

# NTRsupport: Security

This document describes security issues of **NTRsupport**

## • Physical Security (ASP model)

**NTRglobal** guarantees that NTRsupport has:

- **Environmental security**
- **Electrical security**
- **Physical security**
- **Architectural security**

## • Storage Areas

The storage areas of the data warehouses typically have the following physical characteristics:

- **Technical Floor**
- **Fire Protection systems**
- **Racks (Type and Capacity)**
- **Network Cabling**

## • Incident Management

The monitoring system automatically feeds information into the Incident Management System:

- Resolution and Escalation
- Incident Detection

## • System Backup (ASP Model)

To protect its customers and to ensure a rapid recovery in the event of a system failure, NTRglobal regularly backs up its systems and all of its customers' valuable data.

## • Software Certification

NTRsupport is certified by Verisign. The Verisign certificate guarantees to users that they are using an original copy of NTRsupport – a copy supplied by NTRglobal, which has not been modified by any third party. NTRglobal guarantees that the software is free of all viruses.

## • Secure Connections

NTRsupport uses standard ports to establish connections. In addition, the License version can be installed behind a firewall or Router/Proxy which translates network addresses (NAT).

The design of NTRsupport guarantees that the connection will be made in seconds even when both users are using NAT or Firewall.

The connection between the operator and the client is made through a secure logical tunnel. A direct connection is made between the two parties if one is possible, and, if not, the connection is made via the NTRsupport server.

## • Access Security

Operators are only allowed to access a given feature of NTRsupport if the Administrator has given them permission to do so. Different Operators can have different permissions, which means that the Administrator has complete control over which Operators can use, for example, co-surfing or remote control, and which remote control modes (total control, demo or desktop sharing) those Operators are permitted to use.

Administrators can further control Operator access to NTRsupport by defining a range of accepted IP or MAC addresses.

For further security, Administrators and Operators also have the option of logging in to NTRsupport via a 128-bit Secure Socket Layer (SSL) connection.

## • Data Encryption

All of the algorithms used by NTRsupport have been validated by the official tests provided by the creators/owners of that algorithm.

**Encrypted Storage:** Confidential or sensitive data stored in the database are always encrypted. Stored conversations are only decrypted at the moment that the Administrator consults them.

**The Rijndael 256 Algorithm:** NTRsupport uses the Rijndael 256 algorithm for encoding connections made by the video, voice and remote-control modules. This algorithm meets the requirements set by the Federal Information Processing Standard (FIPS.197) and can thus be used by US government organizations for protecting their sensitive data.

*Rijndael was created by the Belgian researchers Vincent Rijmen and Joan Daemen. It is a block encoder that operates using blocks and keys of variable length: 128, 192 or 256 bits.*

## • Blocking User Access to NTRsupport

**Blocking IP Addresses:** NTRsupport offers a sophisticated system for blocking access from specific IP addresses for variable periods of time.

**Blocking User Accounts:** NTRsupport allows Operators to block 'nuisance' users (those with whom they do not wish to communicate).

## • Attack Detection

At the application level the company detects the following types of attack:

- **SQL injection**
- **Cross-site scripting (XSS)**
- **Buffer overflow**
- **Hijacking**
- **Flooding**

## • Virus Detection

When a file is uploaded or transferred to the NTRsupport server, the file is scanned for the presence of viruses or other malignant software.

## • SSL

SSL is a cryptographic protocol that provides a secure connection across the Internet. This enables the client and server applications to communicate in a way that prevents eavesdropping, tampering and message forgery. Users have the option of using a secure (SSL) connection when logging in to NTRsupport, and SSL is set as the default connection type.