Customizing the FNMS Agent using Policy Settings

SOFTLINE KB ARTICLE

Doc type	Publisher	Software	Section	Version/Edition	Author	Creation Date
How To	Softline AG	FlexNet Manager Suite (FNMS)	System Config	FNMS 2019 R1 Previous FNMS releases partially tested.	Klaus Rafeiner	2019-09-16 Version 1.0.0

CONTEXT

This is a technical article that describes how to configure the Flexera Agent using settings that cannot be configured using the FNMS Web User Interface (UI). This article is intended for consultants and technical personal working with FNMS.

CONFIGURING THE FLEXERA AGENT USING THE CENTRAL POLICY

The Flexera agent can me managed centrally by using the “Inventory Settings” (Policy) page that is accessible from the FNMS Web UI from the “Discovery & Inventory > Settings” menu.

In addition to general settings like the Inventory agent schedule, on this page, you can configure certain settings for collecting file evidence on target devices. These settings can be configured independently for the Operating Systems Windows, macOS and Linux/UNIX.

As described in the [GatheringFlexNetInventory.pdf] document provided with each release of FNMS, there are a lot of additional configuration settings for the Flexera agent (NDTRACK) that can be configured either from the command line or by setting the option in the Registry (on Windows computers) or using the CONFIG.INI file (on non-Windows computers). This includes the following settings (as an example):

- `CheckServerCertificate`
- `CheckCertificateRevocation`
- `IncludeExtension`
- `IncludeNetworkDrives`
- `IncludeFileSystemType`
- `IncludeRegistryKey`

Softline Solutions GmbH
Gutenberg-Galerie | Gutenbergplatz 1
D-04103 Leipzig
Sitz der Gesellschaft: Leipzig

Tel.: +49 341 24051-0
Fax: +49 341 24051-199
E-Mail: leipzig@softline-group.com
Web: www.softline-solutions.de

HRB 26058
Registergericht Leipzig
Geschäftsführer:
Martin Schaletzky

Bank: Commerzbank AG
IBAN: DE36 8604 0000 0118 6790 00
BIC: COBADEFFXXX
Ust-ID: DE270894910

This article describes:

1. How to *centrally* configure settings for the Flexera agent including the ones listed above without using 3rd party deployment or configuration tools.
2. How to configure options for file scanning - like excluding folders - using a relative path (*\backup) or including/excluding folders on Windows by name but without using a fixed drive (\temp).
3. How to limit configuration options for the Flexera agent not only by target Operating System but also by using specific “Targets” that you configure in FNMS.

DISCLAIMER

Information provided in this article is not supported by Flexera officially.

While this article allows configuring settings for the Flexera agent, there currently is no workaround for limitations imposed by the fact that FNMS supports a single “Policy” only.

Specifically, Inventory configuration settings cannot be customized. In the BeaconPolicy.xml file, only a single version of these configuration is allowed:

- Agent Schedule
- Agent version for automatic deployment
- IBM PVU Settings

Also, there are a few configuration settings for the Flexera agent that cannot be updated centrally using the “BeaconConfig.xml” file. These settings have to be updated locally or by using a 3rd party configuration tool. These settings include:

- `SelectorAlgorithm`
- `UploadSettings` and any configuration settings below it

Softline Solutions GmbH
Gutenberg-Galerie | Gutenbergplatz 1
D-04103 Leipzig
Sitz der Gesellschaft: Leipzig

Tel.: +49 341 24051-0
Fax: +49 341 24051-199
E-Mail: leipzig@softline-group.com
Web: www.softline-solutions.de

HRB 26058
Registergericht Leipzig
Geschäftsführer:
Martin Schaletzky

Bank: Commerzbank AG
IBAN: DE36 8604 0000 0118 6790 00
BIC: COBADEFFXXX
Ust-ID: DE270894910

TECHNICAL DETAILS

In the [FNMSCompliance] database, all configuration settings that need to be distributed to Flexera agents are stored in the [BeaconTarget] and additional tables linked to it like [BeaconTargetPropertyValue].

Settings in this table are being published to an XML file named “BeaconPolicy.xml”. This file is being downloaded to all Flexera Beacons on a schedule. Flexera agents are downloading this configuration on schedule (daily) from their Beacons.

With this article, an accompanying folder named SQL is provided as a ZIP file (SQL.zip). This folder contains sample SQL scripts referenced in this article.

In the FNMS databases (`[BeaconTargetPropertyValue]` table), setting names for the Flexera Agent will generally be prefixed by `CTracker`, followed by the name of the configuration setting. If you want to include a directory for file system scanning by the Flexera agent, the configuration setting key in the database will be ‘`CTrackerIncludeDirectory`’. The configuration setting value will be the name of the folder to be included. Multiple values need to be separated by a Semicolon (‘;’) character.

For target names, there are three predefined names for different Operating System types differentiated in the FNMS UI (`Target__windows`, `Target__osx` and `Target__unix`). However, any custom target configured in the FNMS UI under “Discovery & Inventory > Discovery and Inventory Rules” can be addressed using the name of the target, too.

When executing the `ListSettingsForBeaconTargets.sql` file against a [FNMSCompliance] database that has default file scanning options configured, the following results are obtained:

Target ID	Name	TargetPropertyKey	TargetPropertyValue
3	Target__osx	CTrackerEmbedFileContentDirectory	/
3	Target__osx	CTrackerExcludeDirectory	
3	Target__osx	CTrackerExcludeEmbedFileContentDirectory	
3	Target__osx	CTrackerIncludeDirectory	/
4	Target__windows	CTrackerEmbedFileContentDirectory	\
4	Target__windows	CTrackerExcludeDirectory	$(WinDirectory)
4	Target__windows	CTrackerExcludeEmbedFileContentDirectory	$(WinDirectory)
4	Target__windows	CTrackerIncludeDirectory	\
5	Target__unix	CTrackerEmbedFileContentDirectory	/
5	Target__unix	CTrackerExcludeDirectory	
5	Target__unix	CTrackerExcludeEmbedFileContentDirectory	

Softline Solutions GmbH
Gutenberg-Galerie | Gutenbergplatz 1
D-04103 Leipzig
Sitz der Gesellschaft: Leipzig

Tel.: +49 341 24051-0
Fax: +49 341 24051-199
E-Mail: leipzig@softline-group.com
Web: www.softline-solutions.de

HRB 26058
Registergericht Leipzig
Geschäftsführer:
Martin Schaletzky

Bank: Commerzbank AG
IBAN: DE36 8604 0000 0118 6790 00
BIC: COBADEFFXXX
Ust-ID: DE270894910

5	Target__unix	CTrackerIncludeDirectory	/

As you can see, file scanning is enabled for all local drives on all supported Operating systems by default. For Windows specifically, the $(WinDirectory) folder – which is C:\Windows by default – is excluded from file scanning.

After downloading these configuration settings to the “BeaconPolicy.xml” file, this looks like (only part of the file displayed):

```
273  <Beacons> ...
309  </Beacons>
310  <Targets>
311    <Target Name="Local" TargetID="1"> ...
324    </Target>
325    <Target Name="VMware vSphere" TargetID="2"> ...
335    </Target>
336    <Target Name="Target__osx" TargetID="3"> ...
347    </Target>
348    <Target Name="Target__windows" TargetID="4">
349      <Properties>
350        <PropertyValue Name="CTrackerIncludeDirectory">\</PropertyValue>
351        <PropertyValue Name="CTrackerEmbedFileContentDirectory">\</PropertyValue>
352        <PropertyValue Name="CTrackerExcludeDirectory">$(WinDirectory)</PropertyValue>
353        <PropertyValue Name="CTrackerExcludeEmbedFileContentDirectory">$(WinDirectory)</PropertyValue>
354      </Properties>
355      <Filters>
356        <Filter xsi:type="PlatformFilter" Include="true" FilterValue="windows" />
357      </Filters>
358      <AgentEvents />
359    </Target>
360    <Target Name="Target__unix" TargetID="5"> ...
374    </Target>
```

After the settings in the “BeaconConfig.xml” file have been downloaded to a computer running the Flexera agent, settings will be stored in the Registry (on Windows devices) and in the CONFIG.INI file (on non-Windows devices).

HOW TO

SETTING CONFIGURATION VALUES

OK – now we know where to find the configuration settings for the Flexera agent in the [FNMSCompliance] database. But how can configuration settings that are not exposed to the FNMS Web UI be updated?

Obviously, we have to do this using some SQL. Luckily, FNMS has a stored procedure named `BeaconTargetPropertyValuePutByKeyNameBeaconTargetID` that allows adding an additional (new) configuration setting for the Flexera agent.

After adding the new configuration setting, there is an additional stored procedure named `BeaconPolicyUpdateRevision` that will enforce the new configuration settings to the “BeaconConfig.xml” file.

