NetOp® Remote Control

moving expertise - not people

Security

Technical article

Complete, scalable, and secure remote control software for IT professionals

Remote control in the IT industry is the process of being able to see the screen of a remote computer and being able to control its keyboard and mouse. NetOp Remote Control is designed specifically to meet the needs of corporate business and contains numerous features to help IT professionals get the most out of remote control technology. It is typically used for network management, system administration, and in helpdesk environments.

Based on an incredibly stable, fast, and user-friendly remote control system, this program supports all commonly used operating systems and communication protocols. The program's intuitive interface and variable settings mean you can literally mould the system to support the way you do business. And what differentiates NetOp Remote Control from its competitors is the comprehensive security regime that can be adjusted to exactly meet your needs. This scalable product can grow with your organization, and the security features can be scaled up to offer security protection to even the most demanding of organizations, for example, banks.

This white paper describes the key features and benefits of NetOp Remote Control. In particular it presents the security objectives that ensure you can use this remote control software across large networks with no risk of data or resources being accessed without authorization.

Example of key features

The key features of NetOp Remote Control include:

- Remote control
- Remote management
- File transfer
- Scripting
- ActiveX components
- Multi-chat
- Audio chat
- Send message
- Demonstrate
- Remote program launch
- Control computer state
- Get inventory
- Request help
- Multiple protocols
- Multiple platforms

- Encryption

- Masking

- Event logging

- Security

Threats to security

It is absolutely essential in remote control software that you can ensure that access to data is protected from unauthorized users.

The process of remote control—being able to see the screen of a remote computer and controlling its keyboard and mouse—creates an environment that needs careful security considerations. When securing a remote control session, the Guest computer, Host computer, and data transmissions involved in the remote control process must all be taken into consideration. The Guest computer initiates the remote control session by attempting to take control of the remote PC, or Host computer. Typically, an IT employee or an administrator controls the Guest computer, and the Host computer belongs to an end user, often an employee requesting assistance. Securing access to the Guest and Host computers is absolutely necessary.
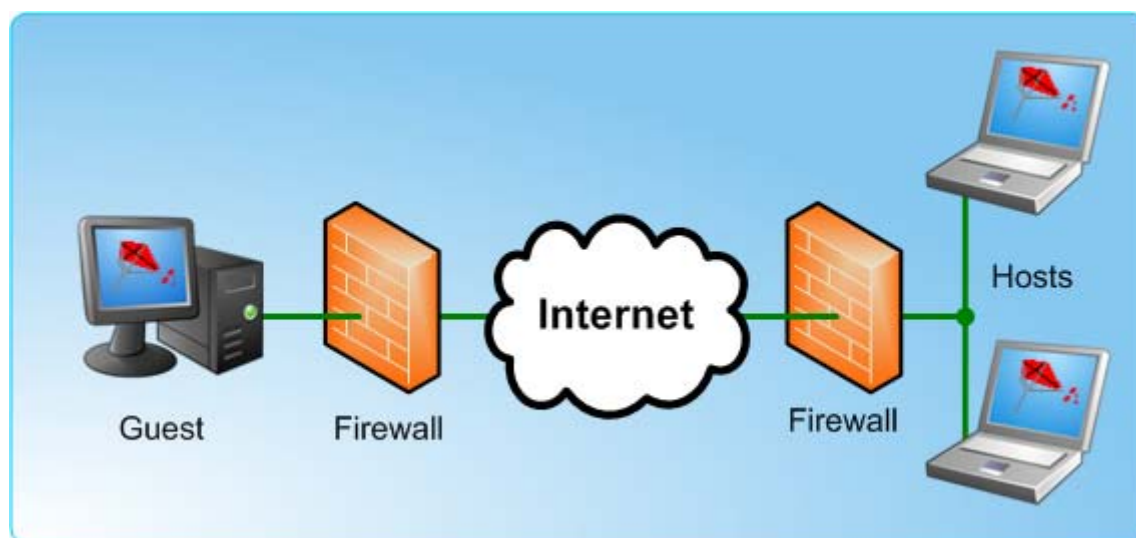
There are many ways that unauthorized people can gain access to your confidential information and business data on your computer. For example, hackers can use foot printing, which involves gathering information about a potential target. Examples of foot printing are port scans, ping sweeps, and NetBIOS enumeration that can be used by attackers to glean valuable system-level information to help prepare for more significant attacks. The type of information potentially revealed by foot printing includes account details, operating system and other software versions, server names, and database schema details.

