NetSupport Manager

Implementing and using the Connectivity Server

Summary

With the increased use of the internet, common questions asked by customers using NetSupport Manager are: "Can I connect to and remote control a machine behind a firewall?" and "Does NetSupport Manager work with Network Address Translation (NAT)?"

Both have been possible in previous versions of NetSupport Manager; however, to do so involved complex configurations of firewalls to allow incoming connections.

Now, NetSupport Manager includes a Connectivity Server (Gateway) component that will simplify the method of connection and remove the need for complex firewall configurations.

What is the NetSupport Connectivity Server?

The NetSupport Connectivity Server is a component in NetSupport Manager which provides a stable and secure method for connecting Clients and Controls via the internet using HTTP and delivers web-based remote control without the need for modifications to existing firewall configurations.

The Connectivity Server acts as a go-between for a NetSupport Control and NetSupport Client - and when using a Connectivity Server, there is no direct communication between the Client and Control.

When the NetSupport Client is configured to use the HTTP protocol, the Client connects to the Connectivity Server at startup. A user at a NetSupport Control can connect to the Gateway using the HTTP protocol and browse for connected Clients, then connect to any number of Clients that are attached to the Connectivity Server.

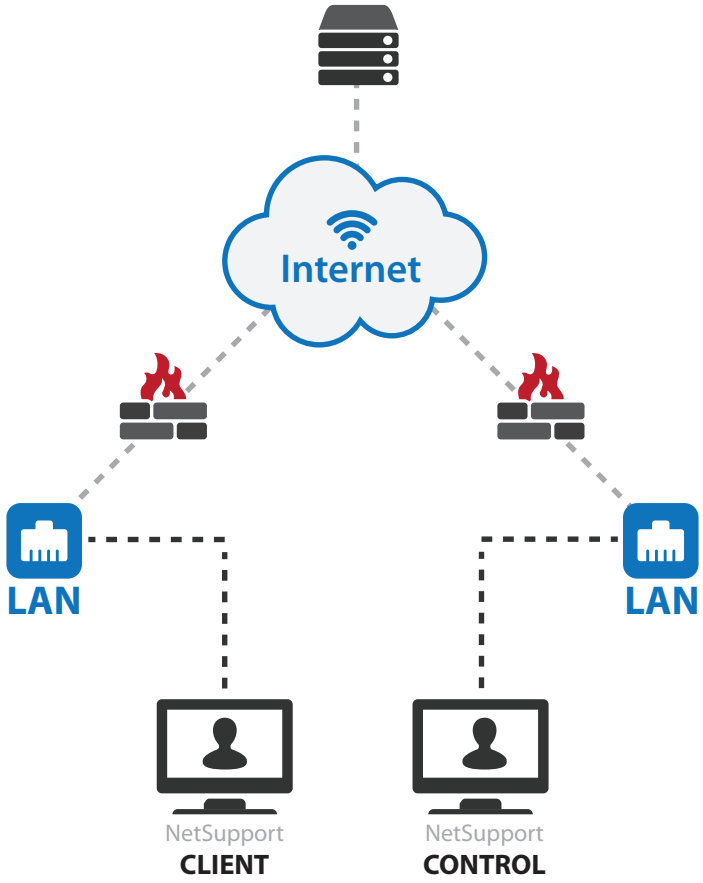
As there is no direct connection between the NetSupport Client and Control, and the protocol used is HTTP, it means that each of the machines can be situated behind a firewall configured to use NAT without the need to make configuration changes to the firewall.

In order for the Connectivity Server to connect a Client and Control, both the NetSupport Control and Client must be able to connect to the Connectivity Server using the HTTP protocol on the Connectivity Server's configured port (the default port is 443).

The Connectivity Server can be located in various network locations, as shown in the following scenarios.

A Secondary Connectivity Server can also be installed and Clients configured with the Secondary Connectivity Server information. This allows for Connectivity Server redundancy. When the Primary Connectivity Server is unavailable, the Clients automatically switch to using the Secondary Connectivity Server.

Once the Primary Connectivity Server is available, the Clients will switch back to the Primary Connectivity Server, and the Secondary Connectivity Server will go into standby mode again. This process does not disrupt any active remote control sessions that are in progress.



