This includes the relationship between the license and the entity

	it currently belongs to. Any unassigned licenses in NIMS will remain available in OMS.
Permissions	Access permissions given to user groups in NIMS are migrated to OMS. These settings include the type of interactions user groups can make on entities. Any unique permission settings for user groups will be given an automatically generated authorization policy named *ConversionGeneratedPolicy* with a number appended to the name. The generated name can be manually renamed.
Shared Filters	Any shared filters that NIMS was aware of will migrate to OMS. This includes the logic of each filter, the name of each filter, and the "available" or "deleted" status of each filter.
Syslog Event Export	Configuration details for exporting log events to a Syslog server will be migrated. This includes the RFC format of the Syslog messages, the target IP address of one Syslog server, and your selection if log events are forwarded to the Syslog server (for example: enabled versus disabled). The facility number is not migrated. If you actively use the Syslog event export feature in NIMS, this will continue in OMS uninterrupted.
Users	All users set in NIMS are migrated to OMS. This includes each user's authentication management type (local or remote authentication), email address if one exists, the user names, and finally the password if it is a locally managed user. Password fields remain masked in OMS.
User Groups	All user groups are migrated from NIMS to OMS. This includes any relationship between users and user groups, access permissions of user groups to entities and entity groups, and permissions the user group has for interacting with entities.

Authorization list

The user group permissions in NIMS have been consolidated and simplified in OMS.

Observer

- Administer—Grants users the ability to administer probes and probe instances.
- Log User Activity—Grants users the ability to view log file activity.
- Protocol Definitions—Grants users the ability to view protocol definitions.
- Redirect—Grants users the ability to change where a probe instance is connected.
- Shared Filters—Grants users the ability to modify filters marked as shared in Observer.
- Artifact Reconstruction
  - Reconstruct Stream—Controls whether HTML and other non-VoIP streams can be reconstructed.
  - Voice and Video Playback—Control whether VoIP content can be reconstructed.

Observer Apex

- No Access: Use of Apex is denied.

- User: User may create and use:
  - Application Dependency Mapping
  - Dashboards
  - Execute dashboards
  - Widgets
- System: Cannot use anything in User, but may
  - Change options under **System**
  - Use the log
  - Connect to a GigaStor
  - Use a drill down
  - Set and manage alarms
- Admin/Full: User *and* System access.

Observer Infrastructure

- Access Level—
  - No Access: Use of OI is denied.
  - User: User may connect to device groups.
  - System: User access, plus Connect to device groups and view status and properties.

    Edit device groups.

    Start/stop polling.
  - Admin/Full: System access, plus Create and delete device groups and routes.

    Activate device groups.

    Edit maps.
- Web Reports—Grants users ability to view reports in a web browser.

Observer Management Server

- Access Level—
  - No Access: Use of OMS is denied.
  - System: Allows the user the ability to change options under **System**.
  - Admin/Full: System access, plus ability to control (add, modify, delete):