Another method that can be used to hack into your computer system is scanning. Scanning involves searching IP networks for open ports with port scanners or searching telephone

systems for enabled modems with a dialer program. Hackers can attempt to crack a password, either online or offline—the latter option requires a copy of the account database. They can also try wire tapping, which involves using a protocol analyzer to search for session data containing useful information.

Finally, hackers can attempt to hijack a session, that is, they can try to takeover one end of an already established session or they can attempt to send invalid packets to a remote computer to either bring it down or change the contents of the memory, for example, to allow access without authentication (this procedure is called buffer overflow).

Secure remote control

It is essential that your remote control program contain security features that counteract the methods described to hack into a computer. NetOp Remote Control solves these security threats with a security strategy that in essence does not trust the Guest computer. NetOp security controls the access of NetOp Hosts by NetOp Guests and it can be managed locally by each Host or centrally administrated by NetOp Security Management.

NetOp Remote Control contains security features that:

- Secure the Host computer against unauthorized access across the wire.
- Support the need for minimal physical access to server rooms.
- Protect the traffic between NetOp modules against eavesdropping and unauthorized alteration of data.
- Run the Host components in proper security contexts on the operating system.
- Prevent unauthorized change of the Host configuration.
- Provide a broad range of security policies and alerting options.
- Offer extensive event logging.

These security features are described in more detail in the following sections.

Securing the Host from unauthorized access

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

MAC/IP address check

One of the best ways to ensure security is to restrict connections from outside an organization. With a **MAC/IP Address Check** feature, the Host computer can restrict connections with Guests to only those whose addresses appear in a predefined list.

The Host can filter the Guest addresses it communicates with based on:
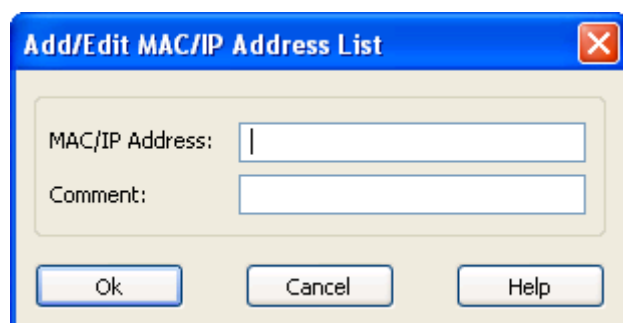
When this feature is enabled, the Host only communicates with Guest computers if their addresses are listed in the predefined list. This feature is designed to use the original MAC/IP address (or the NAT address) of the Guest.

Closed user group

Additional protection of the Host can be applied by using Closed user group serial numbers, which in the initial connection handshake reject intruders using Guest modules with normal retail or trial serial numbers.

Authentication

Authentication is required each time a Guest attempts to connect to a Host computer. Any remote control application should be able to integrate with the current authentication scheme that is deployed across your private network, whether it is a Windows Domain, LDAP server, or RSA SecurID server. The reason why it should support multiple authentication schemes, including one that can stand alone independent of what is available on the network, is to avoid recreating users' accounts that already exist on the network just for your remote control solution and to avoid incompatibilities between operating systems.

Authentication ensures that each user is authorized, not just the computer attempting the connection. Otherwise, if an attacker were to somehow break into a Guest computer, they'd be able to connect to any Host computer that the Guest was authorized to access at some previous point in time.

