OMS Essentials 17.5.1.0

Getting Started Guide

1 Dec 2018

Table of Contents

1

Chapter 1: Understanding OMS architecture

An architectural image shows the components of the Observer Analyzer Platform.

OMS controls access to all parts of the Observer Platform ecosystem using its own internal list or from Active Directory, RADIUS, TACACS+, or LDAP.

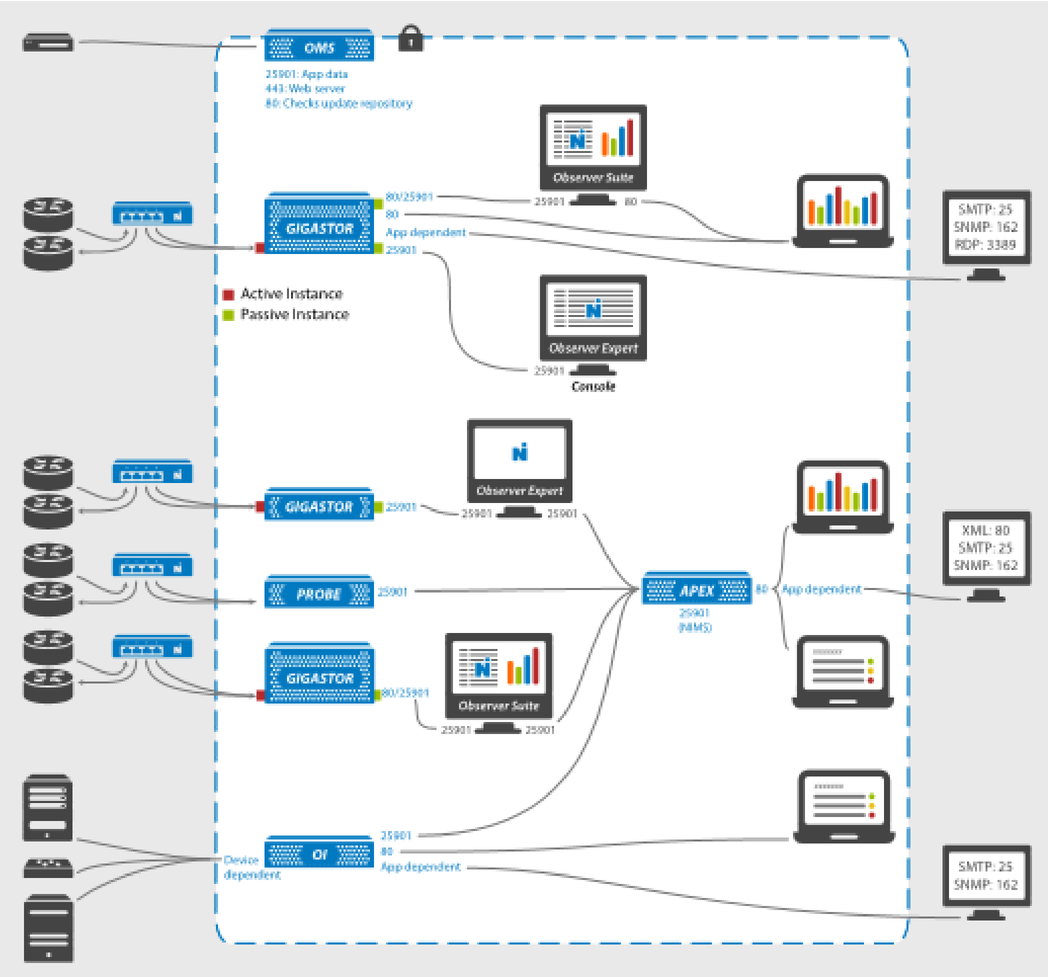
Packets between your network devices pass through an Observer nTAP to the active probe instance on the Observer GigaStor. Observer Suite connects to a passive instance for trending and expert data. Expert data is viewable in Observer, and trending data is available from dashboards in a web browser.

Observer Expert Console connects to a passive probe instance on a GigaStor for expert data.

Observer Apex produces reports by consolidating trending data from numerous sources, including Observer Suite, Observer Expert (both of which may have multiple trending sources), Expert Probes, GigaStors, and Observer Infrastructure (OI).

If you are viewing an Apex dashboard whose data comes from a GigaStor, you can drill down from the dashboard into the packets on the GigaStor. This is accomplished by drilling down from a Business Group with a Data Source that is the Active Instance (running trending). To data-mine the packets using Observer, use a passive instance on the same GigaStor.

Figure 1: Observer Platform architecture



2

Chapter 2: Understanding user accounts

A user account provides an individual a user name and password to connect to assets managed by OMS.

All users who want to access an asset managed by OMS must have a user account in OMS that is either verified locally with an internally-stored password or through a third-party authentication server. To use an asset or asset element:

- A user account must be verified. As an OMS administrator, you can choose to use a combination of locally and remotely authenticated user accounts in your environment.
- A user account must be a member of a user group to connect to any assets.
- A user group's permission policy determines the level of access to each asset, including no access.
- The asset or asset element must be in a user group to which the user account is also a member.
- A user account may be a member of zero, one, or more user groups.

Permissions for verified and constantly reverified whenever a user attempts an action (such as logging in, redirecting a probe, starting a packet capture, viewing a report, and so on). If the account has been disabled or deleted, the user is denied access.

There are three types of users:

- **Local user**: User name and password are entered into and authenticated by OMS. Local users are easier to configure and manage for small teams who are not using third-party authentication servers or for groups in a lab or testing environment who want to remain separate from the wider enterprise for their testing.
- **Remote user**: User name and password are from and authenticated by a third-party authentication server. If you are adding more than a handful

of users, we recommend these accounts be imported into OMS rather than manually added. If your organization has a large number of users to manage, you may want to choose to authenticate users remotely since it reduces your burden as an OMS administrator. It is also one less password each user must remember and maintain.

