FortiNAC

Persistent Agent Deployment and Configuration

Version: 9.1

Date: December 19, 2023

Rev: ad

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

What it Does

The Persistent Agent resides on the host machine and works in conjunction with the FortiNAC Agent Server to complete tasks such as registration, authentication and scanning, as well as provide additional information to FortiNAC about the host (adapters, applications, etc).

How it Works

In order to utilize the Persistent Agent, it must be installed on the end machine. Once the agent is installed and its service is started, the agent will attempt to communicate with FortiNAC. The general process the Persistent Agent uses to communicate is as follows:

1. Identify the name of the FortiNAC Agent Server with which the agent should communicate. This information can be provided to the agent in two ways:
    - Persistent Agent settings configured via…
        - Software distribution
        - Last successful communication with FortiNAC
    - Discovery process - lookup for DNS SRV records from…
        - Production DNS server
        - FortiNAC Captive Portal

    Agent 5.3 and greater: Option available to disable SRV lookups (are enabled by default)

2. Attempt to establish communication to the server. By default, this is done over SSL/TLS using TCP port 4568 (requires SSL certificates installed on FortiNAC).

3. Once SSL/TLS communication is established, the agent uses either UDP port 4567 or TCP port 4568 for most all other agent/server communication. See Persistent Agent Server Discovery Process in the Appendix for port and version information.

Requirements

- SSL Certificates installed in FortiNAC (Persistent Agent Certificate Target).
- Do not block TCP 4568 or UDP 4567 ports on network

Onboarding Use Cases

Determine how machines will register based on security policies and requirements. Listed below are common use cases.

Company Asset Windows Domain (Silent Onboard (Single-Sign-On)): Persistent Agent is distributed to Windows domain machines via imaging or software management program. Windows machines are automatically registered when the user logs on to the domain. The registered host is not associated with any specific owner, but FortiNAC is able to track the logged on user. This method is recommended for Windows domain machines and is transparent to the end user.

Company Asset macOS Machines (Silent Onboard): Persistent Agent is distributed to macOS machines via imaging or software management program. The macOS machine automatically registers upon connecting to the network once the installed Persistent Agent communicates with FortiNAC. The registered host is not associated with any user record. This registration method is transparent to the end user. **Note**: Logged on users are not tracked for macOS and Linux.

Company Asset Linux Machines (Silent Onboard): Persistent Agent is distributed to Linux machines via imaging or software management program. The Linux machine automatically registers upon connecting to the network once the installed Persistent Agent communicates with FortiNAC. The registered host is not associated with any user record. This registration method is transparent to the end user. **Note**: Logged on users are not tracked for macOS and Linux.

Company Asset macOS Machines (Onboard Through Isolation): Persistent Agent is distributed to macOS machines via imaging or software management program. User is prompted to enter credentials in order to register. If network is under enforcement, device is isolated until registered. The machine is registered to the user. **Note:** This method cannot be used in conjunction with the Windows Domain Single-Sign-On method.

Company Asset Linux Machines (Onboard Through Isolation): Persistent Agent is distributed to Linux machines via imaging or software management program. User is prompted to enter credentials in order to register. If network is under enforcement, device is isolated until registered. The machine is registered to the user. **Note:** This method cannot be used in conjunction with the Windows Domain Single-Sign-On method.

Personal Devices: Agent is either pre-installed or must be installed via the Captive Portal upon initial connection to the network. User enters credentials to register. Device is registered to the user.

Agent Deployment Preparation

Planning is required before the Persistent Agent can be deployed.

Deployment Methods

Considerations:

- Whether or not rogue hosts are isolated and presented with the Captive Portal.
- Ability to install software through the use of a software management program (such as a GPO Policy, Casper or Munki).
- Whether or not hosts login to a domain.

Software Management Program

This method is recommended in corporate environments and in any environment where software is used to distribute programs to hosts.

When using software management programs (such as a GPO Policy, Casper or Munki), the administrator has the ability to modify the Persistent Agent settings and push them to the hosts. This provides flexibility to adjust the settings used for agent communication to be the most appropriate for the environment and use case.

Important: If a software management program is used to install the agent, then it should also be used for updating the agent version.

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.

Imaging

If computers are imaged prior to deployment, the agent software can be included in the master image.

Captive Portal

This method is recommended in environments where distribution via software management is not available.

The end user downloads the agent through the Captive Portal during the onboarding process. If there are multiple FortiNAC Pods and users are allowed to roam between them, DNS SRV records will be required in the production domain server(s) for proper agent communication while roaming.

Manual Installation

This method is commonly used for testing purposes before pushing the agent globally. The agent file is downloaded from the Administrative UI and installed on an individual host via a USB drive or some other means.

FortiNAC SSL Certificates

In order for the agent to successfully communicate, SSL Certificates must be installed in FortiNAC. Hosts running the agent must have the appropriate Certificate Authority (CA) root/intermediate certificate installed to validate trust. There are different certificates available to secure communication.

Corporate Owned Internal CA: Using either a SAN (Subject Alternative Name) or Wildcard certificate is recommended in a High Availability or multi-pod environment. This allows the administrator to use the same certificate on all FortiNAC appliances.

When this is needed:

- Prevent non-corporate devices with the agent installed from communicating with FortiNAC.

Requirements:

- FortiNAC must have all the internal CA's intermediate and root certificates installed. See Cookbook recipe FortiNAC SSL Certificates for installation instructions.
- Host must have all the internal CA's root certificates installed for the Local Machine (not the Current User). This can be done via Group Policy, Software Management Distribution program or manually. See KB article Verify Trusted Certificate Authorities on Windows or MacOSX.

Public Third Party SSL certificates: root/intermediate certificates are typically updated via OS updates automatically. Using either a SAN (Subject Alternative Name) or Wildcard certificate is recommended in a High Availability or multi-pod environment. This allows the administrator to use the same certificate on all FortiNAC appliances. Public certificates are commonly used in educational facilities.

When this is needed:

- Environments where Internal CA Certificates are not available.

Requirements:

- FortiNAC must have all the public CA's intermediate and root certificates installed. See Cookbook recipe FortiNAC SSL Certificates for installation instructions.

FortiNAC Settings for Persistent Agent

Required configurations for the Agent (if any) and FortiNAC. They are configured using the Administration UI.

Considerations:

- The number of FortiNAC systems in use (single or multiple).
    - If multiple systems, which ones a host would be allowed to connect when roaming between sites.
- If High Availability is configured.
- Whether or not to use DNS SRV records for server identification. (Note: SRV records are not needed if the server names are specified in the Persistent Agent Settings).
- Whether or not it is desired for the agent to be invisible to the end user.
- Desire for rogue domain hosts to automatically register upon logging in to the domain.

"Require Connected Adapter" Feature in Multi-Pod Environment

When a Persistent Agent communicates to a FortiNAC pod, if any of the adapters represented by the Persistent Agent are online on the pod, FortiNAC accepts the communication. If none of the adapters represented by the Persistent Agent are online on the pod, FortiNAC responds to the agent that it should attempt to communicate to the next FortiNAC Server in the "allowedServer" list.

If the checkbox is not enabled, FortiNAC does not discern whether or not the host is connected to its pod. Consequently, if there are no ACLs blocking agent traffic between pod locations, the agent will continue to communicate with the original pod.

When this is needed: In multi-pod **e**nvironments where there are no ACLs blocking agent communication between pods. This feature ensures the agent communicates with its local pod when roaming.

Navigate to **Security Configuration > Agent Settings > Security Management**

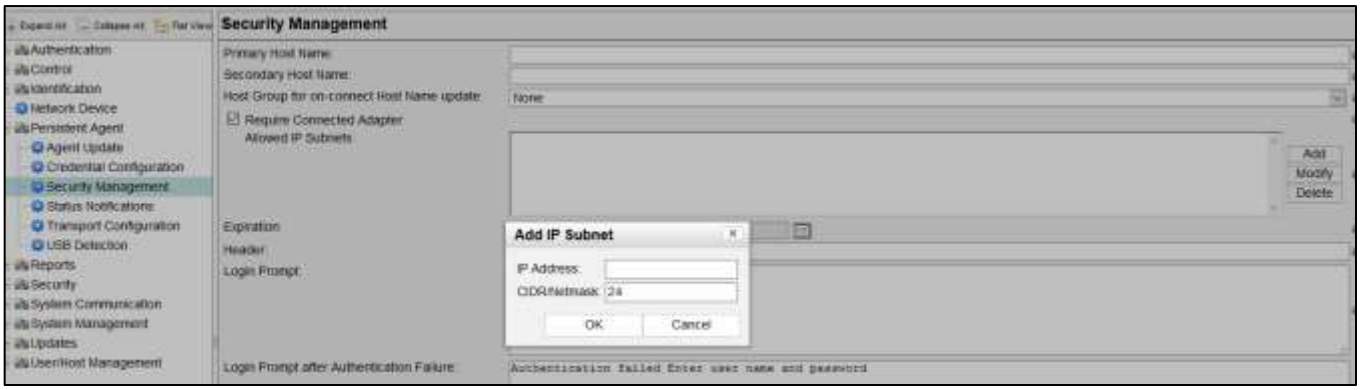
Allowed IP Subnets

Pods requiring the "Require Connected Adapter" option may need to communicate with agents on computers whose online status cannot be determined. Examples are:

- VPN-connected machines
- VMs in a server farm behind an aggregated link
- Machines behind a switch that is not managed by FortiNAC

In such situations, the "Allowed IP Subnets" option can be used. This option allows FortiNAC to communicate with agents from the specified subnets regardless of connection status.

Both the "Require Connected Adapter" and "Allowed IP Subnets" options are found in the Administration UI under **System > Settings > Persistent Agent > Security Management**.



For more information regarding this option, refer to the Settings/Persistent Agent Settings/Security Management section of the Administration Guide.

Other screens applicable to Persistent agent configuration are under **System > Settings > Persistent Agent.** These should be reviewed and edited based upon requirements.

Global Updates (Global agent should *not* be enabled if upgrading via software management)
Credential Configuration
Security Management
Status Notifications
Transport Configuration
USB Detection

For Multiple Pod environment use cases, see the following in the Appendix for recommended Settings for FortiNAC and agent software:
Agent Distributed Via Software Management/Image
Agent Distributed Via Software Management/Image (DNS Sub Domains)
Agent Distributed Via Captive Portal

Persistent Agent Settings

Persistent Agent settings are configurable when distributing the agent via software. They are not configurable when the agent is downloaded from the Captive Portal. Default values apply for any settings not modified.

The following are commonly used settings. For a complete list of settings, refer to the following sections in the Administration Guide:
Persistent Agent on Windows
Persistent Agent on macOS
Persistent Agent on Linux

Security: Indicates whether security is enabled or disabled. By default, Security is enabled.
Why this is needed:

- Protect from potential "Man in the Middle" attacks.
- Required when using the Restrict Roaming feature.
- Required when using the Require Connected Adapter feature.

Important:

- It is strongly recommended to leave security enabled. SSL certificates must be installed in FortiNAC and endstations.
- **Agent versions 5.3 and greater**: This option is no longer available. Security cannot be disabled and SSL certificates are required.

Home Server: Server with which the agent always attempts to communicate prior to those in the Allowed Servers list. If upgrading from agent version 2.x, Home Server is populated by the contents of Server IP. If Home Server is not set, it is automatically populated using Server Discovery. Home Server is updated in the default location (e.g. HKLM\Software\Bradford Networks\Client Security Agent) and does not change once populated.
When this is needed: The production Domain Server does not have SRV records for the appliance.

Allowed Servers: 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 Servers with which the agent can communicate.
When this is needed:

- High Availability configurations (Layer 2 or Layer 3): IP address or the FQDN of both Primary and Secondary FortiNAC Servers must be included. Using the shared IP address (available in Layer 2 HA configurations) is no longer recommended.
- In multi-pod environments where it is desired to restrict the agent communication to only a portion of the appliances the agent could potentially talk to, ***or…***
- The production Domain Server does not have SRV records for the appliances.

