NetWitness® Platform

Version 12.5

Licensing Management Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2024

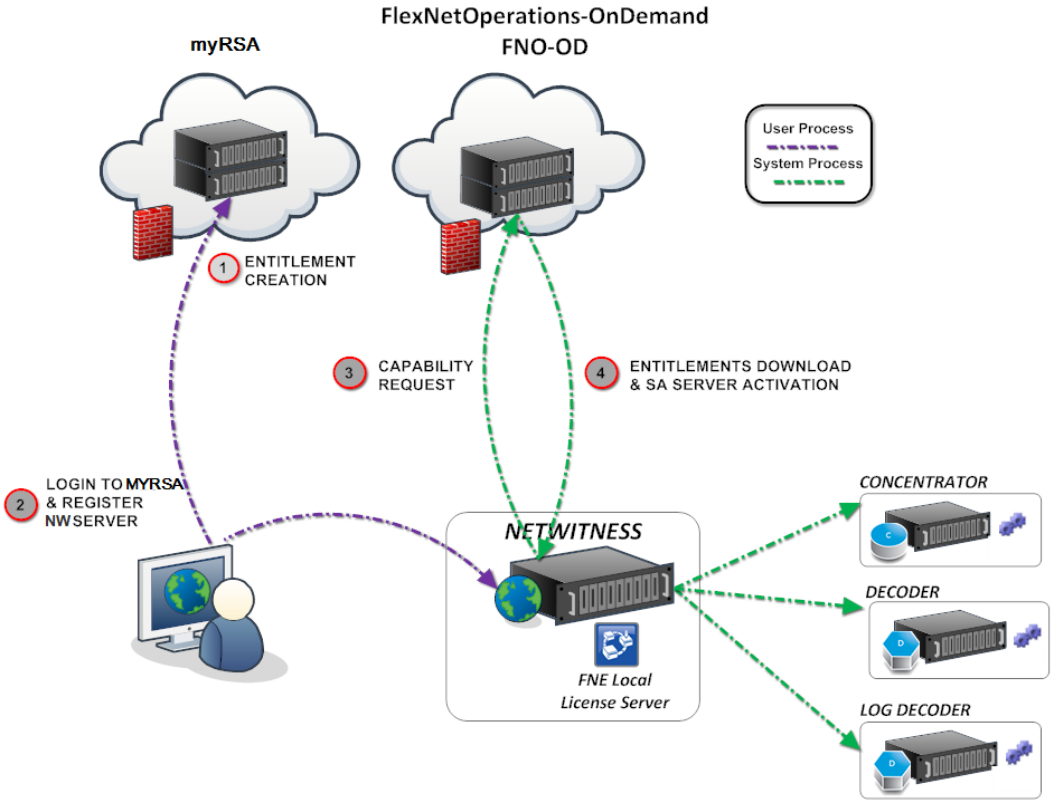
Contents

Entitlement Capability Implementation **5**
NetWitness Platform Licensing Overview **7**
Obtain License Server ID from NetWitness Platform User Interface **8**
Access myRSA **9**
Register the Server (Online Registration) **11**
Map Entitlements **16**
View Current Licenses 18
View and Manage Licenses 18
Register the Server (Offline Capability Request) **20**
Prerequisites 20
Download an Offline Request for Submission to myRSA 20
Upload an Offline Capability Response to NetWitness Platform 23
Refresh Licenses 23
License Types **24**
Choosing a License Type 24
Throughput Licenses 25
Appliance Licenses 26
User and Entity Behavior Analytics Licenses 26
Endpoint Licenses 27
Out-of-the-Box Trial License 27
Configure License Support For Multiple NetWitness Servers **28**
Configure License Notifications **29**
About Out-of-Compliance Banners **31**
Troubleshoot Licensing **33**
Out-of-Compliance Banners 33
Common Log and Configuration Files 33
NetWitness Server Problems 33
Wrong License Mapping Issue 34
License Details **36**
Related Topics 37
Usage Trends 40

Reassign Service Licenses **45**
View and Export Usage Stats **48**
Settings **50**
Out-of-Compliance Reference **53**
Out-of-Compliance State 54
License Approaching Out-of-Compliance 55
License Usage Calculations for Decoder and Log Decoder Services **57**

Entitlement Capability Implementation

This topic describes how licensing of appliances and services is implemented in NetWitness. The entitlement capability leverages myRSA (https://my.rsa.com/) as the mechanism for entitlement delivery.



Key	Description
1	**Entitlements Created and Available to Customer.** After a customer order is processed, the entitlements (licenses) become available in myRSA. The entitlements are tied to an individual account.
2	**Register NetWitness Server on myRSA and Map Entitlements to the Local License Server (LLS).** • Customers log on to myRSA and view the entitlements to which they have access within their account. • Customers map entitlements to their Local License Server using the License Server ID (displayed in the NetWitness (Admin) **> System > Info** panel). The License Server ID is used only for mapping entitlements to a Local License Server and does not pertain to appliance activation.

Key	Description
3	**Synchronize the Server and Download Mapped Entitlements.** There are two methods for customers to synchronize with FlexNet Operations-On Demand (FNO-OD) and download the mapped entitlements to their LLS. • **Sites with Internet connectivity.** If the LLS has Internet connectivity, the LLS attempts to synchronize with FNO-OD every 24 hours over HTTP (TCP-80). Customers with Internet connectivity can also perform on-demand synchronization, using the **Refresh** option in the (Admin) **> System > Licensing** panel on the NetWitness Server. For more information, see Register the Server (Online Registration). After the synchronization, endpoint entitlements that were mapped to the Local License Server on the NetWitness Platform appliance are synchronized on hourly basis by port 443. • **Sites in closed environments.** Customers can synchronize the mapped entitlements by downloading a capability request and importing it on the NetWitness Server. For more information, see Register the Server (Offline Capability Request). After the synchronization, entitlements that were mapped to the Local License Server on the NetWitness appliance are synchronized, but the entitlements have not been used in any way. For example, if you have purchased 10 Decoders and 10 Concentrators, 10 of 10 Decoder entitlements and 10 of 10 Concentrator entitlements would be available on the NetWitness Server.

Note: FNO-OD is the license server in the cloud on myRSA. The URL is rsasecurity.subscribenet.com. The customer's firewall must allow communications between this URL on port 80 (whatever it resolves to when using lookup or whois) and the NetWitness IP address.

NetWitness Platform Licensing Overview

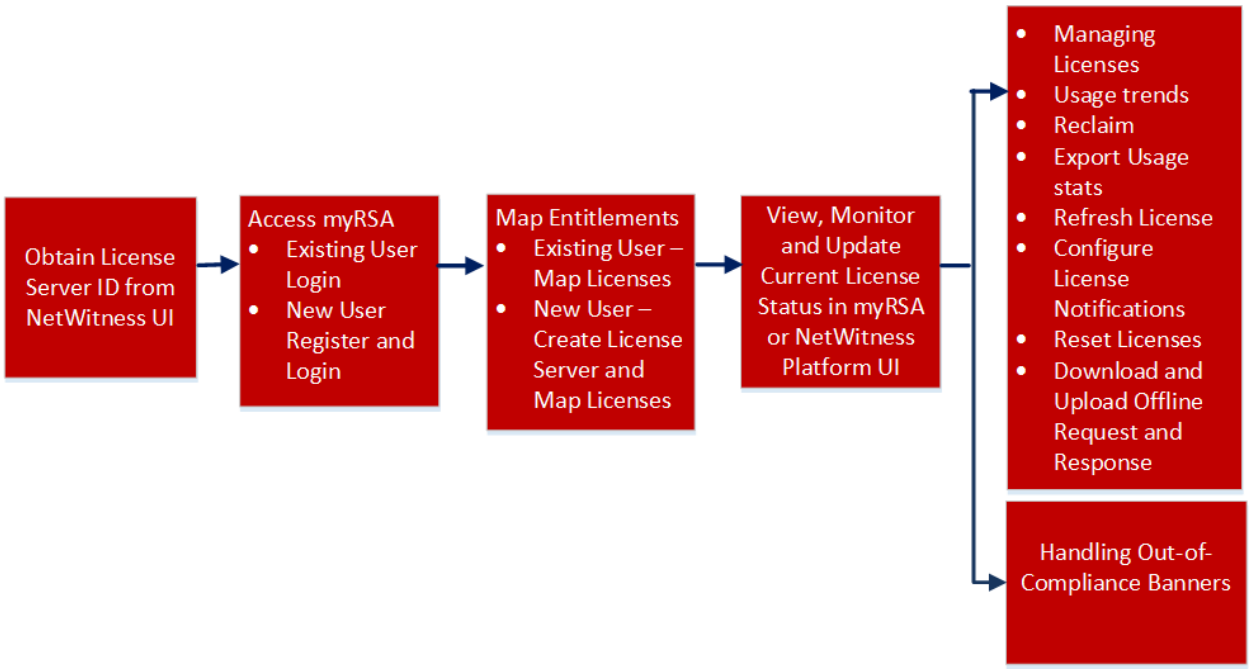
After you have purchased the licenses and have received all the relevant email communications, perform the steps required to map entitlements in NetWitness. You must perform each step in the proper sequence.

This document is divided into three parts:

- How to obtain license information from myRSA and view in the NetWitness Platform UI
- Understanding License Types and its functionality
- Troubleshooting or maintenance information

Workflow

The following workflow illustrates the end-to-end licensing process after you have the NetWitness product installed .



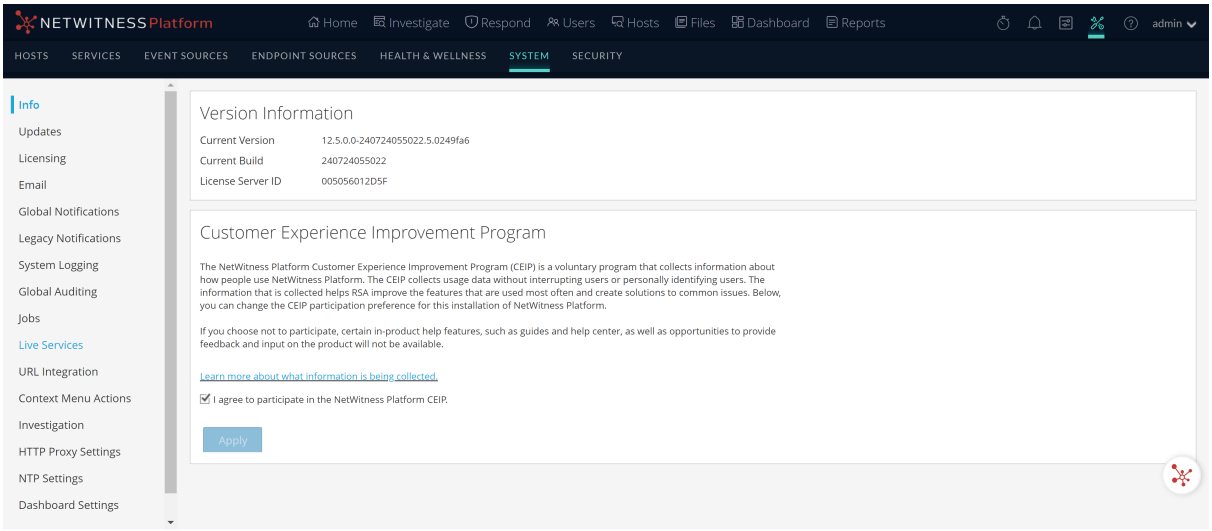
Obtain License Server ID from NetWitness Platform User Interface

Before you begin the licensing process, you must make sure that you obtain the License Server ID displayed in the NetWitness User Interface which is generated on the successful installation of the product.

To obtain the license service ID:

1. Log in to the NetWitness user interface.
2. Go to **(Admin) > System**.

   The Admin System view opens to display the Version Information in the **Info** panel.

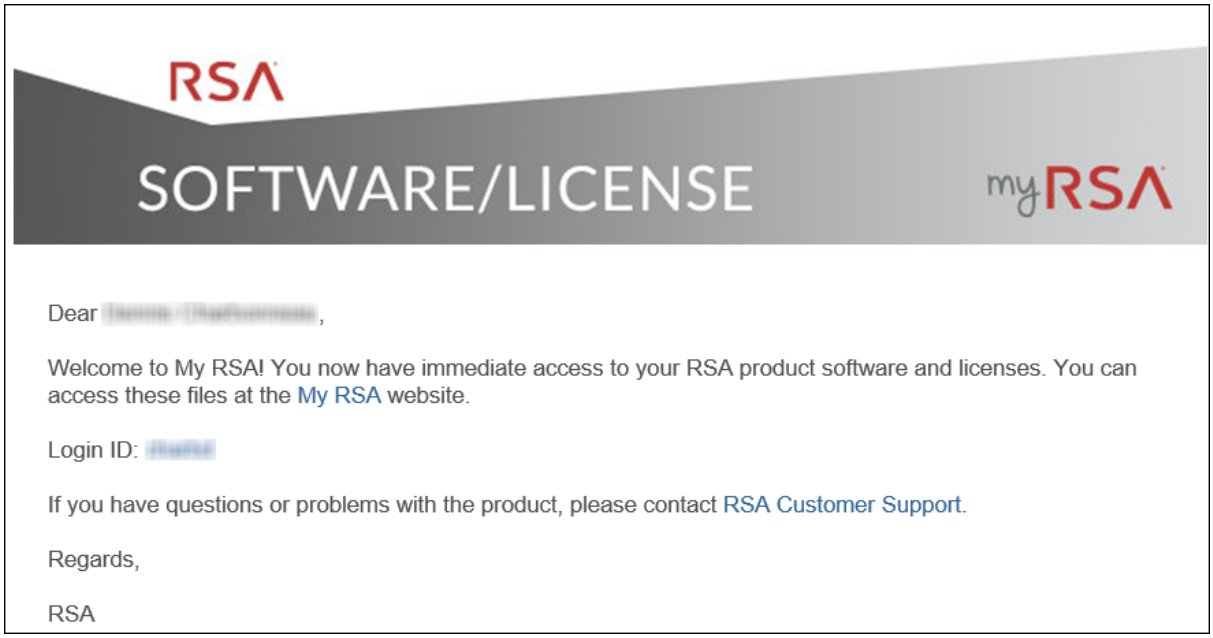


3. Under **Version Information**, locate the **License Server ID** and make a note.
   Log in to **myRSA** and enter the License Server ID to view your entitled license information. For more information, see Access myRSA.

Access myRSA

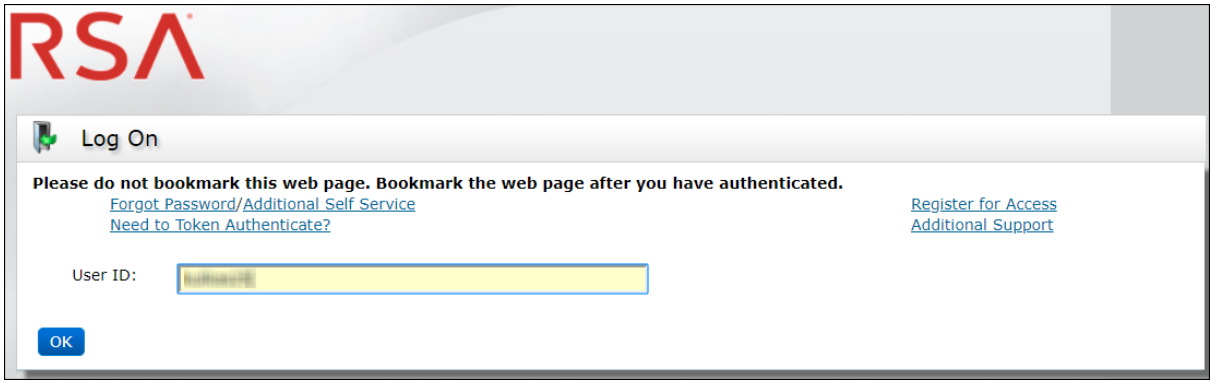
You will receive an order confirmation e-mail. Refer to your myRSA email for login information. If you are a new myRSA user, you also receive an e-mail containing instructions on how to create a new account. Your myRSA Welcome e-mail message contains system log in instructions to myRSA. This document provide you instructions on how to map your product licenses on the myRSA website.

1. The new users instruction e-mail contains a **Click Here** link. This link opens an Enrollment Portal, where the Risk-Based Authentication (RBA) method must be configured for the account.
2. After the RBA method is enabled, a Confirmation e-mail message containing the User ID (which is your e-mail address), along with a temporary password is sent. After the first login, you are prompted to change the password. Once the password is changed, you are logged into myRSA.



Note: If you have a pre-existing account for the RSA Link or RSA Online websites, you receive only one e-mail on how to use your existing login credentials. You must log into myRSA with your existing User ID, password, and RSA method.

3. When you navigate to https://my.rsa.com/, the **RSA Secure Logon** screen is displayed.



4. Enter your User ID and click **OK**, which displays the **Password** field. When you enter the password, you are logged into myRSA.