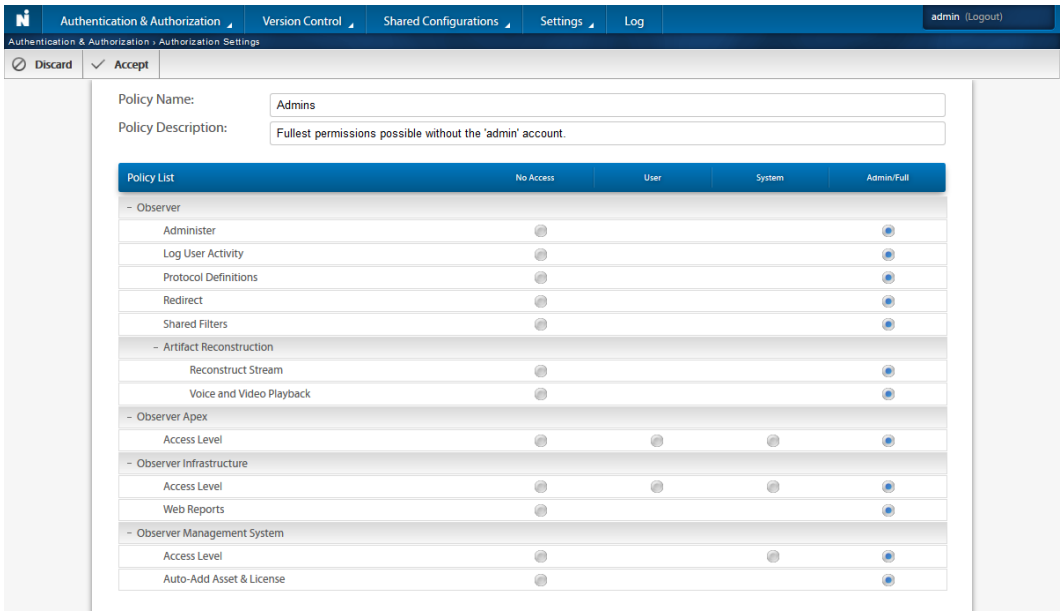
Assets	Asset groups
Authentication	Auto-adding assets and licenses
Licenses	Permissions
Security	Shared filters
Shared protocols	Updates
Upgrades	Users

User groups

- Auto-Add Asset & License—Grants users the ability to auto-add new assets to OMS plus license them if **System** > **Settings** is set to allow those.

More details about user group permissions—known as authorization policies in OMS—can be found at Understanding permission policies in the OMS User Guide.

Figure 1: This settings page is located at: **Auth** > **Authorization** under **New** or **Edit**.



For Active Directory users only

Active Directory settings in NIMS cannot be automatically migrated in a way that is valid to v17 OMS. This is because OMS uses a different Active Directory implementation with different API calls than NIMS. This new implementation is through the WinLDAP API.

Unlike NIMS, you no longer need a local user account that matches the domain user account. It was a requirement in NIMS to have a local, dedicated system account for Active Directory. This user account is no longer needed; it is not used by OMS. Instead, OMS uses binding options (like Bind DN) to communicate with Active Directory. You can view the options you will need for configuring Active Directory at OMS by visiting Active Directory settings (page 9).

Active Directory settings

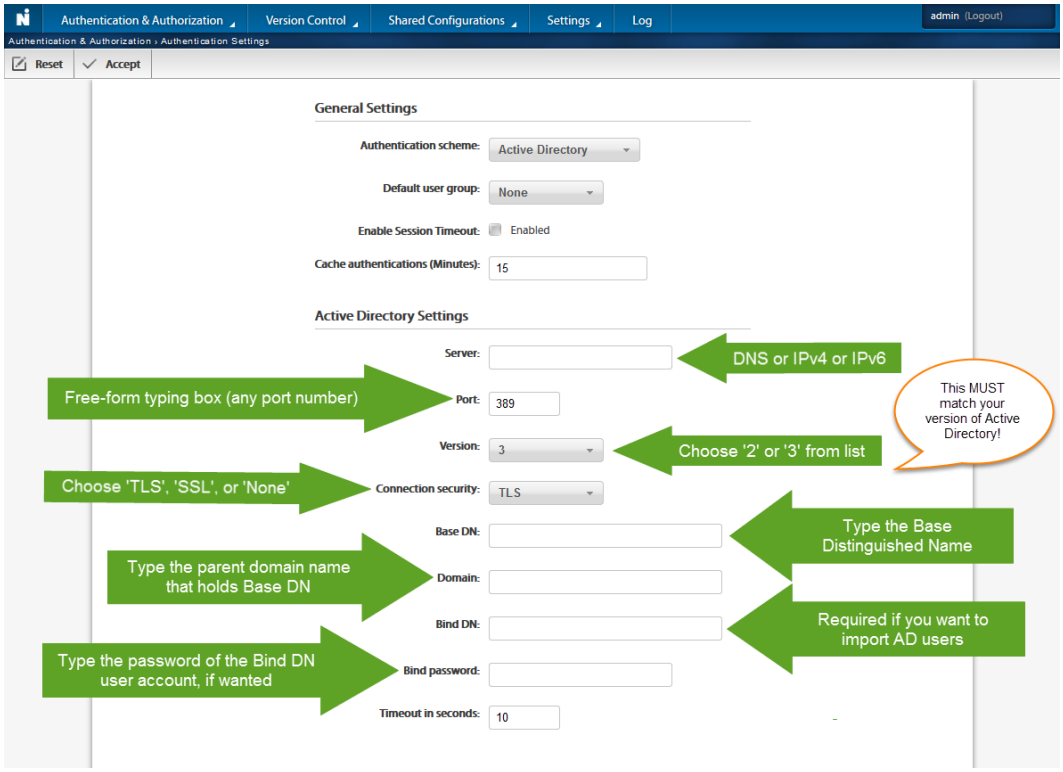
Use the information to assist you when configuring the **Authentication** to use Active Directory.

