



# **NetFlow Optimizer™**

---

## **Installation and Administration Guide**

**Version 2.4.8 (Build 2.4.8.0.2)**

**February 2017**

# Contents

<b>Overview .....</b>	<b>3</b>
How NetFlow Optimizer Works .....	3
How External Data Feeder for NFO Works .....	3
<b>NetFlow Optimizer Installation Guide.....</b>	<b>4</b>
<b>Before You Install NFO .....</b>	<b>4</b>
Pre-Installation Checklist .....	4
Minimum Requirements .....	4
Supported Platforms.....	4
Virtual Hardware .....	4
Supported Browsers .....	5
Required Network Ports .....	5
Sizing the NFO Virtual Appliance .....	5
<b>Installing NFO.....</b>	<b>6</b>
Deploy the NFO Virtual Appliance .....	6
Linux RPM Installation .....	7
Linux TAR Installation.....	8
Windows Installation .....	8
<b>Upgrading NFO.....</b>	<b>9</b>
Upgrading the NFO Virtual Appliance or RPM Installation.....	10
Upgrading TAR Installation .....	10
Upgrading Windows Installation.....	11
<b>Removing NFO .....</b>	<b>11</b>
Removing the NFO Virtual Appliance .....	11
Removing RPM Installation .....	11
Removing TAR Installation .....	12
Removing Windows Installation .....	12
<b>NetFlow Optimizer Administration Guide .....</b>	<b>13</b>
<b>Configuring NFO .....</b>	<b>13</b>
Configure the Root SSH Password for the NFO Virtual Appliance .....	13
Configure the User Password for the NFO .....	13
Assign a Permanent License to NFO.....	14
Start NetFlow Optimizer.....	14
Update Input and Output .....	14
Input Summary .....	14
Output Summary .....	15
Starting and Stopping NetFlow Optimizer .....	16
Enabling and Configuring Modules .....	16
Configure Top Traffic Monitor Module Parameters.....	17
Data Sets Summary .....	17
Status .....	18
Configuring Advanced Features .....	19
Output Tab .....	19
Services Tab .....	19
Data Feeder Tab .....	22
Server Tab.....	22
Admin .....	23
Change Password .....	23
Forgot Password .....	23
Active Directory Authentication.....	24
Two Factor Authentication (2FA) .....	26
Disabling Admin Account.....	26

Licensing .....	27
License Details .....	27
Apply a License .....	28
Server Configuration Parameters .....	28
Linux kernel settings for high-volume processing .....	28
Secure Connection Configuration (HTTPS) .....	29
Create a local Certificate Signing Request (CSR) .....	29
Import the Certificate .....	29
Copying NFO Configuration.....	30
<b>External Data Feeder for NFO Getting Started Guide .....</b>	<b>31</b>
<b>Before You Install External Data Feeder for NFO .....</b>	<b>31</b>
Pre-Installation Checklist .....	31
Minimum Requirements .....	31
Supported Platforms.....	31
Required Network Ports .....	31
Required Internet Destinations .....	32
<b>Installing External Data Feeder for NFO .....</b>	<b>32</b>
Linux RPM Installation .....	32
Linux TAR Installation.....	33
Windows Installation.....	34
<b>Upgrading External Data Feeder for NFO .....</b>	<b>35</b>
Upgrading the External Data Feeder for NFO RPM Installation .....	35
Upgrading the External Data Feeder for NFO TAR Installation .....	36
Upgrading the External Data Feeder for NFO Windows Installation .....	36
<b>Removing External Data Feeder for NFO.....</b>	<b>37</b>
Removing the External Data Feeder for NFO RPM Installation .....	37
Removing the External Data Feeder for NFO TAR Installation.....	37
Removing the External Data Feeder for NFO Windows Installation .....	37
<b>External Data Feeder for NFO Administration Guide.....</b>	<b>38</b>
<b>Configuring External Data Feeder for NFO .....</b>	<b>38</b>
Verifying External Data Feeder for NFO Status .....	38
Verifying External Data Feeder for NFO Linux Installation .....	38
Verifying External Data Feeder for NFO Windows Installation .....	38
Authentication Configuration.....	38
X509 authentication.....	39
User/password authentication .....	40
Import the Certificate into External Data Feeder for NFO truststore.....	40
Proxy Server Configuration .....	41
Copying External Data Feeder for NFO Configuration.....	41

# Overview

The *NetFlow Optimizer Installation and Administration Guide* provides information about deploying and configuring NFO including how to configure it to send syslog messages to Splunk® Enterprise, VMware® vRealize™ Log Insight™, or any other SIEM system.

## Announcement of product name change

Our core product NetFlow Integrator, or NFI, is now called NetFlow Optimizer (NFO). NFI Updater, or Updater, is now called External Data Feeder for NFO. All references to NetFlow Integrator (NFI) or NFI Updater in this document apply to NetFlow Optimizer or External Data Feeder for NFO. NFO upgrades can be applied to NFI installations, and External Data Feeder for NFO upgrades can be applied to NFI Updater. Internal file names and directory structures remain the same, so any external scripts you may have will still find logs and other information.

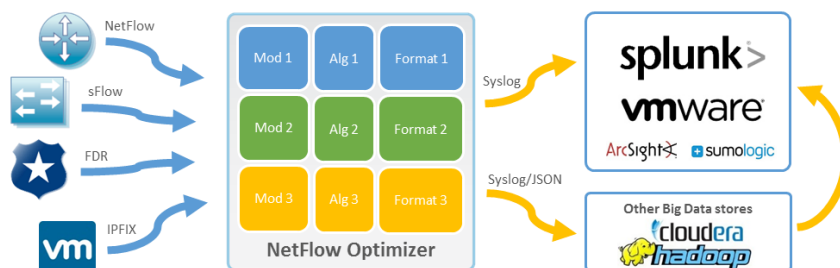
## Intended Audience

This information is intended for anyone who wants to install, configure, or maintain NFO. The information is written for experienced Linux or Windows system administrators who are familiar with virtual machine technology and datacenter operations.

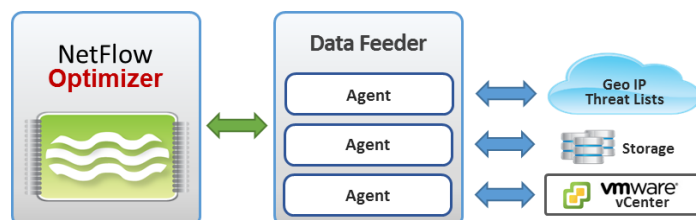
## How NetFlow Optimizer Works

**NetFlow Optimizer** is a software-only processing engine for network flow data (NetFlow, IPFIX, sFlow, jFlow, etc.). **It is not a NetFlow collector.**

NetFlow Optimizer accepts network flow data from network devices (routers, switches, firewalls), applies map-reduce algorithms to the data to extract the information needed to address desired use cases, converts the processed data to syslog (or other formats such as JSON), then sends that useful information to your visualization platform or SIEM.



## How External Data Feeder for NFO Works



External Data Feeder for NFO (EDFN) is a remote component which serves as a knowledge base of information outside of the NetFlow domain. Its task is to provide NetFlow Optimizer with information generally unavailable in the data streams supplied by NetFlow/IPFIX exporters.

EDFN is comprised of a Platform and a collection of Agents each of which is designed to obtain information of a certain kind. The Platform provides a common interface for the Agents' configuration and data exchange and serves as a conduit for delivering information collected by the Agents to the NetFlow Optimizer. Typically External Data Feeder for NFO is installed on a separate server with access to the internet.

# NetFlow Optimizer Installation Guide

---

## Before You Install NFO

### Pre-Installation Checklist

Please be sure to have the following before you begin the installation of the NetFlow Optimizer software:

- You have to login as **root** for Linux and **administrator** for Windows installations and updates
- License – A **license** is required before you can begin using NetFlow Optimizer software. Please register at <https://www.netflowlogic.com/register-form/> to get your FREE evaluation license or contact [sales@netflowlogic.com](mailto:sales@netflowlogic.com)
- Network Device - Please refer to the “Configuring NetFlow Data Export” section in your Cisco (or other) device documentation

### Minimum Requirements

NetFlow Logic distributes NFO as a virtual appliance in OVA file format, as RPM or TAR.GZ for Linux, or as EXE for Windows. Various resources and applications must be available for the virtual appliance to run successfully.

### Supported Platforms

You can install the NetFlow Optimizer virtual appliance or software on a platform with the following specifications.

Specification	Details
Virtual Appliance	VMware ESXi 5.x and above
Linux	Linux kernel 2.6+ on <ul style="list-style-type: none"><li>- CentOS 5.5, 6.5, 6.7, 7</li><li>- Debian 6.0</li><li>- RHEL 5.5, 6.5, 6.7, 7</li><li>- SUSE ES 11</li></ul>
Windows	Windows 2008 R2, 2012, and 2012 R2 (64-bit)
CPU, Memory, Disk Space	<ul style="list-style-type: none"><li>- CPU: Min 4 CPU cores (8 or 16 CPU cores for higher performance)</li><li>- Memory: Min 4 GB (16 GB recommended)</li><li>- Disk Space: 20 GB</li></ul>

### Virtual Hardware

During deployment of the NFO virtual appliance you can select different sizes according to the ingestion requirements for the environment. The small configuration requires the following virtual resources.

- 4 vCPUs, 2GHz each
- 8GB RAM
- Approximately 20GB storage space

## Supported Browsers

You can use one of the following browsers to connect to the NFO Web user interface.

- Mozilla Firefox 38.0 and up
- Safari 6.0 , 7.0
- Google Chrome 34.0 and 43.0 and up
- IE10, IE11, and MS Edge

## Required Network Ports

The following network ports must be accessible.

Port	Protocol
8443/TCP	NetFlow Optimizer GUI
9995/UDP	NetFlow/IPFIX Ingestion (plus all ports for ingestion as necessary)
20047/TCP and 20048/TCP	NetFlow Optimizer internal services

## Sizing the NFO Virtual Appliance

By default, the NFO virtual appliance has 4 vCPUs, 8GB of virtual memory, and 20GB of disk space provisioned.

### Standalone Deployment

You can change the settings according to the environment for which you intend to collect NetFlow.

During the virtual appliance deployment, you can select the size of the appliance as follows.

Option	Number of VMs	NetFlow Ingest Rate	vCPUs	Memory
Small	200	2,000 flows/sec	4	8GB
Medium	2,000	20,000 flows/sec	8	16GB
Large	5,000+	50,000+ flows/sec	16	32GB

# Installing NFO

## Deploy the NFO Virtual Appliance

To deploy the NFO virtual appliance, follow the standard OVF deployment procedure.

Download the NFO virtual appliance. VMware distributes the NFO virtual appliance as an `.ova` file. Deploy the NFO virtual appliance by using the vSphere Client.

