External Data Feeder for NFO

Installation and Administration Guide

Version 2.4.9 (Build 2.4.9.0.3)

May 2017

Contents

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

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.

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 - 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 CPU cores for higher performance) - Memory: 2 GB - Disk Space: 2 GB

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
443/TCP	External Data Feeder for NFO Agents secure Internet communication
8443/TCP	NetFlow Optimizer communication

Required Internet Destinations

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

URL	Agent
http://rules.emergingthreats.net/	C&C list
http://geolite.maxmind.com/	Geo locations monitor
http://reputation.alienvault.com/	Host reputation monitor
https://secure.dshield.org/	Threat Feeds addresses
https://feeds.dshield.org/	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, perform the following:

1. Change `uri` parameter in `updater.properties` file located in `/opt/nfi-updater/conf` to IP address of NetFlow Optimizer:
   `uri = https://<nfo-host>:8443`

2. Change **NFO** tomcat configuration:

   a. Stop NFO tomcat service

   b. Edit `/opt/flowintegrator/tomcat/conf/web.xml` file

   c. Change `cors.allowed.origins` parameter value from `http://localhost:8443` to `http://<nfo-host>:8443`. Where `<nfo-host>` is exactly the same string as in the `updater.properties`. Use `http`, not `https` in the web.xml property, it is not a typo - secure communication will be used.

   d. Start NFO tomcat service.

   e. Restart EDFN 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 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 10 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 13 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, perform the following:

3. Change `uri` parameter in `updater.properties` file located in `/opt/nfi-updater/conf` to IP address of NetFlow Optimizer:
   `uri = https://<nfo-host>:8443`

4. Change **NFO** tomcat configuration:

   a. Stop NFO tomcat service

   b. Edit `/opt/flowintegrator/tomcat/conf/web.xml` file

   c. Change `cors.allowed.origins` parameter value from `http://localhost:8443` to `http://<nfo-host>:8443`. Where `<nfo-host>` is exactly the same string as in the `updater.properties`. Use `http`, not `https` in the web.xml property, it is not a typo - secure communication will be used.

   d. Start NFO tomcat service.

   e. Restart EDFN 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 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 10 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 13 for further instructions.

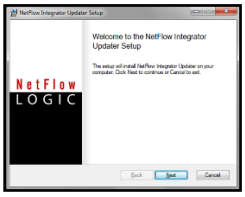
Windows Installation

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

If External Data Feeder for NFO is installed on a separate server, perform the following:

5. 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. Change **NFO** tomcat configuration:

   a. Stop NFO tomcat service

   b. Edit `%NFO_HOME%\tomcat\conf\web.xml` file

   c. Change `cors.allowed.origins` parameter value from `http://localhost:8443` to `http://<nfo-host>:8443`. Where `<nfo-host>` is exactly the same string as in the `updater.properties`. Use `http`, not `https` in the web.xml property, it is not a typo - secure communication will be used.

   d. Start NFO tomcat service.

   e. Restart EDFN service.

7. 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 10 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 13 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
`$updater_home/conf/updater.properties`	NetFlow Intergrator URI and other parameters
`$updater_home/conf/.updater_keystore`	Default self-signed certificate for X509 authentication
`$updater_home/conf/.updater_truststore`	Default self-signed NFO tomcat certificate
`$updater_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.

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.

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 13 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:

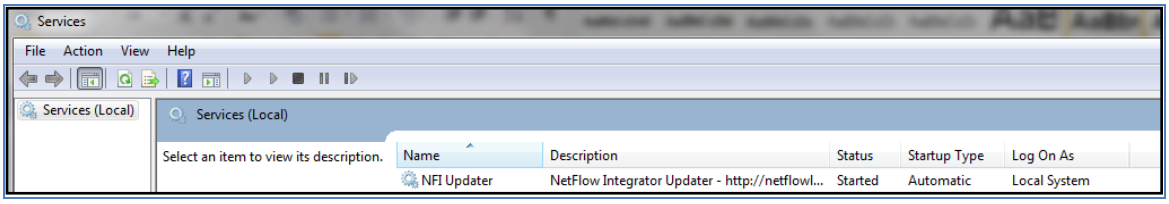
1. Enter the following command to check the status
   `/etc/init.d/nfi_updd status`

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 logins 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_trustore 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

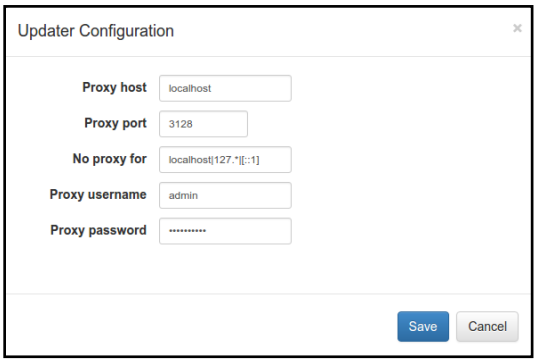
External Data Feeder for NFO could be configured to use Proxy Server authentication before it can access external URLs.

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*).