Authentication scheme	The system or service for managing user names, passwords, groups, and authentication, can be specified. **Local** Exclusively managed within this system. **LDAP** Any LDAP directory service (do not select for configuring Windows Active Directory)

	Active Directory Windows Active Directory service **RADIUS** RADIUS authentication server **TACACS+** TACACS+ authentication server
Default User Group	Any end user who is not assigned to a user group is automatically placed into the group chosen from this list and given the permissions it grants. The default is **None**. If set to **None**, any user attempting to log in must already exist in the Users table before any authentication attempt to the third-party authentication server is made. If the attempting user does not exist in the Users table, they are always denied and no authentication attempt is made.
Enable Session Timeout	If selected, user sessions terminate after N-minutes of inactivity. This minimizes the chances of an unattended user session being hijacked.
Session Timeout (Minutes)	Sets the duration of user inactivity before a session terminates. Valid Input: The default is 0, which means that the session never times out.
Cache authentications (Minutes)	Sets how long, in minutes, successful authentications are cached. This reduces the frequency of authentication requests made to the third-party authentication server.
Server	The host address of the Active Directory server. Valid Input: Valid addresses include IPv4, IPv6, or DNS name.
Port	The port number of the Active Directory server. The default is 389.
Version	The protocol version of LDAP the Active Directory host uses.
Connection security	The security type for authenticating and encrypting connections.
Base DN	The Base Distinguished Name is the point in the directory tree from which users are verified. This might be the root or some place lower in the tree to limit the number of users returned. Required. Example: dc=networkinstruments,dc=com Administrators should find the Base DN directly from the Active Directory server to ensure accuracy.
Domain	The parent domain name. A fully-qualified domain name (FQDN) does not need to be specified.
Bind DN	The Bind Distinguished Name is required for importing user accounts from the Active Directory server. The Bind DN user account needs domain user privileges, and administrators should find a suitable Bind DN directly from the Active Directory server to ensure accuracy.
Bind password	The password of the Bind DN.
Timeout in seconds	The duration (in seconds) a connection attempt waits before aborting. The default is 10. A connection retry attempt is made if this value elapses.

To use Active Directory, you must configure this Active Directory settings page after OMS is installed.

Figure 2: This settings page is located at: **Auth** > **Authentication**.



Installing and licensing

Follow the specific details for installing the software and getting your product licensed.

How to stop the NIMS Windows service

Stop the Windows service for NIMS that is running on the *primary* NIMS system. If you use a secondary NIMS (failover or redundant), the secondary NIMS system can continue operating at this time.

Do not uninstall NIMS. Many of your settings and configuration details will be migrated to OMS by keeping NIMS installed. This part of the migration only requires you turn off the NIMS Windows service to avoid any issue. This is a precautionary step.

To stop the NIMS service running in Windows:

1. In Windows, choose **Start** > **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
2. Select **Network Instruments Management Server Service** and choose to **Stop** the service.

The NIMS Windows service of the primary NIMS system has stopped. You are ready to install OMS.

How to install OMS over NIMS

OMS can be installed directly on top of NIMS. This is the recommended method of migrating because most NIMS settings will migrate to OMS during installation.

Prerequisite(s):

See Supported Operating Systems (page 12) for a list of supported operating systems.

