

This Quick Start introduces Websense Network Agent and summarizes the steps needed to successfully deploy the component in your network.

- ➔ **Overview** *What is Network Agent?, page 1*
- ➔ **Deployment Planning** *Where does Network Agent belong in the network?, page 2*
- ➔ **Configuration** *Using TRITON - Web Security to configure Network Agent, page 10*
- ➔ **Verification** *Verifying that Network Agent is working, page 15*
- ➔ **Troubleshooting** *Top Troubleshooting Tips, page 16*

What is Network Agent?

Websense Network Agent monitors Internet traffic for all or specified machines in a network.

- ◆ When you install Websense Web security solutions in standalone mode, Network Agent is used to filter both HTTP and non-HTTP traffic.
- ◆ When you integrate Websense Web security solutions with a firewall, proxy, or caching product, the integrated product passes HTTP and HTTPS content to Websense software for filtering. Traffic using other protocols can be managed by Network Agent.

Network Agent also captures bandwidth usage data for use in filtering and reporting.

When Network Agent is used to filter non-HTTP protocols, it can detect malicious peer-to-peer applications and spyware, even when they tunnel over ports commonly used for legitimate Internet communication. In addition, Network Agent can filter requests for Internet applications used for:

- ◆ instant messaging
- ◆ streaming media
- ◆ file sharing
- ◆ proxy avoidance
- ◆ Internet mail
- ◆ other network or database operations

When do I need more than one Network Agent instance?

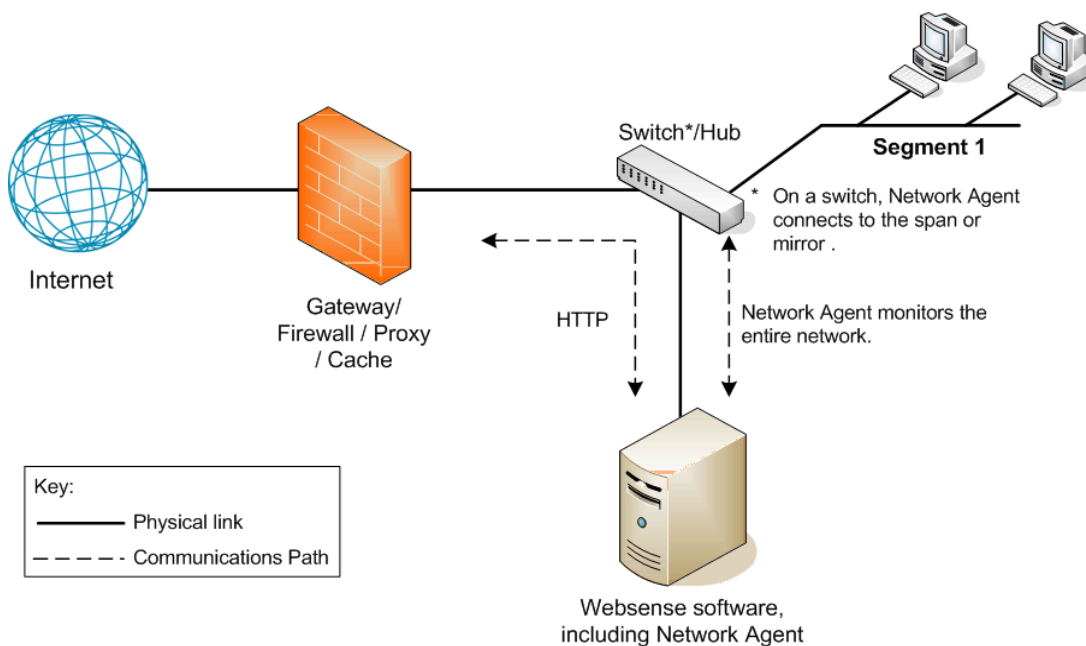
In a busy network, you may need multiple Network Agent instances to monitor all segments of your network.

The size and configuration of the network, the hardware capabilities of each Network Agent machine, and the volume and type of network traffic all play a role in determining how many Network Agent instances are needed. Some sites can use one Network Agent machine for every thousand users; others use one Network Agent machine for several thousand users.

Consult the *Deployment Guide* for detailed recommendations based on the size of your network and the volume of traffic being processed. In addition, Websense Technical Support and Sales Engineering can assist with deployment decisions.

Where does Network Agent belong in the network?