- **admin**: A special type of local user. It cannot be deleted or disabled nor does it need to be a member of any user groups. It has full access at all times. The default password is `admin`—this password is case-sensitive—and should be changed for your environment.

3

Chapter 3: Understanding user groups

OMS controls access to the assets it manages through user groups. Different groups have access to different assets or have different levels of access to the same asset. This access is controlled through the permission policy associated with the user group. Assigning permissions to a group rather than to each unique user makes maintenance for the OMS administrator much easier.

User groups are collections of users, asset groups, and single assets. By assigning a permission policy to the group, you control what access members of the groups have.

OMS does not have a default user group. You must create at least one user group, associate a permission policy with it, and add users to the group before any user can access any assets managed by OMS.

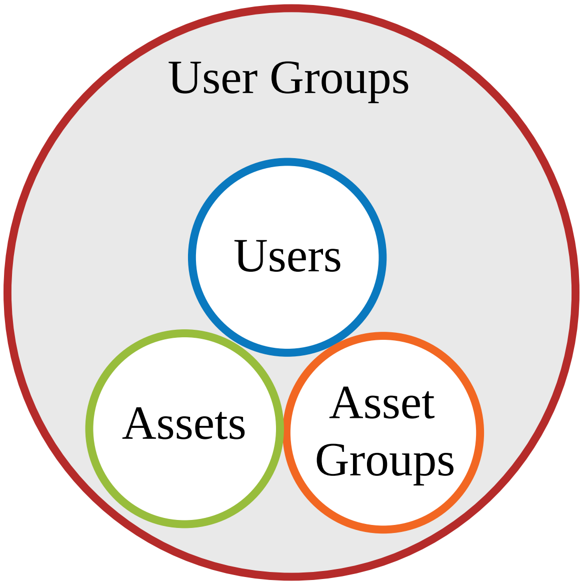
User group permissions are additive. When a user is a member of multiple groups, the user is granted the least restrictive permissions. If a user is a member of multiple user groups and at least one of the user groups allows access to the feature, then that group's permissions are in effect for that feature. That means if one group has access to a feature and another group does not, any user who is a member of both groups is indeed granted access.

Some examples of groups you might create may be based on:

- **Location**—Suppose you want Pat to have full access to the local probes in Chicago, but not allow him to capture packets on probes located in the central office in New York. Create two Authentication permission policies ("Chicago Probes" and "New York Probes") and two user groups ("Admins" and "Operators") with the appropriate permissions policy set. Add Pat to both user groups. By adding Admins (who have full permissions) to the access list for Chicago Probes, Pat is granted full access permission to any probe in the Chicago asset group. By adding Operators to the access list for New York Probes, Pat will have more restricted access to the New York Probes.

- **Employment status: internal vs. contractor**—Suppose Pat is a contractor and you want contractors to have the ability to use the network trending, but not to administer the probe or set properties. Create two Authentication permission policies ("Employee Permissions" and "Contractor Permissions") and two user groups ("Employees" and "Contractors") with the appropriate permissions policy set. As a member of the Contractors user group, Pat will not be able to change a probe's properties but will be able to see how the network is performing based on statistical analysis of the packets through network trending.
- **Responsibility: security team vs. network team**—Suppose Pat is a network administrator. As a network administrator, Pat needs access to many things, but all security analysis and artifact and stream reconstruction is handled by the security team of which Pat is not a member. Create two Authentication permission policies ("Security Permissions" and "Network Admin Permissions") and two user groups ("Security Admins" and "Network Admins") with the appropriate permissions policy set. As a member of the 'Network Admins' user group, Pat will not be able to reconstruct any artifacts such as VoIP calls or viewed websites, but will be able to capture and analyze traffic from a probe.
- **OMS role**—Suppose Pat is an OMS administrator while Chris is not. As an OMS administrator, Pat has the ability to add users, change passwords, and other tasks. Meanwhile, Chris is a user of the Observer Platform who should not have the same rights as Pat. Create an 'OMS Admin' group and add Pat to it. Add Chris to the 'Observer Platform' group.

Figure 2: User Groups



Chapter 4: How to configure how user accounts authenticate

Users are granted access after validating with OMS or a third-party authentication server like Active Directory, LDAP, RADIUS, or TACACS+.

Rather than maintaining separate user accounts on each asset, all assets on your network can query OMS to authenticate users. OMS can do it using an internally stored list of users and their passwords or forward the authentication request to a third-party authentication server.

1. Starting in the dashboard, click **Auth** > **Authentication**.
2. In the **Authentication Scheme** list, choose:
   - **Active Directory** and configure the Active Directory settings (page 10).
   - **LDAP** and configure the LDAP settings (page 12).
   - **Local** and configure the list of users and passwords manually.
   - **RADIUS** and configure the RADIUS settings (page 15).
   - **TACACS+** and configure the TACACS+ settings (page 16).
3. Click the accept icon ✓.

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.

