



HP Network Capture

Software Version: 7.11

User Guide

Document Release Date: June 2015
Software Release Date: June 2015

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2002 - 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://softwaresupport.hp.com>.

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to

<https://softwaresupport.hp.com> and click **Register**.

Support

Visit the HP Software Support Online web site at: <https://softwaresupport.hp.com>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to: <https://softwaresupport.hp.com> and click **Register**.

To find more information about access levels, go to: <https://softwaresupport.hp.com/web/softwaresupport/access-levels>.

HP Software Solutions & Integrations and Best Practices

Visit **HP Software Solutions Now** at <https://h20230.www2.hp.com/sc/solutions/index.jsp> to explore how the products in the HP Software catalog work together, exchange information, and solve business needs.

Visit the **Cross Portfolio Best Practices Library** at <https://hpln.hp.com/group/best-practices-hpsw> to access a wide variety of best practice documents and materials.

Contents

HP Network Capture	6
Which Metric Should I Choose?	8
Tips to Improve Measurement Accuracy	10
Installation and Upgrade	11
Installing Network Capture	12
System Requirements and Resource Utilization	13
Secure Communication in Network Capture	14
Network Capture Server Installation	16
Network Capture Agent Installation	18
Installing the Network Capture Agent	18
Uninstalling the Network Capture Agent	19
Firewall Configuration	19
Reverting an Installation	21
Upgrade Compatibility	22
Log and Configuration Files	23
Login	24
Licensing Network Capture	24
Changing between Secure and Non-Secure Communication Post Installation	26
Enabling Secure Communications	27
Disabling Secure Communications	28
Using Network Capture	29
Moving Around	30
Creating Endpoints	30
Configuring a Monitor	32
Adding and Deleting Monitor Folders	32
Defining the Interval for Concurrent Bandwidth Monitors	33
Configuring Latency and Packet Loss	34
Configuring Bandwidth	36
Configuring Web Server Parameters	37
Start Monitoring	38
Viewing Data	38
Zoom In and Zoom Out	41
Searching for Data	43
Analyzing Data	44
Performance Statistics	44
Using Network Profiles	45
Exporting Data	46
Defining and Updating Users	47
Account Settings	48
Setting Schedules	49
FAQs and Troubleshooting	49

Obtaining Technical Support53

Send Us Feedback55

HP Network Capture

HP's Network Capture records actual network conditions, enabling the import and recreation of network environments into pre-production and testing labs. In addition, Network Profiles utilize data that includes real-world network conditions of mobile and broadband Internet users from major cities around the world. This data is used to accurately assess and analyze the performance of distributed applications using HP's applications.

When you record network conditions, your goal is probably to see how your applications will react with various network parameters. Perhaps you're consolidating your data server, and want to check how various applications will behave in production network conditions. Perhaps you're testing a new feature and want to ensure that each business process will perform well in production.

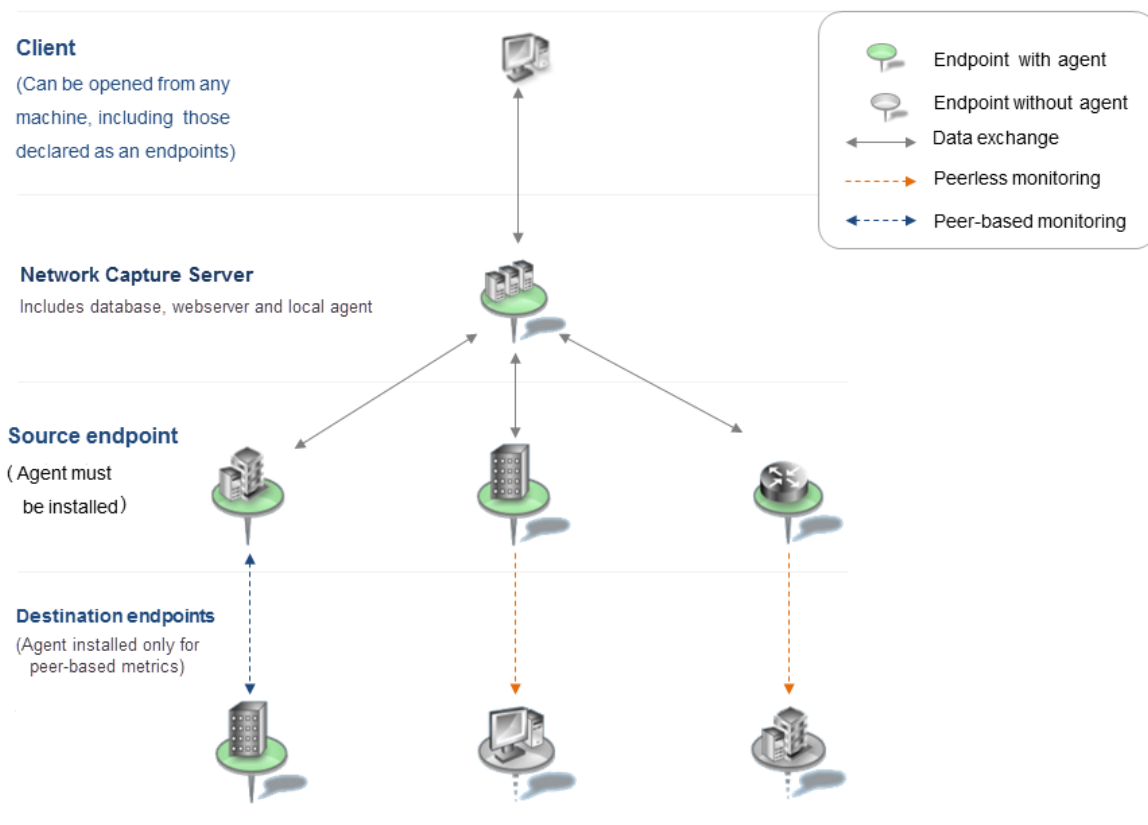
Use Network Capture to record and identify application performance problems occurring at a remote location, by measuring network conditions such as latency, packet loss, bandwidth availability across any given network topology. Network Capture can measure production links around the globe for a duration of up to one month.

After completing a recording, you can export the data for reporting purposes, or emulate these conditions in HP's network emulation products. You can export a complete run, or a specific period within the run, for example, the period with the highest latency values.

With Network Capture's web-based interface, you can record up to 25 simultaneous links (license dependent), and view the actual locations on the dynamic map. You can search easily for specific monitors, users and results. Schedule the monitors to start and stop at different times and for various durations, including recurrence if required.

Network Capture provides powerful analysis options to select the lowest, mean and highest conditions from the recorded data. A variety of measurements and calculations provide detailed information that can be used to evaluate application response time under various conditions.

This diagram shows the relationship of the components in the Network Capture configuration.



Concurrent Measurements of more than one Metric

While latency, loss and jitter can be measured concurrently, bandwidth cannot be measured in parallel, because doing so impacts the accuracy of the measurements. Therefore, Network Capture optimizes the percentage distribution, or the system overall time allocation between measurements of bandwidth and latency, packet loss and jitter.

For the best system configuration conditions, at least 75% of the measurement's duration is devoted to latency, loss and jitter measurements and up to $\pm 25\%$ to bandwidth. When measuring with the worst network configuration conditions, at least $\pm 75\%$ of the duration is devoted to latency, loss and jitter. For further information, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).

The scheduling algorithm is optimized and automatically calibrated to support a star topology, where the center (root) of the topology is set as the source of all the monitors.

See also:

- ["Which Metric Should I Choose?" on the next page](#)
- ["Tips to Improve Measurement Accuracy" on page 10](#)

Which Metric Should I Choose?

The following table compares certain features of each metric that is used to measure network conditions.

Note: All metrics are less accurate when the Endpoint is running CPU-intensive processes. Load-generating tasks should not be run on an Endpoint machine. Network accelerators and proxy servers intercepting Network Capture traffic may hinder the accuracy of the results.

Network overhead is affected by the probing interval and other factors.

Metric	Requirements	Most Accurate When	Least Accurate When	Measurement Of	Network Overhead
ICMP Echo (Ping)	Target machine should be configured to respond to ICMP requests.	ICMP packets are handled with the same priority as UDP and TCP packets	When ICMP packets have low priority	ICMP echo request and echo response	Minimal
UDP	Network Capture agent installed on both Endpoints. UDP port must be allowed in the firewall.	Usually accurate; best choice for measuring VOIP behavior	When UDP packets have low priority	UDP transmission time	Minimal
TCP (peer-less)	Available only for peerless targets. Requires a TCP server listening to the selected port and that no TCP proxies are present on the path.	Usually accurate	Target machine runs Windows XP	TCP connection setup (TCP handshake)	Minimal
TCP (peer-based)	Used to measure TCP Response Time. Network Capture agent installed on both Endpoints. TCP port must be allowed in the firewall.	Windows 7 is the operating system	Jitter is very high (varies up to 3x from one packet to another); also when the Target machine is running MS Windows XP	TCP response time per data packet	Minimal

Metric	Requirements	Most Accurate When	Least Accurate When	Measurement Of	Network Overhead
HTTP Response Time	Requires HTTP server (e.g. web server) on target Endpoint.	HTTP Request/Response Roundtrip Time	Minor variance due to Server HTTP processing time; note that proxies and caches influence results	HTTP Response Time	Depends on the HTTP request chosen, usually minimal.
Unidirectional Estimate	Target Endpoint should respond to either NTP ICMP echo, or ICMP timestamp requests. UDP port allowed on firewalls between source and target.	Inbound link is available	Inbound link is congested and ICMP is chosen as the "pinging protocol"	Outbound available bandwidth	Substantial
Bidirectional estimate	Network Capture agent installed on both Endpoints. UDP port allowed on firewalls between source and target endpoints.	Not dependent upon other factors to increase accuracy	Traffic is bursty and has high throughput	Outbound and inbound available bandwidth	Moderate
Robust Bidirectional Sample	Network Capture agent installed on both Endpoints. TCP port allowed on the firewall.	Accurate when bandwidth is low (<50Mb) and roundtrip time is low (<120ms)	Traffic is bursty and has high throughput	Outbound and inbound available bandwidth	Substantial

Note:

TCP Packet Loss: When an acknowledgment of the TCP header is not received, retries are attempted to establish the connection, usually three to four times, depending upon the operating system.

A packet is defined as lost using the TCP protocol:

- If Network Capture detects that a retransmission has occurred.

HTTP Packet Loss:

Prior to measuring with the HTTP protocol, a connection between both Endpoints needs to be defined. Once established, a header request is sent.

Packets are considered to be lost in the following cases:

- No connection is established between monitor endpoints.
- Server response is not as defined by the user.
- The response time takes longer than the acceptable value defined by the user using the Timeout parameter.

Tips to Improve Measurement Accuracy

- When measuring Unidirectional Bandwidth to a specific Target Endpoint, avoid measuring additional bandwidth metrics to the same Target.
- To provide more accurate bandwidth measurements, avoid measuring both latency and bandwidth simultaneously especially if the Available Bandwidth is low. The reason for this recommendation is that peerless metrics (ICMP, TCP and HTTP) may take measurements simultaneously with the bandwidth probing, and may utilize some of the available bandwidth.
- For additional information about bandwidth measurements, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).

