GO ANYWHERE®
A HelpSystems Solution

GoAnywhere Gateway User Guide

Version 2.8.1




Copyright Terms and Conditions

202004220839

Table of Contents

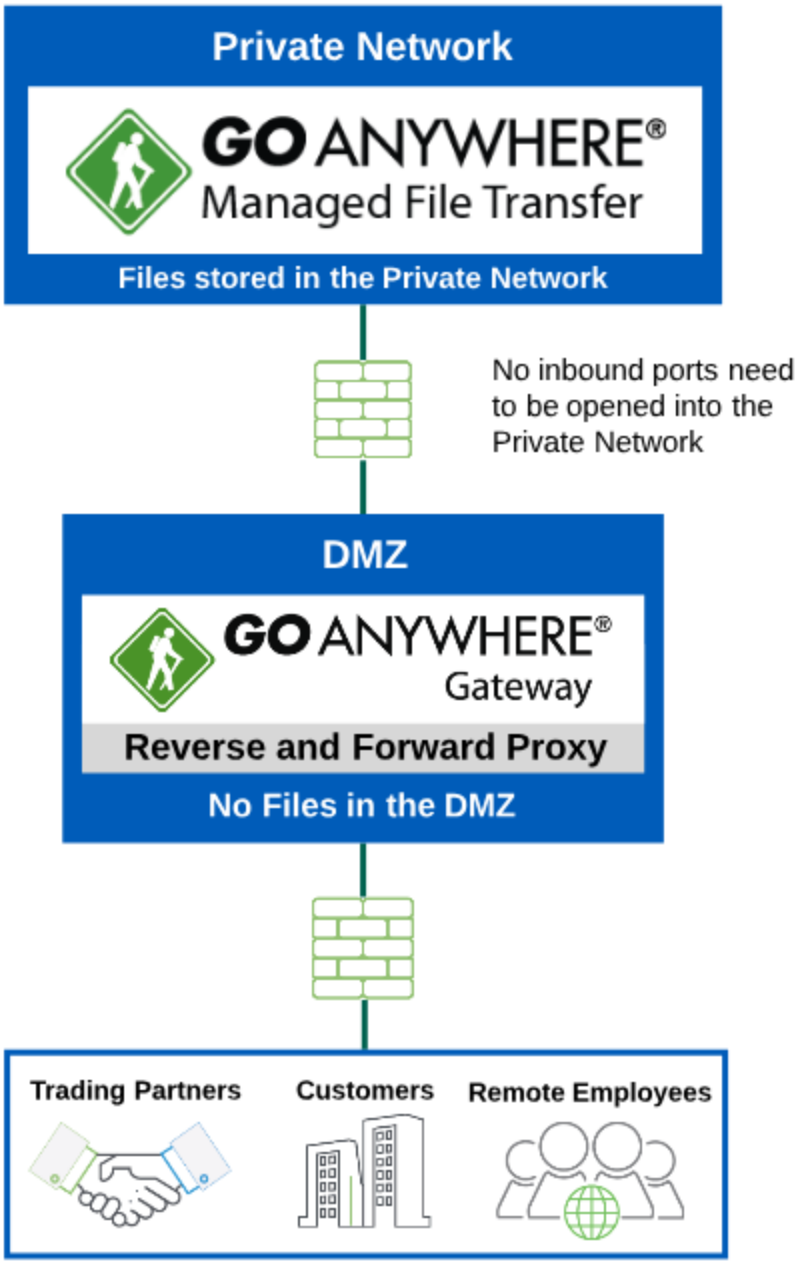
Introduction

GoAnywhere Gateway is both an enhanced reverse proxy and forward proxy. It provides an additional layer of network security when your organization needs to safely exchange data with your trading partners. When using GoAnywhere Gateway as a reverse proxy, no inbound ports need to be opened into the private/internal network and no sensitive data needs to be stored in the demilitarized zone (DMZ).

GoAnywhere Gateway is a software-only solution which is installed in the DMZ or public-facing network. Trading Partners only connect to authorized ports on GoAnywhere Gateway, which routes requests over a proprietary channel to back-end services (for example, FTP, SFTP, HTTP, & GoFast servers) in the private/internal network. This approach allows your organization to keep sensitive information (for example, data files, user credentials, keys, certificates) in the private/internal network, keeping your DMZ in compliance.

When GoAnywhere Gateway is used as a forward proxy for outbound connections, it will hide the identities and locations of those internal systems.

In essence, GoAnywhere Gateway serves as a transparent interface between internal systems and external systems without exposing sensitive files and the private/internal network. This is an essential solution for meeting strict security policies and complying with state privacy laws, HIPAA, PCI DSS, SOX, ISO 27000 and GLBA.


Private Network
GO ANYWHERE®
Managed File Transfer
Files stored in the Private Network
No inbound ports need to be opened into the Private Network
DMZ
GO ANYWHERE®
Gateway
Reverse and Forward Proxy
No Files in the DMZ
Trading Partners
Customers
Remote Employees

GoAnywhere Gateway offers the following features and benefits:

- No incoming ports need to be opened into the private/internal network- reduces the risk of network intrusion
- No sensitive data files need to be stored in the DMZ
- No user credentials, permissions, certificates and keys need to be stored in the DMZ
- Hides the locations and identities of internal systems
- Service configurations are maintained/stored in the private network
- Supports FTP, FTPS, SFTP, SCP, HTTP, HTTPS, AS2, and GoFast file transfer protocols
- Built-in load balancer to distribute workloads across multiple GoAnywhere MFT systems
- No special hardware components required; software-only solution
- Installs to Windows, Linux, AIX, UNIX and Solaris operating systems

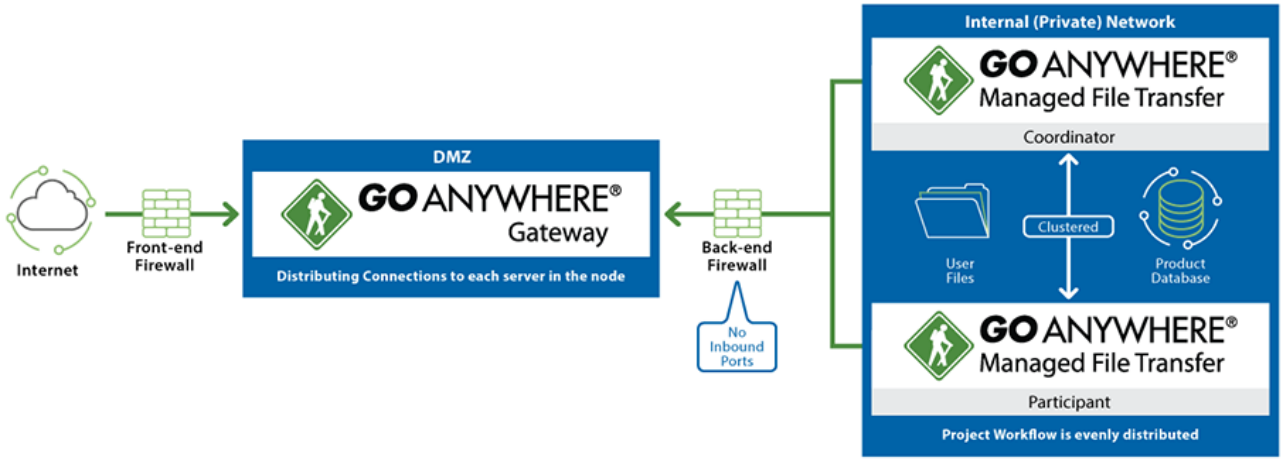
How Does it Work?

GoAnywhere Gateway can serve as both a Reverse Proxy and a Forward Proxy. Typically GoAnywhere Gateway is installed in the demilitarized zone (DMZ) and GoAnywhere MFT is installed in the private/internal network.

At startup, GoAnywhere MFT creates an outbound connection to GoAnywhere Gateway, which is used as a "control channel" for passing commands and messages between the products. This control channel will initially provide the proxy details (IP and port mappings) to GoAnywhere Gateway, at which point it will start up "listeners" on the designated IPs and ports for incoming traffic.

Reverse Proxy

When an external client (trading partner) connects to a listener on GoAnywhere Gateway in the DMZ, GoAnywhere Gateway will make a request over the control channel to GoAnywhere MFT in the private/internal network. GoAnywhere MFT will then create a new outbound data channel to GoAnywhere Gateway. This data channel will be attached to the desired service (for example, FTP, FTPS, SFTP, HTTP/s, AS2, & GoFast) and all traffic for that session will be routed over this new data channel including client authentication requests, data and commands. When the session is terminated, the corresponding data channel will be removed.



Forward Proxy

The Forward Proxy in GoAnywhere Gateway allows you to route client requests from GoAnywhere MFT (in the internal network) to external FTP, FTPS, SFTP, SCP, and GoFast servers without revealing the identity or locations of your internal systems. The Forward Proxy is additionally used by GoAnywhere MFT to route active and passive FTP and FTPS data connections through GoAnywhere Gateway.

When a process in GoAnywhere MFT needs to make an outbound connection through the proxy, a request is made to GoAnywhere Gateway with the address of the intended destination. GoAnywhere Gateway will then establish the connection to that destination and will bridge it to the requesting system.

Installing GoAnywhere Gateway

The following sections describe how to install GoAnywhere Gateway on the supported platforms.

System Requirements

GoAnywhere Gateway installs to all popular enterprise server operating systems. Listed below are the supported operating systems and minimum hardware/software requirements for installing GoAnywhere Gateway.

Windows® (32-bit and 64-bit)	
Versions	Windows Server® 2012 R2 Windows Server® 2016 Windows Server® 2019 Windows 8® Windows 10®
Disk Space Usage	100 MB
Minimum Memory	256 MB
JRE (Java Runtime Environment)	1.8.0 or higher must be installed prior to the installation.

Linux® (32-bit and 64-bit)	
Disk Space Usage	100 MB
Minimum Memory	256 MB
JRE (Java Runtime Environment)	1.8.0 or higher must be installed prior to the installation.

All other UNIX Platforms (AIX, HP-UX, Solaris, Mac OS X)	
Disk Space Usage	50 MB
Minimum Memory	256 MB

All other UNIX Platforms (AIX, HP-UX, Solaris, Mac OS X)	
JRE (Java Runtime Environment)	1.8.0 or higher must be installed prior to the installation.

Preparing for a Gateway Installation

GoAnywhere Gateway is designed to work with multiple network interface cards (NIC) and gives you the flexibility to assign Gateway features to use a specific NIC. Prior to installing GoAnywhere Gateway, it is recommended that you determine the IP address and ports that Gateway will use to listen on for connections from GoAnywhere MFT. Typically, the installer will auto-populate these fields using the server where Gateway is installed. If the server has multiple NIC cards, then the first NIC card identified will be used. Gateway will attempt to assign protocols to use pre-selected default ports. If a default port is already in use on your system, you will need to specify a different available port. These settings can be updated any time after installation using the gateway.xml file.

Setting	Purpose
Controller Address	The IP address that GoAnywhere Gateway will listen on for control connections from GoAnywhere MFT. This is typically the IP address of the server where GoAnywhere Gateway is installed.
Controller Port	The port that GoAnywhere Gateway will listen on for control connections from GoAnywhere MFT. The default port is 9100.
Data Address	The IP address that GoAnywhere Gateway will listen on for data connections from GoAnywhere MFT. Like the Controller Address, this is typically the IP address of the server where GoAnywhere Gateway is installed.
Data Port	The port that GoAnywhere Gateway will listen on for data connections from GoAnywhere MFT. The default port is 9101
Shutdown Port	The port that GoAnywhere Gateway will listen on for shutdown requests. The default port is 9105.
Proxy Considerations **Note**: Detailed proxy settings can be found in the Gateway Server Configuration table.	
Proxy Enabled	The proxy feature must be enabled in order to route Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT. This feature can also be used as an outbound proxy from GoAnywhere MFT.

Setting	Purpose
Proxy Address	The IP address that GoAnywhere Gateway will listen on for Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT. This is typically the IP address of the server where GoAnywhere Gateway is installed.
Proxy Port	The port that GoAnywhere Gateway will listen on for Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT. The default proxy port is 9102.
Passive Proxy Address	The IP address on which the GoAnywhere Gateway should listen for incoming passive FTP data connections from external clients. This is typically the external IP address of the server where GoAnywhere Gateway is installed.
Passive Proxy From Port	The beginning port in the range of ports available for FTP passive data connections from external clients. The default port is 30000.
Passive Proxy To Port	The ending port in the range of ports available for FTP passive data connections from external clients. The default port is 32000.
Active/Forward Proxy Address	The IP address GoAnywhere Gateway will use when active data connections are requested. This address is also used to establish outbound connections to remote servers when GoAnywhere Gateway is used as a forward proxy. The value should be the local IP you used when establishing an outbound connection from the GoAnywhere Gateway server, and is typically the external IP address of the server where GoAnywhere Gateway is installed.
GoFast File Transfer Acceleration Considerations	
UDP Enabled	The UDP data server provided by GoAnywhere Gateway allows the GoFast accelerated file transfers from GoAnywhere MFT to proxy through GoAnywhere Gateway. GoFast is a licensed feature of GoAnywhere MFT.
Internal UDP Address	The IP address or host name of the Gateway UDP data server. This is where GoAnywhere MFT will connect to when sending out GoFast packets during data transfers. This is typically the IP address of the server where GoAnywhere Gateway is installed.
Internal UDP From Port	UDP data ports are assigned dynamically for each file transfer. This is the low end UDP data port number for the range of UDP ports used for GoFast file transfers. The default is 9201.

Setting	Purpose
Internal UDP To Port	The high end UDP data port number for GoFast file transfers. The default is 9300.
External UDP Address	The IP address or host name of the external UDP data server. This is where GoFast clients will send UDP packets during GoFast data transfers. This is typically the IP address of the server where GoAnywhere Gateway is installed.
External UDP From Port	UDP data ports are assigned dynamically for each file transfer. This is the low end UPD data port on the external GoFast server. The default is 32001.
External UDP To Port	The high end UDP data port number for the external GoFast file server. The default is 32100.

Example IP Address and Port Configurations

The following tables illustrate example IP address and port configurations for GoAnywhere Gateway.

Single Network Interface Card

In this example, the server where GoAnywhere Gateway is installed contains a single network interface card. This settings on this table is consistent with the auto populated IP addresses and ports you might encounter during installation.

Server IP Address: 10.1.2.43	Port
Controller Address: 10.1.2.43	**Control Channel**: 9100
Data Address: 10.1.2.43	**Data Channels**: 9101
Proxy Address: 10.1.2.43	**Shutdown**: 9105
Passive Proxy Address: 10.1.2.43	**Proxy**: 9102
Active/Forward Proxy Address: 10.1.2.43	**Passive Proxy Range**: 30000 - 32000
Internal UPD Address: 10.1.2.43	**UDP Range**: 9201-9300
External UDP Address: 10.1.2.43	**External UDP Range**: 32001-32100

Dual Network Interface Cards

In this example, the server where GoAnywhere Gateway is installed contains two network interface cards. The administrator of the server has designated one NIC for internal IP addresses,

and the other designated for external IP addresses.

NIC 1

Internal IP Address 10.1.2.43	Port
Controller Address: 10.1.2.43	**Control Channel**: 9100
Data Address: 10.1.2.43	**Data Channels**: 9101
Proxy Address: 10.1.2.43	**Shutdown**: 9105
Internal UPD Address: 10.1.2.43	**Proxy**: 9102
	UDP Range: 9201-9300

NIC 2

External IP Address 172.16.2.200	Port
Passive Proxy Address: 172.16.2.200	**External UDP Range**: 32001-32100
External UDP Address: 172.16.2.200	**Passive Proxy Range**: 30000 - 32000
Active/Forward Proxy Address: 172.16.2.200	

Installing Gateway in a Virtual Environment

GoAnywhere Gateway can be installed in most virtual environments, including VMware, Microsoft Azure, Amazon EC2, and more. When installing in a virtual environment, the MAC address on the server where Gateway is installed must be static. Your Gateway license will become invalid if the MAC address changes, and a new license must be issued by contacting HelpSystems.

Installing GoAnywhere Gateway on Linux

Perform the following steps to install GoAnywhere Gateway on x86-based Linux 32-bit and 64-bit operating systems. If installing to a non x86 based system, refer to the section titled Installing GoAnywhere Gateway on Unix. The installer creates a link in the `/etc/init.d` (or `/etc/systemd/system` if systemd is detected) directory which can be used to start, stop and restart the GoAnywhere Gateway daemon.

1. Download or copy the appropriate installer to the target system.
2. Open a Terminal window.
3. If you are not already logged in as `root`, switch the user to `root` by running the `su` command.
4. Change the working directory to the directory where the installer file was downloaded by running the `cd` command (for example, `cd [installer_directory]`)

5. Change the permissions on the installer file to make it an executable. This can be done by running the command `chmod 755 [installer_file_name]`
6. Launch the installer by running the command `./[installer_file_name]`. If a Desktop environment is not available on the target system, the installer must be launched in console mode using the command `./[installer_file_name] -c`
7. Follow the on-screen instructions to complete the installation.
8. Install a license by referring to the section titled Requesting and installing License.
9. Refer to the Administering GoAnywhere Gateway section to learn how to start and stop GoAnywhere Gateway.
10. To configure GoAnywhere MFT for interfacing with GoAnywhere Gateway, please refer to the GoAnywhere MFT manual.

> **NOTE:**
> During installation, you will be prompted with some options such as IP addresses and port numbers that should be used by GoAnywhere Gateway. Please refer to the Server Configuration section for details.

Silent Install - Linux

The GoAnywhere Gateway installation can be automated by using a silent install option.

To perform a silent install of GoAnywhere Gateway on Linux:

1. Copy the GoAnywhere Gateway Linux installer file to the Linux server.
2. Execute the downloaded installer file using the following command:

```
[installer_filename].sh -q
```

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

> **EXAMPLE:**
> [installer file name].sh -q -Vgagateway.dataPort=9101 -Vgagateway.shutdownPort=9105

For parameters for silent install on Linux, see the Parameters table.

Installing GoAnywhere Gateway on Windows

Perform the following steps to install GoAnywhere Gateway on x86-based Windows 32-bit and 64-bit operating systems. The installer creates a Windows Service that starts automatically when the system is booted.

1. Download or copy the appropriate installer to the target system.
2. Log in to the target system as an administrator.
3. Launch the installation wizard by double clicking on the downloaded installer file.
4. Follow the on-screen instructions to complete the installation.
5. Record the License Request Bundle, and then follow the instructions on the Requesting and Installing License page to license the product.
6. Refer to the Administering GoAnywhere Gateway section to learn how to start and stop GoAnywhere Gateway.
7. To configure GoAnywhere MFT for interfacing with GoAnywhere Gateway, please refer to the *GoAnywhere MFT Managed File Transfer User* Guide.

NOTE:
During installation, you will be prompted with some options such as IP addresses and port numbers that should be used by GoAnywhere Gateway. Please refer to the Server Configuration section for details.

Silent Install - Windows

The installation of GoAnywhere Gateway can be automated by using a silent install option. Silent install uses the Windows command line to execute the installation.

To perform a silent install of GoAnywhere Gateway on Windows:

1. Log into the target Windows system as an administrator.
2. Open the command prompt and use the cd command to navigate to the directory containing the GoAnywhere Gateway installer.
3. Enter the command to execute the GoAnywhere Gateway installer.

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

EXAMPLE:
[installer file name].exe -q -Vgagateway.dataPort=9101 -Vgagateway.shutdownPort=9105

The following command is used to silently install GoAnywhere Gateway using all default install directories, ports, and service names:

```
[installer file name].exe -q
```

For parameters for silent install on Windows, see the Parameters table.

Installing GoAnywhere Gateway on UNIX

Perform the following steps to install GoAnywhere Gateway on AIX, HP-UX, Solaris or non x86-based Linux systems. The installer creates a link in the `/etc/init.d` (or `/etc/systemd/system` if systemd is detected) directory which can be used to start, stop and restart the GoAnywhere Gateway daemon.

1. If not already installed, load Java Runtime Environment (JRE) version 7.0 (1.7.0) or later.
2. Download or copy the appropriate installer to the target system.
3. Open a Terminal window.
4. If you are not already logged in as `root`, switch the user to `root` by running the `su` command.
5. Change the working directory to the directory where the installer file was downloaded by running the `cd` command (for example, `cd [installer_directory]`)
6. Change the permissions on the installer file to make it an executable. This can be done by running the command `chmod 755 [installer_file_name]`
7. Launch the installer by typing the command `./[installer_file_name]`. If a Desktop environment is not available on the target system, the installer must be launched in console mode using the command `./[installer_file_name] -c`
8. Follow the on-screen instructions to complete the installation.
9. Install a license by referring to the section titled Requesting and installing License.
10. Refer to the Administering GoAnywhere Gateway section to learn how to start and stop GoAnywhere Gateway.
11. To configure GoAnywhere MFT for interfacing with GoAnywhere Gateway, please refer to the *GoAnywhere MFT Managed File Transfer User Guide*.

> **NOTE:**
> During installation, you will be prompted with some options such as IP addresses and port numbers that should be used by GoAnywhere Gateway. Please refer to the Server Configuration section for details.

If the installer cannot find a compatible JRE, follow the steps below:

1. Define an environment variable named `INSTALL4J_JAVA_HOME` to point to the home directory of the JRE (for example, `export INSTALL4J_JAVA_HOME=/usr/lib/jvm/java-1.7.0-sun/jre`).
2. Clear the Installer cache by removing the file named `.install4j` from your home directory (for example, `rm /root/.install4j`).
3. Run the installer again as outlined in step 7 above.

How to change the JRE after GoAnywhere Gateway is installed:

1. Edit the [Install Directory]/.install4j/pref_jre.cfg file and update the path to the preferred JRE.
2. Restart the GoAnywhere Gateway service.

Silent Install - UNIX

The GoAnywhere Gateway installation can be automated by using a silent install option.

To perform a silent install of GoAnywhere Gateway on AIX, HP-UX, Solaris or non x86-based Linux systems (UNIX):

1. Copy the GoAnywhere Gateway UNIX installer file to the UNIX server.
2. Execute the downloaded installer file using the following command:

```
[installer_filename].sh -q
```

Parameters that begin with -V must be specified as a key=value pair. Separate each -V parameter with a space.

EXAMPLE:
[installer file name].sh -q -Vgagateway.dataPort=9101 -Vgagateway.shutdownPort=9105

For parameters for silent install on UNIX, see the Parameters table.

Silent Install Parameters

The following table contains the required and optional parameters for a silent install on Windows, Linux, and AIX, HP-UX, Solaris or non x86-based Linux systems (UNIX):

Parameter Name	Description	Required
-q	Displays no user interface.	Yes
-dir	The directory path where GoAnywhere Gateway will be installed.	No
-Vgagateway.serviceDisplayName	The display name of the GoAnywhere Gateway service. **NOTE:** This parameter is used only for silent install on Windows.	No

Parameter Name	Description	Required
-Vgagateway.serviceName	The name of the GoAnywhere Gateway service (this is typically the same as the serviceDisplayName). **NOTE:** This parameter is used only for silent install on Windows.	No
-Vgagateway.controllerAddress	The IP address that GoAnywhere Gateway will listen on for control connections from GoAnwhere MFT. This is typically the IP address of the server where GoAnywhere Gateway is installed.	No
-Vgagateway.controllerPort	The port that GoAnywhere Gateway will listen on for control connections from GoAnywhere MFT. The default port is 9100.	No
-Vgagateway.dataAddress	The IP address that GoAnywhere Gateway will listen on for data connections from GoAnywhere MFT. This is typically the IP address of the server where GoAnywhere Gateway is installed.	No
-Vgagateway.dataPort	The port that GoAnywhere Gateway will listen on for data connections from GoAnywhere MFT. The default port is 9101.	No
-Vgagateway.shutdownPort	The port that GoAnywhere Gateway will listen on for shutdown requests. The default port is 9105.	No

Parameter Name	Description	Required
-Vgagateway.proxyEnabled	The proxy feature must be enabled in order to route Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT.	No
-Vgagateway.proxyAddress	The IP address that GoAnywhere Gateway will listen on for Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT. This is typically the IP address of the server where GoAnywhere Gateway is installed.	No
-Vgagateway.proxyPort	The port that GoAnywhere Gateway will listen on for Active and Passive data connections from the FTP and FTPS Services in GoAnywhere MFT. The default proxy port is 9102.	No
-Vgagateway.passiveProxyAddress	The IP address on which the GoAnywhere Gateway should listen for incoming passive FTP data connections from external clients. This is typically the external IP address of the server where GoAnywhere Gateway is installed.	No
-Vgagateway.passiveProxyPortRangeFrom	The beginning port in the range of ports available for FTP passive data connections from external clients. The default port is 30000.	No

Parameter Name	Description	Required
-Vgagateway.passiveProxyPortRangeTo	The ending port in the range of ports available for FTP passive data connections from external clients. The default port is 32000.	No
-Vgagateway.activeProxyAddress	The IP address GoAnywhere Gateway will use when active data connections are requested. This address is also used to establish outbound connections to remote servers when GoAnywhere Gateway is used as a forward proxy. The value should be the local IP you used when establishing an outbound connection from the GoAnywhere Gateway server, and is typically the external IP address of the server where GoAnywhere Gateway is installed.	No
-Vgagateway.internalUdpPortRangeFrom	The low end UDP data port number for the range of UDP ports used for GoFast file transfers. The default is 9201.	No
-Vgagateway.internalUdpPortRangeTo	The high end UDP data port number for the range of UDP ports used for GoFast file transfers. The default is 9300.	No
-Vgagateway.externalUdpPortRangeFrom	The low end UDP data port number for the external GoFast file server. The default is 32001.	No
-Vgagateway.externalUdpPortRangeTo	The high end UDP data port number for the external GoFast file server. The default is 32100.	No

Requesting and Installing a Gateway License

Before GoAnywhere Gateway can be started, a license must be installed. Licenses are managed in the GoAnywhere Customer Portal and can be accessed by logging in to your account at https://my.goanywhere.com. Within the Portal, navigate to the license page, find an available GoAnywhere Gateway license, and then choose activate.

License Considerations

GoAnywhere Gateway requires the purchase of a base license. If GoAnywhere MFT is clustered, then the purchase of the GoAnywhere Gateway Load Balancer feature is also required.

For more information on licensing considerations, please contact your sales representative.

Installing the License

In order to use GoAnywhere Gateway, a valid license (either an evaluation or a permanent) must be installed on the system. Perform the following steps to request and install a license:

1. Log in to the system where GoAnywhere Gateway is installed.
2. Open a command line or terminal. (Windows users must run the command line as an Administrator.)
3. Change the working directory to the directory where GoAnywhere Gateway is installed (for example, `cd [install_directory]`).
4. Run the command `./gagateway license`. Follow the instructions displayed on the screen to request a license. If a license is already installed, this command will display the current license information.

Once your license is activated on the Customer Portal, download the license to your workstation by clicking the Download button. You can also download the license at any time by expanding the Active license row and clicking the Download button under the license key.

Once the gateway.lic file is downloaded, copy the file to the installation directory on the GoAnywhere Gateway server that produced the license activation request.

Windows Example

- **Installation Directory**: C:\Program Files\HelpSystems\GoAnywhere Gateway
- **License File Location**: C:\Program Files\HelpSystems\GoAnywhere Gateway\gateway.lic

Linux/Unix Example

- **Installation Directory**: /usr/local/HelpSystems/GoAnywhere_Gateway
- **License File Location**: /usr/local/HelpSystems/GoAnywhere_Gateway/gateway.lic

Once the license has been placed in the correct installation directory, you must stop and then start the GoAnywhere Gateway service.

The activated license exclusively belongs to the GoAnywhere Gateway installation that produced the activation request. It cannot be used to upgrade or run any other install of GoAnywhere Gateway.

Deactivating a Gateway License

A GoAnywhere Gateway License can be deactivated. This is useful when you are migrating Gateway from one server to another. Follow the instructions to deactivate a Gateway License:

1. Log in to the system where GoAnywhere Gateway is installed.
2. Open a command line or terminal. (Windows users must run the command line as an Administrator.)
3. Change the working directory to the directory where GoAnywhere Gateway is installed (for example, `cd [install_directory]`).
4. Run the command `./gagateway deactivateLicense`. Follow the instructions displayed on the screen to deactivate the license on the GoAnywhere Customer Portal.

Administering GoAnywhere Gateway

The topics in this section provide instructions for administering GoAnywhere Gateway, such as Starting and Stopping GoAnywhere Gateway and other miscellaneous commands.

Instructions for upgrading GoAnywhere Gateway can be found in the *GoAnywhere Gateway Upgrade Guide* which can be downloaded from the GoAnywhere Customer Portal.

Starting GoAnywhere Gateway

The instructions for starting GoAnywhere Gateway depends on the operating system. Perform the steps in the appropriate section to start GoAnywhere Gateway.

Windows

1. Log in to the target Windows system where GoAnywhere Gateway is installed.
2. Open the Services window from the Control Panel.
3. Right-click the GoAnywhere Gateway service in the Services window.
4. Click Start from the context menu.

Linux and UNIX

1. Log in to the target Linux/UNIX system where GoAnywhere Gateway is installed.
2. Open a Terminal window.
3. If your system supports systemd, execute the command `systemctl start gagatewayd` Otherwise, execute the command `/etc/init.d/gagatewayd start`

Stopping GoAnywhere Gateway

The instructions for stopping GoAnywhere Gateway depends on the operating system. Perform the steps in the appropriate section to stop GoAnywhere Gateway.

Windows

1. Log in to the target Windows system where GoAnywhere Gateway is installed.
2. Open the Services window from the Windows Control Panel.
3. Right-click the GoAnywhere Gateway service in the Services window.
4. Choose Stop from the context menu.

Linux and UNIX

1. Log in to the target Linux/UNIX system where GoAnywhere Gateway is installed.
2. Open a Terminal window.
3. If your system supports systemd, execute the command `systemctl stop gagatewayd` Otherwise, execute the command `/etc/init.d/gagatewayd stop`

Miscellaneous Commands

Display GoAnywhere Gateway's Version

Perform the following steps to display the installed version of GoAnywhere Gateway:

1. Open a Command window or Terminal.
2. Change the directory to the installation directory.
3. Run the command `./gagateway version`

Display the License Information

Perform the following steps to display the license information:

1. Open a Command window or Terminal.
2. Change the directory to the installation directory.
3. Run the command `./gagateway license`. If a license is already installed, the license information will be displayed on the console. If no license is installed, information needed to request a license is displayed.

Display Java Runtime Environment (JRE) Configuration

Perform the following steps to display the JRE configuration:

1. Open a Command window or Terminal.
2. Change the directory to the installation directory.
3. Run the command `./gagateway jvmconfig`

Upgrading the Java Virtual Machine (JRE)

GoAnywhere supports OpenJDK versions of Java provided by Oracle, IBM, and Azul. Depending on the operating system, GoAnywhere Gateway may use a JRE that is bundled with the application or it may use an existing JRE which is already installed. Follow the steps below to determine which JRE is being used and then take the appropriate upgrade steps.

Determine Java (JRE) version and Location

1. Run the operating system command prompt as Administrator and navigate to the folder that contains the GoAnywhere Gateway Software.
2. Run the command `gagateway jvmconfig` (on Linux, `./gagateway jvmconfig`).
3. Updating the JRE:
    - If the Java Home is configured to [INSTALL_DIR]/jre, you are using the embedded JRE. Use the Upgrade instructions below to upgrade your embedded JRE.
    - If the Java Home is configured to any other directory, you are using an external JRE. Upgrade your external JRE to Java 8 or later.

Cleaning Up Existing Embedded JRE Folders

Even if GoAnywhere Gateway is using an external JRE, it is possible that an embedded JRE still exists within the application. If so, the upgrader may attempt to use the embedded JRE rather than the one used to start GoAnywhere Gateway. In order to prevent the upgrader from using the old embedded JRE, you must remove the [INSTALL_DIR]/jre folder, or rename the [INSTALL_DIR]/jre to something like [INSTALL_DIR]/jre.old.

Upgrading the External JRE

Follow your Java vendor's instructions to upgrade your External JRE. Once the JRE is upgraded to Java 8 or later, ensure the unlimited strength JCE policy files are installed and the Java execution environment is correct.

Later versions of Java 8 include these files by default. Installing these files is only required if GoAnywhere Gateway fails to start with an error indicating that the policy files are not installed. Use the following procedures if you are instructed to install the JCE policy files:

JCE Policy Files

Before GoAnywhere Gateway can be started or upgraded using the new JRE, it requires installation of the unlimited strength JCE policy files. To use the unlimited strength JRE policy files, copy the **US_export_policy.jar** file and the **local_policy.jar** file from the **jce_policy_files/oracle/1_8** folder (located in the GoAnywhere Gateway installation folder) to the **jre/lib/security** folder (located in the JRE's installation directory).

For IBM platforms (e.g. AIX), copy the unlimited strength JCE policy files of **US_export_policy.jar** and **local_policy.jar** from the **jce_policy_files/ibm** folder (located in the GoAnywhere Gateway installation folder) to the **jre/lib/security** folder (located in the JRE's installation directory).

Changing JAVA_HOME For Windows

The JAVA_HOME environment variable needs to be set to the appropriate location for Java 8. To set the Java version used to run GoAnywhere Gateway on Windows, follow these steps:

1. Open the **Control Panel** and navigate to **System And Security** > **System**.
2. Click the **Advanced system settings** link.
3. On the **Advanced** tab, select Environment Variables, and then edit JAVA_HOME to point to where the JDK software is located, for example, C:\Program Files\Java\jdk8. If the JAVA_HOME variable is not set, click on the **New** button in the System Variables section and add the JAVA_HOME variable with the proper path (for example, C:\Program Files\Java\jdk8).

Changing JAVA_HOME For Linux

The JAVA_HOME environment variable needs to be set to the appropriate location for Java 8. To set the Java version used to run GoAnywhere Gateway on Linux, run the following command before executing the GoAnywhere Gateway upgrade script.

```
export JAVA_HOME='/path/to/jre'
```

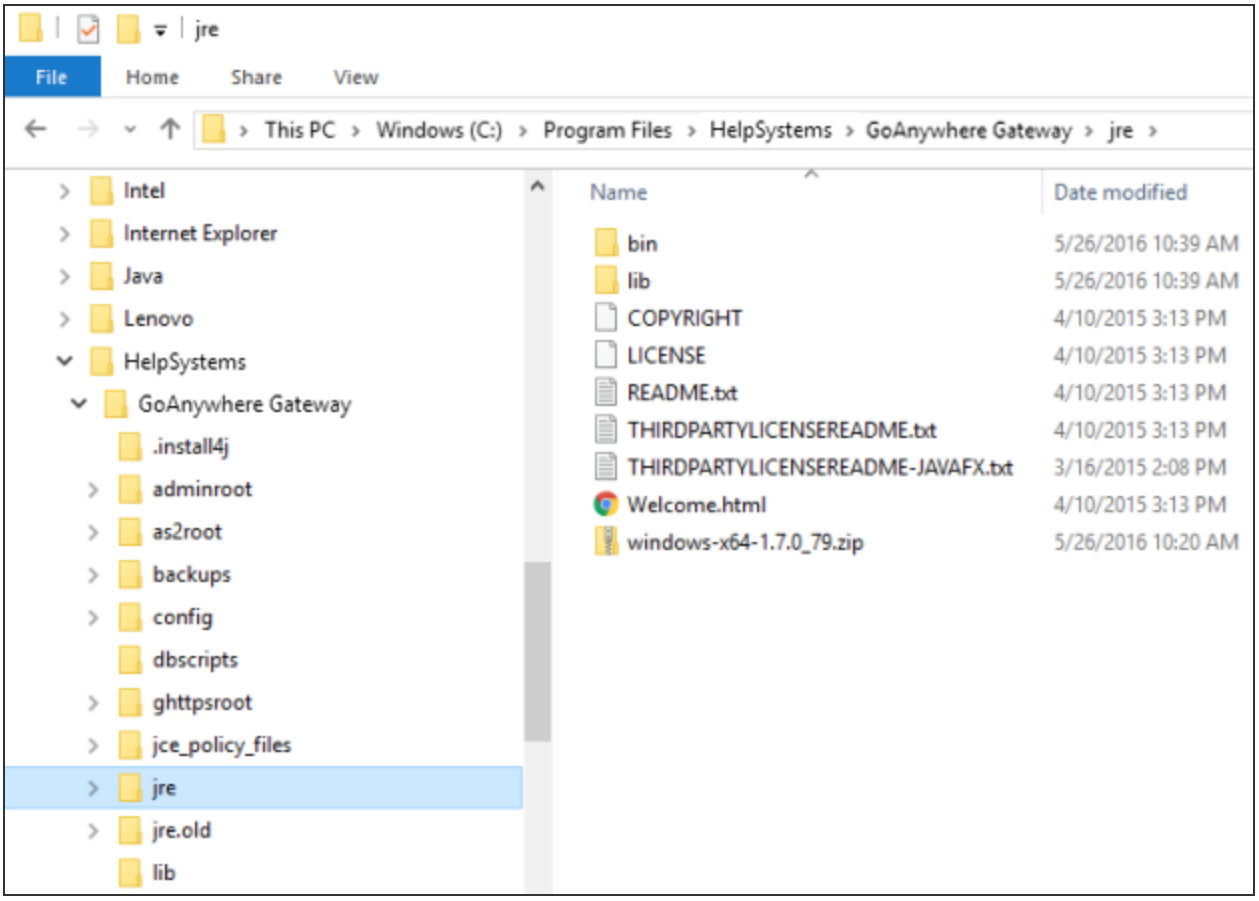
'/path/to/jre' is the absolute path to the JRE, for example: '/usr/lib/jvm/jdk8/jre'

Upgrading the Embedded JRE (Windows)

Use the following instructions to upgrade the embedded JRE to Java 8 on Windows installations:

1. Download the appropriate JRE bundle.
   - http://www.linomafiles.com/releases/goanywhere/jrebundles/windows-x86-1.8.0_131.zip
   - http://www.linomafiles.com/releases/goanywhere/jrebundles/windows-x64-1.8.0_192.zip
2. Shut down GoAnywhere Gateway.
3. Navigate to the installation directory. By default, this is C:\Program Files\HelpSystems\GoAnywhere Gateway
4. Rename the old 'jre' folder to 'jre.old'. In some cases, this folder might be called 'jre6'. If so, rename this file to 'jre6.old'. If both 'jre' and 'jre6' folders exist, rename both folders.
5. Create a new 'jre' folder in the installation directory and copy the downloaded JRE bundle into that directory.
6. Extract the contents of the JRE bundle into the current directory.

The following image illustrates the resulting folder structure in the installation directory:



7. Start GoAnywhere Gateway.
8. Verify Java has been upgraded to Java 8 or later by running the `gagateway jvmconfig` command.

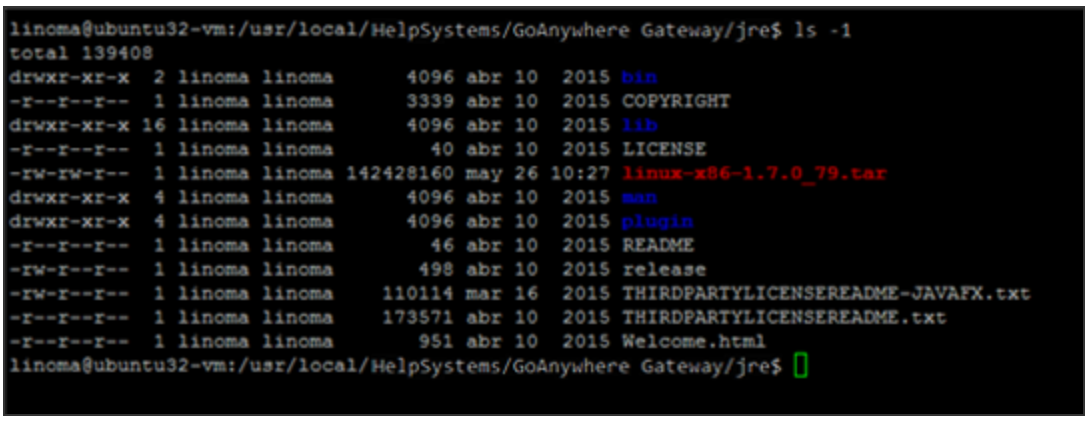
Upgrading the Embedded JRE (Linux)

Use the following instructions to upgrade the embedded JRE to Java 8 on Linux installations:

1. Download the appropriate JRE bundle.
   - http://www.linomafiles.com/releases/goanywhere/jrebundles/linux-x86-1.8.0_131_zulu.tar.gz
   - http://www.linomafiles.com/releases/goanywhere/jrebundles/linux-x64-1.8.0_192_zulu.tar.gz
2. Log in as the user account that owns the GoAnywhere Gateway installation directory and its contents. This is typically the same user account used to start and stop GoAnywhere Gateway.
3. Shut down GoAnywhere Gateway.
4. Navigate to the installation directory. For example, /usr/local/HelpSystems/GoAnywhere Gateway.

5. Rename the old 'jre' folder to 'jre.old'. In some cases, this folder might be called 'jre6'. If so, rename this file to 'jre6.old'. If both 'jre' and 'jre6' folders exist, rename both folders.
6. Create a new 'jre' folder in the installation directory and copy the downloaded JRE bundle into that directory.
7. Extract the contents of the JRE bundle into the current directory.
    - $ gunzip linux-x64-1.8.0_192_zulu.tar.gz
    - $ tar -xvf linux-x64-1.8.0_192_zulu.tar

The following image illustrates the resulting folder structure in the installation directory:

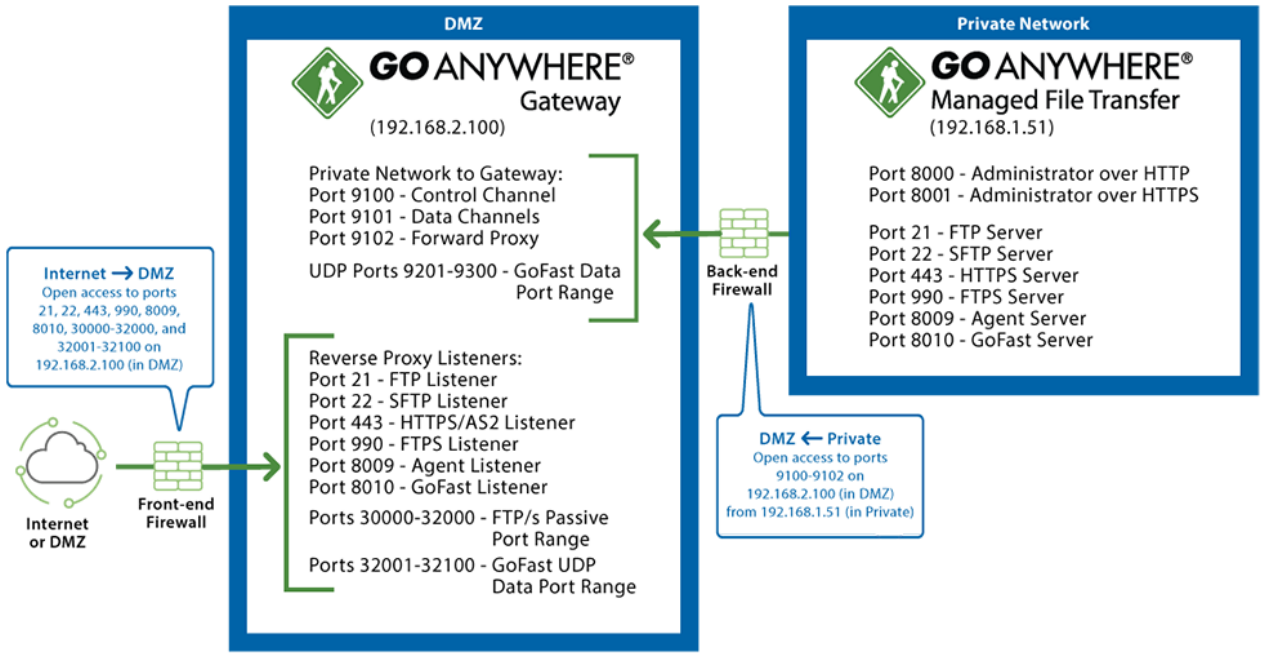


8. Start GoAnywhere Gateway.
9. Verify Java has been upgraded to Java 8 or later by running the `./gagateway jvmconfig` command.

Firewall Configuration

In order to provide protection for sensitive files and the private (internal) network, GoAnywhere Gateway should be installed in the DMZ and GoAnywhere MFT should be installed in the private network. The front-end and back-end firewalls should be configured to open only specific port numbers to the products.

> **NOTE:**
> The diagram below shows the firewall settings if the default port numbers were used in GoAnywhere Gateway and GoAnywhere MFT. The IP addresses shown are for demonstration purposes only.



Front-end Firewall Configuration

The standard port numbers for the desired file transfer protocols that need to be opened through the front-end firewall to GoAnywhere Gateway in the DMZ:

- **21** - FTP
- **22** - SFTP
- **443** - HTTPS
- **990** - FTPS
- **8009** - Agents
- **8010** - GoFast
- **30000-32000** - Must be opened to support passive mode for FTP or FTPS
- **32001 - 32100** - GoFast UDP data ports

Back-end Firewall Configuration

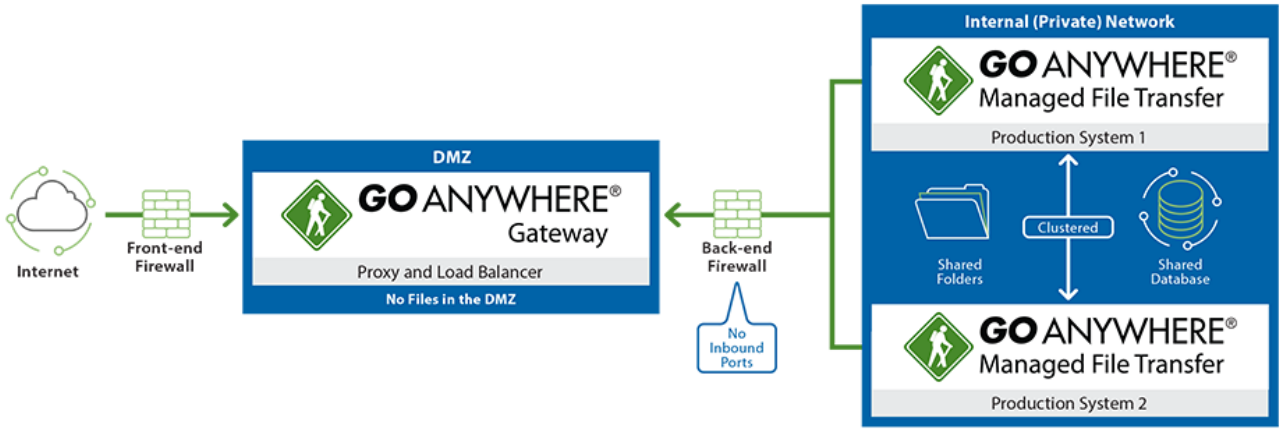
In order to establish control and data channels from GoAnywhere MFT to GoAnywhere Gateway, the following ports must be opened through the back-end firewall from the Private Network to GoAnywhere Gateway in the DMZ:

- **9100** - GoAnywhere MFT outbound connection to the GoAnywhere Gateway control connection listener. This is used for the persistent control connection between GoAnywhere MFT and GoAnywhere Gateway.
- **9101** - GoAnywhere MFT outbound data connection that is used to handle client connections from the protocol listeners (FTP, SFTP, HTTPS, FTPS, AS2, GoFast) in GoAnywhere MFT. A connection is made from GoAnywhere MFT to this port for each client connection.
- **9102** - Used for the Forward Proxy services.
- **9201-9300** - The UDP GoFast data port range.

Load Balancing

GoAnywhere Gateway can serve as a load balancer for distributing workloads across multiple GoAnywhere MFT installations within a cluster. This active-active framework provides greater high availability for mission-critical environments.

> **NOTE:**
> Load Balancing is a licensed feature for GoAnywhere Gateway. Contact HelpSystems for licensing information.



As a load balancer, GoAnywhere Gateway spreads connections evenly across the clustered systems. This load balancing algorithm is called “round-robin”, which is a common load balancing standard.

FTP, FTPS, SFTP, and GoFast are stateful protocols and use the round robin algorithm to load balance connections across the systems in the cluster.

HTTP/S is a stateless protocol which also uses the round robin algorithm, however it needs to persist each connection (for a period of time) to the same HTTP/S server in order to maintain the integrity of the session. This is important because the user’s HTTP/S session is typically only able to be serviced by a single HTTP/S server at a time.

Similarly to HTTP/S, the Agent load balancer rule also uses the round robin algorithm with session persistence, but the session persistence is removed once all connections from that IP address are closed.

The configuration settings for the round-robin load balancing rules must be specified in the gateway.xml file (found in the `[install_directory]/config` folder).

- For new installations, the gateway.xml file already has the rules provided for load balancing with GoAnywhere MFT in a clustered environment.

- Prior installations of GoAnywhere Gateway that upgrade to version 2.0.0 or later will need to add the Load Balancing rules to the gateway.xml file (if you are licensed to use this feature).
- Agent Load Balancing Rules must be added to the gateway.xml file if you upgrade to version 2.4.0 or later (and you are licensed to use Agents).

The configuration options for the Load Balancing rules are detailed in the Server Configuration section.

GoAnywhere Gateway Configuration

GoAnywhere Gateway's configuration can be customized by editing the configuration files located in [install_directory]/config. The files in this directory are XML files, which can be edited with any text or XML editor. Listed below are the two configuration files that can be edited:

gateway.xml - contains the basic configuration options such as the IP addresses and port number that GoAnywhere Gateway should use. Advanced security options (found in the next section) can be configured.

log4j2.xml - contains the options for customizing the logs generated by GoAnywhere Gateway. With this configuration file, you can control the level of logging, redirect the logs to a Syslog server, etc.

Server Configuration

To configure the GoAnywhere Gateway server, open the `gateway.xml` file located in the `[install_directory]/config` directory using a text or XML editor.

Listed below are the attributes that can be updated:

Attribute Name	Description
controllerAddress	The local IP address on which GoAnywhere Gateway should listen for Control Connections from GoAnywhere MFT. Be sure this IP address is reachable from the system where GoAnywhere MFT is installed.
controllerPort	The port number on which GoAnywhere Gateway should listen for Control Connections from GoAnywhere MFT. The default port number is 9100. Be sure this port is open for outbound connections on the firewall protecting the private network.
dataAddress	The local IP address on which GoAnywhere Gateway should listen for Data Connections from GoAnywhere MFT. When an external client connects to the GoAnywhere Gateway, GoAnywhere MFT opens a data connection which attaches to the desired service. The IP address specified here should be accessible from the system where GoAnywhere MFT is installed.

Attribute Name	Description
dataNATAddress	The IP Address that GoAnywhere MFT should connect to when establishing a data connection with GoAnywhere Gateway. GoAnywhere Gateway will send this address to GoAnywhere MFT when a new client connects. This should be used only if connections from GoAnywhere MFT to GoAnywhere Gateway are routed through a NAT firewall.
dataPort	The port number on which GoAnywhere Gateway should listen for Data Connections from GoAnywhere MFT. The default port number is 9101. Be sure to open this port for outbound connections on the firewall protecting the private network.
dataNATPort	The port number GoAnywhere Gateway will direct GoAnywhere MFT to connect to when establishing a data connection. This should be used only if connections from GoAnywhere MFT to GoAnywhere Gateway are routed through a NAT firewall.
forwardProxyLocalAddress	The local IP address GoAnywhere Gateway will use when active data connections are requested. This address is also used to establish outbound connections to remote servers when GoAnywhere Gateway is used as a forward proxy. The value should be the local IP you wish to have used when establishing an outbound connection from the GoAnywhere Gateway server.

Attribute Name	Description
proxyAddress	The local IP address on which the Outbound Proxy component of GoAnywhere Gateway should listen for incoming requests. The Outbound Proxy works similar to a SOCKS Proxy, which accepts CONNECT and BIND requests from clients. A CONNECT request is used to connect out to another system on the Internet, whereas the BIND request is used to temporarily listen on a port for accepting incoming connections from a system on the Internet. The Outbound Proxy is used by the FTP and FTPS services in GoAnywhere MFT to facilitate routing of passive and active data connections through the GoAnywhere Gateway. When an external FTP client requests a data connection in passive mode, the FTP service sends a BIND request to the Outbound Proxy. GoAnywhere Gateway then listens on a temporary port for the incoming connection. After accepting the connection, any data is routed to the intended destination. When an external FTP client requests an active data connection, the FTP service sends a CONNECT request to the Outbound Proxy specifying the IP address and port it should connect to. Once the connection is established, any data will be routed to the intended destination. The Outbound Proxy can also be used by GoAnywhere MFT when using the FTP, FTPS, SFTP and SCP protocols.

Attribute Name	Description
proxyNATAddress	The IP Address that GoAnywhere MFT should connect back to when establishing an FTP Active or Passive data connection through GoAnywhere Gateway. GoAnywhere Gateway will send this address to GoAnywhere MFT during the initial handshake, and GoAnywhere MFT will connect to this address when an FTP/S client requests an Active or Passive data connection (see proxyAddress). This should be used only if you are supporting FTP/S Active or Passive data connections in GoAnywhere MFT, and if all connections from GoAnywhere MFT to GoAnywhere Gateway are routed through a NAT firewall. This is not required when using *GoAnywhere Gateway* as a forward proxy from GoAnywhere MFT.
proxyPort	The port number on which the Outbound Proxy component of GoAnywhere Gateway should listen for incoming connections. The default port number is 9102. Be sure to open this port for outbound connections on the firewall protecting the private network.
proxyNATPort	The port number which GoAnywhere Gateway will direct GoAnywhere MFT to connect to when establishing an FTP Active or Passive data connection through GoAnywhere Gateway. GoAnywhere Gateway will send this port to GoAnywhere MFT during the initial handshake, and GoAnywhere MFT will connect to this port when an FTP/S client requests an Active or Passive data connection (see proxyPort). This should be used only if you are supporting FTP/S Active or Passive data connections in GoAnywhere MFT, and if all connections from GoAnywhere MFT to GoAnywhere Gateway are routed through a NAT firewall. This is not required when using GoAnywhere Gateway as a forward proxy from GoAnywhere MFT.
passiveProxyAddress	The local IP address on which the GoAnywhere Gateway should listen for incoming passive FTP data connections from external clients.
passiveProxyPortRangeFrom	The beginning port in the range of ports available for FTP passive data connections.
passiveProxyPortRangeTo	The ending port in the range of ports available for FTP passive data connections.

Attribute Name	Description
proxyEnabled	The outbound proxy component of GoAnywhere Gateway can be enabled or disabled.
sharedSecret	The Shared Secret is a password used to identify GoAnywhere MFT installation as an authorized client that is allowed to connect to GoAnywhere Gateway. If specified, the Shared Secret must also be configured in GoAnywhere MFT's Gateway Configuration page. Shared Secret is available in GoAnywhere MFT version 5.4 and higher. For more information about configuring the Shared Secret in GoAnywhere MFT, see the *GoAnywhere MFT User Guide*.
shutdownPort	The port number on which GoAnywhere Gateway should listen for shutdown requests. For security reasons, GoAnywhere Gateway binds the shutdown listener on the LOOPBACK address, thus ensuring shutdown requests are accepted only from the local host. The default port number is 9105.
minThreads	The minimum number of spare threads that GoAnywhere Gateway should always have available. The default value is 10.
maxThreads	The maximum number of threads that GoAnywhere Gateway is allowed to use. The default value is 2000.
threadKeepAlive	The number of seconds an unused thread would stay alive before it is discarded. The default value is 60 seconds.
udpEnabled	Enables the UDP data service for GoFast accelerated file transfers. Valid values are 'true' or 'false.'
udpInternalAddress	The IP address or host name of the internal UDP data server. This is where GoAnywhere MFT will connect to when sending out GoFast packets during data transfers.
udpInternalPortRangeFrom	UDP data ports are assigned dynamically for each file transfer. This is the low end UDP data port number for the range of UDP ports used for GoFast file transfers. The default is 9201.
udpInternalRangeTo	The high end UDP data port number for GoFast file transfers. The default is 9300.

Attribute Name	Description
udpExternalAddress	The IP address or host name of the external UDP data server. This is where GoFast clients will send UDP packets during GoFast data transfers.
udpExternalPortRangeFrom	UDP data ports are assigned dynamically for each file transfer. This is the low end UPD data port on the external GoFast server. The default is 32001.
udpExternalPortRangeTo	The high end UDP data port number for the external GoFast file server. The default is 32100.
udpTimeout	The number of seconds before the UDP ports close after no data is sent over them. The default is ten seconds.

* You can run the `./gagateway jvmconfig` command to view a list of available TLS protocols and cipher suites.

Enabling SSL Control Channel and/or SSL Termination

The following elements and attributes can be added to the `gateway.xml` file within the SSL element to enable and configure SSL on the control channel and/or SSL termination for proxy connections. For more information, see the *GoAnywhere MFT User Guide*.

privateKeyStore

The privateKeyStore element defines the location of the private keys used for control channel SSL and/or SSL termination. The following table lists the attributes for the privateKeyStore element.

Attribute Name	Description
path	The path to the Key Store on the GoAnywhere Gateway server that contains the Private Keys.
type	The Key Store type, either JKS, BCFKS, or PKCS12. The default is JKS.
password	The password to access the Key Store.

EXAMPLE:

```
<privateKeyStore path="C:\Users\kharris\gateway.p12" type="PKCS12"
password="Help1234">
```

control

The control element defines which key in the private keystore to use for SSL on the control channel as well as settings that apply to that connection. The control element must be added within the privateKeyStore element. The following table lists the attributes for the control element.

Attribute Name	Description
keyAlias	The key alias identifies the private key to use for SSL on the control channel.
keyPassword	The password for the private key. If this attribute is not defined, the privateKeyStore password will be used.
protocol	The SSL protocol to use for the control channel.
enabledProtocols	A list of comma separated SSL protocols.
enabledCipherSuites	A list of comma separated cipher suites.

EXAMPLE:
<control keyAlias="controlssl" keyPassword="Help5678" protocol="TLS" enabledProtocols="TLSv1,TLSv1.1,TLSv1.2" enabledCipherSuites="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256"/>

termination

The termination element defines which key in the private keystore to use for SSL termination as well as other SSL settings. The termination element must be added within the privateKeyStore element. The following table lists the attributes for the termination element.

NOTE:
SSL termination on the Gateway does not support client certificate authentication.

NOTE:
It is recommended to only use SSL termination for HTTPS connections.

Attribute Name	Description
keyAlias	The key alias identifies the private key to use for SSL termination.
keyPassword	The password for the private key. If this attribute is not defined, the privateKeyStore password will be used.
protocol	The SSL protocol to use for SSL termination.
enabledProtocols	A list of comma separated SSL protocols.
enabledCipherSuites	A list of comma separated cipher suites.

EXAMPLE:
<termination keyAlias="gatewayssl" keyPassword="Help5678" protocol="TLS" enabledProtocols="TLSv1,TLSv1.1,TLSv1.2" enabledCipherSuites="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256"/>

trustKeyStore

If the proxy address is configured for SSL termination and SSL rewrap, this trust store is used to trust certificates from the service within GoAnywhere MFT. If this element is not defined, GoAnywhere Gateway will trust any certificate from the GoAnywhere MFT service. The following table lists the attributes for the trustKeyStore element.

Attribute Name	Description
path	The path to the Key Store that contains trusted certificates.
type	The Key Store type, either JKS, BCFKS, or PKCS12. The default is JKS.
password	The password to access the Key Store.

EXAMPLE:
<trustKeyStore path="C:\Users\kharris\Desktop\trustedKeys.jks" type="JKS" password="changeit"/>

Load Balancing Rules

The following attributes can be defined for each load balancing rule:

Rule

Attribute	Description
name	A unique name that identifies the load balancer rule. The GoAnywhere Gateway configuration specified in GoAnywhere MFT will use this name when defining the load balancing option for a particular service. Use the recommended name of "default" for stateful protocols like FTP, FTPS, SFTP, & GoFast. Use the name "https" for stateless protocols like HTTP/S, and "agents" for GoAnywhere Agents.

NOTE:
The Load Balancing Rule must be specified on the Gateway Configuration page in GoAnywhere MFT.

Load Balancer

Attribute	Description
algorithm	The load balancer algorithm to use for the rule. The supported algorithm is "roundrobin".

Session Persistence

Attribute	Description
type	For stateless protocols, like HTTPS, sessions must be persisted based on IP addresses. The valid value is "ip". For agents, sessions must be removed once all connections from that IP address are closed. The valid value is "agentip".
timeout	When using Session Persistence, this setting determines the expiration of a persisted session. This time is specified in seconds and should be equal to or greater than the session timeout specified for the HTTPS service in GoAnywhere MFT. Connections received from the same IP address before the timeout will be routed to the same GoAnywhere MFT system as the previous connection. The timeout is also reset each time a connection is made from the same IP address. The "agent" load balancer rule does not use a timeout value.

GoAnywhere Gateway must be restarted for any changes to take effect. If the controllerAddress or controllerPort have changed, all instances of GoAnywhere MFT that are setup to use this gateway must also be updated, and the connection to GoAnywhere Gateway must be restarted.

Sample gateway.xml Configuration

Listed below are the contents of a sample server configuration file for GoAnywhere Gateway.

```
<?xml version="1.0" encoding="UTF-8"?>
       <gateway controllerAddress="192.168.1.212"
       controllerPort="9100" dataAddress="192.168.1.212"
       dataPort="9101" shutdownPort="9105"
       proxyEnabled="true"proxyAddress="192.168.1.212"
       proxyPort="9102"
       passiveProxyAddress="192.168.1.212"
       passiveProxyPortRangeFrom="30000"
       passiveProxyPortRangeTo="32000"
       forwardProxyLocalAddress="192.168.1.212"
       sharedSecret="goanywhere"
       udpEnabled="false"
       udpInternalAddress="192.168.1.212"
       udpInternalPortRangeFrom="9201"
       udpInternalPortRangeTo="9300"
       udpExternalAddress="192.168.1.212"
       udpExternalPortRangeFrom="32001"
       udpExternalPortRangeTo="32100"
       minThreads="10" maxThreads="2000" threadKeepAlive="60">
       <ssl>
       <privateKeyStore path="C:\Users\kharris\gateway.p12"
       type="PKCS12" password="Help1234">
       <control keyAlias="controlssl" keyPassword="Help5678"
       protocol="TLS" enabledProtocols="TLSv1.2"
       enabledCipherSuites="TLS_RSA_WITH_AES_256_CBC_SHA"/>
       <termination keyAlias="gatewayssl"
       keyPassword="Help5678" protocol="TLS"
       enabledProtocols="TLSv1.2"
       enabledCipherSuites="TLS_RSA_WITH_AES_256_CBC_SHA"/>
       </privateKeyStore>
       <trustKeyStore path="C:\Users\kharris\trustedKeys.jks"
       type="JKS" password="changeit"/>
       </ssl>
       <rules>
         <rule name="default">
          <loadBalancer algorithm="roundrobin" />
         </rule>
         <rule name="https">
           <loadBalancer algorithm="roundrobin">
               <sessionPersistence type="ip"
               timeout="300" />
           </loadBalancer>
          </rule>
          <rule name="agent">
           <loadBalancer algorithm="roundrobin">
```

```
                <sessionPersistence type="agentip">
            </loadBalancer>
          </rule>
        </rules>
</gateway>
```

Logging Configuration

The logging configuration can be updated by editing the `log4j2.xml` file located in the `[install_directory]/config` directory. By default, logs are written to a file named `gagateway.log`, located in the `[install_directory]/logs` directory. GoAnywhere Gateway can also send messages to an enterprise Syslog server. To change the file logging settings, edit one or more parameters in the "appender" section of the default configuration below that is colored green. Listed below are the various parameters and their descriptions:

Element Name	Attribute Name	Description
RollingFile	fileName	The file to which logs are written. The value can either be an absolute path or relative to the installation directory. Escape any backslashes used in the path by adding another backslash (e.g. C:\\logs\\gagateway.log).
RollingFile	filePattern	The file pattern to use when archiving logs after they've reached the size limit. The value can either be an absolute path or relative to the installation directory. The variable reference '%i' can be used in the pattern to indicate the index of the archived log file. Escape any backslashes used in the path by adding another backslash (e.g. C:\\logs\\gagateway.log).
SizeBasedTriggeringPolicy	size	The maximum size that the log file is allowed to reach before being rolled over to backup files. The value must be a whole number, followed by KB, MB or GB to represent Kilobytes, Megabytes and Gigabytes respectively.

Element Name	Attribute Name	Description
DefaultRolloverStrategy	max	The maximum number of retained backup files. When the backup files reach the specified limit, the oldest backup is deleted. The value must be a whole number. If set to zero, no backup files are created.

Syslog Logging Configuration

By default Syslog logging is disabled. You can enable Syslog logging by uncommenting the sections in blue. To uncomment, remove the `<!--` and `-->` around the blue sections. Listed below are the various parameters that can be adjusted for Syslog logging:

Element Name	Attribute Name	Description
Syslog	protocol	The protocol used for dispatching log messages to the Syslog server. Valid values are - UDP and TCP.
Syslog	host	The host name or IP address of the Syslog server.
Syslog	port	The port number on which the Syslog server is listening for incoming connections and/or log events. The Port value must be a number between 1 and 65535.
Syslog	facility	The Syslog facility name to which messages are logged. Valid values are - KERN, USER, MAIL, DAEMON, AUTH, SYSLOG, LPR, NEWS, UUCP, CRON, AUTHPRIV, FTP, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6 and LOCAL7.
Syslog	appName	The application ID you would like to assign to the messages that are sent to the Syslog server. The default value is gagateway.
Syslog	charset	Specify the character set to use for encoding the log messages. The default value is UTF-8, which works well for all character data.

Log Level Configuration

The type of messages logged by GoAnywhere Gateway can be adjusted by changing the log level. The default log level is `info`, which logs important informational messages along with any warnings and errors. The supported log levels are:

- **Error** - Logs only the error messages
- **Warn** - Logs all errors and warning messages
- **Info** - Logs all errors, warnings and important informational messages
- **Debug** - Logs all above messages along with additional debug level messages
- **Trace** - Logs all above messages along with the tracing of data that is sent or received

To change the log level, update the line `<Logger name="com.linoma.gag" level="info" additivity="false">` to the desired level. Setting the level to `Debug` or `Trace` may degrade the performance of GoAnywhere Gateway under high load.

> **NOTE:**
> Changes made to the configuration file requires restarting of GoAnywhere Gateway to take effect.

Default log4j2.xml Configuration

Listed below are the contents of the logging configuration file that is shipped with GoAnywhere Gateway. Please note that the comments in the file are excluded. The sections colored in green are used for file logging, whereas the sections in blue are used for Syslog logging. Syslog logging is disabled by default.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE log4j2:configuration SYSTEM "log4j2.dtd">
<log4j2:configuration
xmlns:log4j2="http://jakarta.apache.org/log4j2/" debug="false">

<RollingFile name="FileAppender" fileName="logs/gagateway.log"
filePattern="logs/gagateway.log.%i">
    <Policies>
           <SizeBasedTriggeringPolicy size="5 MB"/>
    </Policies>>
    <DefaultRolloverStrategy fileIndex="min" min="1" max="10" />
    <PatternLayout>
           <Pattern>%d{yyyy-MM-dd hh:mm:ss a} %-5p %m%n</Pattern>

    </PatternLayout>
</RollingFile>

<!--
<Syslog name="SyslogAppender" host="localhost" port="514"
protocol="UDP"
       facility="user" appName="gagateway" charset="UTF-8">
       <PatternLayout>
            <Pattern>%-5p %m</Pattern>
       </PatternLayout>
       </Syslog>
       -->
```

```
<Logger name="com.linoma.gag" level="info" additivity="false">
       <AppenderRef ref="FileAppender" />
       <!-- <AppenderRef ref="ConsoleAppender" /> -->
       <!-- <AppenderRef ref="SyslogAppender" /> -->
       </logger>
```

```
<Root level="error">

       <AppenderRef ref="FileAppender" />
       <!-- <AppenderRef ref="ConsoleAppender" /> -->
       <!-- <AppenderRef ref="SyslogAppender" /> -->

</Root>
```

Backup and Recovery

GoAnywhere Gateway can be backed up or configured on another system for failover purposes.

Backup and Recovery

GoAnywhere Gateway does not have a built-in backup function, so you will need to use a separate tool to make a copy of the necessary files.

The only files for GoAnywhere Gateway requiring a backup are the configuration files located in **[Install Directory]/config**. Additionally, the log files, located in **[Install Directory]/config** can be archived for historical purposes.

In the event of a disaster, GoAnywhere Gateway can be recovered by performing a clean install on a new server and restoring the archived configuration files. If the IP address on the restored machine is different than the original machine, you will need to update the Address fields in the restored **[Install Directory]/config/gateway.xml** configuration file to the new IP address. Additionally, the Service Mappings on the Gateway Manager page within GoAnywhere MFT will need to be updated to the new address.

A new license file is required when restoring GoAnywhere Gateway on a new machine.

Failover

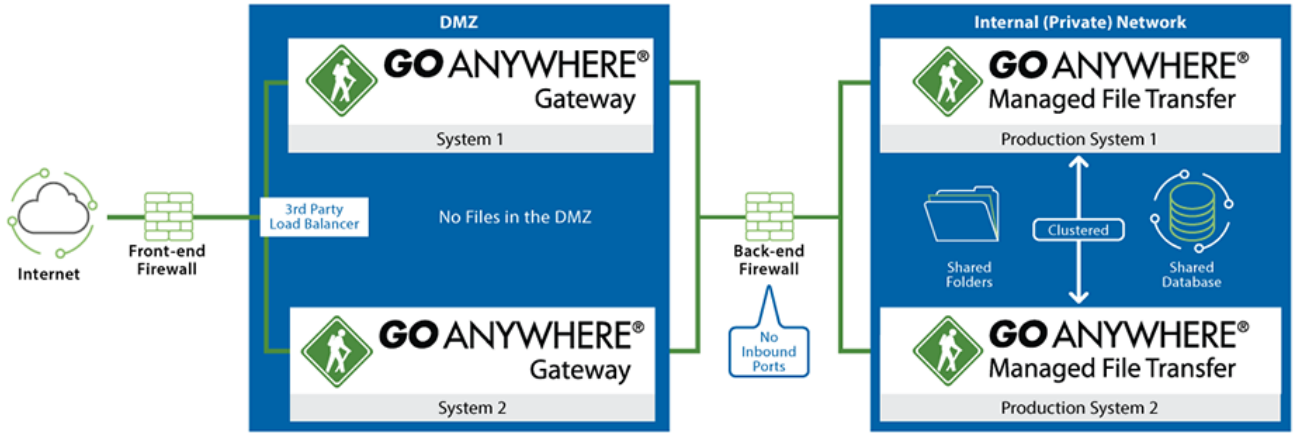
Follow the steps to set up a failover copy of GoAnywhere Gateway:

1. Install GoAnywhere Gateway onto the failover machine using one of the regular installation methods (depending on your OS) outlined earlier in this manual.
2. Get a license key from HelpSystems for the failover machine and install it.
3. Test the GoAnywhere Gateway installation on the failover machine to make sure it works properly.

4. Shut down the GoAnywhere Gateway subsystem/service on the failover machine, since GoAnywhere Gateway should not be running on both the production and failover machines at the same time.

GoAnywhere Gateway and High Availability

GoAnywhere MFT can be clustered with two or more servers and Gateway proxies for high availability. In the example below, a 3rd party load balancer is sending inbound connections across two GoAnywhere Gateways, which are installed in the DMZ, and no inbound ports are opened to the Private Network. Each GoAnywhere MFT node in the cluster is configured to use each Gateway.



GoAnywhere MFT Configuration

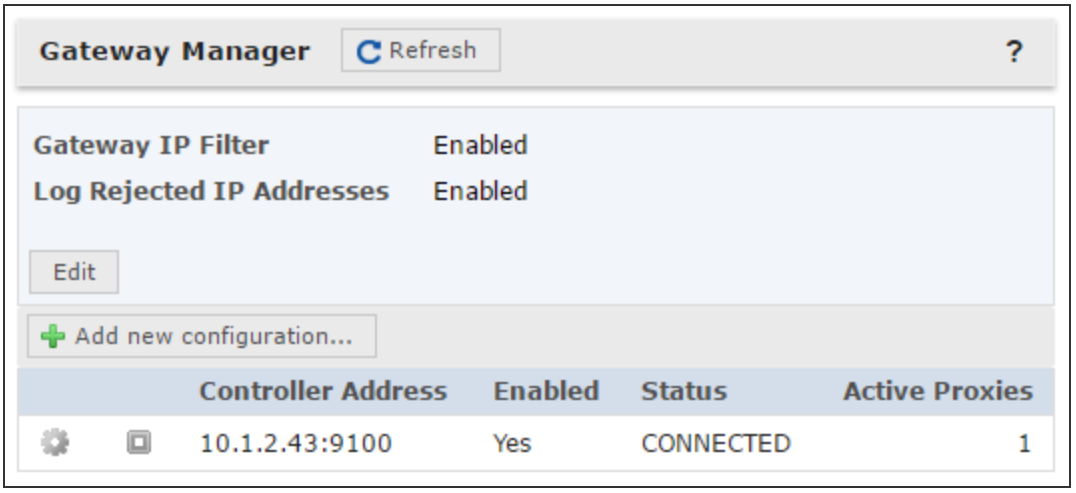
Once GoAnywhere Gateway IP addresses, port numbers, and optional SSL settings have been configured, GoAnywhere MFT must be configured with service mappings that will be used for connections with Gateway.

Gateway Manager

The Gateway Manager in GoAnywhere MFT provides the ability to control the GoAnywhere Gateway connection and view the current status of the GoAnywhere Gateway. When GoAnywhere Gateway is running in a cluster configuration, the service mappings for each system in the cluster are displayed in the Gateway manager.

To manage the GoAnywhere Gateway, log in to GoAnywhere MFT as an Admin User with the **Product Administrator** role.

From the main menu bar, select **Services** and then click the **Gateway Manager** link.



Page Toolbar

The following actions are available from the page toolbar:

- **Refresh** the page.
- Add a new Gateway configuration by clicking the **Add new configuration** link.
- Disable a Gateway connection by clicking the **Disconnect Gateway** icon. Click the **Connect Gateway** icon to reestablish a connection. The status field displays the current connection status. View the Gateway Details for more connection information.

> **NOTE:**
> If a connection is established, but GoAnywhere Gateway is unable to start a proxy listener, a warning icon will appear next to the proxy in the **Active Proxies** column. When this occurs, click the **Actions** icon and select **View** to view error details.

Gateway IP Filter and Log Rejected IP Address

Click the **Edit** button to configure the Gateway IP Filter and Rejected IP Address Log.

- **Gateway IP Filter** - When enabled on GoAnywhere Gateway versions 2.3 and later, the GoAnywhere MFT server sends the stored IP Filter entries to GoAnywhere Gateway. Gateway will then filter client connections based on the IP Filter Whitelist and Blacklist managed by GoAnywhere.
- **Log Rejected IP Address** - When enabled, GoAnywhere Gateway will log rejected IP addresses in the Gateway log file on the Gateway installation.

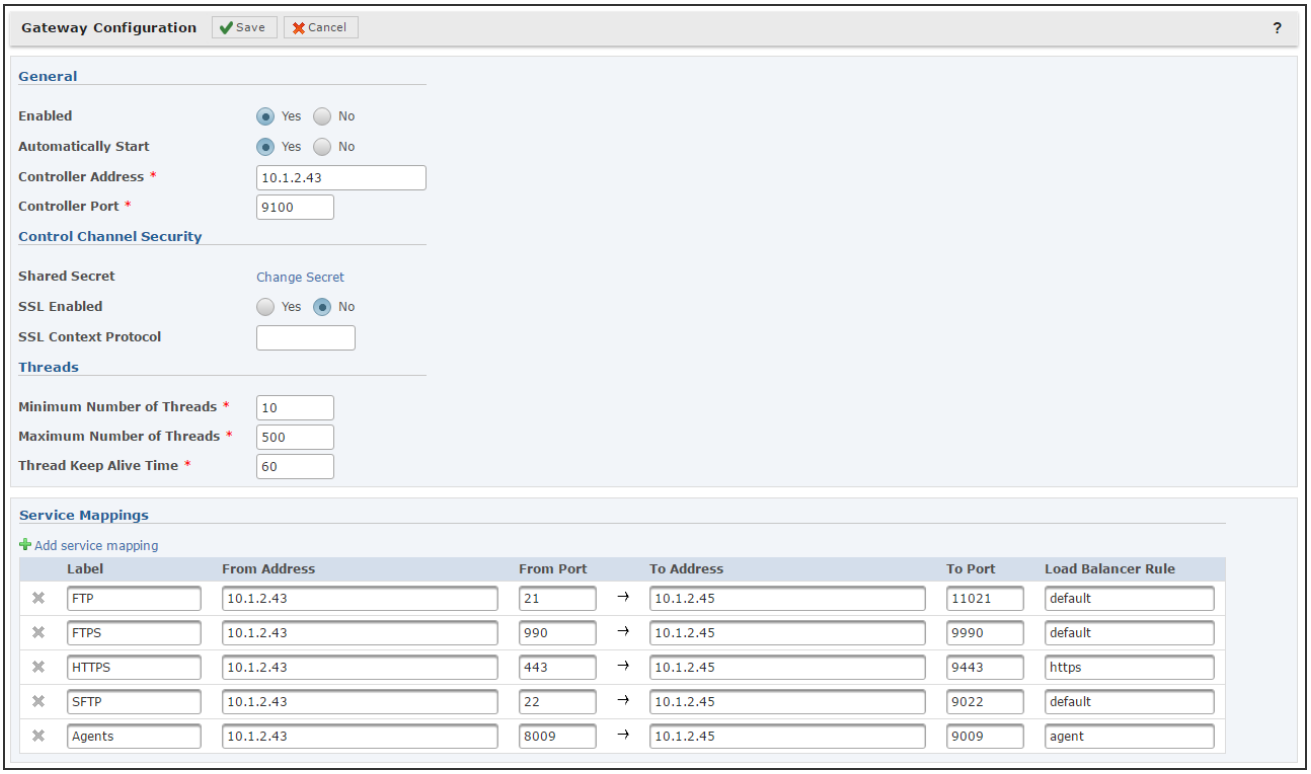
Gateway Manager Actions

The following actions are available by selecting the **Actions** icon:

- View Gateway Details by clicking the **View** icon.
- Edit a Gateway by clicking the **Edit** icon (the Gateway must be disabled to edit the configuration).
- Delete a Gateway by clicking the **Delete** icon (the Gateway must be disabled to delete the configuration).
- Copy a Gateway by clicking the **Copy** icon.

Gateway Configuration

The Gateway Configuration page contains the operating parameters, service mappings, and control channel security for GoAnywhere Gateway.



General

Enabled

GoAnywhere Gateway can be enabled or disabled. By default, GoAnywhere Gateway is disabled.

Automatically Start

Specify if you would like to start the GoAnywhere Gateway connection automatically when GoAnywhere MFT starts.

Controller Address

The Controller Address is the IP address of the server running GoAnywhere Gateway. This address must match the controller address defined in the gateway.xml file.

Controller Port

This is the port on which GoAnywhere Gateway listens for incoming control connections. The default port is 9100 and must match the port defined in the gateway.xml file.

Control Channel Security

Shared Secret

GoAnywhere Gateway version 2.3 or later can require GoAnywhere MFT to provide a password (the Shared Secret) to ensure unwanted GoAnywhere MFT installations can not make connections to the Gateway installation. Specify a password that is supplied to GoAnywhere Gateway when a connection is established. The Shared Secret must also be configured in the gateway.xml file on the

secured Gateway installation. To update an existing Shared Secret, click the **Change Shared Secret** link and specify a new shared secret.

SSL Enabled

When enabled, the proprietary control channel between GoAnywhere MFT and GoAnywhere Gateway is secured using SSL. The gateway.xml file must be configured to use SSL.

SSL Context Protocol

Specify the protocol to use when creating the SSL Context. The value you need to specify here depends on the security providers you have installed in the JRE (Java Runtime Environment). If left blank, the default value is TLS.

Threads

Minimum Number of Threads

The minimum number of threads reserved for connections to GoAnywhere Gateway. The default is 10 threads.

Maximum Number of Threads

The maximum number of threads that can be used for connections to GoAnywhere Gateway. This determines the maximum number of simultaneous requests that can be handled. The default is 2000 threads.

> **NOTE:**
> Changing the thread values can alter performance. Too few Maximum Threads and transfers will fail, but too many threads may limit performance of other applications on the same server. Modify these values to obtain the optimal performance for your configuration requirements.

Thread Keep Alive Time

The amount of time (in seconds), that an idle thread will wait before it is released. The default is 60 seconds.

> **NOTE:**
> Increasing this value will likely cause higher CPU and memory usage on the GoAnywhere MFT server. However, connections will start faster since they will not need to create new threads as frequently.

Service Mappings

Each Service (FTP, FTPS, HTTPS, and SFTP), is mapped from GoAnywhere Gateway to the corresponding service in GoAnywhere MFT. When a control connection is established, these mappings are sent to the GoAnywhere Gateway server. GoAnywhere Gateway listens for incoming connections on the "From Address" and "From Port" for each service mapping. When a connection occurs, GoAnywhere Gateway forwards the traffic to GoAnywhere MFT based on the "To Address" and "To Port" service mappings.

If more Service Mappings are needed (for example, more than one listener for a particular service), click the **Add service mapping...** link to add a new Service Mapping entry row. If a Service Mapping is no longer needed, click the **Delete** icon to delete the corresponding Service Mapping.

Label

An identifier for the service mapping.

From Address

The IP address that GoAnywhere Gateway will use to listen on for incoming traffic. Optionally leave the From Address field blank to listen for client connections on the same address as the defined Controller Address.

From Port

The port that GoAnywhere Gateway will use to listen on for incoming connections. The standard ports are 21 for FTP, 990 for FTPS, 22 for SFTP and 443 for HTTPS/AS2.

To Address

The IP address of the local GoAnywhere MFT system.

To Port

The port that the service listener is using for the particular service on the GoAnywhere MFT system.

Load Balancer Rule

The Load Balancer Rule is used by GoAnywhere Gateway to configure the load balancing for each service mapping. This rule is defined in GoAnywhere Gateway and should be round-robin for FTP, FTPS and SFTP protocols. For HTTPS, the Load Balancer is also round-robin, but is configured to use IP based session persistence for stateless HTTPS connections. The agent option also uses round-robin with IP address session persistence, but the session persistence is removed once all connections from that IP address are closed. By default, the following rules are defined in GoAnywhere Gateway.

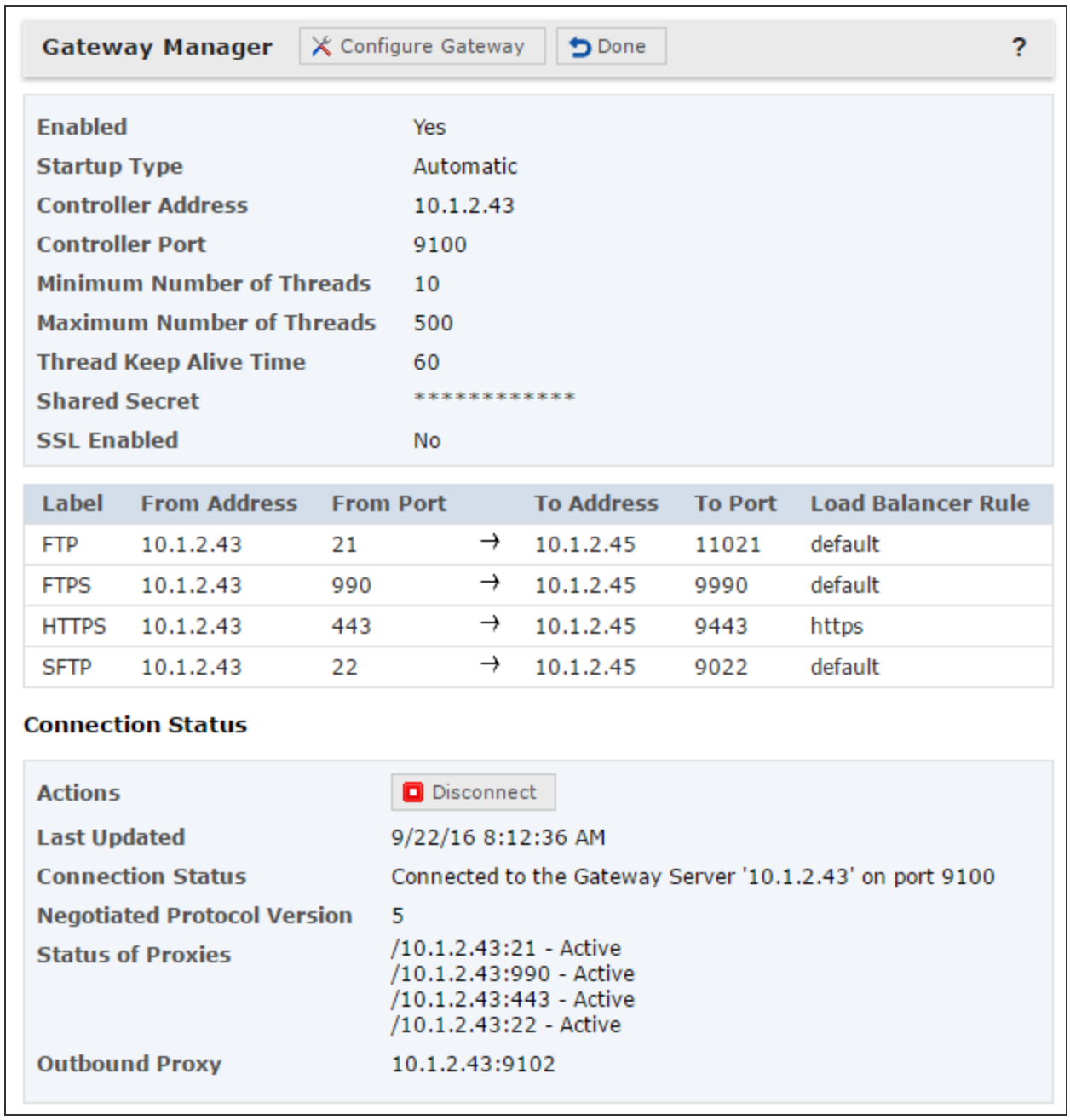
- **default** - This rule should be used for FTP, FTPS, SFTP, and GoFast.
- **https** - This rule should be used for HTTPS and AS2.
- **agent** - This rule should be used for Agents.

> **NOTE:**
> AS2 (S/MIME over HTTP(S)) uses the HTTPS Service.

> **NOTE:**
> Changes made to the Service Mappings will take effect the next time the connection to the *GoAnywhere Gateway* is reset. To reset the connection, click the **Disconnect** button and then the **Connect** button on the Gateway Manager page.

Gateway Details

The view Gateway Manager page in GoAnywhere MFT displays the current details for the selected Gateway connection. Click the **Done** button to return to the Gateway Manager.



Available Options

- Configure the GoAnywhere Gateway settings by clicking the **Configure Gateway** link in the page toolbar.
- Control the connection to the GoAnywhere Gateway by clicking the Actions button. The button toggles based on the connection status.
  - **Disconnect** - Stops GoAnywhere Gateway and releases all proxies.
  - **Connect** - Starts GoAnywhere Gateway and establishes proxy connections.

Uninstalling GoAnywhere Gateway

This section describes how to uninstall the GoAnywhere Gateway product.

Windows uninstall instructions

Perform the following steps to uninstall GoAnywhere Gateway from Windows:

Step	Description
1	End the GoAnywhere Gateway service on the Windows system.
2	Browse to the installation directory of GoAnywhere Gateway. The default install directory is C:\Program Files\HelpSystems\GoAnywhere Gateway.
3	Run the file named uninstall.exe to uninstall the product.

Linux and Unix uninstall instructions

Perform the following steps to uninstall the GoAnywhere Gateway product from Linux:

Step	Description
1	Login to the Linux system as root and open a Terminal window.
2	Change the working directory to where GoAnywhere Gateway is installed (for example, **cd /usr/local/HelpSystems/GoAnywhere_Gateway**).
3	If your system supports systemd, stop the GoAnywhere Gateway product by executing the following command: **systemctl start gagatewayd** Otherwise, use **/etc/init.d/gagatewayd stop**
4	Uninstall the GoAnywhere Gateway product by executing the following shell script: **./uninstall.sh**

Glossary

[install_directory]

The directory where GoAnywhere Gateway is installed. The default installation directory on Windows is C:\Program Files\HelpSystems\GoAnywhere Gateway. The default location on Linux and Unix platforms depends on the OS configuration.

Backend firewall

A firewall facing the DMZ, which is configured to allow incoming traffic into certain IP/ports within the Private (internal) network.

Control Channel

A connection initiated by GoAnywhere MFT (running in the private network) to the GoAnywhere Gateway (running in the DMZ) to exchange proprietary messages.

Data Channel

A connection initiated by GoAnywhere MFT (running in the private network) to the GoAnywhere Gateway (running in the DMZ). When an external client connects to GoAnywhere Gateway's proxy listener, a Data Channel is opened to route the traffic from the external client to the target service.

DMZ (Demilitarized Zone)

In computer security, a DMZ, or demilitarized zone is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

Frontend Firewall

A firewall facing the public internet, which is configured to allow incoming traffic into certain IP/ports within the DMZ.

GoAnywhere MFT

GoAnywhere MFT is a Managed File Transfer solution which provides centralized control and auditing of file transfers and workflows for the enterprise. GoAnywhere MFT supports popular file transfer protocols including SFTP, SCP, FTP/s, HTTP/s, AS2, Web Services, SMTP, POP3 and IMAP. To learn more about GoAnywhere MFT, please visit www.GoAnywhere.com.

Thread

Threads are used to process multiple requests simultaneously within the application.