LDAP settings

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

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 LDAP server. Required. Valid Input: Valid addresses include IPv4, IPv6, or DNS name.
Port	The port number accepting connections to the LDAP server. The default is 389.
Version	The LDAP protocol version the LDAP server 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

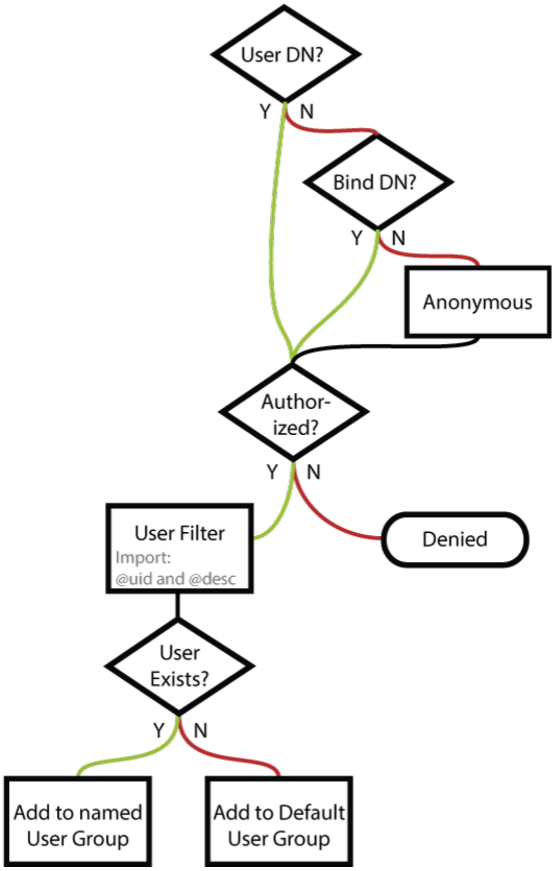
	Administrators should find the Base DN directly from the LDAP server to ensure accuracy.
Bind DN	The Bind Distinguished Name (**Bind DN**) is required for importing user accounts from the LDAP server. The Bind DN user account needs domain user privileges, and administrators should find a suitable Bind DN directly from the LDAP server to ensure accuracy.
Bind password	The password of the Bind DN. This is the password of the user set in 'Bind DN'.
Timeout in seconds	The duration a connection attempt waits before aborting. A connection retry attempt is made if this value elapses.
Synchronize LDAP groups with OMS	If selected, specified LDAP groups are brought directly into OMS as dynamic user groups. Any addition or removal of users in an underlying LDAP group will affect the OMS user group in the same manner. You must designate which LDAP groups are used for this purpose by writing an LDAP query in **Group filter**.
Synchronization	LDAP group synchronization can be performed automatically or manually. **Periodic** Automatically synchronize with LDAP at recurring periods. **Manual** Require manual synchronizations, and never synchronize automatically. With either choice, you can always synchronize by clicking '**Synchronize Now**'.
Synchronization Rate (hours)	Sets how frequently OMS synchronizes with the LDAP server, in hours. Each synchronization, OMS refreshes imported LDAP groups with any user additions and removals that occurred on the LDAP server during that time. Valid Input: Valid values are 1-24.
Group DN	The Distinguished Name of a group is the point in the directory tree from which groups are contained. Example: **ou=MIN,ou=USA,ou=UserGroups** -or- **ou=Groups,ou=Security** This might be the beginning of all groups or some place lower in the tree to limit the number of groups returned.
Group filter	The full LDAP query that determines which LDAP groups are imported and synchronized as OMS user groups. LDAP groups that are returned by your query become OMS user groups. Example: **(&(objectCategory=Group)(cn=USA-MIN-USERS-Net-Administrators))** Valid Input: The maximum number of characters is 16383.
Group ID attribute	The attribute in which the ID for each group is stored.

	If no group ID attribute is provided, then IDs are created automatically. Example: **uidNumber** -or- **objectGUID**
Group name attribute	The attribute in which the desired group name for each group is stored. Required. When synchronizing groups, the value in this attribute is mapped to the **Group Name** field in the **User Groups** table. Example: **cn** -or- **displayName**
Group description attribute	The attribute in which the desired description for each group is stored. When synchronizing groups, the value in this attribute is mapped to the **Description** field in the **User Groups** table. Example: **(&(objectCategory=group)(description=*))**
User DN	The User Distinguished Name (DN) is a user that will authenticate to the LDAP tree using a bind request. This user will be someone with access to search all or part of the LDAP directory tree. If left blank, and anonymous bind request is used. Use a User DN if: Use if LDAP installation does not support anonymous bind, and you do not want to save a bind DN and password. You have a fairly simple LDAP hierarchy and want to skip the initial search for users. You want to restrict who can log on. This is done through the Base DN. The Bind DN is different from where the user object is located.
User filter	The user filter restricts who may use the Observer Platform. The filter limits what part of the LDAP tree is used to validate user accounts so that OMS does not have large lists of users who do not require access to the Observer Platform. Required. Example: **(&(objectClass=person)(uid=$1))** Find all entries with an `objectClass` of 'person' where the `uid` is the **User DN** (represented by `$1`), including 'anonymous.' Valid Input: The maximum number of characters is 16383.
User ID attribute	The name of the attribute in which the user ID for each user is stored. If no user ID attribute is provided, then IDs are created sequentially starting with 90000000.
Username attribute	The name of the attribute in which the user name for each user is stored. Required. This used primarily when importing users. When importing users, values in the *uid* attribute are mapped to the Username field for display in the **Users** list.
User description attribute	The name of the attribute in which the description for each user is stored. This used primarily when importing users. When importing users, values in the *displayName* attribute are mapped to the Description field for display in the **Users** list.

Understanding how OMS authenticates with LDAP

OMS authenticates with the LDAP server when a bind request is accepted.

To authenicate with the LDAP server, the following steps are performed for a bind request:



RADIUS settings

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

You can use your RADIUS server to authenticate users, but you cannot import a list of users from it. You can, however, manually enter them or get a list of users from your domain server and then switch the authentication type.