Authentication is the process of verifying the identity of a user based on a set of logon credentials. There are two types of authentication: local authentication and centralized authentication. Local authentication means that identity information is available in a database on each Host computer and centralized authentication means that identity information is available in a database on a shared remote computer.

Local authentication

When authentication is done locally, identity information is available in a database on each Host computer. A default password can be set up for all Guest users (Shared NetOp), or alternatively you can set up individual Guest IDs and passwords for each Guest user (Individual NetOp).

You can also authenticate each Guest against the local Windows user database using Windows user name, password, and the local computer name.

Centralized authentication

NetOp Remote Control offers a totally centralized security regime using the Windows NT SAM database, Microsoft Active Directory, Directory Services via LDAP, or NetOp Security Server.

For example, using Microsoft Active Directory each Guest is authenticated against Windows 2000 or Server 2003 Active Directory Service. And using Windows NT SAM database, each Guest is authenticated against Windows NT Security Account Manager database.

Authenticating users against a Directory Service via LDAP is an open design, which allows compatibility with all directory services. There are default configurations for Microsoft Active Directory, Novell eDirectory, Novell NDS, Netscape Directory Server, iPlanet Directory Server, and Sun ONE Directory Server.

NetOp Security Server

The NetOp Security Server is a special Host module that can answer queries from other NetOp modules about session permissions and rights across a network connection by forwarding queries to the ODBC database. The program must have access to the ODBC database containing security relations between the Guests and the Hosts. The NetOp Security Manager configures how the NetOp Security Servers operate in your network. It is a database client program that can edit information in an ODBC database of your choice. The database is input to the NetOp Security Servers, and it is from this information the Security Servers allow or deny NetOp Guests access to NetOp Hosts. The NetOp Security Manager must run on a Windows XP, 2000, or NT 4.0 platform for full functionality.
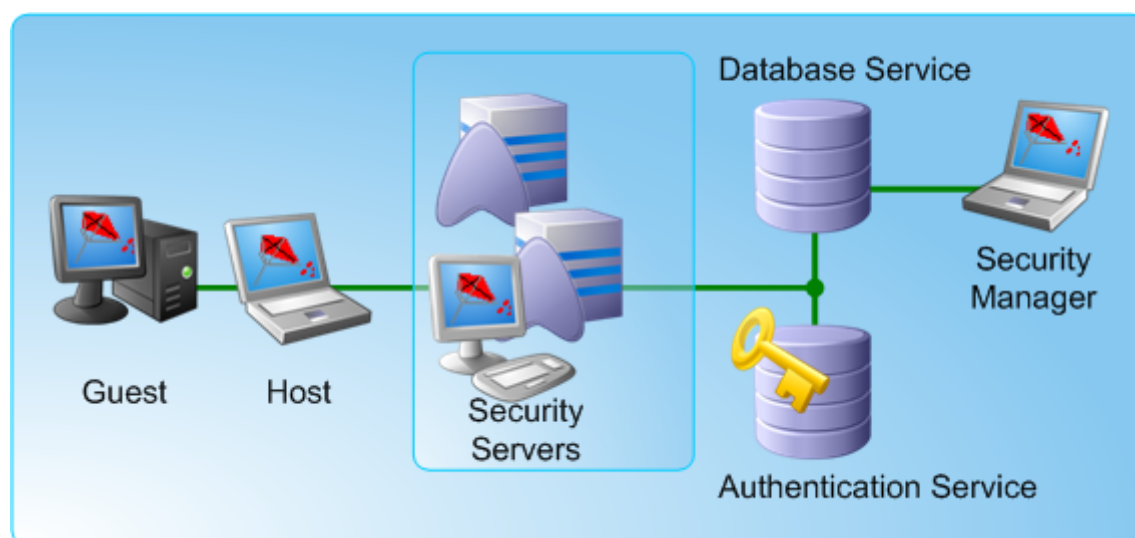

Using the NetOp Security Server the system can authenticate the Guest identity against NetOp, Windows, Directory Services, Smart Card or RSA SecurID Authentication Services. Multiple servers can provide fault-tolerance and load balancing, so it is preferable to use more than one NetOp Security Server.