Restrict Roaming: If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent will attempt to communicate with servers whose SRV records were received, but may not be listed as either the Home Server or one of the Allowed Servers. This feature only applies when the Home Server entry is populated and Security is enabled. By default, Restrict Roaming is disabled.

When this is needed:

- To restrict agent communication to only the names specified in the homeServer and AllowedServers settings.

Balloon Notifications: Enables or Disables Balloon Notifications on a per-machine or per-user basis. By default, this setting is enabled.
When this is needed: To alert end user of host state changes.

Login Dialog: Enables or Disables the login dialog on a per-machine or per-user basis. By default, this setting is enabled.
When this is needed:

- Users are required to manually enter their credentials for registration or authentication.

System Tray Icon: Enables or Disables the System Tray Icon on a per-machine or per-user basis. By default, the System Tray Icon is displayed.

Last Connected Server (Requires Persistent Agent version 4.1.4 or higher):
The Persistent Agent keeps track of the FortiNAC server that it most recently successfully connected to and tries to connect to that server first when it needs to reconnect. If connecting to that server is unsuccessful, the Persistent Agent then attempts to connect to the other servers in the list, which are the servers from SRV records, followed by any that are from the Home Server or Allowed Servers.
When this is needed: Improves performance of the Persistent Agent in environments with multiple FortiNAC servers. Most helpful in multi-pod environments where there are several appliances the agent could attempt to connect.

Discover Servers, Priority, and Ports: (Requires Persistent Agent version 5.3 or higher): Enable or Disable Discovery via SRV. The agent will search for SRV Records to prioritize servers and override default ports. If connections to servers are not limited, agents will connect to the discovered server names as well. Enabled by default.
When this is needed: Required when neither homeServer nor AllowedServers are configured. In such cases, FortiNAC must perform discovery to determine the name of the appliance with which to communicate. Otherwise, communication will fail. See Persistent Agent Server Discovery Process for details.

Use the space below to note which settings (if any) will need to be changed from their default values.

Home Server:
Allowed Servers:
Restrict Roaming:
Balloon Notifications:
Login Dialog:
System Tray Icon:
Discovery using SRV Lookup:

For Multiple Pod environment use cases, see the following in the Appendix for recommended Settings for FortiNAC and agent software:
Agent Distributed Via Software Management/Image
Agent Distributed Via Software Management/Image (DNS Sub Domains)
Agent Distributed Via Captive Portal

Stage Agent for Deployment

Software Management Program

1. Ensure latest agent has been downloaded to FortiNAC. For instructions see **Download new agent packages** in section Agent Packages of the Administration Guide.

2. Copy the installer(s) to the machine that will be distributing the agent. Use the installer file formats listed below for the specific operating systems.

   Windows: **.msi**
   Linux (Debian, Ubuntu): **.deb**
   Linux (RHEL, Fedora, CentOS): **.rpm**

   For instructions see **Download the Persistent Agent For custom distribution** in section Agent Packages of the Administration Guide.

3. Configure the software management program to distribute the agent package and Persistent Agent software settings. Modify the Persistent Agent settings as necessary based upon the information from the section Software Modifiable Settings for the Persistent Agent.

   Important: It is strongly recommended to push the Persistent Agents settings separately; do not modify the installer. If the installer is modified in any way, any or all customization may be removed upon updating or uninstalling the agent.

   Configuration can be done in a variety of ways:
   - If Group Policy will be used, see Agent Settings and Packages Domain Distribution in the Appendix for instructions.
   - For all other management programs, refer to vendor documentation for operation instructions.

The Persistent Agent settings are configured within the Policy Settings (as opposed to default settings). These settings take precedence over the Default Settings.

Persistent Agent Policy Settings Location

Windows	32-bit operating systems (Registry Key): HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent 64-bit operating systems (Registry Key): HKLM\Software\wow6432node\Policies\Bradford Networks\Persistent Agent

MacOS	/Library/Preferences/com.bradfordnetworks.bndaemon.policy
Linux*	/etc/xdg/com.bradfordnetworks/ PersistentAgentPolicy.conf

*Best practice: PersistentAgentPolicy.conf should be ASCII encoding. As of FortiNAC 8.7.0, UTF-8 can also be parsed.

For more details, see Persistent Agent Settings File Location on Host in the Appendix.

For implementation steps for company asset use cases and recommended Persistent Agent Settings, refer to the following sections:

Windows Domain (Silent Onboard (Single-Sign-On))
MacOS Machines (Onboard Through Isolation)
Linux Machines (Onboard Through Isolation)
MacOS Machines (Silent Onboard)
Linux Machines (Silent Onboard)

Imaging

1. Choose a secure staging area for the machines to be imaged. Keep the switch in this area out of enforcement to ensure the machine has proper network access and can complete the imaging process. If port is under enforcement, FortiNAC may inadvertently switch the VLAN and interrupt the process.

2. Ensure latest agent has been downloaded to FortiNAC. For instructions see **Download new agent packages** in section Agent Packages of the Administration Guide.

3. Download agent package from FortiNAC to the machine with the master image. Use the file formats listed below for the specific operating systems.

   Windows: **.exe**
   Linux (Debian, Ubuntu): **.deb**
   Linux (RHEL, Fedora, CentOS): **.rpm**

   For instructions see **Download the Persistent Agent For custom distribution** in section Agent Packages of the Administration Guide.

4. Install the agent software. Refer to the applicable section in the Administration Guide:
   Installation for Windows
   Installation for macOS
   Installation for Linux

   Important: It is strongly recommended to configure the Persistent Agents settings separately; do not modify the installer. If the installer is modified in any way, any or all customization may be removed upon updating or uninstalling the agent.

5. Configure the Persistent Agent software settings as necessary based upon the information from the section Software Modifiable Settings for the Persistent Agent. The Persistent Agent settings are configured within the Policy Settings (as opposed to default settings). For details, see Persistent Agent Settings File Location on Host. Configuration can be done in a variety of ways:

    - Group Policy: see Agent Settings and Packages Domain Distribution in the Appendix for instructions.
    - For all other software management programs, refer to vendor documentation for operation instructions.
    - Add configuration as part of the master image.

The Persistent Agent settings are configured within the Policy Settings (as opposed to default settings). These settings take precedence over the Default Settings.

Persistent Agent Policy Settings Location

Windows	32-bit operating systems (Registry Key): HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent 64-bit operating systems (Registry Key): HKLM\Software\wow6432node\Policies\Bradford Networks\Persistent Agent
MacOS	/Library/Preferences/com.bradfordnetworks.bndaemon.policy
Linux*	/etc/xdg/com.bradfordnetworks/ PersistentAgentPolicy.conf

*Best practice: PersistentAgentPolicy.conf should be ASCII encoding. As of FortiNAC 8.7.0, UTF-8 can also be parsed.

For more details, see Persistent Agent Settings File Location on Host in the Appendix.

For implementation steps for company asset use cases and recommended Persistent Agent Settings, refer to the following sections:

Windows Domain (Silent Onboard (Single-Sign-On))
MacOS Machines (Onboard Through Isolation)
Linux Machines (Onboard Through Isolation)
MacOS Machines (Silent Onboard)
Linux Machines (Silent Onboard)

Captive Portal

1. Configure Captive Portal Pages. For instructions refer to section Portal Content Editor in the Administration Guide.

2. Ensure latest agent package has been downloaded to FortiNAC. For instructions see **Download new agent packages** under section Agent packages in the Administration Guide.

3. If High Availability environment (Layer 2 or Layer 3):
   - Navigate to **Security Configuration > Agent Settings > Security Management**
   - Primary Host Name: Primary Server IP or hostname
   - Secondary Host Name: Secondary Server IP or hostname

   Using the shared IP address (available in Layer 2 HA configurations) is no longer recommended.

4. If hosts are able to roam between multiple FortiNAC pods, create SRV records on the production DNS server(s) using the configurations outlined in section DNS server configuration in the in the Administration Guide.

5. Configure the Endpoint Compliance Policy to deliver the agent to a small number of test hosts during registration. Use the file formats listed below for the specific operating systems.

   Windows: **.exe**
   Linux (Debian, Ubuntu): **.deb**
   Linux (RHEL, Fedora, CentOS): **.rpm**

   For instructions refer to section Endpoint compliance policies in the Administration guide.

6. Validate the following:
   - Downloading and installation of the agent
   - Scanning
   - Remediation process

7. Once validation is complete, modify the policy configuration to the appropriate criteria for delivering to registering hosts.

Manual Installation

Prior to globally distributing the agent, it is common practice to download the agent from a file share or USB drive and run the installer on a select number of test machines.

1. Ensure latest agent has been downloaded to FortiNAC. For instructions see **Download new agent packages** in section Agent Packages of the Administration Guide.

2. Download agent package from FortiNAC. Use the file formats listed below for the specific operating systems.

   Windows: **.exe**
   Linux (Debian, Ubuntu): **.deb**
   Linux (RHEL, Fedora, CentOS): **.rpm**

   For instructions see **Download the Persistent Agent For custom distribution** in section Agent Packages of the Administration Guide.

3. Install the agent on the end machine. Refer to the applicable section in the Administration Guide:
   Installation for Windows
   Installation for macOS
   Installation for Linux

4. Modify the Persistent Agent settings (if necessary) using the notes taken during the section Software Modifiable Settings for the Persistent Agent.

The Persistent Agent settings are configured within the Policy Settings (as opposed to default settings). These settings take precedence over the Default Settings.

Persistent Agent Policy Settings Location

Windows	32-bit operating systems (Registry Key): HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent 64-bit operating systems (Registry Key): HKLM\Software\wow6432node\Policies\Bradford Networks\Persistent Agent
MacOS	/Library/Preferences/com.bradfordnetworks.bndaemon.policy
Linux*	/etc/xdg/com.bradfordnetworks/ PersistentAgentPolicy.conf

*Best practice: PersistentAgentPolicy.conf should be ASCII encoding. As of FortiNAC 8.7.0, UTF-8 can also be parsed.

For more details, see Persistent Agent Settings File Location on Host in the Appendix.

Registration Use Cases: Company Assets

Windows Domain (Silent Onboard (Single-Sign-On))

Windows machines are automatically registered when the user logs on to the domain. This method is recommended for Windows domain machines and is transparent to the end user.

How it Works:
The agent listens for changes in the Windows logon sessions. Any session activity (such as logon, logoff, lock, unlock or remote connection) triggers the agent to send the information to FortiNAC.

1. The Persistent Agent and applicable Persistent Agent Settings are pushed to the domain machines.
2. User enters credentials to logon to the Windows domain.
3. The Persistent Agent submits the NETBIOS domain name and sAMAccountName to FortiNAC.
4. FortiNAC determines the directory group to which the user belongs.
5. If the directory group matches, the applicable Passive Agent Configuration is applied.
6. Based on the Passive Agent Configuration, the Windows machine is registered.

Requirements:

- Under **System > Settings > LDAP > User Attributes**, Identifier = **sAMAccountName**
- Agent Deployment Method: Software Management Program
- Windows machine is a member of a domain
- User ID is a valid User ID in the domain
- User account must have Last Name

Review Software Modifiable Settings for the Persistent Agent for other settings that may need to be modified.

Configure

Important: To prevent network interruption, register all Windows domain assets from within the production network prior to the enforcement phase of the implementation.

1. In the FortiNAC Administrative UI, navigate to **Security Configuration > Agent Settings > Credential Configuration.**
2. Select "**Enable Registration**" and "**Register as Device**."
3. Select Authentication Type.
4. Click **Save Settings**.
5. Navigate to **Security Configuration > Passive Agent**.
6. Click **Add**.

7. Configure the Passive Agent Rule to register Windows domain machines during the initial push of the agents. Set the following:
    - If rule will only apply to members of a specific AD Group.
    - Register As: **Device**.
    - Whether or not the host will be scanned.
    - FortiNAC Host Group to which host will be added. Adding hosts to a group (such as "Company Assets") helps keep track of which hosts were registered using this rule and not some other means.
8. Click **OK**.
9. Verify FortiNAC can match a userID against the rule:
    - Click **Test**
    - Enter a User Name that should authenticate to the domain.
    - Enter Domain Name
    - Click **OK**
    - A message should display stating the rule matches.
10. Configure any other necessary FortiNAC configurations. See FortiNAC Settings.
11. Push Persistent Agent settings to existing Windows machines using a software management program. See Stage Agent for Deployment - Software Management Program.

