



## Securing the NetSupport Client

### Overview

This document is designed to provide an overview of the security features available within NetSupport Manager and NetSupport School. For detailed information on individual functions please refer to the relevant product help files or product manual.

### Environments, Considerations and Requirements.

#### NetSupport School – Environments.

Typically, NetSupport School is implemented within schools, colleges and universities, where the environment is fairly standard and the computers are already locked down – often with Active Directory. The types of user roles are also fairly easy to work out and usually consist of Students, Teachers, ICT and Administration staff. NetSupport School often doubles up as a Remote Support tool for the ICT staff.

#### NetSupport School – Considerations.

When considering how best to secure NetSupport School it is worth taking into account the following:

- **Students will not always co-operate with the Teacher** - therefore security features that require the student to perform an action are often not suitable.
- **There should be little or no interaction required from the Student** - i.e. User Acknowledgement where a Student can decide whether to allow or disallow the teacher to connect to their computer is not practical in the education environment.
- **Teachers need to be in Control at all times** – as above if the teacher has to rely on the Student to perform an action in order that they can connect to them they are not in full control of the Student.
- **User Rights** – unlike a corporate environment where employees may have the right to privacy, students will not have “sensitive” data that should not be seen by the Teacher. Therefore the requirement to notify the student that you are watching them is less important. In fact the majority of customers do not want the Student to know whether they are being monitored to ensure that they use the computer correctly at all times, regardless of whether NetSupport is running.
- **Students are very clever** – NetSupport School in the wrong hands could be very disruptive in the educational environment so it is important that there are no “back doors” that Students could use. It is therefore important to secure NetSupport School.

#### NetSupport School – Requirements.

Although there will be exceptions, the majority of NetSupport School customers have the following security requirements from NetSupport School:

- To restrict unauthorised access to the NetSupport Tutor
- Restrict unauthorised access to the Administration network.
- Keep things simple and in the Teachers full control.



# Securing the NetSupport Client

## Securing the NetSupport School Tutor

### Basic Security

#### Only install the Tutor on the Teachers computer

If the Tutor program is installed on Students machines it is more accessible and therefore increases the risk of them being able to use it to gain unauthorised remote access to other computers.

#### Secure the computer where the Tutor program is installed

If a Teacher leaves their computer unattended the Student may access the Tutor application. It is therefore necessary to apply password protected screen savers and implement a security policy requiring users to lock their computer if leaving it unattended.

#### Restricting which logged on users can run the Tutor program

If a Student were to log onto the Teachers computer they should not be able to run the Tutor program. Active Directory or NetSupport Protect are two ways of restricting what applications logged on users can run.

### NetSupport School Tutor Security options

#### Profiling the NetSupport School Tutor

NetSupport School allows you to set up multiple Tutor Profiles for different users, each with a pre-defined set of options. On start-up, if multiple profiles have been created the NetSupport Tutor program will dialog requiring the Teacher to select which profile to use. Each profile can be configured to connect to a specific group of Students reducing the chance of the Teacher connecting to the wrong computers.

#### Password protecting the Tutor Profiles

Setting a password will require the user to enter a password before they can use the selected profile. If the Teacher does not enter the correct password they will not be able to use the profile.

#### Password protecting the Tutor Configurator

The Tutor configuration can be protected by setting a password. This acts independently of the Tutor password if set. Each time a Tutor user subsequently wants to make changes to the configuration, they will be prompted to enter the password.

#### Recording Replay Files at the Tutor

A security video file recording all mouse movements and keyboard actions of a Teacher while they are connected to the Student can be created. Replay files are stored locally at the Tutor computer.



## Securing the NetSupport Client

### Securing the NetSupport School Student

#### Basic Security

##### Don't install the Student Configurator unless absolutely necessary

By installing the NetSupport Student Configurator you are making it more accessible to the Students. NetSupport School Students configurations can be deployed and managed using the NetSupport Deployment utility – this is much easier and removes the need to install the Student configurator component onto each computer.

