NetFlow Optimizer™

Installation and Administration Guide

Version 2.4.9 (Build 2.4.9.0.3)

May 2017

Contents

NetFlow Optimizer Installation Guide

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.

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
- 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 - CentOS 5.5, 6.5, 6.7, 7 - Debian 6.0 - RHEL 5.5, 6.5, 6.7, 7 - SUSE ES 11
Windows	Windows 2008 R2, 2012, and 2012 R2 (64-bit)
CPU, Memory, Disk Space	- CPU: Min 4 CPU cores (8 or 16 CPU cores for higher performance) - Memory: Min 4 GB (16 GB recommended) - Disk Space: 20 GB

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://	The DHCP configuration on the virtual appliance failed. If it is failed: • Power off the NFO virtual appliance. • Right-click the virtual appliance and select Edit Settings. • Set a static IP address for the virtual appliance.

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 12 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 12 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 12 for more information.

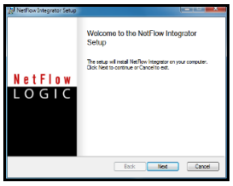
Windows Installation

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 12 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
`$nfo_home/tomcat/bin/setenv.sh`	Environment variables
`$nfo_home/tomcat/conf/.tomcat_keystore`	Default self-signed certificate
`$nfo_home/tomcat/conf/.truststore`	External Data Feeder for NFO certificate
`$nfo_home/tomcat/conf/server.xml`	Keystore password
`$nfo_home/server/etc/server.cfg`	Server configuration (Note: some Web GUI configurations are in this file as well)
`$nfo_home/java/jre8/jre/lib/security/cacerts`	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 29 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

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, transalted 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.

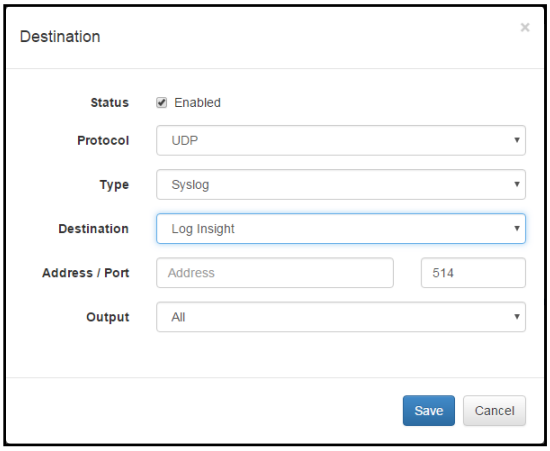
4. Type = Syslog, Output = Original NetFlow/IPFIX only – indicates both #2 and #3 combined.

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



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

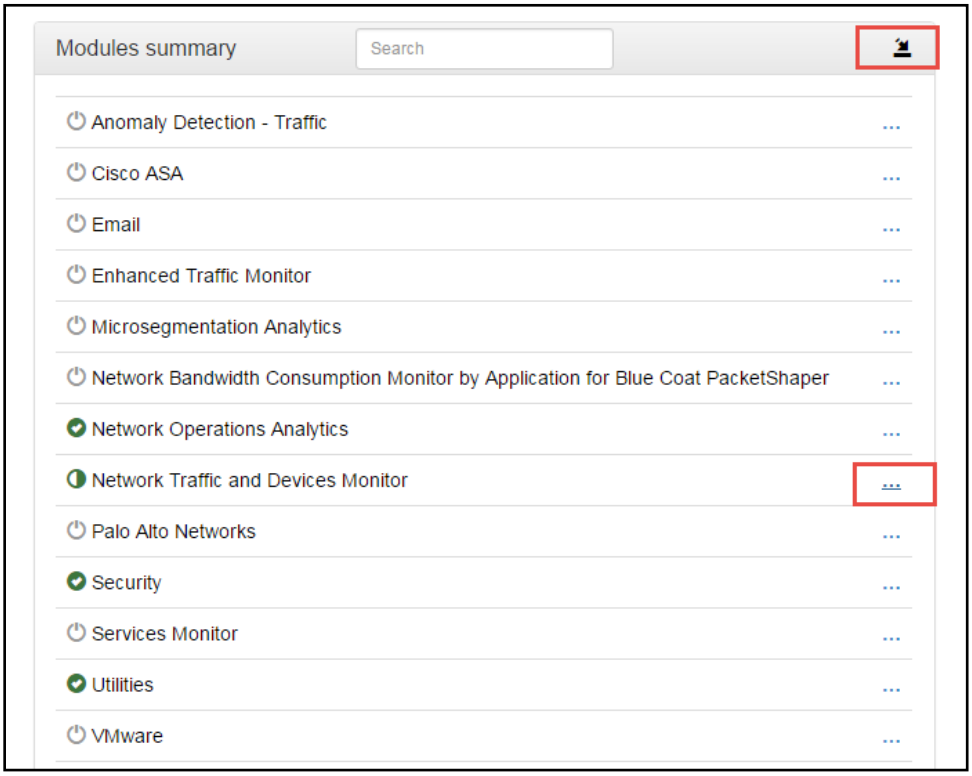
Click on the 'Stop' button  to stop the server