Installation and Upgrade

HP's Network Capture records actual network conditions and enables the import and recreation of network environments into pre-production and testing labs. This data is used to accurately assess and analyze the performance of distributed applications using the HP Network Virtualization network appliance and desktop applications.

This section describes how to install, upgrade, and license the product, including:

- [Installing Network Capture](#) 12
- [Reverting an Installation](#) 21
- [Upgrade Compatibility](#) 22
- [Log and Configuration Files](#) 23
- [Login](#) 24
- [Licensing Network Capture](#) 24
- [Changing between Secure and Non-Secure Communication Post Installation](#) 26

Installing Network Capture

The Network Capture Server installer installs the Server, Web Server and Agent components. To conduct peer-based probing, the Network Capture Agent must also be installed on the Target machine. To install Network Capture components, you must have Windows™ Local Administrator permissions.

Note: Certain installation errors may be displayed in the MS Windows Installer logs and not in the Network Capture logs. For more information, see ["Log and Configuration Files"](#) on page 23.

- [System Requirements and Resource Utilization](#) 13
- [Secure Communication in Network Capture](#) 14
- [Network Capture Server Installation](#) 16
- [Network Capture Agent Installation](#) 18
- [Firewall Configuration](#) 19

System Requirements and Resource Utilization

System Requirements can vary according to the usage on the specific Server and Agent machine.

Three levels of usage are defined for the Agent:

- **Light:** Agent, either a Source or a Target, is involved in up to 5 concurrently running monitors
- **Medium:** Agent, either a Source or a Target, is involved in up to 10 concurrently running monitors
- **Heavy:** Agent, either a Source or a Target, is involved in up to 25 concurrently running monitors

Note: Since an Agent is always installed on the Server machine as part of the Server installation, consider the Agent requirements when determining the system requirements.

Network Capture Server System Requirements

The minimum requirements for Network Capture Server (including the Web Server component) are:

Processor	1.3 GHz (32 bit or 64 bit)
Memory	2 GB RAM
Free Hard Disk Space	100 GB of free disk space (includes space for recordings)
Network Adapter	Network Interface Card, WIFI, Cellular Cards or Virtual NICs
Browser	<ul style="list-style-type: none">• Internet Explorer 7.0 or higher• FireFox 4.0 or higher <p>Note: Supported screen resolution is 1280x800 and higher with a zoom level of 100%.</p>
Operating Systems (English versions only)	Microsoft Windows: <ul style="list-style-type: none">• Server 2003 SP2 (32/64bit)• Server 2003 R2 SP2 (32/64bit)• Server 2008 SP2 (32/64-bit)• Server 2008 R2 (64 bit)• Server 2008 R2 Hyper-V (64-bit)• Windows 8.1 (32/64-bit)• Windows 2012 R2 (64-bit)
Remote Access	Microsoft RDP for supported operating systems
Virtualization	VMware ESXi 4.0 Windows 2008 HyperV (64 bit) VMware Workstation 6.0 and higher

Network Capture Agent System Requirements

The requirements for the Network Capture Agent are:

Processor	<ul style="list-style-type: none">• Light usage: 1.3 GHz (32 bit or 64 bit)• Medium usage: 2 GHz (32 or 64 bit)• Heavy: 3 GHz Dual-Core (32 or 64 bit)
Memory	<ul style="list-style-type: none">• Light usage: 1 GB RAM

	<ul style="list-style-type: none"> • Medium usage: 2 GB RAM • Heavy usage: 4 GB RAM
Free Hard Disk Space	1 GB of free disk space
Network Adapter	Ethernet or Network Interface Card, WIFI, Cellular Cards, Virtual NICs
Virtualization	<ul style="list-style-type: none"> • VMware ESXi 4.0 • Windows 2008 HyperV (64 bit) • VMware Workstation 6.0 or higher
Network Capture Agent (standalone) English versions only	Microsoft Windows: <ul style="list-style-type: none"> • Server 2008 SP2 (32/ 64 bit) • Server 2008 R2 (64 bit) • Windows 7 (32/64 bit) *
*Light and medium usage only	

Resource Utilization with Heavy Usage

	Agent CPU	Server CPU	Agent Memory
Windows Server 2008 32 Core 2 Duo E7500 3 GHz 4 GB RAM	30%	7%	1 GB
Windows 7 Enterprise Core 2 Duo E7500 3 GHz 4 GB RAM	30%	-	1 GB

Secure Communication in Network Capture

Encrypted communication is supported on Network Capture:

- from the Client (browser) to the Web Server component
- from the Web Server component to the Server
- from the Agent to the Server

Encrypted communication is not supported on Network Capture:

- from an Agent to any other Agent, including the local Agent installed on the Server machine.

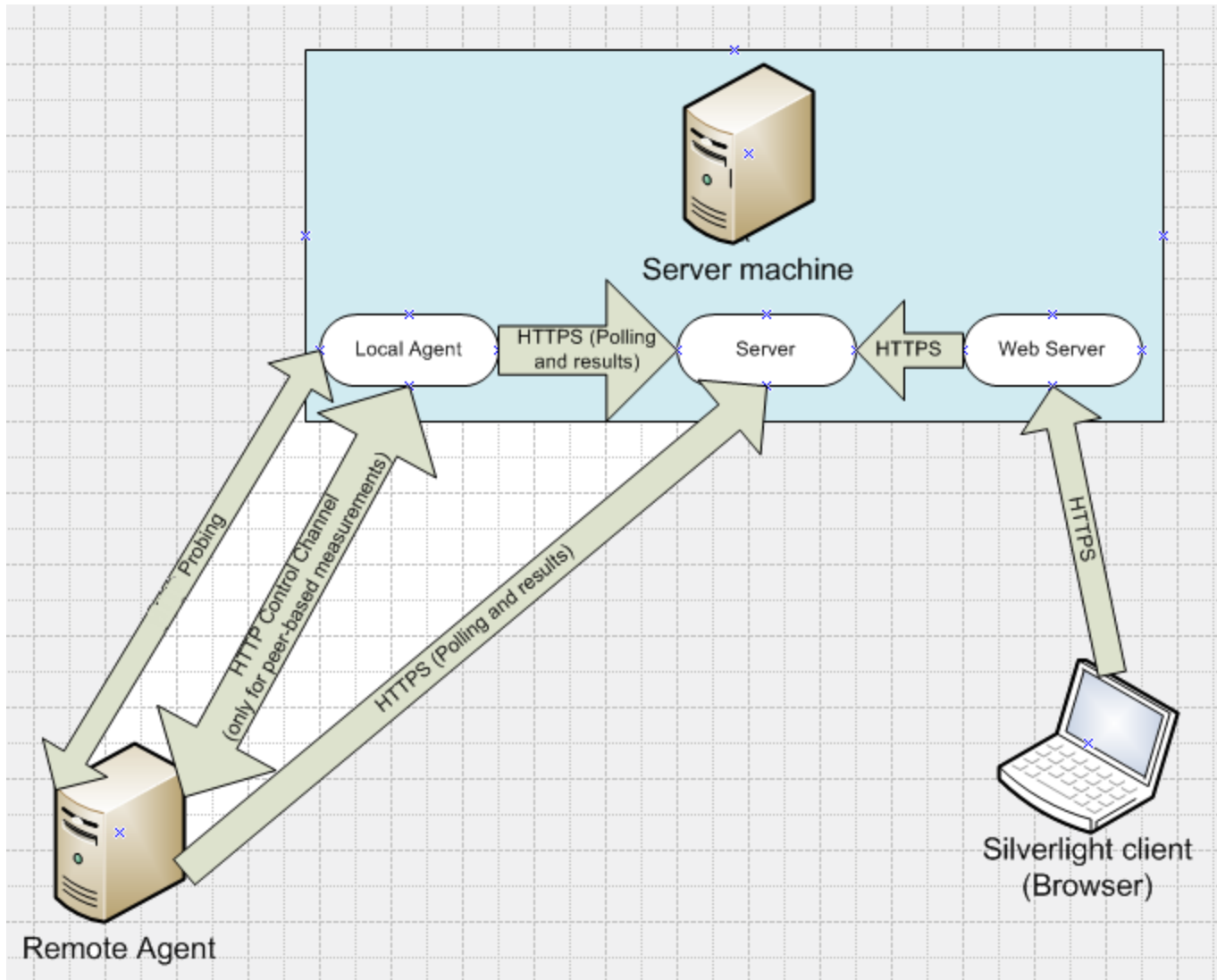
Enabling secure communication on the Network Capture Server creates a self-signed certificate on the Server machine.

Note: Neither Clients nor Agents have any means to validate the Server certificate used during the secure connection to the Server. Therefore:

- A security warning is displayed when a user logs on to the Network Capture UI. This warning is presented by the web browser, because the browser does not recognize the Server certificate.
- Agents log a warning message containing the certificate information and then silently accept it.

Consequently, although the established connection is using HTTPS, it is vulnerable to the man-in-the-middle attack.

The diagram shows the secure and non-secure channels, when secure communication is enabled on the Server and Agent.



Note: Firewall rules must be defined for each "arrow" in the diagram. For details, see ["Firewall Configuration" on page 19](#).

For example, in a configuration where:

- The Remote Network Capture Agent is listening on port 80
- The Network Capture Server is listening on port 443
- The Local Network Capture Agent is listening on port 90
- A Monitor is configured with the Local Agent as the Source and the Remote Agent as the Destination, and it measures latency using the TCP Protocol on port 997 (default port).

The following channels use the following ports:

- Source and Destination Agents use secured communication via port 443 to publish themselves and poll; the Source sends results back to the Server.
- The Destination Agent contacts the Source via the non-secured control channel using port 90 if the Destination Agent restarts or undergoes a crash recovery.
- Source Agent connects to the Destination Agent via the non-secured control channel on port 80.
- Source Agent probes for latency using non-secured communication on port 997.

Network Capture Server Installation

The Network Capture Server installer also installs the Network Capture Web Server and a local Network Capture Agent.

Prerequisites

- **IIS** (must be installed prior to installation of the Network Capture Server). For IIS 7.0, ensure that IIS 6.0 Metabase Compatibility is enabled.

Note: Windows 8.1 and Windows 2012 R2 require the following settings:

- Web Server > Common HTTP Features > Static Content
- Web Server > Performance > Static and Dynamic Content Compression
- .NET Framework 4.5 Features > WCF Services > HTTP and TCP Activation

- **MySQL** Standard Edition or higher, that includes:
 - MySQL Server, version 5.1 or higher

Note:

- MySQL Server versions 5.5.42 and 5.5.43 are not supported.
- The latest tested MySQL Server version is 5.6.24.

- MySQL Connector/NET, version 6.8.3 or higher

Note: MySQL configuration such as port settings, the 'root' user password and database connection type should not be altered after completing the Network Capture installation. If MySQL configuration changes are required, contact support at <https://softwaresupport.hp.com/>.

- **WinPcap** 4.1.2 or higher <https://www.winpcap.org/install/default>

Note: For Windows 8.1 and Windows 2012 R2, use WinPcap 4.1.3 or higher.

