



Security Specifications



This document contains information which is the property of NTR. Its contents may not be copied, photocopied, reproduced, translated or summarized; either partially or in its entirety, by any means whatsoever, without the prior written permission of NTR.

Net Transmit & Receive reserves the right to change the contents described in this document, at any time and without prior notice.

The products and companies which are referred to in this document are registered by the pertinent companies or brand owners.

Copyright © 2006 by NET TRANSMIT & RECEIVE.
All Rights Reserved
Printed in Barcelona, Spain.

NTR inquieto v5.5 – Security Specifications

Table of Contents

Introduction	4
1. Certified Software	4
2. Login security	5
3. Data Encryption	6
4. Encrypted Storage	6
5. Updatable Algorithms	7
6. Connection security	7
7. Site Administration Security	8
8. Tool and Service Security	8
a) Security during Chat	8
b) Cosurfing	9
c) Remote Control (Inquiero Remote Control)	9
d) Installable Remote Control	11
e) Voice/Videoconference	12
9. User block	12
10. Physical Security in the Hosting platform (ASP version)	13
11. Data protection	13
12. Conclusion from External Auditors	13
Summary – NTR inquieto v5.5 Security	14

Introduction

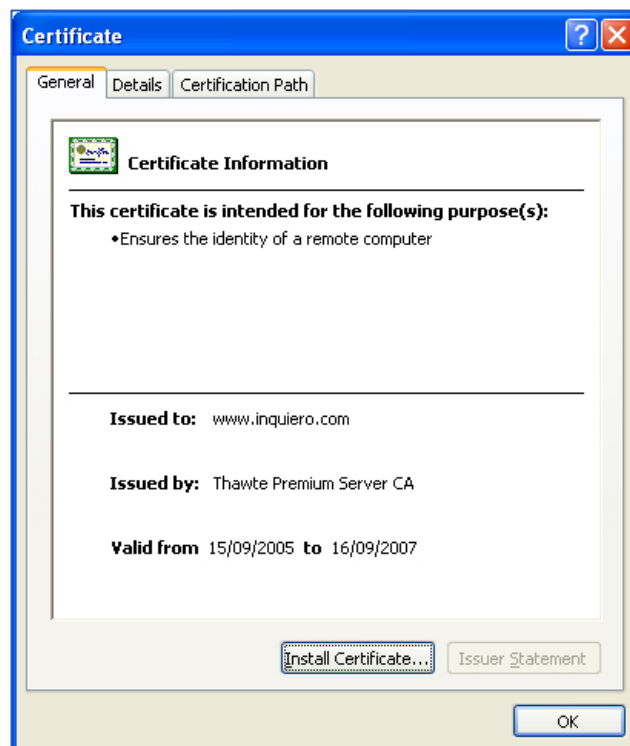
This document is of a technical nature. It describes the main security mechanisms incorporated in **NTR inquiero** which guarantee security of data at all levels.

All aspects related to security have been a primary concern from the start of the design process in **NTR inquiero**. The product code is 100% NTR property, and the continuously revised security measures incorporated in the product, prevent unauthorized access to data, programs and systems used by **NTR inquiero** hence protecting companies and customers who use our product.

Around 4.000 customers currently using **NTR inquiero v5.5** worldwide can attest of the reliability of the product.

1. Certified Software

NTR inquiero v5.5 holds the **Verisign Certificate**, assuring users that the software is original, that it cannot be altered and is virus-free.