Scenario 1

NetSupport Connectivity Server on the public internet

In this scenario, the NetSupport Connectivity Server is installed on the public internet.

In this example, no configuration changes would normally need to be made to either of the firewalls. However, the machine that is running the NetSupport Connectivity Server is freely available on the internet and could be open to an attack.

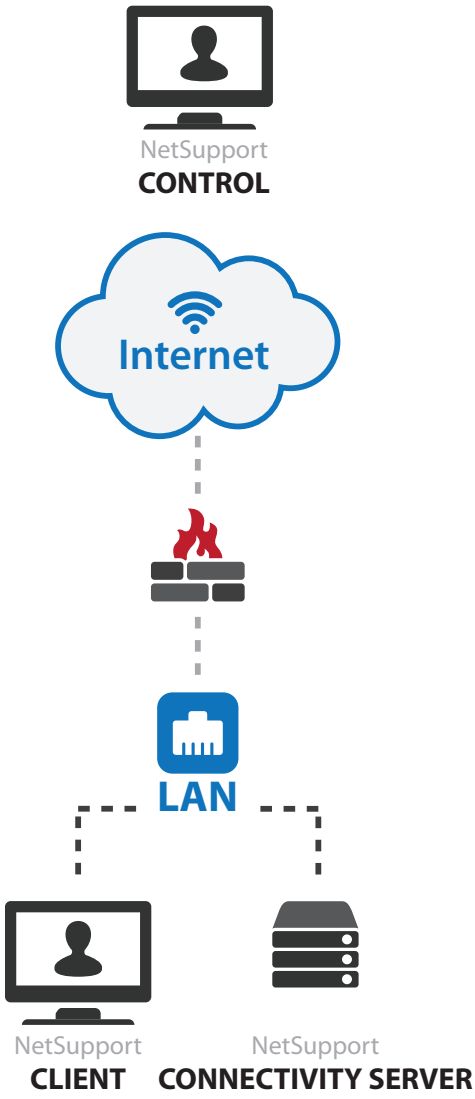
Scenario 2

NetSupport Connectivity Server on the NetSupport Client network with a NetSupport Control on the public internet

In this scenario, the firewall at the NetSupport Client site would need to be configured to allow incoming HTTP connections to the Connectivity Server (on the configured port number).

This would be similar to having a web server installed on the Client network and making it publicly available to users on the internet.

This example could be used to provide remote access to users working from home.