    32-bit operating systems (Registry Key): **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent**

    64-bit operating systems (Registry Key): **HKLM\Software\wow6432node\Policies\Bradford Networks\Persistent Agent**

Recommended Persistent Agent Settings

Option	Value	Data Type	Data	Function
Home Server	homeServer	String	FortiNAC Server or Application Server fully-qualified hostname	Name of FortiNAC appliance with which the agent must communicate.
Allowed Servers	allowedServers	String	Comma-separated list of fully-qualified hostnames with which the agent can communicate. "a.example.com, b.example.com" (Important: no spaces between commas and names)	Needed if agent could potentially roam to multiple FortiNAC appliances (NCM environment or High Availability).

Recommended Persistent Agent Settings (continued)

Option	Value	Data Type	Data	Function
Restrict Roaming	restrictRoaming	DWORD	1	Agent will only communicate with server names provided by homeServer and allowedServers settings.
Login Dialog	LoginDialogDisabled	DWORD	1	Credential popup will not display to the user.
System Tray Icon	ShowIcon	DWORD	0	System tray icon will not display.
Balloon Notifications	ClientStateEnabled	DWORD	0	State change notifications will not display.

12. Push Persistent Agent installer (.msi) to existing Windows machines using a software management program. It is not necessary to reboot the domain machine.
13. Once the agent has been pushed, Windows machines will register the next time they are logged in to the domain.

Validate

If any of the below do not work as expected, see KB article Troubleshooting the Persistent Agent.

1. Login to domain
2. Search for Windows machine in **Users & Hosts > Hosts.**
3. Verify the following:
   - Host record displays as registered.
   - UserID is displayed under "Logged On User" column.
   - The appropriate Endpoint Compliance Policy matches (right click on host and select **Policy Details**)
   - The applicable scan runs (right click on host and select **Host Health**)
   - The scan result accurately reflects the machine posture (e.g. does the scan pass when it should have failed?)

After the network has been enforced:

1. (This step applies if the only machines registering using the PA are Windows computers). Disable the "Enable registration" option in the **Security Configuration > Agent Settings > Credential Configuration**. This prevents automatic registration of non-domain machines that have the Persistent Agent. **Note:** If Mac or Linux machines are also registered using the PA, this setting must remain enabled.
2. Use a secure staging area for newly purchased/imaged PC's to register Windows domain machines.
   - Adding the agent to the disk image is recommended.
   - Keep the switch in this area out of enforcement so the machine can login to the domain.

MacOS Machines (Onboard Through Isolation)

How it Works:

1. Device connects to the network.
2. Persistent Agent initiates communication with FortiNAC.
3. FortiNAC determines the host is a rogue and sends message to the agent to prompt for credentials.
4. The agent displays a pop-up dialog box.
5. User enters credentials in the dialog box.
6. Persistent Agent submits the credentials to FortiNAC.
7. FortiNAC validates the user credentials with the authentication server.
8. Once authentication is successful, FortiNAC registers the device to the user record.

Note the following:

- This method cannot be used in conjunction with the Windows Domain Single-Sign-On method
- Logged on users are not tracked for Mac and Linux
- It is recommended to push the agent to a sample group of machines for validation first.

Requirements:

- Agent Deployment Method: Software Management Program
- Root access to the Mac machine

Configure

1. Navigate to **Security Configuration > Agent Settings > Credential Configuration**
2. Select "**Enable Registration**"
3. Configure any other FortiNAC configurations noted previously.
4. Create the Persistent Agent Settings policy file to be pushed to macOS machines. This file will override the default settings.

    a. Install Persistent agent on a test machine. For instructions, see section **Installation for macOS** of the Administration Guide in the Fortinet Document Library.

    b. In the test machine CLI using Terminal, create the policy file **com.bradfordnetworks.bndaemon.policy**

```
sudo cp /Library/Preferences/com.bradfordnetworks.bndaemon.plist /Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist
```

Note: Root access is required. If already logged in as root, the use of "sudo" in the syntax is not required.

    c. Modify the new policy plist file with the appropriate Persistent Agent Settings. The following table provides recommended settings. Review Software Modifiable Settings for the Persistent Agent for additional options.

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy <value> -<Data Type> <Data>
```

Recommended Persistent Agent Settings

Option	Value	Data Type	Data	Function
Home Server	homeServer	String	FortiNAC Server or Application Server fully-qualified hostname	Name of FortiNAC appliance with which the agent must communicate.
Allowed Servers	allowedServers	String	Comma-separated list of fully-qualified hostnames with which the agent can communicate. "a.example.com, b.example.com" (Important: no spaces between commas and names)	Needed if agent could potentially roam to multiple FortiNAC appliances (NCM environment or High Availability).
Restrict Roaming	restrictRoaming	Integer	1	Agent will only communicate with server names provided by homeServer and allowedServers settings.
System Tray Icon	ShowIcon	Integer	0	System tray icon will not display.
Balloon Notifications	ClientStateEnabled	Integer	0	State change notifications will not display.

Example

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy homeServer -string server.company.com
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy allowedServers -string
server1.company.com,server2.company.com
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy restrictRoaming -integer 1
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy ShowIcon -integer 0
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy ClientStateEnabled -integer 0
```

To view contents of the file:
sudo defaults read /Library/Preferences/com.bradfordnetworks.bndaemon.policy

5. Push **com.bradfordnetworks.bndaemon.policy** to the **/Library/Preferences/** directory on existing macOS machines using a software management program.
6. Push the agent package to macOS machines using the software management program.

Validate

1. Connect host to network. Pop-up dialogue box should appear in machine to prompt for credentials.
2. Search for Windows machine in **Users & Hosts > Hosts.** Verify the Host record displays as rogue.

3. After entering credentials in pop-up dialogue box, confirm the appropriate Endpoint Compliance Policy matches (right click on host and select **Policy Details**).
4. To verify the applicable scan runs, right click on host and select **Host Health.**
5. Verify the scan result accurately reflects the machine posture (e.g. does the scan pass when it should have failed?)

If any of the above do not work as expected, see KB article Troubleshooting the Persistent Agent.

Linux Machines (Onboard Through Isolation)

How it Works:

1. Device connects to the network.
2. Persistent Agent initiates communication with FortiNAC.
3. FortiNAC determines the host is a rogue and sends message to the agent to prompt for credentials.
4. The agent displays a pop-up dialog box.
5. User enters credentials in the dialog box.
6. Persistent Agent submits the credentials to FortiNAC.
7. FortiNAC validates the user credentials with the authentication server.
8. Once authentication is successful, FortiNAC registers the device to the user record.

Note the following:

- This method cannot be used in conjunction with the Windows Domain Single-Sign-On method
- Logged on users are not tracked for Mac and Linux

Requirements:

- Agent Deployment Method: Software Management Program
- Root access to the Mac machine

Configure

1. Navigate to **Security Configuration > Agent Settings > Credential Configuration**
2. Select "**Enable Registration**"
3. Configure any other FortiNAC configurations noted previously.
4. Create the Persistent Agent Settings policy file to be pushed to Linux machines. This file will override the default settings.

    a. Install Persistent agent on a test machine. For instructions, see section Installation for Linux of the Administration Guide.
    b. In the test machine CLI, create policy file PersistentAgentPolicy.conf by making a copy of PersistentAgent.conf

```
sudo cp /etc/xdg/com.bradfordnetworks/PersistentAgent.conf /etc/xdg/com.bradfordnetworks/PersistentAgentPolicy.conf
```

Note: Root access is required. If already logged in as root, the use of "sudo" in the syntax is not required.

c. Modify the new policy file with the appropriate Persistent Agent Settings. The following table provides recommended settings. Review Software Modifiable Settings for the Persistent Agent for additional options.

vi PersistentAgentPolicy.conf

Best practice: PersistentAgentPolicy.conf should be ASCII encoding. As of FortiNAC 8.7.0, UTF-8 can also be parsed.

Recommended Persistent Agent Settings

Option	Value	Data Type	Data	Function
Home Server	homeServer	String	FortiNAC Server or Application Server fully-qualified hostname	Name of FortiNAC appliance with which the agent must communicate.
Allowed Servers	allowedServers	String	Comma-separated list of additional fully-qualified hostnames with which the agent can communicate. "a.example.com, b.example.com" (Important: no spaces between comma and names)	Needed if agent could potentially roam to multiple FortiNAC appliances (NCM environment or High Availability).
Restrict Roaming	restrictRoaming	Integer	true	Agent will only communicate with server names provided by homeServer and allowedServers settings.
System Tray Icon	ShowIcon	Integer	0	System tray icon will not display.
Balloon Notifications	ClientStateEnabled	Integer	0	State change notifications will not display.

Example

```
allowedServers=server1.company.com,server2.company.com
restrictRoaming=true
ShowIcon=0
ClientStateEnabled=0
```

d. Push **PersistentAgentPolicy.conf** to the **/etc/xdg/com.bradfordnetworks** directory of the Linux machines using a software management program.
e. Push agent package to Linux machines using the software management program.

Validate

1. Connect host to network. Pop-up dialogue box should appear in machine to prompt for credentials.
2. Search for Windows machine in **Users & Hosts > Hosts.** Verify the Host record displays as rogue.
3. After entering credentials in pop-up dialogue box, confirm the appropriate Endpoint Compliance Policy matches (right click on host and select **Policy Details**).
4. To verify the applicable scan runs, right click on host and select **Host Health.**
5. Verify the scan result accurately reflects the machine posture (e.g. does the scan pass when it should have failed?)

If any of the above do not work as expected, see KB article Troubleshooting the Persistent Agent.

MacOS Machines (Silent Onboard)

The macOS machine automatically registers upon connecting to the network once the installed Persistent Agent communicates with FortiNAC. This method is transparent to the end user.

How it Works:

1. Device connects to the network.
2. Persistent Agent initiates communication with FortiNAC.
3. FortiNAC registers the device (does not associate device with user).

Note the Following:

- This method can be used in conjunction with the Windows Domain Single-Sign-On method.
- Logged on users are not tracked for Mac and Linux.

Requirements:

- Agent Deployment Method: Software Management Program
- Root access to the Mac machine

Review Software Modifiable Settings for the Persistent Agent for other settings that may need to be modified.

Configuration

1. Navigate to **Security Configuration > Agent Settings > Credential Configuration**
2. Select "**Enable Registration**" and "**Register as Device**."
3. Configure any other necessary FortiNAC configurations. See FortiNAC Settings.
4. Create the Persistent Agent Settings policy file to be pushed to macOS machines. This file will override the default settings.
    a. Install Persistent agent on a test machine. For instructions, see section Installation for macOS of the Administration Guide.

b. In the test machine CLI using Terminal, create the policy file **com.bradfordnetworks.bndaemon.policy**

```
sudo cp /Library/Preferences/com.bradfordnetworks.bndaemon.plist /Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist
```

c. **Note:** Root access is required. If already logged in as root, the use of "sudo" in the syntax is not required.

d. Modify the new policy plist file with the appropriate Persistent Agent Settings. The following table provides recommended settings. Review Software Modifiable Settings for the Persistent Agent for additional options.

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy <value> -<Data Type> <Data>
```

Recommended Persistent Agent Settings

Option	Value	Data Type	Data	Function
Home Server	homeServer	String	FortiNAC Server or Application Server fully-qualified hostname	Name of FortiNAC appliance with which the agent must communicate.
Allowed Servers	allowedServers	String	Comma-separated list of fully-qualified hostnames with which the agent can communicate. "a.example.com, b.example.com" (Important: no spaces between commas and names)	Needed if agent could potentially roam to multiple FortiNAC appliances (NCM environment or High Availability).
Restrict Roaming	restrictRoaming	Integer	1	Agent will only communicate with server names provided by homeServer and allowedServers settings.
Login Dialog	LoginDialogDisabled	Integer	1	Credential popup will not display to the user.
System Tray Icon	ShowIcon	Integer	0	System tray icon will not display.
Balloon Notifications	ClientStateEnabled	Integer	0	State change notifications will not display.

Example

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy homeServer -string server.company.com
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy allowedServers -string a.example.com, b.example.com
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy restrictRoaming -integer 1
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy LoginDialogDisabled -integer 1
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy ShowIcon -integer 0
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy ClientStateEnabled -integer 0
```

To view contents of the file:
sudo defaults read /Library/Preferences/com.bradfordnetworks.bndaemon.policy

5. Push **com.bradfordnetworks.bndaemon.policy** to the **/Library/Preferences/** directory on existing macOS machines using a software management program.
6. Push the agent package to macOS machines using the software management program.