2. Login Security

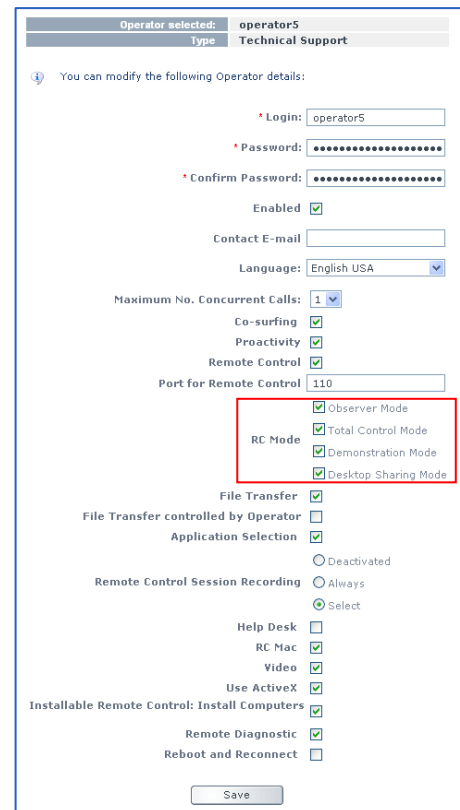
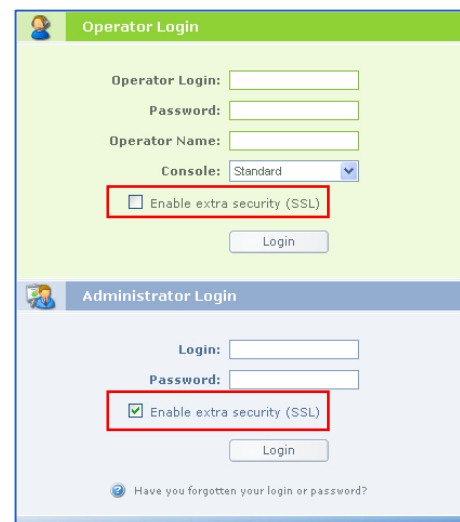
NTR inquiero limits access to all features by using usernames and passwords and by allowing define a wide range of user profiles. Based on this premise, each Operator of the service can only access the **NTR inquiero** features which the Administrator has defined for that Operator.

E.g. a site administrator can decide which Operators will be allowed to use the co-surfing feature, which will use remote control, the remote control modes to be used (total control, demo, desktop sharing modes).

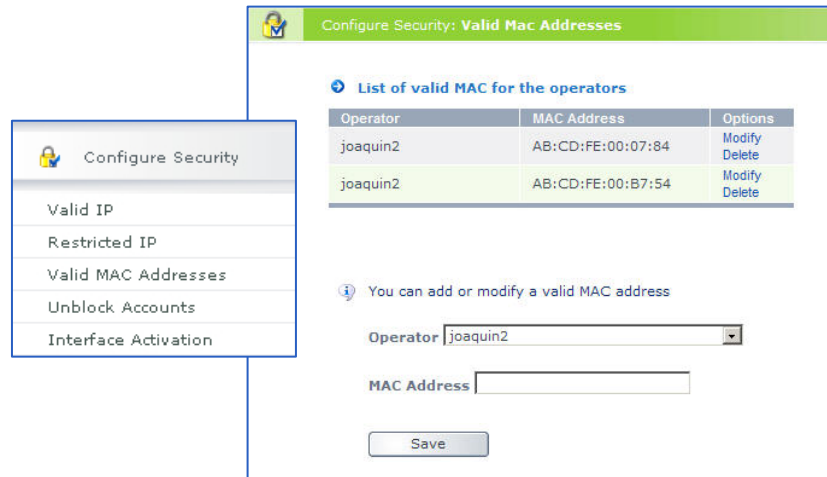
Operator login is done by means of password authentication. Where Operators or Administrators incorrectly enter their password or username three times, their account is blocked for a few minutes, and the event is registered in the Security reports found in the Administration centre.

Operator and Administrator passwords never travel via the internet when connecting to the service. The password is authenticated on the same computer where it is saved in deconstructed form, encrypted with the **md5 algorithm**, making recovery impossible.

Optionally, Administrator and Operator Login can be done via 128-bit **SSL (Security Socket Layer)**.