##### If using a Client32.ini file to configure the Student NTFS file security should be applied

Although the NetSupport Student configuration file has a checksum to ensure that the configuration cannot be changed easily it is possible to overwrite the client32.ini file with another, less secure one. Therefore the file should always be secured using NTFS file Security to prevent this.

##### If available use Active Directory to configure the Student

NetSupport provide Active Directory ADM templates for the configuration of the Student component, these remove the requirement for a client32.ini, and allow central configuration. If available, it is recommended that Student component is configured using Active Directory.

#### NetSupport School Student Security Options

##### Security Key

Adding a Security key requires both the Tutor and Student to have the same encrypted key before the Student component will accept a connection. This removes the risk of an unauthorised person installing a Tutor and connecting to computers.

##### User Acknowledgement

If enabled, a Remote Control session cannot take place until the Student has confirmed that they accept the connection being made. This option is useful if installing the software on administration networks where potentially sensitive data is displayed. User Acknowledgement will give the User the opportunity to close any sensitive documents before allowing the Remote User to view their screen.

##### Display customisable text when connected and/or Viewing a Student

To ensure that a remote user is aware that their computer is being viewed or is connected a message can be displayed on their desktop.

##### Apply a Configurator password

As an extra level of security, a password can be associated with a Configuration File. This prevents unauthorised amendment of this Student configuration. When the Configurator is next started, the user must enter the required password before being able to change any Student parameters in this Configuration file.



## Securing the NetSupport Client

### NetSupport Manager

#### Environments, Considerations and Requirements.

##### NetSupport Manager – Environments.

NetSupport Manager is installed in many varying environments; these may be Managed Service Providers requiring remote access to a single computer on a customer's site, financial institutions wishing to remote control their ATM machines, or one of many other scenarios where secure remote access to computers is required.

The types of access that remote users require also depends on their role within the organisation – for example, the computer being controlled may be an unattended server and will therefore require security features that do not rely on the user authorising the connection. Alternatively, the remote user may require access to a computer but not access to the data that can be accessed from this computer.

There are several different scenarios and network topologies that require different security features to allow everyone to do their job whilst at the same time not compromising security.

##### NetSupport Manager – Considerations.

As the security requirements for NetSupport Manager are varied things to be considered also vary. The following are high level areas of consideration when designing a security policy for NetSupport Manager:

- Securing the Users Computer.
- Protecting the Users Data.
- Protecting the Employee (Human rights/Privacy).
- Securing Servers/Unattended Computers.
- Protecting the Remote User.

##### NetSupport Manager – Requirements.

The following are some of the requirements that may be included as part of a security policy for NetSupport Manager:

- Restricting unauthorised access to computers.
- Restricting unauthorised access to data.
- Notify users of the remote users actions/intended actions.
- Providing an Audit of events.
- Different access for different users/roles.
- A strong set of security features.
- Control and Client side security.



## Securing the NetSupport Client

### Securing the NetSupport Manager Control

#### Basic Security.

##### Only install the NetSupport Control where required

The NetSupport Control should only be installed where required, if the Control is installed on all computers the risk of it being used to gain remote access to other computers without permission increases considerably.

##### Secure the computer where the NetSupport Control program is installed

If the User leaves their computer unattended it may be used without permission, therefore applying password protected screen savers and enforcing policy requiring users to lock their computer if leaving it unattended are important.

##### Restricting which logged on users can run the NetSupport Control program

If a unauthorised user were to log onto the Control users computer they should not be able to run the Control program. Active Directory or NetSupport Protect are two ways of restricting what applications logged on users can run.



## Securing the NetSupport Client

### **NetSupport Manager Control Security Options**

The following section lists NetSupport Control security related features. These have been categorised as follows:

- Securing the NetSupport Manager Control.
- Protecting the Control User.
- Protecting the User.
- Protecting the Data.

