Feature sheet

Security Settings

with NetSupport Manager

PIN Connect

PIN : 41452

Give this code to the end user to

Waiting for Client to connect...

With workforces now dispersed across hybrid work environments, having the technology to allow employees to operate effectively while staying secure is key for every company.

That's where NetSupport Manager can help. With security features from activity logs and user acknowledgement to 256-bit encryption, smartcard support and AD integration, it's no wonder it's the choice of military and financial institutions across the globe.

NetSupport Connectivity (Gateway) Server security options

Gateway Key

A NetSupport Connectivity Server can be configured with multiple Gateway keys. Each Client that connects to the NetSupport Connectivity Server needs to be configured with a Gateway key that matches the one set at the NetSupport Connectivity Server. If the key configured at the Client machine does not match, it will not be permitted to connect to the NetSupport Connectivity Server. The Control can be configured with different Gateway icons to browse the Clients on the NetSupport Connectivity Server using different Gateway keys, allowing you to control which Clients are visible to which Control. Again, if the Control is not configured with a Gateway key that matches one of the keys on the NetSupport Connectivity Server, it will not be permitted to browse the NetSupport Connectivity Server to retrieve the list of Clients to connect to.

SSL/TLS certificates

SSL/TLS certificates have been added for superior data security to help ensure that all data sent across the Gateway is encrypted. Customers can enter their own certificate or allow the Gateway to create and use a Let's Encrypt certificate.

Gateway operators

Another option to restrict who has access to the NetSupport Connectivity Server is to include Gateway operators. These are user accounts you can configure on the NetSupport Connectivity Server, allowing only the specified operators to browse the NetSupport Connectivity Server. This can prove beneficial if, for example, a person who knows the Gateway key leaves the organisation. Instead of changing the Gateway key, you can just remove their operator account, knowing they will no longer have access to browse the NetSupport Connectivity Server.

Two-factor authentication (2FA) is now available for operators connecting to the Gateway to start a remote connection. This extra layer of security uses time-based OTP (TOTP) or DUO Push to authenticate the operator for up to 12 hours.

To further strengthen Client authentication and authorisation across the network, NetSupport Manager now supports businesses using RADIUS authentication – and even allows them to use it in combination with 2FA, according to the level of verification required for a specific Client.

✓ Event logging

NetSupport Connectivity Server activity logging is on by default and stored in the following location:

C:\Program Files\Common Files\NSL\Connectivity Server\

Settings for the NetSupport Connectivity Server component are made via the Connectivity Server Configurator. This is accessible by right-clicking on the NetSupport Connectivity Server icon in the system tray.

Client security options

The NetSupport Manager Client includes several different options to secure access to the remote Clients, whether you connect to them directly or via the NetSupport Connectivity Server.

✓ User authentication

It is possible to configure the Client to use a locally stored username and password for the connection, which will be stored in the Client Configuration file, or you can choose to authenticate access to the Client using NT authentication or AD authentication, choosing a group from your domain to authenticate against. When one of these options is selected at the Client, when a Control attempts to connect, it will be prompted to enter a username and password. These will need to match the details selected at the Client to permit the Control to connect.

If the name of the Client executable changes, it will be prevented from running to help combat and protect against exploits and malware. A handy feature for ensuring no untoward activity is taking place.

✓ Security key

Provides additional security that enables Control users to connect only if the Control has the same security key as the Client. Optionally, this can be set as the serial number in your NetSupport Licence file. You must set the security key at both the Client and the Control.

✓ User acknowledgement

When a Control user attempts to connect, a message will be displayed at the Client. Unless the user at the Client explicitly accepts the request, the connection will be refused.

Encryption

With encryption turned on, all the information sent between the Control and Client is very difficult for others to read. NetSupport Manager offers a range of encryption options, ranging from 56 Bit DES to 256 Bit AES, enabling you to find the necessary balance between security and performance. The higher the level of encryption, the higher the potential for decreased performance. Choose the level of encryption to be used while a Control is connected. By default, encryption is set to ‘none’ for all connections and 56 bit DES for HTTP connections.

> “Excellent customer service. The product is ***secure***, ***effective*** and ***stable***. I am very satisfied with the software and happy to recommend it for IT support purposes.”
>
> *James Hill – Premiserv*

Smartcard authentication

If this option is selected at the Client, then the Control will be required to enter a user ID and password as well as the smartcard and PIN to connect to the Client.

Access privileges

Using the Client configuration, you can disable certain remote control features when you connect to the Client, such as to prevent File transfer or disable Control mode when viewing.

Client profiles

It is possible to configure different levels of Control access depending on which user authenticates with the Client for the connection using the Client profiles.

Customisable text

Customisable text enables you to add customisable messages which are displayed at the Client machine when a Control is connected, so the end-user is aware of the remote connection.

Replay Files

When enabled, a Replay File recording will be created each time the Control views a Client PC with the option enabled.

Client logging

Log files record the activity that takes place at a Client machine while it is being remote controlled. Standard information would include the name of the Control that had initiated the connection and the date and time that the session started and ended. The text files that are created provide a useful audit trail, but you can also enhance Client security using this feature.

The Client log file can be edited to only show selected information to further support data protection. For example, to protect personal data such as usernames when receiving support. You can also clear Client log files older than “x” days, if required.

✓ Client Configurator password

The Client Configurator password allows you to restrict access to the Client Configurator using a locally stored password for the Client Profile or by specifying an NT Group of users that can authenticate to access the Client Configrator.

The above options for the NetSupport Manager Client/Control can be applied locally on a Client using the NetSupport Manager Configurator or using the AD Template files for both AD group policy and can be ingested into Intune Configuration Profiles. Settings applied via Group policy will override any local configurations applied.

Control security options

The NetSupport Manager Control also includes a number of different security options to secure access and limit functionality.

✓ Control password

Allows a password to be set at the Control. You will then be prompted for this each time you start the Control.

✓ Control logging

Once enabled, each time the Control subsequently connects to a Client, the activity for that session will be recorded.

✓ Replay Files

When enabled, a Replay File recording will be created each time the Control views a Client PC.

✓ Control interface settings

The Control interface settings allow you to configure which different components for the named configuration are available, such as disabling access to the Auto Groups or Gateway list section of the Control interface.

✓ Control function

The Control function settings allow you to restrict certain features such as the File Transfer or Reboot options.

✓ Control profiles

The NetSupport Control can be configured with different Control configurations, allowing you to set different profiles for your different Control users.

The above options for the NetSupport Manager Control can be applied locally using the NetSupport Manager Control Settings or enforced using the NetSupport Manager Control AD Template files via AD Group Policy. Settings applied via Group Policy will override any local configurations applied.