Validate

1. Connect host to network.
2. Search for Windows machine in **Users & Hosts > Hosts.**
3. Verify the following:
   - Host record displays as registered.
   - UserID is displayed under "Logged On User" column.
   - The appropriate Endpoint Compliance Policy matches (right click on host and select **Policy Details**)
   - The applicable scan runs (right click on host and select **Host Health**)
   - The scan result accurately reflects the machine posture (e.g. does the scan pass when it should have failed?)

If any of the above do not work as expected, see KB article Troubleshooting the Persistent Agent.

After the network has been enforced:
1. Leave "**Register as Device**" enabled.
2. Create a scan policy that checks for a specific value defining the asset.
3. Do one of the following:
   a. Enable Forced Remediation. If the host fails the scan, the host will register. However, it will be marked "At Risk" and placed in an Isolation VLAN.
   b. Forced Remediation alternative: send an email notification for the Security Risk Host event. **Note:** if Forced Remediation is not used, non-domain machines with the Persistent Agent that auto register may gain access to the production network.

MacOS Manual Registration

Device is registered via Administrative UI by an administrator. This method is transparent to the end user.

Configuration Procedure:
1. Navigate to **Users & Hosts > Hosts**.
2. Search for device. Right click and select **Register as Host** or **Register as Device**.

Linux Machines (Silent Onboard)

The Linux machine automatically registers upon connecting to the network once the installed Persistent Agent communicates with FortiNAC. This method is transparent to the end user.

How it Works:

1. Device connects to the network.
2. Persistent Agent initiates communication with FortiNAC.
3. FortiNAC registers the device (does not associate device with user).

Note the Following:

- This method can be used in conjunction with the Windows Domain Single-Sign-On method.
- Logged on users are not tracked for Mac and Linux.

Requirements:

- Agent Deployment Method: Software Management Program
- Root access to the Mac machine

Review Software Modifiable Settings for the Persistent Agent for other settings that may need to be modified.

Configuration

1. Navigate to **Security Configuration > Agent Settings > Credential Configuration**
2. Select "**Enable Registration**" and "**Register as Device**."
3. Configure any other necessary FortiNAC configurations. See FortiNAC Settings.
4. Create the Persistent Agent Settings policy file to be pushed to Linux machines. This file will override the default settings.

    a. Install Persistent agent on a test machine. For instructions, see section **Installation for Linux** of the Administration Guide in the Fortinet Document Library.
    b. In the test machine CLI, create policy file PersistentAgentPolicy.conf by making a copy of PersistentAgent.conf

```
sudo cp /etc/xdg/com.bradfordnetworks/PersistentAgent.conf /etc/xdg/com.bradfordnetworks/PersistentAgentPolicy.conf
```

Note: Root access is required. If already logged in as root, the use of "sudo" in the syntax is not required.

c. Modify the new policy file with the appropriate Persistent Agent Settings. The following table provides recommended settings. Review Software Modifiable Settings for the Persistent Agent for additional options.

vi PersistentAgentPolicy.conf

Best practice: PersistentAgentPolicy.conf should be ASCII encoding. As of FortiNAC 8.7.0, UTF-8 can also be parsed.

Recommended Persistent Agent Settings

Option	Value	Data Type	Data	Function
Home Server	homeServer	String	FortiNAC Server or Application Server fully-qualified hostname	Name of FortiNAC appliance with which the agent must communicate.
Allowed Servers	allowedServers	String	Comma-separated list of fully-qualified hostnames with which the agent can communicate. "a.example.com, b.example.com" (Important: no spaces between commas and names)	Needed if agent could potentially roam to multiple FortiNAC appliances (NCM environment or High Availability).
Restrict Roaming	restrictRoaming	Integer	true	Agent will only communicate with server names provided by homeServer and allowedServers settings.
Login Dialog	LoginDialogDisabled	Integer	1	Credential popup will not display to the user.
System Tray Icon	ShowIcon	Integer	0	System tray icon will not display.
Balloon Notifications	ClientStateEnabled	Integer	0	State change notifications will not display.

Example

```
allowedServers=a.example.com,b.example.com
restrictRoaming=true
ShowIcon=0
ClientStateEnabled=0
LoginDialogDisabled=1
```

5. Push **PersistentAgentPolicy.conf** to the **/etc/xdg/com.bradfordnetworks** directory of Linux machines using a software management program.
6. Push agent package to Linux machines using the software management program.

Validate

4. Connect host to network.
5. Search for Windows machine in **Users & Hosts > Hosts.**

6. Verify the following:
    - Host record displays as registered.
    - UserID is displayed under "Logged On User" column.
    - The appropriate Endpoint Compliance Policy matches (right click on host and select **Policy Details**)
    - The applicable scan runs (right click on host and select **Host Health**)
    - The scan result accurately reflects the machine posture (e.g. does the scan pass when it should have failed?)

If any of the above do not work as expected, see KB article Troubleshooting the Persistent Agent.

After the network has been enforced:

1. Leave "**Register as Device**" enabled.
2. Create a scan policy that checks for a specific value defining the asset.
3. Do one of the following:
    a. Enable Forced Remediation. If the host fails the scan, the host will register. However, it will be marked "At Risk" and placed in an Isolation VLAN.
    b. Forced Remediation alternative: send an email notification for the Security Risk Host event. **Note:** if Forced Remediation is not used, non-domain machines with the Persistent Agent that auto register may gain access to the production network.

Registration Use Cases: Personal Devices

How it Works (Persistent Agent pre-installed):

1. Device connects to the network.
2. Persistent Agent initiates communication with FortiNAC.
3. FortiNAC determines the host is a rogue and sends message to the agent to prompt for credentials.
4. The agent displays a pop-up dialog box.
5. User enters credentials in the dialog box.
6. Persistent Agent submits the credentials to FortiNAC.
7. FortiNAC validates the user credentials with the authentication server.
8. Once authentication is successful, FortiNAC registers the device to the user record.

How it Works (Persistent Agent installed via Captive Portal-Assumes network under enforcement):

1. Device connects to the network.
2. FortiNAC determines device is unknown (rogue). Device is isolated and Captive Portal is presented once browser is opened.
3. User enters their credentials to register.
4. FortiNAC matches the device with the appropriate Endpoint Compliance Policy (determines which agent type and version to distribute as well as which scan to run)
5. User is prompted to download the agent.
6. User installs agent.
7. FortiNAC sends message to the agent to prompt for credentials.
8. The agent displays a pop-up dialog box.
9. User enters credentials in the dialog box.
10. Persistent Agent submits the credentials to FortiNAC.
11. FortiNAC validates the user credentials with the authentication server.
12. Once authentication is successful, FortiNAC registers the device to the user record.

Persistent Agent Multiple Pod Use Cases

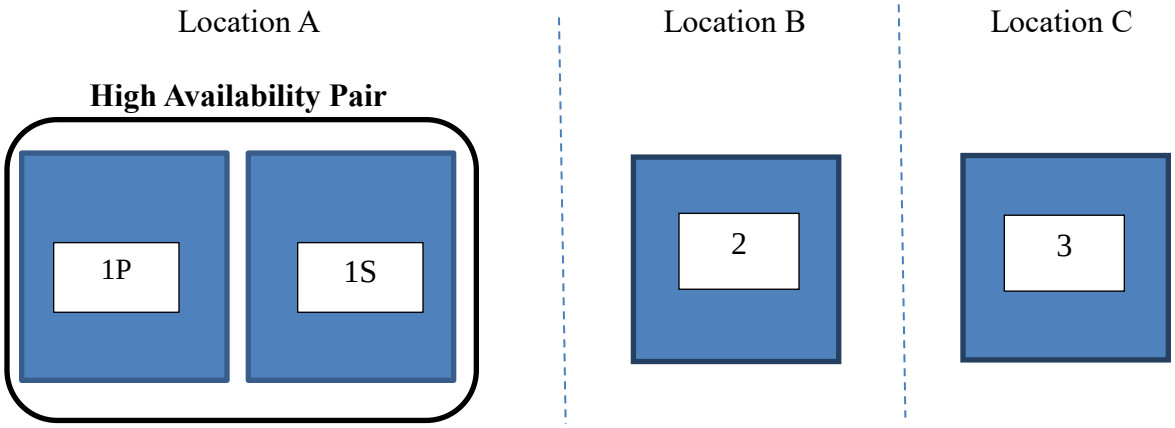
The following pages present two common multiple system environments and illustrate how the agent connects to each pod.

Order of Priority Agent Uses to Connect to Servers:

1. SRV Records
2. Last Connected Server
3. Home Server
4. Allowed Servers

See Persistent Agent Server Discovery Process in the Appendix for full details.

Use Case 1: Agent Distributed Via Software Management



The above example shows three locations:

- Server 1P Application Server and Server 1S Application Server in a High Availability pair at Location A.
- Server 2 Application Server at Location B.
- Server 3 Application Server at Location C.
- Production domain server does not have SRV records for the appliances.
- There are no ACLs configured between sites to block agent traffic.

Use Case 1 Requirements

- Single software image will be pushed to locations A & B.
- Agent communications allowed with Locations A & B only.
- One SSL Certificate will be used for all FortiNAC appliances.

Use Case 1 Recommended Settings and Configurations

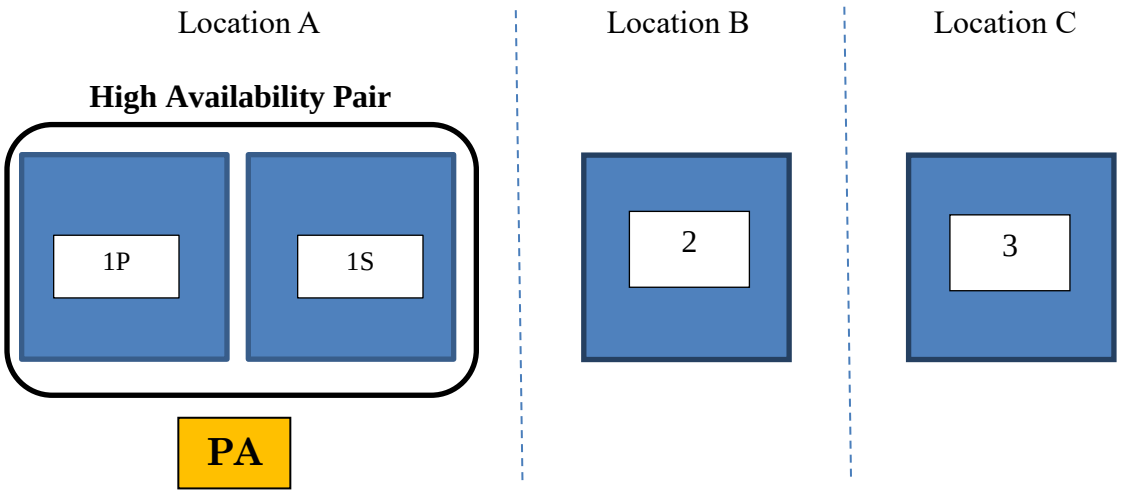
Persistent Agent Settings Configured via Software

Security	enabled
Allowed Servers	Server1P.domain.com Server1S.domain.com Server2.domain.com
Restrict Roaming	Enabled
Login Dialog	disabled
System Tray Icon	disabled

FortiNAC Settings

"Require Connected Adapter" Feature	enabled
Certificate Type for Persistent Agent Target	SAN or wildcard Certificate

Use Case 1 Scenarios: Persistent Agent Discovery - Host Connects to Location A



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
(none)	(none)	(none)	Server1P
			Server1S
			Server2

Server Connection List Order
Server1P
Server1S
Server2

As there are no SRV records and both the Last Connected Server and Home Server entries are empty, the agent will attempt to connect based on the Allowed Servers list.

