HOW-TO

AGENT SETTINGS AND PACKAGES DOMAIN DISTRIBUTION

DATE: 6.22.2018

Contents

Introduction

To take advantage of the Agent Security feature, some settings must be configured on the host. Settings for Windows hosts are configured in the registry. Settings for Mac OS X hosts are configured in Preferences.

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. These templates can be downloaded from the Agent Distribution view in FortiNAC. This document provides steps to deploy the Persistent and Passive Agent and related registry settings via Group Policy to Windows machines. However, customers can opt to distribute the agent and edit registry settings on hosts using another tool.

Requirements

- Active Directory
- Group Policy Objects
- Template Files: The installation program for the templates is run on a Windows server or another Windows system and then the files are copied to the server. The templates listed below are provided by Bradford Networks and contain both the ADM and newer ADMX templates.
    - 32-bit (x86): Bradford Networks Administrative Templates.msi
    - 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi
- Agent Package: Agent packages are provided by Bradford Networks. These files are copied to the server for distribution. A listing of currently released versions for all Bradford products (Release Matrix), as well as Agent release notes, can be downloaded from the Bradford Networks Customer Portal under the Content tab.

Procedure Overview

1. Obtain the following from FortiNAC:
    - GPO Templates
    - Agent Executables
2. Install and configure templates.
3. Copy agent executables to domain server.
4. Push template settings to computers.
5. Push agent executables to computers. Rebooting machines is not necessary.

Procedure

Obtain GPO Templates and Agent Executables

1. In the FortiNAC Administrative UI, navigate to **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window, click either the 32-bit (x86) or the 64-bit (x86_64) link to download the appropriate template file.
3. In the same view, locate the appropriate agent to download. Click on the name of the agent file in blue text in the **File** column of the table. The file is typically saved to the default download location. This is controlled by the browser.

   Note: The Dissolvable, Persistent and Passive Agent packages are included in the list, but only the Persistent and Passive Agent packages may be downloaded through this view. The links appear in blue.

Install and Configure Templates

Install templates using the appropriate set of instructions below. For more information regarding ADMX, refer to article https://msdn.microsoft.com/en-us/library/bb530196.aspx. (Note this article is managed by Microsoft and may change).

ADMX Templates

1. Copy the template file to the domain server or another Windows system with access to the Central Store or local PolicyDefinitions directory.
2. On the Windows system, double-click the **msi** file to start the installation wizard.
3. Click through the installation wizard.
4. Browse to **Program Files\Bradford Networks\Administrative Templates\admx**.
5. Copy the **Bradford Networks.admx** and **en-US** directory to the PolicyDefinitions directory of the central store.
6. Open the Group Policy Editor and navigate to the Group Policy Object desired to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Browse to **Computer Configuration > Administrative Templates > Bradford Networks**.

ADM Templates

1. Copy the template file to the domain server.
2. On the domain server, double-click the **msi** file to start the installation wizard.
3. Click through the installation wizard. At the end, the Microsoft Group Policy Management Console will be launched, if available.
4. Navigate to the Group Policy Object you want to edit, right-click and select **Edit** to display the GPO Editor pane.
5. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates**, shows the current templates pop-up.
6. Click **Add** and browse to **Program Files\Bradford Networks\Administrative Templates**.
7. Select **Bradford Persistent Agent.adm** and click **Open**.
8. Click **Close**, and the Administrative Templates will be imported into the GPO.

Copy Agent Executables to Domain Server

Copy the agent files to the Domain Server for distribution.

Configure Agent Settings

See the table below for settings which can be configured using the Administrative Templates provided. Once configured, push template settings to computers.

Passive Agent Template Settings

Option	Definition
Passive Agent	**Server URL List**— Comma separated list of URLs (http(s)://<server_name>/<- context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly. Example: http://qa228/registration **Note:** The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Persistent Agent Template Settings

Option	Definition
Host Name	Fully qualified host name of the FortiNAC Application Server or the Net- work Sentry Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. **Note:** This is an option for Persistent Agent Version 2.9.x and lower. Persistent Agent Versions 3.0 and higher do not use this setting.
Balloon Notifications	Enables or Disables Balloon Notifications on a per-machine or per-user basis. This setting is not required for configuring Server IP information. Options include: **Enabled** — Forces balloon notifications for host state changes to be enabled on the host. **Disabled** — Forces balloon notifications for host state changes to be disabled on the host. **Not Configured** — Use the non-policy setting (Enabled).
Login Dialog	Enables or Disables the login dialog on a per-machine or per-user basis. This setting is not required for configuring Server IP information. See Using Windows Domain Logon Credentials With Persistent Agent for further instructions. Options include: **Enabled** — The login dialog is enabled. This can be used per-user to override a per-machine setting of Disabled. **Disabled** — The login dialog is disabled. The agent will never prompt the user for credentials. This is useful in certain Single-sign-on configurations. **Not Configured** — The login dialog is enabled, unless overridden by a per-user configuration.
System Tray Icon	Enables or Disables the System Tray Icon on a per-machine or per-user basis. This setting is not required for configuring Server IP information. Options include: **Enabled** — The System Tray Icon is enabled. This can be used per-user to override a per-machine setting of Disabled. **Disabled** — The System Tray Icon is disabled. Disabling the System Tray Icon also disables the following functionality: Status Notifications (Show Network Access Status, Login, Logout), Message Logs and the About dialog. **Not Configured** — The System Tray Icon is enabled, unless overridden by a per-user configuration.

Max Connection Interval	The maximum number of seconds between attempts to connect to FortiNAC.