Scenario 3

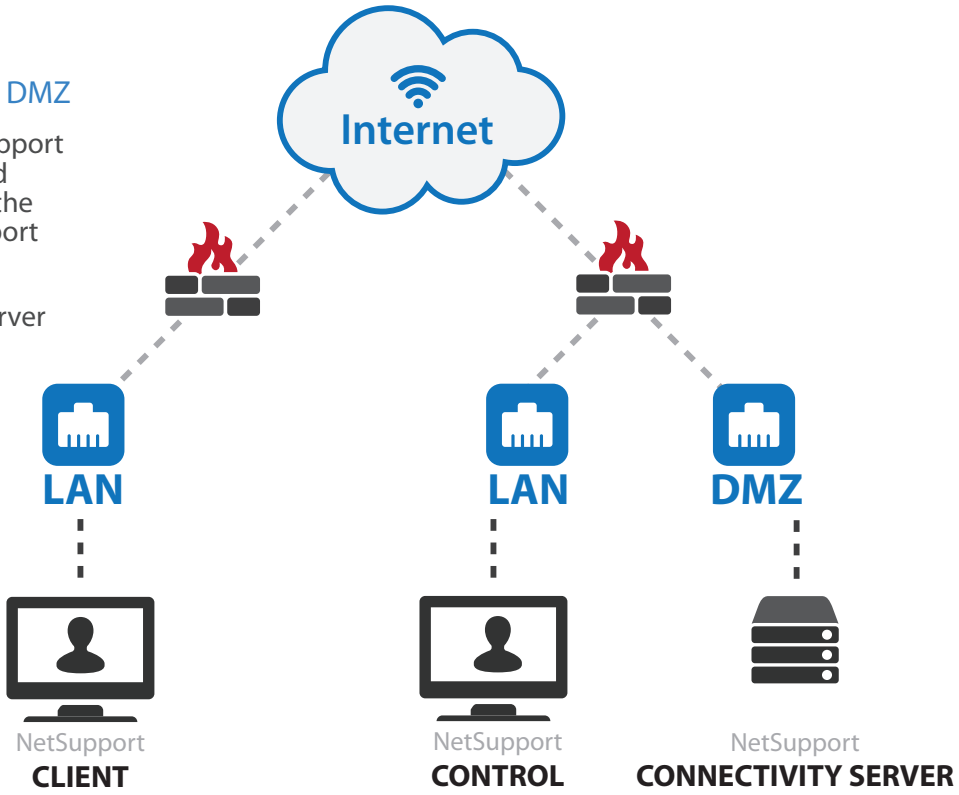
NetSupport Connectivity Server on a DMZ

In this scenario, the firewall at the NetSupport Control site would need to be configured to allow incoming HTTP connections to the Connectivity Server (on the configured port number).

This would be similar to having a web server installed on the DMZ and making it publicly available to users on the internet.

The advantage of this location for the Connectivity Server is that the machine running the Connectivity Server is now protected from external attack by a firewall.

However, this configuration does require some configuration changes to the firewall at the Control site.



Scenario 4

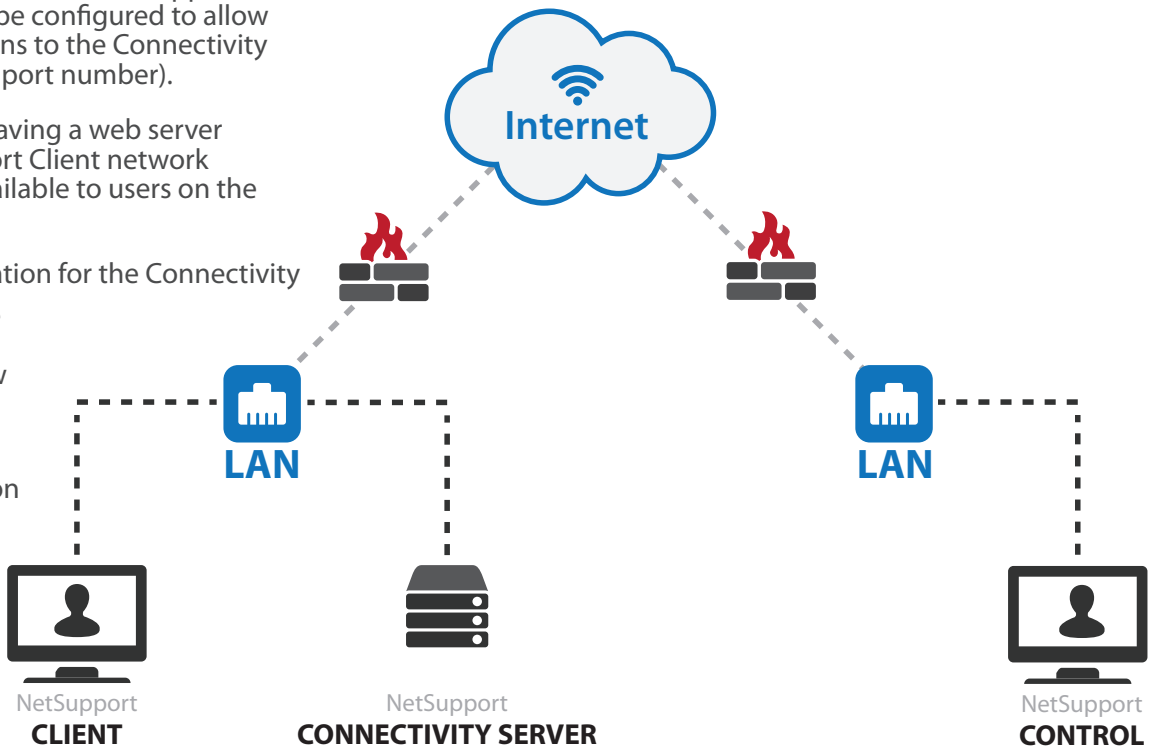
NetSupport Connectivity Server on the Client network

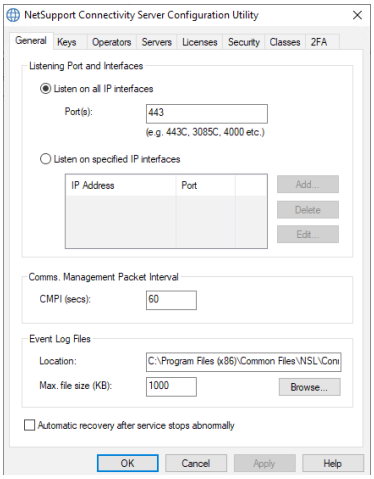
In this scenario, the firewall at the NetSupport Client site would need to be configured to allow incoming HTTP connections to the Connectivity Server (on the configured port number).