1. Download the latest installation file from our update site. If you copied the installation files from our website, start the installation program.

   http://update.viavisolutions.com/latest/OmsSetupx64.exe

2. When the setup program runs, follow the onscreen instructions.

The installation of OMS is finished. Most of your previous settings have been migrated from NIMS. If you use a secondary NIMS system, the secondary NIMS system should also now be providing all NIMS duties.

You are ready to launch OMS for the first time and license the product. If you use a secondary NIMS system, allow it to remain operational while you license the OMS system that was your primary NIMS server.

Supported Operating Systems

Your product must be installed on one of these operating systems to receive assistance from Technical Support.

Product name	64-bit Windows[1]	32-bit Windows
OMS	Windows 7 (SP1 or higher) or newer Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher) or newer	Not supported

1. If your operating has secure boot, it must be disabled. Most versions of Windows from Windows 10 and later have secure boot.

How to license OMS

To license and activate OMS:

1. Launch OMS.
2. Your default web browser will open to the following URL: `https://localhost/OMS`

   Example: If it does not, type the URL in the location bar of your web browser and press **Enter**.
3. Follow the on-screen instructions provided by your web browser to accept the self-signed security certificate.

   Your web browser must accept the self-signed security certificate to continue.
4. Type into the boxes exactly what is listed in your license document.
5. Click the **License** button.

You successfully licensed and activated your product.

If licensing and activating your product remains unsuccessful, please contact Technical Support.

Configuring OMS during first launch

Turn on or off various features (listed below) in the **Global Asset Policy** to configure the foundation of OMS. After you have done that, add or import product licenses so that when assets come online they can request an available license.

Understanding the Global Asset Policy

The Global Asset Policy controls all core functionality of OMS. How you use OMS in your organization is entirely dependent on these settings.

The Global Asset Policy can be modified at **System** > **Settings**.

Authenticate & authorize users using OMS	If selected, all assets managed by OMS will prompt users with a secure login when applications, like Observer, are launched. The login prompt expects a user name and password that has been configured in OMS. Because OMS can authenticate users with third-party authentication services like Active Directory, an example would be to use your Active Directory credentials here (if OMS is configured to do so and your user name has been imported).
Synchronize user protocol definitions through OMS	Synchronizing user protocol definitions is an important step in ensuring that all assets understand the traffic on your network. This is especially important when analysing captures and trending data from other areas of the organization or custom applications. It is highly recommended that protocol definitions remain shared.
Get list of Probe Instances available for redirection from OMS	If selected, all probe instances that a user has permission to redirect, or even see, will appear to them when redirection is attempted. Clearing this setting ensures that no remote probe instances are shown. Probe instances local to the asset being interacted with are shown only.
Share filters with OMS	To share capture filters between assets, this setting must be enabled. The filters that users create and save become synchronized between all assets, so the work of creating filters does not need to be duplicated by multiple people.
Manage licenses with OMS	OMS can manage all of the licenses for your assets. This includes storage of the licenses; the ability to assign them to assets remotely; and the ability to remove them from assets remotely. If your organization does not use this feature, each asset must be manually licensed in that product, such as inside Observer.
Auto-add assets and licenses	For ease of administration, OMS can automatically create and apply the appropriate license to an asset the first time it connects. This option is especially useful when a large number of new assets need to be added to OMS; just ensure the new asset is set to be managed by OMS.
Cache OMS logon credentials	If selected, managed assets will cache OMS user credentials for a set number of hours. During the configurable number of hours, users can continue to log on and use managed assets if OMS

	has become unavailable. For the greatest prevention of OMS downtime, consider using a failover configuration.
Assign auto-add assets to Asset Group	If **Auto-add assets and licenses** is selected and a new asset is automatically added, the asset is placed into this asset group.
Number of hours to cache OMS logon credentials	This sets how many hours that OMS user credentials are cached by managed assets. This option only appears when **Cache OMS logon credentials** is selected.