You define primary and secondary RADIUS servers. Refer to the documentation of your third-party RADIUS server for more details. Choosing RADIUS authentication requires you to enter the IP address of the RADIUS server, along with a "shared secret" that matches a secret on the RADIUS server.

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.
Shared secret	Providing the shared secret, a text string, is necessary for authenticating with the RADIUS host.
Authentication type	The authentication method of the server(s) must be specified.
Server	One RADIUS server is required. If two servers are declared, the first server is used unless unreachable. Valid Input: Valid addresses include IPv4, IPv6, or DNS name.
Port	Modern port assignments for RADIUS access servers are UDP 1812 and 1813. Legacy port assignments are still common: UDP 1645 and 1646.
Retry attempts	The maximum number of connection retries per authentication attempt. If the maximum is reached, no further retries occur until the next authentication attempt. Valid Input: Valid values are 0-9.
Timeout in seconds	The duration a connection attempt waits before aborting. A connection retry attempt is made if this value elapses.

TACACS+ settings

Use the information to assist you when configuring the **Authentication** to use TACACS+.

You can use your TACACS+ server to authenticate users, but you cannot import a list of users from it. You can, however, manually enter them or get a list of users from your domain server and then switch the authentication type.

You define primary and secondary TACACS+ servers. Refer to the documentation of your third-party TACACS+ server for more details. Choosing TACACS+

authentication requires you to enter IP address of the TACACS+ server, along with a "shared secret" that matches a secret on the TACACS+ server.

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.
Shared secret	Providing the pre-shared key, a secret text string, is necessary for authenticating with the TACACS+ host.
Authentication type	The authentication protocol the TACACS+ server accepts requests over must be specified.
Server	One TACACS+ server is required. If two servers are declared, the first server is used unless unreachable. Valid Input: Valid addresses include IPv4, IPv6, or DNS name.
Port	The standard port assignment for TACACS+ login is TCP port 49. Some deployments might use a different port number.

Chapter 5: Understanding assets and asset elements

An *asset* is any hardware appliance or software installation that can be managed by OMS. An *asset element* is the main functional part of an asset with which a user interacts, such as a probe instance, business group, or device group.

For this section, it is important to understand the distinction between an asset and asset element.

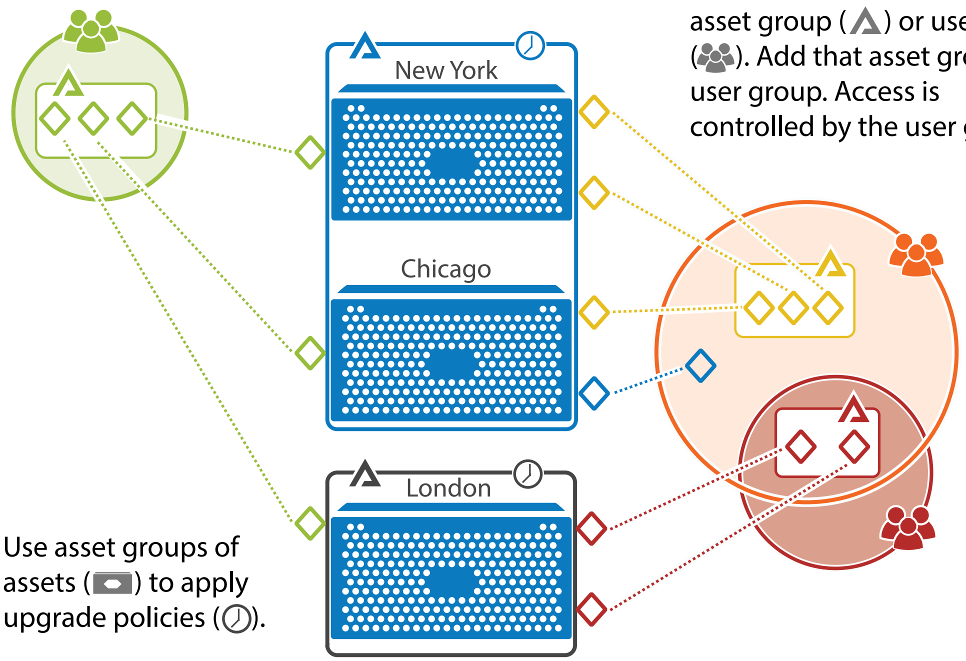
An asset communicates the properties that uniquely identify it the first time it connects to OMS. OMS retrieves information about any available asset elements.

Who may use an asset is controlled through the permission policy of the asset group and through user group membership. When an asset may be upgraded is controlled through its upgrade policy. For this reason, you may want to have your asset groups contain only assets or only asset elements.

Because an asset or asset element may be a member of only one asset group, you must decide how to organize your assets and asset elements. Typically, you do not want to mix assets and assets elements in the same asset group. When you place an asset in a group you automatically grant access to all of its underlying asset elements. Most end users need access to only the underlying asset elements. Moreover, most end users do not need to upgrade the software version of an asset. An asset element cannot be upgraded by itself—only the asset may be upgraded. In other words, asset elements are upgraded only when an asset's software version changes. By keeping assets separate from asset elements in your asset groups, as an OMS administrator you have more granular control over the objects in your Observer Platform environment.

This image shows five asset groups and three user groups. The assets in New York and Chicago are updated together but separately from the asset in London because it is in a different asset group. Multiple asset groups and even individual asset elements can be in a user group (orange user group). An asset group can be in multiple user groups (red asset group).

Figure 3: OMS Relationships



Add asset elements (◇) to an asset group (△) or user group (👥). Add that asset group to a user group. Access is controlled by the user group.

Use asset groups of assets (▬) to apply upgrade policies (🕒).