Restart

Click on the 'Restart' button  to restart the server

Enabling and Configuring Modules

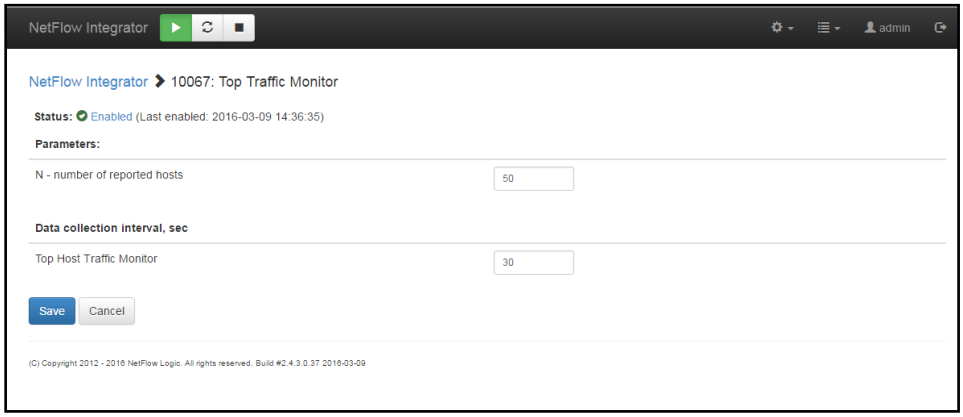
By default NetFlow Optimizer is preconfigured with one Module enabled -- Network Traffic and Device Monitor: 10067 Top Traffic Monitor. You may enable / disable the entire set or each Module by clicking on  / 