The site administrator can restrict Operator access to **NTR inquiero** by defining a range of valid IP or MAC addresses.



3. Data Encryption

All communication is done via the **NTR inquiero** server. When the Operator writes a message, it is encrypted in the Operator's computer using the operator's password, before being sent in encrypted form to the **NTR inquiero** server.

The server decodes the message using the Operator's password, and encrypts it once again using a password previously assigned to the visitor to generate the encryption key. Once encrypted, the newly encrypted message is sent to the customer. (This process is described in more detail in section 8 of this document).

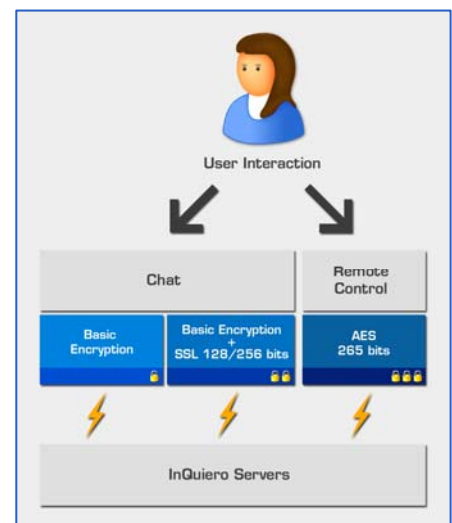
4. Encrypted Storage

Data stored in the database is always encrypted.

Conversations stored are only decoded when the Administrator views them.

NTR inquiero uses three levels of encryption depending on whether the data to be transmitted or stored are messages, passwords or e-mail addresses:

- Some features such as Chat, use basic lineal encryption and 128-bit SSL if the customer so wishes.
- Other features such as Remote control, file transfer, desktop sharing always use 256-bit AES encryption.



- The use of SSL in chat can be enabled or disabled on either (or both) the customer's or operator's side according to the customer's requirements.

5. Updatable Algorithms

The security algorithms used by **NTR inquiero** have been selected by NTR software engineers due to their strength and simplicity. They use standard linear encryption techniques, generating a key from the user's password.

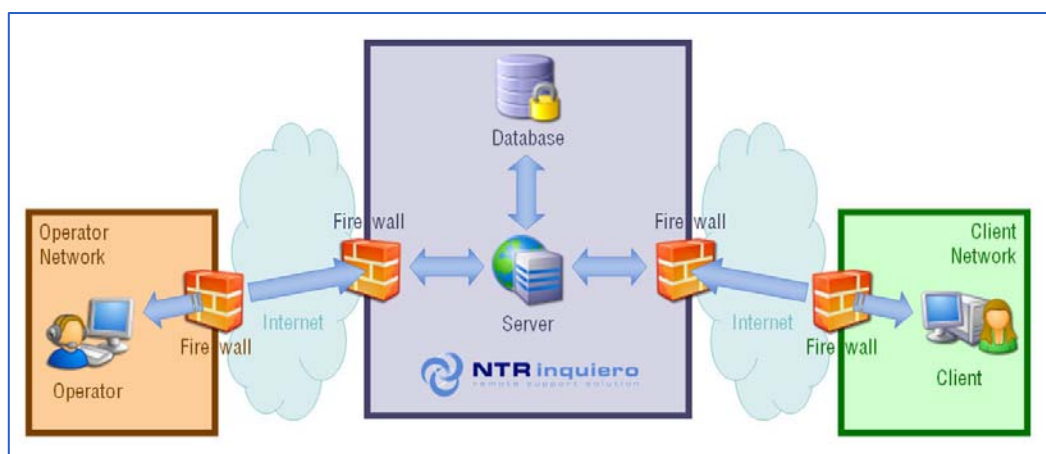
The design of **NTR inquiero** allows all encryption algorithms to be modified virtually, using a component which encapsulates them, in situations requiring additional security.