Persistent Agent Template - Security Settings	
Security Mode	Indicates whether security is enabled or disabled.
Home Server	Server with which the agent always attempts to communicate first. Protocol con- figuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Option	**Definition**
Limit Connections To Servers	**Enabled** — Agent communicates only with its Home Server and servers listed under Allowed Servers list displayed. **Disabled** — Agent searches for additional servers when the home server is unavailable. **Allowed Servers List** — In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Passive Agent Template	
Passive Agent	**Server URL List**— Comma separated list of URLs (http(s)://<server_name>/<- context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly. Example: http://qa228/registration **NOTE:** The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.

Registry Keys

The template setup shown in the table above modifies the Windows host's registry settings. The table below shows the modifications made to the host's registry keys by the Group Policy Object using the administrative template. If using a tool other than GPO, make sure to set the appropriate keys on each host.

Upon installation of the Persistent Agent, the following key is created by default (and can be viewed using the Windows registry editor on the endstation):

```
HKLM\Software\Bradford Networks\Client Security Agent
```

Settings written to the default location remain until one of the following occurs:

- Entry is manually changed.
- Agent is uninstalled.
- Agent is updated.

For this reason, **HKLM\Software\Bradford Networks\Client Security Agent** should not be used when pushing settings via software. Additionally, if the Persistent Agent installer is modified in any way, the update functionality in FortiNAC may remove any or all customization.

When registry settings are pushed to a host via software, one or both of the following keys are used (depending upon the values pushed).

Per-user (control based on User Groups)

```
HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent
```

Per-machine

```
HKLM\Software\Policies\Bradford Networks\Persistent Agent
```

Note:

- On 64-bit operating systems in RegEdit, these registry values will appear in the following key: **HKLM\Software\wow6432node.**
- When the settings are pushed, the values for **HKLM\Software\Bradford Networks\Client Security Agent** will remain the same, but any settings altered via the software push will override those listed in the original key.
- The values set per-user override the values set per-machine.

Passive Agent Settings

Value	Data	Key
ServerURL	**Server URL List** — Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration **NOTE**: The context portion of the Server URL is the area of the captive portal the agents should contact, such as, registration, remediation, or authentication.	**HKEY_USERS\{SID}\Software\ Policies\Bradford Networks \PASSIVE** Or **HKLM\Software\Policies\Bradford Networks\PASSIVE**

Persistent Agent Settings

Value	Data	Key
ServerIP	The fully-qualified hostname to which the agent should communicate. **Data Type:** String **Default:** Not Configured	**HKLM\Software\Policies\Bradford Networks\Persistent Agent**
ClientStateEnabled	**0** - Do not show balloon notifications on status changes. **1** - Show balloon notifications on status changes. **Data Type:** DWORD **Default:** Not Configured	**HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent** Or **HKLM\Software\Policies\Bradford Networks\Persistent Agent**
LoginDialogDisabled	**0** - Enable Login Dialog. **1 -** Disable Login Dialog. **Data Type:** DWORD **Default:** Not Configured (Login Dialog displayed)	**HKEY_USERS\ …** **\Software\Policies\Bradford Networks\Persistent Agent** Or **HKLM\Software\Policies\Bradford Networks\Persistent Agent**
ShowIcon	**0** - Do not show the tray icon. **1** - Show the tray icon. **Data Type:** DWORD **Default:** Not Configured (Tray icon displayed)	**HKEY_USERS\ … \Software\Policies\Bradford Networks\Persistent Agent** Or **HKLM\Software\Policies\Bradford Networks\Persistent Agent**
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. **Data Type:** Integer **Default:** 960	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**

Value	Data	Key
securityEnabled	**0 -** Disable Agent Security **1 -** Enable Agent Security **Data Type:** Integer **Default:** 1	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**
homeServer	The fully-qualified hostname of the default server with which the agent should communicate. **Data Type:** String **Default:** Empty	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**
restrictRoaming	**0 -** Do not restrict roaming. Allow agent to communicate with any server. **1 -** Restrict roaming to the home server and the allowed servers list. **Data Type:** Integer **Default:** 0	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**
allowedServers	Comma-separated list of fully-qualified hostnames with which the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list Example: a.example.com, b.example.com, c.example.com **Data Type:** String **Default:** Empty	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**

Deploy the Persistent Agent

After pushing template settings, push the **.msi** file to the domain machines.

Deploy the Passive Agent

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the Group Policy Object you want to edit.
3. Right-click the Group Policy Object and select **Edit** to display the GPO Editor pane.
4. Click **User Configuration > Policies >Windows > Settings Scripts (Logon/Logoff)** to display the Logon and Logoff script configurations.
5. Double click **Logon** for Logon Properties.
6. Click **Add** and then browse to the location of Bradford Passive Agent.exe.
7. Select **Bradford Passive Agent.exe** to add it to the Script Name field.
8. Enter **-logon** in the Script Parameters field.
9. Click **OK**.
10. To ensure the user is logged off the host upon logging out, do the following:
    a. Follow steps 1-4, and then double-click **Logoff**.
    b. Add **Bradford Passive Agent.exe** to to the Script Name field, and then enter

       -logoff in the Script Parameter field.
11. Click **OK**.

Update Deployed Agents

If using Group Policy or a software management program to deploy the agent, the recommendation is to use the same method for updating the agent version once deployed.

When using Group Policies, add the new agent package and list it as an upgrade to the previous versions. Ensure any previous package referenced by the GPO remains in place until all hosts have successfully moved off that version.

For assistance, consult vendor documentation.