Install Network Agent where can it see all Internet requests (HTTP and non-HTTP) from the machines it is assigned to monitor. This monitoring must be done inside the firewall.



Optionally, deploy multiple Network Agent instances, with each instance monitoring a different segment of the network.

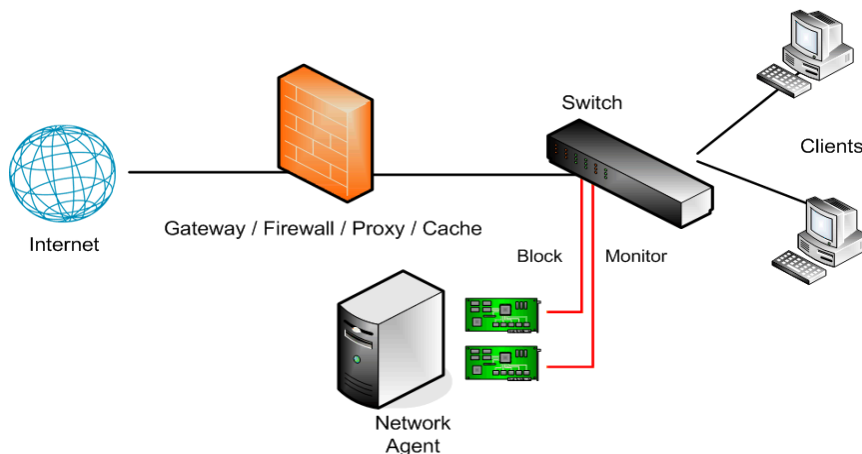
Network Agent machines can connect to the network via a switch (see [Connecting to a switch, page 3](#)) or hub (see [Connecting to a hub, page 4](#)).

Network Agent can be installed on the same machine as some integration products, but should never be installed on the same machine as the firewall (see [Connecting to a gateway, page 4](#)).

If your network includes a router or Network Address Translation (NAT) device, position Network Agent to see the original (not the translated) IP addresses for all monitored machines.

.Network interface cards (NICs)

Network Agent requires at least one network card (NIC) to monitor and block traffic, and can be configured to use multiple NICs.



Each NIC that Network Agent uses for monitoring must be able to see all inbound and outbound traffic for the network or segment that it is configured to monitor.

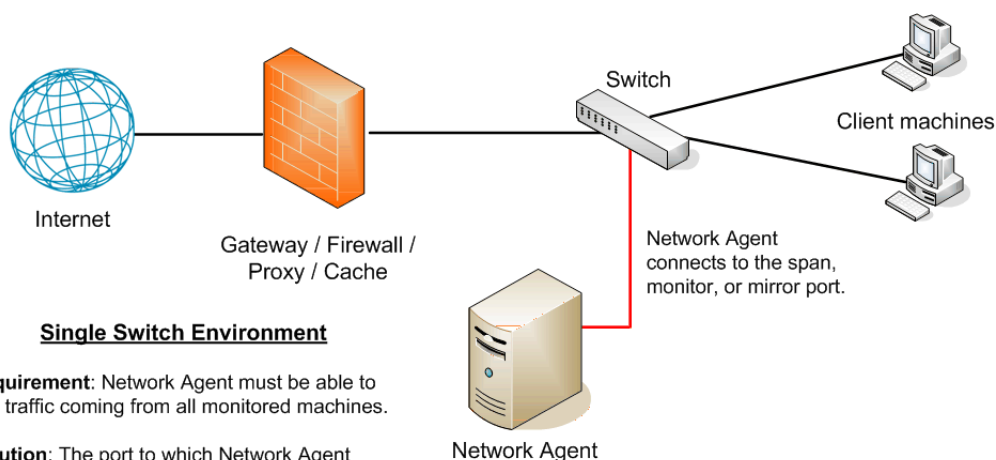
Install and configure each NIC before installing Network Agent:

- ◆ Each NIC must be connected to a hub or switch and enabled in the operating system.
- ◆ The NIC used to monitor traffic must be configured to capture all packets on the network, not only the packets addressed directly to it (promiscuous mode).

If you add a NIC after installing Network Agent, restart the Network Agent service, and then use TRITON - Web Security to configure the new NIC.

Connecting to a switch

If the device connected to the Network Agent machine is a switch, it must support port spanning (mirroring). This means that a copy of all network traffic seen on the switch is sent to the span or mirror port for monitoring.