To achieve NetOp authentication the NetOp Security Server verifies the Guest identity against the database service that holds all the predefined Guest IDs and passwords. To achieve Windows authentication the NetOp Security Server verifies the Guest identity by letting the Host relay the authentication process to the Windows Domain controller. Directory Service Authentication via the security server involves the NetOp Security Server verifying the Guest identity against a Directory Service via LDAP.

Smart Card authentication

With Smart Card authentication the Guest user login credentials are provided by a Smart Card inserted into a Smart Card reader on the Guest PC. Along with the Smart Card the Guest user must enter a corresponding PIN code. The Smart Card identifies the user that logs on and hence derives the access privileges to the Host PC.
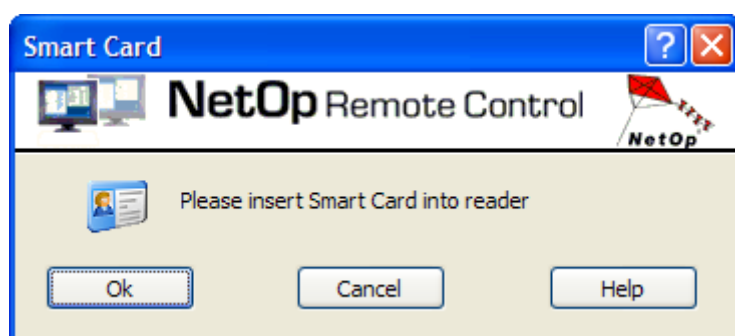
The Host can be setup to require logon with a Smart Card, but if the Guest user doesn't have a Smart Card, the Host can be setup to fall back to authentication based on Windows credentials (Username, Password and Domain) as well.

Two-factor authentication

RSA SecurID authentication via the Security Server means that the NetOp Security Server verifies the Guest identity against an RSA ACE/Server via an RSA ACE/Agent installed on the Security Server using a user name and passcode.

Both methods are known as two-factor authentication.

Triple-factor authentication

RSA SecurID with "triple-factor" authentication via the security server means that the NetOp Security Server combines RSA SecurID two-factor authentication with a shadow NetOp Guest ID password. The advantage of this is that you get even greater protection against attempts to crack the system. By having two independent authentication systems administrated by different staff, fraud committed by internal staff capable of stealing an RSA token-generator and resetting the matching RSA SecurID PIN code becomes even more unlikely.

Callback

Once the Guest user has been authenticated, the next step in the security process is to control access to the Host computer depending on the location of the authenticated Guest user. This is done through a callback feature, which can be used with a modem, ISDN, or TCP and it depends on the authenticated identity of the Guest.
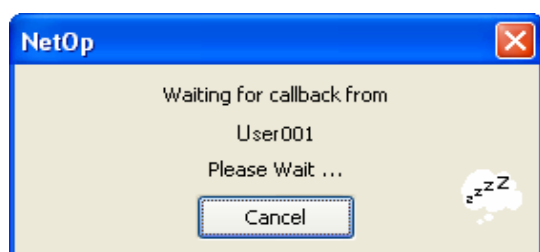

You can set up this feature to call back to a fixed address or to a Guest controlled address, which is known as roving callback.

Even though a Guest passes the authentication process, the callback feature forces the Guest user to be at a specific location and thus introduces another obstacle to prevent intruders.