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

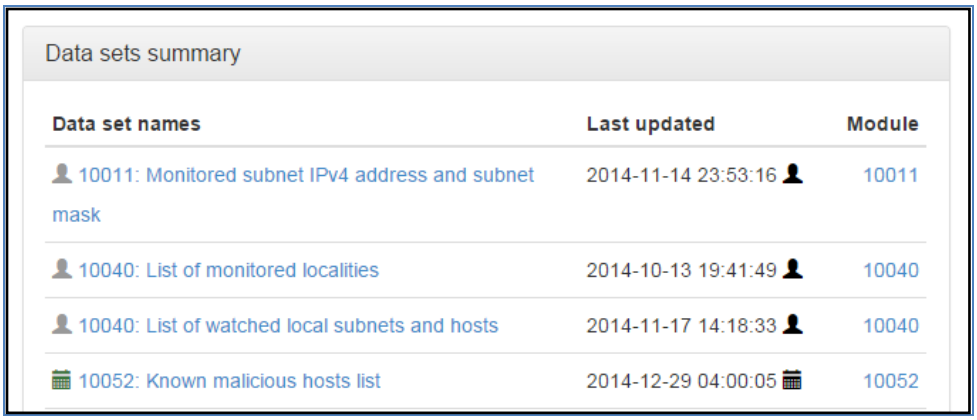


Parameter	Description
N – number of reported hosts	The number of top hosts reported per NetFlow exporter, min = 0, max = 100000, default = 50 (0 indicates all hosts are reported)
Data collection interval, sec	Module logic execution interval, min = 5 sec, max = 86400 sec, default = 300 sec. During this 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 (1st parameter) are converted to syslog and reported.

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

Data Sets Summary

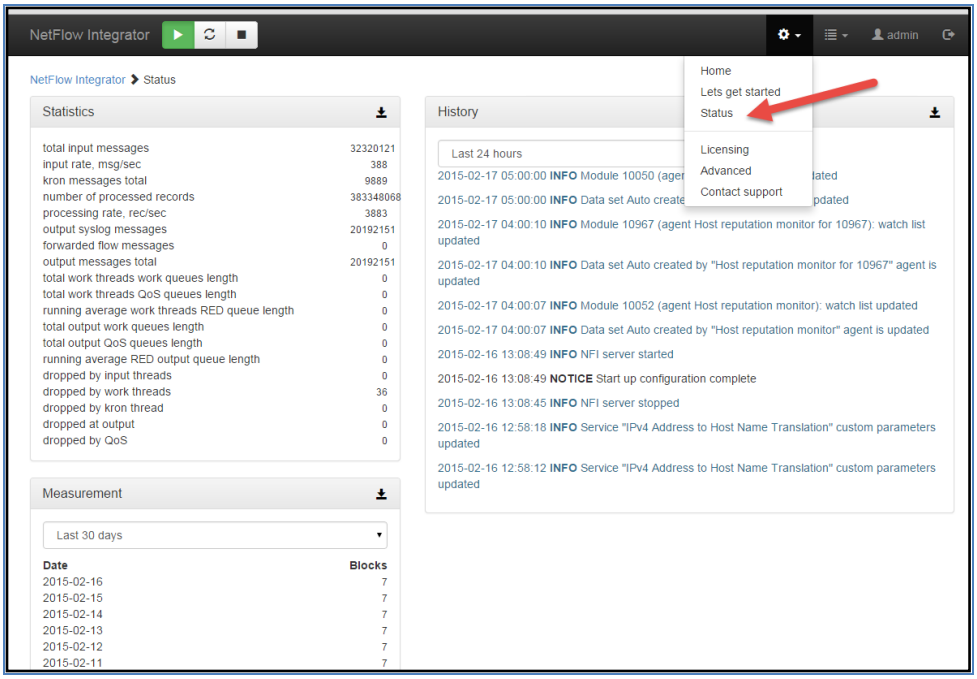
This section contains watch list parameters. Watch lists are created and updated when the corresponding Module is configured.



Some watchlist are created and mainatained 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 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

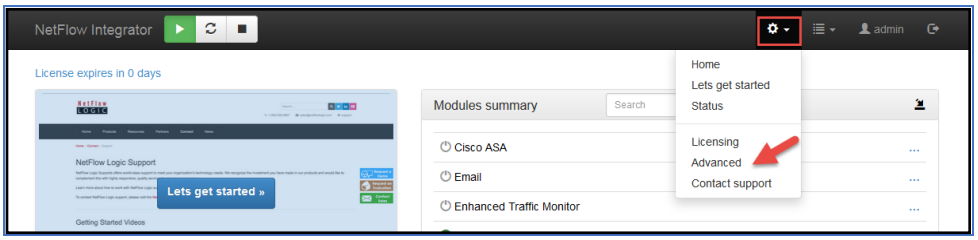
This Service supports protocol version SNMPv2C. It does not support any later versions of the protocol.

The service is always enabled.