Single Switch Environment

Requirement: Network Agent must be able to see traffic coming from all monitored machines.

Solution: The port to which Network Agent connects is configured to span or mirror the port to which the firewall is connected. All Internet traffic that passes through the firewall can then be monitored.

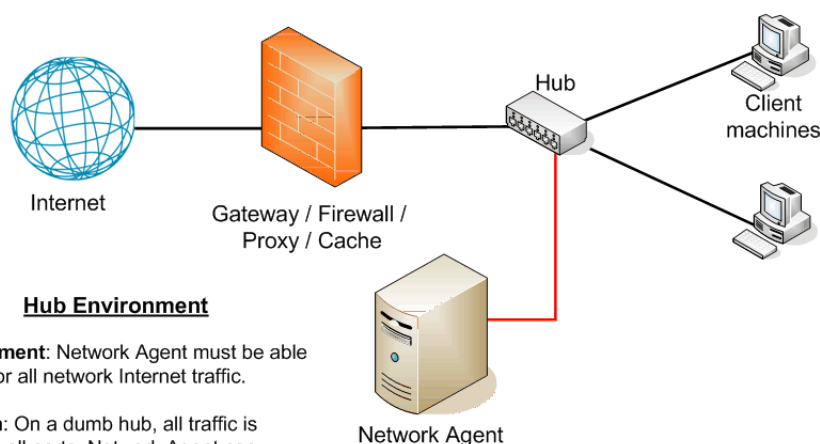
If you use a switch that supports bidirectional spanning (allowing packets to be monitored and sent from the same port), Network Agent needs only one NIC.

Some switches do not allow bidirectional traffic in spanning (mirroring) mode. The network card receiving data on the Network Agent machine can only listen, not send. In this case:

1. Use the NIC connected to the span port to monitor traffic.
2. Install a second NIC on the Network Agent machine. The NIC must have an IP address.
3. Attach the second NIC to a port that can communicate with all monitored machines and the Filtering Service machine.
4. Configure the second NIC as the blocking NIC.

Connecting to a hub

If the device connected to the Network Agent machine is a dumb hub (which distributes traffic to all ports), Network Agent requires only one NIC.



Hub Environment

Requirement: Network Agent must be able to monitor all network Internet traffic.

Solution: On a dumb hub, all traffic is visible to all ports; Network Agent can connect to any active port. On a smart hub, the port must be capable of mirroring or 2-way port spanning.

Network Agent must see the traffic, in both directions, for those segments of the network that it is assigned to monitor. The port to which the Network Agent machine is attached must be capable of bidirectional port spanning (mirroring).

Connecting to a gateway

A gateway provides a connection between two networks, such as between your network and the Internet.

In small to medium-sized Microsoft Windows environments, Network Agent can be installed on the gateway machine. This allows Network Agent to manage and monitor all Internet traffic. The gateway can either be a proxy server or a network appliance. Do **not** install Network Agent on a firewall.







Important

In larger networks, performance can suffer as a result of resource competition between the gateway software and Network Agent.

Planning Worksheets

The next 4 pages of this Quick Start are worksheets that you can use to capture all of the information you need to configure Network Agent for your environment.

-  **Worksheet 1** Ensure that the entire network is visible to Network Agent. Designate any internal (intranet) IP addresses to be monitored.
-  **Worksheet 2** Associate each Network Agent machine with a Filtering Service instance.
-  **Worksheet 3** Identify proxy and cache machines and Network Agent ports.
-  **Work sheet 4** Assign a network card (NIC) to each segment of the network, with no overlap. Identify IP addresses that should not be monitored.

Worksheet 1: Network Agent Global Settings (use once per network)

Network Agent must know which IP addresses are part of your internal network. The agent:

- ◆ Typically ignores communication sent from one internal IP address to another (intranet traffic)
- ◆ Can be configured to monitor traffic sent to specific internal IP addresses (such as Web servers)

This information is **not** used to determine whether or not Internet requests from these IP addresses are monitored.

Internal Network Definition

Identify the IP addresses in your network (by contiguous IP address range or individual IP address).

IP address ranges:

	to	
	to	
	to	
	to	
	to	
	to	

Individual IP addresses:

Internal Traffic to Monitor

List internal IP addresses for Network Agent to monitor for requests from other internal addresses.