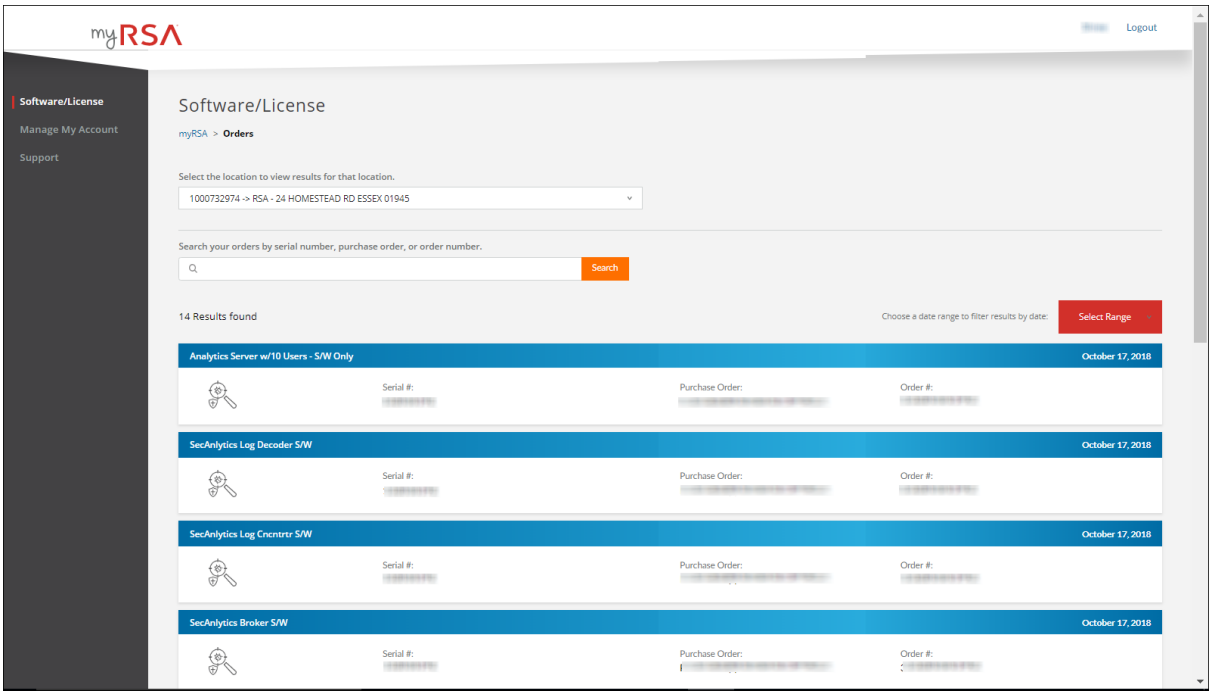
   Your contact e-mail address is used to authenticate your User ID. If the Customer Authentication process is successful, the myRSA Software/License page displays a list of all the following products available which are associated to your site location:

   - RSA Products
   - Serial Numbers
   - Purchase Orders
   - Sales Orders

   Note: You may be prompted to verify your identity through your RBA method, if multiple log in failures occur in a row, or if you have not logged into myRSA within the past several months.

5. In the Sofware/License page, select the Order Location from the drop-down menu. The list of products, sales orders, and purchase orders are filtered and displayed.

   The **Order Detail** screen is displayed.

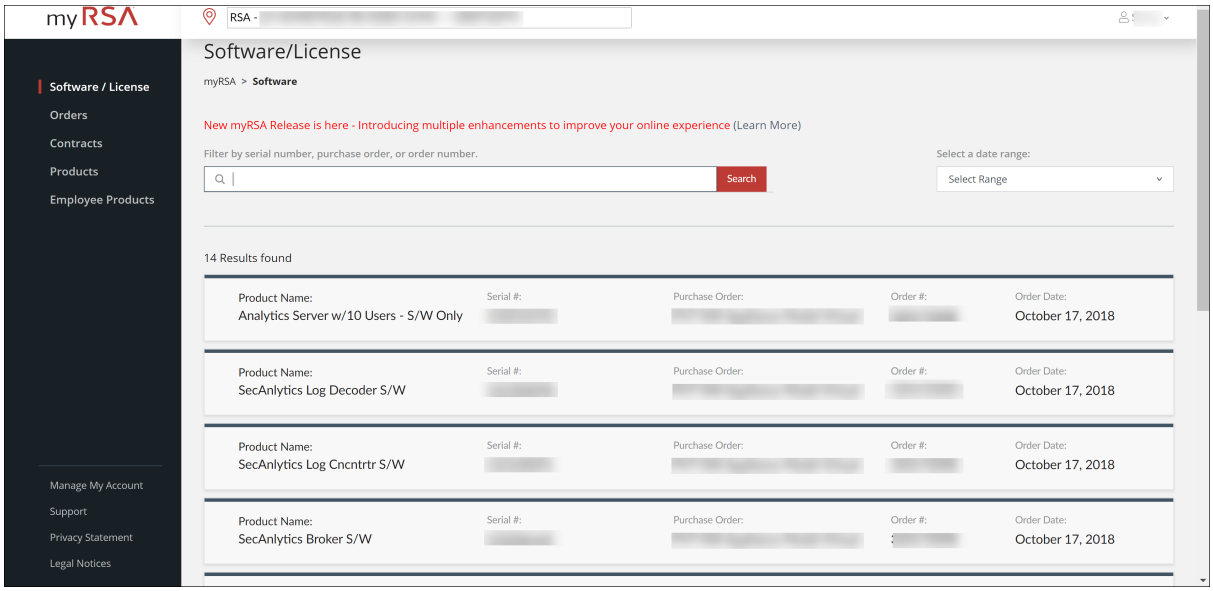


Register the Server (Online Registration)

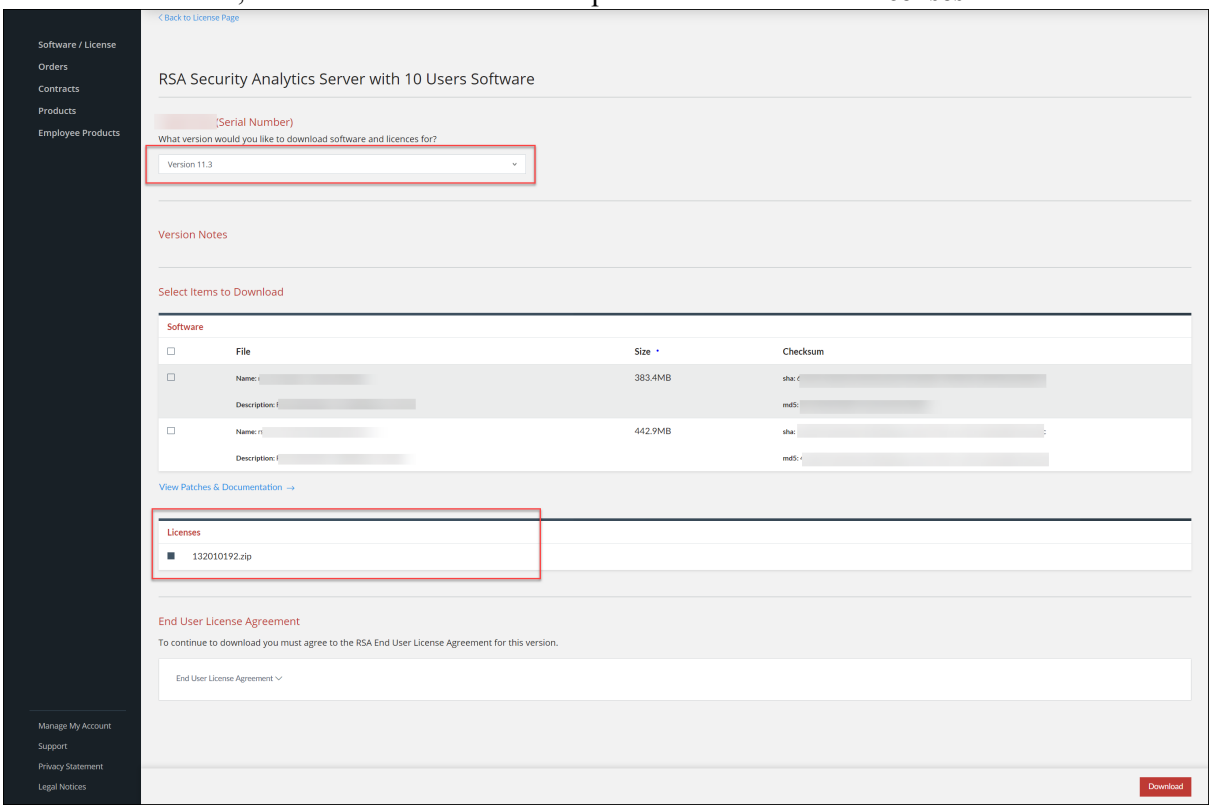
In the NetWitness entitlement process, you need to register the NetWitness Server and map the entitlements to the Local License Server (LLS). There are two methods of synchronizing NetWitness with myRSA: online and offline.

Note: By default NetWitness is configured to synchronize with myRSA at regular intervals hence manual synchronization is not required.

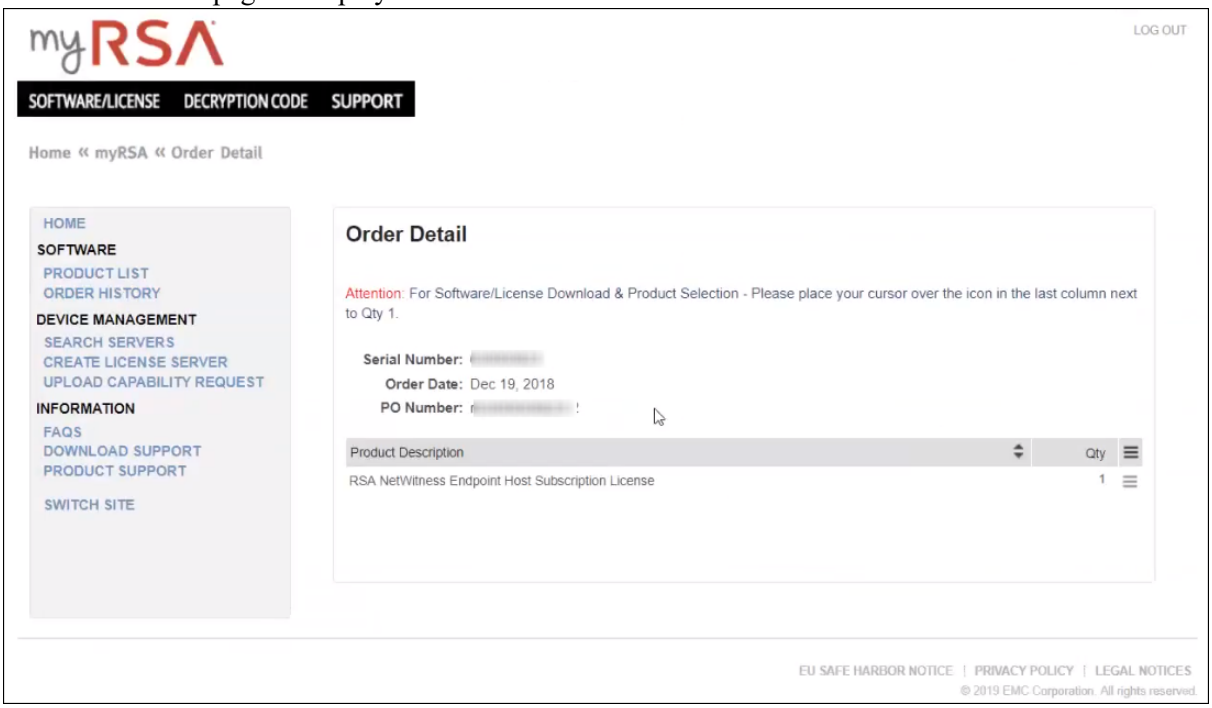
1. On the Sofware/License page, select the Order Location from the drop-down menu. The list of products, sales orders, and purchase orders are filtered and displayed.



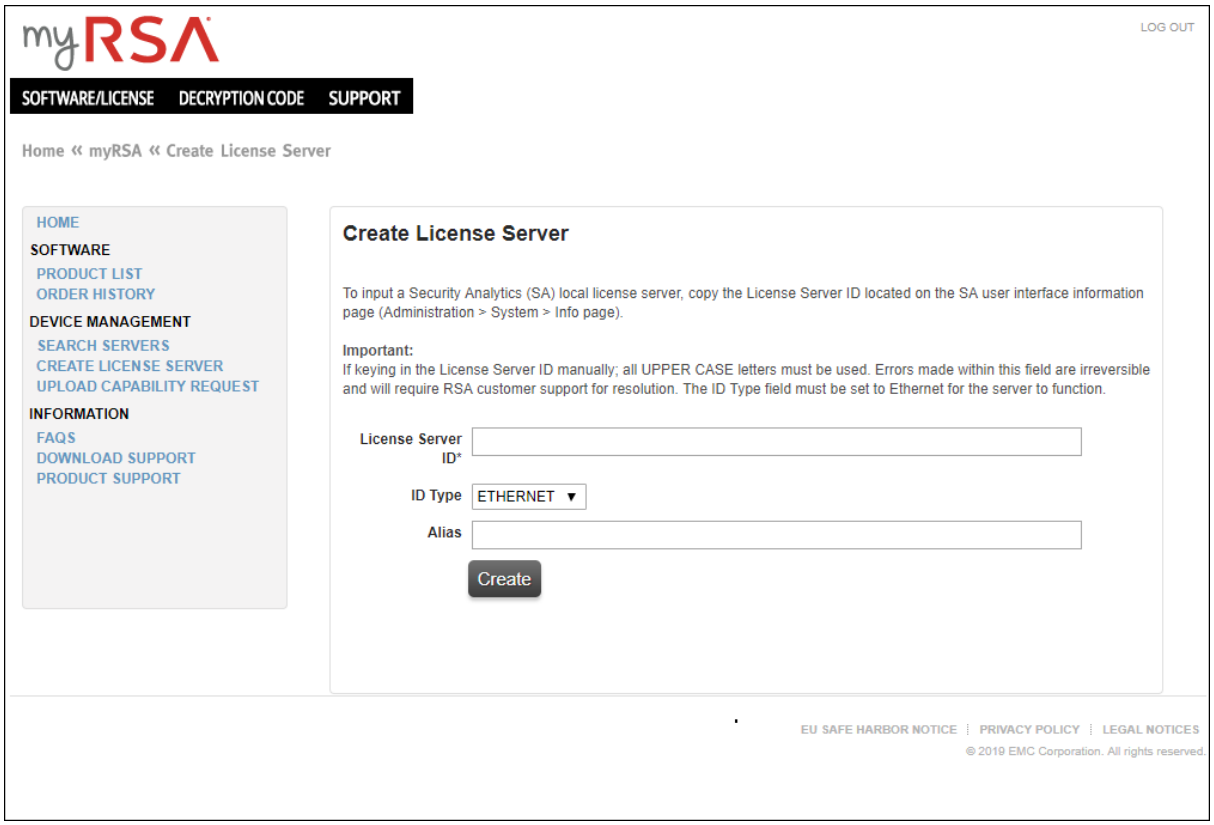
2. Click on a line item, select a version from the drop-down and select the **Licenses** checkbox.