This would be similar to having a web server installed on the NetSupport Client network and making it publicly available to users on the internet.

The advantage of this location for the Connectivity Server is that the machine running the NetSupport Connectivity Server is now protected from external attack by a firewall.

However, this configuration does require some configuration changes to the firewall at the Client site.





Installing the NetSupport Connectivity Server

The NetSupport Connectivity Server can only be installed on the following operating systems (Windows 11, Windows 10, Windows 8, Windows 8.1, Windows 2008, Windows 2003, Windows Server 2012, 2019 and 2022) as it installs as a service.

The Connectivity Server is not installed by default. To install the NetSupport Connectivity Server, run the standard NetSupport installation package. When prompted for an installation type, choose **Custom**.

The next screen will display a list of components. From this list, select **Gateway** and continue through the installation.

At the end of the installation, the "NetSupport Connectivity Server Configuration Utility" will be displayed, as shown below:

General

Here, you can set the port number that the Connectivity Server will accept incoming connections on. The default port is 443, and this number is registered to NetSupport.

When installing the Connectivity Server onto a machine that already has Internet Information Services (IIS) installed, the port number must be changed from 443 to either 3085 (also registered to NetSupport) or another port number.

The default port for the HTTP protocol on the internet is port 80 and you can configure the Connectivity Server to accept connections on this. However, some Internet Service Providers (ISPs) utilise cache or proxy servers that cache HTTP traffic on port 80. If your ISP uses a cache or proxy server, then the Connectivity Server connections will fail.

The Connectivity Server can be configured to listen on specified IP interfaces or on all IP interfaces on the machine.

CMPI (Secs): When configured for Connectivity Server connections, the Client workstation confirms its availability by periodically polling the Connectivity Server. By default, a network packet is sent every 60 seconds, but you can change this if required.

You can also specify the location and maximum size of the Connectivity Server log file. The logging functions of the Connectivity Server are explained in detail later in this document.

Keys

You can add a Gateway key by selecting the Keys tab. Gateway keys are used to authenticate NetSupport Clients and Controls, therefore ensuring that unauthorised users cannot connect to and use the Connectivity Server.

You must set at least one Gateway key before you can apply the configuration, as the Connectivity Server will not accept any connections unless at least one Gateway key is configured.

Operators

The Operators tab allows you to restrict remote control access to a list of specified users. At the Control, a user will be required to configure a username and password in order to browse a Connectivity Server and connect to the Clients. You can also require users to use two-factor authentication to start a remote connection.

Servers

By default, this Connectivity Server will be set to be a standalone Primary Connectivity Server. You can set this Connectivity Server as a standalone Secondary Connectivity which will act as a backup if the Primary Connectivity Server is unavailable. Load Balancing Connectivity Servers can also be set up to spread the load of Clients across multiple servers.

Licenses

The Licenses tab displays all of the NetSupport licenses that have been applied to the Connectivity Server. The Status field shows if the license has been activated. If the license has not been activated, the **Activate** button can be used to initiate the activation process.

This activation process is either performed automatically over the internet or manually by contacting the NetSupport Technical Support team or the local reseller who can supply an activation code.

Security

From the Security tab, the option to **Enable encryption of communications to remote computers** is available. When enabled, all communication in the connection process over the Connectivity Server is encrypted.

Note: The remote computers (Controls and Clients) need to be running NetSupport Manager version 11.00.0005 or later to use the encryption option.

There is an additional option **Block any remote computers not using encrypted communications**. Enabling this option prevents earlier versions of the NetSupport Manager Client that do not support the enhanced level of encryption from connecting to the Connectivity Server.