Additional Settings

Specify how often Network Agent calculates bandwidth use, and whether and how often non-HTTP protocol traffic is logged.

Bandwidth calculation frequency (1-300):

_____ seconds

Log protocol traffic?

Yes No

Frequency (1-300):

_____ minutes

Worksheet 2: Associate Network Agent and Filtering Service

Network Agent sends information to Filtering Service to ensure that HTTP and non-HTTP requests are filtered and logged correctly. Multiple Network Agent instances can connect to each Filtering Service.

Use this worksheet to identify the Filtering Service instance that communicates with each Network Agent instance. You will use this information later to configure Network Agent.

Filtering Service IP address	Network Agent IP address
_____	(List each Network Agent instance that connects to this Filtering Service.)

Filtering Service IP address	Network Agent IP address
_____	(List each Network Agent instance that connects to this Filtering Service.)

Filtering Service IP address	Network Agent IP address
_____	(List each Network Agent instance that connects to this Filtering Service.)

Worksheet 3: Network Agent Local Settings (use one per instance)

Each Network Agent instance must be configured to connect to the correct Filtering Service and identify proxy and cache machines in the network segment it monitors. (NIC settings, covered in the next worksheet, determine which network segment the instance monitors.)

Local Settings for:

This Network Agent (IP address):

Connected to Filtering Service (IP address):

If Filtering Service is unavailable:

Permit all Internet requests

Block all Internet requests

List proxies and caches (by IP address) used by machines the agent monitors:

Providing this information ensures that requests are not logged twice (as originating both from the source machine and from the proxy/cache machine).

Advanced Network Agent Settings:

You can configure which ports Network Agent does or does not monitor for traffic.

Ports used for HTTP traffic:

Ignore traffic on the following ports:

When Websense software is installed in standalone mode, all ports are monitored for HTTP traffic. This cannot be changed.

If you have deployed Websense Content Gateway, this may be used to prevent double logging of HTTPS traffic.

Do not change the Debug Settings unless instructed to do so by Websense Technical Support.

Worksheet 4: NIC Settings (use one per network card)

NIC settings determine which network segment Network Agent monitors, which network card (in a multiple NIC machine) is used for monitoring and which is used for blocking, and what type of network traffic (HTTP, non-HTTP, or both) Network Agent monitors.

NIC settings for:

This network card (description):	IP address:
_____	_____
Use this NIC to monitor traffic?:	Use this NIC to block traffic?
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

Monitoring Settings

Which machines should this NIC be used to monitor?

All None Specific (list IP addresses or ranges below)

IP address ranges cannot overlap, and individual IP addresses cannot fall within an already listed range.

_____	to _____
_____	to _____
_____	to _____
_____	to _____
_____	_____
_____	_____
_____	_____

List machines within the monitored ranges that should not be monitored:

_____	_____
_____	_____

Filtering Options

If Websense software is installed in standalone mode, Network Agent must be used to filter HTTP and non-HTTP requests, and related options appear disabled in TRITON - Web Security.

Should Network Agent log HTTP requests?	Filter HTTP requests not sent through the integration product?
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
The following protocol management options apply to standalone and integrated deployments.	
Filter non-HTTP requests?	Calculate bandwidth use by each protocol?
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No