This is a working T-SQL code example that needs to be run against the [FNMSCompliance] database:

```
-- Set @BeaconTargetID based on @TargetName
DECLARE @BeaconTargetID INT
SELECT  @BeaconTargetID = BeaconTargetID FROM BeaconTarget
WHERE NAME = 'Target__windows'

-- Configure the registry key bo be read
EXEC dbo.BeaconTargetPropertyValuePutByKeyNameBeaconTargetID
       @BeaconTargetID = @BeaconTargetID,
       @KeyName = 'CTrackerIncludeRegistryKey',
       @Value   = 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentBuild'

-- Update the Beacon Policy
EXEC dbo.BeaconPolicyUpdateRevision
```

As you probably guessed, this code will add a configuration setting to FNMS that forces all Flexera agents running on Windows to retrieve the Windows Build number from the Windows Registry. The value retrieved by the Flexera Agent (ndtrack) will be stored in the NDI file and will be uploaded to the [FNMSInventory] database via a Beacon.

Please note that exposing additional custom data retrieved by the Flexera agent to the FNMS Web UI - like the Windows Build number - will usually require adding a custom field to the Inventory object in FNMS, and customizing the Managesoft READER and WRITER XML files to make sure that the custom value is being picked up (populated).

Softline Solutions GmbH
Gutenberg-Galerie | Gutenbergplatz 1
D-04103 Leipzig
Sitz der Gesellschaft: Leipzig

Tel.: +49 341 24051-0
Fax: +49 341 24051-199
E-Mail: leipzig@softline-group.com
Web: www.softline-solutions.de

HRB 26058
Registergericht Leipzig
Geschäftsführer:
Martin Schaletzky

Bank: Commerzbank AG
IBAN: DE36 8604 0000 0118 6790 00
BIC: COBADEFFXXX
Ust-ID: DE270894910

A working code example for adding the scanning of registry settings on Windows computers is contained in the "`FlexAgentWinIncludeRegistryKey.sql`" file provided with this article.

Let us look at a few additional examples for configuring settings for the Flexer agent.

ENABLING SCANNING OF NFS FILE SYSTEMS ON UNIX

By default, the Flexera agent on Linux/UNIX will only scan local using the default (Ext3, Ext4, BtrFS) file system types. In case you want additional file systems that are mounted on your computer but use UFS, ZFS, LOFS or NFS as the file system type, you must use the IncludeFileSystemType directive for the Flexera agent.

The `FlexAgentUnixEnableScanNFS.sql` script that is provided with this article is setting this directive for all Flexera Agents running on any Linux/UNIX computers.

EXCULDING FOLDERS FROM SCANNING USING A RELATIVE PATH

A common problem on non-Windows computers is that the amount of data obtained from scanning the file system can become extensive. One way to minimize the amount of data is to exclude a generic relative path, like */temp from scanning.

This setting cannot be configured in the FNMS Web UI, as it gives an "Invalid folder name" error message when trying to save your configuration data.

The SQL file FlexAgentExcludeFoldersOnTarget.sql provided with this article will allow to exclude two generic folders (*/temp and */backup) from file system scanning, but do this on computers that are located in a specific target only.

RESULTS

It will usually take two days or more – depending on the scheduling that you configure for your Flexera agents – until results of your customizations will have an effect. You can speed this up by

- manually triggering the download of the Policy to your Beacon(s) from the Beacon UI
- manually triggering the download of the Policy to your client computers and subsequently manually triggering the generation of an Inventory

Command line options are available in the FNMS documentation and are summarized in the next paragraph.

CHECKING RESULTS

It is suggested that you test your configuration settings in a testing environment before using them on a production system. After applying your customizations:

- Check the output of the ListSettingsForBeaconTargets.sql script that is provided with this article.
- Check the "BeaconConfig.xml" file that is downloaded to your Beacons to make sure that this file contains the customzations that you configured
- After the policy has been updated on your client computers, check the Registry on Windows computers or the CONFIG.INI file on non-Windows computers to make sure that your customizations have been picked up by the Flexera agent. You can run "`mgspolicy -t machine`" as an Administrator (root) user on your clients to enforce downloading the latest version of the policy.
- Run the Flexera Agent - i.e. by running "ndtrack -t machine" as an Administrator (root) user – and compare the NDI file that is being created and uploaded with an NDI file that has been created on the same computer before customizations have been applied.

FURTHER INFORMATION

Additional technical information – including documentation on how to add custom fields to FNMS – can be found in the FNMSSystemReference.pdf document that is provided by Flexera for download with the FlexNet Manager Suite FNMS.