Assets are the two most recent major versions of:

Asset	Asset Elements
Observer Analyzer	Probe instances
Observer GigaStor and Observer probes	Probe instances
Observer Apex	Business groups
Observer Infrastructure (OI)	Device groups
Observer Matrix	N/A

6

Chapter 6: Understanding auto-adding assets and licenses

Having assets automatically added to OMS reduces the upfront configuration necessary for the OMS administrator.

Two common scenarios, both of which are equally valid, make sense under different circumstances.

If you already have several existing Observer Platform products and now you want to centrally manage them, then configure assets to submit their licenses when they request to be managed by OMS. As assets connect to OMS for the first time, they are added to OMS. There is little for you as the OMS administrator to do other than to add the asset to an asset group. However, depending on the configuration of your Global Asset Policy, these assets might be automatically assigned to an asset group. There is nothing more you need to do in these cases.

If you do not have any existing Observer Analyzer Platform products or you acquired several new assets and you are deploying them simultaneously, then preload the asset licenses into OMS. Whenever an asset connects for the first time, it requests a license and to be added, which OMS issues and grants. As assets come online, as an administrator, you may need to add the asset to an asset group. However, depending on the configuration of your Global Asset Policy, these assets might be automatically assigned to an asset group. There is nothing more you need to do in these cases.

Unlike in previous versions, after an asset is managed by OMS it is permanently managed by OMS unless the asset is deleted (not disabled) from OMS. There is no option on the local asset that allows a user to remove the asset from OMS management.

This table describes the process of what happens when a users requests to automatically add an asset.

Table 1. Auto-Adding An Asset

If the asset[1]...	Then[2]...
Already exists in OMS and is licensed	1. OMS verifies the asset's ID and its license. It is already managed by OMS.
Already exists in OMS and is not licensed	1. OMS verifies the asset's ID. 2. The asset requests a license from OMS. a. If a license for that asset type exists, a license is issued and the asset is now managed by OMS. b. If no license for that asset type is available, the request is rejected. The asset cannot be used.
Does not exist in OMS and is licensed	1. The asset requests to be added. 2. OMS verifies the license from the asset and adds the license to the managed licenses. 3. OMS adds the asset to its assets list. The asset is now managed by OMS.
Does not exist in OMS, is not licensed, and a license exists	1. The asset requests to be added and a license. 2. The asset requests a license from OMS. a. If a license for that asset type exists, a license is issued. OMS adds the asset to its assets list. The asset is now managed by OMS. b. If no license for that asset type is available, the request is rejected. The asset cannot be used.
Does not exist in OMS, is not licensed, and no license exists for it	1. The asset requests to be added and a license. 2. The request is rejected. The asset cannot be used.

[1] Only probes, Observer GigaStor, and Observer are supported for automatically adding assets.

[2] Assumes user has the right to auto-add assets and licenses (separate permissions).

7

Chapter 7: How to manage software versions using OMS

Assets and asset groups can be upgraded or downgraded according to the upgrade policy applied to them.

The initial set up required for managing asset software versions is complex. However, it is complex only due to the need to plan transfer and installation times, select which assets to control, and understand the upgrade policy precedence. This setup process only needs to be performed when necessary, so it becomes easier to maintain after initial setup.

- If you are setting up an upgrade policy and version control for the first time, we recommend following each step in order.
- If you are modifying an existing upgrade policy or fine-tuning the version control, you can choose to follow the step(s) that are most relevant.

These are the overall steps for managing software versions using OMS, and each is described in fuller detail in other sections:

1. Configure the settings for version control using How to download upgrades for upgrade policies to use (page 23).
2. Create an upgrade policy using How to create an upgrade policy (page 23).
3. Try applying an upgrade policy to either of the following:
   a. An asset group using How to update asset groups (page 25).
   b. An individual asset using How to update individual assets (page 25).
4. Learn about the hierarchy of upgrade policies and what policy takes effect using Understanding which upgrade policy is in effect on assets (page 29).

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 Analyzer 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.

How to create an upgrade policy

Create and use an upgrade policy to automate the transfer and installation of software upgrades to assets or asset groups.

To create an upgrade policy:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. Click the new icon ⊕.

3. Complete the fields shown using information in Settings and options of an upgrade policy (page 24).
4. Click **Accept**.

You successfully created an upgrade policy. If you apply the upgrade policy (page 25) to an asset or asset group, the upgrade policy takes effect.

Settings and options of an upgrade policy

The upgrade policy settings control the upgrade behavior of assets. These behaviors take effect after the upgrade policy is applied to an asset or asset group.

Name	The name of this upgrade policy.
Description	Upgrade policy descriptions are optional.
Allow to auto-upgrade	Sets if this upgrade policy is active. If selected, the upgrade policy is enabled. Assets that subscribe to an enabled upgrade policy are automatically upgraded.
Also allow to auto-downgrade to the current OMS version	If selected, Observer Platform applications running later versions than OMS is distributing are automatically downgraded.
Limit upgrade transfer speed to	Sets the preferred maximum transfer speed in kilobits per second. Use the value '0' to disable this bandwidth restriction.
Transfer schedule	This sets the window of time OMS can transfer upgrade data to assets. Scheduling the upgrade transfer does not define when the transfer should start or finish.
Install schedule	This sets the window of time OMS can initiate an upgrade installation of your assets. Scheduling the upgrade installation does not define when the upgrade installation should start or finish.

How to disable an upgrade policy

You can temporarily discontinue an upgrade policy by disabling it. Each asset configured to use a disabled upgrade policy will use the global upgrade policy instead.

To disable an upgrade policy:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. Click an upgrade policy to select it.
3. Click the edit icon ✎.
4. Clear **Allow to auto-upgrade**.
5. Click **Accept**.