To further enhance security, SSL/TLS certificates can be used. These also allow the Clients and the Controls to verify that the Connectivity Server they are connecting to is genuine. If you already have an SSL/TLS certificate, you can enter it here or allow the Connectivity Server to create and use a *Let's Encrypt* certificate.

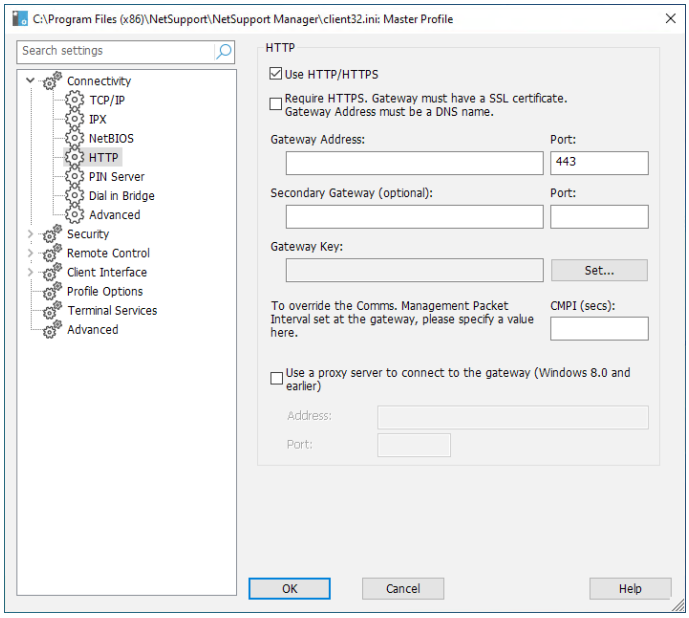
2FA

Two-factor authentication provides an extra layer of security when Control users connect to Clients on a Connectivity Server. NetSupport Manager supports time-based one-time password (TOTP) and Duo Push. From here, you can enter your TOTP or Duo details.

Configuring Clients to use the NetSupport Connectivity Server

To configure a Client to use the HTTP protocol, you will need to use the NetSupport Manager Client Configurator.

- Run the NetSupport Manager Configurator and select the **Advanced** option.
- Select **Connectivity** - **HTTP**.
- To enable HTTP, select the **Use HTTP/HTTPS** option.
- Enter the port number which the Connectivity Server you are going to use is configured for, the default is 443
- Enter the IP address of the Primary NetSupport Connectivity Server



- Enter the optional Secondary Connectivity Server IP address and port number and click **Set** to enter the Gateway key. The Gateway key entered must be identical to one of the Gateway keys added to the Connectivity Server.
- Enter the proxy server details if the Client is connecting to the internet via a proxy server.

Once the required configuration details have been entered, click **OK** to save the configuration and restart the NetSupport Client. The Client should then connect to the Connectivity Server.

The entire configuration for a NetSupport Client is stored in the client32u.ini configuration file. This file can be easily copied or deployed (using the NetSupport Manager Deploy tool) to other Client machines. For further details about NetSupport Manager Deploy, see the online help or the NetSupport Manager user manual.

Configuring the Control to use the NetSupport Connectivity Server

Before you can connect to a NetSupport Client using a NetSupport Connectivity Server, you must add the Connectivity Server to your Control Console. To do this, follow the steps below:

- Open the NetSupport Manager Control.
- In the left-hand pane, select the **Internet Gateways** folder.
- Double-click **Add a Gateway**.
- The Add a Gateway wizard will appear, enter the name and description and click **Next**. Here, you can enter any details you wish to describe the Connectivity Server.
- Enter the IP address of the Connectivity Server and the port number that the Connectivity Server is configured to use (default is 443).
- To require a secure connection over HTTPS, select **Require HTTPS/TLS** (an SSL/TLS certificate needs to be applied to the Connectivity Server).
- If required, select the **Use Proxy Server** option and enter the proxy server IP address and port number. Click **Next**.
- Click **Set** and enter the Gateway key.
  Note: If the Connectivity Server is configured with multiple Gateway keys, when you browse for Clients on this Connectivity Server, you will only see the Clients that are using the same Gateway key as entered
- If operators have been configured on the Connectivity Server, click **Set** in the username and password section and enter the matching username and password. Click **Finish**.

It is possible to configure multiple Connectivity Servers in the Control Console with the same IP address but with different Gateway keys.