User controlled access

The next access criteria that the Guest is forced to meet is via the Host user. The Host user can allow or deny an access request and therefore manually control access to the Host computer.
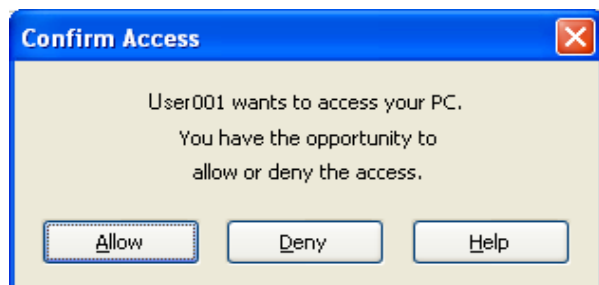

There is an option to bypass the **Confirm Access** dialogue box, if no user is logged on to the computer. With NetOp Remote Control, you can also customize the message that appears on the Host computer.

Authorization

The final access criteria that the Guest is forced to meet is called authorization. This is the process of determining which actions are allowed for an authenticated user. Authorization can be done locally or centrally using security roles. A security role is a group of allowed actions. You can set different security roles limiting what Guest users can see or do on a Host computer depending on which role they are assigned. One or more groups and user accounts can be assigned to each security role. The total number of allowed actions is calculated by adding actions from each security role that the user has membership of. The Host user has to confirm access, if the Guest user is present in at least one security role. Security roles can be managed locally for all supported platforms or centrally via the NetOp Security.
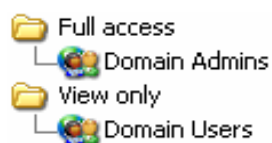

A NetOp Host can, from a security point of view, be handled either as a computer or as a logged on user. For Host users logging on to different computers, security roles based on the Host user identity work very well. You can also specify an individual computer as a Host, but this requires that you explicitly enter security roles for each and every computer into the database. Fortunately, you can add computers to computer groups in your Windows Domain.

If a Guest connects to a computer and no one is logged on to that computer, the Guest user obtains the accumulated rights that the Host computer and its group has. When you add a new computer to a group, it will automatically be subject to the same NetOp security procedures as all the other PCs in that group.