How to import asset licenses

Existing licenses will have successfully migrated from NIMS to OMS (versions 15, 16, and 17 licenses). You can import licenses into OMS at this time if you own additional licenses that were never added to NIMS, like new version 17 licenses for Observer or GigaStor.

Prerequisite(s):

You must have the license file provided to you from VIAVI. It can be located on your local hard drive or a network share.

A OMS license file (.lic) is a tab delimited text file that contains all of the your asset license numbers.

Follow these steps to import licenses:

1. Starting in the dashboard, click **Version** > **Licenses**.
2. Click the import icon .
3. Click **Browse**.
4. Locate the license file provided to you.
5. Click the import icon .

The licenses are uploaded and now available. Available licenses can be assigned to existing assets or users who attempt to automatically add an asset can request one of the available licenses.

How to add an asset license

For environments with only a handful of assets, manually adding asset licenses is the recommended procedure—as opposed to importing them in bulk.

Prerequisite(s):

You must have the license information provided to you from VIAVI.

> **Tip!** If you have many licenses to enter, you may want to import the licenses. See How to import asset licenses (page 14) for details.

Follow these steps to add an asset license:

1. Starting in the dashboard, click **Version** > **Licenses**.
2. Click the new icon .
3. Complete all of the fields. Pay particular attention to the license number.
4. Click **Accept**.

The license is added and now available. Available licenses can be assigned to existing assets, or users attempting to automatically add an asset can request one of the available licenses.

Upgrading assets to v17

All of your auto-upgrade settings will have migrated from NIMS to OMS. Assets in OMS all follow the same upgrade behavior as before migration, but these are now conveyed in upgrade policies.

OMS contains a mechanism, named an upgrade policy, for automatically pushing upgrades to assets. Upgrade policies remove the need to distribute new versions of the asset software using outside channels like FTP and network shares. Plus, an upgrade policy provides unattended installation, so coordinating personnel to be present at the time and place of installation is now a choice—it is no longer a requirement.

How to modify the global upgrade policy

To affect the upgrade policy of all assets that are not specifically given an upgrade policy, you can modify the global upgrade policy.

By default, all assets use the **Global Upgrade Policy** as an upgrade policy unless explicitly changed.

To modify the global upgrade policy:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. In the rightmost pane, click **Global Upgrade Policy** to select it.
3. Click the edit icon .
4. Modify the global upgrade policy.
5. Click **Accept**.

Now, any asset or asset group not given an upgrade policy will follow the settings in the global upgrade policy.

How to download upgrades for upgrade policies to use

Upgrade policies, that are configured to transfer or install new software versions, rely on files downloaded from VIAVI by OMS. Configure your download settings to ensure new versions are brought into OMS and can be pushed to assets using an upgrade policy.

Some settings must remain configured for OMS to automatically download software upgrades for upgrade policies make use of. Otherwise, upgrade policies that are configured to transfer or install new software versions must wait for an OMS administrator to manually check for and download these files from the VIAVI upgrade repository.

> **Note:** Firmware updates to the capture card are bundled with Observer software upgrades. During installation of an Observer software upgrade, any firmware updates available to your capture card will be applied.

To ensure software upgrades are automatically being downloaded for your upgrade policies to make use of, follow these steps:

1. Starting in the dashboard, click **Version** > **Upgrade Versions**.
2. Select one by clicking a table row.
3. Click the preferences icon .
4. Ensure **Check for upgrades** is selected in the **General Preferences** area, as it is enabled by default.

   If selected, OMS periodically checks for upgrades. Scheduled transfers and installs rely on knowing if new versions exist.
5. In the **Download Preferences** area, configure a **Download upgrades** schedule to be **Daily** or **Day of Week** and set one or more time frames for downloads to occur.

   Example: For example, click **Daily**. Next, ensure the **Daily Schedule** check box is selected. Then, click the plus symbol (+) to create a new time frame. Finally, click the newly created time frame to adjust the hours when downloads can occur, and click **OK**.
6. Click the accept icon .

You successfully configured OMS to automatically check for upgrades and download them according to a schedule. The downloaded upgrades are used by upgrade policies configured to transfer or install software upgrades.

Index