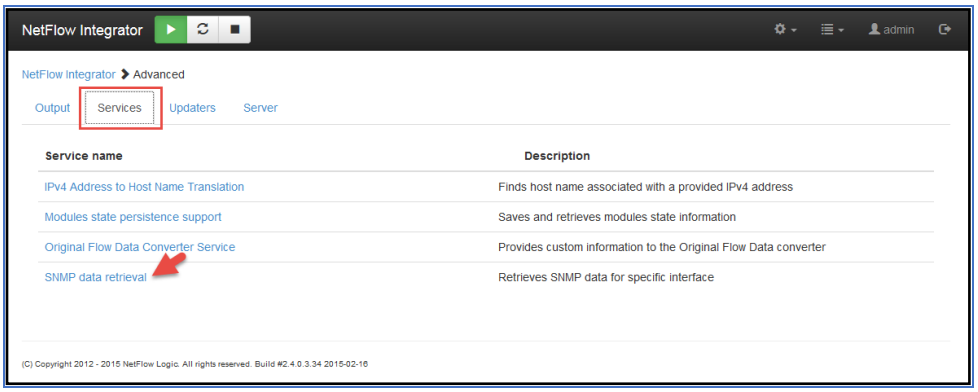
 Please note that the Service replies in SNMP index fields to be present in Flow records.

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.

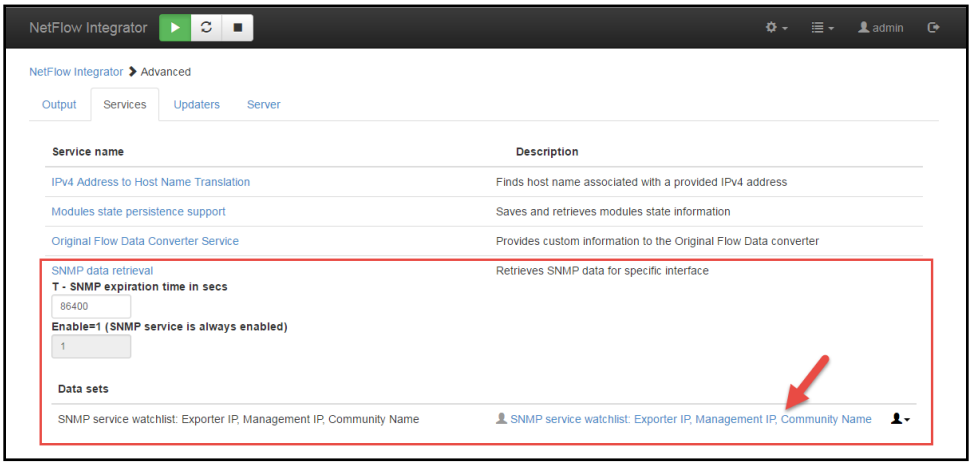
Select Advanced from top left navigation bar:



Go to Services tab and select SNMP data retrieval:



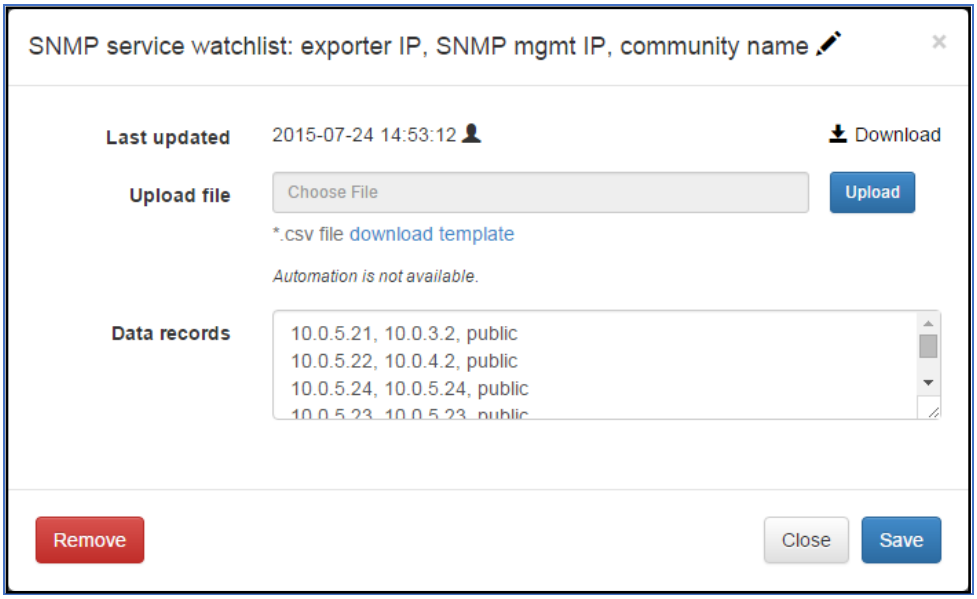
Click on “SNMP service watchlist: Exporter IP, Management IP, Community Name” link:



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.



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

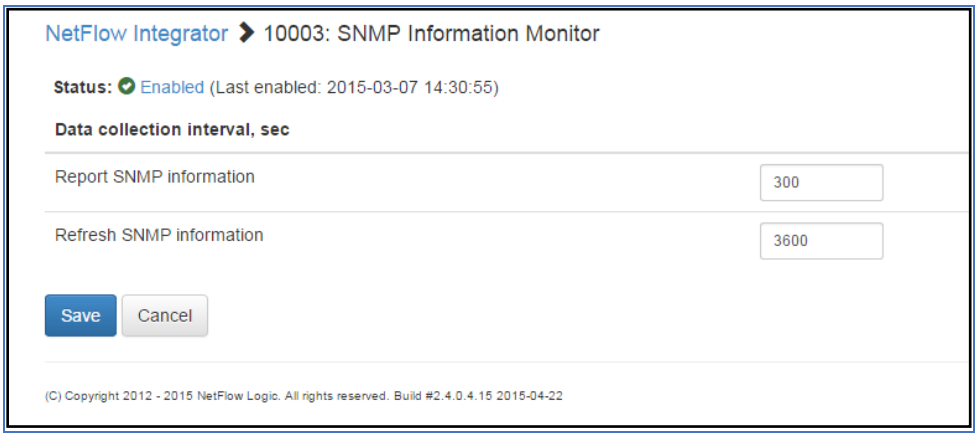
NFO Utility Module (10003: SNMP Information Monitor)

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:



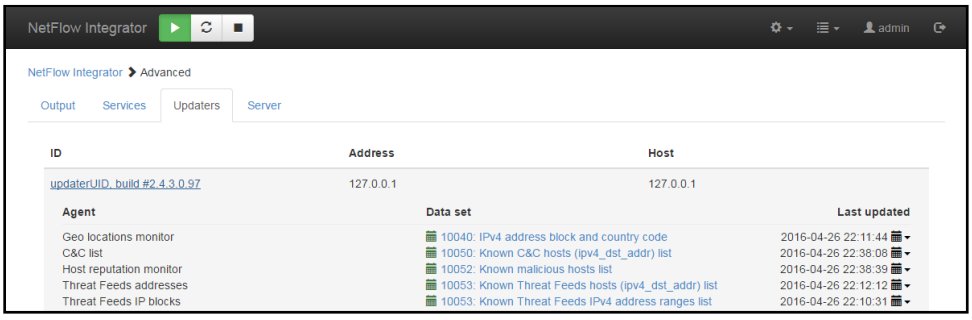
Future releases of NetFlow Optimizer

The following features are scheduled to be implemented in upcoming releases of NFO:

1. Add ability to specify arbitrary OID (NFC-5308).

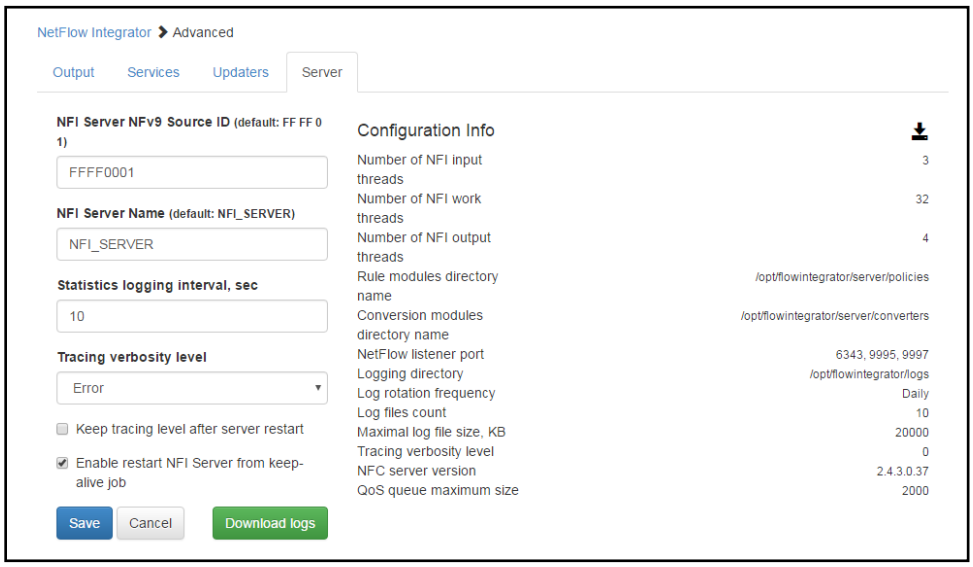
Data Feeder Tab

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



Server Tab

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



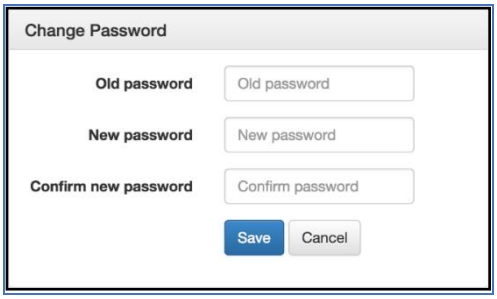
Admin

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



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`

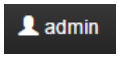
3. Restart NFO Tomcat service