### Prerequisites

- Verify that you have a copy of the NFO virtual appliance `.ova` file.
- Verify that you have permissions to deploy OVF templates to the inventory.
- Verify that your environment has enough resources to accommodate the minimum requirements of the NFO virtual appliance. See Minimum Requirements.
- Verify that you read and understand the virtual appliance sizing recommendations. See Sizing the NFO Virtual Appliance.

### Procedure

1. In the vSphere Client, select **File > Deploy OVF Template**.
2. Follow the prompts in the Deploy OVF Template wizard.
3. On the Deployment Configuration page, select the size of the NFO virtual appliance based on the size of the environment for which you intend to collect NetFlow.
4. On the Disk Format page, select a disk format.
  - **Thick Provision Lazy Zeroed** creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. The data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time, on first write from the virtual appliance.
  - **Thick Provision Eager Zeroed** creates a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

IMPORTANT: Deploy the NFO virtual appliance with thick provisioned eager zeroed disks whenever possible for better performance and operation of the virtual appliance.

  - **Thin Provision** creates a disk in thin format. The disk grows as the data saved on it grows. If your storage device does not support thick provisioning disks or you want to conserve unused disk space on the NFO virtual appliance, deploy the virtual appliance with thin provisioned disks.
5. (Optional) On the Properties page, set the networking parameters for the NFO virtual appliance.

If you do not provide network settings, such as IP address, DNS servers, and gateway, NFO utilizes DHCP to set those settings.



**CAUTION** Do not specify more than two domain name servers. If you specify more than two domain name servers, all configured domain name servers are ignored in the NFO virtual appliance.

Use comma to separate domain name servers.

6. (Optional) On the Properties page, set the root password for the NFO virtual appliance.
7. Follow the prompts to complete the deployment.

For information on deploying virtual appliances, see the *User's Guide to Deploying vApps and Virtual Appliances*.

After you power on the virtual appliance, an initialization process begins. The initialization process takes several minutes to complete. At the end of the process, the virtual appliance restarts.

8. Navigate to the **Console** tab and check the IP address of the NFO virtual appliance.

IP Address Prefix	Description
https://	The DHCP configuration on the virtual appliance is correct.
http://	<p>The DHCP configuration on the virtual appliance failed. If it is failed:</p> <ul style="list-style-type: none"><li>• Power off the NFO virtual appliance.</li><li>• Right-click the virtual appliance and select Edit Settings.</li><li>• Set a static IP address for the virtual appliance.</li></ul>

## What to do next

- To enable SSH connections to the NFO virtual appliance, configure the root password in the virtual appliance console. See *Configure the Root SSH Password for the NFO Virtual Appliance*.
- The NFO Web interface is available at `https://<nfo-host>:8443` where `NFO-host` is the IP address or host name of the NFO virtual appliance.
- Log in to NetFlow Optimizer, apply license, and continue configuration. See *Configuring NFO* on page 13 for more information.

## Linux RPM Installation

Download the NFO RPM package.

### Procedure

To begin the RPM installation of NFO in the default directory `/opt/flowintegrator` perform the following:

Open a shell prompt and enter the following command to begin the installation

```
rpm -ihv <RPM-package>
```

To begin the RPM installation of NetFlow Optimizer in another directory, perform the following:

Open a shell prompt and enter the following command to begin the installation

```
rpm -ihv --relocate /opt=<new-path> <RPM-package>
```



## What to do next

A message will display indicating that the NetFlow Optimizer installation has been successfully completed.

- The NFO Web interface to complete the setup is available at `https://<nfo-host>:8443` where `NFO-host` is the IP address or host name of the NFO server.
- Log in to NetFlow Optimizer, apply license, and continue configuration. See Configuring NFO on page 13 for more information.

## Linux TAR Installation

Download the NFO TAR package.

### Procedure

To begin the TAR installation of NFO in the default directory `/opt/flowintegrator` perform the following:

1. Open a shell prompt and enter the following command to un-compress the installer  

```
tar zxvf <TAR-package> -C /opt/flowintegrator
```
2. Go to the `/opt/flowintegrator` directory and enter the following command to begin the installation  

```
setup.sh -i
```

To begin the TAR installation of NetFlow Optimizer in another directory, perform the following:

1. Open a shell prompt and enter the following command to un-compress the installer  

```
tar zxvf <TAR-package> -C <directory>
```
2. Go to the `/opt/flowintegrator` directory and enter the following command to begin the installation  

```
setup.sh -i
```

## What to do next

A message will display indicating that the NetFlow Optimizer installation has been successfully completed.

- The NFO Web interface to complete the setup is available at `https://<nfo-host>:8443` where `NFO-host` is the IP address or host name of the NFO server.
- Log in to NetFlow Optimizer, apply license, and continue configuration. See Configuring NFO on page 13 for more information.

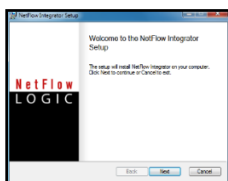
## Windows Installation

Download the NFO Windows installation package.

### Procedure

To begin the Windows installation of NetFlow Optimizer perform the following:

1. Open the installation file and click 'Run' to launch the installer and Click 'Next' To begin the 'NetFlow Optimizer Setup'



2. Click 'Next' to install NetFlow Optimizer in the default location:  
`C:\Program Files\NetFlow Logic\NetFlow Optimizer`
3. Click on 'Install' To begin the installation (follow the installation steps)
4. Click on 'Finish' to complete the installation and exit the installer

## What to do next

Go to Start > Programs > NetFlow Logic > NetFlow Optimizer to open the URL for the login page to complete the setup using the default browser.

- The NFO Web interface to complete the setup is available at `https://<nfo-host>:8443` where NFO-host is the IP address or host name of the NFO server.
- Log in to NetFlow Optimizer, apply license, and continue configuration. See Configuring NFO on page 13 for more information.

# Upgrading NFO

You upgrade a single instance of NFO by installing the latest version over your existing installation. During the upgrade the installer package preserves all NFO configurations, except configuration files changed manually. These files, if changed, are backed up into `conf-backup.<date>.tar.gz` file (<date> is archive date), and should be restored manually, if necessary.

The following is a list of some configuration files.

File	Purpose
<code>\$nfo_home/tomcat/bin/setenv.sh</code>	Environment variables
<code>\$nfo_home/tomcat/conf/.tomcat_keystore</code>	Default self-signed certificate
<code>\$nfo_home/tomcat/conf/.truststore</code>	External Data Feeder for NFO certificate
<code>\$nfo_home/tomcat/conf/server.xml</code>	Keystore password
<code>\$nfo_home/server/etc/server.cfg</code>	Server configuration (Note: some Web GUI configurations are in this file as well)
<code>\$nfo_home/java/jre8/jre/lib/security/cacerts</code>	Trusted certificates imported into Java Runtime cacerts keystore




After upgrade, validate default configuration and restore from the backup if it is required.  
If you didn't modify these files, ignore the caution.

## Upgrading the NFO Virtual Appliance or RPM Installation

### Procedure


To begin the upgrade of NFO Virtual Appliance or RPM perform the following:

1. Open a web browser and go to the NFO URL, entering the NFO hostname or IP address
2. Example:  
`https://<nfo-host>:8443`
3. Click on the 'Stop' button  at the top of the page to stop the server
4. The 'Play' button will turn grey indicating that the NetFlow Optimizer has stopped
5. Login directly or SSH and copy the new installation file into the /opt installation directory
6. RPM the NetFlow Optimizer for Linux installation file into the /opt installation directory  
`rpm -Uhv <RPM-package>`
7. A message will display indicating that the NFO setup has been successfully completed along with the URL for the login page

## Upgrading TAR Installation

### Procedure


To begin the upgrade of NFO TAR installation, perform the following:

1. Open a web browser and go to the NFO URL, entering the NFO hostname or IP address
2. Example:  
`https://<nfo-host>:8443`
3. Click on the 'Stop' button  at the top of the page to stop the server
4. The 'Play' button will turn grey indicating that the NetFlow Optimizer has stopped
5. Go to the existing installation directory and enter the following command to begin the uninstall  
`setup.sh -u`
6. Copy the upgrade installation package for Linux into the existing installation directory
7. Open a shell prompt and enter the following command to un-compress the installer  
`tar zxvf <TAR-package> -C <directory>`
8. A message will display indicating that the NFO setup has been successfully completed along with the URL for the login page

# Upgrading Windows Installation

## Procedure

To begin the upgrade of NFO on a Windows platform, perform the following:

1. Open a web browser and go to the NFO URL, entering the NFO hostname or IP address
2. Example:  
`https://<nfo-host>:8443`
3. Click on the 'Stop' button  at the top of the page to stop the server
4. The 'Play' button will turn grey indicating that the NetFlow Optimizer has stopped
5. Open the upgrade installation file and click 'Run' to launch the installer and Click 'Next' To begin the 'NetFlow Optimizer Setup'
6. Click 'Next' to install NetFlow Optimizer in the default location:  
`C:\Program Files\NetFlow Logic\NetFlow Optimizer`
7. Click on 'Install' To begin the installation (follow the installation steps)
8. Click on 'Finish' to complete the installation and exit the installer

# Removing NFO

## Removing the NFO Virtual Appliance


## Procedure

Manually remove the NetFlow Optimizer virtual appliance files from the hypervisor.

# Removing RPM Installation

## Procedure

To begin the removal of NFO RPM installation, perform the following:

1. Open a web browser and go to the NFO URL, entering the NFO hostname or IP address
2. Example:  
`https://<nfo-host>:8443`
3. Click on the 'Stop' button  at the top of the page to stop the server
4. The 'Play' button will turn grey indicating that the NetFlow Optimizer has stopped
5. Open a shell prompt and enter the following command to begin the uninstall  
`rpm -e flowintegrator`

6. Remove the install path if the full uninstall needed

```
rm -rf <directory>
```

## Removing TAR Installation

### Procedure

To begin the removal of NFO TAR installation, perform the following:

1. Open a web browser and go to the NFO URL, entering the NFO hostname or IP address

2. Example:

```
https://<nfo-host>:8443
```

3. Click on the 'Stop' button  at the top of the page to stop the server

4. The 'Play' button will turn grey indicating that the NetFlow Optimizer has stopped

5. Go to the existing installation directory and enter the following command to begin the uninstall

```
setup.sh -u
```

6. Leave the installation directory

```
cd ..
```

7. Remove the install path if the full uninstall needed

```
rm -rf <directory>
```

## Removing Windows Installation

### Procedure

To begin the removal of NFO Windows installation, perform the following:

1. Go to Control Panel > Programs > Programs and Features and select the NetFlow Optimizer program
2. Follow the steps to uninstall the program

NOTE: You may need to manually remove the NetFlow Optimizer files from the installation directory prior to restarting the system.

# NetFlow Optimizer Administration Guide

---

## Configuring NFO

If you install several instances of NFO you can configure the first instance, and then copy configuration from the first instance to another one. Please see Copying NFO Configuration section on page 30 for details.

### Configure the Root SSH Password for the NFO Virtual Appliance

By default the SSH connection to the virtual appliance is enabled with root password `changeme` or the one that was set during deployment. You can change it from the VMware Remote Console.

#### Prerequisites

Verify that the NFO virtual appliance is deployed and running.

#### Procedure

1. In the vSphere Client inventory, click the NFO virtual appliance, and open the Console tab.
2. Click the Console window area. If the splash screen did not appear, press Space button on keyboard.
3. Go to a command line by following the key combination specified on the splash screen.
4. In the console, type `root`, and press Enter; type current password, and press Enter.
5. Type `passwd root` and press Enter.

The following message is displayed in the console:

```
Changing password for user root. New password:
```

6. Type a new password for the root user, press Enter, type the new password again for the root user, and press Enter.

The password must consist of at least eight characters, and must include at least one upper case letter, one lower case letter, one digit, and one special character. You cannot repeat the same character more than four times.

The following message is displayed:

```
passwd: all authentication tokens updated successfully.
```

#### What to do next

You can use the root password to establish SSH connections to the NFO virtual appliance.

### Configure the User Password for the NFO

1. Open a web browser and go to the following URL, entering the NetFlow Optimizer hostname or IP address:  
`https://<nfo-host>:8443`
2. Click on proceed to continue to the login page

**Note:** In the event you receive a warning message during login such as 'The sites security certificate is not trusted!' click on the 'proceed anyway' button to continue to the log in page.


3. Enter the following default credentials on the login page and click 'Sign In'

Username: admin


Password: changeme

4. Click on 'Agree' to accept the license agreement
5. Enter a new password at the change password prompt and click 'Save'

## Assign a Permanent License to NFO

1. Go to top navigation bar, select gear icon  > Licensing
2. Click on 'Choose files' to upload and apply your license
3. Proceed to the next step

## Start NetFlow Optimizer

1. Click on the 'Play' button  next to the NetFlow Optimizer status to Start the server

The 'Play' button will turn green indicating that the NetFlow Optimizer has started and is running

2. Proceed to the next step

## Update Input and Output


By default NetFlow Optimizer is preconfigured with one active data input port number 9995. To change the default data input port number or to add additional data inputs, follow the steps below

### Input Summary

By default NetFlow Optimizer is preconfigured with one active data input port number 9995. To change the default data input port number or to add additional data inputs, follow the steps below

1. Click on the 'edit' symbol to change the existing data input port

A screenshot of a user interface element showing a text input field containing the number '9995'. To the left of the input field is a green checkmark icon. To the right of the input field are two icons: a pencil (edit) and a trash can (delete).

2. Click 'Save'
3. Click on the 'plus' symbol  to add additional data input ports
4. Click 'Save'
5. Proceed to the next step

## Output Summary


You may add several output destinations, specifying the kind of data to be sent to each destination.

NFO supports the following varieties of outputs:

1. Type = Repeater – indicates that flow data received by NFO should be retransmitted to that destination, e.g your legacy NetFlow collector.
2. Type = Syslog, Output = Modules Output only – indicates the destination for syslogs generated by NFO Modules. Use this option for Splunk, VMware Log Insight, and other SIEM system.
3. Type = Syslog, Output = Original NetFlow/IPFIX only – indicates the destination for Original Flow Data, translated into syslog, one-to-one. Use this option to archive all underlying flow records NFO processes for forensics. This destination is typically Hadoop or another inexpensive storage, as the volume for this destination can be quite high.
4. Type = Syslog, Output = Original NetFlow/IPFIX only – indicates both #2 and #3 combined.

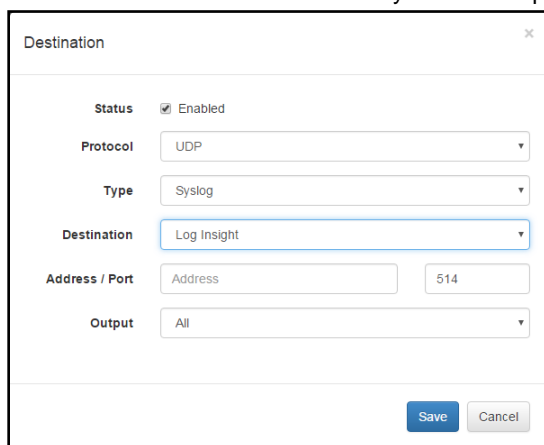
Please note that **Repeater** option allows you to specify the IP address, but not the destination port. This feature was designed so NFO can be "**inserted**" between NetFlow exporters and legacy NetFlow collectors. NFO will use the input port number and the exporter IP address when forwarding the original message received from the exporter.

To configure output destination:

1. Click on the 'plus' symbol  to add data outputs



2. Enter the destination information for your data output


A screenshot of a "Destination" configuration modal window. The window has a title bar with a close button. Inside, there are several configuration fields: "Status" with a checked "Enabled" checkbox; "Protocol" set to "UDP"; "Type" set to "Syslog"; "Destination" set to "Log Insight"; "Address / Port" with "Address" and "514" input fields; and "Output" set to "All". At the bottom right, there are "Save" and "Cancel" buttons.

3. Click 'Save'
4. Proceed to the next step



# Starting and Stopping NetFlow Optimizer

## Start

Click on the 'Play' button  next to the NetFlow Optimizer Server Status to start the server. A message will display indicating that the server has been started



## Stop

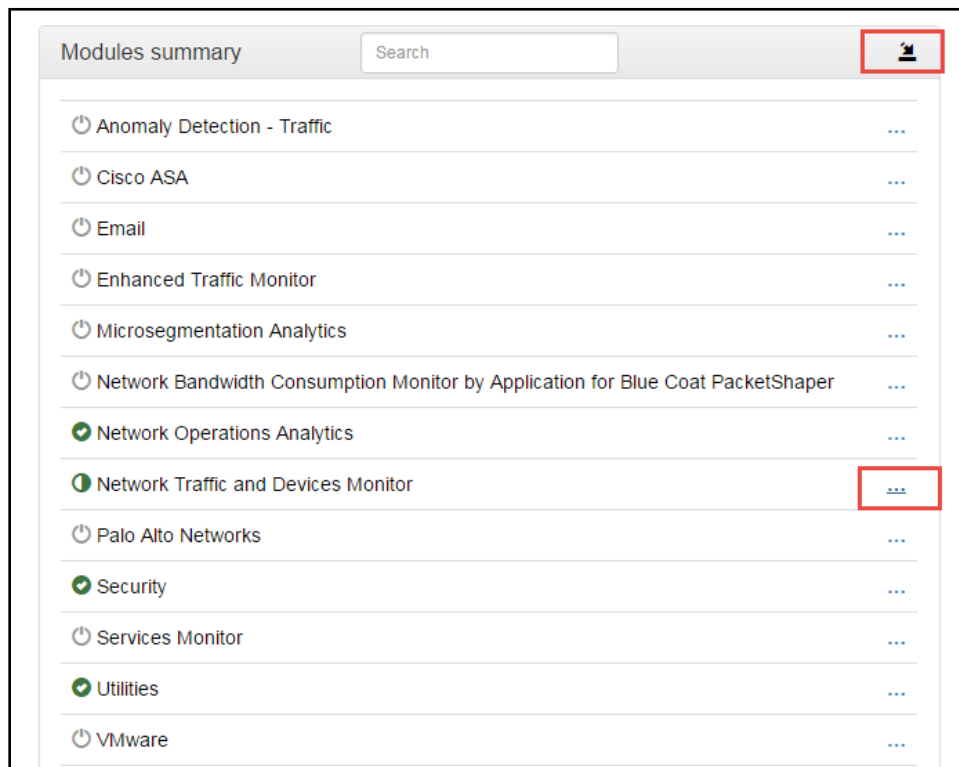
Click on the 'Stop' button  to stop the server


## Restart


Click on the 'Restart' button  to restart the server

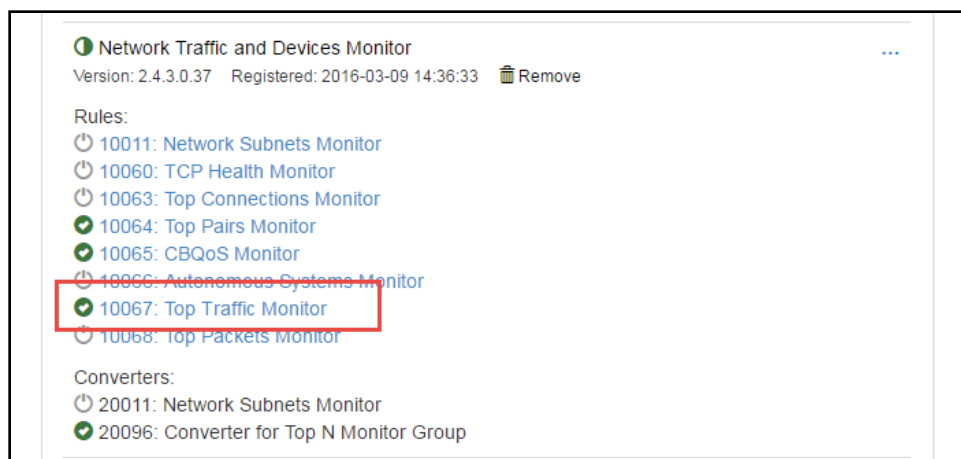
# Enabling and Configuring Modules

By default NetFlow Optimizer is preconfigured with one Module enabled -- Network Traffic and Device Monitor: 10067 Top Traffic Monitor. You may enable / disable the entire set or each Module by clicking on  / 

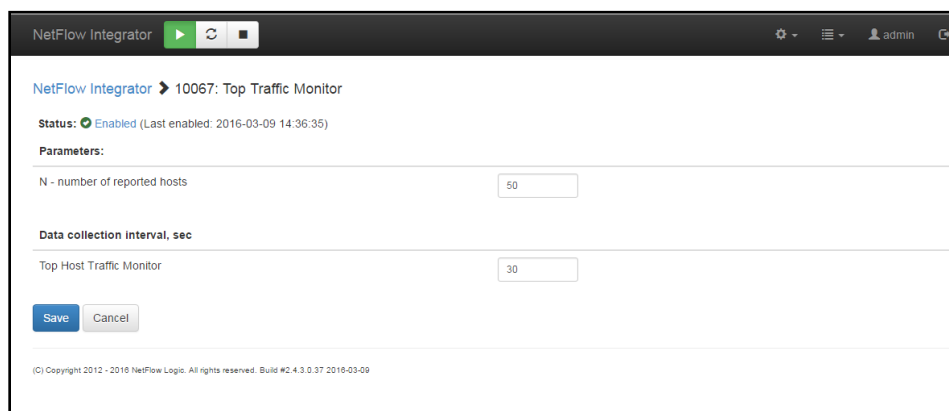


To add or update a Module, click on 'Upload' button .

To configure Module parameters expand Module set  and click on its' name.



## Configure Top Traffic Monitor Module Parameters











Parameter	Description
N – number of reported hosts	The number of top hosts reported per NetFlow exporter, min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Data collection interval, sec	Module logic execution interval, min = 5 sec, max = 86400 sec, default = 300 sec. During this time bytes and packets are summed up in in-memory database by source IP, destination IP, ports, and protocol. At the end of data collection interval the list of consolidated flows is sorted by bytes, and only top N records (1 <sup>st</sup> parameter) are converted to syslog and reported.

See NetFlow Optimizer User Guide for more information on other Modules functionality and configuration.

## Data Sets Summary

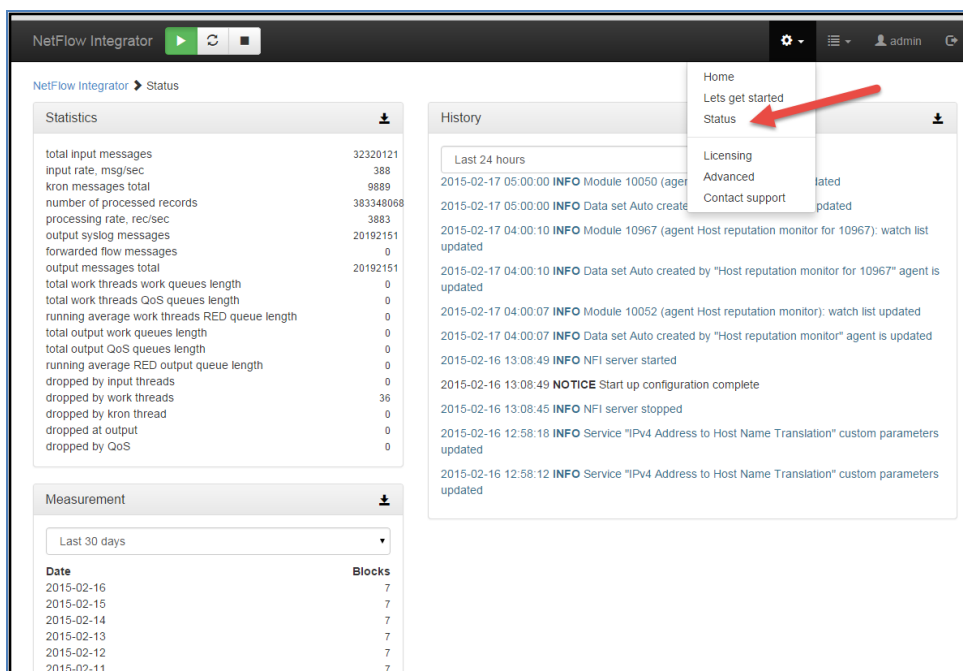
This section contains watch list parameters. Watch lists are created and updated when the corresponding Module is configured.

Data sets summary		
Data set names	Last updated	Module
 10011: Monitored subnet IPv4 address and subnet mask	2014-11-14 23:53:16 	10011
 10040: List of monitored localities	2014-10-13 19:41:49 	10040
 10040: List of watched local subnets and hosts	2014-11-17 14:18:33 	10040
 10052: Known malicious hosts list	2014-12-29 04:00:05 	10052

Some watchlist are created and maintained manually (e.g. Monitored subnet IPv4 address and subnet mask for Module 10011: Network Subnets Monitor), and some can be automatically loaded and updated via External Data Feeder for NFO (e.g. Known malicious hosts list for Module 10052: Host Reputation Monitor).

## Status

This section shows detailed NFO Input / Output statistics, message history, and license usage in Blocks.




The screenshot shows the NetFlow Integrator Status page. The sidebar on the left contains two main sections: 'Statistics' and 'Measurement'. The 'Statistics' section lists various metrics such as total input messages, input rate, and processing rate. The 'Measurement' section shows a table of data for the last 30 days, with columns for 'Date' and 'Blocks'. The main area of the page displays a 'History' log of events, including messages about module updates and server status. A red arrow points to the 'Status' link in the top navigation menu.

The following table contains description and explanation for packet drops. If you see these drop counts, you can find more information in NFO logs.

Drop	Description
dropped by input threads	Total number of packets received by NFO and dropped because they did not pass basic validation tests, e.g. packets are not one of known flow format – NetFlow v5/v9, sFlow, IPFIX, e.t.c. Packets can also be dropped by input threads if NFO is unable to queue them for subsequent processing, e.g. out of memory, queue overflow, e.t.c.

dropped by work threads	The number of packets dropped when flow records is processed by Modules, e.g. there is no NFv9 or IPFIX Template for the flow record, or when there are other problems when processing flows, or when processed flows could not be placed in the Output queue. A small number of these drops is expected when NFO is restarted, while Templates are not yet received.
dropped by kron thread	The number of packets dropped by "Data collection interval" triggers caused by queue overflow.
dropped at output	The number of packets dropped by NFO due to Output queue overflow.
dropped by QoS	The number of packets dropped by NFO internal Quality of Service mechanism to avoid congestions. These drops are also included in one of the drops statistics above.

## Configuring Advanced Features

To access Advanced configuration section click on the gear icon  on the right side of the navigation bar. This section contains several tabs with additional NFO configurations.

### Output Tab

This tab allows you to enable / disable original flow output. When this option is enabled, in addition to output from Modules, all original flow records are also converted to syslog messages one-to-one and sent out. Please note that you may configure a separate destination for this output, such as your Hadoop cluster.

This tab also contains various syslog options.

### Services Tab

This tab allows you to enable and configure NFO built-in services.

#### IPv4 Address to Host Name Translation

This service is using FQDN resolution to enrich your flow data with real-time domain names. This service is enabled by default.

#### Modules state persistence support

This service saves Module state which is used in case NFO server is restarted. It is always enabled and has no configuration parameters.

#### Original Flow Data Converter Service

This service is for Blue Coat Packeteer-2 device. It allows you to map ClassIDs to application names.

#### SNMP Data Retrieval Service

This Service supports protocol version SNMPv2C. It does not support any later versions of the protocol.

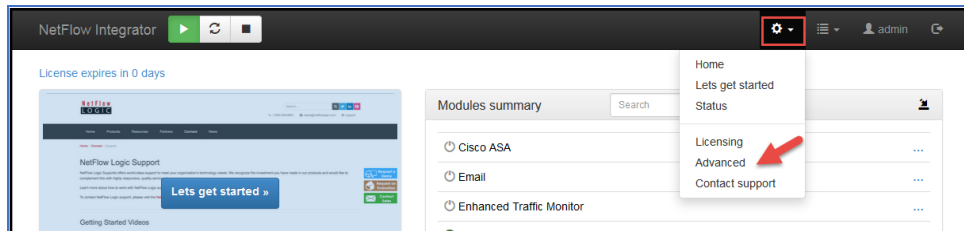
The service is always enabled.



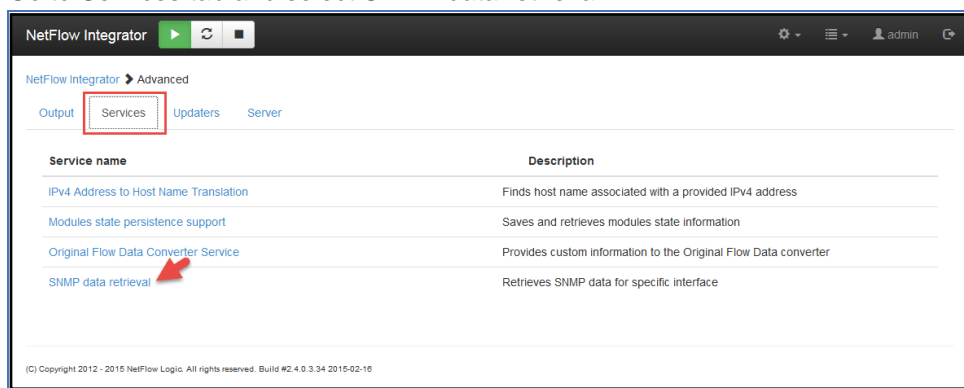
Please note that the Service replies in SNMP index fields to be present in Flow records.

NFO Modules query this Service to get SNMP data, passing Exporter IP and Interface SNMP index as parameters. SNMP information polled from network devices is cached in the Service (OIB + Exporter IP + if SNMP index), until it expires.

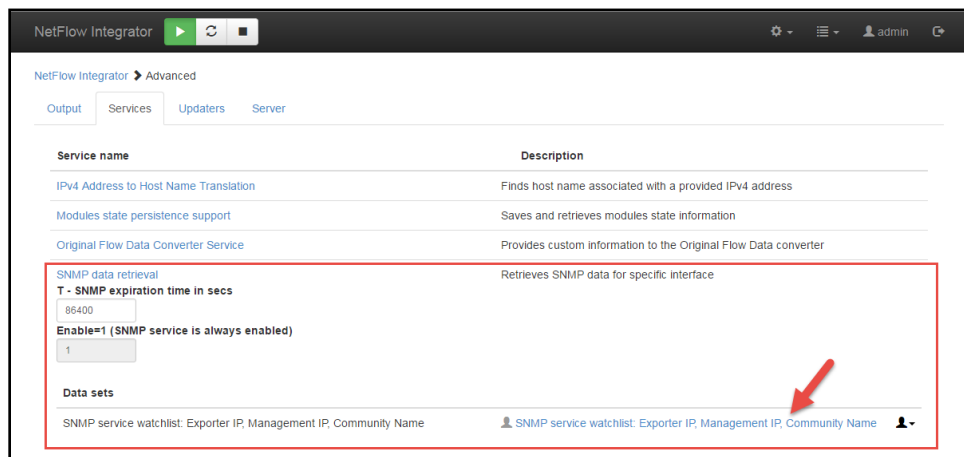
Select Advanced from top left navigation bar:



Go to Services tab and select SNMP data retrieval:



Click on “SNMP service watchlist: Exporter IP, Management IP, Community Name” link:



The service has the following parameters:

- T – SNMP expiration time in secs – expiration time of SNMP data held in cache, default is 86400 seconds (1 day).
- SNMP service watchlist: exporter IP, snmp mgt IP, community string – allows mapping exporter IP address to SNMP management IP address, if different.

Specify IP address pairs – Exporter IP, SNMP Management IP – in data records field or prepare cvs file with Exporter IP, SNMP Management IP, and community string and upload it. Set Community string to "public", if it is left default on network devices.

SNMP service watchlist: exporter IP, SNMP mgmt IP, community name ✕

**Last updated** 2015-07-24 14:53:12 👤 **Download**

**Upload file**    
 \*.csv file [download template](#)  
 Automation is not available.

**Data records**

10.0.5.21, 10.0.3.2, public
10.0.5.22, 10.0.4.2, public
10.0.5.24, 10.0.5.24, public
10.0.5.23, 10.0.5.23, public

The following SNMP OIDs are polled:

1. Interface index (ifIndex) – OID - 1.3.6.1.2.1.2.2.1.1
2. Interface description (ifDescr) - OID 1.3.6.1.2.1.2.2.1.2
3. Interface type (ifType) - OID 1.3.6.1.2.1.2.2.1.3
4. Size of the largest packet (ifMtu) - OID 1.3.6.1.2.1.2.2.1.4
5. Interface bandwidth (ifSpeed), (ifHighSpeed) - OID 1.3.6.1.2.1.2.2.1.5, OID 1.3.6.1.2.1.31.1.1.1.15
6. Interface physical address (ifPhysAddress) - OID 1.3.6.1.2.1.2.2.1.6
7. Desired state of the interface (ifAdminStatus) - OID 1.3.6.1.2.1.2.2.1.7
8. Operational state of the interface (ifOperStatus) - OID 1.3.6.1.2.1.2.2.1.8
9. IP address to which this entry's addressing information pertains (ipAdEntAddr) - OID 1.3.6.1.2.1.4.20.1.1
10. Index value which uniquely identifies the interface to which this entry is applicable (ipAdEntIfIndex) – OID 1.3.6.1.2.1.4.20.1.2
11. Interface InetAddressType (ipAddressAddrType) - OID 1.3.6.1.2.1.4.34.1.1
12. Interface InetAddress (ipAddressAddr) - OID 1.3.6.1.2.1.4.34.1.2
13. The index value that uniquely identifies the interface to which this entry is applicable (ipAddressIfIndex) - OID 1.3.6.1.2.1.4.34.1.3
14. Interface duplex status (dot3StatsDuplexStatus) - OID 1.3.6.1.2.1.10.7.2.1.19

15. An index value that uniquely identifies an interface to an ethernet-like medium (dot3StatsIndex) - OID 1.3.6.1.2.1.10.7.2.1.1

16. Interface name (ifName) - OID 1.3.6.1.2.1.31.1.1.1.1

## NFO Utility Module (10003: SNMP Information Monitor)

This Module queries SNMP information from the Service and sends it out in syslog format as follows:

```
May 22 11:04:51 10.0.5.9 May 22 11:04:51 ff:ff:00:01 nfc_id=20003 exp_ip=10.0.5.21
mgmt_ip=10.0.3.2 sysName=GW02.nfclab ifIndex=2 ifName="Fa0/1"
ifDescr="FastEthernet0/1" ifType=6 ifMtu=1500 ifSpeed=100000000
ifPhysAddress=0016ffffffc7 ifIPAddress=
```

```
May 22 11:04:51 10.0.5.9 May 22 11:04:51 ff:ff:00:01 nfc_id=20003 exp_ip=10.0.5.24
mgmt_ip=10.0.5.24 sysName=HP-E2620-48-upper ifIndex=2 ifName="2" ifDescr="2" ifType=6
ifMtu=1500 ifSpeed=100000000 ifPhysAddress=ffffffecffff ifIPAddress=na
```

The Module has the following configuration parameters:

The screenshot shows the configuration interface for the '10003: SNMP Information Monitor' module. The status is 'Enabled' with a green checkmark, and it was last enabled on 2015-03-07 at 14:30:55. There are two input fields: 'Report SNMP information' set to 300 and 'Refresh SNMP information' set to 3600. At the bottom, there are 'Save' and 'Cancel' buttons. A copyright notice at the very bottom reads: '(C) Copyright 2012 - 2015 NetFlow Logic. All rights reserved. Build #2.4.0.4.15 2015-04-22'.

## Data Feeder Tab

This tab shows External Data Feeder for NFO connected to NFO. You can configure Modules' watch list parameters and frequency of updates here.

The screenshot shows the 'Data Feeder' tab in the NetFlow Integrator. It displays a table with columns for ID, Address, and Host. The first row shows 'updaterUID\_build #2.4.3.0.97' at address '127.0.0.1' on host '127.0.0.1'. Below this, there is a section for 'Agent' and 'Data set' with a 'Last updated' column. The agents listed are 'Geo locations monitor', 'C&C list', 'Host reputation monitor', 'Threat Feeds addresses', and 'Threat Feeds IP blocks'. The data sets listed are '10040: IPv4 address block and country code', '10050: Known C&C hosts (ipv4\_dst\_addr) list', '10052: Known malicious hosts list', '10053: Known Threat Feeds hosts (ipv4\_dst\_addr) list', and '10053: Known Threat Feeds IPv4 address ranges list'. The last updated times are all from 2016-04-26.

ID	Address	Host
updaterUID_build #2.4.3.0.97	127.0.0.1	127.0.0.1

Agent	Data set	Last updated
Geo locations monitor	10040: IPv4 address block and country code	2016-04-26 22:11:44
C&C list	10050: Known C&C hosts (ipv4_dst_addr) list	2016-04-26 22:38:08
Host reputation monitor	10052: Known malicious hosts list	2016-04-26 22:38:39
Threat Feeds addresses	10053: Known Threat Feeds hosts (ipv4_dst_addr) list	2016-04-26 22:12:12
Threat Feeds IP blocks	10053: Known Threat Feeds IPv4 address ranges list	2016-04-26 22:10:31

## Server Tab

This tab allows you to configure additional NFO server parameters, set tracing level, and download logs for issue resolution.

NetFlow Integrator > Advanced

Output Services Updaters **Server**

**NFI Server NFv9 Source ID** (default: FF FF 0 1)

**NFI Server Name** (default: NFI\_SERVER)

**Statistics logging interval, sec**

**Tracing verbosity level**


☐ Keep tracing level after server restart  
☒ Enable restart NFI Server from keep-alive job

**Configuration Info**

Number of NFI input threads	3
Number of NFI work threads	32
Number of NFI output threads	4
Rule modules directory name	/opt/flowintegrator/server/policies
Conversion modules directory name	/opt/flowintegrator/server/converters
NetFlow listener port	6343, 9995, 9997
Logging directory	/opt/flowintegrator/logs
Log rotation frequency	Daily
Log files count	10
Maximal log file size, KB	20000
Tracing verbosity level	0
NFC server version	2.4.3.0.37
QoS queue maximum size	2000

**Save** **Cancel** **Download logs**

## Admin

To access the User management section click on the icon  located on in the top right of the navigation bar. Here you can change *admin* password, enable Active Directory authentication, or configure two factor authentication based on x509 v3 certificate.

## Change Password

To change the password

**Change Password**

**Old password**

**New password**

**Confirm new password**

**Save** **Cancel**

1. Enter the Old Password
2. Enter the New Password, Confirm the New Password
3. Click 'Save'

## Forgot Password

In order to reset admin password you will require root or administrator access to the system where NetFlow Optimizer is installed. The password will be reset back to 'changeme'. To reset admin login password perform the following:

1. Go to the directory where the password file is stored

Windows: C:\Program Files\NetFlow Logic\NetFlow Optimizer\tomcat\data

Linux: /opt/flowintegrator/tomcat/data



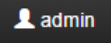
2. Delete the following file: `nf2sl_password`
3. Restart NFO Tomcat service

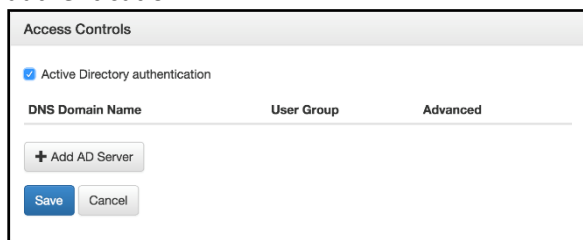
Windows: Restart NFO Tomcat using Windows Services

Linux: `/etc/init.d/tomcat_nfo restart`

## Active Directory Authentication

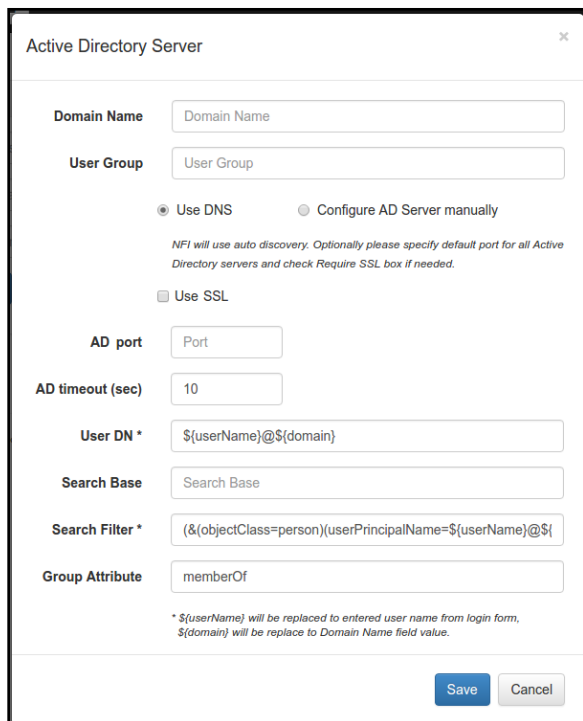
### Procedure

1. Click on  icon on the right side of the navigation bar and check Active directory authentication



The 'Access Controls' dialog box shows the 'Active Directory authentication' checkbox checked. Below it, there are tabs for 'DNS Domain Name', 'User Group', and 'Advanced'. An '+ Add AD Server' button is visible on the left, along with 'Save' and 'Cancel' buttons at the bottom.

2. Click on Add AD Server button



The 'Active Directory Server' configuration dialog box contains the following fields and options:

- Domain Name:** Text input field.
- User Group:** Text input field.
- Configuration Method:** Radio buttons for 'Use DNS' (selected) and 'Configure AD Server manually'.
- AD port:** Text input field with 'Port' as a placeholder.
- AD timeout (sec):** Text input field with '10' as a value.
- User DN \*:** Text input field with the placeholder `${userName}@${domain}`.
- Search Base:** Text input field with 'Search Base' as a placeholder.
- Search Filter \*:** Text input field with the placeholder `(&(objectClass=person)(userPrincipalName=${userName}@${domain}))`.
- Group Attribute:** Text input field with 'memberOf' as a placeholder.

At the bottom, there are 'Save' and 'Cancel' buttons. A footnote at the bottom states: *\* \${userName} will be replaced to entered user name from login form, \${domain} will be replace to Domain Name field value.*

3. Specify Domain Name
4. Specify User Group
5. Select "Use DNS" or "Configure AS Server manually"

6. Check “Use SSL” if needed
7. If “Configure AS Server manually” is selected, specify AD host name or IP address
8. Specify AD port

9. Press ‘Save’ button to save your settings



The following steps are required if SSL is enabled:

1. Export AD certificate or root CA. Also AD certificate can be exported using following commands:

Linux: `echo | openssl s_client -connect <address>:<port> 2>&1 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' | cat > AD.crt`

Where <address> and <port> are AD server address and port respectively. Default AD server port for SSL connections is 636 or 3269. Certificate is stored into AD.crt file and can be read using following command:

Windows: `C:\Program Files\NetFlow Logic\NetFlow Optimizer\java\jre8\bin\keytool.exe -printcert -file AD.crt`

Linux: `/opt/flowintegrator/java/jre8/bin/keytool -printcert -file AD.crt`

2. Import AD certificate or root CA into Java Runtime trusted keystore. Keystore has default password changeit.

Windows: `C:\Program Files\NetFlow Logic\NetFlow Optimizer\java\jre8\bin\keytool.exe -import -trustcacerts -alias ADName -file AD.crt -keystore C:\Program Files\NetFlow Logic\NetFlow Optimizer\java\jre8\jre\lib\security\cacerts -storepass changeit`

```
Linux: /opt/flowintegrator/java/jre8/bin/keytool -import -trustcacerts -alias ADName  
-file AD.crt -keystore /opt/flowintegrator/java/jre8/jre/lib/security/cacerts -  
storepass changeit
```

Where *ADName* and *AD.crt* are certificate name and file name respectively.

3. Restart NFO Tomcat if certificate has been imported

Windows: Restart NFO Tomcat using Windows Services

Linux: `/etc/init.d/tomcat_nfo restart`



**For troubleshooting** please check `logs/nf2sl.log`. Logs trace level can be changed in the `/opt/flowintegrator/tomcat/webapps/ROOT/WEB-INF/classes/log4j.xml` file. Following lines should be added after last `<category>` section and before `<root>` section:

```
<category name="com.netflowlogic.nf2sl.service.security.ADAuthenticationProvider">  
  <priority value="TRACE" />  
</category>
```

Restart NFO Tomcat after changing trace level.

## Two Factor Authentication (2FA)

If your organization requires Two Factor Authentication to support certificate policies for administrators, you can configure it using x509 Authentication panel.

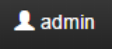
Please contact [support@netflowlogic.com](mailto:support@netflowlogic.com) for detailed instructions.

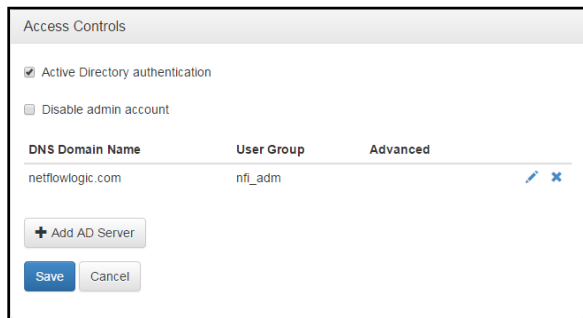
## Disabling Admin Account

Once Active Directory Integration is configured, you can optionally disable the *admin* account.

### Procedure

To disable *admin* account perform the following:

1. Click on  icon on the right side of the navigation bar and check Active directory authentication



Access Controls

☒ Active Directory authentication

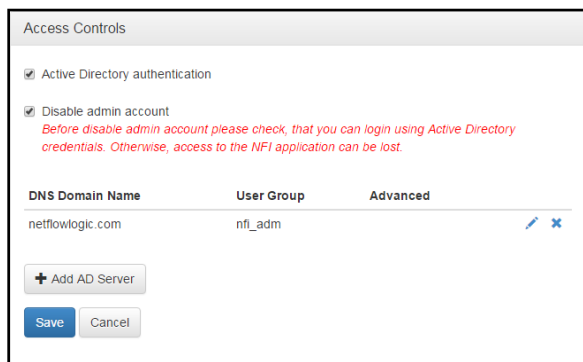
☐ Disable admin account

DNS Domain Name	User Group	Advanced
netflowlogic.com	nfi_admin	<a href="#">edit</a> <a href="#">delete</a>

[+ Add AD Server](#)

[Save](#) [Cancel](#)

2. Select Disable admin account



Access Controls

☒ Active Directory authentication

☒ Disable admin account

*Before disable admin account please check, that you can login using Active Directory credentials. Otherwise, access to the NFI application can be lost.*


DNS Domain Name	User Group	Advanced
netflowlogic.com	nfi_admin	<a href="#">edit</a> <a href="#">delete</a>

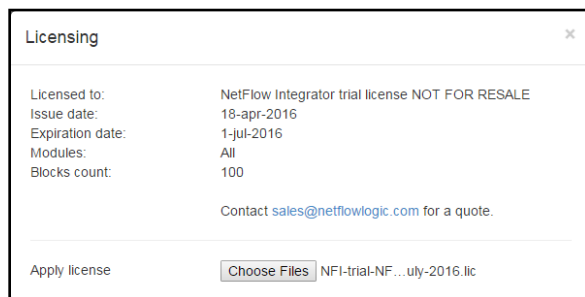
[+ Add AD Server](#)

[Save](#) [Cancel](#)

3. Press 'Save' button to save your settings

## Licensing

The licensing page displays information about the license for NetFlow Optimizer. To access the licensing page go to top navigation bar, select gear icon  > Licensing



Licensing

Licensed to:	NetFlow Integrator trial license NOT FOR RESALE
Issue date:	18-apr-2016
Expiration date:	1-jul-2016
Modules:	All
Blocks count:	100

Contact [sales@netflowlogic.com](mailto:sales@netflowlogic.com) for a quote.

Apply license [Choose Files](#) NFI-trial-NF...uly-2016.lic

The Licensing page displays the following information

## License Details

Licensed to: The organization the license was issued and the license type

Issue date: The date the license was issued by NetFlow Logic support

Expiration date: The date the license will expire

Blocks count: The number of blocks available for use with the license (a single block is 1000 records per second)

## Apply a License

To apply a new license perform the following from the licensing page

1. Click on the 'Choose Files' button
2. Select the license file
3. Click Ok to apply the license

## Server Configuration Parameters

There are several additional NetFlow Optimizer parameters located in `<nfo_home>/server/etc/server.cfg` file. You have to restart NetFlow Optimizer if you change them. Please contact us at <https://www.netflowlogic.com/connect/support/> if you need assistance.

```
TRACE_ERR
LOG_DIR ../logs
LOG_ROT_DIR ../logs/bak
LOG_ROT_DAILY
LOG_COUNT 10
LOG_FILE_SIZE_KB 20000
SVR_ID NFI_SERVER
NF_PORT 9995
TIME_ZONE GMT
OFD_OUTPUT JSON
```

## Linux kernel settings for high-volume processing

The default Linux kernel settings are not sufficient for high-volume packet rate. This can lead to dropped packets and data loss. We recommend that you change both the receive buffer in NFO and the socket read buffer size in Linux kernel.

To change the receive buffer to `<N>` bytes, add the following string to `<nfo_home>/server/etc/server.cfg`:

```
IT_RCVBUF <N>
```

The valid values for parameter N are 124928 through 56623104. The default value is 12582912.

To change the socket read buffer size in Linux kernel to `<N>` bytes for current session, execute (under root privileges) `sysctl -w net.core.rmem_max N` in a console. To make this change persistent, add the following string to `/etc/sysctl.conf`:

```
net.core.rmem_max=<N>
```

Then run the following command to reload the settings from the file:

```
sysctl -p
```

To check what the socket read buffer size is currently used, execute the following command:

```
sysctl net.core.rmem_max.
```

## Notes:

1. NFO effectively uses the least size of those buffers.
2. NFO Virtual Appliance has the socket read buffer size 12582912 -- the default value for NFO receive buffer.

## Secure Connection Configuration (HTTPS)

This section describes how to install a certificate from a Certificate Authority into Tomcat. Self-signed certificate is already installed in `$NFO_HOME/tomcat/conf/.tomcat_keystore`, the keystore password is "password" and private key password is the same.

If you want to replace self-signed certificate to a new one from a Certificate Authority, use following steps from <http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html>

HTTPS parameters are configured in the `tomcat/conf/server.xml` configuration file (Connector section). All Connector attributes are described here: <https://tomcat.apache.org/tomcat-7.0-doc/config/http.html>. If keystore path or password are changed, corresponding Connector attributes should be modified.

## Create a local Certificate Signing Request (CSR)

In order to obtain a Certificate from the Certificate Authority of your choice you have to create a so called Certificate Signing Request (CSR). That CSR will be used by the Certificate Authority to create a Certificate that will identify your website as "secure". To create a CSR follow these steps:

- Delete preinstalled self-signed certificate:

```
$NFO_HOME/java/jre8/jre/bin/keytool -delete -alias tomcat \
    -keystore $NFO_HOME/tomcat/conf/.tomcat_keystore
```

- Create a local Certificate:

```
$NFO_HOME/java/jre8/jre/bin/keytool -keysize 2048 -genkey -alias tomcat \
    -keyalg RSA -keystore $NFO_HOME/tomcat/conf/.tomcat_keystore
```

Note: In some cases you will have to enter the domain of your website (i.e. `www.domain.org`) in the field "first- and lastname" in order to create a working Certificate.

- The CSR is then created with:

```
$NFO_HOME/java/jre8/jre/bin/keytool -certreq -keyalg RSA -alias tomcat \
    -file certreq.csr -keystore $NFO_HOME/tomcat/conf/.tomcat_keystore
```

Now you have a file called `certreq.csr` that you can submit to the Certificate Authority (look at the documentation of the Certificate Authority website on how to do this). In return you get a Certificate.

## Import the Certificate

Now that you have your Certificate you can import it into your local keystore. First of all you have to import a so called Chain Certificate or Root Certificate into your keystore. After that you can proceed with importing your Certificate.

- Download a Chain Certificate from the Certificate Authority you obtained the Certificate from.  
For Verisign.com commercial certificates go to: <http://www.verisign.com/support/install/intermediate.html>  
For Verisign.com trial certificates go to: [http://www.verisign.com/support/verisign-intermediate-ca/Trial\\_Secure\\_Server\\_Root/index.html](http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html)  
For Trustcenter.de go to: <http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>  
For Thawte.com go to: <http://www.thawte.com/certs/trustmap.html>

- Import the Chain Certificate into your keystore

```
$NFO_HOME/java/jre8/jre/bin/keytool -import -alias root \
  -keystore $NFO_HOME/tomcat/conf/.tomcat_keystore \
  -trustcacerts -file <filename_of_the_chain_certificate>
```

- And finally import your new Certificate

```
$NFO_HOME/java/jre8/jre/bin/keytool -import -alias tomcat \
  -keystore $NFO_HOME/tomcat/conf/.tomcat_keystore \
  -file <your_certificate_filename>
```



Please see Import the Certificate into External Data Feeder for NFO truststore section on page 40 in *External Data Feeder for NFO Getting Started Guide* for additional information.

## Copying NFO Configuration

This section describes how to copy NFO configuration from machine A to B. We assume that NFO is already installed and configured on machine A. NFO stores all configuration, including Module's parameters, in the installation directory, so it can be simply copied from machine A to B.

### Procedure

Use the following steps to do this on Linux:

On machine A:

1. Stop Tomcat service: `/etc/init.d/tomcat_nfo stop`
2. Create copy of installation: `tar -czf flowintegrator_copy.tar.gz /opt/flowintegrator`
3. Start Tomcat service: `/etc/init.d/tomcat_nfo start`
4. Copy `flowintegrator_copy.tar.gz` to B.

On machine B:

5. Install same version of NFO as on A. Don't configure NFO.
6. Stop Tomcat service: `/etc/init.d/tomcat_nfo stop`
7. Remove all NFO files: `rm -rf /opt/flowintegrator`
8. Extract copy of NFO: `tar -xzf flowintegrator_copy.tar.gz /opt/`
9. If Tomcat on B should use different SSL certificate, reconfigure it.
10. Start Tomcat service: `/etc/init.d/tomcat_nfo start`
11. Check that Tomcat has been started and has same configuration as on machine A.

# External Data Feeder for NFO Getting Started Guide

---

Depending on your requirements NetFlow Optimizer and External Data Feeder for NFO can be installed on the same server or separately. If you are going to use NFO NetFlow enhancement functionality, such as GeoIP resolution, Cyber Security Threat Lists – External Data Feeder for NFO must be installed on the server with Internet access, so it can access and provide NFO with information generally unavailable in the data streams supplied by NetFlow/IPFIX exporters. External Data Feeder for NFO is administered through NetFlow Optimizer GUI.

## Before You Install External Data Feeder for NFO

### Pre-Installation Checklist

Please be sure to have the following before you begin the installation of the External Data Feeder for NFO software:

- You have to login as root for Linux and administrator for Windows installations and updates
- You have successfully installed NetFlow Optimizer and you know its IP address

### Minimum Requirements

NetFlow Logic distributes External Data Feeder for NFO as RPM or TAR.GZ for Linux, or as EXE for Windows.

### Supported Platforms

You can install the NetFlow Optimizer virtual appliance or software on a platform with the following specifications.

Specification	Details
Linux	Linux kernel 2.6+ on <ul style="list-style-type: none"><li>- CentOS 5.5, 6.5, 6.7, 7</li><li>- Debian 6.0</li><li>- RHEL 5.5, 6.5, 6.7, 7</li><li>- SUSE ES 11</li></ul>
Windows	Windows 2008 R2, 2012, and 2012 R2 (64-bit)
CPU, Memory, Disk Space	<ul style="list-style-type: none"><li>- CPU: Min 4 CPU cores (8 CPU cores for higher performance)</li><li>- Memory: 2 GB</li><li>- Disk Space: 2 GB</li></ul>

### Required Network Ports

The following network ports must be allowed for outbound connections.



Port	Protocol
80/TCP	External Data Feeder for NFO Agents Internet communication
8443/TCP	NetFlow Optimizer communication

## Required Internet Destinations

The following Internet destinations must be allowed for outbound http-connections.

URL	Agent
<a href="http://rules.emergingthreats.net/">http://rules.emergingthreats.net/</a>	C&C list
<a href="http://geolite.maxmind.com/">http://geolite.maxmind.com/</a>	Geo locations monitor
<a href="http://reputation.alienvault.com/">http://reputation.alienvault.com/</a>	Host reputation monitor
<a href="http://www.dshield.org/">http://www.dshield.org/</a>	Threat Feeds addresses
<a href="http://feeds.dshield.org/">http://feeds.dshield.org/</a>	Threat Feeds IP blocks

# Installing External Data Feeder for NFO

If you installed several instances of NFO, you need to install External Data Feeder for NFO for each NetFlow Optimizer instance.

## Linux RPM Installation

Download the External Data Feeder for NFO RPM package.

### Procedure

To begin the RPM installation of External Data Feeder for NFO in the default directory `/opt/nfi-updater` perform the following:

Open a shell prompt and enter the following command to begin the installation

```
rpm -ihv <RPM-package>
```

To begin the RPM installation of External Data Feeder for NFO in another directory, perform the following:

Open a shell prompt and enter the following command to begin the installation

```
rpm -ihv --relocate /opt=<new-path> <RPM-package>
```



If External Data Feeder for NFO is installed on a separate server, change `uri` parameter in `updater.properties` file located in `/opt/nfi-updater/conf` to IP address of NetFlow Optimizer:  
`uri = https://<nfo-host>:8443`

## What to do next

A message will display indicating that the External Data Feeder for NFO installation has been successfully completed.

- Verify that NetFlow Optimizer and External Data Feeder for NFO are connected by going to `NetFlow Optimizer > Advanced > Updaters`
- Change default `updater` user's password. Login into NetFlow Optimizer using `updater/changeme` credentials and change the password. See Authentication Configuration section on page 38 for more information.
- If you require Proxy Server authentication before External Data Feeder for NFO can access external URLs, see *Proxy Server Configuration* section on page 41 for further instructions.

## Linux TAR Installation

Download the External Data Feeder for NFO TAR package.

### Procedure

To begin the TAR installation of External Data Feeder for NFO in the default directory `/opt/nfi-updater` perform the following:

1. Open a shell prompt and enter the following command to un-compress the installer  

```
tar zxvf <TAR-package> -C /opt/nfi-updater
```
2. Go to the `/opt/nfi-updater` directory and enter the following command to begin the installation  

```
setup.sh -i
```

To begin the TAR installation of External Data Feeder for NFO in another directory, perform the following:

1. Open a shell prompt and enter the following command to un-compress the installer  

```
tar zxvf <TAR-package> -C <directory>
```
2. Go to the directory and enter the following command to begin the installation  

```
setup.sh -i
```



If External Data Feeder for NFO is installed on a separate server, change `uri` parameter in `updater.properties` file located in `/opt/nfi-updater/conf` to IP address of NetFlow Optimizer:  
`uri = https://<nfo-host>:8443`

## What to do next

A message will display indicating that the External Data Feeder for NFO installation has been successfully completed.

- Verify that NetFlow Optimizer and External Data Feeder for NFO are connected by going to `NetFlow Optimizer > Advanced > Updaters`
- Change default `updater` user's password. Login into NetFlow Optimizer using `updater/changeme` credentials and change the password. See Authentication Configuration section on page 38 for more information.

- If you require Proxy Server authentication before External Data Feeder for NFO can access external URLs, see *Proxy Server Configuration* section on page 41 for further instructions.

## Windows Installation

Download the External Data Feeder for NFO Windows installation package.

### Procedure

To begin the Windows installation of External Data Feeder for NFO perform the following:


1. Open the installation file and click 'Run' to launch the installer and Click 'Next' To begin the 'External Data Feeder for NFO Setup'



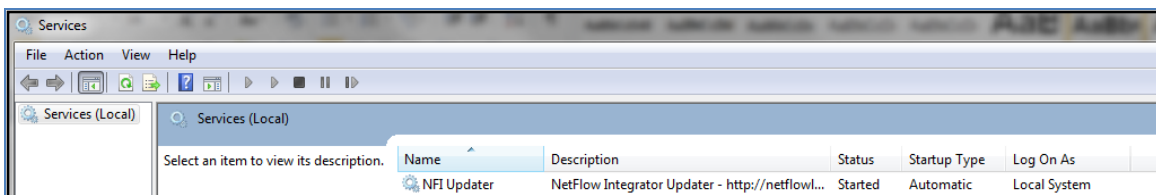
2. Click 'Next' to install External Data Feeder for NFO in the default location:

C:\Program Files\NetFlow Logic\NFI Updater

3. Click on 'Install' To begin the installation (follow the installation steps)
4. Click on 'Finish' to complete the installation and exit the installer

5.  If External Data Feeder for NFO is installed on a separate server, change uri parameter in `updater.properties` file located in C:\Program Files\NetFlow Logic\NFI Updater\conf to IP address of NetFlow Optimizer  
`uri = https://<nfo-host>:8443`

6. Use Windows Services to check External Data Feeder for NFO status



### What to do next

- Verify that NetFlow Optimizer and External Data Feeder for NFO are connected by going to NetFlow Optimizer > Advanced > Updaters
- Change default updater user's password. Login into NetFlow Optimizer using `updater/changeme` credentials and change the password. See Authentication Configuration section on page 38 for more information.

- If you require Proxy Server authentication before External Data Feeder for NFO can access external URLs, see *Proxy Server Configuration* section on page 41 for further instructions.

# Upgrading External Data Feeder for NFO

You upgrade a single instance of External Data Feeder for NFO by installing the latest version over your existing installation. During the upgrade the installer package preserves all External Data Feeder for NFO configurations, except configuration files changed manually. These files, if changed, are backed up into `conf-backup.<date>.tar.gz` file (<date> is archive date), and should be restored manually, if necessary.

The following is a list of some configuration files.

File	Purpose
<code>\$updater_home/conf/updater.properties</code>	NetFlow Intergrator URI and other parameters
<code>\$updater_home/conf/.updater_keystore</code>	Default self-signed certificate
<code>\$updater_home/java/jre8/jre/lib/security/cacerts</code>	Trusted certificates imported into Java Runtime cacerts keystore



After upgrade, validate default configuration and restore from the backup if it is required.  
If you didn't modify these files, ignore the caution.

When upgrading External Data Feeder for NFO on RHEL 7, the messages like these might be displayed:

```
Cleaning up / removing...
2:nfi-updater-2.4.0.3.34-linux      warning: file /opt/nfi-updater/lib/wasync-
1.4.0.jar: remove failed: No such file or directory
warning: file /opt/nfi-updater/lib/netty-3.9.2.Final.jar: remove failed: No such file
or directory
warning: file /opt/nfi-updater/lib/async-http-client-1.8.11.jar: remove failed: No
such file or directory
```

This is a normal situation and these messages should be ignored.

## Upgrading the External Data Feeder for NFO RPM Installation

### Procedure

To begin the upgrade of External Data Feeder for NFO perform the following:

1. Login directly or SSH and copy the new installation file into the `/opt` installation directory
2. Backup configuration files from `/opt/nfi_updater/conf` folder before installation
3. RPM the NetFlow Optimizer for Linux installation file into the `/opt` installation directory  
`rpm -Uhv <RPM-package>`
4. Restore configuration files from step 2 and restart External Data Feeder for NFO service:  
`/etc/init.d/nfi_updd restart`

## What to do next

A message will display indicating that the External Data Feeder for NFO installation has been successfully completed.

- Verify the version (Release number) of External Data Feeder for NFO by going to `NetFlow Optimizer > Advanced > Updaters`

# Upgrading the External Data Feeder for NFO TAR Installation

## Procedure

To begin the upgrade of External Data Feeder for NFO perform the following:

1. Login directly or SSH and copy the new installation file into the `/opt` installation directory
2. Backup configuration files from `/opt/nfi_updater/conf` folder before installation
3. Enter the following command to begin the uninstall  
`setup.sh -u`
4. Copy the upgrade installation package for Linux into the existing installation directory
5. Open a shell prompt and enter the following command to un-compress the installer  
`tar zxvf <TAR-package> -C <directory>`
6. Restore configuration file from step 2
7. Enter the following command and begin the setup  
`setup.sh -i`

## What to do next

A message will display indicating that the External Data Feeder for NFO installation has been successfully completed.