Any assets that are assigned the disabled upgrade policy now use the global upgrade policy. This continues until the disabled upgrade policy is re-enabled. For details about the global upgrade policy, see How to modify the global upgrade policy (page 26).

How to delete an upgrade policy

Delete an upgrade policy to remove it from the assigned assets and asset groups it was assigned to, plus from OMS. Assets and asset groups without an upgrade policy will immediately begin using the default upgrade policy instead.

To delete an upgrade policy:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. Click an upgrade policy to select it.
3. Click the garbage can icon 🗑.
4. Click **Yes** to confirm the deletion.

The upgrade policy has been deleted from OMS. Assets and asset groups that were assigned this upgrade policy now use the default upgrade policy instead.

How to update asset groups

All assets in an asset group can follow the same upgrade behavior. Use an upgrade policy on an asset group to control the upgrading behavior of the entire group.

Prerequisite(s):

Before following these steps, an upgrade policy must have already been created.

To use an upgrade policy to update asset groups managed by OMS:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. Applying an upgrade policy is an easy drag-and-drop operation from the **Upgrade policies** list to an asset group in the **Asset Groups** table.

   The name of the upgrade policy appears in the **Upgrade Policy** column of the table, confirming that it has been applied.

Now, when an asset either obtains a license from OMS or is contacted by OMS (approximately every hour), OMS verifies that the client has the active version and upgrades or downgrades if necessary.

How to update individual assets

Individual assets can also have an upgrade policy applied to them.

Prerequisite(s):

Before following these steps, an upgrade policy must have already been created.

To use an upgrade policy to update software on a per-asset basis:

1. Starting in the dashboard, click **Version** > **Upgrade Policies**.
2. Applying an upgrade policy is an easy drag-and-drop operation from the **Upgrade policies** list to an asset in the **Assets** table.

   The name of the upgrade policy appears in the **Upgrade Policy** column of the table, confirming that it has been applied.

Now, when an asset either obtains a license from OMS or is contacted by OMS (approximately every hour), OMS verifies that the client has the active version and upgrades or downgrades if necessary.

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.

Upgrade Version settings

Some settings affect the downloading of available upgrade versions, the port used, and if any applications should be excluded.

Check for upgrades	If selected, OMS periodically checks for upgrades. Scheduled transfers and installs rely on knowing if new versions exist. If cleared, users must manually check for available upgrades before any scheduled transfers or installs can occur.
Automatically match OMS version	If selected, the active version will automatically be set to match the OMS version.
Upgrade server port	Sets which TCP port is used by the upgrade file server. The default port is 8008.
Preferred speed (Kbps)	Sets the preferred maximum transfer speed in kilobits per second. Use the value '0' to disable this bandwidth restriction.
Download upgrades	Schedules the download of available upgrade versions. Downloaded versions will not automatically install unless an installation schedule or upgrade policy allows it.

Expert Console Observer	If selected, this upgrade policy does not apply to Expert Console Observer.
Observer	If selected, this upgrade policy does not apply to Observer.
Observer Infrastructure	If selected, this upgrade policy does not apply to Observer Infrastructure (OI).
Observer Apex	If selected, this upgrade policy does not apply to Observer Apex.

8

Chapter 8: Understanding the OMS upgrade process

In OMS, an upgrade policy can automate the transfer and installation of software versions, such as when new releases must be deployed to remote sites. Careful planning is required to ensure successful transfer and installation.

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.

Under what circumstances should I use an upgrade policy?

There are no steadfast requirements or conditions that must be met for an upgrade policy to prove beneficial.

However, there are scenarios where an upgrade policy proves especially useful. Here are a few examples:

- You need to upgrade off-site assets that you have no direct access to.
- You have many assets that need to be upgraded; an upgrade policy can apply to full asset groups.
- You want to transfer the installation files during non-peak network times.
- You have limited uplink speeds and need to throttle the transfer speed.

- You want to ensure the installation occurs during non-peak network times, like overnight.[1]
- You want to resume the data transfer from the point of termination if the connection terminates unexpectedly.[1]

Understanding which upgrade policy is in effect on assets

Individual assets always honor the nearest upgrade policy. For example: if an asset has an upgrade policy applied to it, that upgrade policy is always honored —even if the asset is a member of an asset group that has its own upgrade policy.

This behavior allows individual assets to follow a different upgrade policy than the upgrade policy applied to its parent asset group.

In the context of any specific, individual asset:

- If an upgrade policy is missing from both an asset and its asset group, then the default upgrade policy takes precedence.
- If an upgrade policy is missing from an asset but one exists on its parent asset group, then the upgrade policy of the asset group takes precedence.
- If an upgrade policy exists for both an asset and its asset group, then the upgrade policy of the asset takes precedence.

Table 2. Which upgrade policy is in effect on a specific asset?

Upgrade policy applied to asset	Upgrade policy applied to asset group	Default upgrade policy is enabled	Policy that takes precedence on the asset
X	X	X	Asset
X		X	Asset
X	X		Asset
	X	X	Asset Group
	X		Asset Group
		X	Default Upgrade Policy
			No policy

How does the scheduled transfer operate?

Scheduling your upgrade transfer is an effective strategy for limiting the ill-effects of network resource consumption otherwise caused by an on-demand upgrade transfer. Because upgrade data is sent over the same link that the target assets use for other duties, it is recommended that upgrade transfers are only scheduled during opportune times. Scheduling the upgrade transfer does not define when the transfer should start or finish. This sets the window of time OMS can transfer upgrade data to assets. OMS makes every attempt to send

[1] These options are only available to Observer Analyzer and probes already at or above version 16.1.

data during the scheduled transfer time, but you should schedule a large enough time frame for OMS to facilitate the transfer.

If a transfer cannot successfully finish within the time frame you set, OMS resumes the transfer—from where it was interrupted—during the next time frame available.[1] For example, if you set a one-hour transfer window for Tuesday each week, and the transfer did not complete during that hour, then the transfer is suspended until the following Tuesday for the transfer to resume.

How does the scheduled installation operate?

When asset upgrades occur, the probe must be stopped from its monitoring duties during the upgrade installation and must ultimately reboot. These two events cause downtime. Therefore, by controlling the installation time, you can control when the downtime occurs. In this way, scheduling the upgrade installation is, essentially, scheduling the time frame an asset outage is acceptable. Scheduling the upgrade installation does not define when the upgrade installation should start or finish. This sets the window of time OMS can initiate an upgrade installation of your assets.

9

Chapter 9: Understanding asset licenses and licensing

Each Observer Platform product requires a product license for full operation. OMS can deliver to those products (assets) any matching licenses that you own. This eliminates needing to license each asset one-by-one from each of their own interfaces. Plus it also allows you to manage licenses in one central application.

To fully operate, each asset requires its own license. A valid product license enables you to the use of the product and version specified by the license and according to the user agreement. Whether or not you are using OMS, every Observer Platform product requires a unique license. You cannot share licenses between assets and users as there is no “floating seat” or “user seat” license model. Additionally, licenses are asset-driven and therefore never associated with any user account. A contact name may be shown in license document itself, but this has no ties to a user sign in. OMS does not alter the licensing model for Observer Platform products in any way, but it does make it easier to license products and maintain those licenses.

All licenses can be added to a central repository. OMS can maintain all of your Observer Platform product licenses in one place so you never lose them. You can see which licenses your institution owns[1]; which license is applied to a specific asset, if any; which licenses are available to be applied; and plus you have the ability to non-destructively disable licenses. Overall license management by OMS can be turned on or off using the Global Asset Policy and is enabled by default.

If you unlicense an asset, the license returns to your available licenses. This means the license can then be freely applied to another product or reapplied to the one you stripped it from. However, in all cases, you still have only one license and it can be applied to one asset only. For example, removing a license from Observer Analyzer “A” and then applying that license to Observer “B” means

[1] Only licenses in OMS that you enter manually or import in bulk are shown.

that Observer “A” can no longer fully function. There is no round-robin licensing agreement or mechanism that allows Observer “A” and “B” to share a single license—one will be licensed, while the other will not be. In this example you need two Observer licenses if you intend to use Observer “A” and Observer “B”.

> **Tip!** Valid licenses can be automatically assigned (page 20) to assets the first time they connect to OMS.

Some licenses have special characteristics that you should be mindful of when applying them to assets. For example, the Observer GigaStor Software Edition (GSE) has a variety of licenses that allow a set storage size for data retention, and therefore it is not economically sound to license a system having 4 TB of total storage, only, with a 32 TB GSE license. In cases where OMS automatically licenses an asset (page 20) with a license that is not optimal for the intended use of that product, you should reverse the licensing process to unlicense it, and then apply the most correct license. If you have no available licenses—all licenses have been applied to all assets—you may need to unlicense a similar asset and swap the licenses of these two assets from one to the other. One method for reserving a special license from being auto-assigned is to disable the license immediately after you add it to OMS. This ensures it cannot be auto-assigned, and gives you full control of where it will be placed.

10

Chapter 10: How to upgrade OMS

New and past versions of OMS software are made available to you directly from VIAVI. Use the OMS upgrade tool to check for, download, or install a version of OMS.

Prerequisite(s):

- Internet access to **update.viavisolutions.com** (port 80) is required on the system interacting with the VIAVI upgrade repository. This includes checking for upgrades and downloading upgrades. Only OMS requires this; none of your managed assets do.
- Only if your application or appliance is managed by OMS, LAN access to the OMS system over port 8008 (default) is required for downloading upgrades. The port can be changed (page 26) in OMS.
- Proxy settings (page 35) can be used if direct Internet access is unavailable.

The OMS upgrade tool allows you to:

- Check the VIAVI upgrade repository for old and new versions of OMS.
- Download any available version of OMS for offline installation.
- Install any available version of OMS without needing to leave the OMS interface.

How to retrieve a list of available OMS versions

A listing of OMS software versions to upgrade or downgrade to is available directly in OMS. Connect to the VIAVI upgrade repository to retrieve the latest listing of available versions.

Note: Interacting with the upgrade repository requires web connectivity over TCP port 80 or 8008 (by default) on the OMS system. This can be

> achieved with direct connectivity from OMS to the web or by configuring a proxy in the proxy configuration settings of OMS for downloads. The upgrade repository is hosted by VIAVI and no public mirrors are used.

To ensure your product is using the latest code available, always check the in-product update capability even if you have recently installed. It is strongly recommended that all product updates and upgrade are performed using the in-product update methods instead of installing the executable using Windows File Explorer.

To retrieve a list of available versions, click **System** > **Update** .

To retrieve a list of available versions:

1. Starting in the dashboard, click **System** > **Update**.
2. Click the refresh icon ↻.

OMS connects to the upgrade repository and displays the versions available for download. Release notes for each version are available for viewing.

How to download a version of OMS

New or old versions of OMS can be downloaded from the upgrade repository. OMS is not automatically installed after downloading a version using this method. Instead, this method is suitable for scheduled installation or installation from Windows Explorer.

> **Tip!** It is strongly recommended that you perform product updates using the in-product update method instead of installing with Windows File Explorer.