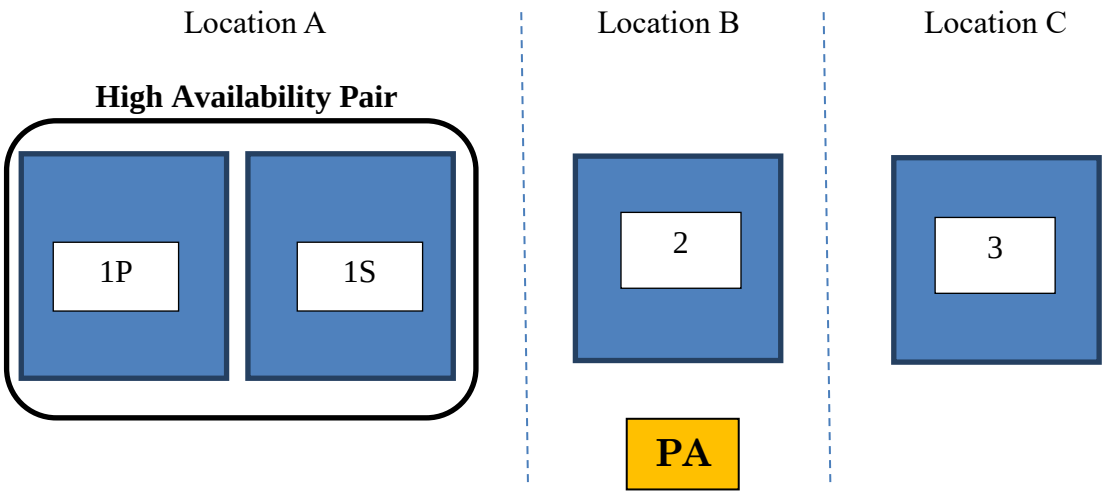
Resulting behavior:

1. Agent attempts to communicate with Server1P. Server1P is active and sees the host online so it responds.
2. Both the Last Connected Server and Home Server entries are populated with Server1P.

Last Connected Server	Home Server (Default Location)	Allowed Servers
Server1P	Server1P	Server1P
		Server1S
		Server2

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 1 Scenarios: Persistent Agent Discovery - Host Roams from Location A to Location B



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
Server1P	None	Server1P	Server1P
			Server1S
			Server2

Server Connection List Order
Server1P (Last Connected Server *and* Home Server)
Server1S (Next in Allowed Servers List)
Server2 (Next in Allowed Servers List)

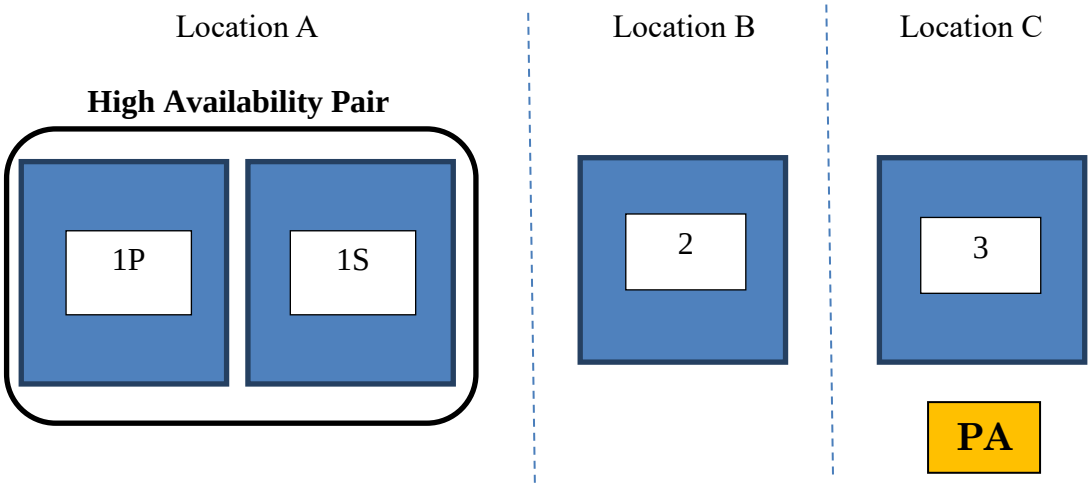
Resulting behavior:

1. Agent attempts to communicate with Server1P. Server1P sees the host offline, so it directs the agent to try the next server.
2. Agent attempts to communicate with Server1S. Server1S is in standby and does not respond.
3. Agent attempts to communicate with Server2. Server2 sees the host online so it responds.
4. The Last Connected Server entry is updated to Server2.

Last Connected Server	Home Server (Default Location)	Allowed Servers
Server2	Server1P	Server1P
		Server1S
		Server2

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 1 Scenarios: Persistent Agent Discovery - Host Roams from Location B to Location C



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
Server2	None	Server1P	Server1P
			Server1S
			Server2

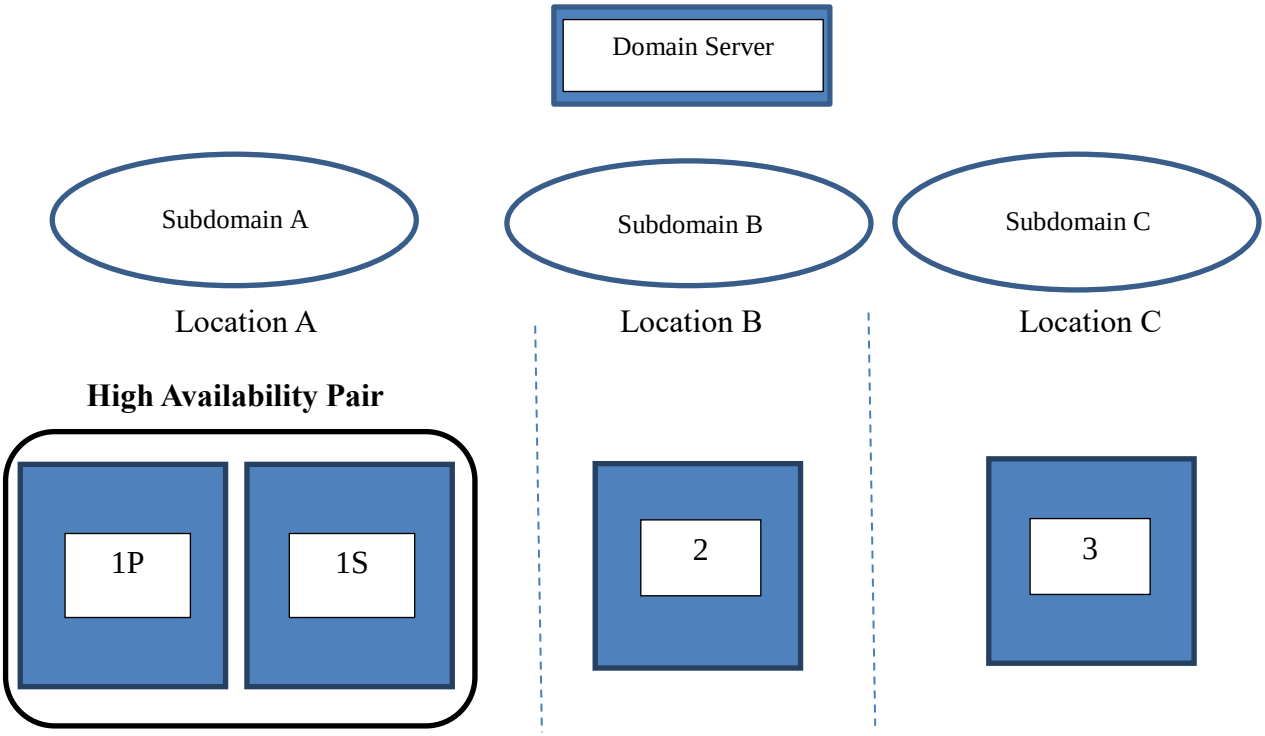
Server Connection List Order
Server2 (Last Connected Server)
Server1P (Home Server *and* first in Allowed Servers List)
Server1S (Next in Allowed Servers List)

Resulting behavior:

1. Agent attempts to communicate with Server2. Server2 sees the host offline, so it directs the agent to try the next server.
2. Agent attempts to communicate with Server1P. Server1P sees the host offline, so it directs the agent to try the next server.
3. Agent attempts to communicate with Server1S. Server1S is in standby and does not respond.

The agent will not attempt to connect to Server3 because it is not in the Allowed Servers list.

Use Case 2: Agent Distributed Via Software Management (DNS Sub Domains)



The above example shows three locations:

- Server 1P Application Server and Server 1S Application Server in a High Availability pair at Location A.
- Server 2 Application Server at Location B.
- Server 3 Application Server at Location C.
- Production domain server with SRV records for locations A, B and C.
- There are no ACLs configured between sites to block agent traffic.

Use Case 2 Requirements

- Single software image will be pushed to locations A & B.
- Agent communications allowed with Locations A & B only.
- One SSL Certificate will be used for all FortiNAC appliances.

Use Case 2 Recommended Settings and Configurations

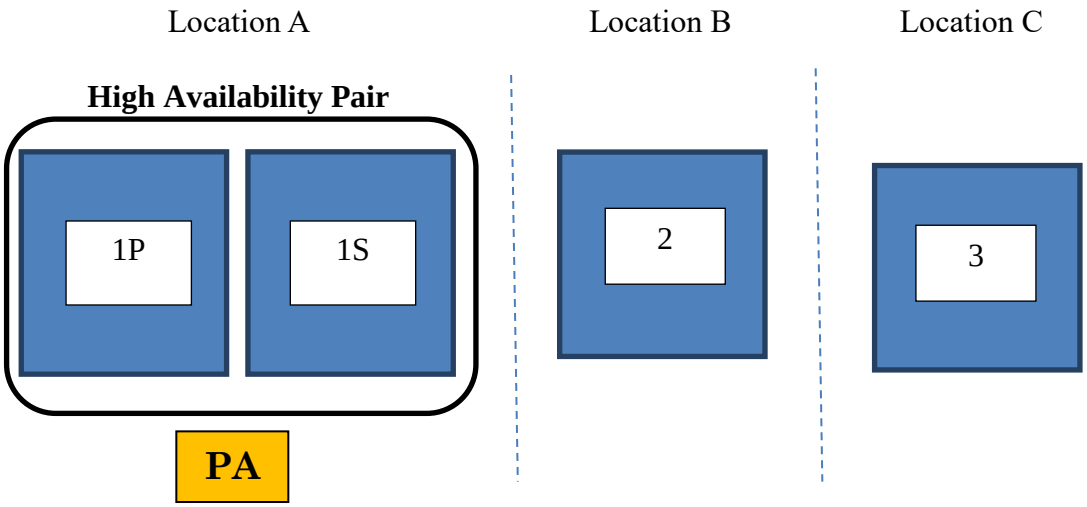
Persistent Agent Settings Configured via Software

Security	enabled
Allowed Servers	Server1P.a.domain.com Server1S.b.domain.com Server2.c.domain.com
Restrict Roaming	Enabled
Login Dialog	disabled
System Tray Icon	disabled

FortiNAC Settings

"Require Connected Adapter" Feature	enabled
Certificate Type for Persistent Agent Target	SAN or wildcard Certificate

Use Case 2 Scenarios: Persistent Agent Discovery - Host Connects to Location A



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
(none)	1P	(none)	Server1P
	1S		Server1S
			Server2

Server Connection List Order
Server1P (SRV *and* Allowed Servers List)
Server1S (SRV *and* Allowed Servers List)
Server2 (Next in Allowed Servers List)

Since SRV records were received for 1P and 1S and they are part of the Allowed Servers list, they will be prioritized. Since both the Last Connected Server and Home Server entries are empty, the agent will then proceed to attempt connection based on the Allowed Servers list.