6. Connection Security

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

The operator only needs an Internet connection and a browser to connect to **NTR inquiero**. The system will redirect the voice, video and remote control sessions established during a session.

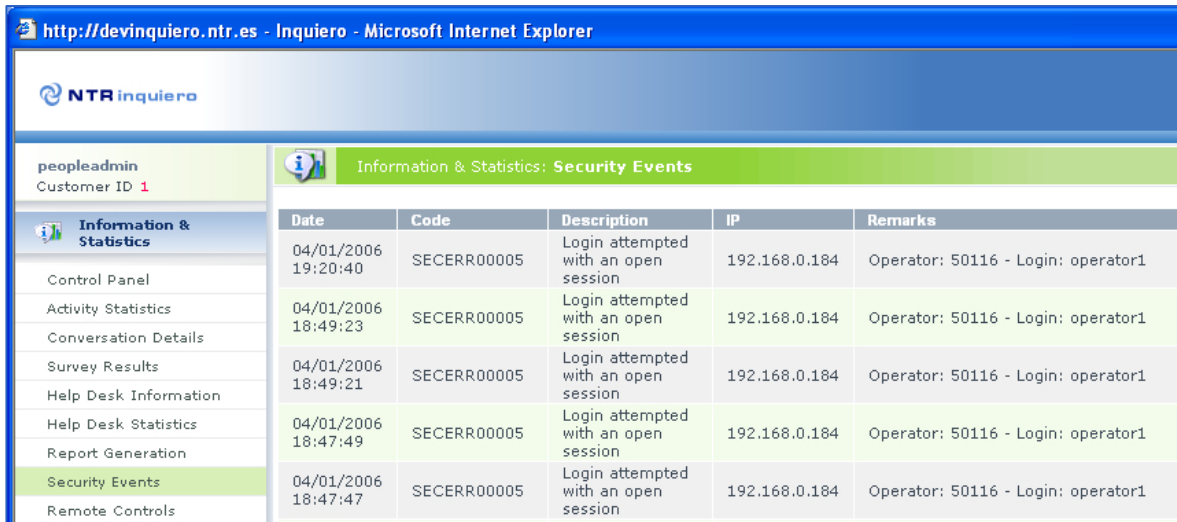
Each operator can only access the features defined by the NTR inquiero administrator in their user profile. Using the **NTR inquiero** Administration center, a port can be assigned to a specific operator.



The design of **NTR inquiero** guarantees that connection will be done in seconds, even between users with NAT on both sides.

7. Site Administration Security

The site administrator can revise all events related with security, obtaining reports containing the date, time and IP address of failed login attempts.



Date	Code	Description	IP	Remarks
04/01/2006 19:20:40	SECERR00005	Login attempted with an open session	192.168.0.184	Operator: 50116 - Login: operator1
04/01/2006 18:49:23	SECERR00005	Login attempted with an open session	192.168.0.184	Operator: 50116 - Login: operator1
04/01/2006 18:49:21	SECERR00005	Login attempted with an open session	192.168.0.184	Operator: 50116 - Login: operator1
04/01/2006 18:47:49	SECERR00005	Login attempted with an open session	192.168.0.184	Operator: 50116 - Login: operator1
04/01/2006 18:47:47	SECERR00005	Login attempted with an open session	192.168.0.184	Operator: 50116 - Login: operator1

8. Tool and Service Security

To strengthen security, **NTR Inquiero v5.5** prevents the same URL from being reused. If a user attempts to connect to a used URL link a second time, a security error page appears. For this reason, the **Refresh, Back, Forward** and **<F5>** functions have been disabled. Links to files annexed from the **"Send File"** and **"Receive file"** functions expire after the first use.