Local authorization

Local authorization means that information about security roles is available in a database on each Host computer. The NetOp Host must authorize the Guest's allowed actions against the local NetOp database that contains the security roles.
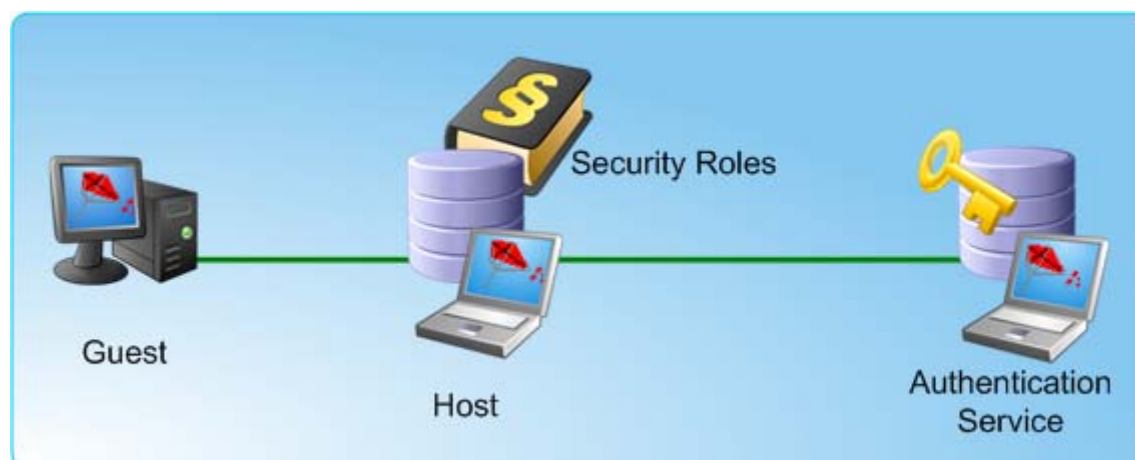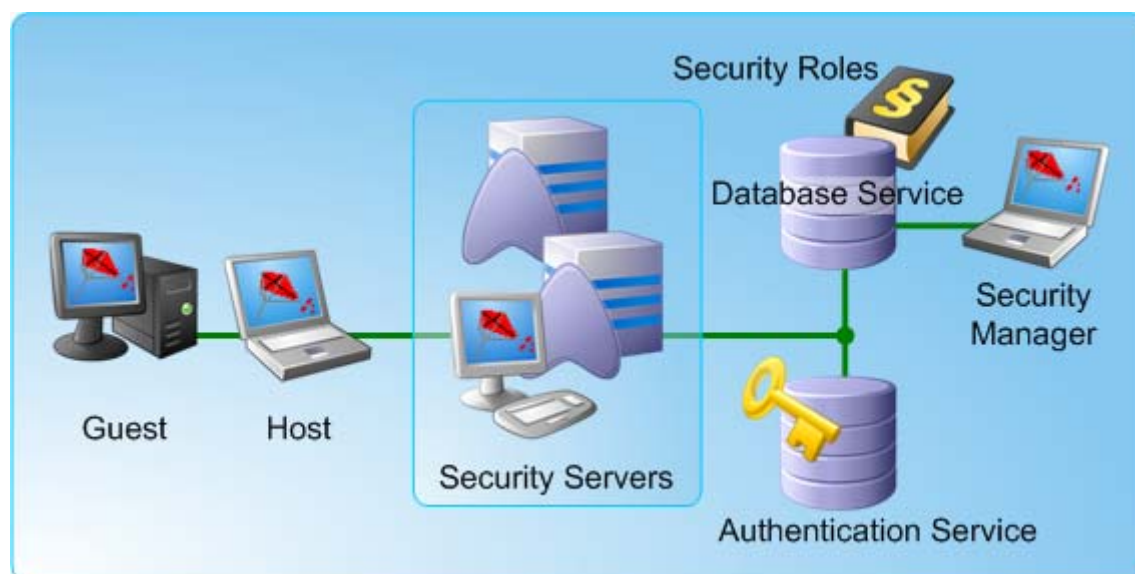
Local and centralized authentication services are used to check group membership to determine whether a user belongs to a security role or not. These include NetOp, Windows, or Directory Services Authentication Services.

Centralized authorization

Centralized authorization means that information about security roles is available in a database on a shared remote computer. Via the NetOp Security Server, the Guest's allowed actions are authorized against a centralized database service containing security roles.

Authentication services are often used to check group membership to determine whether a user belongs to a security role or not. This includes NetOp, Windows, Directory Services, Smart Card or RSA SecurID authentication services.

NetOp authorization via Security Server

By checking for membership of Guest ID groups at the database service, the NetOp Security Server controls allowed actions for the authenticated Guest user's identity.

Windows authorization via Security Server

By checking for membership of Windows Security Groups at a Windows Domain Controller, the NetOp Security Server controls allowed actions for the authenticated Guest user's identity.

Directory Services authorization via Security Server

By checking for membership of groups at a Directory Service, the NetOp Security Server controls allowed actions for the authenticated Guest user's identity.

RSA SecurID authorization via Security Server

By checking for membership of special groups at the database service, the NetOp Security Server controls allowed actions for the authenticated Guest user's identity. This is independent of any RSA ACE/Server groups.

Smart Card authorization via Security Server

By checking the user's Smart Card for membership of groups at the database service, the NetOp Security Server controls allowed actions for the authenticated Guest user identity.

System logon using Smart Card

In areas such as the financial sector a high level of security is imperative, as the servers are mission critical. So access to the servers needs to be highly restricted - physical access to server rooms needs to be kept to a minimum and only authorized personnel allowed limited access to the servers. This could be IT administrators who need to have access to the servers to be able to carry out maintenance work.

To prevent intruders from getting access to the system, a security policy requiring users to log on to the Windows operating system using a Smart Card can be defined. Normally, the user would need to be physically present at the local machine to apply the Smart Card. This obviously poses a problem, if access to the server room is limited and when using remote control for maintenance work.