Using TRITON - Web Security to configure Network Agent

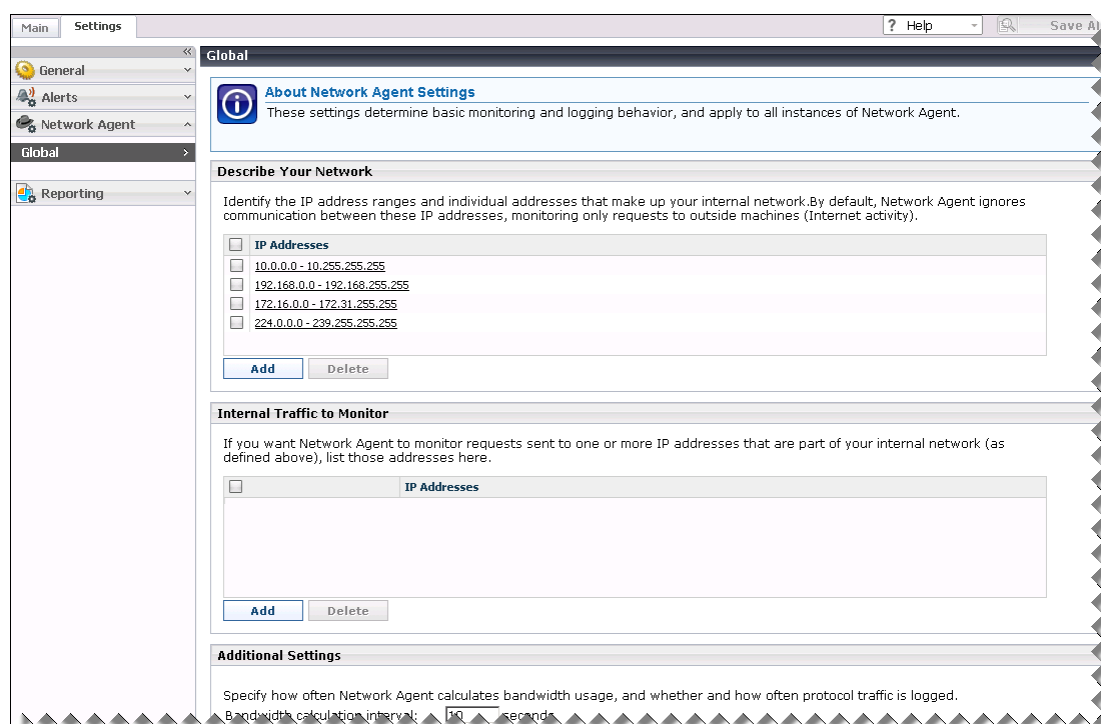
Use TRITON - Web Security to configure Network Agent to recognize machines in your internal network, communicate with Filtering Service, monitor traffic from specified machines, log appropriate data, and more.

To configure Network Agent settings in TRITON - Web Security, select the **Settings** tab of the left navigation pane, and then expand the **Network Agent** section.

To configure Global settings:

Refer to Planning Worksheet 1 for help in configuring Network Agent Global settings. All Network Agent instances in your network use these settings.

1. Select **Global**, under Network Agent, in the left navigation pane.



2. Use the **Internal Network Definition** list to identify all IP addresses in your network.



Important

This information is **not** used to determine which machines are monitored for filtering. Instead, it allows Network Agent to ignore internal network communications while monitoring Internet traffic.

An initial set of entries is provided by default. You can add additional entries, or edit or delete existing entries.

Be sure to include all IP addresses that are part of your network, whether or not you want Network Agent to monitor traffic to or from the machine. Later, you will configure whether Network Agent monitors traffic to specific internal IP addresses, and specify which IP addresses are monitored for outgoing Internet traffic.

- Click **Add** to add an IP address or IP address range to the list.
- Click an entry in the list to edit it.
- Mark the check box next to an entry, and then click **Delete** to remove it from the list.

IP address ranges in the list cannot overlap, and you cannot enter an individual IP address that falls within a range already in the list.

3. Use the **Internal Traffic to Monitor** list to specify internal IP addresses (included in the Internal Network Definition list) for which you **do** want Network Agent to monitor connections from other internal IP addresses. You might include internal Web servers, for example, to help track access to internal resources.

Any requests sent from within the network to the specified internal machines is monitored by Network Agent. This traffic can be filtered and will appear in reports.

By default, the list is blank.

4. Use the **Additional Settings** options allow you to determine how often Network Agent calculates bandwidth usage, and whether and how often protocol traffic is logged:

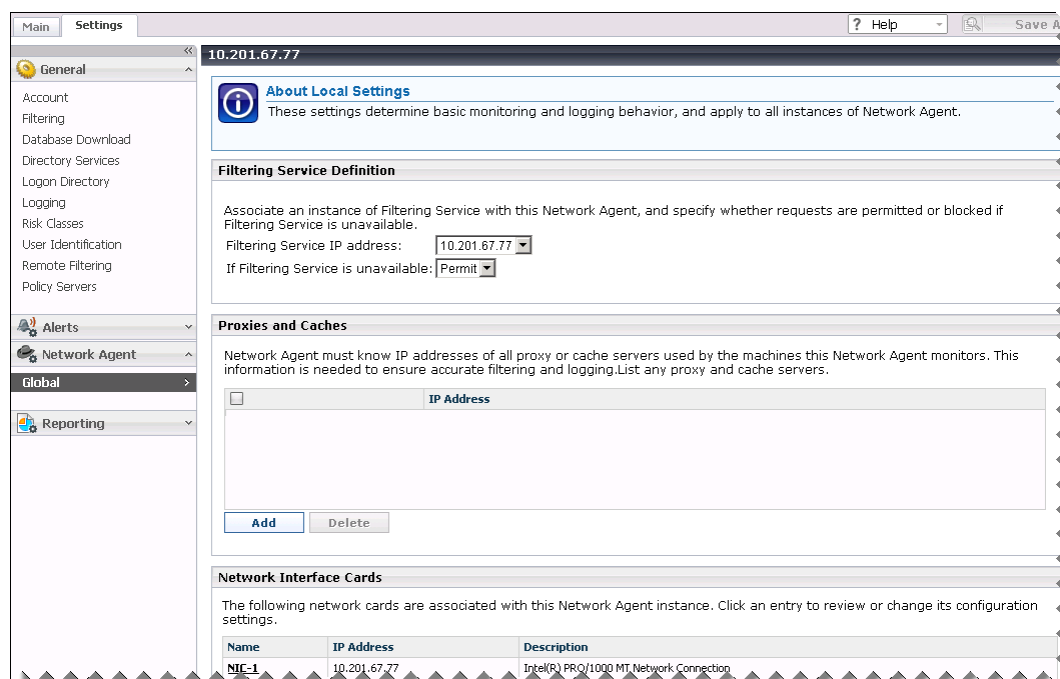
Field	What to do
Bandwidth calculation interval	Enter a number between 1 and 300 to specify how frequently, in seconds, Network Agent should calculate bandwidth usage. An entry of 300, for example, indicates that Network Agent will calculate bandwidth every 5 minutes. The default is 10 seconds.
Log protocol traffic periodically	Mark this option to log protocol traffic for use in reports, and to enable the Logging interval field.
Logging interval	Enter a number between 1 and 300 to specify how frequently, in minutes, Network Agent logs information about protocol traffic. An entry of 60, for example, indicates that Network Agent will write to the log file every hour. The default is 1 minute.

5. When you are finished making changes, click **OK** to cache the changes. Changes are not implemented until you click **Save All**.

To configure local settings:

Refer to Planning Worksheets 2 and 3 for help in configuring local settings. Only the selected Network Agent instance uses these settings.

1. Under Settings > Network Agent, highlight or click Global, and then select the IP address of the Network Agent instance that you want to configure. The IP address of the selected instance appears in the title bar at the top of the content pane.



2. Select the **Filtering Service IP address** that identifies the Filtering Service instance with which this Network Agent will communicate (Planning Worksheet 2). If Network Agent and Filtering Service are installed on the same machine, the local IP address is selected by default.
3. Indicate whether Network Agent should block or permit all requests **If Filtering Service is not available**.
4. Use the **Proxies and Caches** list to specify an proxy or cache machines that monitored machines use to access the Internet. This keeps Network Agent from identifying requests from both the client machine and the proxy or cache machine, which could result in duplicate log records or incorrect filtering.
5. Under the Network Interface Cards list, expand **Advanced Network Agent Settings**:
 - a. If Websense software is installed in integrated mode, indicate the **Ports used for HTTP traffic** in your network.
If you have installed Websense software in standalone mode, all ports are monitored and the field is disabled.
 - b. If you want Network Agent to ignore traffic on specific ports, mark **Configure this Network Agent instance to ignore traffic on the following ports**, and then enter one or more ports.
If you have deployed Websense Content Gateway, this may be used to prevent double logging of HTTPS traffic.