3. Click **Download**.
The Order Detail page is displayed.

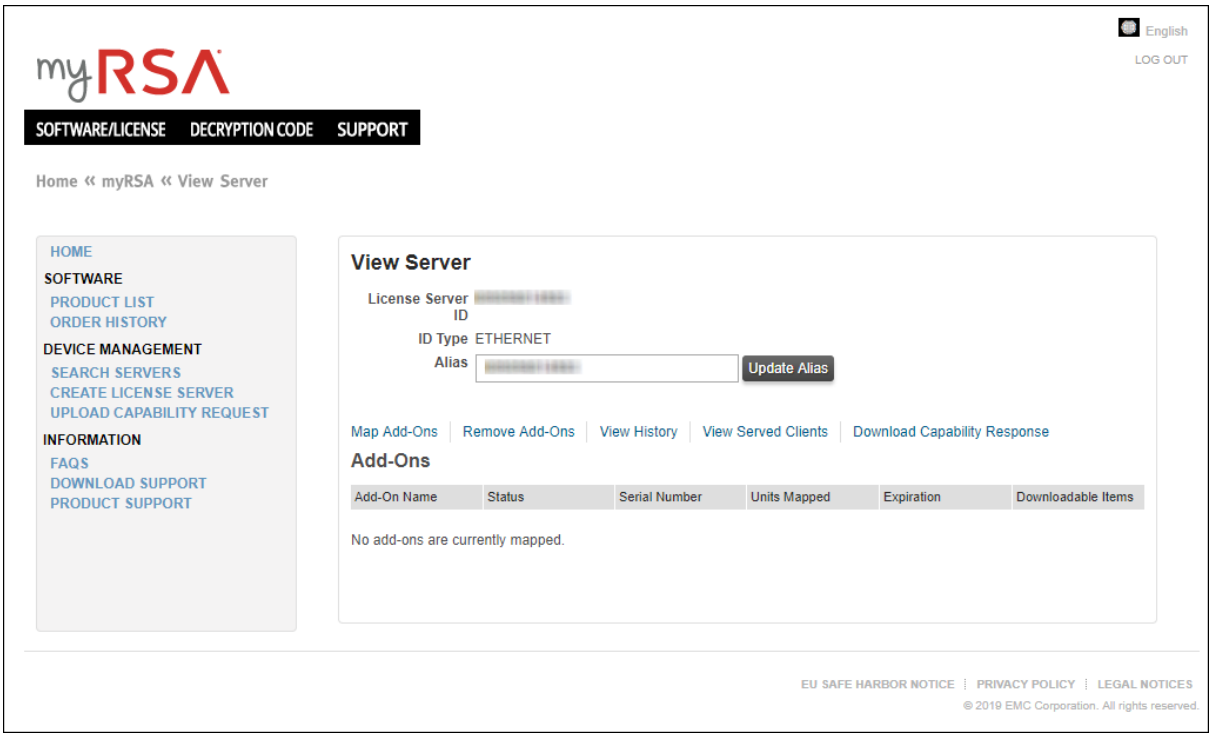


4. Click **Create License Server**.



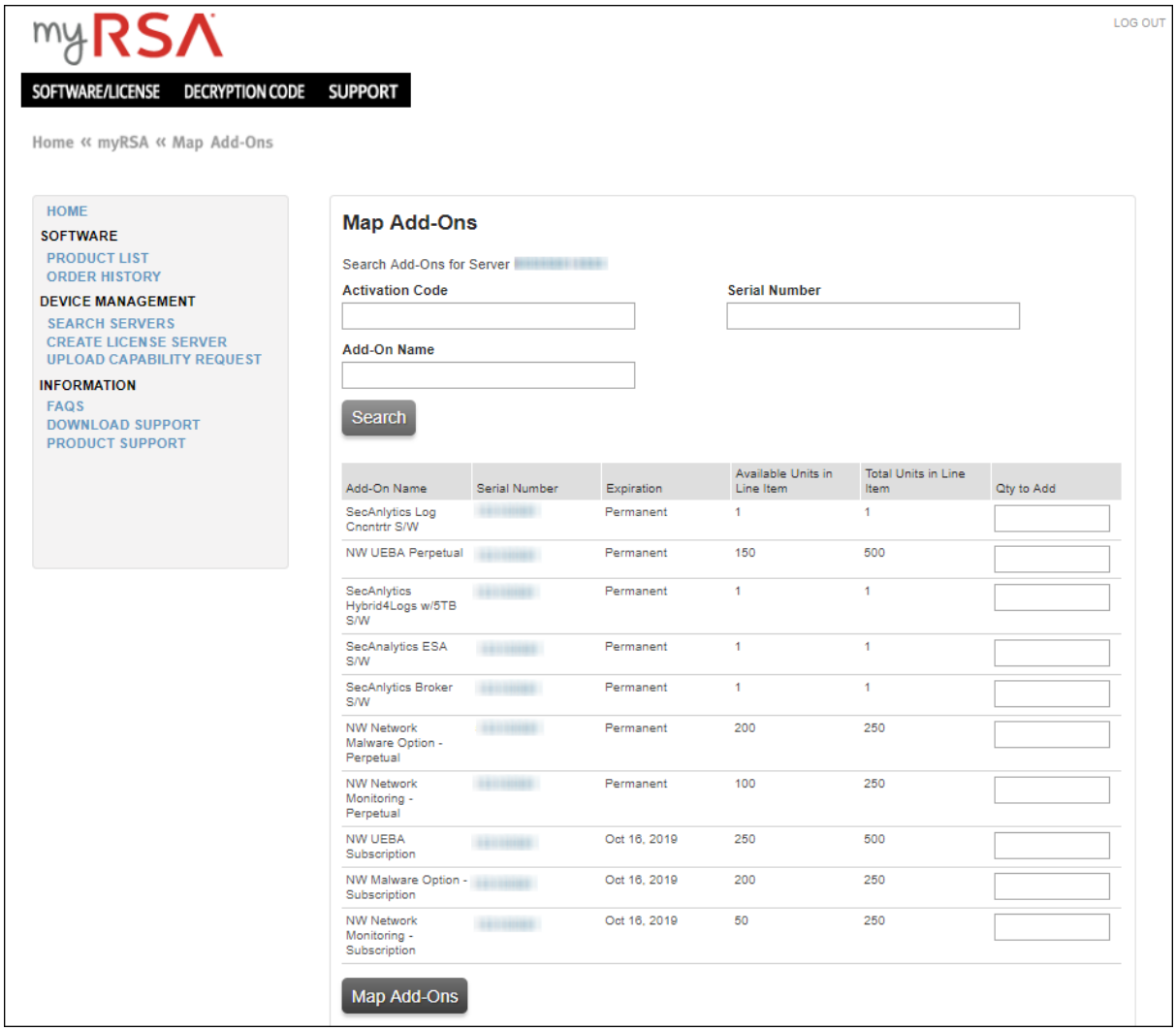
5. Complete the following fields:
   - Copy or enter (in uppercase letters) the License Server ID in the License Server ID field.
   - In the **ID Type** drop-down, select **ETHERNET** (the default value).
   - In the **Type** drop-down, select **Ethernet** (the default value).
   - (Optional) In the **Alias** field, type an alias to your Appliance ID.
6. Click **Create**.

   The View Server page is displayed.



7. Click Map Add-Ons.

   The Map Add-Ons page is displayed.



8. After you have registered the license server and viewed the license details, you must map the entitlements. For more information, see Map Entitlements .

Note: By default NetWitness host is configured to synchronize with myRSA at regular intervals and also a designated nameserver (DNS). No action is required.

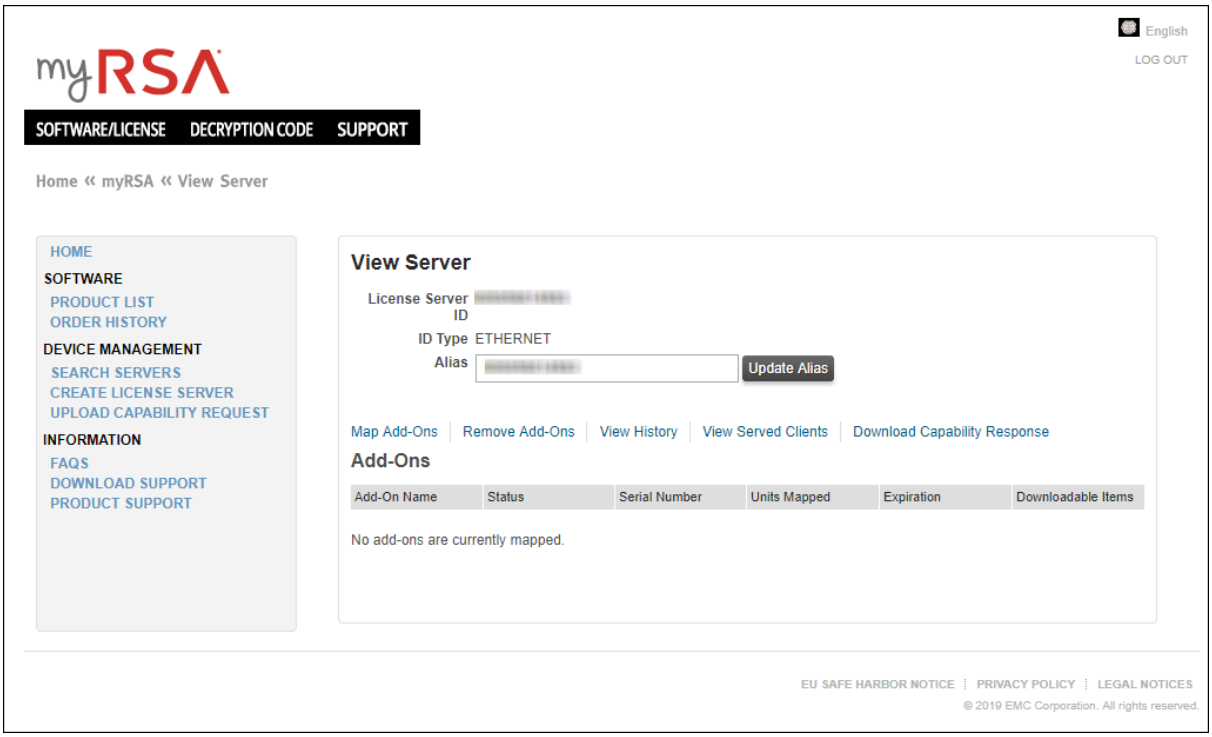
Note: In a multiple NetWitness deployment where the services are connected to both primary and secondary NetWitness hosts and the services are licensed only with the primary NetWitness, a license expiry message is shown for the same services on the secondary NetWitness. You can ignore the message and continue using the product.

Map Entitlements

Mapping entitlements involves choosing the quantity of available entitlements to pull to the NetWitness Server during synchronization.

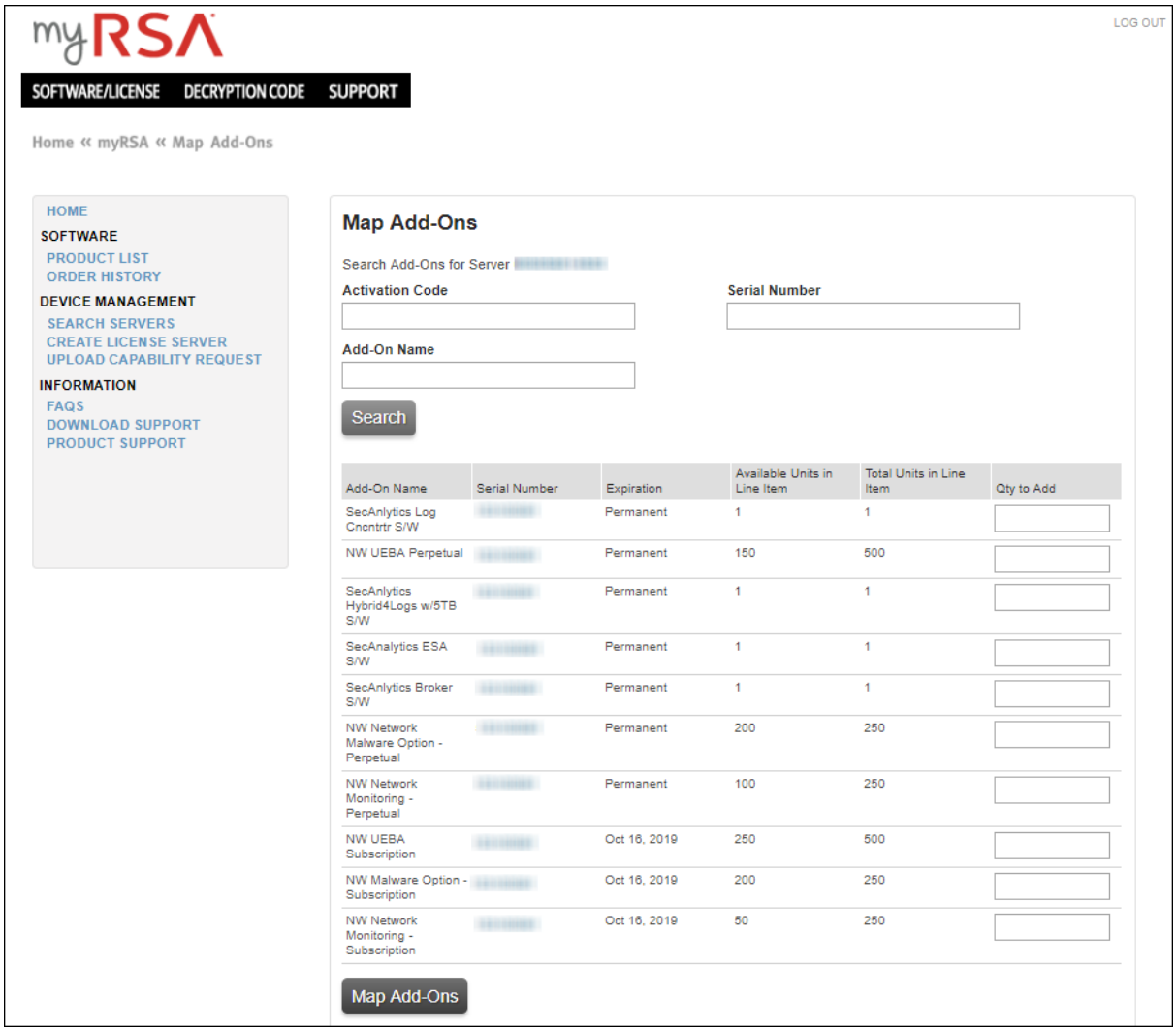
To map appliance entitlements to the server:

1. Log in to myRSA.
2. Click on the **SEARCH SERVERS** and then click on the License Server ID to view the entitled Server Details.



3. Click **Map Add-Ons**s.

   The Map Add-Ons page is displayed.



The Add-On table lists all entitlements that are available for your account. The table has a row for each NetWitness product entitlement, with the following information:

- **Add-On Name**: The name of the entitlement; for example, SMC Concentrator or SMC Decoder.
- **Serial Number**: The serial number associated with a product.
- **Expiration**: For licenses that are not permanent, the expiration information is displayed. The value in this field is a specific date (for example, Oct 6, 2019) or a time range (for example, 90 days). If the value is a time range, the expiration period begins when the add-on is mapped to a server.
- **Available Units in Line Item**: The quantity of entitlements currently available for that license. This quantity is the difference between the Total Units and the entitlements that have been mapped to a NetWitness Server for licensing.
- **Total Units in Line Item**: The total quantity of entitlements tied to a specific license.
- **Quantity to Add**: The number of entitlements for a specific license.

4. To designate the quantity of entitlements to map to the NetWitness Server from a license, type a quantity in the **Units to Configure** column.
5. Click **Map Add-Ons**.

   The View Server page displays a message indicating that the entitlements were successfully mapped to the NetWitness Server.

   Entitlements are now dedicated and set aside from an accounts pool. The message **License Not Generated** is displayed in the **Status** column for each entitlement. The entitlements are not yet full attached to the license server ID until the **Download Capability Response** link is clicked. Once done, a bin file is downloaded and on a page refresh the **Status** column will change to **License Generated**. At this point the license is fully attached to the license server ID and ready for use by NetWitness. The bin file that was downloaded can be manually applied to the NetWitness UI or the user can wait until the License Server checks in to pull the newly applied license to the NetWitness UI. If manually applying the bin file, it will expire within 48 hours of being created. If it expires before applying, simply click the **Download Capability Response** link for a new file.
6. (Optional) If you want to add more entitlements, use the **Map Add-Ons** option.
7. (Optional) If you want to remove entitlements, use the **Remove Add-Ons** option.

Now you can synchronize and pull down the mapped entitlements to the NetWitness Server

View Current Licenses

After you have completed the license process, you can view the current licensing status in the NetWitness UI.

Each NetWitness Server is a license server providing capabilities to entitle services connected to it. To make entitlements available for licensing services, the entitlements must be mapped to the Local License Server (LLS) on the NetWitness Server.

Note: If licensing a hybrid system, which has a Concentrator and Decoder on the same appliance, each component must be licensed separately.

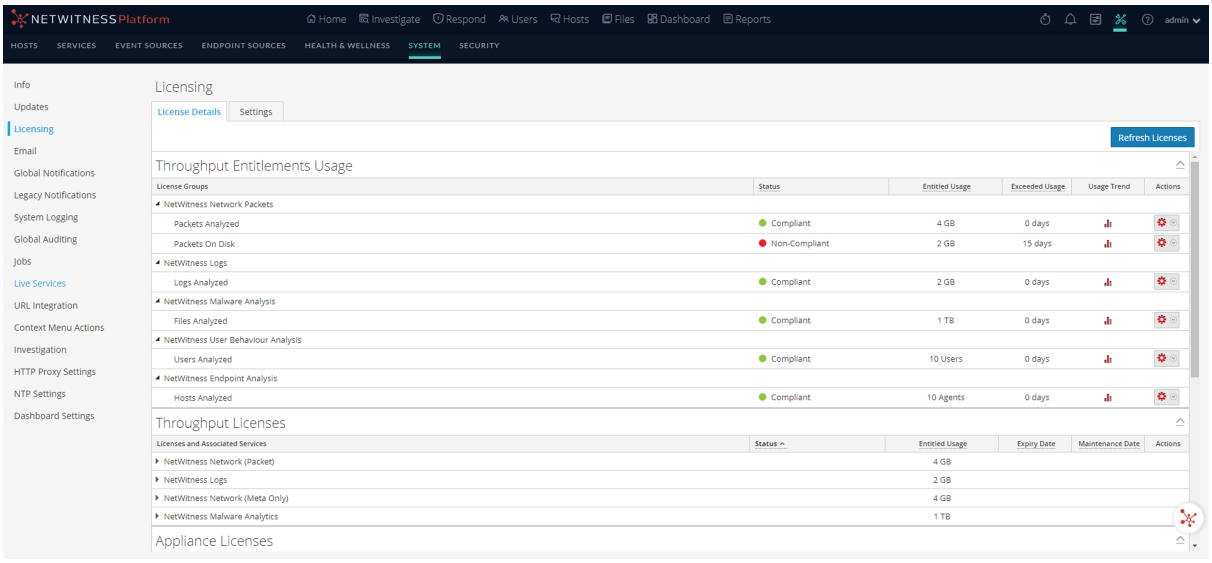
View and Manage Licenses

In NetWitness, you can view and manage available licenses.

To view the licenses that are available on this instance of NetWitness:

1. Go to **(Admin) > System.**
2. In the options panel, select **Licensing**.

   The **License Details** tab is displayed.



Each license is listed in the grid by license type. Information includes the status of the license indicated using color-coded circles and the related information.

Register the Server (Offline Capability Request)

NetWitness manages licensing through a Local License Server (LLS). Each client appliance is shipped with an installed LLS. This topic provides instructions for offline synchronization of the Local License Server (LLS) with the online repository. For more information on the functional description of the LLS, see Entitlement Capability Implementation.

If you are unable to register the NetWitness Server online, you can download an offline capability request in NetWitness and upload that binary request to the myRSA Portal. If the NetWitness Server is not connected to the Internet, you can perform offline synchronization of entitlements through the View Server page in myRSA.

Prerequisites

Before implementing the NetWitness Platform entitlements capability offline, ensure the following

- The NetWitness Server is registered to myRSA (https://my.rsa.com/) and entitlements are mapped. Internet access is not required for offline synchronization.
- An Offline Capability Request has been downloaded from the NetWitness UI to be uploaded to myRSA.
- An Offline Response has been uploaded to NetWitness that was received from myRSA within 24 hours.