The Security Server, which communicates with a Windows server, however, works around this problem by supporting system logon using Smart Card tunneling. This enables users such as IT administrators to log on locally to the Windows operating system of a remote Host machine by using a Smart Card and a Smart Card reader at the Guest machine. The Guest user's credentials are then tunneled from the Guest machine to the Windows operating system of the Host machine.

Protecting the traffic

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

- MAC/IP address check
- Closed user group
- Authentication
- Callback
- User controlled access
- Authorization
- IP address (TCP and UDP).
- MAC address (IPX and NetBIOS).

- Deny any communication with NetOp modules not using exactly the same Closed user group serial number.

- Prevent employees from using the modules outside the organization.

- Prevent access from outside the organization.

- 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 including NetOp 6.x/5.x compatible for communication with older NetOp modules.

- 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.

Using proper security contexts

The NetOp Helper Service ensures that proper security contexts are used when using remote control software. The NetOp Helper Service is responsible for launching the Host module and dynamically changes its security context. The service runs as a local system account and performs tasks such as installing the Web Update feature that requires administrator privileges to schedule the automatic download and installation of new build.

In terms of security contexts, the Host module runs as a very limited account (LocalService or anonymous) and impersonates the logged on user account, if any. All remote tasks, including file transfer, are performed in the logged on user's security context. Without a logged on user the limited account is used.

By running the impersonation scheme the NetOp Helper Service ensures that a Guest user cannot gain more rights than the logged on Host user has. If the Guest user needs additional rights, he or she can log off the Host desktop and log on again with a more privileged account.

Preventing unauthorized change of the Host configuration

The Host module has a maintenance password feature that can protect the password of the Host configuration under all platforms. This protects the Guest's access security and protects all other configurations.
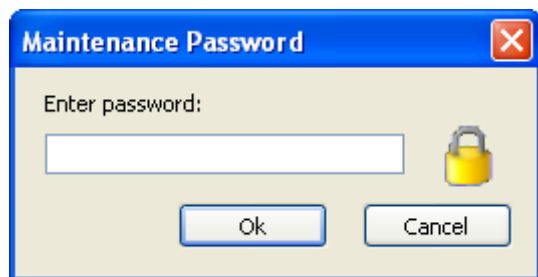
It also prevents the Host user from unloading the Host and stopping Host communication. It protects Host configuration files and ensures that the **Tools** menu commands are disabled when the Host is connected and when the Host is communicating.

Security policies and alerting options

There are a number of security policies in place that help to protect the remote control environment. For example, after exceeding the maximum number of invalid logon attempts, the Host can be configured to disconnect the Guest user or even restart Windows to reduce the number of invalid logon attempts per hour. After the Guest user has been disconnected from the Host, the Host computer can be configured to automatically lock the computer, log off Windows, or restart Windows. This ensures that physical access to the Host desktop is secured.

By default, the Windows system group 'Everyone' gives users access to most of the file system. To access the Host's NTFS based file system with the NetOp File Manager when no Host user is logged on, you must either secure the file system by following the recommendations from Microsoft or you must disable the ability of NetOp to transfer files before local logon. For file transfer sessions when a Host user has logged on, the Guest user operates with the logged on Host user's rights.

Remote control sessions can be recorded and saved for documentation or as security evidence to show what really took place during the session. Both the Guest and Host computer can record the session—for security reasons it is recommended to use the Host recording. The Guest configuration can, however, be configured to force recording on the Guest computer and even to disconnect if the recording fails.

A number of timeouts have been implemented to ensure high availability of the Host. During logon, the Guest user can be given a fixed amount of seconds to enter logon credentials. Without this feature an intruder could make a denial of service (DoS) attack by connecting to a number of Hosts without fulfilling the logon sequence. To make room for the next Guest, a period of inactivity will force the passive Guest user off.