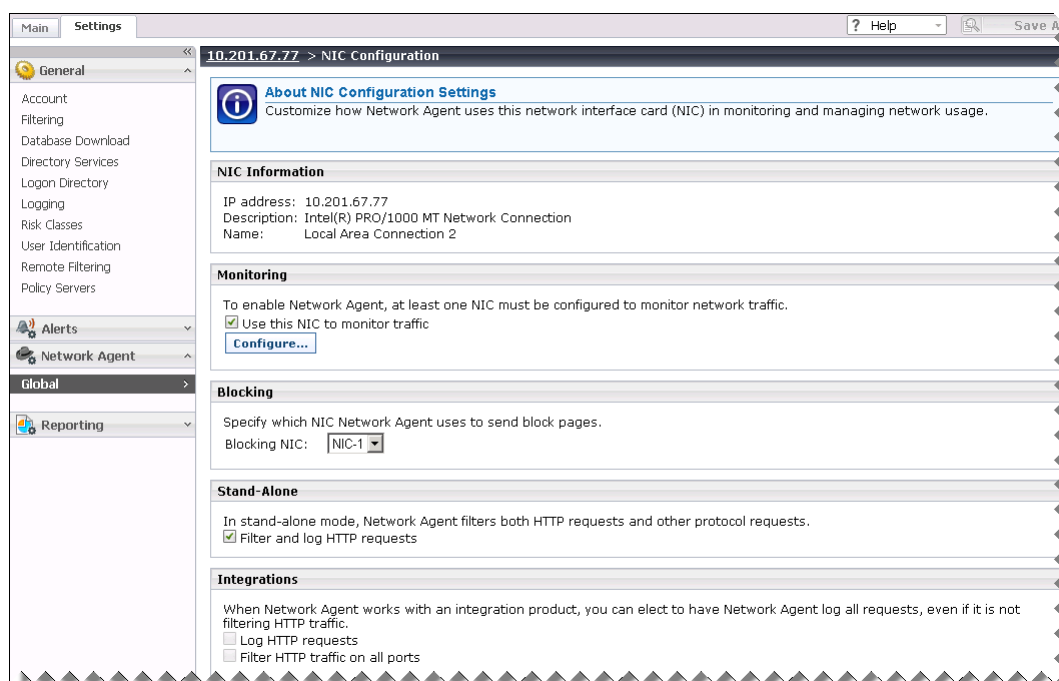
Do not make changes to the **Debug Settings** options unless directed to do so by Websense Technical Support.

- Click **OK** to cache your changes. Changes are not saved until you click **Save All**.

To configure NIC settings:

Refer to Planning Worksheet 4 for help in configuring NIC settings. These settings determine which NIC is used for monitoring and which is used for blocking and communication with other Websense components. They also determine which machines this Network Agent instance monitors, and how the agent responds to requests for non-HTTP protocols.

- Click an entry in the **Network Interface Cards** list on the Local Settings page for the Network Agent instance that you are configuring.



The **NIC Information** list provides a description of the selected network card.

- Indicate whether or not to **Use this NIC to monitor traffic**.

If the Network Agent machine has multiple NICs, you can configure more than one NIC to monitor traffic.



Note

If Network Agent runs on a Linux machine with multiple NICs, the operating system determines in real-time which NIC to use for monitoring. Network Agent may sometimes use a NIC other than the one specified here.

- If this NIC will be used for monitoring, click **Configure**, and continue with step 3.
- If this NIC will not be used for monitoring, go to step 4.

3. Use the **Local Settings > NIC Configuration > Monitor List** page to configure monitoring behavior:
 - Use the **Monitor List** to identify which IP addresses (All, None, or Specific) this Network Agent instance monitors.
If you select **Specific**, add the IP address ranges and individual IP addresses that this Network Agent should monitor.
 - Under **Monitor List Exceptions**, add any IP addresses within the monitored ranges that Network Agent should not monitor.
 - When you are finished making changes, click **OK** to return to the NIC Configuration page.
4. Indicate which NIC Network Agent should use as a **Blocking NIC**. This NIC is also used for communication with other Websense software components, and must have an IP address.
5. If you are using Websense software in standalone mode, the Stand-Alone and Integrations options are disabled. Continue with step 6.
If you have integrated Websense software with a firewall, proxy, network appliance, or other product:
 - Select **Log HTTP requests** to improve accuracy in Websense reports.
 - Select **Filter all requests not sent over HTTP ports** to use Network Agent to filter only those HTTP requests not sent through the integration product.
6. Under Protocol Management, indicate whether Network Agent should be used to **Filter non-HTTP protocol requests** and **Measure bandwidth by protocol**.
7. Click **OK** to cache your changes, and then click **Save All** to implement them.

Verifying that Network Agent is working

After configuring Network Agent in TRITON - Web Security, use a network protocol analyzer to ensure that the monitoring NIC is able to see traffic from all of the machines that it is configured to monitor.

If you do not have a preferred network analysis tool, Websense software includes a simple Network Traffic Detector utility that you can use to ensure that Network Agent can see traffic from all monitored machines.