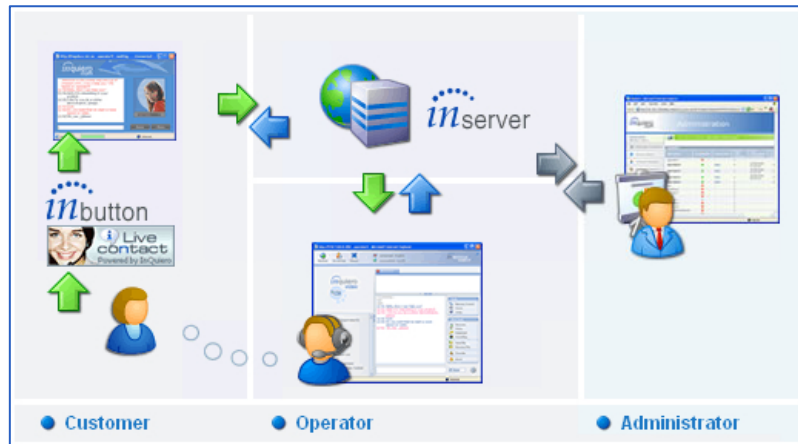
a) Security during Chat

Text chat can support 128-bit SSL.

All text messages (Chat) sent by **NTR Inquiero** use the following procedures:

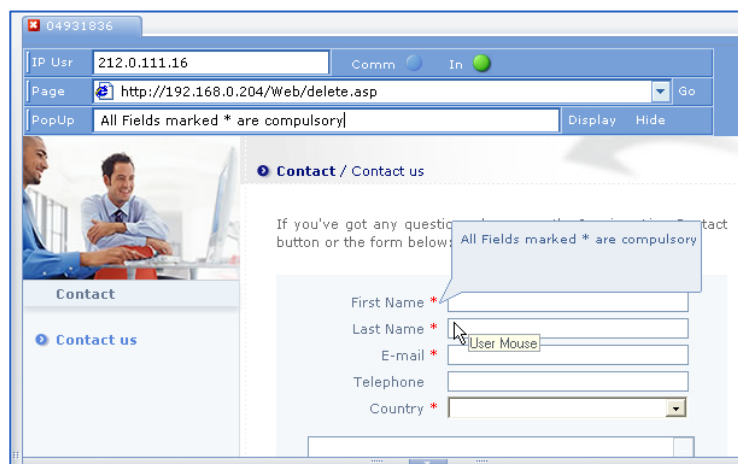
1. The sender sends the coded message to the server, using the user password to generate the encryption key.
2. The server decodes the messages and encodes it once again, but this time using the receiver's password to generate the encryption key. The message encoded with this key is saved in the server and sent in encoded form to the receiver.
3. The receiver decodes the message using the key constructed from their password.

All chat conversations are stored in the database in encrypted form, and can only be accessed by the site administrator.



b) Co-surfing

Co-surfing is the joint-navigation tool of **NTR inquiero** which allows the operator to view the movements, page, mouse movements and input contents of a site user visiting in real-time. The content of the page of the visitor is processed by functions which are in charge of sending the necessary information to the server. These functions are not capable of recovering sensitive data, e.g. if the user is entering the password in a field of the screen, **NTR inquiero** can only recover the asterisks shown in this field.