For certain purposes the Host computer can be set up to run in Stealth mode. This means that the Host module is not displayed on the desktop or in the Task Manager's application list. It also means that the Host user will not be aware of the fact that the computer can be remote controlled.

Other security policies include keeping the Host name and logged-on user name private, which means that the Host does not respond to broadcast communication but only to direct connections.

Finally, list boxes, balloon tips, or tones can alert Host users when a Guest user is accessing their computer.
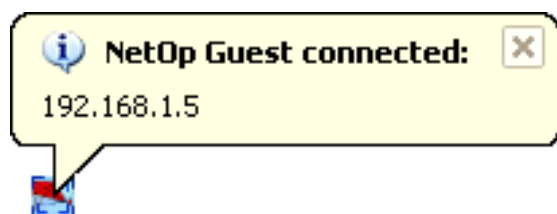
Host users can receive these optional connection notifications upon, during, or after connection.

Extensive event logging

Event logging records session activity and logon attempts and proves that your security settings are working. You can set up the best security system, but without any documentation of an attack that is in progress, you wander about in the dark.

NetOp Remote Control includes an extensive event-logging feature that enables you to log session activity and logon attempts to multiple logging destinations. These logging destinations include a local file (you can log NetOp events on the local computer), the NetOp Security Server (you can log NetOp events in the database of a central NetOp Security Server group), a Windows Event Log (you can log NetOp events to the local and remote Windows Event Log), and an SNMP enabled management console (you can log NetOp events by sending SNMP traps to a SNMP enabled central management console, such as HP OpenView). More than 100 NetOp events can be logged.

Business benefits of secure remote control

Complete, scalable, and secure remote control for IT professionals provides a number of business benefits. NetOp Remote Control:

- Improves business efficiency by minimizing down time for employees through the instantaneous helpdesk solution.

- Helps system administrators work easily from one location and connect directly to end users' computers, speeding up the ease and efficiency of technical solutions to software issues.

- Provides a protected connection—completely protected from unauthorized access, which is essential to the stability of an organization's network and a business's integrity.

- Reduces costs of IT departments and increases productivity; NetOp Remote Control has a proven track record of providing a fast ROI.

- Security configuration can be defined both decentrally and centrally.

- Provides a scalable solution that is suitable for many different companies; from small organizations with modest remote control and security needs up to very large organizations with 100,000 plus users and very high demands for security.

Conclusion

Protecting confidential information, such as business plans, marketing strategies, sales figures, or employee records from getting into the wrong hands, from being leaked, tampered with, or destroyed, is essential to the success of any organization.

Remote control applications can be very beneficial when providing high quality technical support. However, if the software lacks tight security features, a remote control application can jeopardize a company's crucial information, making it vulnerable to attack. Having enough security to ensure a protected connection and block out possible network intrusions is absolutely necessary when utilizing remote control software as a remote support solution.

When purchasing remote control software, security should be just as much of a deciding factor as platform support, speed, and usability features. A good remote control application will be well-rounded and stable; providing cross platform support, quick remote connections (over high bandwidth or dial-up), a number of usability features that improve the remote control process, and rock-solid security to protect all enterprise data and block attackers.

Who is Danware?

Danware's core business is to develop and market software products based on the NetOp® core technology—a technology that enables swift, secure, and seamless transfer of screens, sound, and data between two or more computers.

The company has two product lines, Desktop Management and Education. The core Desktop Management product, NetOp® Remote Control, enables remote control of one or more computers. NetOp® School, the core Education product, is a software solution for computer-based classroom teaching. All are Plug and Play products with extensive functionality, flexibility and user-friendliness.

Danware's products are sold in more than 80 countries, and in 2006 the turnover was approximately EUR 12.9 million. Danware's shares are listed on the Copenhagen Stock Exchange (name DANW) and are part of the SmallCap+ index. Danware has subsidiaries in the U.S.A., the UK, and Germany.

For further information, please see www.danware.com.