To use the Network Traffic Detector:

1. Launch the utility:
 - (Windows) Go to **Start > Programs > Websense > Network Traffic Detector**.
 - (Linux) Navigate to the Websense software installation directory (by default, `/opt/Websense`) and enter the following command:

```
./NetworkTrafficDetector.sh
```

2. Select a network card from the **Network Adapter** drop-down list.
3. Check the addresses that appear in the **Monitored Network Ranges** list to verify that all appropriate subnetworks are listed.
4. Use the **Add Subnetwork** and **Remove Subnetwork** buttons to change which parts of the network are tested.
5. Click **Start Monitoring**.

The Network Traffic Detector detects computers in the network by monitoring the information they send across the network. The **Number of Computers Detected** list shows a running count of IP addresses from which traffic has been detected.

6. To see specific information about the IP addresses detected by the tool, select a subnetwork in the Monitored Network Ranges list, and then click **View Detected Computers**.

If a specific IP address is not listed, verify that it is generating network traffic. To do this, go to the machine, launch a browser, and navigate to a Web site. Then return to the Network Traffic Detector and see if the computer appears in the **Detected Computers** dialog box.

7. When you have finished testing network traffic visibility, click **Stop Monitoring**.

If some computers are not visible:

- ◆ Review the network configuration and NIC placement requirements.
- ◆ Review the more detailed network configuration information in the *Installation Guide* for your Websense software.
- ◆ Verify that you have properly configured the monitoring NIC.

Top Troubleshooting Tips

Network Agent cannot communicate with Filtering Service

When Filtering Service has been uninstalled and reinstalled, the Network Agent does not automatically update the internal identifier (UID) for Filtering Service.

To re-establish connection to Filtering Service:

1. Open TRITON - Web Security and select the **Settings** tab of the left navigation pane.
2. Expand the **Network Agent** section, and then select a Network Agent IP address.
3. Select the Filtering Service IP address from the drop-down list.
4. Click **OK** to cache your changes, and then click **Save All**.

Network Agent fails to start with stealth mode NIC

On Linux systems that include a network card configured in stealth mode, there are 2 potential issues that may prevent Network Agent from starting:

- ◆ A stealth mode NIC may inadvertently be selected for communication (blocking) in the Websense software installer. Use TRITON - Web Security to select a different blocking NIC.
- ◆ If Network Agent is bound to a NIC configured for stealth mode, and then the NIC IP address is removed from the Linux configuration file (`/etc/sysconfig/network-scripts/ifcfg-<adapter name>`), Network Agent will not start.

To reconnect Network Agent to the NIC, restore the IP address in the configuration file.

Spanning or mirroring is configured incorrectly

If Network Agent connect to a switch, it must be able to see all traffic for the network or segment that it monitors. This means that it must connect to the span, mirror, or monitor port (though the term varies by manufacturer, the function is the same).

The span port mirrors all the traffic that leaves the network segment, so traffic is simultaneously sent to the monitoring port to which Network Agent is connected.

Monitor (span, mirror) only the port going to the firewall or router port, not the entire network.

Router or firewall traffic is being monitored in the wrong direction

Monitor (span, mirror) the traffic going to the firewall or router. On Cisco switches, this means you need to specify **Tx**. On HP and 3Com switches, you need to specify **Egress**.

To log bytes sent and received, set both **Tx** and **Rx** (Cisco) or both **Egress** and **Ingress** (HP, 3Com).

Mono-directional spanning (mirroring, monitoring) is used with a single NIC

Websense strongly recommends using a switch that supports bidirectional spanning. If such a switch is used, Network Agent can function successfully with a single network card performing both monitoring and blocking.

If the switch does not support bidirectional spanning, Network Agent must use separate NICs for monitoring and blocking.

Teamed NICs (TNICs)

TNICs share the load under one common identity, with four adapters load-balancing under a single IP address. This is also known as link aggregation or trunking.

Websense recommends against using teamed NICs for Network Agent.

An anti-spoofing mechanism has been used in the switch

Either disable the anti-spoofing mechanism or contact Websense Technical Support for additional options.

Are other tools available for verifying that the Network Agent machine sees the traffic?

Yes. Wireshark is a free, popular, open source network protocol analyzer, available for Windows and Linux systems from www.wireshark.org.

Contact Websense Technical Support or Sales Engineering for information about other network tools that can help verify Network Agent behavior.

Can a network tap be used with Network Agent?

Yes. A tap can be used with the Network Agent machine. Network Agent must be able to see the traffic in both directions.