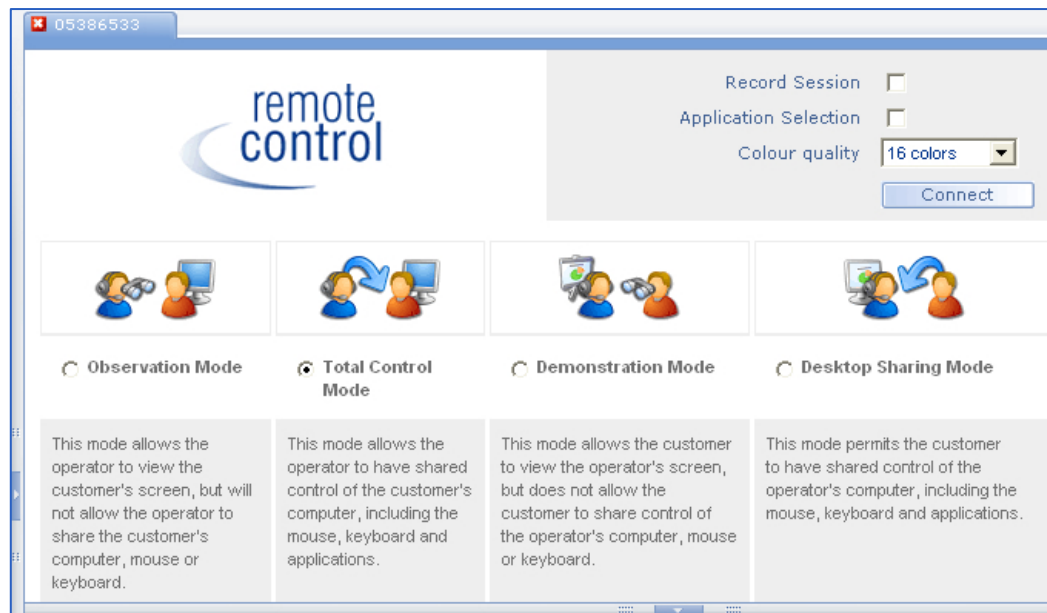
c) Remote Control (Inquiero Remote Control)

256-bit Encryption: Remote control sends and receives packages via a TCP connection, using a generic protocol adapted by **NTR**, which uses the **Rijndael 256-bit** encryption algorithm.

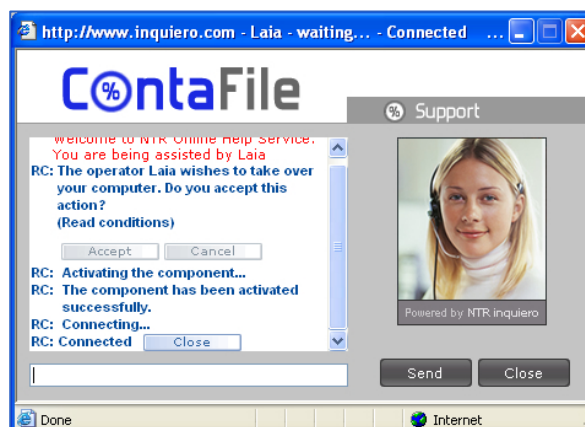
Sender/Receiver Authentication: The remote control compresses and codes the data packets before sending them with, in addition to own TCP, data about the sender and receiver, guaranteeing the authentication of both.

In both Remote control and File transfer, the information packets always travel compressed and encrypted with the 256-bit Rijndael algorithm.

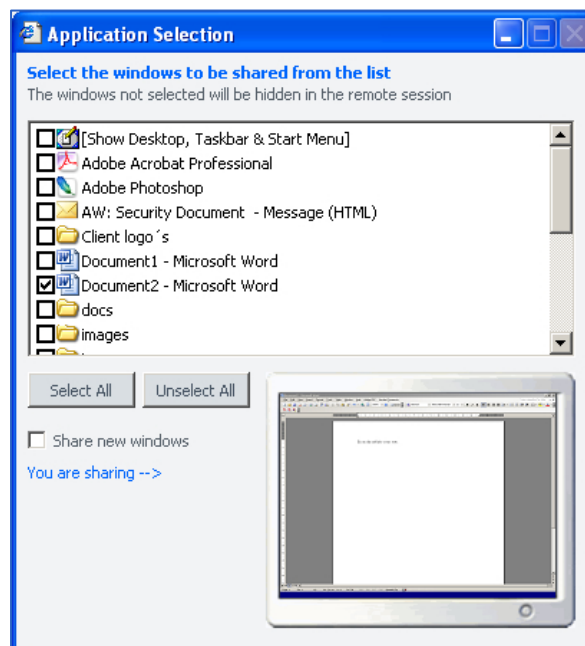
When a remote control session ends, the server leaves no trace of the connection previously established.