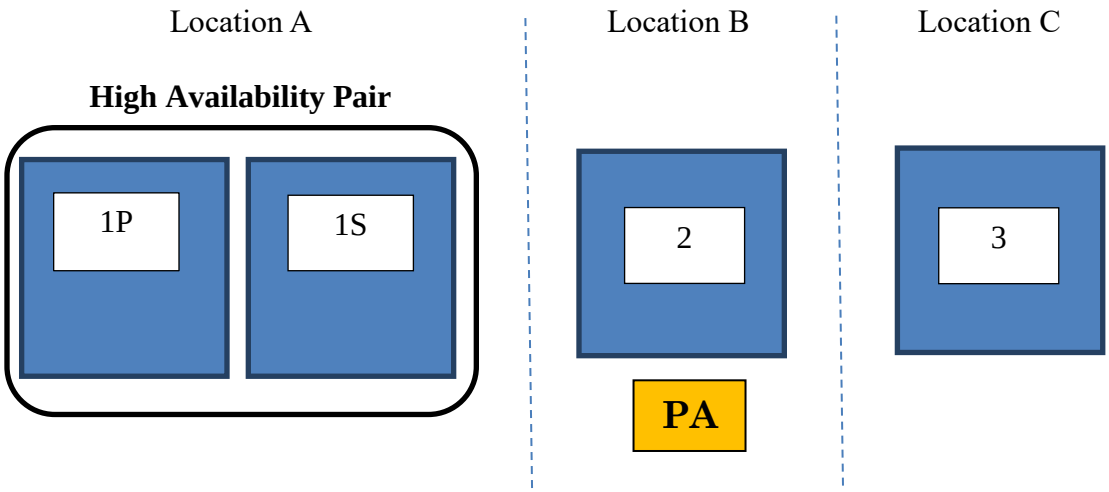
Resulting behavior:

1. Agent attempts to communicate with Server1P. Server1P is active and sees the host online so it responds.
2. Both the Last Connected Server and Home Server entries are populated with Server1P.

Last Connected Server	Home Server (Default Location)	Allowed Servers
Server1P	Server1P	Server1P
		Server1S
		Server2

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 2 Scenarios: Persistent Agent Discovery – Roams from Location A to B



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
Server1P	Server2	Server1P	Server1P
			Server1S
			Server2

Server Connection List Order
Server2 (SRV *and* in Allowed Servers List)
Server1P (Last Connected Server *and* Home Server)
Server1S (Next in Allowed Servers List)

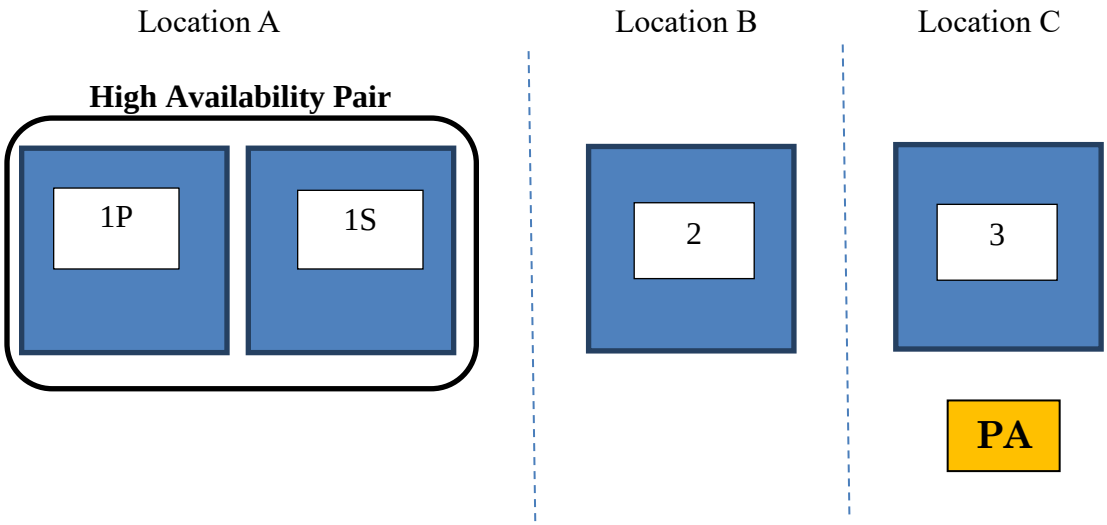
Resulting behavior:

1. Agent attempts to communicate with Server2. Server2 is active and sees the host online so it responds.
2. The Last Connected Server entry is updated to Server2.

Last Connected Server	Home Server (Default Location)	Allowed Servers
Server2	Server1P	Server1P
		Server1S
		Server2

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 2 Scenarios: Persistent Agent Discovery – Roams from Location B to C



Last Connected Server	SRV Records Received	Home Server (Default Location)	Allowed Servers
Server2	Server3	Server1P	Server1P
			Server1S
			Server2

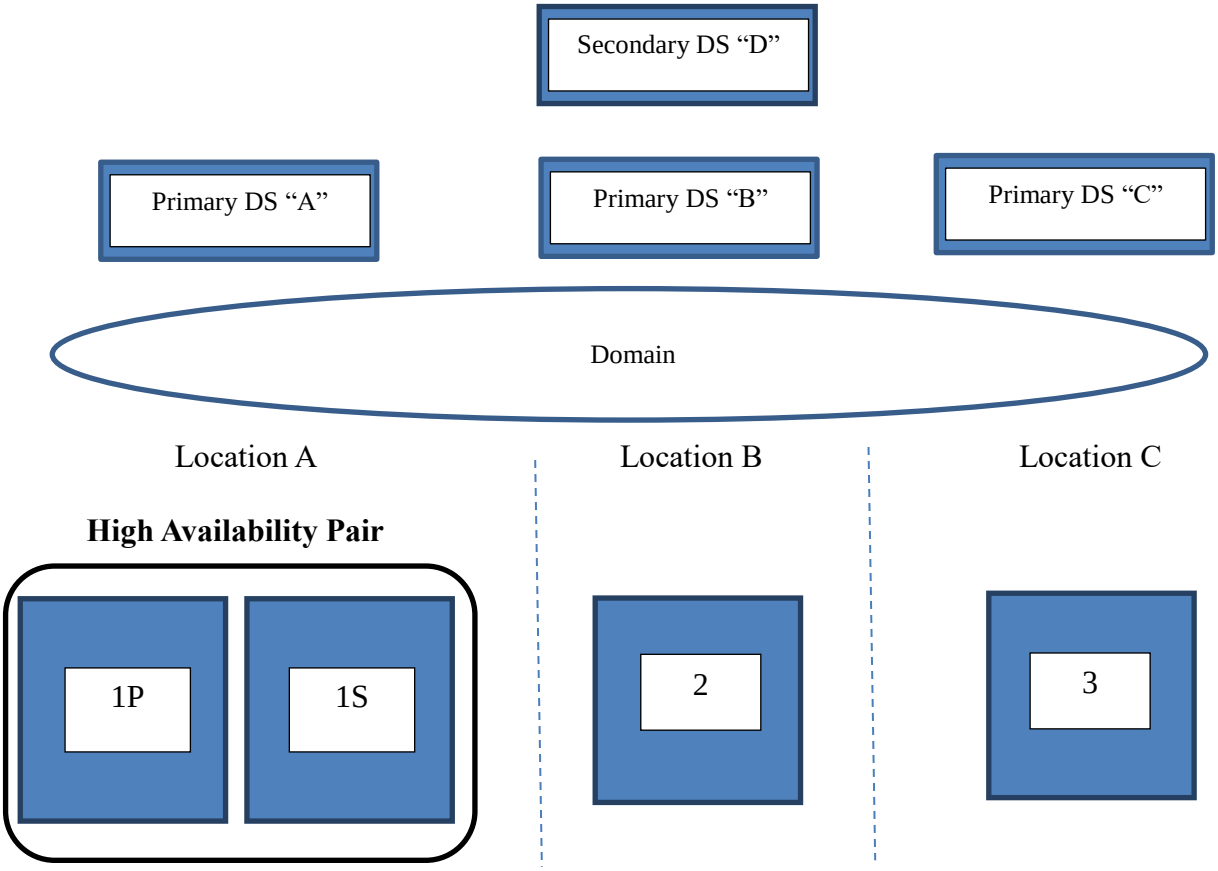
SRV record was received for Server3, but Server3 is not in the Allowed Servers List. Since Restrict Roaming is enabled, the agent will not attempt to connect to Server3.

Server Connection List Order
Server2 (Last Connected Server)
Server1P (Home Server *and* first in Allowed Servers List)
Server1S (Next in Allowed Servers List)

Resulting behavior:

1. Agent attempts to communicate with Server2. Server2 sees the host offline, so it directs the agent to try the next server.
2. Agent attempts to communicate with Server1P. Server1P sees the host offline, so it directs the agent to try the next server.
3. Agent attempts to communicate with Server1S. Server1S is in standby and does not respond.

Use Case 3: Agent Distributed Via Captive Portal



The above example shows three locations:

- Server 1P Application Server and Server 1S Application Server in a High Availability pair at Location A.
- Server 2 Application Server at Location B.
- Server 3 Application Server at Location C.
- Primary Production domain server A with SRV records for location A
- Primary Production domain server B with SRV records for location B
- Primary Production domain server C with SRV records for location C
- Secondary Production domain server D for all 3 locations.
- There are no ACLs configured between sites to block agent traffic.

Use Case 3 Requirements

- Host downloads Agent via Captive Portal.
- Agent communications allowed at all locations.
- One SSL Certificate will be used for all FortiNAC appliances.

Use Case 3 Recommended Settings and Configurations

Persistent Agent Settings (Automatically Configured Upon Agent Installation)

Security	enabled
Restrict Roaming	disabled
Login Dialog	enabled
System Tray Icon	enabled

FortiNAC Settings

"Require Connected Adapter" Feature	enabled
Certificate Type for Persistent Agent Target	SAN or wildcard Certificate

Since there is no Allowed Servers List to configure, DNS SRV records must be created in the production DNS Server. This will allow agents roaming between locations to communicate with the proper FortiNAC appliance.

DNS SRV Records

Primary Production Domain Server A	Server 1P, Server 1S
Primary Production Domain Server B	Server 2
Primary Production Domain Server C	Server 3
Secondary Production Domain Server D	Server 1P, Server 1S, Server 2, Server 3

Example:

DS A

_bradfordagent._udp SRV 0 0 4567 server1p.npu.ac.com
_bradfordagent._tcp SRV 0 0 4568 server1p.npu.ac.com

_bradfordagent._udp SRV 1 0 4567 server1s.npu.ac.com
_bradfordagent._tcp SRV 1 0 4568 server1s.npu.ac.com

DS B

_bradfordagent._udp SRV 2 0 4567 server2.npu.ac.com
_bradfordagent._tcp SRV 2 0 4568 server2.npu.ac.com

DS C

_bradfordagent._udp SRV 3 0 4567 server3.npu.ac.com
_bradfordagent._tcp SRV 3 0 4568 server3.npu.ac.com