To download an available version of software for later installation, visit the repository and download any self-extracting setup executable:

1. Starting in the dashboard, click **System** > **Update**.
2. (Optional) Click the check for updates icon ↻.

   Example: (Optional) Doing this ensures all available versions are shown.
3. Select one by clicking a table row.
4. Click the download icon ⤓.

   If not previously downloaded, the download begins, and you can view its transfer progress.

You successfully downloaded a software upgrade.

How to install a version of OMS

Installing a software upgrade downloads the self-extracting setup executable and immediately installs the upgrade.

To install a software upgrade:

1. Starting in the dashboard, click **System** > **Update**.

2. Select one by clicking a table row.
3. Click the install icon 💾.

   The download begins, and you can view its transfer progress.

   After the download completes, the software upgrade begins installing.

You successfully installed the selected software upgrade. A notification appears if any errors occur during the upgrade.

Upgrade settings

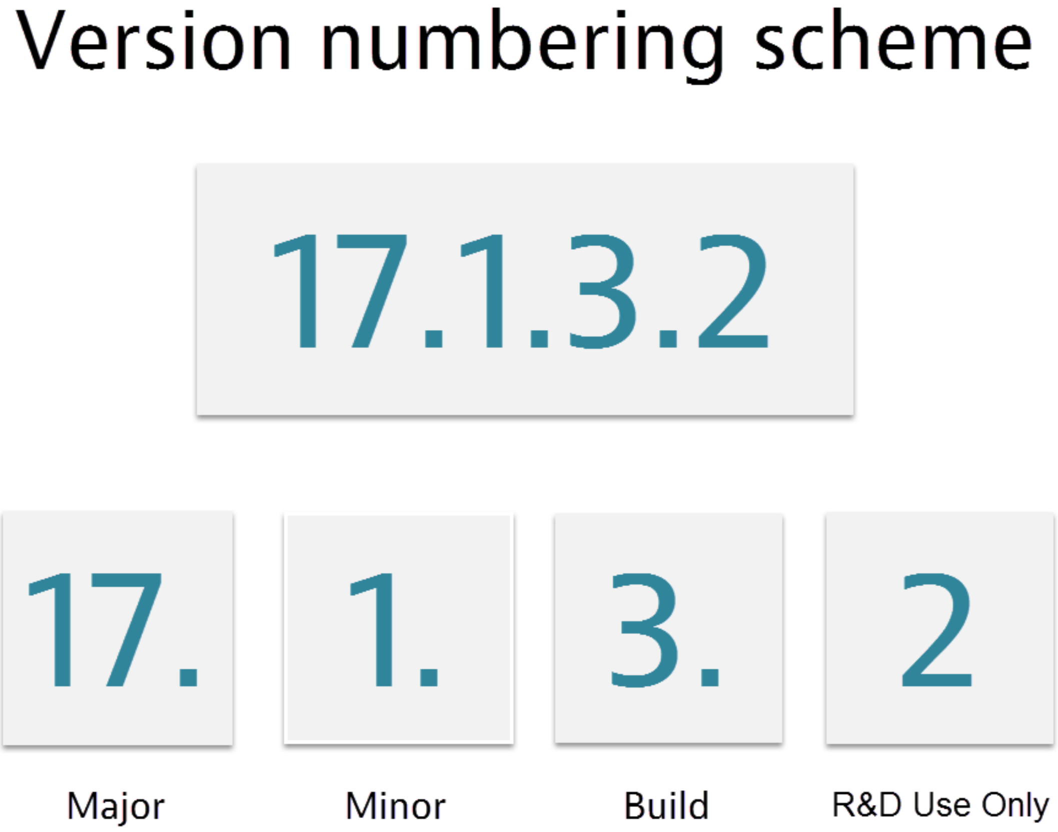
There are several settings that change the behavior of version upgrades.

Check for upgrades	If selected, OMS periodically checks for upgrades. Scheduled transfers and installs rely on knowing if new versions exist. If cleared, users must manually check for available upgrades before any scheduled transfers or installs can occur.
Show downgrade options	If selected, any available downgrade versions are displayed in the available versions list. It is recommended to leave this cleared (disabled) if downgrading to previous versions is not desirable.
Preferred speed (Kbps)	Sets the preferred maximum transfer speed in kilobits per second. Use the value '0' to disable this bandwidth restriction.
Use proxy server	If selected, a proxy server is used for downloading upgrade versions.
Proxy type	Sets which type of proxy server to connect to.
Proxy address	The IP address or DNS name of the proxy server.
Proxy port	The port number accepting connections to the proxy server.
Proxy user	Sets the user name expected by the proxy server for authentication. Leave this box empty if authentication is not required.
Proxy password	Sets the password used to authenticate with the proxy server. Leave this box empty if authentication is not required.
Download upgrades	Schedules the download of available upgrade versions. Downloaded versions will not automatically install unless an installation schedule or upgrade policy allows it.
Install upgrades	Schedules the installation of downloaded version upgrades. This setting affects version upgrades that are downloaded both automatically or manually.

Version numbering

Observer Platform products use a four-field decimal scheme for product versions.

Figure 4: Version numbering scheme



Portion of version number	Some defining characteristics[1]
(**17**.1.3.2) — **Major**	Major version indicator. Full platform version. Moving past this number requires a new license for your product (or products).
(17.**1**.3.2) — **Minor**	Minor version indicator. New core functionalities, communication libraries, bug fix roll-ups, and more.
(17.1.**3**.2) — **Build**	Build version indicator. Bug fixes and minor feature enhancements.
(17.1.3.**2**) — **R&D Use Only**	Used for R&D purposes only, should generally be 0.

[1] These are representative examples only. No development efforts are restricted to just the examples shown.

Index