#### **Securing the NetSupport Manager Control**

To prevent unauthorised access to the NetSupport Manager Control or to functions available within the Control interface, one or more of the following features should be considered:

- A Control Password.
- Control Profiling.
- Hiding the Client list, Group list, Dial-up list and/or Gateway list.
- Making the Client list, Group list, Dial-up list and/or Gateway list Read Only.
- Disabling the Browse function.
- Disabling certain Remote Functions.
- Disabling certain View Modes.
- Exit on Disconnect.

#### **Protecting the Control User**

To provide a record of what the Control user did whilst connected to the remote computer an audit can be created giving details of the session:

- Event logging.
- Recording the Remote session.

#### **Protecting the User**

To ensure that the user is aware of the Control users intentions and has the opportunity to stop them or close sensitive documents, one or more of the following functions may be used:

- Specifying the Control Name.
- Specifying the Control Description.
- Prompting to provide additional information when connecting.
- Providing a message on disconnect.

#### **Protecting Data**

To ensure that data at the users computer is protected from the Control user, either whilst being viewed on screen or whilst it is being transferred, one or both of the following options are available:

- Using Encryption.
- Blanking the Client Screen.



# Securing the NetSupport Client

## Securing the NetSupport Manager Client

### Basic Security

#### Don't install the Client Configurator unless absolutely necessary

By installing the NetSupport Client Configurator you are making it more accessible to unauthorised access. NetSupport Manager Configurations can be deployed and managed using the NetSupport Deployment utility – this is much easier and removes the need to install the Client configurator component onto each computer.

#### If using a Client32.ini file to configure the Client apply file security

Although the NetSupport Client configuration file has a checksum to ensure that the configuration cannot be changed easily it is possible to overwrite the client32.ini file with another, less secure one. Therefore the file should always be secured using NTFS file Security.

#### If available use Active Directory to configure the Client

NetSupport provide Active Directory ADM templates for the configuration of the Client component. These remove the requirement for a client32.ini, and allow central configuration. If available, it is recommended that Client configuration through Active Directory is used.

### NetSupport Manager Security Options

The following NetSupport Client security related features have been categorised as follows:

- Securing the NetSupport Manager Client.
- Protecting the Control User.
- Protecting the User.
- Protecting the Data.

#### Securing the NetSupport Manager Client

Preventing unauthorised access and use of the NetSupport Client can be achieved using a combination of the following features:

- Profiling the NetSupport Client to provide different feature sets for different remote users/groups.
- Using a proprietary username and password to establish a remote connection.
- Using NT Authentication to establish a connection.
- Using Active Directory Authentication to establish a connection.
- Disabling features available to remote users.
- Implementing a Security key.
- Restricting connections to certain IP or IPX addresses/ranges.
- Locking the computer on disconnect.
- Logging the computer off on disconnect.
- Restarting the computer on disconnect.
- Protecting the Client configurator using a proprietary username and password.
- Protecting the Client configurator using NT authentication.
- Always Prompt for username and password.

#### Protecting the Control User

To provide a record of what the Control user did whilst connected to the remote computer an audit can be created providing details of the session:

- Event logging to a file.
- Event logging to the Event log.



## Securing the NetSupport Client

- Denying the connection if no log file available.
- Recording the Remote session.

### Protecting the User

To ensure that the user is aware of the Remote users intentions and has the opportunity to stop them or close sensitive documents, one or more of the following functions may be used:

- User acknowledgement.
- Displaying message on disconnect.
- Displaying a message whilst connected.
- Displaying a message whilst being viewed.
- Beep whilst connected.

### Protecting the Data

To ensure that data at the users computer is protected either from the Control user either whilst being viewed on screen or whilst it is being transferred, one or both of the following options are available:

- Force Controls to use encryption.
- Setting a minimum encryption level.
- Forcing the remote user to inherit the logged on users file system permissions.
- Applying restrictions to the local file system for the remote user.