DS D

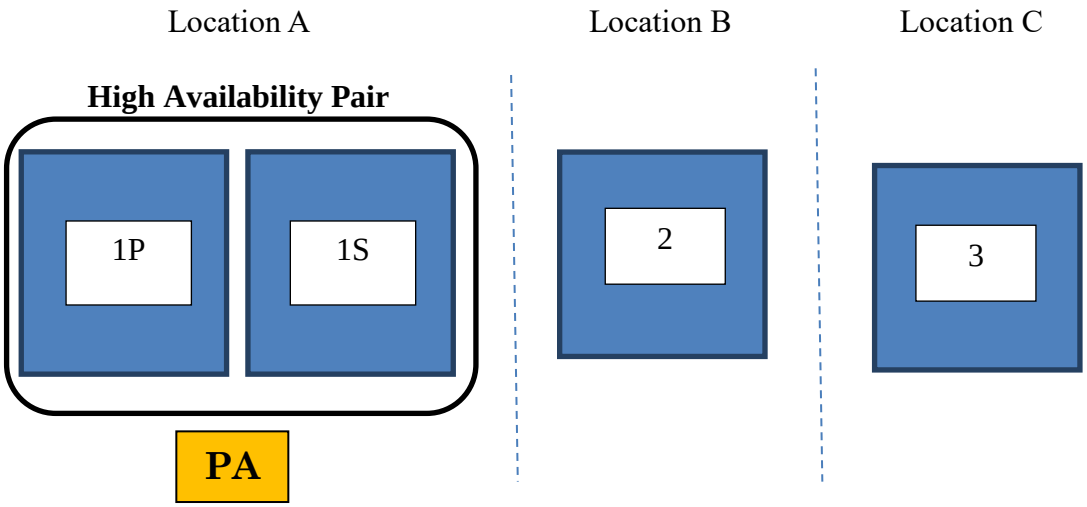
```
_bradfordagent._udp        SRV 0 0 4567 server1p.npu.ac.com
_bradfordagent._tcp        SRV 0 0 4568 server1p.npu.ac.com

_bradfordagent._udp        SRV 1 0 4567 server1s.npu.ac.com
_bradfordagent._tcp        SRV 1 0 4568 server1s.npu.ac.com

_bradfordagent._udp        SRV 2 0 4567 server2.npu.ac.com
_bradfordagent._tcp        SRV 2 0 4568 server2.npu.ac.com

_bradfordagent._udp        SRV 3 0 4567 server3.npu.ac.com
_bradfordagent._tcp        SRV 3 0 4568 server3.npu.ac.com
```

Use Case 3 Scenarios: Persistent Agent Discovery - Host Connects to Location A



Last Connected Server	SRV Records Received	Home Server (Default Location)
(none)	1P	(none)
	1S	

Server Connection List Order
Server1P (SRV)
Server1S (SRV)

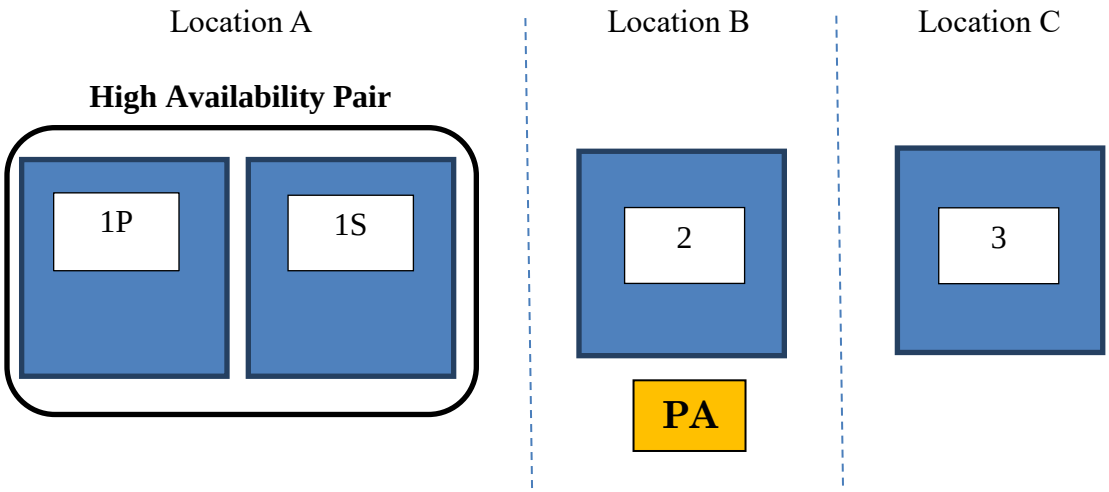
Resulting behavior:

1. Rogue host connects to network managed by Server 1P and is isolated. During the registration process, agent is downloaded from Server 1P and installed.
2. Agent attempts to communicate with Server1P. Server1P is active and sees the host online so it responds.
3. Both the Last Connected Server and Home Server entries are populated with Server1P.

Last Connected Server	Home Server (Default Location)
Server1P	Server1P

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 3 Scenarios: Persistent Agent Discovery – Roams from Location A to B



Last Connected Server	SRV Records Received	Home Server (Default Location)
Server1P	Server2	Server1P

Server Connection List Order
Server2 (SRV)
Server1P (Last Connected Server *and* Home Server)

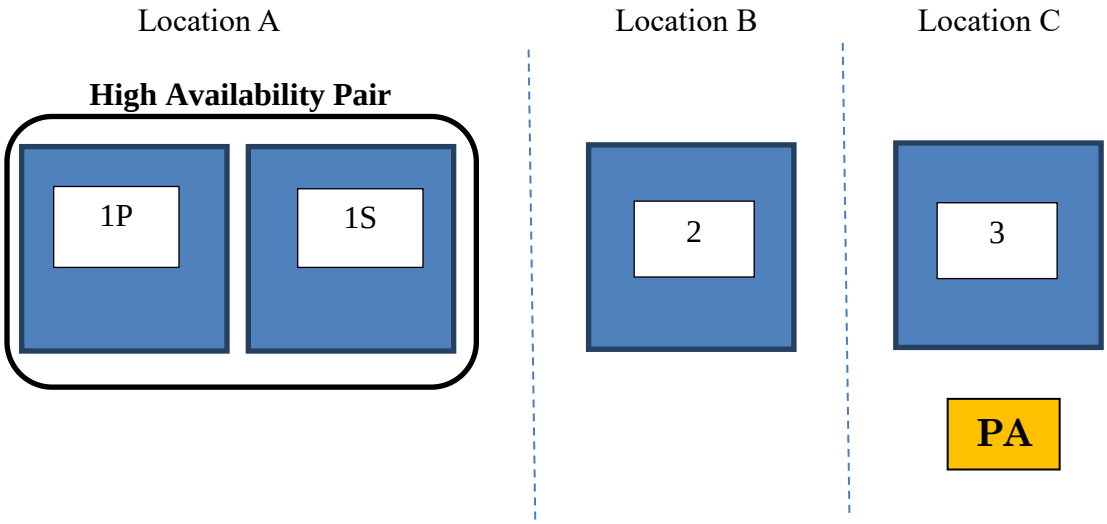
Resulting behavior:

1. Agent attempts to communicate with Server2. Server2 is active and sees the host online so it responds.
2. The Last Connected Server entry is updated to Server2.

Last Connected Server	Home Server (Default Location)
Server2	Server1P

The next time the agent attempts to communicate, unless the agent receives a DNS record from a different server in the list, the agent will try to connect to the Last Connected Server first.

Use Case 3 Scenarios: Persistent Agent Discovery – Roams from Location B to C and Primary DNS server is Down



Primary DS "C" is unreachable. Therefore, Secondary DS "D" is queried. DS "D" responds with SRV records for all FortiNAC appliances.

Last Connected Server	SRV Records Received	Home Server (Default Location)
Server2	Server1P	Server1P
	Server1S	
	Server2	
	Server3	

Server Connection List Order
Server2 (SRV *and* Last Connected Server)
Server1P (SRV *and* Home Server)
Server1S (SRV)
Server3 (SRV)

Resulting behavior:

1. Agent attempts to communicate with Server2. Server2 sees the host offline, so it directs the agent to try the next server.
2. Agent attempts to communicate with Server1P. Server1P sees the host offline, so it directs the agent to try the next server.
3. Agent attempts to communicate with Server1S. Server1S is in standby and does not respond.
4. Agent attempts to communicate with Server3. Server3 sees the host online and responds.

Troubleshooting

Related KB Articles

Troubleshooting the Persistent Agent
Connection issues with the Fortinet Persistent Agent
Windows Persistent Agent logs
Linux Persistent Agent Logs
macOS Persistent Agent logs

Debugging

Use the following KB article to gather the appropriate logs using the debugs below.
Gather logs for debugging and troubleshooting

Note: Debugs disable automatically upon restart of FortiNAC control and management processes.

Function	Syntax	Log File
Persistent Agent activity	`nacdebug -name PersistentAgent true`	/bsc/logs/output.nessus
Disable debug	`nacdebug -name <debug name> false`	N/A

Appendix

Persistent Agent Server Discovery Process

The Persistent Agent communicates on the following ports:

- Agent 3.x and 4.x: TCP 4568 and UDP 4567
- Agent 5.x and later with NAC 8.1 and lower: TCP 4568 and UDP 4567
- Agent 5.x and later with NAC 8.2 and later: TCP 4568 only
- All versions: TCP 80 (required for upgrades)

Discovery using SRV lookups (steps 2, 7 & 8) can be disabled in agent versions 5.3 and greater.

The discovery process is as follows:

1. The Persistent Agent starts.
2. The agent checks DNS for SRV records of _bradfordagent._udp.*example.com* and _bradfordagent._tcp.*example.com*.
3. The agent looks at the host registry (Windows) or preferences (OS X), or .conf (Linux).
4. First it checks the entry for lastConnectedServer. If lastConnectedServer is set, it adds the server to the top of the list.**
5. Then it checks the entry for HomeServer. If HomeServer is set, it adds it to a list.
6. Then the agent checks the entry for AllowedServers. This entry contains a list of additional servers to which the agent can connect. It adds each of these servers to the list.
7. If SRV records are returned, the agent processes them in reverse priority order (highest value first). If homeServer is not already set, the name contained in the SRV response is written to the host registry HKLM\Software\Bradford Networks\Client Security Agent (Windows) or preferences (OS X, Linux).*
8. For each SRV record:
    a. If the name is not already in the list, and restrictRoaming is disabled, the agent adds the name to the top of the list and to the lastConnectedServer value.**
    b. Otherwise, if the name is already in the list, the agent moves the name to the top of the list.
9. Now that the list of servers is complete, the agent tries to connect to each server over SSL/TLS until it successfully connects to one. Unless security is disabled on the agent, this is done over SSL/TLS (requires valid certificate installed for the Persistent Agent Certificate Target).
10. Once the agent has successfully connected to a server, that server will be set to the lastConnectedServer value, and moved to the top of the list.**
11. Once a server has been added to the lastConnectedServer, if restrictRoaming is enabled, it will remain at the top of the list until that server is no longer reachable by the agent. At that point the list will be parsed until the agent connects to a server and then that server will be moved to lastConnectedServer and to the top of the list.**

*Registry/preferences settings remain until one of the following occurs:

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

**Requires Agent Version 4.1.4 and higher.

Note: If the agent cannot be configured through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. Agents can then query the DNS servers to determine the FortiNAC server with which they should communicate.

Windows Files Directories and Commands

There are two locations where Persistent Agent Settings are stored:

- **Default Settings**: Upon installation of the Persistent Agent, the default settings are written to the vendor locations indicated in the chart below. Settings written to the default location remain until one of the following occurs:
  - Entry is manually changed.
  - Agent is uninstalled.
  - Agent is updated.

  Important:
  - The default location should not be used when pushing settings via software.
  - If the Persistent Agent installer is modified in any way, the update functionality in FortiNAC may remove any or all customization.

  Persistent Agent Default Settings Location
  32-bit operating systems (Registry Key):

  64-bit operating systems (Registry Key):

- **Policy Settings**: Used when pushing settings via software. These settings take precedence over the Default Settings. Policy Settings can only be changed via software push.

Description	Registry Key
(32-bit operating systems) Created upon installation of the agent. Contains all default Persistent Agent settings	HKLM\Software\Bradford Networks\Client Security Agent
(64-bit operating systems) Created upon installation of the agent. Contains all default Persistent Agent settings	HKLM\Software\wow6432node\Bradford Networks\Client Security Agent
(32-bit operating systems) Contains all non-default (Policy) Persistent Agent settings	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent
(64-bit operating systems) Contains all non-default (Policy) Persistent Agent settings	HKLM\Software\wow6432node\Policies\Bradford Networks\Persistent Agent

Stop/start the agent service

1. Under Services in the Control Panel, select **FortiNAC Persistent Agent Service**.
2. Stop the agent: right click and select **stop**.
3. Once the service shows stopped, right click and select **start**.

Alternatively, right click and select **restart**.