Express Authorization: NTR Inquiero Remote Control informs each user of any operation taking place on their computer during the session. For this reason, it requests express authorization to start a session in any of the remote control modes available in NTR Inquiero and for each file transfer done during a session.



Visible Application Selection: To guarantee the privacy of data, the Operator and Customer can use the Application Selection feature when starting a remote control session, which allows each user determine which applications on their desktop are to be hidden from the other during the remote control session.



End session with a single click: Both users (Operator and Customer) can end the remote control session at any moment by pressing the **Close** icon of the window.

d) Installable Remote Control

The Installable Remote Control from **NTR inquiero** can be installed on computers and servers allowing the operator to access an unattended computer, without requiring the presence of a user. It allows restart remote computers and re-establish the connection with the Operator afterwards.

During the running of the service, **security measures are maximized on all levels:**

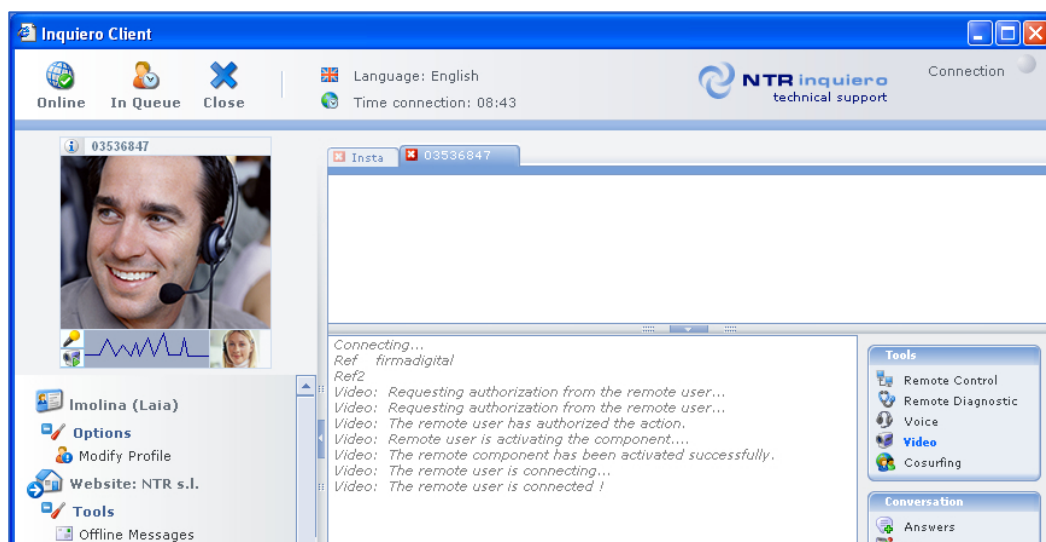


- The access password of a guest computer does not travel via the internet, meaning that it cannot be recovered by ill-intentioned users.
- The user password is coded using the destructive **triple-DES** algorithm, which destroys the password afterwards.
- Both the protocol at the start of the remote control session (connection to the *Socket Server*) and the packets sent and received during the remote control session are coded using the Rijndael 256-bit security algorithm, which meets the requirements of the Federal Information Processing Standard (FIPS-197).
- The service installed in the guest computer does not leave any ports open listening.

Installable Remote Control allows configure various security options; for example, the remote computer automatically locks on ending the session or the session disconnects automatically after the minutes indicated in a determined field.

e) VoIP/Videoconference

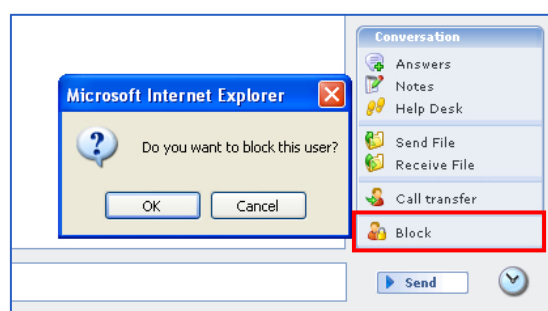
- During a video or voice session, packets are sent encrypted with a special compression algorithm.