The following components will be installed as part of the installation if they are not already installed on your machine:

- Microsoft .NET Framework 4.0 Full
- Microsoft Visual C++ 2005 SP1 Redistributable Package
- Dynamic IIS Content Compression (highly recommended to enhance performance and reduce the load on network resources; may utilize additional machine resources)

To install the Network Capture Server:

1. As the Administrator, run **NC.Server.Setup.exe** and follow the instructions in the wizard. If required, a customized port can be selected during the installation process. During the installation, you can change the Network Capture Server and the local Agent port number. This may be required, if an another application (such as Skype) is using the default port.

Note: IP Addresses are not recommended if dynamic IP Addresses are used, as they can change when the machine is rebooted; use the hostname, URL or FQDN.

Note: If the Server machine is behind NAT, only the external address should be defined; do not use the internal host name or IP as the Server address. For the local Agent that is installed with the Server, see ["Network Capture Agent Installation" on the next page](#).

Configure the NAT device to enable port forwarding of the Network Capture Server port defined during installation (80\443 or user-defined).

2. Restart the host machine when the installation completes.
3. Ensure that the Network Capture Server and Agent Services are up and running.

Enabling Secure Communication (HTTPS) on the Server

Secure Communication (HTTPS) is enabled on the Network Capture Server as part of the installation wizard; make sure to select the **HTTPS** option.

Note: If you enable HTTPS on a non-default port, you must perform the following steps after installation.

In IIS Manager, in the Site Bindings dialog box, add an additional binding for the IIS Default Web Site using the following parameters:

- Type: https
- IP Address: All Unassigned
- Port: <your custom port>
- SSL certificate: <select the certificate created by Network Capture>

You can also enable secure communication at any time post-installation. For details, see ["Changing between Secure and Non-Secure Communication Post Installation" on page 26](#).

For additional details regarding secure communication components, see ["Secure Communication in Network Capture" on page 14](#).

Uninstalling Network Capture Components

Remove all three components separately:

- Network Capture Web Server
- Network Capture Agent
- Network Capture Server

To uninstall the Network Capture Server Components:

1. Login to the UI and stop all running monitors.
2. Back up recording files, by default in C:\Program Files\HP\NetworkCapture\CatcherFiles, to another place on your hard drive, or another location.
3. As the Administrator, in the Control Panel double-click the **Add/Remove programs** icon, select the HP Network Capture component, and click the **Change/Remove** button. Follow the on-screen instructions.

OR

Run **NC.<component>.Setup.exe** and select **Remove**; follow the instructions in the wizard.

During the uninstall, you will have the option to retain your database for future use. Ensure that you know your MySQL 'root' user password.

Restart the host machine when the uninstallation of all components completes.

Network Capture Agent Installation

For all types of measurements, the Network Capture Agent must be installed on the Source Endpoint. In addition, bidirectional bandwidth and other peer-based measurements require an Agent at the Target Endpoint. For details, see ["FAQs and Troubleshooting" on page 49](#).

Installing the Network Capture Agent

Prerequisites

- WinPcap 4.1.2 or higher

Note: For Windows 8.1 and Windows 2012 R2, use WinPcap 4.1.3 or higher.

The following components will be installed as part of the installation if they are not already installed on your machine:

- Microsoft .NET Framework 4.0 Full
- Microsoft Visual C++ 2005 SP1 Redistributable Package

To install the Network Capture Agent:

Login to the Network Capture user interface. From the Options menu select **Download Agent** and download the **NC.Agent.Setup.exe** file. This file is also available in the installation package.

Note: In the browser, make sure to allow Popup windows and the 'Download Files' option is enabled in the browser Security Settings.

As an administrator, run **NC.Agent.Setup.exe** file and follow the instructions in the wizard. During the installation, you can change the Network Capture Agent port number. This may be required, if another application (such as Skype) is using the default port. If Server is configured for secure communication, make sure to select the **Secure Connection (HTTPS)** option. Secure communication may be enabled at any time post-installation. For details, see ["Installing the Network Capture Agent" above](#).

For additional details regarding secure communication components, see ["Secure Communication in Network Capture" on page 14](#).

Note:

- IP Addresses are not recommended if dynamic IP Addresses are used, as they can change when the machine is rebooted; use the hostname, URL or FQDN.
- During installation of the Network Capture Agent, when specifying the Network Capture Server address and port, ensure that you enter the Network Capture Server details in the same format as you have entered it in the Network Capture Server installation.

For example, if you entered the host name during the Network Capture Server installation, use the same host name, not the IP address, during the Network Capture Agent installation.

- If the Network Capture Agent is behind NAT and is required to communicate with other Source or Target Agents that are not behind the same NAT, both the internal and external addresses must be provided. Configure the NAT device to enable port forwarding of the Network Capture Agent's port, defined during the installation (80 or user-defined), and in addition, enable port forwarding of any metrics' ports that are used by the Monitors. For details, see port specifications in ["Firewall Configuration" below](#).

Uninstalling the Network Capture Agent

To uninstall the Network Capture Agent:

1. Login to the UI and stop all running monitors.
2. Backup the file **NC.Agent.Host.exe.GUID** (this file may not be present in every configuration), by default located in \<AgentRootFolder>\Bin.
3. As the Administrator, in the Control Panel, double-click the **Add/Remove Programs icon**, select **HP Network Capture Agent**, and click the **Change/Remove button**. Follow the on-screen instructions.

Or

Run **NC.Agent.Setup.exe** and select **Remove**; follow the instructions in the wizard.

4. When reinstalling or upgrading, replace the file **NC.Agent.Host.exe.GUID** with the original file that was backed up.
5. Restart the host machine when the installation completes.
6. When reinstalling or upgrading:
 - a. Login to the Network Capture UI.
 - b. In the Endpoint page's toolbar, click **Scan All Endpoints Availability**. Two Endpoints with the same address are displayed; delete the Endpoint with the Status of Unreachable one (red icon).

Firewall Configuration

Ensure that ports required for Network Capture internal communications and monitoring are not blocked by any firewalls.

Network Capture Server

The following ports are generally involved:

- 443 for secure communication (may vary, depending upon the operating system)
- 80 for non-secure communication (may vary, depending upon the operating system)

Note: Since the Network Capture Server also includes a local Agent, make sure to configure the required Agent ports on the firewall as described in the following sections.

Network Capture Source Agents

For communication with the Network Capture Server:

- Outbound TCP port 80\443 (or another TCP port defined during Network Capture Server installation)

For communication with the Network Capture Target Agent:

- Outbound TCP port 80 (or another TCP port defined during Network Capture Target Agent installation)

For the following metrics:

- **TCP peerless:** outbound TCP 80 (or another user-configurable port)
- **TCP peer based:** outbound TCP 997 (or another user-configurable port)
- **UDP:** outbound UDP 997 (or another user-configurable port)
- **Unidirectional Estimate:**
 - Outbound UDP 53 (or another user-configurable probing port)
 - Outbound ICMP timestamp or ICMP Echo reply (according to selected Pinging Protocol)
- **Bidirectional Estimate:** outbound UDP 998 (or another user-configurable port)
- **Robust Bidirectional Sample:** outbound TCP 995 (or another user-configurable port)

Target Agent Based Endpoints

For the communication with Network Capture Source Agent:

- Inbound TCP port 80 (or another user-configurable TCP port) is open

For the following metrics:

- **ICMP metric:** ICMP Echo reply
- **TCP peerless:** inbound TCP 80 (or another user-configurable TCP port)
- **TCP peer based:** inbound TCP 997 (or another user-configurable TCP port)
- **UDP:** inbound UDP 997 (or another user-configurable port)
- **Unidirectional Estimate:**
 - Inbound UDP 53 (or another user-configurable probing port)
 - Inbound ICMP timestamp or ICMP Echo reply (according to selected Pinging Protocol)
- **Timestamp\ICMP Echo reply\Inbound UDP:** 123 according to the selected pinging protocol
- **Bidirectional Estimate:** inbound UDP 998 (or another user-configurable port)
- **Robust Bidirectional Sample:** inbound TCP 995 (or another user-configurable port)

Target Agent Less Endpoints

For the following metrics:

- **ICMP:** ICMP Echo reply.
- **TCP peerless:** (inbound TCP 80\customized)
- **Unidirectional Estimate:**
 - Inbound UDP 53 (or another user-configurable probing port)
 - Inbound ICMP timestamp or ICMP Echo reply (according to selected Pinging Protocol)

Reverting an Installation

When an install is aborted, the Network Capture installation provides two ways of reverting a PC to its previous state.

Installation rollback

- Rollback is an integrated feature. No user interaction is needed to trigger it.
- Rollback Actions are triggered when the setup encounters an abort (automatic failure or manual cancellation).
- Modifications performed by the setup program are reversed.
 - Installed files will be removed.
 - Shortcuts or registry entries added will also be removed.
 - New directories created by the install and log files will NOT be removed.

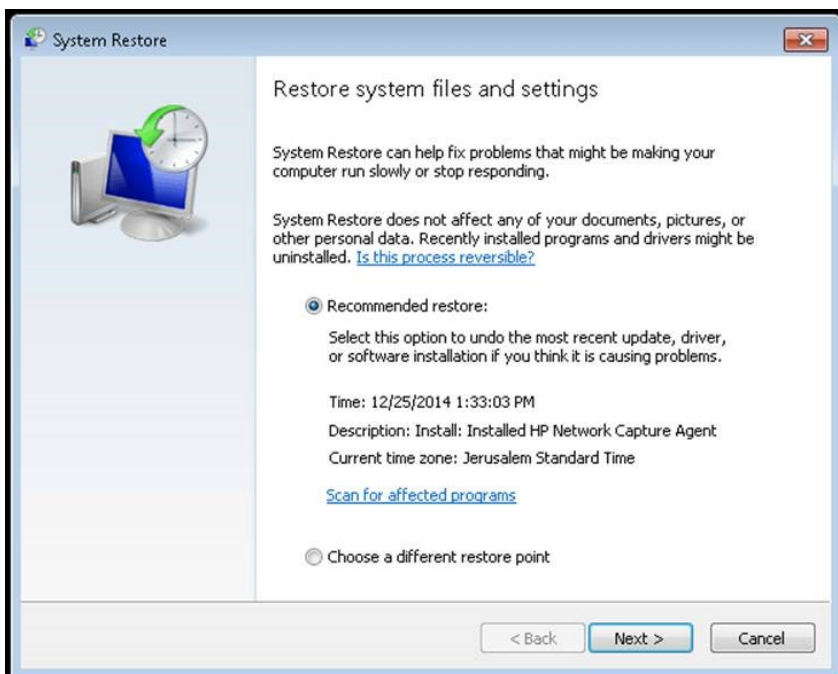
System Restore Point

If your PC has become corrupt during the software install, you may run System Restore, which is a native Windows feature. This feature automatically monitors and records key system changes to your PC. The Network Capture installation supports System Restore by setting multiple system restore points, including before starting the file transfer; you may then use the System Restore wizard to restore the system to its latest successful restore point. Or you may choose a different restore point manually.

Note: Not all Windows versions utilize System Restore.

- Supported versions include (but are not limited to): Windows XP, Windows 7, Windows8
- Unsupported versions include (but are not limited to): Windows Server 2008

To initiate system restore go to Start -> System Restore.



Upgrade Compatibility

Upgrading from Network Capture v6.0 or v7.0 to v7.11

Note: Previous versions of HP Network Capture were formerly Shunra NetworkCatcher v6.0 or v7.0.

To upgrade the Network Capture Server:

Note: When upgrading from a previous version of HP Network Capture to Network Capture v7.11 all Agents must be given the Name and Address in the exact format with the same values that were defined in v6.0 or v7.0.

1. Backup the MySQL 'NC' and 'Security' databases to ensure that you can access the original data if required. By default, the database is located in:
 - On Win 2003: C:\Documents and Settings\All Users\Application Data\MySQL\MySQL Server 5.1\Data
 - On Win 2008, Win 8.1, and Win 2012 R2: C:\ProgramData\MySQL\MySQL Server 5.1\data
2. Log in to Network Capture and stop all running monitors.
3. Uninstall all Network Capture components, refer to "[Uninstalling Network Capture Components](#)" on [page 17](#).
4. Install the Network Capture Server v7.11. For details, see "[Installing Network Capture](#)" on [page 12](#). Ensure that you install the Network Capture Server in the original installation path, to avoid difficulties with licensing.

Note: If the existing database is very large, the install may be a time-consuming process. To

avoid data corruption, do not interrupt the install procedure.

5. Restart the host computer.

Upgrading the Remote Agent

1. Backup the file **NC.Agent.Host.exe.GUID** (when upgrading from v7.0), by default located in **\<AgentRootFolder>\Bin**.
2. Uninstall the Network Capture Agent, refer to ["Uninstalling the Network Capture Agent" on page 19](#).
3. Login to the newly installed Network Capture user interface; from the Options menu select **Download Agent** and download the **NC.Agent.Setup.exe** file. This file is also available in the installation package.
4. Install the Network Capture Agent. For details, see ["Installing the Network Capture Agent" on page 18](#).
5. Replace the file **NC.Agent.Host.exe.GUID** with the original file that was backed up (when upgrading from v7.0).
6. Login to the Network Capture UI.
7. In the Endpoint page's toolbar, click **Scan All Endpoints Availability**. Two Endpoints with the same address are displayed; delete the Endpoint with the Status of 'Unreachable' (red icon).

Log and Configuration Files

By default, the logging level is 'Info' which just notes the problem without any explanation. You can adjust the level to 'Error' or other choices in the configuration file per component.

Configuration Files

The configuration files in which you can change the logging levels are found by default in:

- **Server:** **NC.Server.Host.exe.config** (in ...\\HP\\Network Capture\\Server\\Bin)
- **Agent:** **NC.Agent.Host.exe.config** (in ...\\HP\\Network Capture\\Agent\\Bin)
- **Web Server:** **web.config** (in ...\\HP\\Network Capture\\Web Server\\)

Log Files

The supported log levels are (from the most to the least detailed):

- **DEBUG:** highly detailed information, that logs each database operation; slows down the Server considerably
- **INFO:** provides information that is usually sufficient to troubleshoot ordinary issues
- **WARN:** warnings only
- **ERROR:** indicates the origin of a problem origin, usually does not contain sufficient information for troubleshooting

Log files are located by default in 64 bit systems in this folder:

- C:\Program Files (x86)\HP\Network Capture\Server (or Agent or Web Server)\Logs

Log files are located by default in 32 bit systems in this folder:

- C:\Program Files\HP\Network Capture\Server (or Agent or Web Server)\Logs
- Log files overwrite previous files once the allotted memory has been exceeded.

Logs in the MS Windows Installer

Certain installation errors may be displayed in the MS Windows Installer logs and not in the Network Capture logs. These logs are usually only required when troubleshooting is necessary:

- The setup logs are located in the %Temp% folder
- Windows Installer logs are not generated by default. To view these logs in the %Temp% folder, this key should be added to the Registry prior to installation:
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer] "Logging"="voicewarmupx"

Login

Once the Network Capture Server is installed, in your browser navigate to: **http(s)://<Network Capture Server address>/network_capture**

Use **Administrator/Administrator** as the user name and password, then change the username and/or password to restrict access.

Note: Microsoft Silverlight will be installed when opening the Network Capture user interface the first time. The first login may take a few minutes until the content is transferred from the Web Server component.

Licensing Network Capture

The Network Capture **Trial License** provides:

- Up to 10 concurrently running monitors
- Up to 100 endpoints
- 30 days usage; each run can record for up to 7 days

The Network Capture **Standard License** provides:

- Up to 25 concurrently running monitors
- Up to 100 endpoints
- Analysis
- Scheduling
- Export
- Can be used indefinitely; each run can record for up to 31 days

Requesting and Installing a License Key

After the trial license expires, you will have to obtain a license by sending your Host ID to HP, where it is used to generate the License Key. The License Key is sent back to you by email within 1 business day, and you enter it in the Network Capture License Manager.

To request a License Key:

1. Login to the Network Capture UI as a Network Capture Administrator.
2. From the toolbar, click **Options > License manager**.

The screenshot shows the 'HP Network Capture License Manager' window. It has a title bar with a close button (X). The main content area is titled 'Obtain License'. It contains two text input fields: 'Host ID' with the value '3DF6 4BB5 E438 99CD 3C' and a hint 'Press Ctrl+c to copy', and 'License Key' with the placeholder 'Enter License Key here' and a hint 'Press Ctrl+v to paste'. Below these is an 'Activate' button. Further down, it displays 'License: Professional' and 'Expiration Date: 8/30/2015 12:00:00 AM'. A table lists features and their status:

Features	Status
Maximum Concurrent Measurements	25
Maximum Endpoints	100
Export to NTX	Enabled
Enable Analysis	Enabled
Monitor Scheduling	Enabled

At the bottom right is a 'Close' button.

3. Record the Host ID.
4. Access the HP Licensing site (<http://www.hp.com/software/licensing>) and do one of the following:
 - If you have a valid license Entitlement Order Number (EON), enter your EON to activate your license.
 - To obtain a new license, click Contact HP Licensing to locate a Regional Licensing Support Center.

Your license activation request will be routed to the HP licensing team for processing. The licensing team will contact you to request the Host ID of your Network Capture machine.

To install a License:

1. As a Network Capture Administrator, from the toolbar, click **Options > License manager**.
2. In the License Key text field, enter the License Key provided to you by HP; the Activate button becomes active.
3. Click **Activate**, then click **Close**.

Changing between Secure and Non-Secure Communication Post Installation

This section includes:

- [Enabling Secure Communications](#)27
- [Disabling Secure Communications](#)28

Enabling Secure Communications

To enable secure communication on the Network Capture Server:

1. In the Network Capture UI, stop all running monitors.

Note: "IIS 6 Metabase Compatibility", an IIS role service must be installed.

2. Open a command window (Start > Run > CMD).
3. Change directory to <Server root directory>\bin directory, and run:
`SimpleNCServerSecurity.exe -m=all -s -p=<customized port (default is 443)>`

Note:

- It is recommended to first run this command as a 'trial run' before executing the configuration as follows:
`SimpleNCServerSecurity.exe -m=all -s -p=<customized port/default is 443> -n`
Ensure that no errors are present in the output window.
- If you enable HTTPS on a non-default port, you must perform the following steps after installation.
In IIS Manager, in the Site Bindings dialog box, add an additional binding for the IIS Default Web Site using the following parameters :
Type: https
IP Address: All Unassigned
Port: <your custom port>
SSL certificate: <select the certificate created by Network Capture>

4. Restart the HP Network Capture Server service.
5. To change the local Agent mode, see the following section.

To enable secure communication on the Agent:

1. Login to the UI and stop all running monitors.
2. Uninstall the Network Capture Agent. For details, see "[Uninstalling the Network Capture Agent](#)" on [page 19](#).
3. Install the Agent according to "[Installing the Network Capture Agent](#)" on [page 18](#) and select the **Secure communication** checkbox.

Note: It is possible to enable secure communication on the Agent without reinstalling the Agent; however, it involves manual configuration of system files and may result in corrupted data. Therefore, before attempting this procedure, backup any Network Capture Agent files that will be modified. For instructions about how to conduct this procedure, contact support at <https://softwaresupport.hp.com/>.

4. Restart the Network Capture Agent Service.

Disabling Secure Communications

To disable secure communication on the Server:

1. In the Network Capture UI, stop all running monitors.
2. Open a command window (Start > Run > CMD).
3. Change directory to <Server root directory>\bin directory, and run:

```
SimpleNCServerSecurity.exe -m=all -p=<customized port/default is 80>
```

Note: It is recommended to first run this command as a 'trial run' before executing the configuration as follows:

```
SimpleNCServerSecurity.exe -m=all -p=<customized port/default is 80> -n
```

Ensure that no errors are present in the output window.

4. Restart the HP Network Capture service.
5. To change the local Agent mode, see the following section.

To disable secure Communication (HTTPS) on the Agent:

1. Login to the UI and stop all running monitors.
2. Uninstall the Network Capture Agent. For details, see ["Uninstalling the Network Capture Agent" on page 19](#).
3. Install the Agent according to ["Installing the Network Capture Agent" on page 18](#) and do not select the **Secure communication** checkbox.

Note: Secure communication on the Agent can be disabled without reinstalling the Agent; however, this involves manual configuration of system files and may result in corrupted data. Therefore, before attempting this procedure, backup any Network Capture Agent files that may be modified. For instructions about how to conduct this procedure, contact support at <https://softwaresupport.hp.com/>.

4. Restart the Network Capture Agent Service.

For additional details regarding secure communication components, ["Secure Communication in Network Capture" on page 14](#).

Using Network Capture

HP's Network Capture monitors network conditions by sending and receiving data packets between one or more destinations. In addition, create Network Profiles to provide network conditions for specific networks. For an overview, see ["HP Network Capture " on page 6](#).

Let's get started with HP's Network Capture and find out how to record, analyze and export network conditions, including:

- [Moving Around](#)30
- [Creating Endpoints](#)30
- [Configuring a Monitor](#)32
- [Start Monitoring](#)38
- [Viewing Data](#)38
- [Analyzing Data](#)44
- [Using Network Profiles](#)45
- [Exporting Data](#)46
- [Defining and Updating Users](#)47
- [Setting Schedules](#)49
- [FAQs and Troubleshooting](#)49
- [Obtaining Technical Support](#)53

Moving Around

It is recommend that the screen resolution be set to 1280 x 800 (or higher) with zoom level of 100%. The Network Capture interface can only be viewed in the 32-bit browsers.

Network Capture provides a number of ways to customize how you view and input information:

- To select items, click on them, for example, when viewing Results of a Monitor, click **ICMP** to view the ICMP results, or click again to hide the results.
- Choose to display monitors and results in either Tree or List view, with or without the Map.
- View the details about a particular Endpoint, Monitor, Profile or User, by selecting the Tree or Grid icon.

Drag And Drop

In the "Monitors" and "Profiles" view, you can add folders drag and drop folders and subfolders within the tree.

Map View

You can display or hide the map when you are configuring Monitors or Endpoints, by clicking the **map** icon.

Save

When you leave an item, such as a Monitor, your additions and updates are automatically saved. In addition, you can manually save any modifications by selecting the **Save** button.

Undo

To cancel any modifications, select the **Undo** button, which reverts the data to the previously saved data.

Refresh All

Use **Refresh All** to display the most updated data from the Network Capture Server in the user interface. The UI is updated automatically every 15 minutes.

Creating Endpoints

An Endpoint represents a network node at a given address. Within a monitor, an Endpoint is either the Source Endpoint (the location from which you are measuring) or the Target (the destination to which you are measuring). Endpoints can be defined as a Data Center, Web Server, Application Server, Network Element, etc. The Source Endpoint must have a Network Capture Agent installed; on the Target Endpoint it is only required for certain metrics.

Once an Agent is installed on a machine, it will appear in the UI as an Endpoint; therefore **it is recommended not to create an Endpoint before installing the Agent.**

To create an endpoint manually (not recommended):

1. As Administrator, from the Monitors page, select **Endpoints**.
2. Click the **New Endpoint** icon, then type:
 - Name: up to 100 alpha-numeric characters
 - Address: the machine's address; it can be a host name, FQDN, IP, or URL of up to 255 characters.

Note:

- If the Endpoint is behind NAT, provide the address of the NAT device behind which the Endpoint is located and configure the Internal Address using the Advanced Settings icon. It represents the Endpoint's machine address, it can be a Host name or FQDN of up to 255 characters.
- If, when initializing a Monitor, the Server does not recognize the Source Agent, this may be due to issues with DNS Resolution. Since the Server must be able to recognize the Source Agent, use one of the following:
 - Fully-Qualified Domain Name, such as "server1.company.com" (To verify this property, right-click the **My Computer** icon, select **Properties** and scroll to the **Full Computer Name**)
 - IP Addresses are not recommended if dynamic IP Addresses are used, as they can change when the machine is rebooted
- Type: select one of the categories such as **Data Center, Remote Office, etc.**; the location on the map displays the icon of the selected Type
- Description: provide relevant details that identify the endpoint (optional) up to 255 characters
- HP Agent Installed: select if the Network Capture Agent is to be installed at this location; mandatory for Source Endpoints

Note: If you define an Endpoint prior to installing it, during the installation of the Agent, make sure to enter the Agent address and name as you defined it when creating an Endpoint in the Network Capture UI.

To edit an Endpoint:



In the list of Endpoints, select an Endpoint, then edit the details. The modified data can be saved manually, or is saved automatically when you leave the modified Endpoint.



To delete an Endpoint:

Select the Endpoint you wish to delete and click the **Delete** icon.

Note: Endpoints cannot be deleted and Endpoint addresses cannot be edited when they are used in existing monitors.

Endpoint statuses

	Unresolved: the Endpoint was added in UI before it was installed on a host machine
	Reachable: the Agent can poll the Network Capture Server and obtain commands

	Unreachable: the Agent cannot poll and receive commands from the Server
	Agentless: An agent has not been installed and configured

The status of the Endpoint is updated approximately every 5 minutes; the green icon indicates that it is reachable and able to access the Network Capture Server.

Note: Although both peerless and peer-based Endpoints can be defined on the same machine, this may reduce the accuracy of concurrent measurements. For more information, see ["Tips to Improve Measurement Accuracy" on page 10](#).

Configuring a Monitor

You can run up to 25 monitors simultaneously (license dependent).

- [Adding and Deleting Monitor Folders](#)32
- [Defining the Interval for Concurrent Bandwidth Monitors](#)33
- [Configuring Latency and Packet Loss](#)34
- [Configuring Bandwidth](#)36
- [Configuring Web Server Parameters](#)37

Adding and Deleting Monitor Folders

The Tree view contains the "Monitors" root folder. You can add folders and subfolders to this or any other folder, and also drag and drop folders within the tree. Folder names can be up to 255 characters.

To add a folder:

Click the **New Folder** icon and provide the relevant details.

To add subfolders:

Select the parent folder and click the **New Folder** icon and provide the relevant details.

To delete a folder:

As long as the folder or its subfolders do not have any active runs, select the folder and select the **Delete** icon in the toolbar or the keyboard **Delete** button.

To configure a monitor:

1. In the Monitors view, click the **New Monitor** icon.
2. Define the following:
 - **Name:** Type a name, up to 100 alphanumeric characters.
 - **Source:** Select an endpoint (only those endpoints that have an Agent installed are visible).
 - **Target:** Select an endpoint from the list.
 - **Duration:** Scroll or use the arrows to set the time period for the recording.

- For Latency and Bandwidth settings, select the checkbox beside the required metric. To adjust the settings, click the **Settings** button beside the metric. For more information, see ["Configuring Latency and Packet Loss" on the next page](#) and ["Configuring Bandwidth" on page 36](#).
 - **Description:** optional (up to 255 characters).
3. Click **Save** (or will be saved automatically when you leave Monitor). The parameters are validated during the 'Save' operation.
 4. To begin measuring, click the **Run Monitor** icon.

Note: If the following metrics are measuring to the same Target Agent, even if they are not in the same monitor, they should not be configured to use the same port:

Robust Bidirectional Sample Bandwidth and

- TCP (peer-based)
- TCP (peerless)
- HTTP

TCP (peer-based) and

- TCP (peerless)
- HTTP

To delete a monitor:

Click the **Delete Monitor** icon in the toolbar when the Monitor is not running.

To delete a run:

Click the **Delete Run** (trash can) icon in the Results view.

Defining the Interval for Concurrent Bandwidth Monitors

Peerless Bandwidth measurements block the Source Agent, and peer-based bandwidth metrics block both the Source and Target Agents from conducting other measurements while they probe.

This causes a delay in the execution of any other monitor the Agent has queued. To avoid congestion, the Agent redefines the Bandwidth Interval setting of its active monitors, keeping a ratio of 75% latency and packet loss to 25% bandwidth.

This ratio determines the calculation of the 'Time Window' which correlates to the bandwidth interval. The Time Window is determined by the types and number of bandwidth metrics to and from a specific Agent. The probing time of Unidirectional Bandwidth takes about 20 seconds. Therefore, if the same Agent is a Source for three Unidirectional Bandwidth Monitors that are defined to measure every 20 seconds, for any given minute no other measurements will occur. To prevent this situation, the actual Bandwidth Interval for each Source Agent is defined as:

Interval = No x TW

Each bandwidth metric uses a different coefficient (C) to calculate the Time Window (TW).

Where:

No=Number of outgoing bandwidth measurements from the specific Agent

$TW \text{ (Time Window)} = C \times (N_i + 1)$

C=80 for Unidirectional Bandwidth

C=20 for Bidirectional Bandwidth

C=120 for Robust Bidirectional

N_i=number of incoming bandwidth measurements to the specific Agent

For the example above with three Unidirectional Bandwidth monitors, the Time Window will equal 80 seconds (20 seconds for bandwidth probing and 60 seconds for latency and packet loss measurements). Each bandwidth monitor will have an Interval of 240 seconds.

Note: The Time Window is calculated per Agent, and the maximal value determines the Time Window for all running Monitors.

To reduce the actual probing interval (time between probing samples) the following are recommended:

- Use the default bandwidth metric (Bidirectional Bandwidth).
- Avoid running multiple monitors to and from the same Agent. Instead, either spread the Monitors between more Agents, or have the Monitors run one after the other.

Note: Installing several agents in the same location could create conflicts if they use the same physical link.

Configuring Latency and Packet Loss

To measure the latency and packet loss, select one of the following probing metrics:

- ["TCP \(Peer-based\)" below](#)
- ["TCP \(Peerless\)" on the next page](#)
- ["UDP" on the next page](#)
- ["ICMP" on the next page](#)

TCP (Peer-based)

The Source Endpoint sends packets via a TCP connection to the Peer, and measures the TCP response time. Less accurate results are obtained when high jitter is present.

- **Interval:** Select a value or use the default of 5 seconds.
- **Packet Size:** The packet size to be used when probing (in bytes).
- **Peer Port:** Type the number of an available port on which no server is listening, or use **Auto Select** to scan a predefined list of ports and to locate an available port.

Note: Due to an issue in MS Windows XP's implementation of the TCP/IP stack, TCP Available Bandwidth may measure inaccurate packet loss rates. If possible, avoid Monitors that use TCP when the endpoint's operating system is Windows XP. If only one endpoint machine runs XP, it is preferable that this endpoint be the Target.

TCP (Peerless)

Measures the time it takes to establish a new TCP session (sending a SYN packet and receiving a SYN ACK packet). For network measurement, using agent-less TCP, a TCP/HTTP server is required on the Target Endpoint.

Note: If a network accelerator or a proxy service is in the network path, the network measurements may not be accurate, as the accelerator or proxy may respond to the request instead of the required server.

- **Interval:** Select a value or use the default of 3 seconds
- **Peer Port:** Type the port number for the port that connects to the Target server.
- **Include DNS Resolution:** Select to include the domain name IP address resolution as part of the measurement.

Note: Due to an issue in MS Windows XP's implementation of the TCP/IP stack, TCP may measure inaccurate packet loss rates. If possible, avoid Monitors that measure using TCP when the endpoint's operating system is Windows XP. If only one endpoint machine runs XP, is preferable that this endpoint be the Target.

UDP

This protocol measures the Echo response received when packets are sent over UDP. UDP uses specified port numbers and checksums to check if the packets have arrived correctly, but does not guarantee reassembly of packets in the correct order.

- **Interval:** Set a value or use the default of 3 seconds.
- **Packet Size:** Select a value in bytes by defining the size of packets sent by the Source Endpoint to be used as probes.
- **Timeout:** Defines the period after which the sent packet is considered lost if not received by the recipient host, or use the default.
- **Peer port:** Only ports that are open on firewalls between the source and target machine can provide accurate results; if a port is closed the measurement will display complete packet loss. Choose **Auto Select** for Network Capture to scan a list of predefined list of ports to locate a port that's available.
- **Specific port:** Type or select a port number. Autoscans selects ports based on the defaults set in the **NC.Protocols.config** file located in **<Network Capture Agent home directory>\Bin\AgentImplementation**. You can modify this file to define alternate ports to be scanned.

ICMP

The Source Endpoint sends an ICMP Echo Request (ping) to the Target Endpoint; if the target is available, the target host responds by sending an ICMP reply back to the Source Endpoint. The Latency measurement is the round trip time.

Note: Ensure that the operating system on the Target Endpoint is configured properly to receive and process ICMP Echo Request and Reply messages, so that the ICMP Echo Request/Reply messages can travel along the path between the Source and the Target machines.

Interval: Select a value greater than 100 ms, or use the default of 1 second. When selecting a values less than 1 second use a short duration for the monitor, otherwise many samples are taken and the database may fill to capacity. Bandwidth may be measured with multiple concurrent monitors. For more information, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).

Packet Size: Select a value in bytes; the value includes the IP and ICMP headers.

Timeout: Defines the period after which the sent packet is considered lost if a response is not received by the agent.

Configuring Bandwidth

Bandwidth measurement can be of outbound and/or inbound traffic. When unidirectional bandwidth is recorded, the outbound bandwidth is measured and the incoming bandwidth is estimated according to a predefined ratio. When the bidirectional metrics are measured, both the outbound and inbound metrics are measured.

Three metrics can be recorded:

- Unidirectional Bandwidth
- Bidirectional Estimate Bandwidth
- Robust Bidirectional Sample Bandwidth

Unidirectional Bandwidth

Measures the outbound bandwidth availability and estimates the inbound bandwidth availability. Use this metric when you are unable to place an agent at the Target endpoint, for example a web server such as <http://www.example.com>. This protocol may place a moderate load on the network. Note that results may not be fully accurate when the network is undergoing heavy traffic conditions.

- **Interval:** Set to 2 minutes or higher, as each probe usually requires about 15 seconds. Bandwidth may be measured with multiple concurrent monitors. For details, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).
- **Pinging Protocol:** Recommended to choose **Auto Select**, which selects the first available protocol in the following order: NTP, ICMP Timestamp and then ICMP Echo. Each of these can also be selected individually. Both NTP and ICMP Timestamp provide more accurate results, and the response on the return trip is not influenced by the network conditions.

Note: To measure unidirectional bandwidth using the NTP pinging protocol, the NTP service must be enabled.

- **Port:** Type a valid Port number, or choose **Auto Select** for Network Capture to scan a list of predefined list of ports to locate an available port. Network Capture validates that the selected port is indeed available (i.e., not blocked by firewalls); and if not, the run is aborted. Autoscan selects ports based on the defaults set in the **NC.Protocols.config** file located in **<Network Capture Agent home directory>\Bin\AgentImplementation**. You can modify this file to define alternate ports to be scanned.

Bidirectional Estimate Bandwidth

This protocol measures bidirectional bandwidth availability. Both the Source and Target Endpoints require an installed HP Agent. Select Bidirectional Estimate to measure both upstream and downstream

bandwidth availability; polling usually occurs at three second intervals.

- **Interval:** Set to 2 minutes or higher. Bandwidth may be measured with multiple concurrent monitors. For more information, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).
- **Port:** Choose Auto Select for Network Capture to scan a list of predefined list of ports to locate an available port. To select a specific port, type a valid Port number, or use the up/down arrows. Network Capture validates that the selected port is indeed available (i.e., not blocked by firewalls), and if not, the run is aborted.
- **Probing Protocol:** This displays the protocol that is used to generate network traffic.

Robust Bidirectional Sample Bandwidth

Measures bidirectional bandwidth availability. Both the Source and Target Endpoints require an installed HP Agent. Accurate measurements are obtained when the bandwidth capacity is less than 50 Mbps and the Round Trip Time is less than 120 seconds. Bidirectional Sample places a substantial traffic load on the network.

Note: Due to a issue in MS Windows XP's implementation of the TCP/IP stack, Robust Bidirectional may measure lower than available bandwidth when the round-trip packet loss rate is high (higher than 2%) and the probing machine is Windows XP. This means that downstream available bandwidth results when Windows XP runs on the Target endpoint, and upstream results when XP runs on the source endpoint may be affected.

- **Interval:** Set to 2 minutes or higher. Bandwidth can be measured with multiple concurrent monitors. For more information, see ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#).
- **Port:** Both the Source and Target require an installed HP Agent. Or Choose **Auto Select** for Network Capture to scan a list of predefined list of ports to locate an available port. To select a specific port, type a valid port number, or use the up/down arrows. Network Capture validates that the selected port is indeed available (i.e., not blocked by firewalls); and if not, the run is aborted. Autoscan selects ports based on the defaults set in the **NC.Protocols.config** file located in **<Network Capture Agent home directory>\Bin\AgentImplementation**. You can modify this file to define alternate ports to be scanned.
- **Probing Protocol:** This displays the protocol that is used to generate network traffic.

Configuring Web Server Parameters

HTTP Response Time measures the length of time required for the HTTP response to be received from the Target Endpoint. This includes DNS lookup time, TCP connection establishments, server processing time and network latency.

HTTP Response Time

Requires a web server at the Target Endpoint.

- **Interval:** Select a value, or use the default of 30 seconds.
- **HTTP Method:** Select **Get** or **Head** (Head usually provides more accurate results).
- **Timeout:** Defines the period after which the request is considered lost if no response is received from the web server. Select a value or use the default.
- **Resource Path:** The path to the requested resource, e.g. / or /index.html.

- **Port:** Select the port number on which a TCP/HTTP server is listening for incoming requests (by default 80 or 443) or type a specific port number.
- **Max Redirections:** The number of redirections to follow. Usually "0" since a reply from the Target Server is expected.
- **User Agent:** The user agent string to be used when contacting the web server. Some web servers may only reply to predefined agents. The default value uses the Firefox 4.0 user agent string.
- **Status Code:** Select the Status Code that is expected to be received from the web server. When a received status code does not match the one specified, the request is considered lost. Select a specific status code, or to accept any type of status code that does not indicate an error should be accepted by selecting **Any status code**.
- **Schema:** Select **secure (HTTPS)** or **non-secure (HTTP) communication**.

Start Monitoring

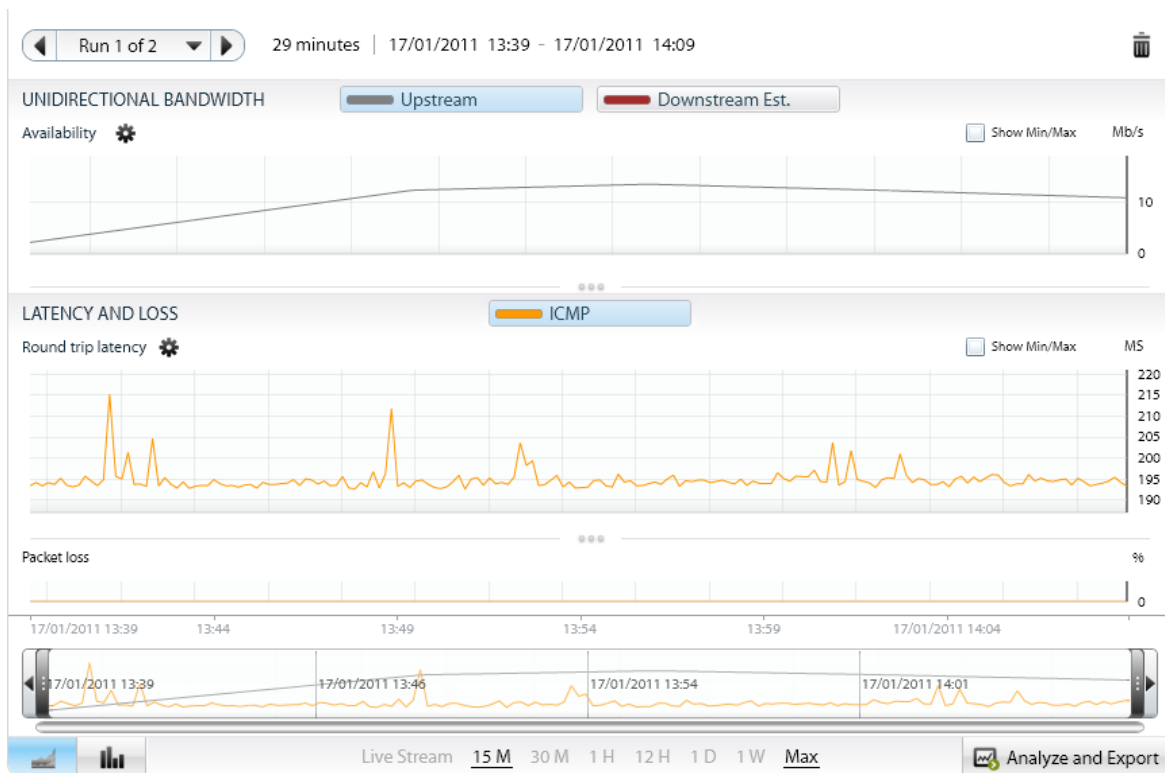
After configuring the Monitor, begin recording by clicking the **Run Monitor** button in the toolbar. Validation of various components occurs in this order:

1. Source Endpoint can poll the Network Capture Server and obtain commands
2. Clock synchronization between the Network Capture Server, involved Agents and the host on which you are viewing results
3. Source Endpoint is able to send results to the Network Capture Server
4. Source Endpoint can communicate with the Target Endpoint (for peer-based monitors' only)
5. Port collisions do not occur

Note: If the Monitor does not start after the Initialization, see ["FAQs and Troubleshooting" on page 49](#).

Viewing Data

When you click **Results** from the Monitors page, Network Capture displays runtime results of the selected run for that monitor; by default the latest 15 minutes results are shown in the Line Chart view. To view offline results, click **Max** to view the entire time span.

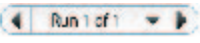


The progress bar at the top indicates the Start and End time, and the percentage of time that has elapsed. You can view current and previous recordings.

Note: If the Source Agent is not accessible for a certain period, the results curve connects the point where the last data was obtained with the result after the timeout, so that a continuous line is displayed.

Click the **Percentile Distribution Graph** icon  to display the data in a percentile distribution graph format.








If the monitor has run more than once, select the required run using the arrows. 

You can open current and previous recordings (the progress bar is only visible for monitors that are currently running).



The status of each monitor is visible according to the icon beside the monitor's name:

	Currently running
	Indicates that a metric in the last run of this monitor did not run successfully
	Idle; not currently running or has completed successfully
	Currently running but some of the protocols have stopped running
	Error: only appears under the Results button if the run stopped with errors. Select this icon to view an explanation of the issue.

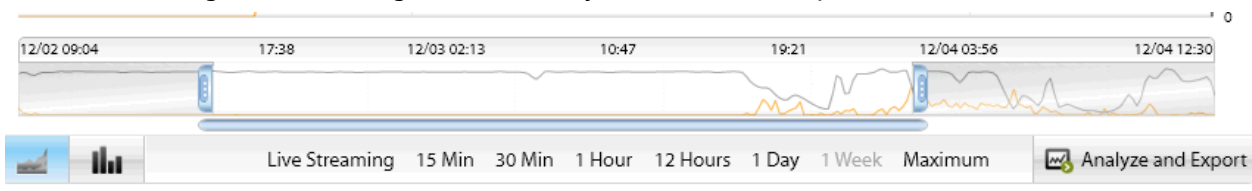
Note: If the Network Capture Server, Agent and the host on which you are viewing results clocks are not synchronized, the time displayed in the Results will not be correct; however, the results are still valid. To synchronize your clocks, in each host computer, ensure that the "Synchronize with an Internet Time Server" option is selected in the Time Settings.

Zoom In and Zoom Out

The granularity of the results shown depends on the length of the recording. Therefore for recordings of longer duration, to view more detailed results, use the Zoom to select a specific time period. By default the most recent results are shown, so that selecting a 12 hour period shows the last 12 hours, not the first 12 hours of the recording. Most of the following options are available in both Line charts and Percentile Distribution chart views.

To select a time range:

- At the bottom of the Results page click a Time Period, from 15 minutes to Maximum (the full range of the recording). Live Streaming: refreshes every with each new sample.



Use the following methods to select a specific time period:

- To find the exact instance of an event in a run, use the tooltip on the vertical blue line in the Results display to indicate the date and time.

23 hours, 58 minutes | 06/01/2011

NDWIDTH Upstream

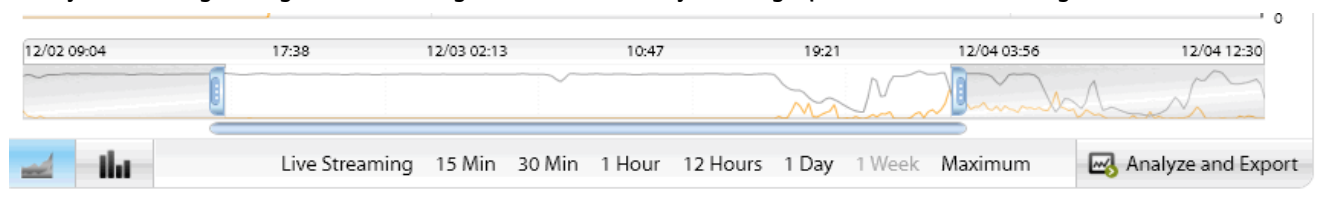
14.5 Mb/s



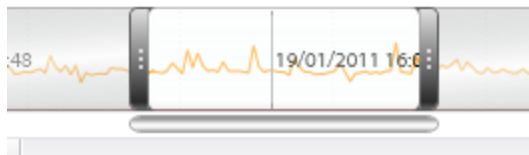
339.34 ms



- Adjust the range using the left and right slider bars to adjust the graph to the selected range.



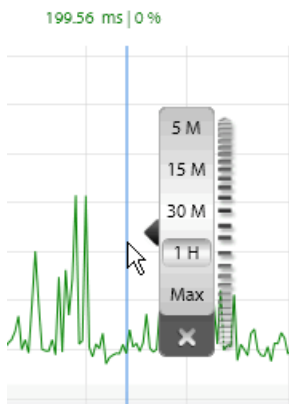
- Slide the magnifier across the slider to the required time period.



- Jump to previous time/next time frame using the arrows at the far left and far right of the slider.

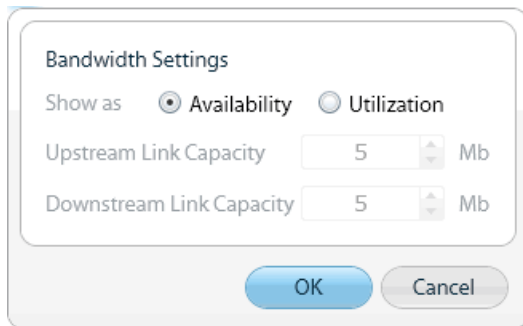


Double-click the graph and use the mouse wheel to select the required time frame.



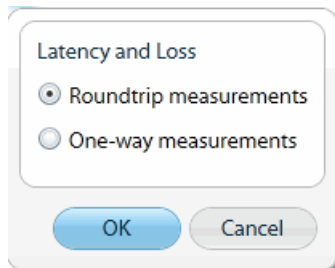
To display Bandwidth as Availability or Utilization:

1. In the Results page, click the **Bandwidth Settings** icon.
2. In the Bandwidth Settings window, select **Availability** or **Utilization**. If you select Utilization, supply the value for the Link Capacity.



To configure Latency and Loss Settings:

1. In the Results page, click the **Latency and Loss Settings** icon.



2. In the Latency Settings select **Roundtrip** or **One-way measurements**.

Searching for Data

You can search for data in the current view by entering either free text, or by selecting one of the drop-down options. A pre-defined search displays all those monitors with a specific status.

Analyzing Data

As Network Capture collects data, you will probably be wondering how to use the data to best advantage when emulating these conditions in HP's performance applications. You'll be exporting a file that contains about a half hour of data, so you'll want to ensure that each file provides a picture of the network at crucial periods.

To analyze the data:

1. In the Results page, click **Analyze and Export** below the graphs.
2. To quickly view specific time periods, select a time period in the **Analyze** section.
Select the time period for which to show these conditions; 1 or 5 minutes are often sufficient. For a longer time span, select 15 or 30 minutes. To export the results, choose the displayed time period or the entire run, according to either latency or bandwidth calculations. For more information, see ["Exporting Data" on page 46](#).
3. For more detailed statistics, select **Performance Statistics**.

Performance Statistics

Bandwidth

The results display the available bandwidth.

The **Lowest** displays lowest observed bandwidth results for selected period.

The **5th Percentile** displays lowest measured bandwidth conditions for selected period excluding rare occurrences.

The **95th Percentile** displays highest observed bandwidth results for selected period, excluding rare bursts or outermost conditions.

The **Typical** displays the geometric mean of the selected period, which indicates the most representative bandwidth conditions.

The **Highest** value displays highest observed bandwidth conditions for selected period.

Latency (Round Trip) and Packet Loss

Low identifies the period with the lowest latency/loss conditions during the selected time-frame.

The **95th Percentile** displays results with the lowest observed latency and packet loss for selected period, ignoring infrequent dips.

The **Mean** value shows the geometric mean of the latency and packet loss (default) or bandwidth measurements, and indicates the most common network conditions in your network. When testing application response time, use this value to simulate typical transaction response.

The **5th Percentile** displays the highest observed latency and packet loss for selected period, but ignores rarely occurring peaks.

Highest identifies the period with highest latency/loss conditions during the selected time-frame.

The **Average Loss** (relevant only for Packet Loss) displays the calculated average of the packets lost in the defined period.

Tips

Use the slider bar to find network conditions for a specific time of day, or use the analyses to find the lowest, mean or highest 1, 5, 15 or 30 minute time frames.

Using Network Profiles

Network Profiles utilize data from monitors that were recorded by Network Capture, or from external sources. These recording can be analyzed so that best, worst or typical conditions obtained during the recording period can be isolated. These conditions can be exported in .ntx format to be used in testing emulations.

Note: When importing a recording in the HP Network Virtualization Modeler's Cloud Shape, the Network Profile is present instead of Monitors, which were present in previous versions of HP Network Capture (formerly Shunra NetworkCatcher).

Network Profiles provide actual recorded network conditions for these types of monitors:

- Mobile
- Stationary
- Monitor-based

The data can be selected according to the Geographic Source and Target, Type of communication, and Duration.

To create a Mobile Profile:

1. Select the **New Profile** icon ; by default a Mobile profile is created. The Profile name can be up to 255 characters.

Note: To create a Stationary or Monitor-base profile, select the required option in the drop-down list, see below.

2. Select the Source and Target cities in the From and To lists.
3. Select the type of connection, either WiFi or Cellular (additional options are available by clicking the **Settings** icon).
4. Select the Device.
5. Select Latency and/or Bandwidth and one of these conditions:
 - **Best:** most favorable observed conditions for selected period
 - **Typical:** geometric mean; displays the most representative conditions
 - **Worst:** displays lowest observed conditions for selected period
6. Select the Emulation Time (duration) of the recording, from one minute to two hours.
7. Select **OK**, or **Save and Add Another**. Network Capture calculates the conditions according to the selected parameters and the results are displayed.

To create a Stationary Profile:

1. Select **Stationary** from the drop-down list beside the **New Profile** icon.
2. Select the Source (client or data center); the Target is a data center.
3. Select **Latency** and/or **Bandwidth** and one of these conditions:
 - **Best:** most favorable observed conditions for selected period
 - **Typical:** geometric mean; displays the most representative conditions
 - **Worst:** displays lowest observed conditions for selected period
4. Select the Emulation Time (duration) of the recording, from one minute to two hours.
5. Select **OK**, or **Save and Add Another**. Network Capture calculates the conditions according to the selected parameters and the results are displayed.

To create a Monitor-based Profile from the Profiles module:

1. Select the Monitor-based from the drop-down list beside the **New Profile** icon.
2. Select the Monitor and then **Run**.
3. Select the Latency metric, such as TCP or HTTP.
4. If Bandwidth was measured, select the Bandwidth metric, such as Bidirectional Estimate.
5. Select one type of conditions:
 - **Best:** most favorable observed conditions for selected period
 - **Typical:** geometric mean; displays the most representative conditions
 - **Worst:** displays lowest observed conditions for selected period
6. Select the Emulation Time (duration) of the recording, from one minute to two hours.
7. Select **Find by Latency** to display the interval with the required conditions according to the latency values, or **Find by Bandwidth** to display the interval in which the required conditions are displayed according to the bandwidth measurements.
8. Select **OK**, or **Save and Add Another**. Network Capture calculates the conditions according to the selected parameters and the results are displayed.

To create a Monitor-based Profile from the Monitoring module:

1. Select the Monitor and **Run**.
2. Analyze according to the required conditions, or manually select the requested time interval.
3. Ensure that other than Bandwidth, only one metric is selected.
4. Open **Analyze and Export**.
5. Select **Save as Network Profile**.
6. Select a Profiles folder, enter a name for the Profile and click **Save**.

Exporting Data

To conduct a network emulation using your actual network conditions, export data from Network Capture in an .ntx file. Then, in the HP Network Virtualization network appliance, or HP Network Virtualization desktop applications, import the file and emulate your network conditions with the recording. Only one metric of either latency and packet loss, or of bandwidth can be present in each .ntx file.

To emulate with the HP Network Virtualization desktop applications, up to 900 Latency and Packet Loss samples can be exported per metric. The number of samples present in the Export file also depends upon the default Interval settings per metric. To alter this Interval in the data that is being exported, using zoom bar, select the time frame for which to export the data.

To emulate with the the HP Network Virtualization network appliance, up to 90,000 samples can be exported. This setting can be modified in the Administration module, Settings.

Note: The Export option may appear to be disabled at first, until the data updates. Export requires supplementary licensing.

To export data:

1. In the Results or Network Profile page, click **Analyze and Export** below the graphs.
2. Select an Export option:
 - Export viewed time frame (when the current view shows a specific portion of the complete run)
OR
 - Save as network profile (from HP Network Virtualization emulation applications, these profiles can be uploaded)
3. Save the file to the required location.

To modify the Export settings:

1. In the Results or Network Profile page, click **Analyze and Export** below the graphs.
2. Select **Settings**, which links to Administration > Settings > Export. These settings can also be accessed directly in the Administration module.

Defining and Updating Users

New users can only be defined, modified and deleted by users with Administrator permissions. Operator can view their own and others' details but not modify them; they can only change their own passwords. For details, see ["Account Settings" on the next page](#).

To define a new user:

Note: Only Administrators can add Users.

1. In the Administration module, click **Users**.
2. Click the **New User** icon and define the properties. Select the account type:
 - Administrator: full permission
 - Operator: can create and modify monitors but cannot create or modify users, endpoints or other settings
3. Define a password of up to 20 alphanumeric characters.

To change the user details or password of a user:

Note: Only Administrators can modify User details.

1. On the Administration page, click **Users** in the Network Capture toolbar.
2. Double-click a user and modify the User's properties as required. Only the User Name, Phone number and Password can be modified.

To delete a user:

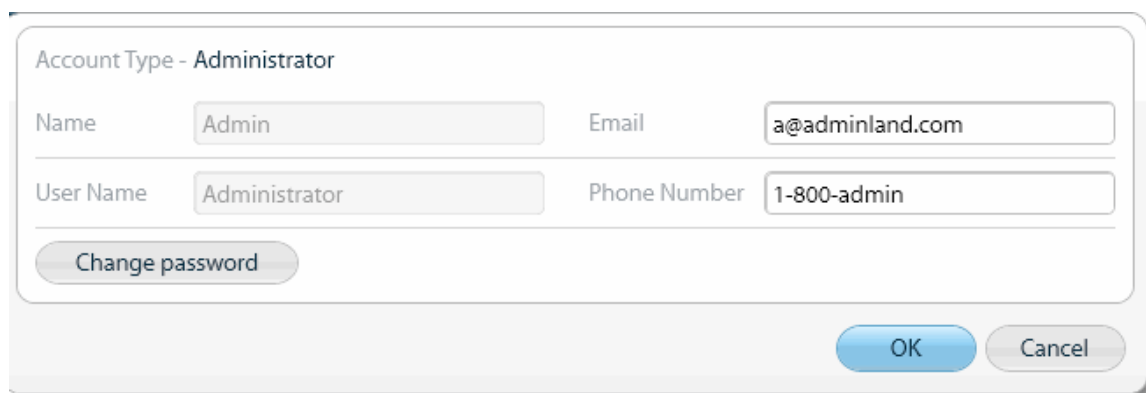
Note: Only Administrators can delete users; however the system-defined Administrator cannot be deleted.

1. On the Administration page, click **Users**.
2. Select a User and click the **Delete User** icon.

All users can reset their own passwords by clicking the "**Regenerate and send password by email**" icon.

Account Settings

To view your account details, click the **Account Settings** icon in the toolbar. The Name and User Name cannot be modified, but the other fields can be updated.



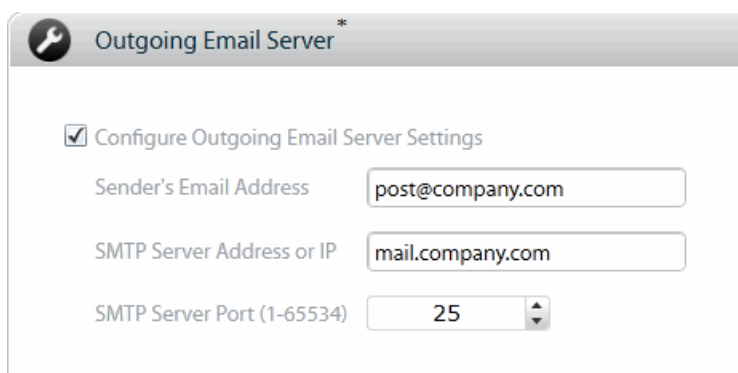
The image shows a dialog box titled "Account Settings". At the top, it says "Account Type - Administrator". Below this, there are four input fields: "Name" with the value "Admin", "Email" with the value "a@adminland.com", "User Name" with the value "Administrator", and "Phone Number" with the value "1-800-admin". Below these fields is a button labeled "Change password". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

Outgoing Email Settings

To reset a password or conduct certain other account updates, valid SMTP Mail Settings must be set. These settings can be configured during installation, or post-installation by selecting **Administration module > Settings > Outgoing Email Server**.

- Sender Email Address: type the email address from which the emails are sent.
- SMTP Server: type the DNS or IP address of the SMTP Server which sends the email.
- Port: by default port 25, or type a different port number.

This configuration does not guarantee that the email will be sent, since networking, authorizations and other factors may prevent this operation. For these issues, contact your System Administrator.



Setting Schedules

Use the Scheduler to start and end a Monitor's recordings according to specific timetables. Schedules can be created when defining a Monitor, or later, but not while the Monitor is running. The Scheduler sets the time according to the time on the machine on which you are defining the Monitor.

To set a Schedule:

1. When defining or editing a Monitor, click the **Scheduling** button.
2. Define the Start and End Times, Set the recurrence if required. The recordings can be set to recur daily, weekly or monthly.
3. Define the duration of each recording.

FAQs and Troubleshooting

I am not able to create a new network profile. The From and To dropdown lists are empty. What should I do?

This occurs when the Network Capture server is behind a proxy.

Locate the HP Network Capture Server service. Go to the service properties, and on the **Log on** tab select **This account**. Enter the administrator user name and password, and restart the service.

I installed the Network Capture Server, and I'm able to open the Network Capture webpage, but I can't log in. Instead I get this error "Communication with Server failed". What should I do?

Start by verifying that the Network Capture Server Service is Started.

Validate that ASP.NET 4.0.30319 is Allowed (depending upon the operating system, in the Web Server (IIS), IIS Manager.

Validate that the .svc file type is mapped to aspnet_isapi.dll. For further information, refer to: <http://msdn.microsoft.com/en-us/library/ms752252.aspx>.


Installation of a secured Network Capture Server fails with this error in the log "ERROR: The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or a nonwhite space character among the padding characters."

1. For information regarding a bug in IISCertObj component on Windows 7 and Windows 2008R2, refer to: <http://support.microsoft.com/kb/982386/en-us>.
2. Install the hotfix as recommended in the article listed above.
3. Reinstall the Network Capture Server.

The Network Capture Server does not start - what next?

Open the MySQL Instance Configuration Wizard and configure a Standard Instance.

An Endpoint is unreachable (red) - what can I do?

First click the **Scan all endpoints** button . The issue may have been resolved since the last scan, or the **Endpoint** icon could be red if no scans have been conducted yet. If it's still showing as inaccessible after the scan, check:

- That the Network Capture Agent Service is active.
- Firewall settings (for details, see "[Firewall Configuration](#)" on page 19).
- For Remote Agents, validate that the Server host name can be 'pinged' from the Agent host.
- To test to see if the problem is from the Source to the Target, or from the Target to the Source, you can start two different monitors in which both the Source and Target. The error message will list the element in the connection in which the problem occurs.
- You may have noticed a message during the installation that Port 80, which is required by the Network Capture Agent is already in use. To remedy this situation, determine which component is utilizing this port and assign another port to the component. Restart the HP NC Agent Service, then click **Scan all Endpoints** and the issue should be resolved.
- If this is not successful, contact support at <https://softwaresupport.hp.com/>.

I'm using Internet Explorer and I can't download the Network Capture Agent

To be able to download the agent via the browser, you'll have to adjust the following settings:

1. In Internet Explorer, open Tools > Internet Options, and select the Security tab.
2. Select **Internet** under **Select a zone to view or change security settings**.
3. Select the **Custom** level.
4. Select **Downloads** in these settings and enable the following:
 - Automatic prompting for file downloading
 - File download

Why won't my peer-based measurement start?

When you select a peer-based protocol, if the port that you have selected on the Target machine is already in use, Network Capture is unable to conduct the measurement.

The Initializing Monitor page is stuck on one of the steps, what should I do?

Close the Initializing Monitor page, click **Refresh All** and restart the monitor.

How can I look for information?

Network Capture provides extensive search capability, whether you are looking for monitors, endpoints, results and so on. For details, see ["Searching for Data" on page 43](#).

I've set Monitors to measure Unidirectional and Bidirectional Bandwidth, but the Monitors are aborted. What could be causing this problem?

Although a number of issues could cause this problem, a common reason is that IPv6, which is not supported in NetworkCatcher v7.0, is enabled. To resolve this issue, on the Source Agent host, deselect **IPV6** (depending upon your operating system, usually located in the **Local Area Connection Properties, Networking tab**).

I reset a password but the email with the new password was not received?

Check the Outgoing Email Server settings (Administration module) to ensure that they are up to date. If this does not solve the problem, contact your system administrator as this issue may be related to SMTP configuration issues.

I really like the user interface design, but something got messed up, the buttons are on top of each other and some of the images are crooked. What's going on?

Set your screen resolution to 1280x800 or higher, with a zoom level of 100%.

How can I save the results?

In the Results view, select **Analyze and Export**, and then save the data in an .ntx file format. For more information, see ["Exporting Data" on page 46](#).

I'm running Network Capture on Windows 2008 and some Monitors are aborted, the error says something about "packet duplication". What can I do?

1. To conduct certain peer-based measurements, ensure that IP Routing is disabled. To disable IP Routing (advanced users only): In the registry editor, navigate to
HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Select the **IPEnableRouter** entry.
2. To disable IP routing for all network connections installed and used by this computer, assign a value of 0.
OR
In the **regedit.exe**, right-click the entry, and then click **Modify**. In **regedt32.exe**, click the required entry > click **Edit** > click the appropriate menu entry.
3. Close the registry editor, then reboot.

Can I view results while Network Capture is recording?

Of course! As soon as you hit the Run Monitor icon, the Results view appears. You might have to wait just a bit until the results are shown in the graph as Network Capture collects the data. Soon you should be able to see a line graph or percentile distribution graph of the latency, packet loss and/or bandwidth until the monitor has run the full duration. After some time has elapsed you can view a specific period, or the entire duration. For details, see ["Viewing Data" on page 38](#).

I selected "Refresh All" or "Scan Endpoints" and it won't stop.

Check the Network Capture Service, if it's Stopped, start it. Then select **F5** to refresh the browser page. If this is unsuccessful, contact support at <https://softwaresupport.hp.com/>.

How many monitors can I run concurrently?

If you have a professional license you can run up to 25 Monitors concurrently.

Why do I need folders?

Well, you might not, you can keep all your monitors in the default folder that is present when you first open Network Capture. However, folders keep your monitors organized, and as you use Network Capture you may have many scenarios. You can choose to group your monitors according to various criteria, such geographic locations, types of applications, etc.

- To add a folder, click the **Add Folder** icon and rename the folder.
- To add subfolders, under each folder, click the **New Folder** icon when the Folder is selected and rename it.
- You can also drag and drop Monitors from one folder to another.

Can I delete a folder?

Yes, as long as the folder or its subfolders do not have any active runs that are currently recording.

How many Agents should I install?

The Network Capture Agent is installed as part of the Network Capture Server.

Therefore, you can measure latency, packet loss, or upstream bandwidth availability from the Server without installing the Network Capture Agent in any other location.

For example, if you have installed Network Capture in a datacenter in New York and need to measure latency, packet loss, and upstream bandwidth to any other location addressable over the network, you can do so without deploying additional Network Capture Agents. If the Network Capture Server is behind NAT, it can partake in both peerless and peer-based monitoring.

However, there are a couple of scenarios where additional agents are required:

- ["Measuring from a Secondary Location" below](#)
- ["Measuring Bidirectional Bandwidth Availability" on the next page](#)
- ["Defining the Interval for Concurrent Bandwidth Monitors" on page 33](#)

Measuring from a Secondary Location

For example, if you have a Network Capture Server installed in your data center in New York, but you require latency, packet loss and upstream measurements from London to a destination in Tokyo, you could install a Network Capture Agent in London. Then you could measure these metrics from London to Tokyo.



Measuring Bidirectional Bandwidth Availability

To measure bidirectional bandwidth measurements to any location, you will also need an Agent at the Target location. For example, to measure from New York to Tokyo, you will have to install an agent in Tokyo. This also applies to measurements from London to Tokyo.

Note that the same Agent may be the Target for one measurement, yet be the Source for another.



Obtaining Technical Support

Technical support is available to all HP Software Ltd. customers through the HP NV site <http://hp.com/go/nv>. Technical support may be obtained through the support site, <https://softwaresupport.hp.com/>.

Send Us Feedback



Can we make this User Guide better?

Tell us how: SW-Doc@hp.com