Windows: Restart NFO Tomcat using Windows Services

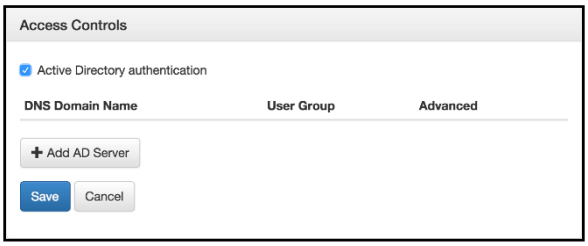
Linux: `/etc/init.d/tomcat_nfo restart`

Active Directory Authentication

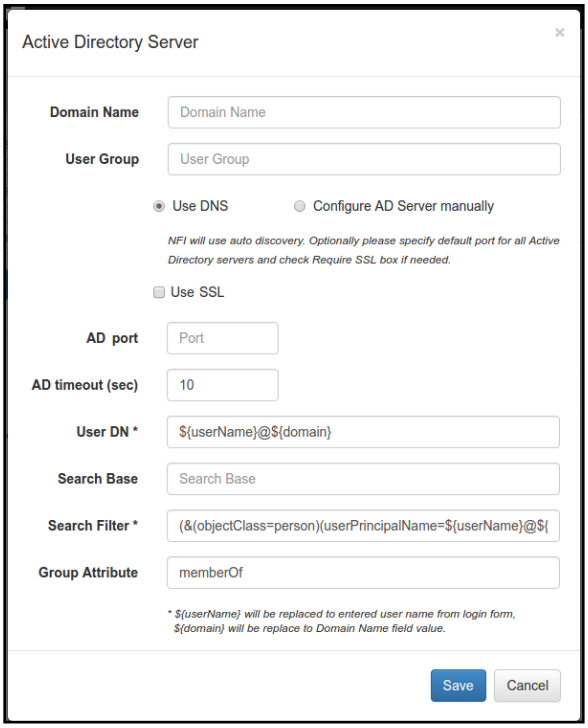
Procedure

1. Click on 

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

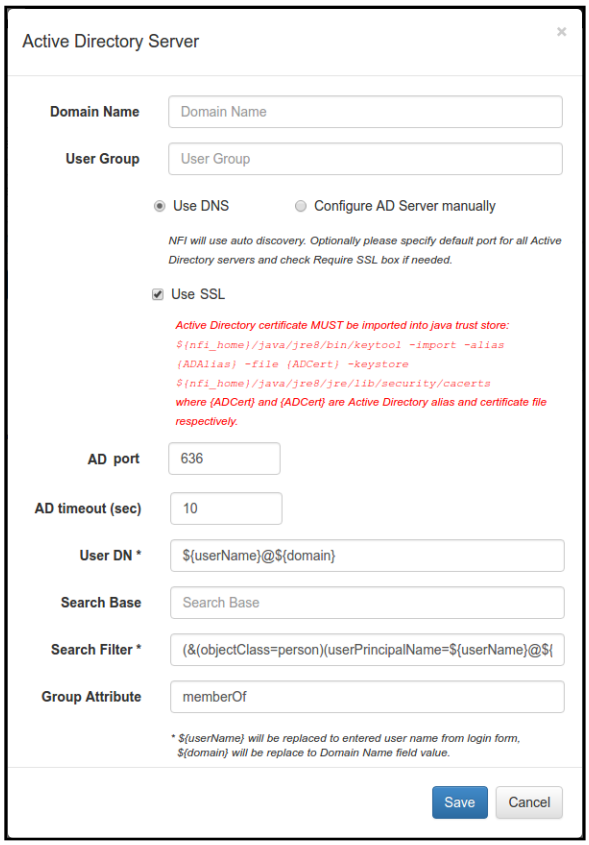


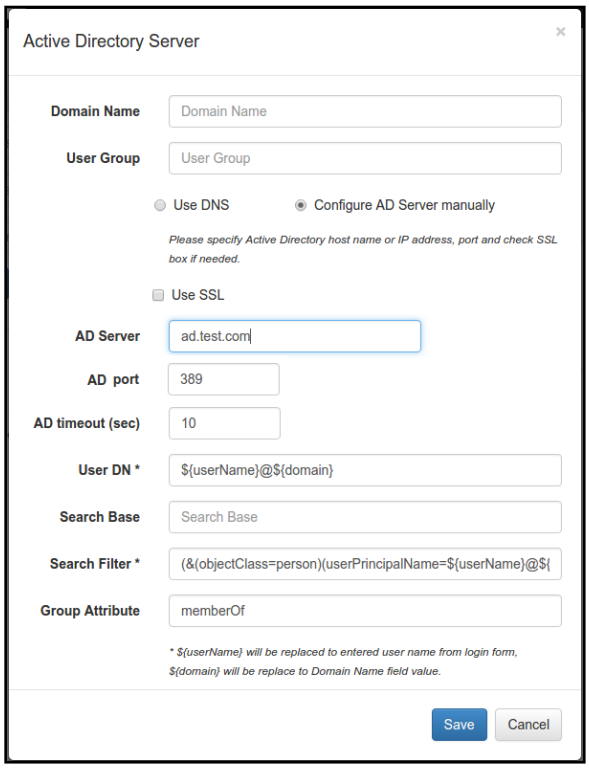
2. Click on Add AD Server button



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`.

