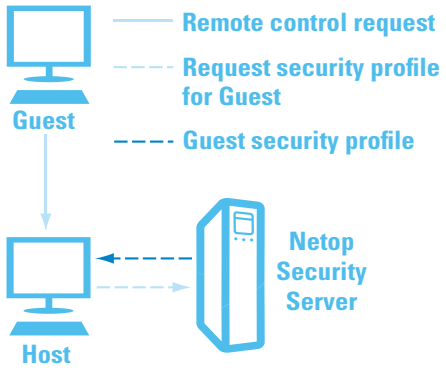
Netop® Security Server

Unique remote solutions

Netop Security Server provides centralized security, administration, authentication and authorization of all remote control users. All remote control activity can be logged and recorded. You are in full control of who can do what, where and when.



Security is an important factor when choosing a remote control solution. Gone are the days where security was a matter of the highest degree of encryption.

Today, a truly secure remote control solution will address **who** can do **what**, **where** and **when**. And when the remote control session is finished it should be able to **document** what actually took place in the session.

The answer to who, what, where and when lies in:

High security authentication

You must be able to authenticate users in a way that complies with your level of security e.g. using directory services, smart cards or token based authentication.

Differentiated access rights

Users should not be treated equally when it comes to security. An administrator is typically given more rights than a support rep, and often it is necessary to limit the rights of external consultants when given remote control access to servers. That is why you must be able to give different rights to different groups.

Easy, centralized and scalable management

If security settings are managed locally on the client or server it becomes a difficult task to change settings even in relatively small networks.

Managing group rights, changing settings should all be as easy as a few clicks. If it is not easy to manage security errors are likely to happen.

Full range documentation

When it comes to compliance you need to be able to show what happened. You want to erase any doubt about what was changed, deleted, etc. in that remote session. Intensive event logging or screen recording makes it easy to show what happened during the remote control session.

The Benefits

- The highest level of security with role based security profiles
- Enforce security policies with a few clicks
- Stay compliant with extensive documentation
- It is fast, easy and time savin

Netop Security Server at a Glance

- The Netop Security Server is a software module running on a central server
- Centralized management of security for Netop Remote Control Solution
- Manage exactly who can remote control which computer(s), when they can do it and which rights they have.
- Manage the remote control rights for compliance with security polices
- Highly scalable and is used in both small organizations and up to networks with 100,000+ users
- All remote activity can be logged locally or centrally on the Netop Security Server
- All remote sessions can be screen recorded and stored locally or on a shared drive.
- Designed for companies with high security requirements and works well with existing infrastructure such as Directory Services, RSA SecurID, Smart Cards etc.

Netop A/S • Bregnerodvej 127 • DK-3460 Birkerod • Denmark
Tel. +45 4590 2525 • sales@netop.com • www.netop.com

Netop

Netop® Security Server

Key Features

Centralized authentication & authorization

Authentication is used to identify the Guest user. This can be done using Netop, Windows, Directory Services, Smartcards or RSA SecurID authentication services.

Centralized authentication means that information about what the Guest can do is available in a database. Via the Netop Security Server, the Guest's allowed actions are authorized against a database service containing security roles.

Centralized logging and recording

Netop Security Server allows for more than 100 events to be logged during session activity and logon attempts. Session can also be fully screen recorded. Logs and recordings can be stored at multiple destinations. These logging destinations include local logging on the Guest or Host and central logging on the Netop Sercurity Server.

Protected traffic

There are several ways that information moving between the Host and Guest modules can be protected:

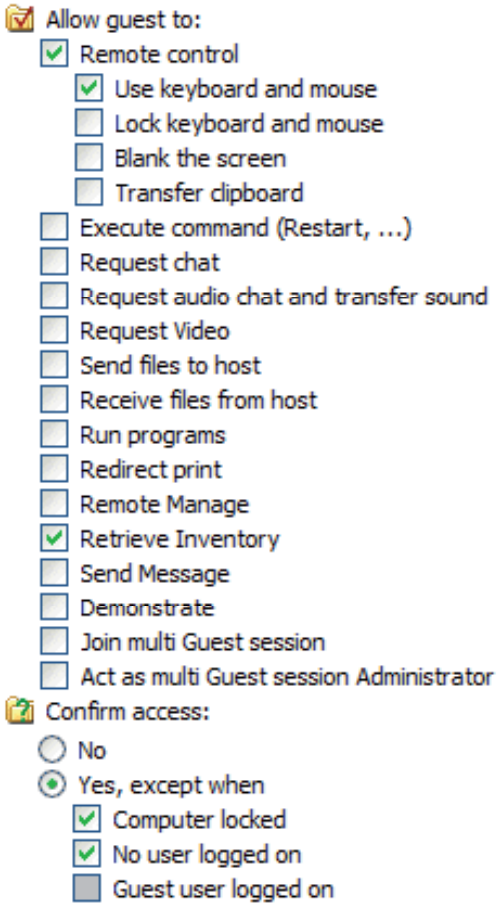
- Encryption - Data transmitted between modules can be encrypted end-to-end using the Advanced Encryption Standard (AES) with key lengths up to 256 bits. Seven different levels are available.
- Integrity and message authentication - The integrity and authenticity of encrypted data is verified using the Keyed-Hash Message Authentication Code (HMAC) based on the Secure Hash Standards SHA-1 (160-bit) or SHA-256 (256-bit).
- Key exchange - Encryption keys for encrypted data transmissions are exchanged using the Diffie-Hellman method with key lengths up to 2048 bits and up to 256-bit AES and up to 512-bit SHA HMAC verification.

Protecting the Host

To gain access to the Host computer, the Guest computer can be forced to meet up to five access criteria:

- MAC/IP address check - only a pre-specified list is allowed access
- Closed user group - license key controlled access
- Authentication - Directory Services, smartcards, tokens
- Callback - the host can do a call back to the host
- User controlled access - user has to accept access

See for yourself



Supported Platforms

- Windows 95
- Windows 98
- Windows Me
- Windows XP
- Windows NT
- Windows 2000
- Windows Server 2000
- Windows Server 2003
- Windows Server 2008
- Windows Terminal Server
- Windows Vista

Netop A/S • Bregnerodvej 127 • DK-3460 Birkerod • Denmark
Tel. +45 4590 2525 • sales@netop.com • www.netop.com

Netop