9. User Block

NTR inquiero incorporates a feature which allows operators to block “annoying” visitors.

The site administrator can manage these blocks and identify the IP of the user.



10. Physical Security in the Hosting Platform (ASP version)

The **NTR Inquiero** servers in its ASP (Application Service Provider) version are hosted in an Internet solutions centre of Colt Telecom, a specially-dedicated environment, independent from the **NTR** facilities.

Colt Telecom applies extremely strict security measures, including **24x7 monitoring**, restricted physical access, backup electric supply, environmental controls, etc. aiming to ensure that the servers are always kept in optimum conditions.

The security installations are carried out by experts in security and are audited by external companies.

11. Data Protection

NTR commits to not using information received from registered users, stored in databases belonging to **NET TRANSMIT & RECEIVE SL.** for commercial means.

NTR takes all possible measures of technical, organizational, and security nature which guarantee the confidentiality and integrity of the information.

12. Conclusion from External Auditors

In the following, we have summarised the reports made by various **companies specialized in auditing software security**, after analysing in depth the functioning of **NTR Inquiero v5.5**.

The reports delivered to NTR on 12th December 2005 indicate that the security offered by NTR Inquiero v5.5 is very advanced, both when applying standard secure connection mechanisms (SSL) and when not.

The main points identified and on which this conclusion has been based are the following:

- **Login Security:** The auditors have checked that *passwords never travel via the internet* when connecting with or without SSL, meaning the risk of interception is practically nil, even without using SSL. This fact has been verified by the auditors using traffic observation tools (network sniffers), and by observing the JavaScript code in the login form.

- **Data Transfer Security:** The auditors have checked that when conversation data or links to sent or received files are transmitted, the data is encoded using the MD5 function with the user's password, and that the option to use SSL for both the Operator and Customer adds an additional coded layer which guarantees absolute confidentiality.

- **Secure Data Storage:** The auditors have confirmed that conversation data is saved in encrypted form in the database and that neither the database or server administrator nor possible intruders can see the contents, since the history stored in the server can only be decrypted by connecting to the application with the password.

Summary – NTR Inquiero v5.5 Security

- **Login Security:** Zero risk of interception since that the *passwords never travel via the internet*.
- Additional security layer: Optional use of **SSL for Administrator, Operator and Customer**.
- Definition of ranges of **Valid IP, valid MAC addresses** and even **Port assignment**.
- Detailed reports on security events which have occurred (failed access attempts, etc.)
- **Data Transfer Security:** Data transmitted is coded beforehand, guaranteeing absolute confidentiality.
- **Express authorization** is required to start a remote control session and for each file transfer.
- **Privacy:** During remote control, each user can select the applications to be shown to the other user during the session.
- **Data encryption is used on three levels.**
- Remote control and File transfer information packets always travel **compressed and encrypted with the 256-bit Rijndael algorithm** and include data which guarantees the authentication of the sender and the receiver.
- **Secure Data Storage:** The data is always stored in encrypted form in the database and can only be decrypted with the Administrator's password.
- **Recording and Storage of Remote Control Sessions**
- **Disconnection of Remote Control Sessions with a single click.**
- **Block "Annoying" visitors** and identify their IP
- The product code is 100% **NTR property**
- **Verisign Certification**, ensuring original software, free of viruses and which cannot be altered.
- Reliability of the product endorsed by almost **4,000 customers** which currently use NTR Inquiero worldwide.
- High security of the product recognised by **External evaluations** done.
- **Data Protection and Processing** in accordance to current law.

More information on www.inquiero.com