Widows: `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`

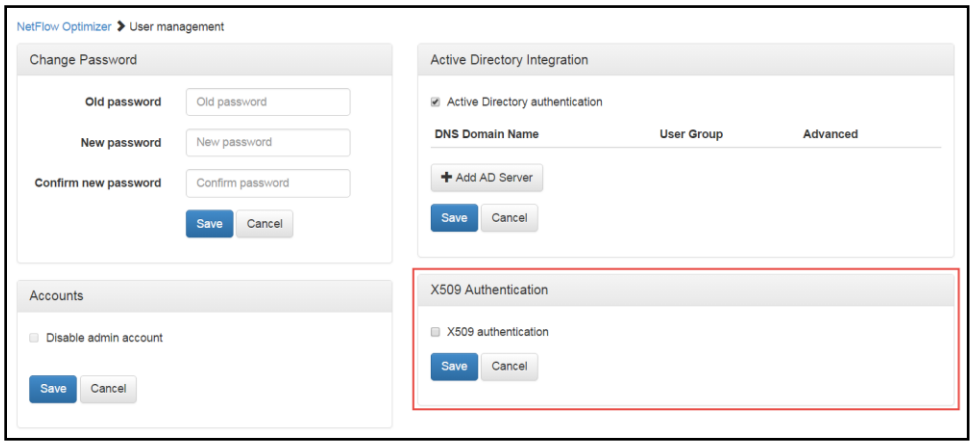
For troubleshooting please check `logs/nf2sl.log`. Logs trace level can be changed in the `/opt/flowintegrator/tomcat/webapps/ROOT/WEB-INF/classes/log4j.xml` file. Following lines should be added after last `<category>` section and before `<root> section`:

```
<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.



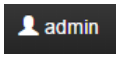
Please contact support@netflowlogic.com for detailed instructions.

Disabling Admin Account

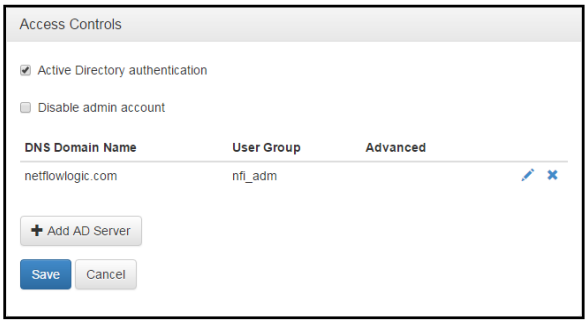
Once Active Directory Integration is configured, you can optionally disable the *admin* account.

Procedure

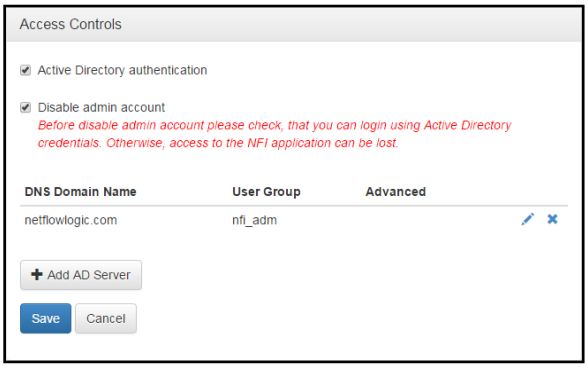
To disable *admin* account perform the following:

1. Click on 

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



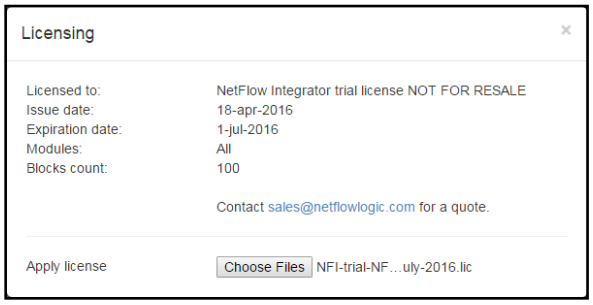
2. Select Disable admin account



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



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
  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 **Error! Reference source not found.** section on page **Error! Bookmark not defined.** 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.