Once you have a Gateway configured in the Control, the Browse option can be used to display the list of Client machines currently connected to the Connectivity Server.

Securing the NetSupport Connectivity Server

The Connectivity Server will support multiple Gateway keys. Each Gateway key must be a minimum of 8 characters. Gateway keys can be added to the Connectivity Server dynamically without disrupting any current Client connections.

The Connectivity Server will not accept connections from a NetSupport Control or Client unless a matching Gateway key configured at Client or Control has also been entered at the Connectivity Server.

Clients can only be configured with one Gateway key, whereas the Control can support multiple Connectivity Servers, each with a different Gateway key. All Gateway key data is sent encrypted between the Client, Control and Connectivity Server. Once connected to the Connectivity Server, all Client and Control security, such as User Validation, Security Keys etc, will function normally.

A Control can only connect and browse for Clients that are using the same Gateway Key as the Control.

Gateway key connection matrix

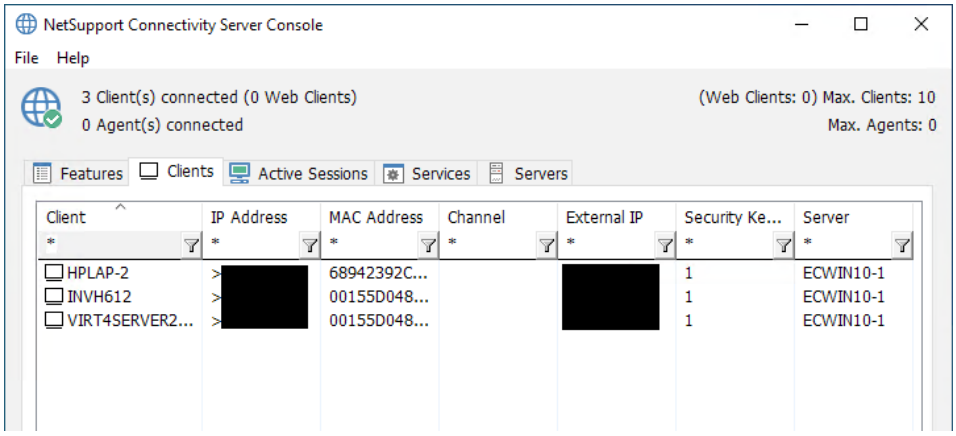
Control Gateway key	Gateway "Gateway keys"	Client Gateway key	Result
"Testing1"	"Testing2"	"Test1"	No connection from Client or Control.
"Testing2"	"Testing1" "Testing2"	"Testing1"	Client connects to Connectivity Server but Control cannot connect to this Client or see the Client in a browse.
"Testing1"	"Testing1"	"Testing1"	Client connects, Control can connect to the Client and see the Client in a browse.
"Testing2"	"Testing1"	"Testing2"	No connection from Client or Control.
"Testing2"	"Testing1" "Testing2" "Test3"		Client connects, Control can connect to the Client and see the Client in a browse.

Logging and monitoring the NetSupport Connectivity Server

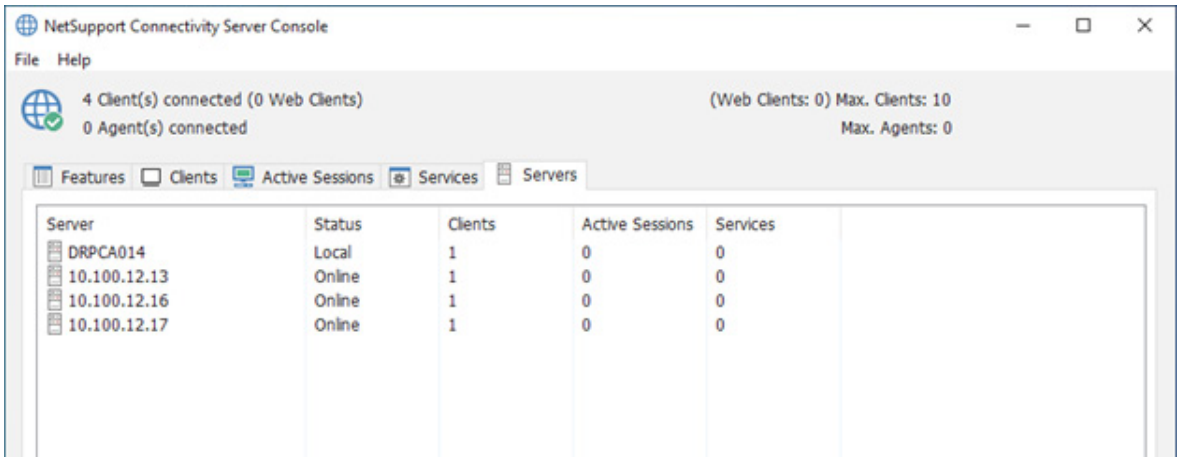
The Connectivity Server runs as a Gateway32 service and is displayed as an icon in the system tray. Right-clicking the icon will display a shortcut menu with options for **Open**, **Configure Connectivity Server** or **About**.