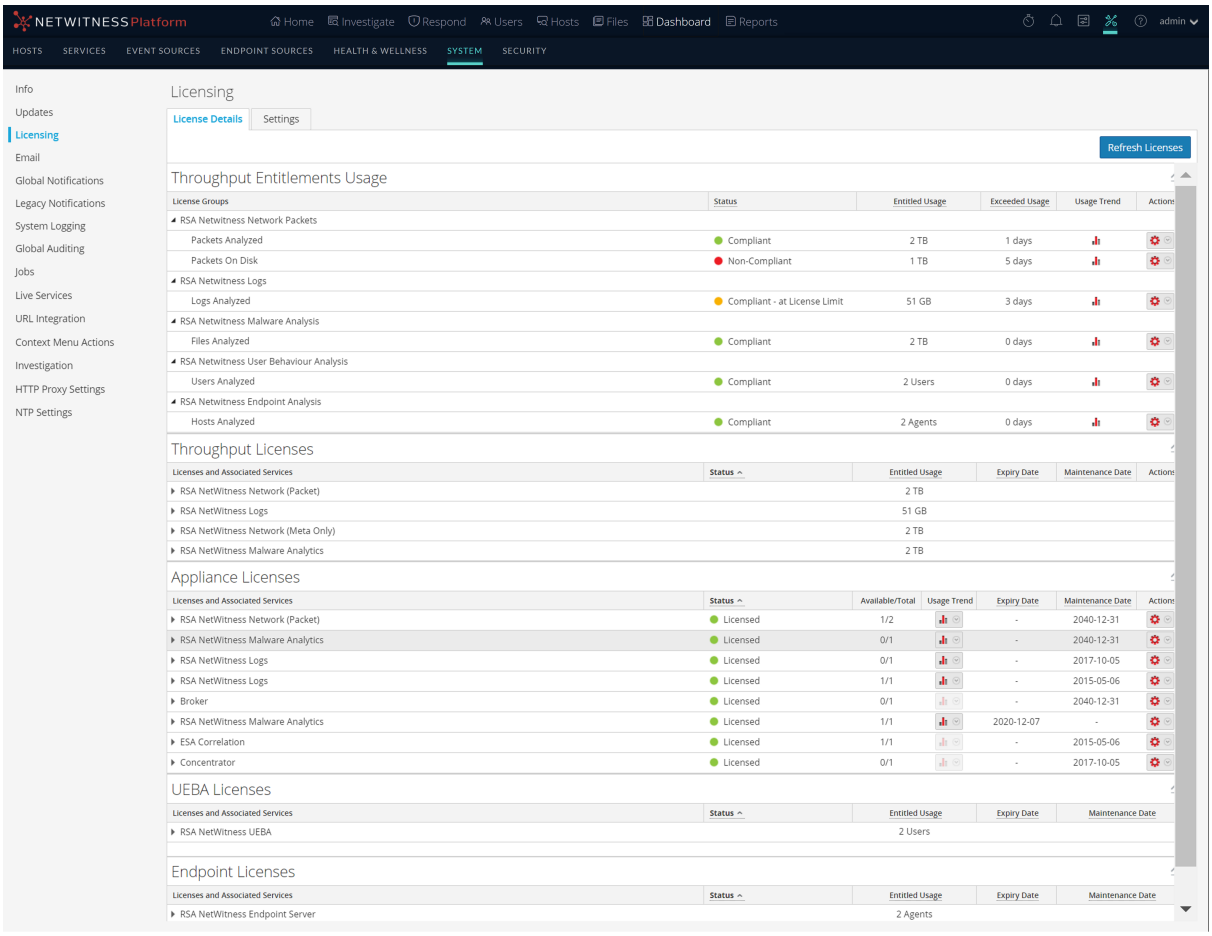
Here is a workflow that describes how to use the offline capability to acquire the licenses from myRSA and view them.

Download an Offline Request for Submission to myRSA

To register the server using an offline capability request:

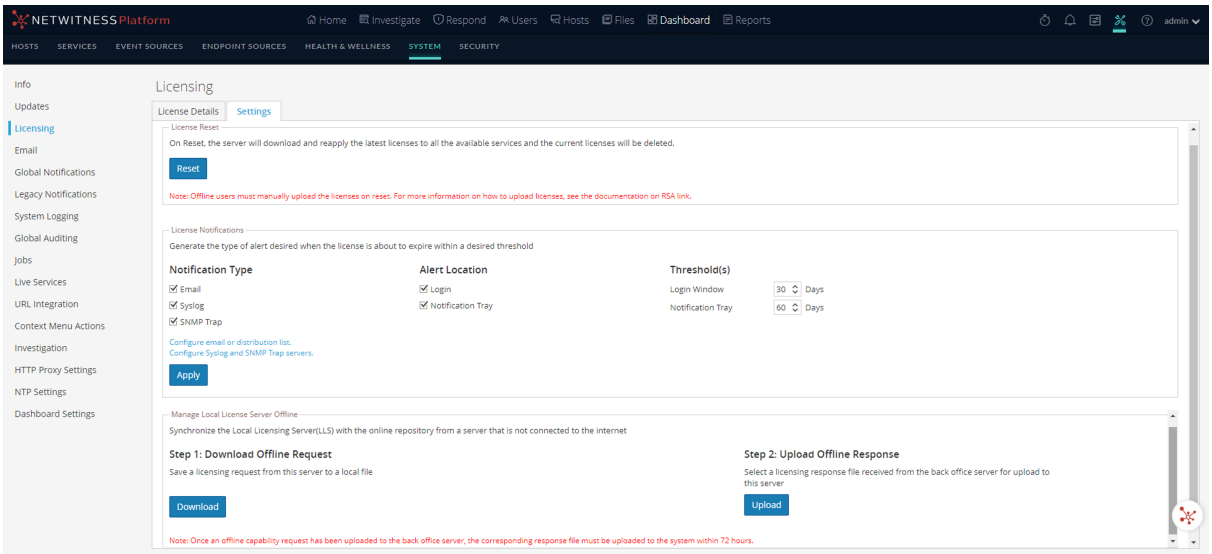
1. Go to **(Admin) > System**.
2. Click **Licensing**.

   The License Details page is displayed.



3. Select the **Settings** tab.

   The Settings page is displayed.

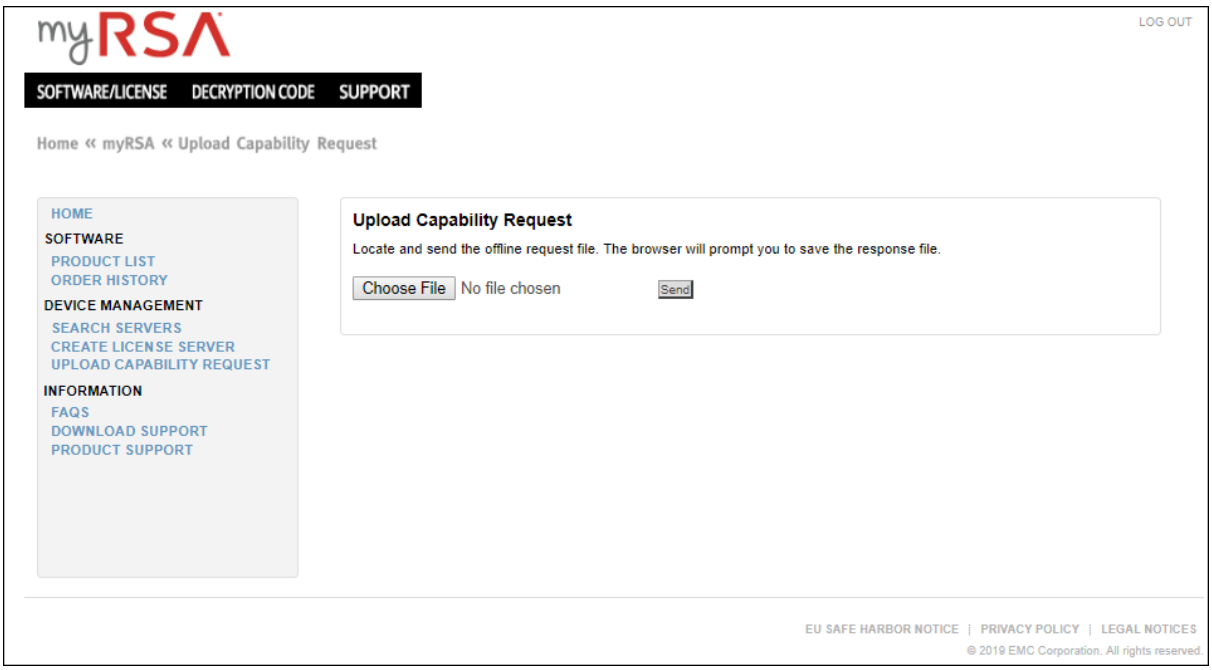


4. In the **Step 1. Download Offline Request** panel, click **Download**.
   A file called **OfflineCapabilityRequest.bin** is downloaded to the local system.

5. Login to the myRSA Portal at https://my.rsa.com/ with your user credentials.
6. Click on a service which needs to be licensed.

   Under **Device Management**, click **Upload Capability Request**.

   The **Upload Capability Request** dialog is displayed.



7. Click **Choose File** and browse the local file system to find the file downloaded from the NetWitness Server. Select **OfflineCapabilityRequest.bin**.

   The filename is displayed next to the **Choose File** button.

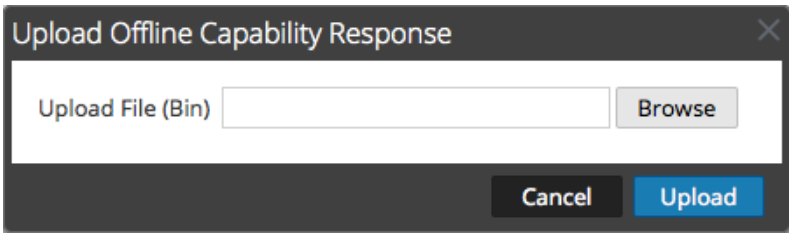
8. Click **Send**.
   The license data in a .bin file format is downloaded. The .bin file contains the data you entered as well as information about any entitlements that have been added to the NetWitness Server. If the server has just been added, there are no entries under **Add-Ons**. The server is registered and you can now map entitlements as described in the following sections.
9. After you download the .bin file from myRSA, login to NetWitness UI to upload the .bin file on the Settings page. For more information, see Upload an Offline Capability Response to NetWitness Platform.

Upload an Offline Capability Response to NetWitness Platform

If the NetWitness Server is not connected to the Internet, you can perform offline synchronization of entitlements through the View Server page in myRSA. To upload an offline capability response (**response.bin**) file saved to the local file system from myRSA:

1. Follow the steps 1 to 3 mentioned in the Download a Capability Request for Submission to myRSA procedure.
2. Login to the NetWitness user interface.
3. Go to **(Admin) > System** > **Licensing** > **Settings** tab.
4. In the **Upload Offline Response** section, click **Upload Response**.

   A dialog to upload the file is displayed.



5. Browse and select the **response.bin** file so that it is displayed in the Upload File (bin) field.
6. Click **Upload**.

   The entitlements are uploaded to NetWitness and the licenses added to the grid in the **Licensing Details** tab. They are available for licensing appliances.

   After you have uploaded the entitlements, you can verify the synchronization by performing any one of the following:

   - To view results in NetWitness, go to **(Admin) > System**>**Licensing** > **Licensing Details** tab. The individual product entitlements that have been pulled down to NetWitness are displayed in the **Available/Total** column.
   - Within the myRSA interface, you can see the status for entitlements changed to **In Sync**.

Refresh Licenses

When a new license is added, to map the view with the new license, click **Refresh Licenses.**

Refreshing your licenses performs the following behind-the-scenes tasks:

- Restarts the LLS server to ensure the latest licenses are pulled down from the central Flexera server.
- Associates any unlicensed service with a valid license (if available).
- Replaces expired or Out-of-the-Box license with valid licenses (if available).

License Types

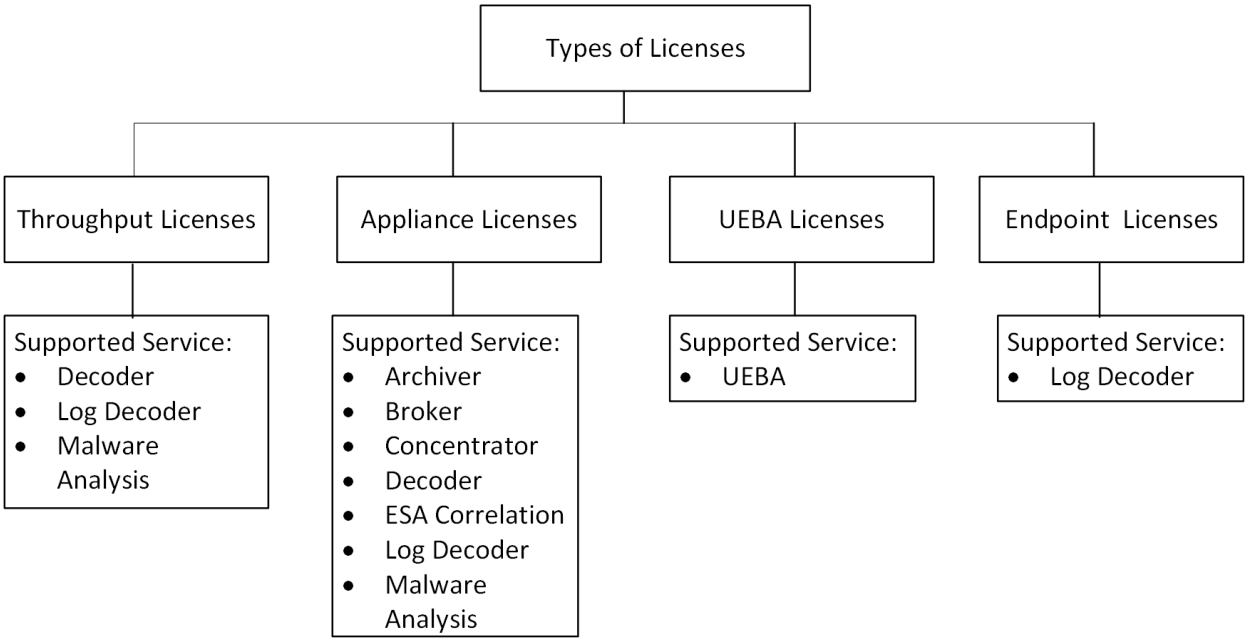
After you have installed the NetWitness software and the required services, you need to acquire the relevant licenses for the each of the services or a group of services based on your requirements. NetWitnessentitlement uses a trust-based licensing model. Appliances continue to function as usual even when the license is out-of-compliance.

Choosing a License Type

The type of license you choose is based on your network requirements. The following types of licenses are available in NetWitness:

- Throughput License
- Appliance License
- UEBA (User and Entity Behavior Analytics)
- Endpoint License

Here is a chart, followed by a description of each license type available for the NetWitness Platform products and services.



Throughput Licenses

Throughput license are based on the amount of data used per day for logs (SIEM), or network (packets) or malware.

The throughput per day is measured in Gigabytes per day for logs, and in Terabytes per day for packets. The total amount of throughput is selected based on the total amount of throughput per day that is being licensed across your entire enterprise deployment of NetWitness Platform. This license is measured as follows:

Service	Unit of Measurement	Increments	License Duration
Network Decoder	Terabytes (TB) per day	1 TB	Subscription or perpetual
Log Decoder	Gigabytes (GB) per day	50 GB	Subscription or perpetual
Malware	Terabytes (TB) per day of Files Analyzed by Malware Analysis	1 TB	Subscription or perpetual

Note: The NetWitness Platform provides Network Meta-Only license in addition to the Network Full Packet license.

Network Full Packet License captures, analyzes, and stores packet payloads and metadata and allows users to retain the packet payload for analysis or for session reconstruction. Network Full Packet License measures the bytes analyzed and the bytes written to the disk for Network Packets.

Network Meta-Only License captures and analyzes packet payloads and discards the packet payload data after analysis. Using this license, NetWitness Platform can be deployed in an environment where full packet capture is not required. This helps to optimally manage the storage space, and easily detect threats without the need to retain the full payload of the sessions. Network Meta-Only License measures the bytes analyzed for Network Packets and can be used with or without the Network Full Packet License.

When customers have both - Network Meta-Only License and Network Full Packet Licenses, the entitlement is aggregated and measured against the bytes analyzed for Network Packets. However, the entitlement for bytes written to disk for Network Packets will continue to be measured against the Network Full Packet Licenses. The following table is an example of how the license is used and analyzed.

Available Licenses	Network Full Packet License	Network Meta-Only License	Network Packet Bytes Analyzed	Network Packet Bytes Written to Disk
10TB of Network Full Packet	10TB	0TB	10TB	10TB
10TB of Network Meta-Only	0TB	10TB	10TB	0TB
10TB of Network Full Packet 5TB of Network Meta-Only	10TB	5TB	15TB	10TB
5TB of Network Full Packet 10TB of Network Meta-Only	5TB	10TB	15TB	5TB

For more information on the status of your license, usage and out of compliance licenses, see About Out-of-Compliance Banners.

Appliance Licenses

NetWitness Platform supports the Appliance license, which is applicable to all hosts that require a license. Other services do not require a license. Appliance licenses are measured as follows:

- Services are licensed automatically if you have a valid appliance based license for a specific service to be licensed.
- Appliance licenses can be purchased as a perpetual license that does not expire and will have a maintenance contract. If you purchase a subscription license, then it will expire if you do not renew the contract.

User and Entity Behavior Analytics Licenses

NetWitness Platform supports the User and Entity Behavior Analytics License (UEBA). UEBA monitors the number of active users from the previous day and sends it to the licensing server. The entitlement is measured for logs and endpoint events for the number of active users and is checked against a user id. If a threshold is identified in a calendar month an appropriate banner is displayed. For more information on banners, see About Out-of-Compliance Banners.

Note: There is no change in the license for multiple UEBA servers, as the license is based on the number of users monitored by UEBA.

Endpoint Licenses

Endpoint license are entitled based on the number of active agents deployed.

There are two types of agents:

- **Advanced Agents**: The license for these agents is based on the number of advanced agents in your deployment. A 90-days trail license period is provided. After the 90-days trial period, a zero MB and zero Agent license is applied to the Log Decoder service and Endpoint service in the NetWitness Endpoint Log Hybrid. Once an Endpoint license is applied any Archivers, Brokers, Concentrators, and ESA are automatically licensed as a result. An usage exceeded banner is displayed when the license goes out-of-compliance in the following scenarios:

  a. If the number of active agents exceeds the number of licensed agents

  b. If the Endpoint Subscription is about to expire in near future or has already expired.

  For example, if you have purchased a license for 50,000 agents and if the number of agents exceeds more than 50,000, the banner is displayed.

  Or, if you have purchased a license for 50k agents but have mapped the entitlements for only 10k agents on myRSA, an out-of-compliance banner is displayed when your usage exceeds these 10k active agents.

- **Insights Agents** - There is no license required for these agents if they are used to collect only endpoint data.
- **Log Collection with Endpoint Agents** - All Endpoint agents (Advanced or Insights) can forward Windows Log data only to a licensed Log Decoder (or Hybrid). Windows Logs sent to a licensed Log Decoder (or Hybrid) will count against either the applied Throughput or Appliance license. Logs may be retained in the NetWitness Endpoint Log Hybrid as long as a Log (SIEM) Throughput license with available capacity is available. In either case, a license for Logs is required, irrespective of the Insights or Advanced agent.

Out-of-the-Box Trial License

NetWitness Platform comes with an OOTB 90-days trial license.

For Endpoint metered license, you will be provided with 0MB Log Decoder license. The 0MB license from the Log Decoder will be utilized after the 90-days trial period is complete. If you are still within the 90-days trial period and if you have an Endpoint Metered license, then the Log Decoder uses the remaining trial license. The Log Decoder will apply the 0MB license only after the trial license completed.

Configure License Support For Multiple NetWitness Servers

If you have multiple NetWitness servers deployed in your environment, and require license support, you must configure multiple Mac addresses.

To configure online:

1. Log in to the NetWitness Server console.
2. Navigate to /opt/netwitness/flexnetls.
3. Edit the local-configuration.yaml file and add the mac address of the back up or secondary host.
   For example, `backup-hostid: 685B3596A5F3` or `backup-hostid: "685B3596A5F3:785B3596A5F3"`.
4. Restart `systemctl restart flexnetls-RSALM`.
5. Obtain the instance details from `wget http://localhost:3333/api/1.0/instances` and set the `"failOverRole"` to `MAIN` to verify the failover.
   For example, `"failOverRole" : "MAIN"`.

To configure offline:

1. Perform the step 1 to step 6 from the online procedure .
2. Download the capability request from NetWitness UI.
3. Upload the request to FNO (myRSA).
4. Upload the response from FNO (myRSA) to the NetWitness UI.

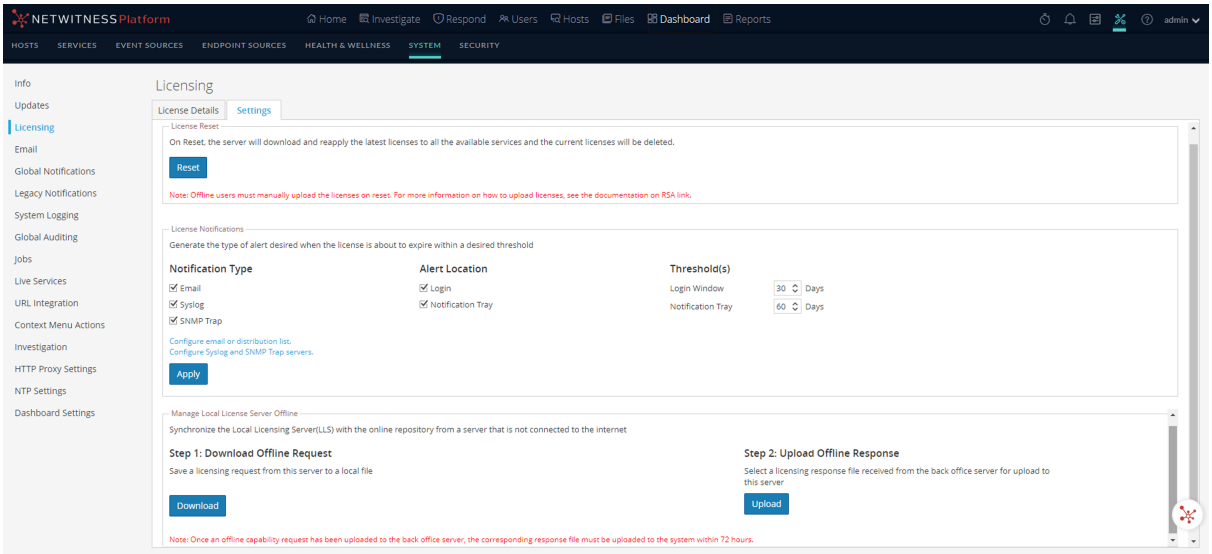
Configure License Notifications

This topic provides instructions for configuring notification settings for the Local License Server (LLS). If you wish to receive alerts about the approaching license expiration date, you can configure NetWitness to send notifications. You can receive notification by email, syslog and SNMP. You can also view the notification during system log on and in the Notification Tray. You can also specify the number of days before expiration as a threshold for notification.

Note: In the Analyst UI, the license notifications will not be displayed in the notification tray or login window when the license goes out of compliance or when the license expires. This is displayed only on the Admin UI.

To configure the notification:

1. Go to **(Admin) > System**.
2. Select **Licensing**.
3. Select the **Settings** tab.



4. Select each of the methods for NetWitness to use when sending a notification about the license status.
   a. To receive a notification at log on, select **Login** and specify the number of days before the license expires that you want to receive notification in the **Login Window Threshold** field.
   b. To receive a notification in the Notifications tray, select **Notification Tray** and specify the number of days before the license expires that you want to receive notification in the **Notification Tray Threshold** field.
   c. To receive an Email notification to a configured distribution list, select **Email** and select **Configure email or distribution list**. The Email panel is displayed in a separate tab, and you can

configure notifications in the Email Server Settings section. Refer to the *System Configuration Guide* for further details.

d. To receive syslog notifications, select **Syslog** and click **Configure Syslog and SNMP Trap servers**. The System Auditing panel opens in another tab and you can configure the system settings.

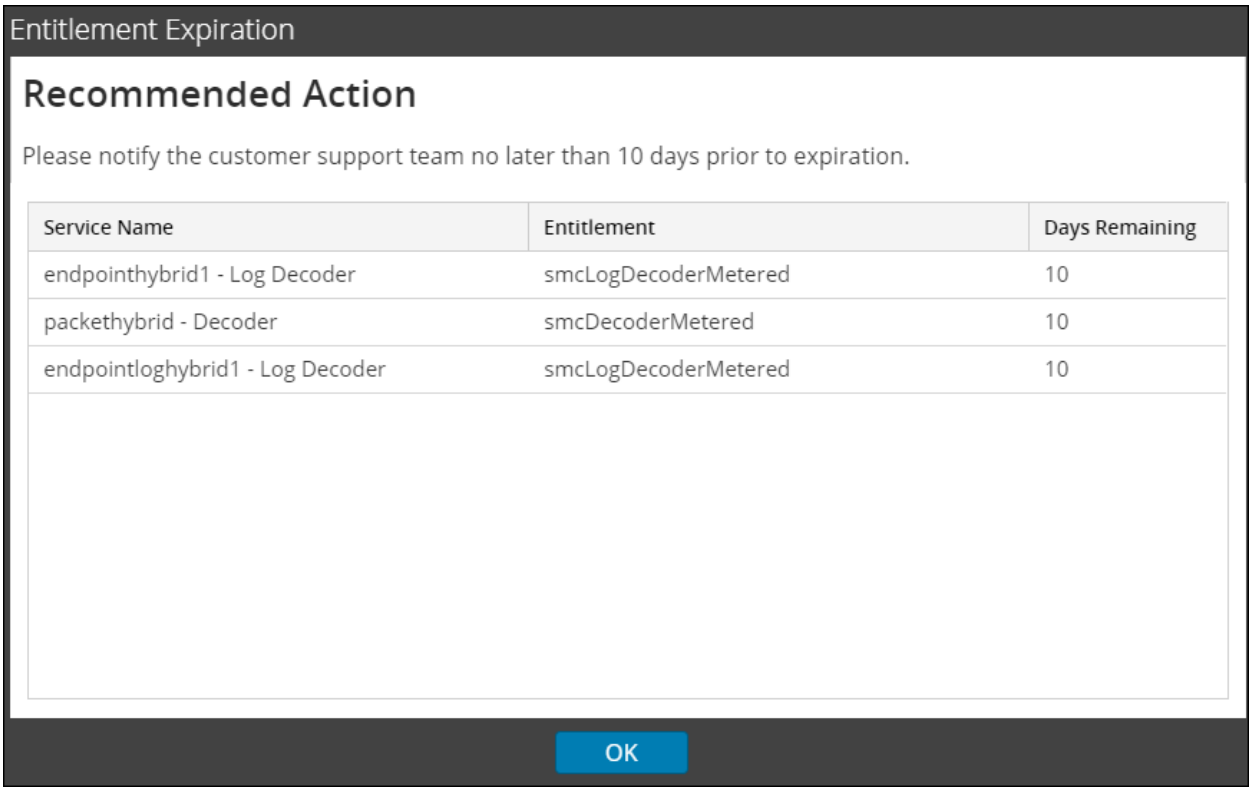
e. To receive notifications through SNMP Trap, select **SNMP Trap** and select **Configure Syslog and SNMP Trap servers.** The System Auditing panel opens in another tab and you can configure the SNMP auditing settings.

5. Click **Apply Notifications**.
   The settings are saved and go into effect immediately.

About Out-of-Compliance Banners

Banners let you know the status of your license and usage compliance.

When a license for a specific service is about to expire, an **Entitlement Expiration** message is displayed with the list of services about to expire.



After you log on, either a red or yellow banner may be displayed, based on the license issue:

- A red banner is displayed if your license has expired, or exceeded the allotted usage, or if the license has internal errors.

Note: A red banner cannot be dismissed and the license issue must be resolved.

- A yellow banner is displayed if the license is approaching expiration or the license is nearing the allotted usage. The banner can be dismissed by clicking the **Reject** button.

Here is an of example of how the license usage is calculated and a way that you can resolve the license issues:

- Contracted daily usage can be exceeded three times in a calendar month. The fourth spike puts the system in an out-of-compliance state. If you are able to keep your usage within compliance for seven consecutive days until the end of calendar month, the Out-of-Compliance Red banner disappears.

- For example, if the fourth spike occurs on November 23, 2019, the Grace Period ends on December 31, 2019 and the Out-of-Compliance Red banner disappears.
- The breach period starts immediately after Grace Period ends. However, if your deployment is in a breach state, you can bring the state back to normal by keeping the usage in a compliant state for seven consecutive days.

Note: Even when the Red banner is displayed, there is no loss of functionality, all NetWitness appliances continue to work with full functionality. All other functionality is included in the license (ESA, storage, and so on).

Troubleshoot Licensing

This topic provides information about possible issues that NetWitness users may encounter when setting up licensing in NetWitness. You can look up explanations of issues and their solutions. NetWitness notifies users of issues using the popup notifications and the system log as described in the "Troubleshoot NetWitness" topic in the *System Maintenance Guide*.

Out-of-Compliance Banners

Problem	Possible Causes	Solutions
Yellow and Red Out-of-Compliance Banners	• A service is not licensed. • A license has expired, or is due to expire within the next two weeks. • Usage exceeds entitled limit. • Usage is approaching entitled limit.	• Contact Customer Support to buy or renew your license. • Reduce usage or • Adjust contracted usage amount

Common Log and Configuration Files

When troubleshooting licensing, the following files contain information that may help to diagnose the problem. Specific conditions for searching the files are described in the troubleshooting tables.

On the NetWitness Server, run `wget` for the following files after you ssh onto the NetWitness Server:

- `http://localhost:3333/api/1.0/features`
- `http://localhost:3333/api/1.0/instances`
- `http://localhost:3333//api/1.0/hostids`
- `http://localhost:3333/api/1.0/capability_request`

NetWitness Server Problems

This table lists possible problems with the NetWitness Server errors that can affect entitlements.

Problem	Possible Causes	Solutions
Some features have been mapped in the central Flexera server, but the NetWitness Server does not display them.	Ensure that the NetWitness Server is connected to the Internet.	To resolve the error execute a License Refresh as follows: 1. GSo to **(Admin) > Services > Licensing.** 2. In the License Details tab, click **Refresh Licenses**. **Note:** If the NetWitness Server is not connected to the Internet, try to synchronize offline. For more information, see Register the Server (Offline Capability Request)
NetWitness Platform Licensing page not showing any license information although there are services available.	Ensure that you have the required entitlements pulled down from the Central Flexera server.	To resolve the error execute a License Refresh as follows: 1. Go to **(Admin) > Services > Licensing**. 2. In the License Details tab, click **Refresh Licenses**.

Wrong License Mapping Issue

Problem	Possible Causes	Solution
Decoder license not available due to core appliances being removed from the NetWitness Server without releasing the license. Several core appliance licenses were not available for use.	Various possible causes.	Reset the license on NetWitness Server.

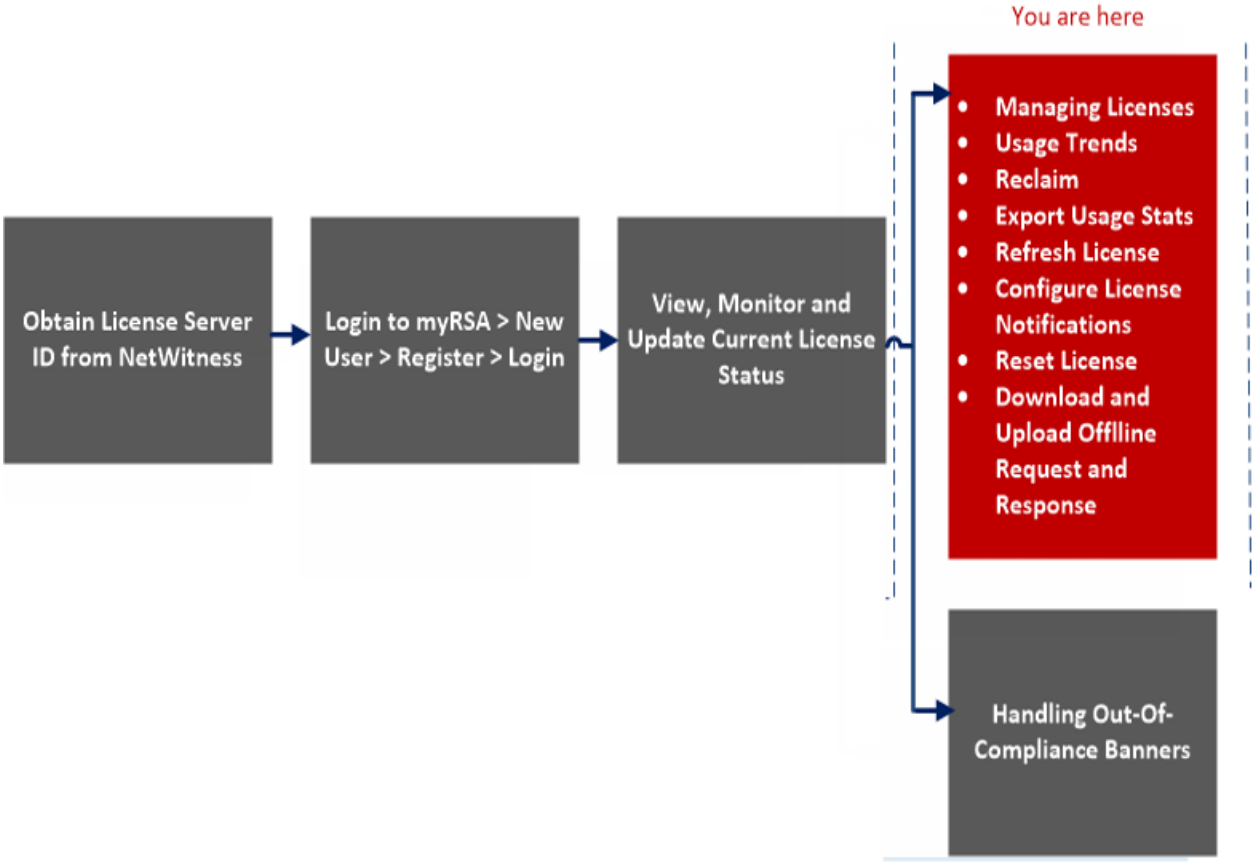
Problem	Possible Causes	Solution
Archiver DACs are not mapped to the license server with all other appliances' licenses.	Various possible causes.	1. Enter **1** in Quantity field to add for each license. 2. Select **Map Add-ons** at the bottom of the screen. 3. Click **Download Capability Request** and upload license to the Offline Capability Request in the User Interface under the **License** tab.
Two new appliances were installed: one Log Hybrid and one Log Archiver. Able to license the Log Hybrid, but the following error occurred when attempting to license the Archiver: "There is an issue with registering your product, please contact NetWitness Customer Support." Also, one of the Concentrators showed as a Trial license, and a separate Log Decoder showed as a Trial license when they should be licensed.	The new entitlements are not mapped to the license server.	Map add-ons to myRSA and upload the `.bin` file into the NetWitness User Interface.

License Details

This topic introduces the features of the System Licensing panel. NetWitness manages licensing through a Local License Server (LLS). Each client appliance is shipped with an installed LLS.

Workflow

This workflow shows the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Obtain License Server ID from NetWitness Platform User Interface

Role	I want to...	Show me how...
Administrator	Synchronize NetWitness Server	Register the Server (Online Registration)
Administrator	Install product licenses from DLC	Access myRSA
Administrator	*Monitor and update current licenses.	View Current Licenses
Administrator	Configure licensing notifications.	Configure License Notifications
Administrator	View Out-of-Compliance banners	About Out-of-Compliance Banners

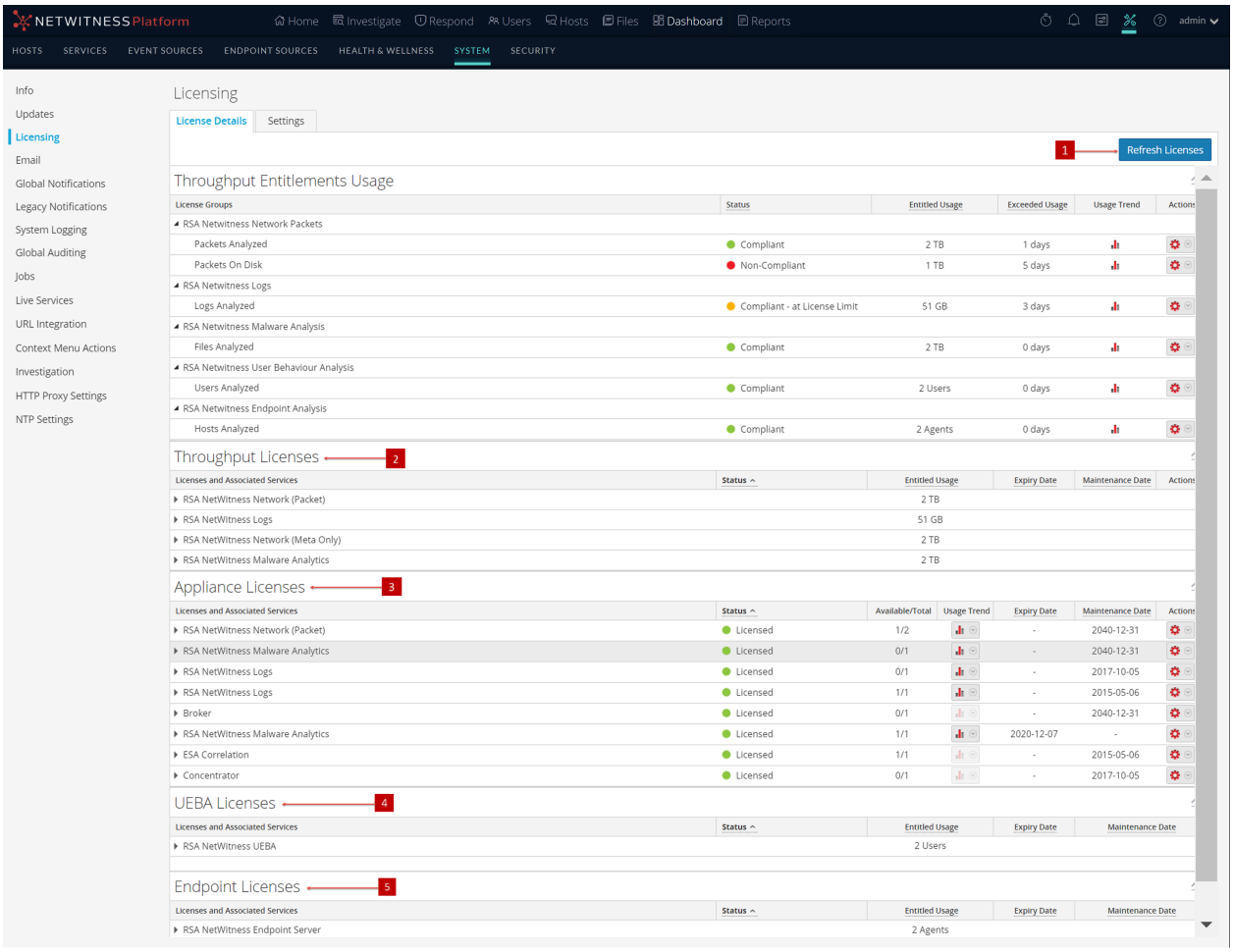
*You can perform this task here.

Related Topics

- Settings
- View and Export Usage Stats

Note: On initial start up, the usage shown in the Licensing page displays zero usage for the initial one hour.

Quick Look



The following table describes the features of the License Details tab.

1	**Refresh Licenses**:Refreshes and maps the new licenses.
2	Displays the following details of the Throughput license or licenses. • **License and Associated Service** - Displays the license and the services assigned to it. • **Status** - Displays the status of the license such as Expired License, Over Usage Limit, Near Usage Limit, and Within Usage limit. • **Entitled Usage** - Displays the entitled usage for aggregate as well as individual services . • **Exceeded Usage** - Displays the number of days the usage exceeded the entitled usage in the last 30 days for each individual service. • **Usage Trend** - Displays the trend of how the license usage has been for a period of time for aggregate as well as individual services. • **Expiry Date** - Displays the expiry date of the customer subscription contract. • **Maintenance Date** - Displays the maintenance expiration date for the permanent license or licenses and the date on which the license or licenses expire.

- **Actions** - Displays the Licensing Actions button that offers the following options:
  - **Export Usage Stats**: Exports license usage statistics for the selected service or license.
  - **Reassign to Another License**: Reassigns an extensively used Throughput license to another unused Throughput license. This is applicable only for Throughput and Appliance license.

3 Displays the following details of the Appliance license or licenses.

- **License and Associated Service** - Displays the license and the services assigned to it.
- **Status** - Displays the status of the license such as Expired License, Over Usage Limit, Near Usage Limit, and Within Usage limit.
- **Available/Total** - Displays the number of available license and the total number of licenses.
- **Usage Trend** - Displays the trend of how the license usage has been for a period of time for aggregate as well as individual services
- **Expiry Date** - Displays the renewal date of the customer subscription contract.
- **Maintenance Date** - Displays the maintenance expiration date for the permanent license or licenses and the date on which the license or licenses expire.
- **Actions** - Displays the Licensing Actions button that offers the following options:
  - **Export Usage Stats**: Exports license usage statistics for the selected service or license.
  - **Reassign to Another License**: Move the license from Appliance to Throughput license.
  - **Reclaim**: This option gets activated when any appliance service is down. When you click **Reclaim** the license becomes available in the pool of the specific license service. This is applicable only for Appliance license.

4 Displays the following details of UEBA license or licenses.

- **License and Associated Service** - Displays the license and the services assigned to it.
- **Status** - Displays the status of the license such as Expired License, Over Usage Limit, Near Usage Limit, and Within Usage limit.
- **Entitled Usage** - Displays the number of entitled users.
- **Actual Usage** - Displays the daily active users.
- **Exceeded Usage** - Displays the number of days the usage exceeded the entitled usage in the last 30 days for each individual service.
- **Usage Trend** - Displays the trend of how the license usage has been for a period of time for aggregate as well as individual services
- **Expiry Date** - Displays the renewal date of the customer subscription contract.
- **Maintenance Date** - Displays the maintenance expiration date for the permanent license or licenses and the date on which the license or licenses expire.
- **Actions** - Displays the Licensing Actions button that offers the following options:
  - **Sort Ascending**

- **Sort Descending**

5 Displays the following details of Endpoint license or licenses.

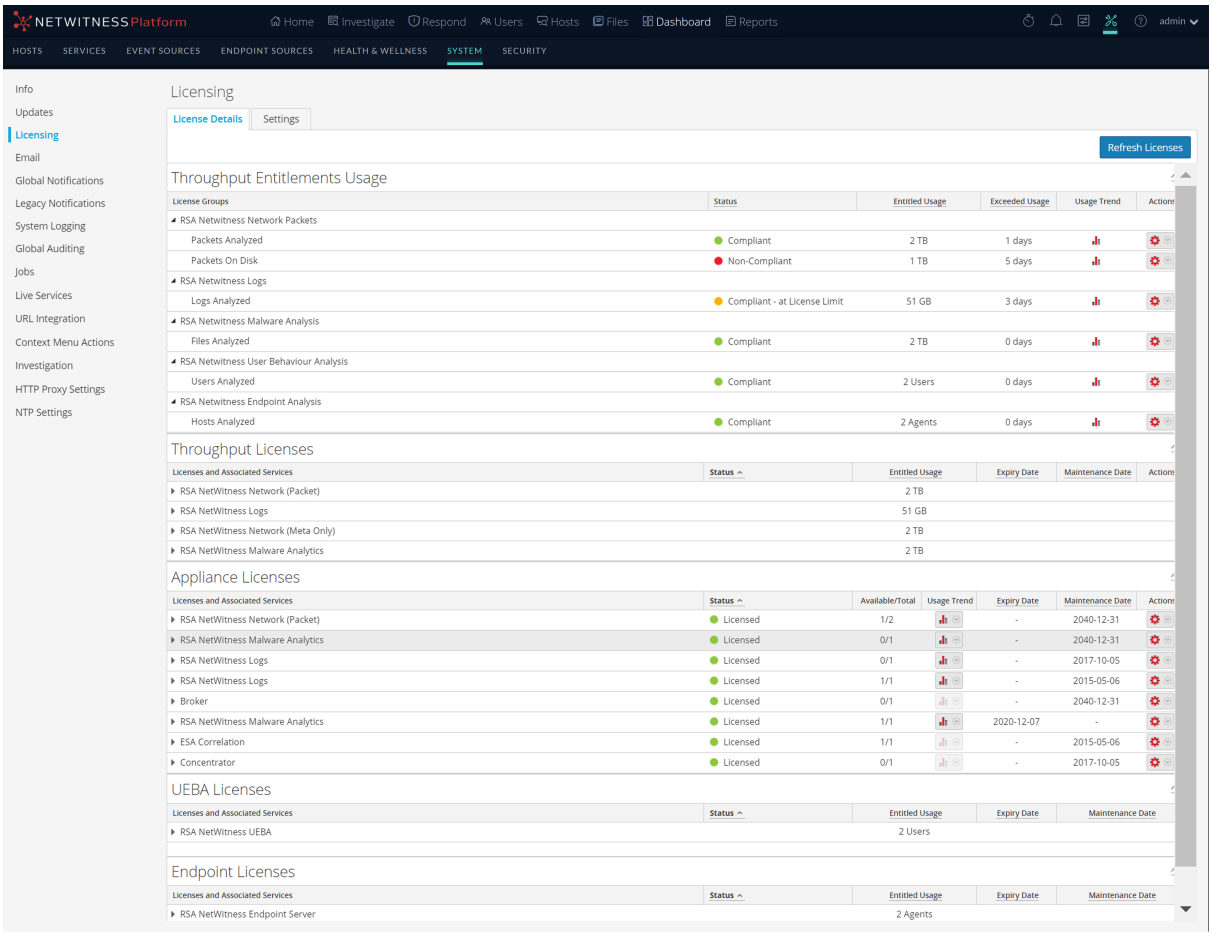
- **License and Associated Service** - Displays the license and the services assigned to it. For example, Endpoint Hybrid or Endpoint Log Hybrid.
- **Status** - Displays the status of the license such as Expired License, Over Usage Limit, Near Usage Limit, and Within Usage limit.
- **Entitled Usage** - Displays the users of the entitled agents .
- **Actual Usage** - Displays the number of daily active agents .
- **Exceeded Usage** - Displays the number of days on which the actual number of agents exceeded the entitled threshold.
- **Usage Trend** - Displays the trend of how the license usage has been for a period of time.
- **Expiry Date** - Displays the renewal date of the customer subscription contract.
- **Maintenance Date** - Displays the maintenance expiration date for the permanent license or licenses and the date on which the license or licenses expire.
- **Actions** - Displays the Licensing Actions button that offers the following options:
  - **Sort Ascending**
  - **Sort Descending**

Usage Trends

You can view the usage trend for aggregate licenses as well as individual licenses. The data is displayed for each day. When you click the usage trend icon, it opens a new window and displays the usage data as a chart. The user can use this data to analyze the license usage in the deployment.

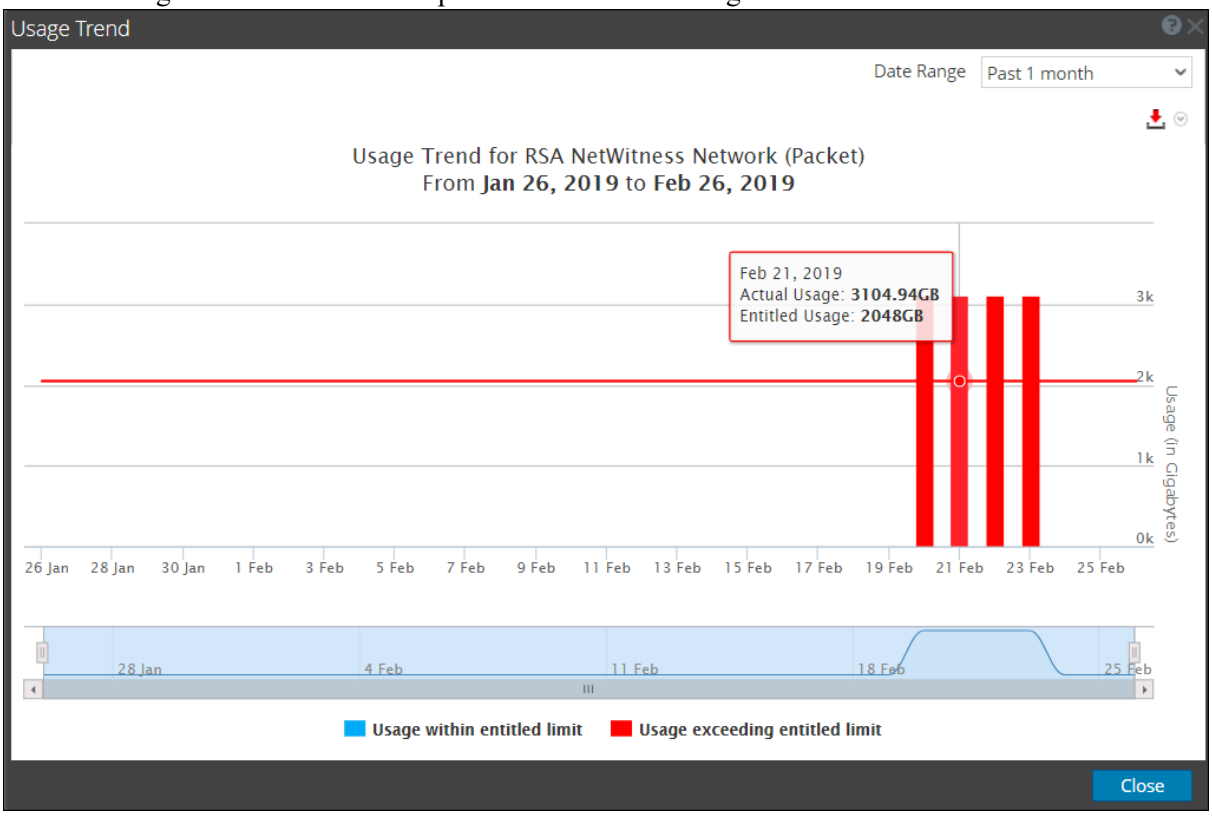
To access this view:

1. Go (Admin) > **System** and select **Licensing**.
   The Licensing page is displayed with the License Details tab opens.

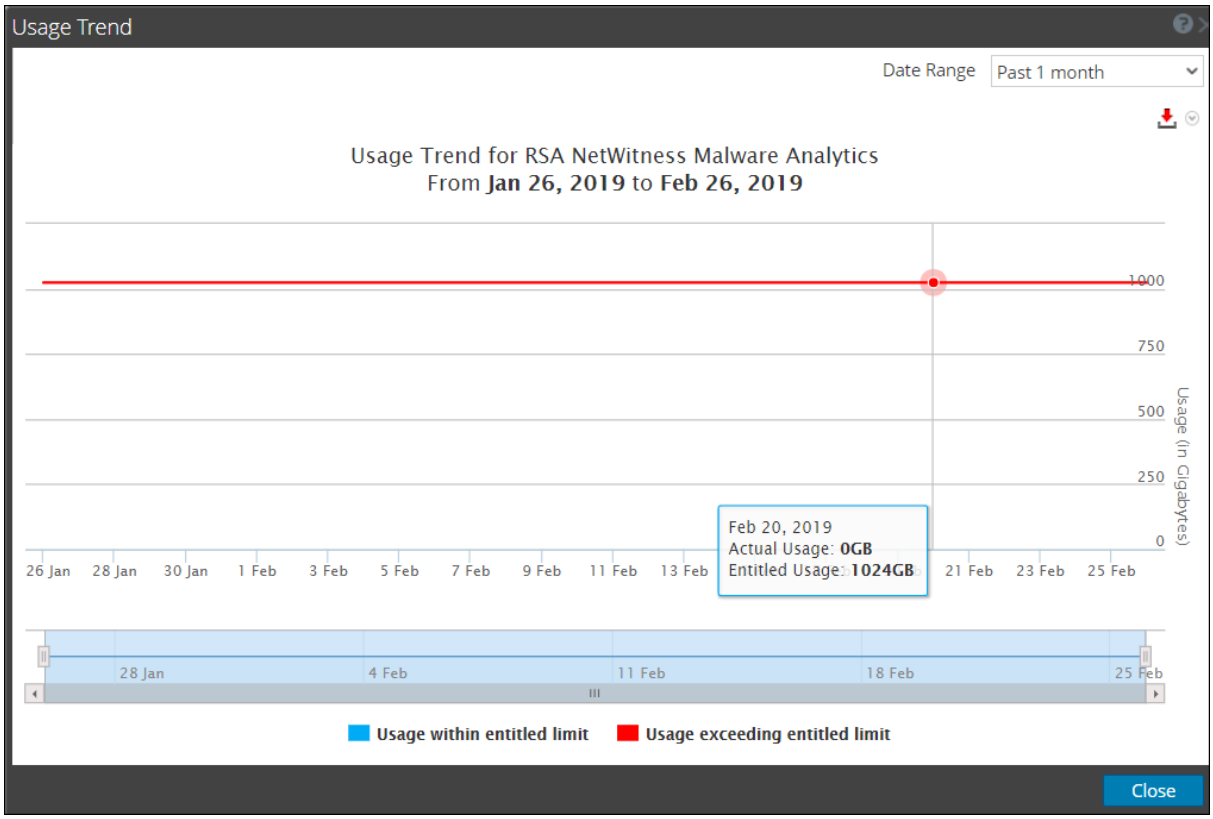


2. Select a service or license and click the icon under the Usage Trend column.
The Usage Trend window is displayed.

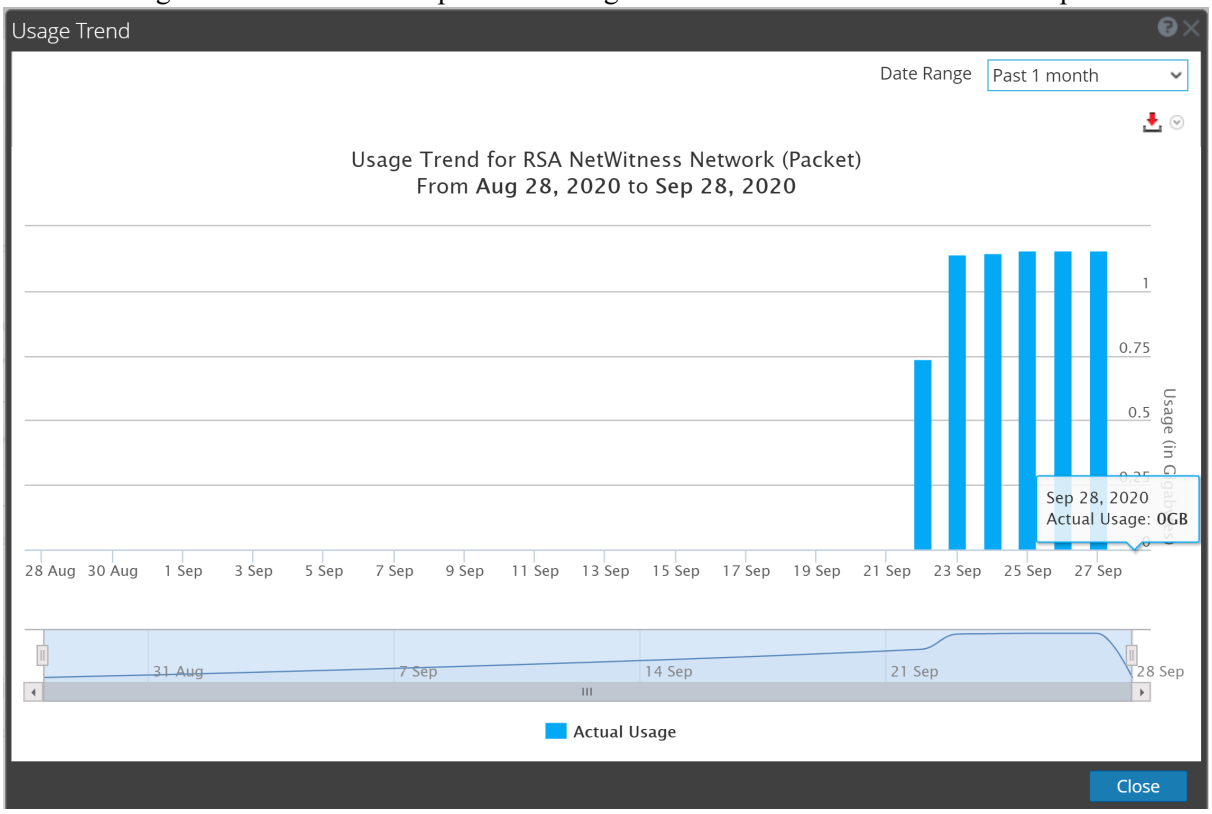
The following screenshot is an example of the Exceeded Usage Trend.



The following screenshot is an example of Within Limits Exceeded Usage Trend.


Usage Trend
Date Range
Past 1 month
Usage Trend for RSA NetWitness Malware Analytics
From Jan 26, 2019 to Feb 26, 2019
1000
750
500
250
0
Usage (in Gigabytes)
Feb 20, 2019
Actual Usage: 0GB
Entitled Usage: 1024GB
26 Jan
28 Jan
30 Jan
1 Feb
3 Feb
5 Feb
7 Feb
9 Feb
11 Feb
13 Feb
21 Feb
23 Feb
25 Feb
28 Jan
4 Feb
11 Feb
18 Feb
25 Feb
Usage within entitled limit
Usage exceeding entitled limit
Close

The following screenshot is an example of the Usage Trend chart for a license with multiple services.



The threshold limit is indicated as a horizontal red-dotted line across the chart. When actual data usage exceeds the entitled daily usage, those days are indicated by red colored bars.
The chart can be generated to collect data for 1 month, 3 months, 6 months, 12 months or custom date range.

These charts can be exported in CSV, and PDF formats by clicking the icon.

Note: The maximum range for which trend can be viewed is 12 months. The pan-zoom bar at the bottom of the chart can be used to narrow the chart to a smaller time range for better visibility in that range.

If the entitled limit exceeds the usage limit then an appropriate out-of-compliance banner is displayed. For more information, see About Out-of-Compliance Banners.

Reassign Service Licenses

You can move service between licenses only if a similar service license is available.

You can move the services between the following licenses.

- Throughput License to Throughput License
- Throughput License to Appliance License
- Appliance License to Throughput License
- Appliance License to Appliance License

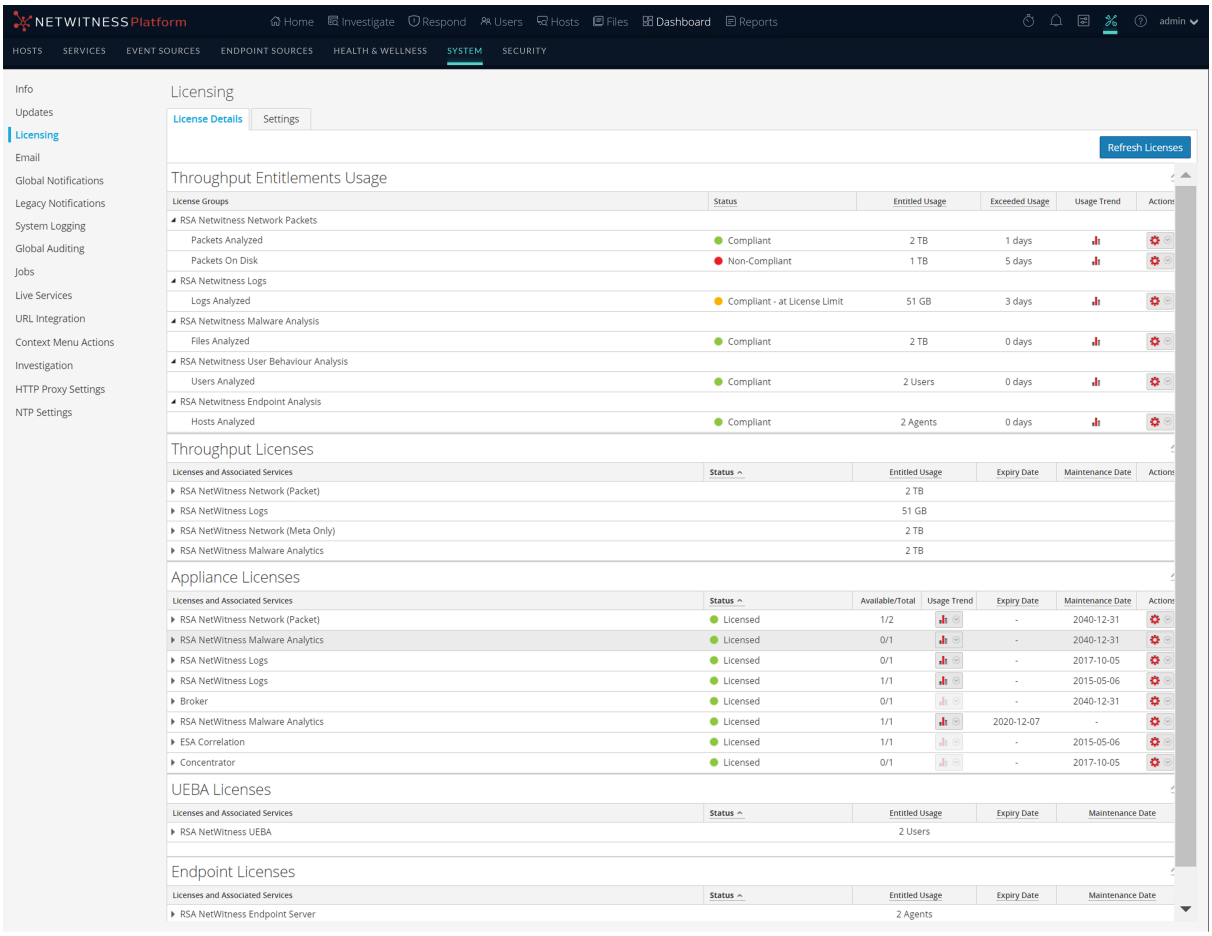
Note: If you want to change the licenses by moving between throughput and appliance, you can do this by selecting the license under the actions of each license. Trail licenses cannot be moved.

You can move the licenses for following reasons:

1. If the subscription based license has expired
2. If there are any unused available license for any service
3. If you want to reduce the usage of the service

To access this view:

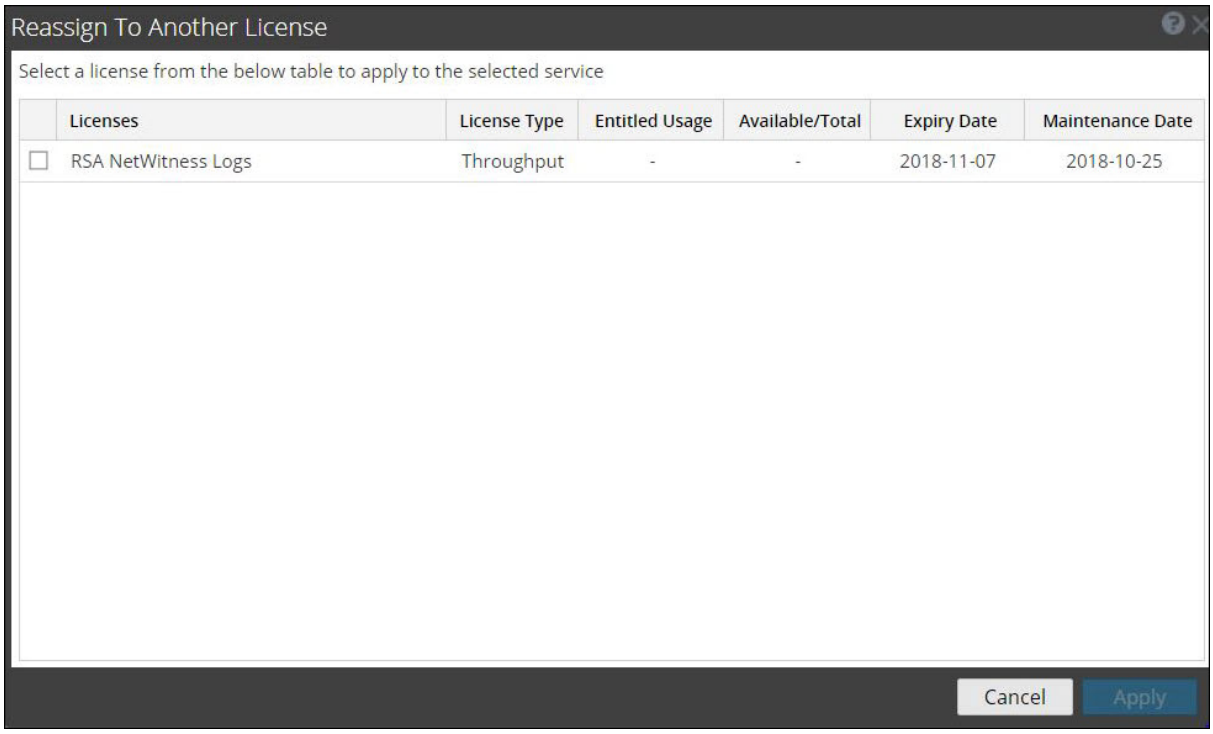
1. Go **(Admin) > System** and select **Licensing**.
   The License Details tab is displayed.



2. Select a service of which you want to move the license.

3. Click , and select the **Reassign to Another License** option.

   The Reassign To Another License dialog is displayed with a list of the available licenses that can be moved.



4. Select a license to be applied for the selected service.
5. Click **Apply**.

Note: The above procedure can be used to move both Throughput Licenses and Appliance Licenses. However, the UEBA and Endpoint licenses cannot be moved.

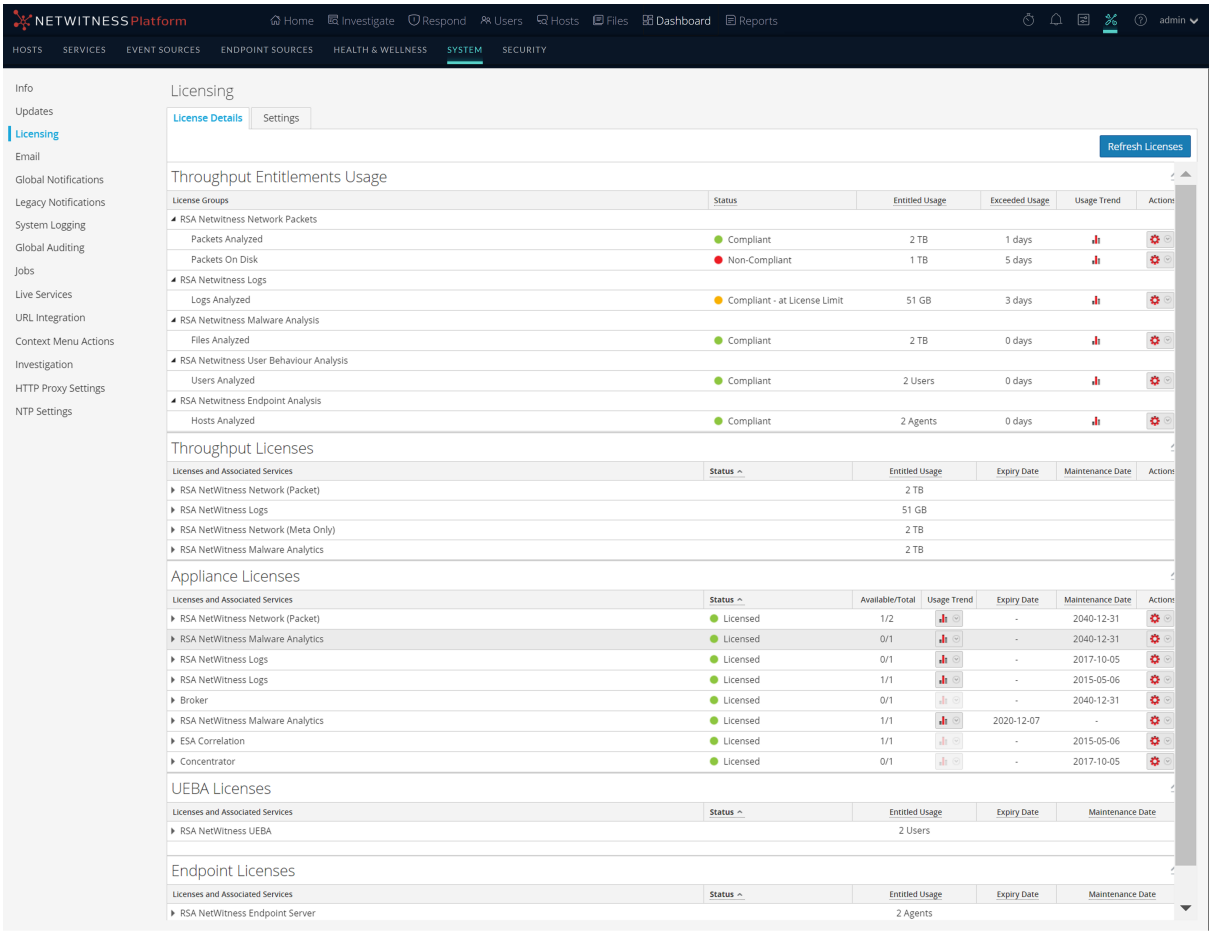
View and Export Usage Stats

NetWitness provides the ability for Administrators to view usage statistics of device types that are eligible for a Throughput , Appliance Licenses such as Log Decoder, Decoder, Malware, UEBA, and Endpoint Server licenses. An hourly usage statistics is captured for all supported services connected to the NetWitness Server and are made available in CSV, and PDF formats. Metrics can be tracked securely, allowing Administrators to save data locally on their systems to use in reporting usage compliance.

To access Export Usage Stats:

1. Go **(Admin) > System** and select **Licensing**.

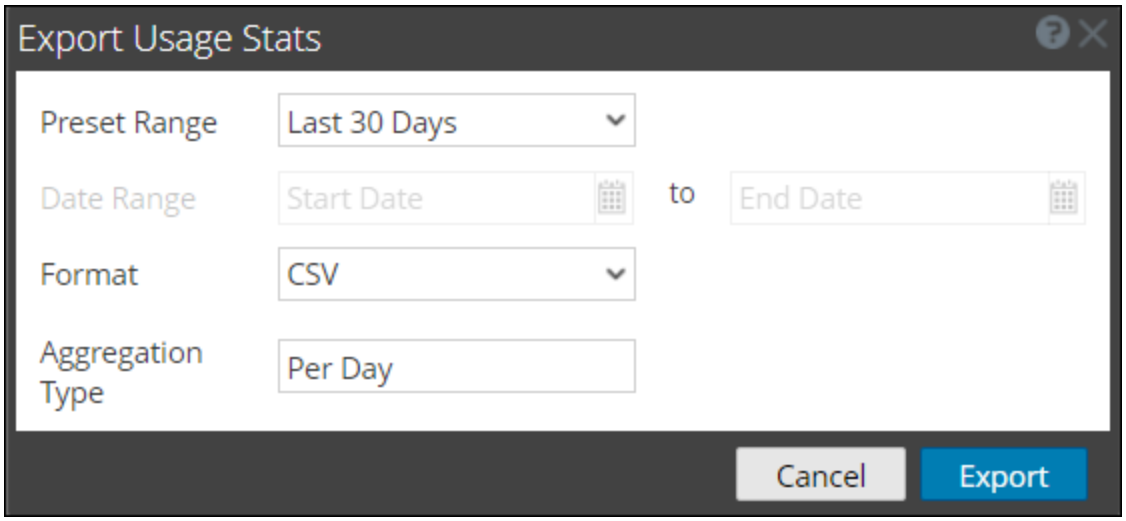
   The License Details tab is displayed.



2. Select a service for which you want to export usage stats.

3. Click , and select the **Export Usage Stats** option.

   The **Export Usage Stats** dialog is displayed.



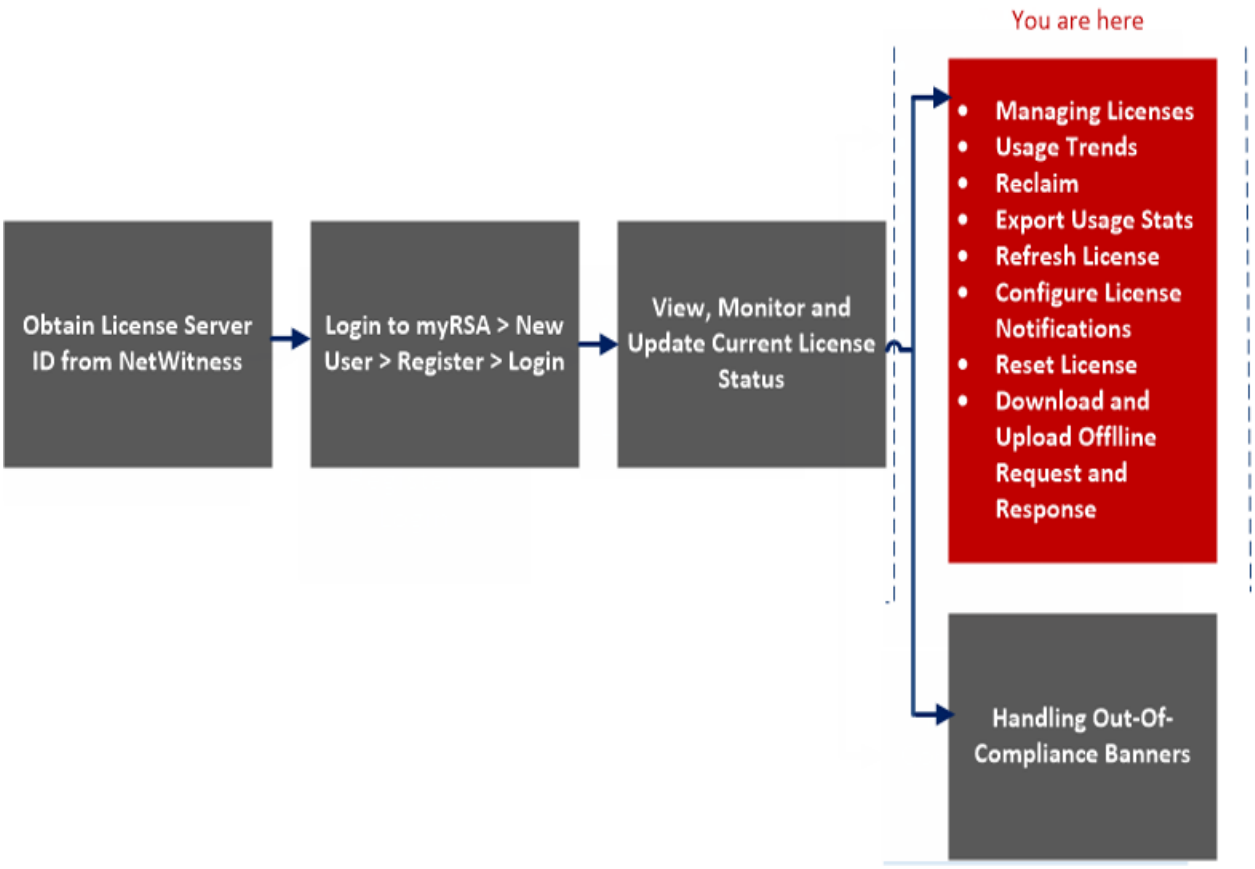
4. Select a **Preset Range**, **Date Range** (in case of custom range), **Format** and **Aggregation Type** to generate the report.
5. Click **Export** to export the report or click **Cancel** to return to the **License Details** tab.

Settings

This topic describes the notification settings for the NetWitness in the **Licensing panel** > **Settings** tab.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Obtain License Server ID from NetWitness Platform User Interface
Administrator	Synchronize NetWitness Server	Register the Server (Online Registration)

Role	I want to...	Show me how...
Administrator	Install product licenses from DLC.	Access myRSA
Administrator	Monitor and update current licenses.	View Current Licenses
Administrator	*Configure licensing notifications.	Configure License Notifications
Administrator	View Out-of-Compliance banners	About Out-of-Compliance Banners

*You can perform this task here.

Related Topics

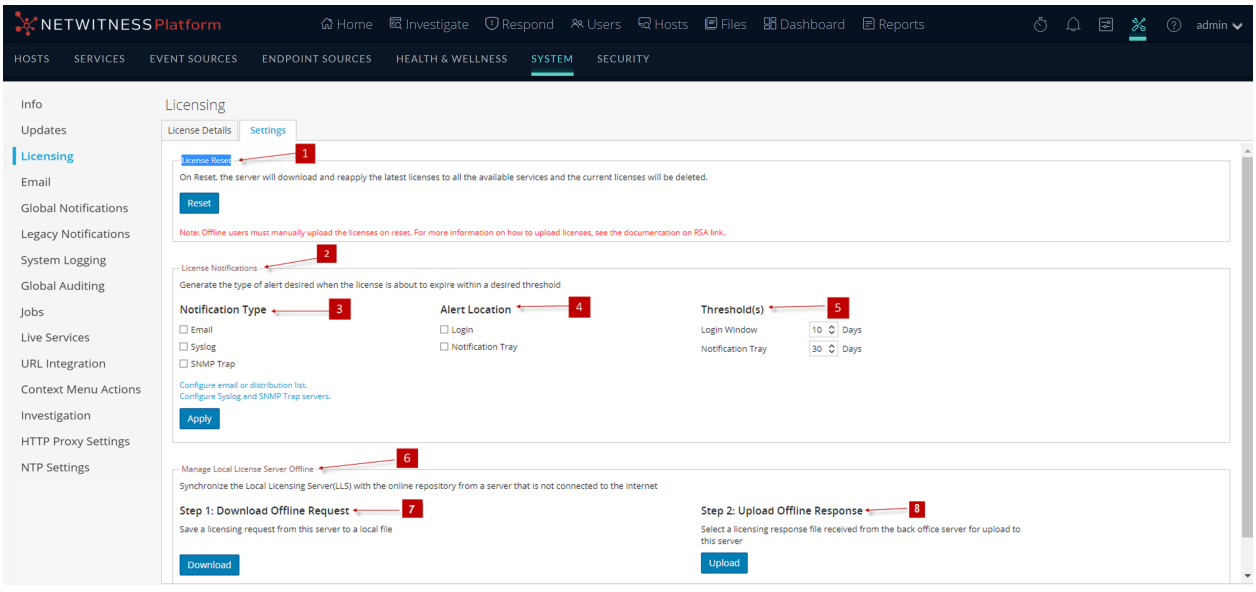
Obtain License Server ID from NetWitness Platform User Interface

Configure License Notifications

Quick Look

From the **Settings** tab you can:

- Configure licensing notifications.
- Download an Offline Capability Request in NetWitness for submission to DLC.
- Within 72 hours, upload to NetWitness an Offline Response that was received from DLC.



The following table describes the **Settings** tab features.

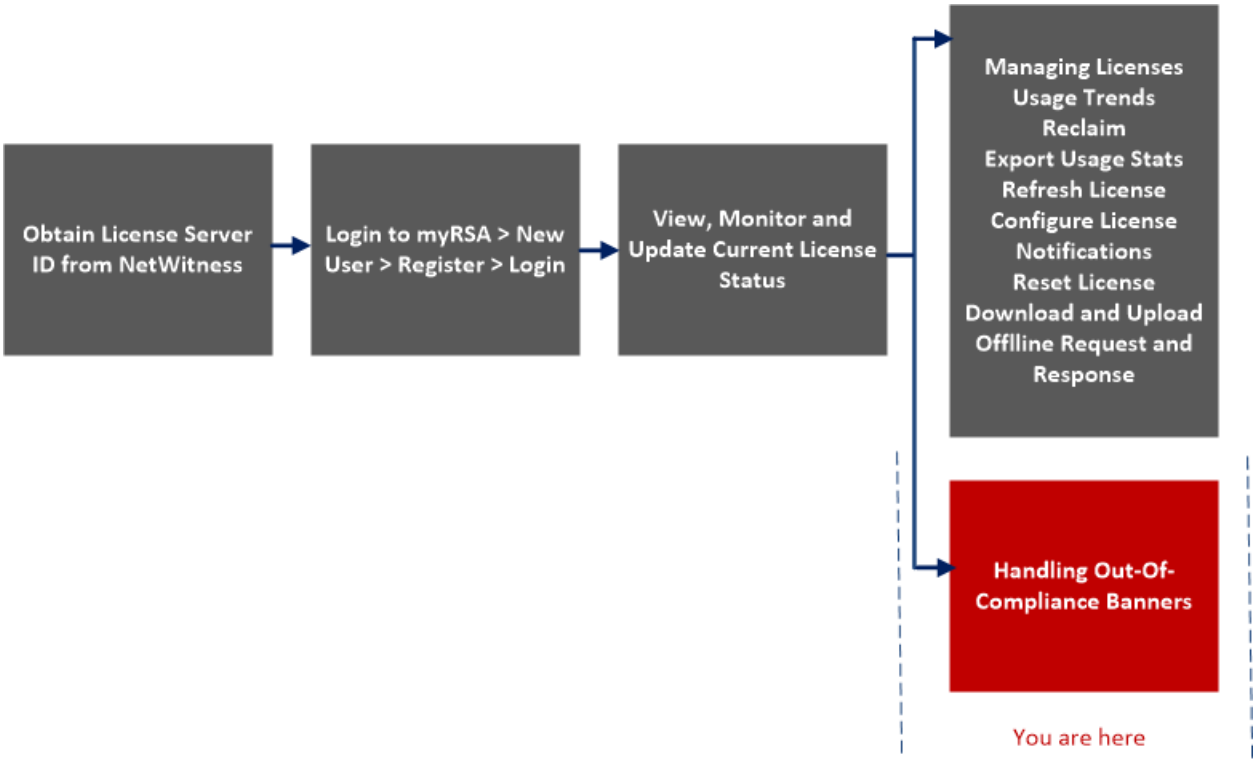
1	Displays the **License Reset** panel which applies the default license settings.
2	Displays the **Licensing Notifications** panel.
3	Displays the **Notification Type**. There are three types of notifications: • **Email:** Checkbox to receive a notification of approaching license expiration in an email message. The email is sent to the configured email or distribution list. • **Syslog:** Checkbox to receive a notification of approaching license expiration in an syslog message. The syslog is generated in accordance with the settings in the Syslog Auditing Settings. • **SNMP Trap:** Checkbox to receive a notification of approaching license expiration in an SNMP trap. The trap is generated in accordance with the settings in the SNMP Auditing Settings.
4	Displays the type of **Alert Notification**. • **Login:** Select this checkbox to receive a notification of your approaching license expiration when you log on to NetWitness. The **Login Window Threshold** field specifies the number of days before the license expires to display the notification at log on. • **Notification Tray:** Select this checkbox to receive a notification of approaching license expiration in the Notifications tray.
5	Displays the **Threshold** field, which specifies the number of days before the license expires to send a notification to the Notifications tray.
6	Displays the **Manage Local License Server Offline** panel.
7	Displays the **Download Offline Request** button. This button enables you to download a request from the NetWitness Platform LLS into a local file for processing by a back-office server. The downloaded bin file should be uploaded to DLC to generate the offline response.
8	Displays the **Upload Offline Request** button. This button enables you to browse for an offline response that you received from the back-office server, and uploads the selected response to NetWitness. The file must be uploaded within 72 hours after receiving the file.

Out-of-Compliance Reference

This topic describes the workflow when your license is out of compliance.

Workflow

This workflow illustrates the end-to-end licensing process.



What do you want to do?

Role	I want to...	Show me how...
Administrator	Register NetWitness Server	Obtain License Server ID from NetWitness Platform User Interface
Administrator	Synchronize NetWitness Server	Register the Server (Online Registration)
Administrator	Install product licenses from DLC.	Access myRSA

Role	I want to...	Show me how...
Administrator	Monitor and update current licenses.	View Current Licenses
Administrator	Configure licensing notifications.	Configure License Notifications
Administrator	*View Out-of-Compliance banners.	About Out-of-Compliance Banners

*You can perform this task here.

Note: When throughput devices are under trial period, warning messages will not be displayed unless usage is observed on the corresponding device.

Out-of-Compliance State

The following sample banner is displayed when a license expires:

If your license has internal errors, the following banner is displayed:

In addition to a red banner being displayed during system log on, an Out of Compliance Acknowledgment dialog is also displayed. Click **Accept** to continue using your NetWitness product.

Licenses may become out-of-compliance due to reasons provided in the following table:

Red Banner Message	Possible Causes	Solutions
One or more services is not licensed.	Trial license period has expired.	Contact Sales team to procure a NetWitness license. Upgrade the services to the latest NetWitness version.
One or more licenses is expired.	Log ingestion usage has been observed after the date of renewal. The license is not valid anymore for the corresponding usage.	Contact Sales team to renew or resolve the license.
You have exceeded license usage limits.	If the allotted daily usage is exceeded on four or more occasions, the Grace Period begins. The Grace Period begins on the day of the fourth occurrence and ends at the end of the following calendar month. Seven continuous days of standard usage will end the Grace Period. If the daily allotted usage is still being exceeded at the end of the Grace Period, the 30-day Breach Period begins. Seven continuous days of standard usage will end the Breach Period.	Contact Sales to extend or increase your allotted usage by purchasing a NetWitness license.
Your Trial license has internal errors.	An internal licensing issue was reported during your Out-of-the-Box Trial period.	Contact Technical Support to resolve this issue.

Note: If a license has not been installed within 90 days, you must contact Sales to purchase a NetWitness license.

License Approaching Out-of-Compliance

When your license is approaching expiration, or it is nearing its allotted usage, a yellow banner with a brief description is displayed. A yellow banner is displayed 14 days before your license is due to expire. You will also see a yellow banner if you are approaching your allotted license usage. You can get rid of the yellow banner by clicking the **Dismiss** button.

The following sample banner is displayed in the NetWitness screen if your license is approaching its allotted usage:

The following table explains the messages that are displayed when you see a yellow banner.

Yellow Banner Message	Possible Causes	Solutions
You are nearing license usage limits.	One or more Throughput licenses has exceeded your allotted usage for three times during the current calendar month. The fourth time that you exceed your allotted usage during the current month will push the deployment into an Out-of-Compliance state.	Contact NetWitness Sales if your allotted usage spikes four times within a calendar month.
One or more licenses is expiring.	One or more licenses is due to expire within 14 days. Or Log ingestion usage has been observed. The license is not valid anymore for the corresponding usage.	Contact NetWitness Sales to purchase a new license.

License Usage Calculations for Decoder and Log Decoder Services

This topic provides information about license usage calculations for Decoder and Log Decoder Services.

- Decoder and Log Decoder generate stats called **Capture Bytes Processed** which is used for license usage calculations.
- Decoders also generate stats known as **Packet Write Bytes** in addition to **Capture Bytes Processed**.
- Every hour, the system compares the current reading with the previous hour's usage.
  - If the current reading is greater than or equal to the previous hour's usage, calculate the per-hour usage as the difference: **currentHourUsage = currentReading - previousHourUsage**.
  - If the current value is less than the previous hour's usage, it indicates a Decoder restart. In this case, set **currentHourUsage = currentReading**.
- At the end of the day, combine the usages of each individual hour for that day.
- The same calculation is carried out for each licensed Decoder in the environment.
- The combined usage of **Capture Bytes Processed** per day of all Log Decoders is shown under **Logs Analyzed**.
- The combined usage of **Capture Bytes Processed** per day of all decoders is shown under **Packets Analyzed**.
- The combined usage of **Packet Write Bytes** per day of all decoders is shown under **Packets on disk**.

Note:
- All the calculations are done based on UTC time.
- The daily usages shown on the UI is also based on UTC, irrespective of the timezone set in the user profile.