- Verify the version (Release number) of External Data Feeder for NFO by going to `NetFlow Optimizer > Advanced > Updaters`

# Upgrading the External Data Feeder for NFO Windows Installation

## Procedure

To begin the upgrade of External Data Feeder for NFO perform the following:

1. Backup configuration files from `C:\Program Files\NetFlow Logic\NFI Updater\conf` folder before installation
2. Open the upgrade installation file and click 'Run' to launch the installer and Click 'Next' To begin the 'External Data Feeder for NFO Setup'

3. Click 'Next' to install External Data Feeder for NFO in the default location:  
`C:\Program Files\NetFlow Logic\NFI Updater`
4. Click on 'Install' To begin the upgrade (follow the installation steps)
5. Click on 'Finish' to complete the installation and exit the installer
6. Restore configuration files from step 1 and restart External Data Feeder for NFO Windows Service.

# Removing External Data Feeder for NFO

## Removing the External Data Feeder for NFO RPM Installation

### Procedure

To remove External Data Feeder for NFO perform the following:

1. Open a shell prompt and enter the following command to begin the uninstall  
`rpm -e nfi-updater`
2. Remove the install path if the full uninstall needed  
`rm -rf <directory>`

## Removing the External Data Feeder for NFO TAR Installation

### Procedure

To remove External Data Feeder for NFO perform the following:

1. Go to the existing installation directory and enter the following command to begin the uninstall  
`setup.sh -u`
2. Leave the installation directory  
`cd ..`
3. Remove the install path if the full uninstall needed  
`rm -rf <directory>`

## Removing the External Data Feeder for NFO Windows Installation

### Procedure

To remove External Data Feeder for NFO perform the following:

1. Go to Control Panel > Programs > Programs and Features and select the External Data Feeder for NFO program.
2. Follow the steps to uninstall the program.

# External Data Feeder for NFO Administration Guide

---

## Configuring External Data Feeder for NFO

If you install several instances of External Data Feeder for NFO you can configure the first instance, and then copy configuration from the first instance to another one. Please see Copying External Data Feeder for NFO Configuration section on page 41 for details.

### Verifying External Data Feeder for NFO Status

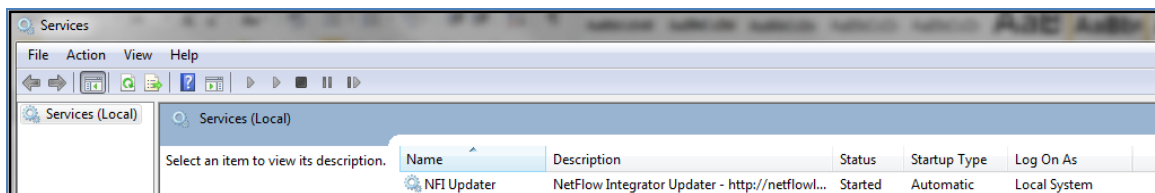
#### Verifying External Data Feeder for NFO Linux Installation Procedure

To verify if External Data Feeder for NFO is running perform the following:

1. Enter the following command to check the status  
`/etc/init.d/nfi_updd status`
2. For the list of available commands enter the following  
`/etc/init.d/nfi_updd`

#### Verifying External Data Feeder for NFO Windows Installation Procedure

Use Windows Services to check External Data Feeder for NFO status



## Authentication Configuration

External Data Feeder for NFO is authenticated to NetFlow Optimizer as `updater` user. This user has only access to a data set maintenance and the ability to change password. This user can login using X509 certificate or using user/password authentication method. Default password for this user is `changeme`. Please change it after the installation.

By default External Data Feeder for NFO logs into NetFlow Optimizer using X509 certificate. We highly recommend changing default self-signed certificate to a new one or switching to a user/password authentication method. In any case default password changing is required.

## X509 authentication

### Procedure

Create a Certificate Signing Request (CSR) with `keytool` and generate a Signed Certificate for the CSR:

1. Delete previous certificate:

```
$UPD_HOME/java/jre8/bin/keytool -delete -alias updater -storepass  
password -keystore $UPD_HOME/conf/.updater_keystore  
  
$NFO_HOME/java/jre8/bin/keytool -delete -alias updater -storepass password  
$NFO_HOME/tomcat/conf/.trust_keystore
```

2. Generate the key pair:

```
$UPD_HOME/java/jre8/bin/keytool keytool -genkey -alias updater -dname  
"CN=updater, OU=, O=, L=, ST=, C=" -validity 365 -keyalg RSA -keysize  
1024 -storepass password -keypass password -keystore  
  
$UPD_HOME/conf/.updater_keystore
```

3. Generate the Certificate Signing Request:

```
$UPD_HOME/java/jre8/bin/keytool -certreq -alias updater -keyalg rsa -storepass  
password -keystore $UPD_HOME/conf/.updater_keystore -file updater.csr
```

4. Generate a signed certificate for the associated Certificate Signing Request.

5. Import the CA certificate into the NetFlow Optimizer keystore:

```
$NFO_HOME/java/jre8/bin/keytool -import -alias root -file CA.crt -  
keystore -storepass password $NFO_HOME/tomcat/conf/.trust_keystore
```

6. Import the signed certificate for the associated updater alias in the keystore:

```
$NFO_HOME/java/jre8/bin/keytool -import -alias updater -file  
updater.crt -keystore -storepass password $NFO_HOME/tomcat/conf/.trust_keystore
```

Self-Signed certificate can be exported instead of steps 3-5:

```
$UPD_HOME/java/jre8/bin/keytool -export -alias updater -storepass  
password -keystore $UPD_HOME/conf/.updater_keystore -file updater.crt
```

### Notes:

1. Certificate **CN** field value must be **updater**.
2. If keystore type, keystore password, key password or key algorithm were changed, these changes have to be added to the `$UPD_HOME/conf/updater.properties` file:

```
keystoreFile = ../conf/.updater_keystore  
keystoreType = jks  
keystorePass = password  
keyPass      = password
```



```
keyAlgorithm = SunX509
```

## User/password authentication

### Procedure

Username/password authentication can be enabled by commenting certificate-related properties and adding following lines into `updater.properties`:

```
user = updater
password = changeme
# keystoreFile = ../conf/.updater_keystore
# keystoreType = jks
# keystorePass = password
# keyPass      = password
# keyAlgorithm = SunX509
```

User password can be changed in the NetFlow Optimizer: login as `updater` user, go to “admin” section, and enter old password (`changeme`) and a new password.

## Import the Certificate into External Data Feeder for NFO truststore

NFO and External Data Feeder for NFO use secure connection (https) for communication. Tomcat certificate and root chain are imported automatically into `$UPD_HOME/conf/.updater_truststore` during first connection. If tomcat certificate is changed, it should be reimported into `.updater_truststore` file manually or `.updater_truststore` can be removed (it will be recreated after External Data Feeder for NFO service restart).

### Procedure

To reimport the certificate perform the following:

1. Enter the following commands to delete previous certificate(s):
  - a. Get list of current trusted certificates:

```
$UPD_HOME/java/jre8/jre/bin/keytool -list -keystore $UPD_HOME/conf/.updater_truststore
```
  - b. Delete all certificates from the previous step:

```
$UPD_HOME/java/jre8/jre/bin/keytool -delete -alias <crtAlias> -keystore $UPD_HOME/conf/.updater_truststore
```
2. Enter the following command to import the chain certificate into the External Data Feeder for NFO truststore:

```
# $UPD_HOME/java/jre8/jre/bin/keytool -import -alias root -keystore $UPD_HOME/conf/.updater_truststore -trustcacerts -file rootCA.crt
```
3. Enter the following command to import tomcat certificate into the External Data Feeder for NFO truststore:

```
# $UPD_HOME/java/jre8/jre/bin/keytool -import -alias tomcat -keystore $UPD_HOME/conf/.updater_truststore -file srv.crt
```
4. After these actions External Data Feeder for NFO service should be restarted.

### What to do next

If certificate is imported automatically (`.updater_truststore` created automatically), certificate fingerprint (md5) can be verified using following command:

```
$UPD_HOME/java/jre8/jre/bin/keytool -list -keystore $UPD_HOME/conf/.updater_truststore
```


.updater\_truststore type, password and path configuration can be changed in the \$UPD\_HOME/conf/updater.properties file.

## Proxy Server Configuration

External Data Feeder for NFO could be configured to use Proxy Server authentication before it can access external URLs.

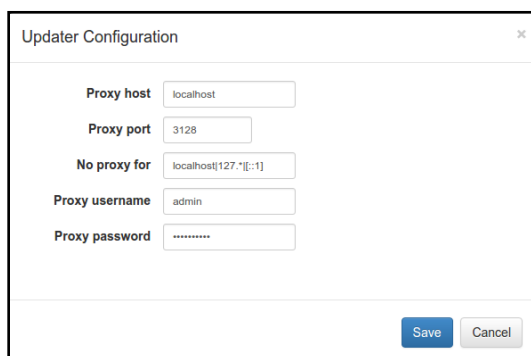
### Procedure

To setup External Data Feeder for NFO Proxy Server configuration perform the following:

1. Click on the gear icon  on the right side of the navigation bar, select Advanced and Data Feeders tab



2. Click on Configuration and specify your Proxy Server parameters



3. Press 'Save' button to save your settings

## Copying External Data Feeder for NFO Configuration

This section describes how to copy External Data Feeder for NFO configuration from machine A to B. We assume that External Data Feeder for NFO is already installed and configured on machine A. External Data Feeder for NFO stores all configuration in the installation directory and in the NFO data base, so it can be simply copied from machine A to B.

### Procedure

Use the following steps to do this on Linux:

On machine A:

1. Stop External Data Feeder for NFO service: `/etc/init.d/nfi_updd stop`
2. Create copy of installation: `tar -czf NFO-updater_copy.tar.gz /opt/nfi-updater`

3. Start External Data Feeder for NFO service: `/etc/init.d/nfi_updd start`
4. Copy `NFO-updater_copy.tar.gz` to B.

On machine B:

5. Install same version of External Data Feeder for NFO as on A. Don't configure External Data Feeder for NFO.
6. Stop External Data Feeder for NFO service: `/etc/init.d/nfi_updd stop`
7. Remove all External Data Feeder for NFO files: `rm -rf /opt/nfi-updater`
8. Extract copy of External Data Feeder for NFO: `tar -xzf nfi-updater_copy.tar.gz /opt/`
9. If External Data Feeder for NFO on B should use different client certificate or tomcat has different certificate, reconfigure `.updater_keystore` or `.updater_truststore` respectively.
10. If NFO and External Data Feeder for NFO are installed on different machines, set `uri` property in the `/opt/nfi-updater/conf/updater.properties` file.
11. Start External Data Feeder for NFO service: `/etc/init.d/nfi_updd start`
12. Check that External Data Feeder for NFO has been started (see Status -> History panel in the GUI, logs should contain line like *INFO [updater] Updater <updaterUID> (x.x.x.x.x) connected*).