Selecting **Open** will display the NetSupport Connectivity Server Console window as shown below.

The Clients tab shows a list of all the NetSupport Clients currently connected to the Connectivity Server.



The Active Sessions tab displays a list of current connections between a NetSupport Control and a NetSupport Client, with the date and time the connection started.



The NetSupport Connectivity Server creates a log file that records activity for the Connectivity Server. The log file name is GWxxx.log, and it is stored in the location specified in the Connectivity Server Configuration Utility General tab.

GW001.log example:

29-Jun-22, 16:11:20, **NetSupport V14.00, running on Windows 11**
29-Jun-22, 16:11:20, **Connectivity Server started, Max. Licensed connections: 5, Listening port: 443**
29-Jun-22, 16:15:32, **Connectivity Server stopped**

The following is a list of events that are written to the NetSupport Connectivity Server log file:

<product_name> <product_version>, running on <operating_system> <operating_system_version> <operating_system_ service_pack> (build <build_number>), platform <platform_number>

This event is logged when the Connectivity Server is first started. A typical example would be as follows:
NetSupport V14.00, running on Windows 11

Gateway started. Max licensed connections: <max_connections> This event is logged when the Connectivity Server is first started.
Failed to start Gateway This event is logged when the Connectivity Server fails to start.
Gateway stopped This event is logged when the Connectivity Server is stopped.
Listening on port <port_number> This event is logged when the Connectivity Server starts listening on the specified port. This occurs during startup and when a change in the Connectivity Server port is applied in the Connectivity Server Configuration Utility.
Failed to bind to listening port <port_number> This event is logged when the Connectivity Server fails to assign the specified port to listen for incoming connections. The port is probably being used by another application.
Reloading configuration This event is logged by the Connectivity Server when the administrator has used the Connectivity Server Configuration Utility to apply configuration changes.
Listen port has changed. All current connections and sessions will be terminated. This event is logged by the Connectivity Server when the administrator modifies the listening port in the Connectivity Server Configuration Utility and then applies the change whilst the Gateway is running.
Reloading Gateway Keys This event is logged by the Connectivity Server when the administrator has used the Connectivity Server Configuration Utility to apply configuration changes – which may have included additions or removals to the list of Gateway keys.
Client <Clientname> connected This event is logged when a Client connects to the Connectivity Server.
Client <Clientname> Disconnected This event is logged when a Client disconnects from the Connectivity Server.
Control <controlname> connected to Client <Clientname> This event is logged when a Control connects to a Client.
Control <controlname> disconnected from Client <Clientname> This event is logged when a Control disconnects from a Client.
Licence exceed. Rejecting connection from Client <Clientname> (<real_ip_address>, <public_ip_address>) This event is logged when a Client connecting to the Connectivity Server exceeds the licensed number of Clients.
Security check failed for Client <Clientname> (<real_ip_address>). Terminating connection from <public_ip_address> This event is logged when a new Client connection fails to provide a valid Gateway key.
Security check failed for Control browse. Terminating connection from <public_ip_address> This event is logged when a Control fails to provide a valid Gateway key during a browse Clients request.
Security check failed for Control <controlname>. Rejecting connection request to Client <Clientname> from <public_ip_address> This event is logged when a Control fails to provide a valid Gateway key during a connection request to a Client.

Client/Control security check failed for Control <controlname>. Rejecting connection request to Client <Clientname> from <public_ip_address>

This event is logged when the Gateway key provided by the Control during a connection request to a Client does not match the Gateway key supplied by the Client.