MacOS Files Directories and Commands

There are two locations where Persistent Agent Settings are stored:

- **Default Settings**: Upon installation of the Persistent Agent, the default settings are written to the files indicated in the chart below. Settings written to the default location remain until one of the following occurs:
  - Entry is manually changed.
  - Agent is uninstalled.
  - Agent is updated.

  Important:
  - The default location should not be used when pushing settings via software.
  - If the Persistent Agent installer is modified in any way, the update functionality in FortiNAC may remove any or all customization.

- **Policy Settings**: Used when pushing settings via software. These settings take precedence over the Default Settings. Policy Settings can only be changed via software push.

Files and Directories

Description	File or Directory
Created upon installation of the agent. Contains all default Persistent Agent settings	/Library/Preferences/com.bradfordnetworks.bndaemon.plist
Contains all non-default (Policy) Persistent Agent settings	/Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist
Directory Persistent Agent package is installed	/Library/Application Support/Bradford Networks/Persistent Agent
Persistent Agent management script	/Library/LaunchDaemons/com.bradfordnetworks.agent.plist

Commands

Description	Command
View default plist file	`sudo defaults read /Library/Preferences/com.bradfordnetworks.bndaemon`

Create a new policy file by making a copy of the default plist file	`sudo cp /Library/Preferences/com.bradfordnetworks.bndaemon.plist /Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist`
Stop the agent: Unload the launchDaemon plist.	`sudo launchctl unload /Library/LaunchDaemons/com.bradfordnetworks.agent.plist`
Start the agent: Reload the launchDaemon plist.	`sudo launchctl load /Library/LaunchDaemons/com.bradfordnetworks.agent.plist`
Uninstall agent	1. Go to `/Library/Application Support/Bradford Networks/Persistent Agent/Uninstall` 2. Once uninstalled, run the following command from the command line (Terminal) to forget the package: `sudo /usr/sbin/pkgutil --forget com.bradfordnetworks.PersistentAgent`

MacOS Agent Installation Example

1. Create a policy plist file for the Persistent Agent:

```
sudo cp /Library/Preferences/com.bradfordnetworks.bndaemon.plist
/Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist
```

2. Set the agent configuration parameter values (replace **fnac1.fortinet.com** and **fnac2.fortinet.com** with the fully qualified FortiNAC appliance host name(s)):

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy homeServer -
string fnac1.fortinet.com

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy allowedServers
-string fnac1.fortinet.com,fnac2.fortinet.com

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy restrictRoaming
-integer 1

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy ShowIcon -
integer 0

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy
ClientStateEnabled -integer 0

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy
LoginDialogDisabled -integer 1

sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon.policy securityEnabled
-integer 1
```

3. Install the newly created configuration file

   /Library/Preferences/com.bradfordnetworks.bndaemon.policy.plist

   With the Persistent Agent package

Linux Files Directories and Commands

There are two locations where Persistent Agent Settings are stored:

- **Default Settings**: Upon installation of the Persistent Agent, the default settings are written to the vendor locations indicated in the chart below. Settings written to the default location remain until one of the following occurs:
  - Entry is manually changed.
  - Agent is uninstalled.
  - Agent is updated.

  Important:
  - The default location should not be used when pushing settings via software.
  - If the Persistent Agent installer is modified in any way, the update functionality in FortiNAC may remove any or all customization.

- **Policy Settings**: Used when pushing settings via software. These settings take precedence over the Default Settings. Policy Settings can only be changed via software push.

Files and Directories

Description	File or Directory
Created upon installation of the agent. Contains default Persistent Agent settings	/etc/xdg/com.bradfordnetworks/PersistentAgent.conf
Contains all non-default (Policy) Persistent Agent settings	/etc/xdg/com.bradfordnetworks/ PersistentAgentPolicy.conf
Script which sets non-default Persistent Agent settings. Home Server Allowed Servers Restrict Roaming Writes to /etc/xdg/com.bradfordnetworks/ PersistentAgent.conf	/opt/com.bradfordnetworks/PersistentAgent/setup
Directory Persistent Agent package is installed	/opt/com.bradfordnetworks/PersistentAgent/
Persistent Agent service	/opt/com.bradfordnetworks/PersistentAgent/bndaemon
Agent logs	/var/log/bndaemon

Commands

Description	Command
Stop the agent	`sudo service bndaemon stop`
Start the agent	`sudo service bndaemon start`
Restart the agent	`sudo service bndaemon restart`
Install rpm file	`sudo rpm -Uvh <agent .rpm filename>`
Uninstall rpm file	`sudo rpm -ev fortinac-persistent-agent`
Install deb file	`sudo dpkg -i <agent .deb filename>`
Uninstall deb file	`sudo dpkg --purge fortinac-persistent-agent`

Agent Settings and Packages Domain Distribution

Administration 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.

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 template is provided by Fortinet and contain both the ADM and newer ADMX templates.
- Agent Package: Agent packages are provided by Fortinet. These files are copied to the server for distribution. Agent release notes can be downloaded from the Fortinet Document Library.

Procedure Overview

1. Obtain the following from FortiNAC:
    - Agent Executables
    - GPO Templates
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.

Step 1: Obtain GPO Templates and Agent Executables

1. In the FortiNAC Administration UI, navigate to **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window click **Download Administrative Templates for Windows Server** to download the 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.

Step 2: 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.

Configure Agent Settings in Template

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

Persistent Agent Template Settings

Option	Definition
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).
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 Network Sentry.
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.
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 Network Sentry servers. If roaming between servers is limited, list the FQDNs of the Network Sentry Application Servers or Network Sentry Servers with which the agent can communicate.

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 Network Sentry 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.

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 Network Sentry. **Data Type:** Integer **Default**: 960	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**
securityEnabled	**0** - Disable Agent Security **1** - Enable Agent Security **Data Type**: Integer **Default:** 1	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**

Value	Data	Key
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**
discoveryEnabled	Enable or Disable Discovery via SRV. The agent will search for SRV Records to prioritize servers and override default ports. If connections to servers are not limited, agents will connect to the discovered server names as well. **0** - Disable Discovery **1** - Enable Discovery **Data Type**: DWORD **Default**: 1	**HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ Bradford Networks\Persistent Agent**

Step 3: Copy Agent Executables to Domain Server

Copy the agent files to the Domain Server for distribution.

For details, refer to Microsoft documentation or contact Microsoft for assistance.

https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

Step 4: Push Template Settings to Computers

Step 5: Deploy the Persistent Agent

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

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. For details, see related Knowledge Base article https://community.fortinet.com/t5/FortiNAC/Technical-Note-Windows-or-Mac-OSX-hosts-with-Persistent-Agent/ta-p/194210.

Important: 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.

Delayed Autostart (Windows)

When configuring monitors, it is possible for false positives to occur depending upon the order services startup. For information on configuring monitors, see Monitor custom scans in the Add or modify a scan section of the Administration Guide.

Startup example (Service C is monitored):

1. Machine powers up
2. Persistent Agent service starts and initiates monitor
3. Service A starts
4. Service B starts
5. Monitor completes
6. Service C starts

Result: Monitor fails because Service C was not running at the time of the monitor.

Configure Delayed Autostart

Using Registry settings, the Agent Service can be configured for Autostart(Delayed), allowing other services to startup first.

Registry entry: HKLM\SYSTEM\CurrentControlSet\services\BNPagent\DelayedAutostart
Data Type: DWORD (32-bit)
Data Value: 1

Registration Entry: HKLM\SYSTEM\CurrentControlSet\services\BNPagent\AutoStartDelay
Data Type: DWORD (32-bit)
Data Value: Value in seconds (ex: 120 = 2 minutes)

It is recommended to test these settings on a machine first to validate the delay is long enough. Once validated, push the registry entries to the Windows machines using a software management program or Group Policy. **Note**: Once settings are pushed to machines, they may require a reboot in order for the settings to apply.

Reference:
https://social.technet.microsoft.com/Forums/Lync/en-US/d8f0e315-74d4-4890-a62f-ef427a8532e1/adjusting-the-autostart-delayed-start-time?forum=winservergen

Shutdown Order of Services (Windows)

When configuring monitors, it is possible for false positives to occur depending upon the order services shutdown. For information on configuring monitors, see Monitor custom scans in the Add or modify a scan section of the Administration Guide.

Shutdown example (Service C is monitored):

1. Shutdown initiated
2. Service C stops
3. Persistent Agent initiates monitor
4. Service B stops
5. Monitor completes
6. Service A stops
7. Persistent Agent stops

Result: Monitor fails because Service C was not running at the time of the monitor.

Configure the order in which services shutdown

Registry Entry: \HKLM\SYSTEM\CurrentControlSet\Control\PreshutdownOrder
Type: REG_MULTI_SZ

Add BNPagent to the top of the list so the service shuts down early in the process:

BNPagent
DeviceInstall
UsoSvc
gpsvc
trustedinstaller

Alternatively, add in the monitored service towards the bottom of the list:

BNPagent
DeviceInstall
UsoSvc
gpsvc
trustedinstaller
<Monitored Service>

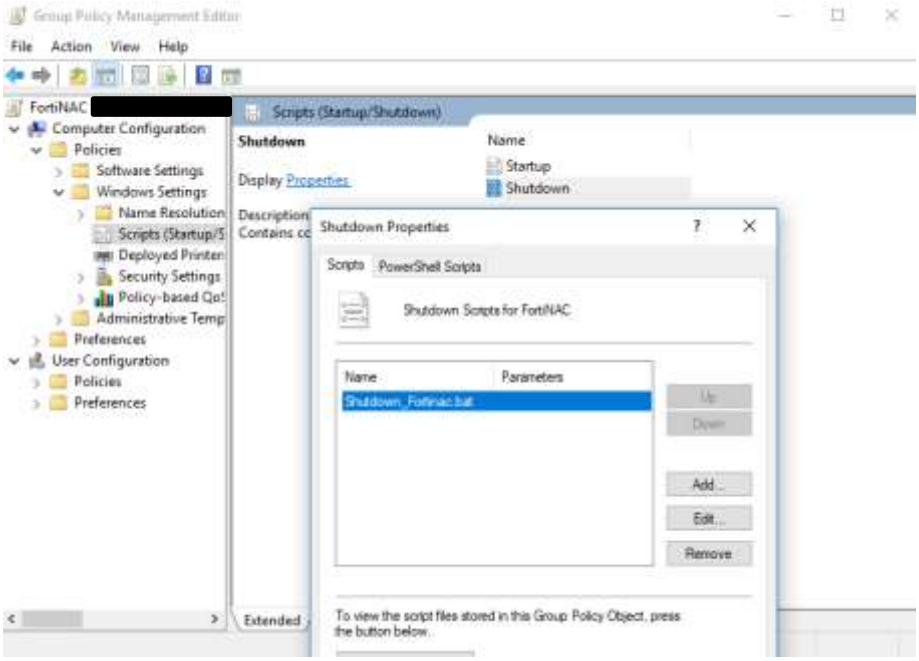
It is recommended to test these settings on a machine first to validate. Once validated, push the registry entries to the Windows machines using a software management program or Group Policy.
Note: Once settings are pushed to machines, they may require a reboot in order for the settings to apply.

GPO Shutdown Script Example

The following GPO script stops the service and logs to file

```
echo net stop BNPagent >>
\\<server>\Logs\FortinacShutdown\FortinacShutdown%Computername%.txt
net stop BNPagent >>
\\<server>\Logs\FortinacShutdown\FortinacShutdown%Computername%.txt 2>&1
echo Fortinac Shutdown on %Computername% %date% %time%. >>
\\<server>\Logs\FortinacShutdown\FortinacShutdown%Computername%.txt
echo ------------------------ >>
\\<server>\Logs\FortinacShutdown\FortinacShutdown%Computername%.txt
```

Place the script here:



Log sample output (FortinacShutdownMyComputer.txt content):

```
net stop BNPagent
The FortiNAC Persistent Agent Service service is stopping.
The FortiNAC Persistent Agent Service service was stopped successfully.

Fortinac Shutdown on MyComputer <timestamp>
-------------------------
```

Silent Install Script Parameters

Installs the Persistent Agent .msi package in quiet mode.
Command line parameter: **/quiet /passive**

The following example is from the Continuum RMM platform: