SECURITY PAPER

NETOP® Remote Control

A Technical Overview of Netop Remote Control Security

Netop Remote Control provides secure access and remote support to devices and end users. This technical paper details the modular structure of Netop Remote Control, the four pillars of security that represent Netop's remote access security strategy, and the multiple options for configuring security settings with Netop components. This paper also provides technical information on the architecture and multiple deployment options of Netop Remote Control.

Netop Remote Control is the choice of the world's largest retailers, financial institutions and manufacturers for secure remote access. Used by half of the Fortune 100, Netop's advanced logging, multi-factor authentication and customizable user rights make it ideal for installations where security and PCI compliance are concerns.

Table of Contents

1. Executive Summary

Netop Remote Control provides secure access and remote support to devices and end users. It is useful for technical support teams, customer service agents and network administrators.

The basic components of Netop Remote Control consist of two remote control software modules: The Guest installed on the technician's computer and the Host installed on the target machine. With Netop Security Server, organizations can manage permissions for hundreds to thousands of users while complying with security regulations and implemented policies.

In terms of connectivity, Netop Remote Control allows agents to connect to a device within the LAN/WAN or to connect from a remote location to a device within a LAN/WAN by using the Netop Gateway. It also enables agents to use a bridge when they want to exchange information or transfer files between different types of networks. In terms of vendor access, the Netop Portal and Netop WebConnect are provided as connectivity.

Netop Remote Control supports both physical and virtualized systems. Netop Remote Control can be run in RDS sessions and connect to other Netop Remote Control modules running in sessions on the same RDS, another RDS, or other networked computers.

The security is achieved through multiple modules and components working together. The four key principles are:

- **Encrypt the line.** Sensitive information is encrypted during transmission over networks to avoid being accessed by malicious individuals.
- **Manage user access.** Netop principles for authentication are primarily based on end-point authentication, e.g. users will be authenticated on each end-point for each session. Netop offers several different user authentication methods.
- **Manage user permissions.** Access to sensitive data is restricted by business need to know. Access privileges can be done locally or centrally using security roles.
- **Document what happens.** Netop Remote Control provides a comprehensive audit trail including logging and recording what happened at any given time and who performed the action during a particular secure remote session.

Netop Remote Control modules and components are highly configurable allowing organizations to balance security needs with performance. They include options for centralization and Internet connectivity and can be hosted by Netop or the customer. Netop has created a flexible and secure IT infrastructure using the Amazon Cloud, which is compliant with the IT security, quality and industry specific standards.

2. Netop Remote Control Modules

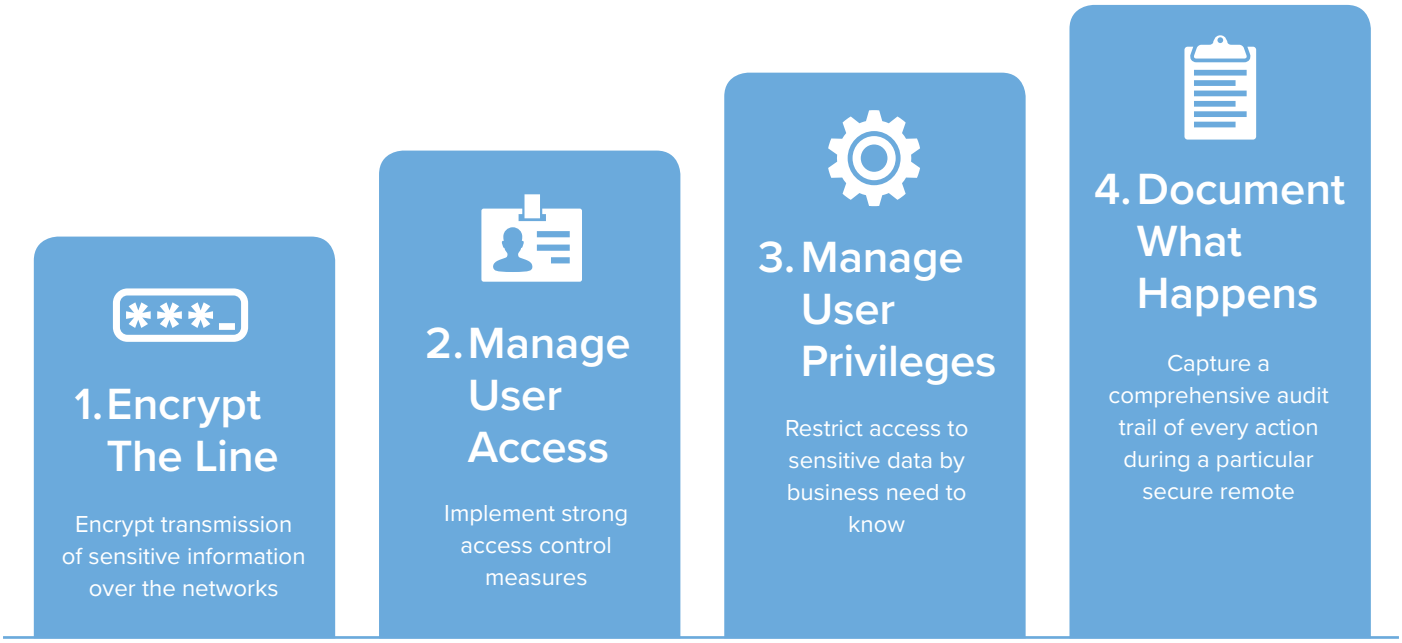
The basic components of Netop Remote Control consist of two remote control software modules: the Guest installed on the technician's computer and the Host installed on the target machine.

Along with the Guest and Host components, Netop Remote Control offers a cloud portal for remotely connecting to users' systems and – if you don't want to rely on a third party to host the support sessions – you can do it all yourself with the Netop WebConnect module.

Netop Remote Control comprises the following modules:

Netop Guest	Allows workers to remotely access and support any machine running a Host module.
Netop Host	Enables the computer to be remote controlled and interacted with from a computer running a Netop Guest or the Netop Portal or through the Netop Remote Control Portal's browser based support console.
Netop WebConnect	A secure web-based service consisting of a Connection Manager that serves as a meeting hub for Netop Guests and Hosts, and at least one Connection Server that routes the traffic between Guests and Hosts. The Connection Server is an extended Host. This is available as a hosted service or as an on premise application.
Netop Portal	A browser-based interface allowing the users to manage Guest authentication and authorization, view connected devices and do remote sessions using a lightweight support console which does not require any kind of installation.
Netop Browser Based Support Console	A browser based interface allowing the supporters to remote control devices, no install required.
Netop Security Server	A centralized authentication server for Hosts. Additionally used as a centralized log server for activity from Host and Guest. Security Server consists of two components. The Security Server module is the engine that runs, listens and processes authentication requests from a Host. The Security Manager is only an interface to edit security roles and role assignments in the database. The Security Manager also allows you to view activity logs stored in the database.
Netop Gateway	Bridges and routes Netop traffic across different communication protocols and networks. Netop Gateway can receive Netop communication that uses one communication protocol and send it using another communication protocol. This ability enables Netop Gateway to provide communication between Netop modules that use mutually incompatible communication devices, typically to connect Netop modules inside a network or Remote Desktop Service environment with Netop modules outside a network or remote desktop service environment.

3. Four Pillars of Security



3.1 Pillar of Security #1: Encrypt the line

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to card holder data environments.

3.1.1. Guest to Host Encryption Options

There are several ways how information moving between the Netop 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.
- **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.

"Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit." – PCI Guidance (PCI DSS Requirement 4.1)

Communicating Netop modules will automatically negotiate to encrypt communication by an encryption type that is enabled on both modules. Netop modules on which no common encryption type is enabled cannot communicate.

3.1.1.1. Very High

Description	Everything is encrypted with 256-bit keys
Scope	Use for communication in environments where security is important and speed is not a major issue.
Encryption	Keyboard and mouse: 256-bit AES Screen and other data: 256-bit AES Logon and password: 256-bit AES
Integrity Check	Keyboard, mouse: 256-bit SHA HMACs Screen and other data: 256-bit SHA HMACs Logon and password: 256-bit SHA HMACs
Key Exchange	Combination of 1024 bits Diffie-Hellman, 256-bit AES and 256-bit SHA.

3.1.1.2 High

Description	All transmitted data is encrypted with 128 bit keys. Keystrokes, mouse clicks and password details are encrypted with 256-bit keys.
Scope	Use for communication in environments where security is important, but speed cannot be ignored.
Encryption	Keyboard and mouse: 256-bit AES Screen and other data: 256-bit AES Logon and password: 256-bit AES
Integrity Check	Keyboard, mouse: 256-bit SHA HMACs Screen and other data: 160-bit SHA HMACs Logon and password: 256-bit SHA HMACs
Key Exchange	Combination of 1024 bits Diffie-Hellman, 256-bit AES and 256-bit SHA.

3.1.1.3 Data Integrity

Description	Data is protected from being changed in transit.
Scope	Use for communication in environments where encryption is prohibited except for authentication.
Encryption	Keyboard and mouse: None Screen and other data: None Logon and password: None
Integrity Check	Keyboard, mouse: 256-bit SHA HMACs Screen and other data: 160-bit SHA HMACs Logon and password: 256-bit SHA HMACs
Key Exchange	Combination of 1024 bits Diffie-Hellman and 256-bit SHA hashes.

3.1.1.4 Data Integrity & Keyboard

Description	Data is protected from being changed in transit and only keystrokes, logon and password details are encrypted.
Scope	Use for communication in environments where speed is important, but you require data integrity check and keystrokes / password details must be encrypted.
Encryption	Keyboard and mouse: 256-bit AES Screen and other data: None Logon and password: 256-bit AES
Integrity Check	Keyboard, mouse: 256-bit SHA HMACs Screen and other data: 160-bit SHA HMACs Logon and password: 256-bit SHA HMACs
Key Exchange	Combination of 1024 bits Diffie-Hellman, 256-bit AES and 256-bit SHA.

3.1.1.5 Keyboard

Description	Only keystrokes, logon and password are encrypted.
Scope	Use for communication in environments where speed is important, but keystrokes and password details must be encrypted.
Encryption	Keyboard and mouse: 256-bit AES Screen and other data: none Logon and password: 256-bit AES
Integrity Check	Keyboard, mouse: 256-bit SHA HMACs Screen and other data: none Logon and password: 256-bit SHA HMACs
Key Exchange	Combination of 1024 bits Diffie-Hellman, 256-bit AES and 256-bit SHA.

3.1.1.6 Netop 6.x/5.x Compatible

Description	Compatibility mode for communication with Netop version 6.x, 5.x and 4.x.
Scope	Use for communication in environments where speed and backwards compatibility are important.
Encryption	Keyboard and mouse: proprietary algorithm Screen and other data: none Logon and password: proprietary algorithm
Integrity Check	Keyboard, mouse: none Screen and other data: none Logon and password: none
Key Exchange	Proprietary algorithm

3.1.2. Netop WebConnect Encryption

WebConnect is a Netop proprietary communication device that enables networked Netop modules to connect easily over the Internet through a Netop connection service called WebConnect without the need to open firewalls for incoming traffic. All traffic will be outbound.

When you use WebConnect, you no longer need to configure and maintain VPNs to support users outside of your network or to provide external access by consultants.

To establish identity and trust between the web browser and Netop WebConnect, the connection is secured via SSL/TLS certificates issued by GlobalSign Domain Validation CA - SHA256 - G2 and ciphers according to security best practices.

Netop WebConnect certificates are provisioned and managed using AWS Certificate Manager in order to be deployed on AWS resources such as Elastic Load Balancer at different applications levels: Netop WebConnect Service and Connection Manager.

3.1.3. Netop Portal Encryption

Netop Portal is a service that provides connectivity across the Internet. It does not require direct visibility between end points, no need to open firewalls for incoming traffic. All traffic will be outbound.

To establish identity and trust between the Netop Portal and the web browser, the connection is secured via TLS certificates issued by Amazon.

Encrypted keys for encrypted data transmissions are exchanged using RSA 2048 bits and SHA256 - G2.

TLS 1.0 - 1.2 is used to authenticate servers and clients and then SSL-secured communication can begin between the server and the client using the symmetric encryption keys that are established during the authentication process.

Netop Portal certificates are provisioned and managed using AWS Certificate Manager in order to be deployed on AWS resources such as Elastic Load Balancer at different applications levels: Netop Portal, Netop Authentication Service and Connection Manager.

For peer-to-peer connections Netop Portal certificates are issued by GlobalSign Domain Validation CA - SHA256 - G2 and ciphers according to security best practices.

Data at rest is encrypted using the industry standard AES-256 encryption algorithm.

3.1.4. Host Communication Profile Encryption (Web communication profile)

Encrypted keys for encrypted data transmissions are exchanged using 2048-bit RSA or 256-bit ECDSA private keys

TLS 1.1 or higher is used to authenticate servers and clients and then SSL-secured communication can begin between the server and the client using the symmetric encryption keys that are established during the authentication process.

Modern ciphers are preferred (AES), modes (GCM). AES-256 is preferred over AES-128 (except for GCM which is preferred over everything else).

3.2. Pillar of Security #2: Manage user access

Netop principles for authentication are primarily based on end-point authentication, e.g. users will be authenticated on each end-point for each session. Netop offers several different user authentication methods.

The Guest Access Security functions of the Host can protect against unauthorized access and limit the actions available to the Guest:

- Upon connection to the Host, the Guest can be authenticated against their Windows login credentials.
- Security roles can be defined on the Host which dictate what remote control actions the authenticated Guest can perform.
- The policy functions can determine how the Host behaves before, during and after the remote control session, including notification, confirm access and illegal connection attempts.

Authentication is required each time a Guest attempts to connect to a Host computer.

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.

Netop Remote Control provides proprietary authentication options for instances when admins don't want to add a user to a network domain structure or for admins working in mixed environments where admins can select from different authentication schemes based on their needs: Portal, Netop Security Server, Windows Domain, LDAP server, RSA SecurID server or RADIUS-based authentication systems.

The reason 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.

For details on the Guest Access Security and guest policies, see the Netop Remote Control User's Guide, section 5.2.4 Guest Access Security.

Authentication is the process of verifying the identity of a user based on a set of login 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.

3.2.1. Guest access methods

Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.

> *"Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism."* – PCI Guidance (PCI DSS Requirement 8.6)

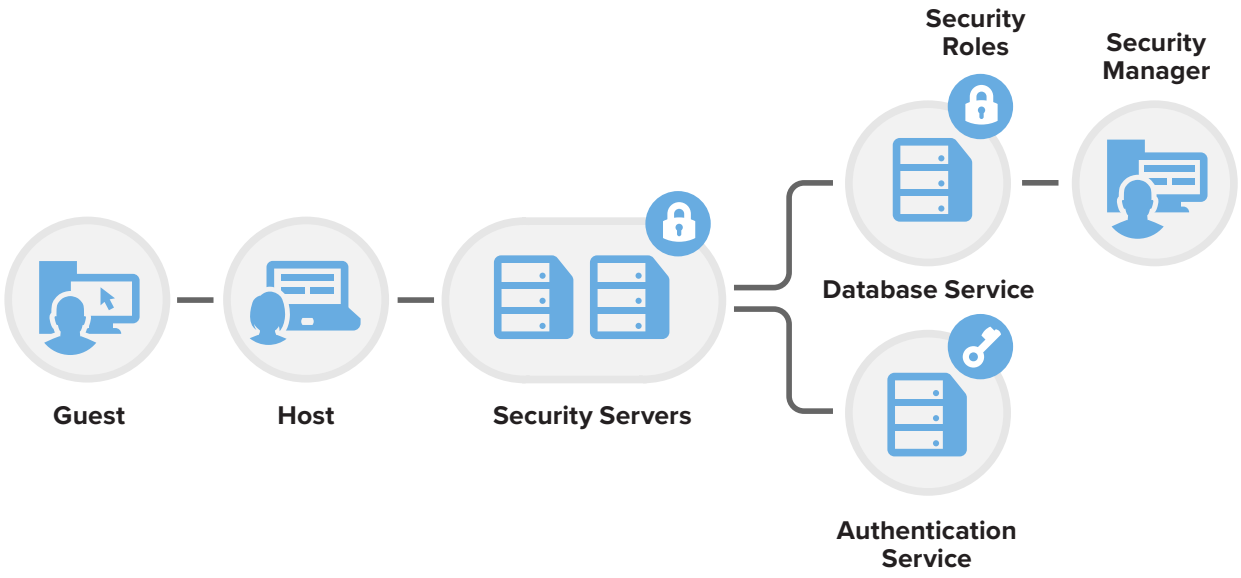
3.2.2.1. Smart Cards

Highly secure environments like governments request the use of Smart Card authentication as the primary method of accessing their information systems.

Smart cards help to eliminate the threat of hackers stealing stored or transmitted information from a computer. The information is processed on the smart card, so it never has to leave the card or be transmitted to another machine.

By using a Smart Card and reader at the Guest machine, the Guest credentials can be authenticated against a Microsoft CA environment. Secure tunneling also allows the Guest user to login remotely to the Host machine using their Smart Card credentials.

For information on how to configure Netop Remote Control to use smart card authentication, either by working with Netop Security Server or directly on the Netop Host, see Netop Remote Control Smart card Integration.

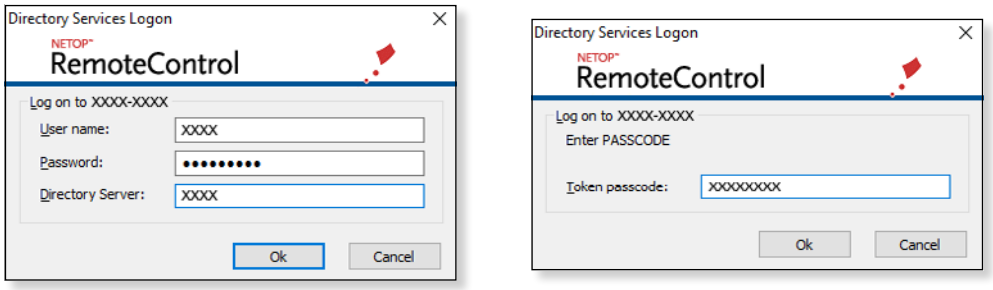


3.2.2.2. Multi-factor authentication

To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer.

Two-factor authentication requires two forms of authentication for higher-risk accesses, such as those originating from outside the network.

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 pass code. This is also known as two-factor authentication.



The Guest's access to the Host is thus validated based on two-factors:

- Something the user knows (credentials)
- Something the user has (pass code received by phone or E-mail).

Netop Remote Control offers extended security with Windows Azure and Remote Authentication Dial-In User Service (RADIUS) multi-factor authentication.

Authentication against RADIUS

RADIUS is a client/server protocol that is often used to centrally validate remote users and authorize their access to existing network resources integrating well with existing technologies including VPN, RAS, Active Directory and Token based authentication solutions.

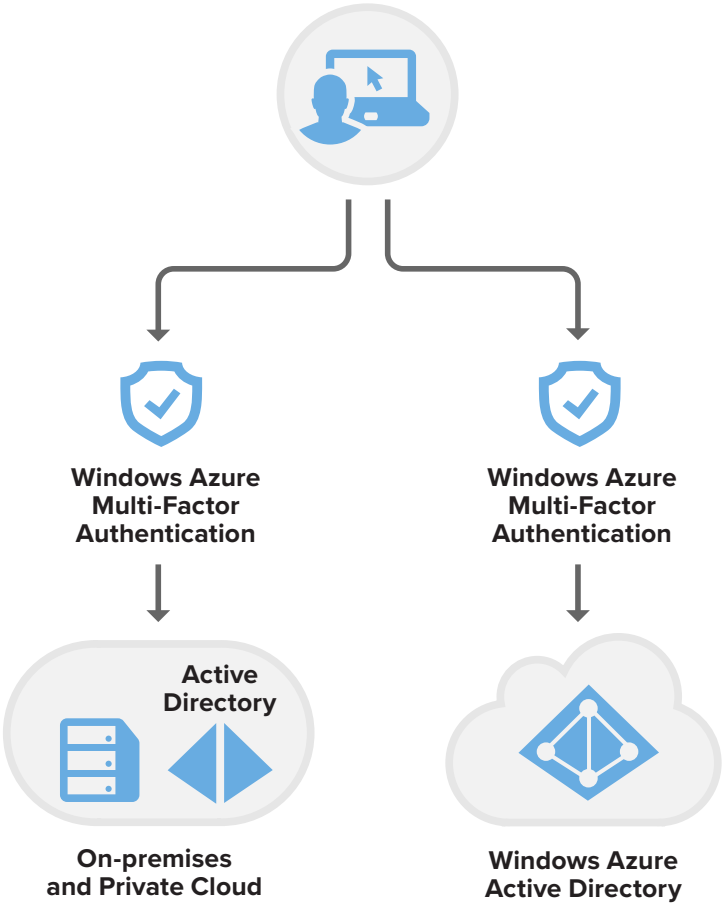
Using RADIUS with Netop Remote Control allows the Security Server to authenticate remote support sessions via compatible multi-factor authentication methods, where the Guest user needs to provide their user name and password initially, followed by a one-time generated pass code that can be derived from a variety of sources including hardware devices or SMS tokens.

For information on how to configure the Guest and Host for RADIUS authentication, see Multi-factor Authentication using Radius.

Windows Azure Multi-Factor Authentication

Windows Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra level of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.

Netop Remote Control provides integration to this service. Companies can use their own Windows Azure Multi-Factor Authentication in Netop Remote Control.



Source: http://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/

For information on how to retrieve the Microsoft Azure information, how to configure and connect to the Host, see Windows Azure Multi-Factor Authentication.

3.2.2.3. 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 using Windows user name, password, and the local computer name.

3.2.2.4. Centralized Authentication

Netop Remote Control offers a totally centralized security regime using the Windows NT SAM database, Microsoft Active Directory, Directory Services via LDAP, Netop Portal 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 Authentication

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.

Using the Netop Security Server the system can authenticate the Guest identity against Netop, Windows (via the Host), Directory Services, 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.

Netop Portal Authentication

Netop Portal services Host requests for Guest Roles with themselves by managing user authentication, querying the central security database for security data, determining the applicable Role and returning the associated access permissions to the Host to apply them.

Besides the user management provided by the Netop Portal, you can choose to integrate the Portal with AD FS or LDAP and apply multi-factor authentication on top of the integration of your choice.

Multi-factor authentication on top of the AD FS authentication

Active Directory Federation Services (AD FS) is a technology that extends your Active Directory configuration to services outside of your infrastructure.

This integration is particularly relevant for scenarios when third party vendors need to get access to devices. It provides a central place to manage and audit the identity information of the users who will be using the Netop Portal.

Instead of manually filling in information for every user, the AD FS integration will allows using data from the company's user store (Single-Sign On authentication extending enterprise identity beyond the firewall). This also means that data from the Netop Portal is synced with the company's data on every user login (name and email). services outside of your infrastructure.

With AD FS, you can give users access to the Netop Portal without them having to manage another set of credentials. The users logging in the Portal will be able to use the same credentials they are already using in the various company applications (e.g. email, computer login). This will mean that the password rules will be the same as the ones for the company. For detailed information on how to configure and use the ADFS integration in the Netop Portal, read this article.

Multi-factor authentication can be added on top of the existing AD FS authentication, thus increasing the overall solution security. For information on how to use the Portal multi-factor authentication, see the Netop Portal User's Guide.

Multi-factor authentication on top of the Lightweight Directory Access Protocol (LDAP) integration

The LDAP integration is relevant for scenarios when your technicians need to get access to devices. It allows you to authenticate them on your Active Directory network.

With LDAP, you can give users access to the Netop Portal by this username format: domain identifier\LDAP username and the domain password.

For security reasons, we use the LDAPS over the Internet to have an encrypted channel between the Netop Portal and the DCs. No passwords are stored in the Netop Portal and they will be checked on every login over an encrypted channel.

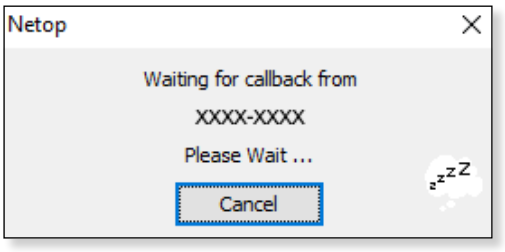
For information on how to set up an LDAPS over the Internet and how to configure it in the Portal, see this article.

Multi-factor authentication can be added on top of the existing LDAPS authentication, thus increasing the overall solution security. For information on how to use the Portal multi-factor authentication, see the Netop Portal User's Guide, section 3.1 Enable Multi-Factor authentication.

Besides the traditional authentication methods, Netop Remote Control offers extensive authentication such as: callback, user controlled access, MAC/IP address checks and Closed User Groups.

3.2.2. 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.



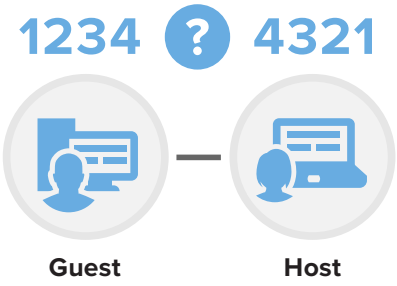
You can set up this feature to call back to a fixed address or to a Guest controlled address, which is known as roving callback.

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.

3.2.3. Closed User Groups

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 retail or trial serial numbers.

With closed user groups, companies can obtain a custom serial number to the software used by service desk representatives and target devices. Then, only in situations when the serial number of the service desk representative's machine matches that of the target device can a connection between the devices be established. Other attempts will automatically be rejected.

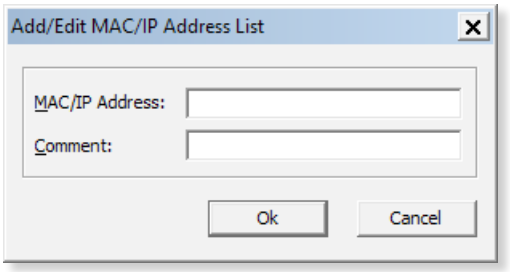


3.2.4. MAC/IP address checks

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

- IP addresses (TCP and UDP)
- MAC addresses (IPX and NetBIOS).

The Host can filter the Guest addresses it communicates with based on:



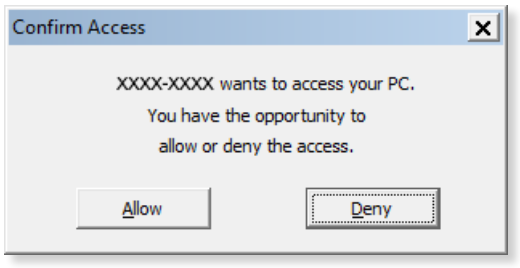
When this feature is enabled, the Host only communicates with Guest computers if their addresses are listed in the predefined list. This feature is designed to use the original MAC/IP address (or the NAT address) of the Guest.

3.2.5. User controlled access

Netop offers the option to allow end users the rights to control whether or not external staff should be permitted to connect to their system.

The Host user can allow or deny an access request and therefore manually control access to the Host computer.

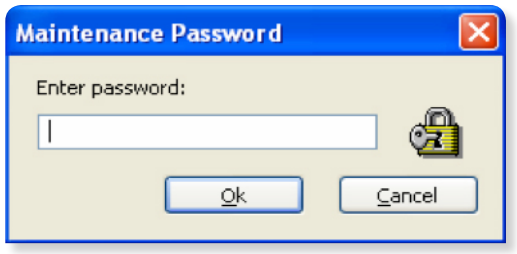
This is done by using a “Confirm Access” where user confirmation / interaction is required before active sessions can be started, where end user actively needs to confirm access before any user are allowed in.



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

3.2.6. Tamper proofing 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.

3.3. Pillar of Security #3: Manage Access Privileges

The final access criteria that the Guest is forced to meet is called access privileges. This is the process of determining which actions are allowed for an authenticated user. Access privileges 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.

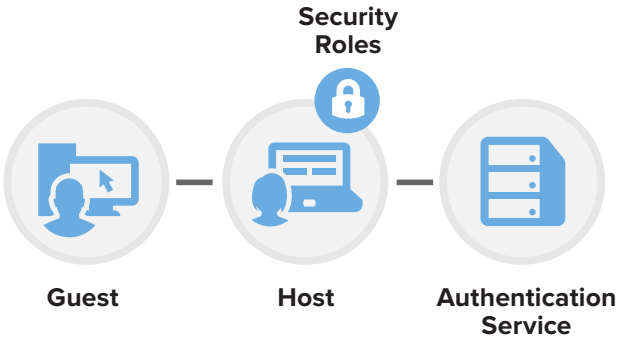
The Host user has to confirm access if the Guest user is present in at least one security role. Security roles can be managed locally for all supported platforms or centrally via the Netop Security Server or via the Netop Portal.

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.

3.3.1. Local Access Privileges

Local access privileges 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.



It also prevents the Host user from unloading the Host and stopping Host communication. 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.

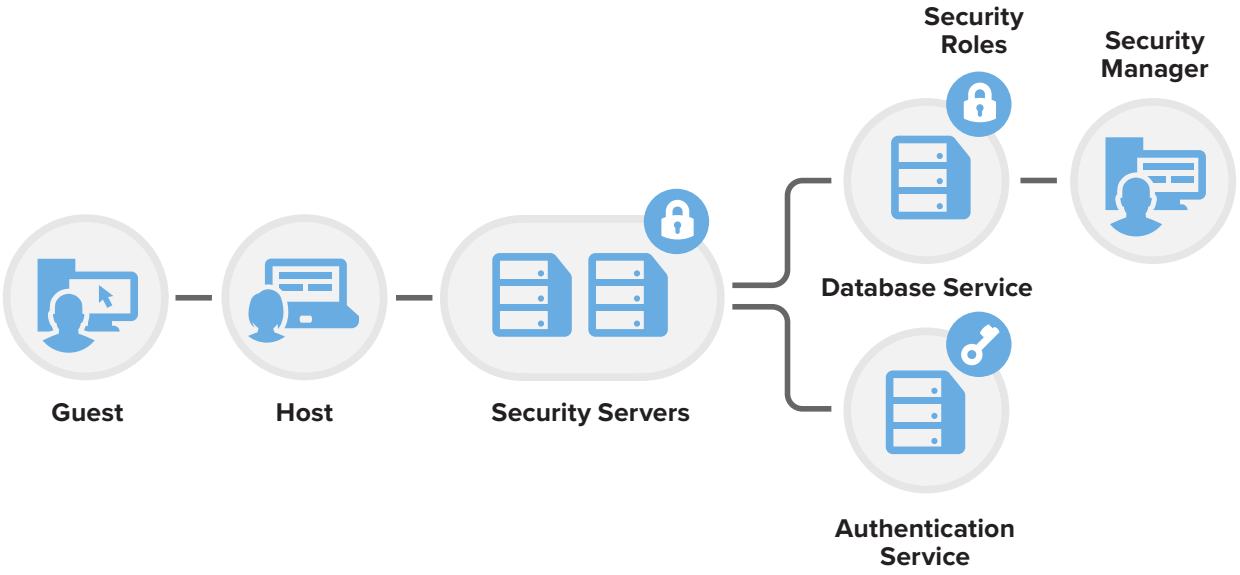
3.3.2. Centralized Access Privileges

Centralized authorization means that information about security roles is available in a database on a shared remote computer

3.3.2.1. Netop Security Server centralized authentication and access privileges

Via the Netop Security Server, the Guest's allowed actions are authorized against a centralized database service containing security roles. Netop Security Server supports connection to several types of database services: Oracle, MS SQL Server, MS Access and DB2.

Once the authentication process has taken place and the Guest credentials have been validated against the Host, the accumulated access privileges are assigned to the Guest for that remote support session. These permissions can be easily managed using the Security Manager and offers great flexibility with different levels of control depending on the Guest users' role within the organization protects Host configuration files and ensures that the Tools menu commands are disabled when the Host is connected and when the Host is communicating.



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, or RSA SecurID authentication services.

Netop Access Privileges via Security Server

By checking for membership of Guest ID groups at the database service (Oracle, MS SQL Server, MS Access or DB2), the Netop Security Server controls allowed actions for the authenticated Guest identity.

Windows Access Privileges 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 identity.

Directory Services Access Privileges via Security Server

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

RSA SecurID Access Privileges 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 identity. This is independent of any RSA ACE/Server groups.

Smart Card Access Privileges

By checking the user's Smart Card for membership of groups at the database service (Oracle, MS SQL Server, MS Access or DB2), the Netop Security Server controls allowed actions for the authenticated Guest user identity.

3.3.2.2. Netop Portal centralized authentication and authorization

The Host will use Netop Portal to authenticate each connecting Guest and assign permissions to it.

Centralized authorization means that access permissions for each remote support session can be defined using security roles via the Netop Portal. These permissions can be easily managed using the Netop Portal and offers great flexibility with different levels of control depending on the Guest users' role within the organization.

Roles are a set of permissions which can be applied to a group of users through Role Assignments.

The permissions defined by roles are applied to users and devices through role assignments. A role assignment is comprised of a role, a group of users (Supporters), and a group of devices. User groups (also known as Supporter Groups) and device groups must be created before new role assignments.

Once the authentication process has taken place and the Guest credentials have been validated against the Host, the accumulated access privileges are assigned to the Guest for that remote support session.

3.4. Pillar of Security #4: Document what happens

Netop Remote Control provides a comprehensive audit trail including logging and recording what happened at any given time and who performed the action during a particular secure remote session. Thus your records are complete, and no unauthorized activity can take place without your knowledge.

The Netop Remote Control Host and Guest have a variety of options for logging Netop activity. Session and connection events as well as action, security and a variety of configuration changes to the module can be sent to the Netop log. Each log has a corresponding code to indicate the intent of the log.

Interpreting log data event codes requires the use of the Netop Remote Control User Guide. Event codes and their definitions can be found in Netop Remote Control User's Guide, section 5.1.15 Log Setup subsection "Available Netop log event codes and arguments".

You can customize logs to meet the needs of your organization by using environmental variables and specific machine settings.

You can customize information for the Host name and Guest name using the following parameters:

Host name

- %A - IP address
- %L - User name of the user under which the Host process runs
- %I - Host ID
- %C - Computer name

Guest name

- %A - IP address
- %U - Authenticated user name (when authenticated against the Host to get access. If Netop authentication is used, the value is replaced with the Guest ID.)
- %I - Guest ID
- %C - Guest computer name
- %L - Logged on user

The Host for Mac and Linux provides capabilities for creating a dynamic Host ID. This is done by adding new options to the Hostname when Naming mode is set to "Enter name or leave blank":

- Environment variables (E.g.: %my-variable%)
- Machine specific settings by using:
  - %M% - mac address
  - %A% - IP address
  - %L% - User name of the user under which the Host process runs
  - %C% - Computer name

3.4.1. Netop Logging

To support security functions, Netop Remote Control includes an extensive event-logging feature that enables you to log session activity and logon attempts to multiple logging destinations:

- In a Netop log on the local computer.
- In a local or a remote Windows Event Log
- In the database of a central Netop Security Server.
- In the Netop Portal
- In an Simple Network Management Protocol (SNMP) enabled management console (by sending SNMP traps to an SNMP enabled central management console),

For details on how to enable the Netop Remote Control Logging, see the Netop Remote Control User's guide, section 2.13 Log events.

For detailed information on which Netop log events are logged by the Guest and Host, see the Netop Remote Control User's guide, section 5.1.15 Log Setup, pages 96 to 108.

3.4.1.1. Local logging

The Netop Host and Guest have a variety of options for logging Netop activity. Session and connection events as well as a variety of configuration changes to the module can be sent to the Netop log.

By default the name of the log file is NETOP.LOG, if not otherwise specified during the log setup. If no path is specified during the logging setup, the log file is located in the Netop configuration files folder, typically C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>. UNC paths are not supported. Only mapped paths are supported.

A new local Netop log file that is created when the Netop module is loaded will overwrite an old local Netop log file with the same path and file name.

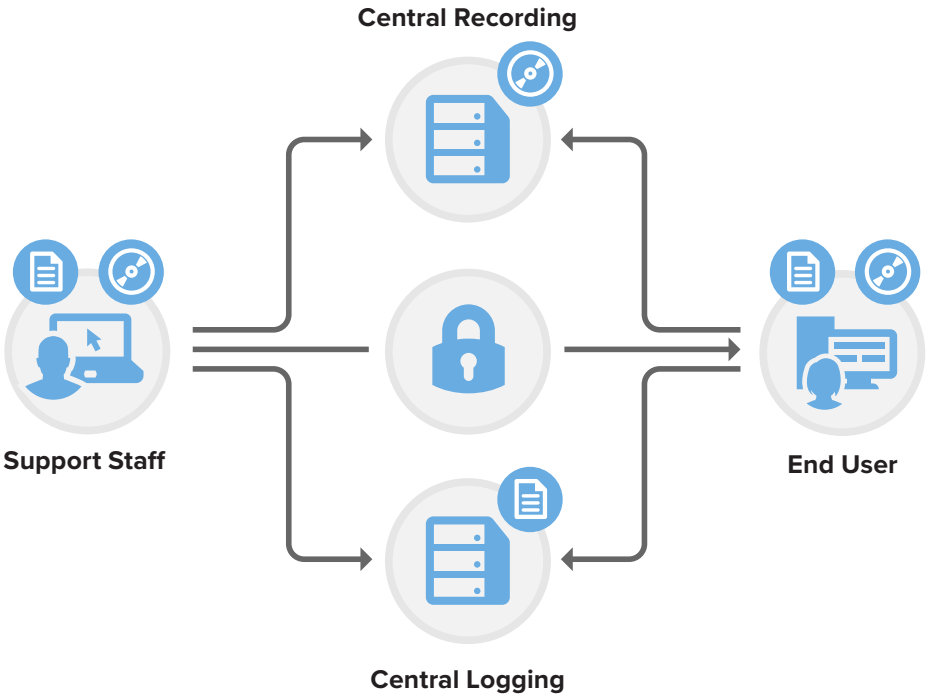
3.4.1.2. Windows Event Logging

Event Logging provides a standard, centralized way for applications (and the operating system) to record important software and hardware events. The Event Logging service records events from various sources and stores them in a single collection called an event log. The Event Viewer enables you to view logs; the programming interface also enables you to examine logs.

For Netop Remote Control running on Windows operating system you can log Netop events in the Windows event log of the computer.

3.4.1.3. Centralized logging: Netop Security Server

Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised. Netop Security Server provides a central log with more than 100 events and stores this information in an ODBC-compliant database for maximum security and scalability. Log data can be kept for an unlimited time along with the physical support session providing complete audit and playback capabilities. Screen recordings are stored in a format that cannot be edited by any video editors.



3.4.1.4. Centralized logging: Netop Portal

Audit logs help you monitor data for any potential security breaches or internal misuses of information.

The Netop Portal offers thorough audit logs (audit trails). The audit logs contain security-relevant data like: the date, time and activity of each user, including sign in events, user creation and removal, role assignments, account configuration and others.

Moreover, the audit logs available in the Netop Portal provide an insight on the Host events and how various parties are using the Netop Portal.

The Host events will be logged in the Portal only when a Netop Portal profile exists on the Host, is active (connected to the Portal), and Portal Logging is enabled for the account the Host belongs to.

In case the Portal profile goes temporarily offline (after having been connected before), events will be retained by the Host until the Portal profile goes back online, or until the Host is closed. When the Portal profile goes back online, if logging is still enabled in the Portal for the Host's account, all retained events will be logged. If logging has meanwhile been disabled for the account, or the Host is closed before the Portal profile re-establishes the connection, all retained events will be discarded.

For details on how to enable the Portal logging and retrieve the audit logs, see the Netop Portal User's Guide.

Interpreting audit logs event codes requires the use of the Netop Remote Control User Guide

3.4.1.5. SNMP logging

In Netop Remote Control all the log events are implemented as possible SNMP traps. They are selectable from the event dialog as the other event types (log locally on a file, log server file and Windows event log). Netop SNMP events are defined in the danware.mib file located in the folder where the Netop module is installed. For detailed information on what's required to get it up and running and how and what to do when making SNMP data and events from Netop Remote Control, read How to set up SNMP for Netop Remote Control.

3.4.2. Screen recording

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.

For documentation purposes you can record remote control sessions. You can choose to record sessions for a specific connection, or you can choose to record sessions for all connections.

NOTE: Recording will reduce remote control session transfer speed. For detailed information on how to record sessions, see the Netop Remote Control User's Guide, section 2.14 Record Sessions.

3.4.3.. Logs retention

Event logs are primarily text entries (or video files) in a database. Organizations can create their own reports to query that info, or can use our tool Remote Access Log Viewer (RALV) available for download here. This gives complete flexibility and autonomy in managing retention of their logs.

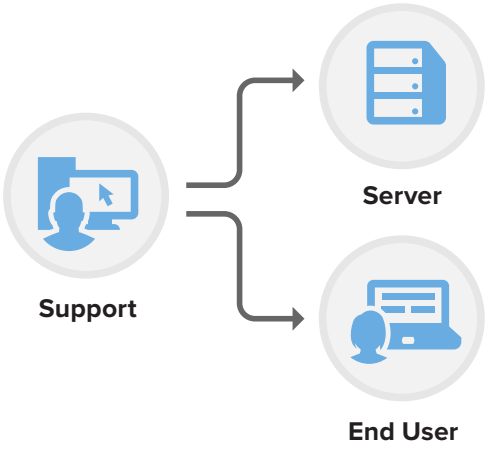
For details on how to configure advanced logging details in the Netop Host and Guest, read this article.

4. Netop Remote Control Architecture

This section describes the various scenarios in which Netop Remote Control is used.

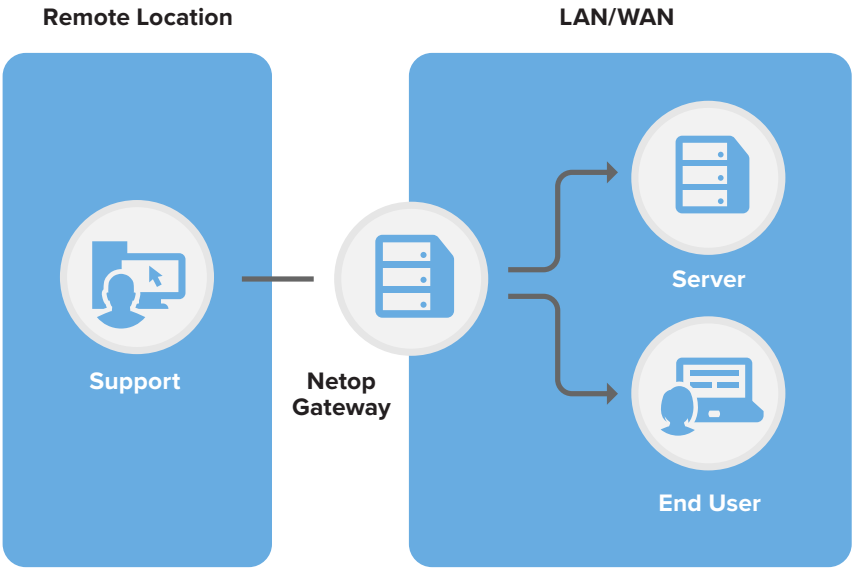
4.1. LAN/WAN Remote Access

The typical scenario consists of Guest – Host connection within a LAN/WAN.



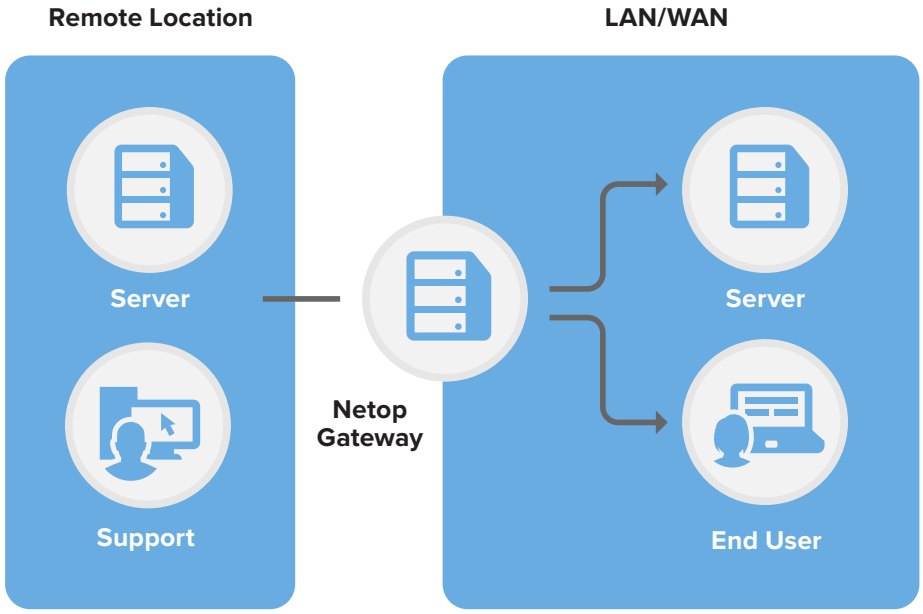
4.2. External Access to LAN/WAN Systems

Agents can connect from a remote location to device within a LAN/WAN by using the Netop Gateway.



4.3. Security Privileges for External Access to LAN/WAN Systems

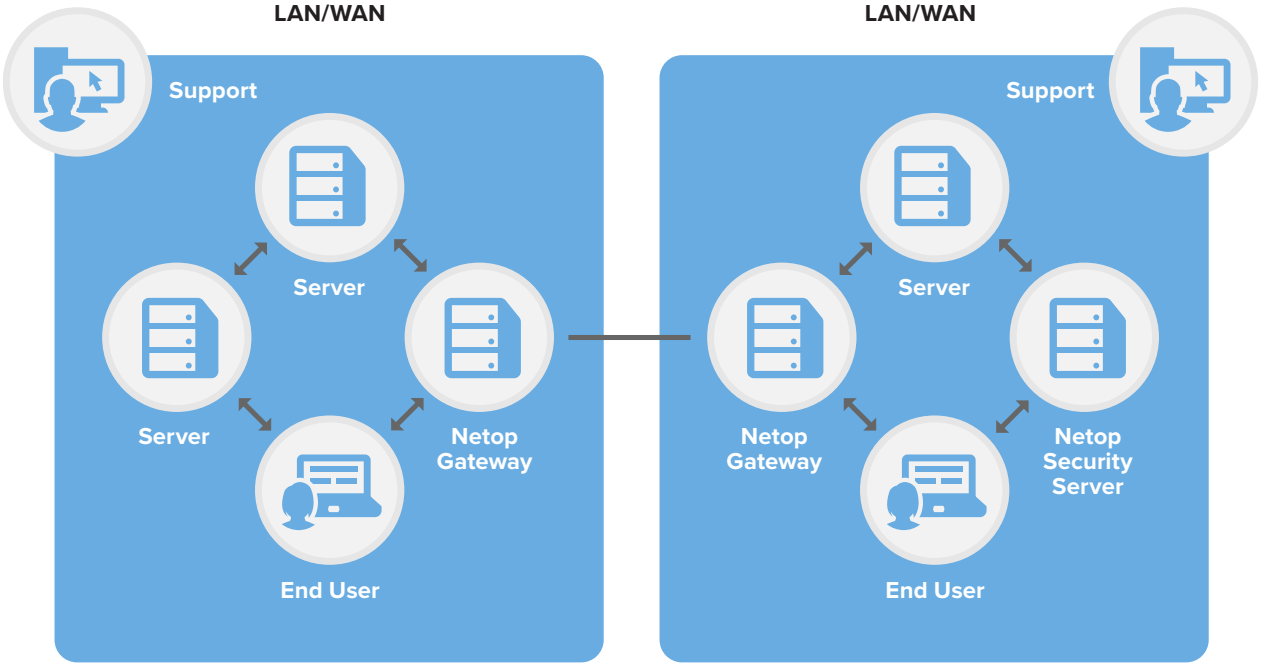
Organizations may need to manage permissions for hundreds to thousands of users while complying with security regulations and implemented policies. Security Server works with your existing infrastructure and integrates with Directory Services, RSA SecurID and Smart Cards.



In a basic remote control scenario, the Host authenticates the Guest via the Security Server before the Guest is allowed to remote control the Host.

4.4. Network Bridging

Netop Remote Control allows agents to use a bridge when they want to exchange information or transfer files between different types of networks.



4.5. Virtualized Environments

Netop Remote Control supports physical systems and virtualized systems.

4.5.1. Virtual Desktop Infrastructure

Virtual Desktop Infrastructure refers to the process of running a user desktop inside a virtual machine that lives on a server in the datacenter. It enables fully personalized desktops for each user.

Netop Remote Control can be used in Virtual Desktop Infrastructure (VDI) as any other software.

4.5.2. Remote Desktop Services

Remote Desktop Services, formerly known as Terminal Service, provides the ability to host multiple, simultaneous client sessions on Windows Server. RDS is capable of directly hosting compatible multi-user client desktops running on a variety of Windows-based and non-Windows-based computers.

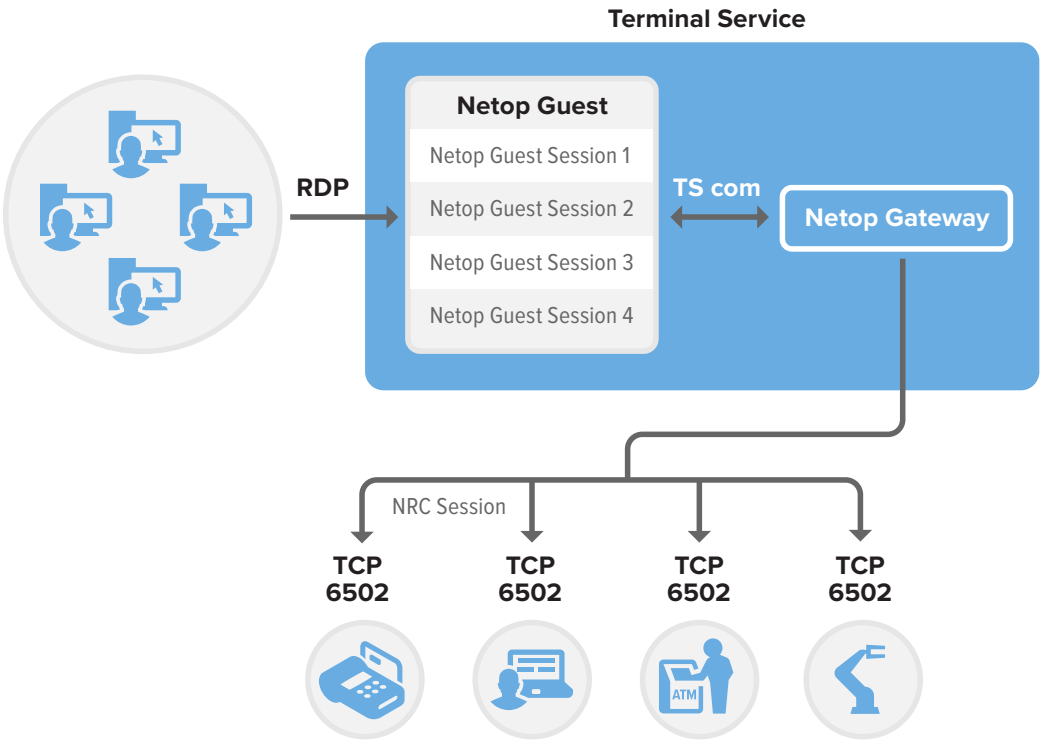
Netop Remote Control can be run in RDS sessions and connect to other Netop Remote Control modules running in sessions on the same RDS, another RDS, or other networked computers.

Since Netop Remote Control modules running on RDS are required to communicate with Netop Remote Control modules running outside the RDS (i.e.: on networked PC's or "fat clients"), the Netop Gateway should be installed and running on the RDS console.

Netop Gateway can receive Netop communication that uses one communication device and send it using another communication device. This ability enables Netop Gateway to provide communication between Netop modules that use mutually incompatible communication devices, typically to connect Netop modules inside a network or RDS environment with Netop modules outside a network or RDS environment.

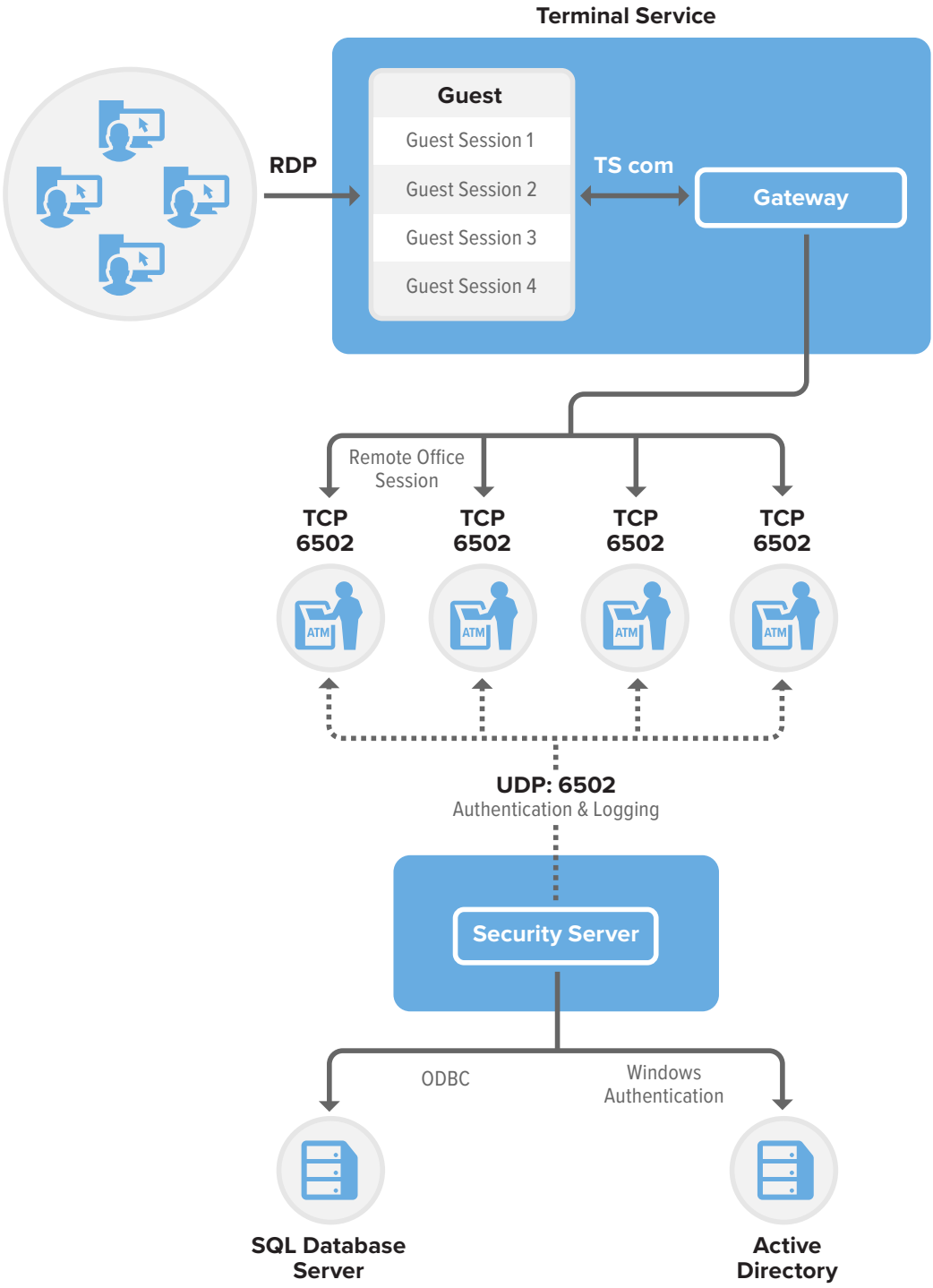
4.5.2.1. Guest running on RDS, Host outside the RDS

For detailed information on how to install and configure a Netop Guest on a RDS machine, so that it becomes available for use in each RDS session started on that server, read Guest Installation on a Terminal Server.



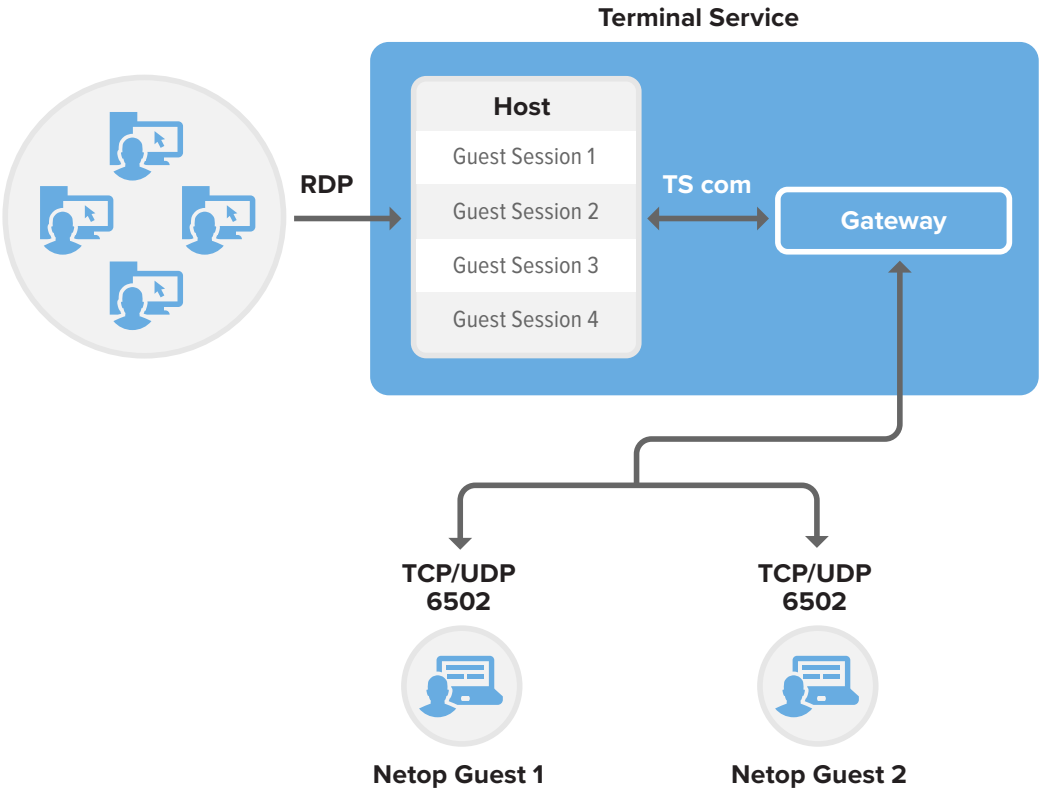
Guest to Host via Netop Security Service

Using Netop Security Server provides centralized security, administration authentication and authorization of all remote control users. All remote control activity can be logged and recorded, allowing the “Host” user to specify the level of access and track activities for each “Guest” user within the server.

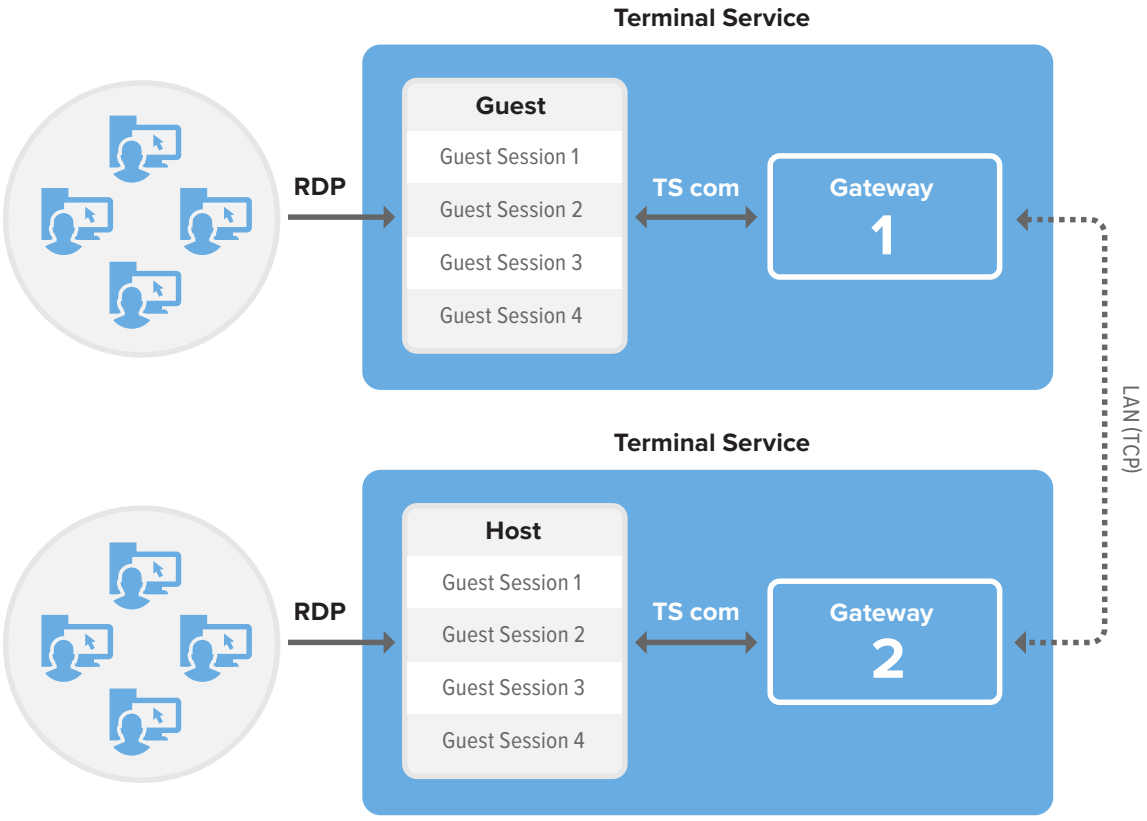


4.5.2.2. Guest outside the RDS, Host running on RDS

For detailed information on how to install and configure a Netop Host on a RDS machine, so that a Netop Guest running outside the RDS can connect to any individual session running on that server, read Host Installation on a Terminal Server.



4.5.2.3. Guest Running on RDS, Host running on a different RDS

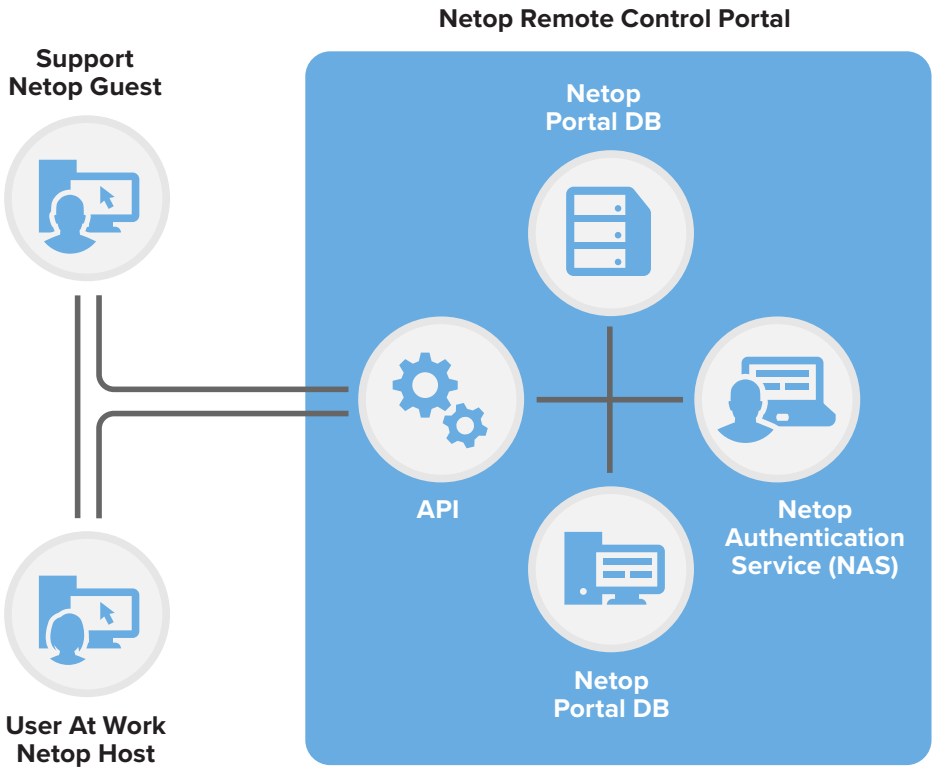


4.6. Secure remote access for third-party vendors: Cloud hosted Portal access

Netop Remote Control for third-party vendors is now browser based as well, it's easy to use and easy to manage. Using the Netop Remote Control Portal it is possible to create a user in the system and grant Third party vendors access to the whole environment, a specific host or group of hosts. For incidental use it is easy to remove a user thereby taking away and preventing access.

The Netop Remote Control Portal is a central hub for managing network access and providing remote support to networked devices. The Portal includes Netop browser-based support console for lightweight, go-anywhere remote support and fast collaboration.

The Netop Remote Control Portal is a central hub for managing network access and providing remote support to networked devices. It uses a centralized database to manage Guest authentication and authorization across the network.

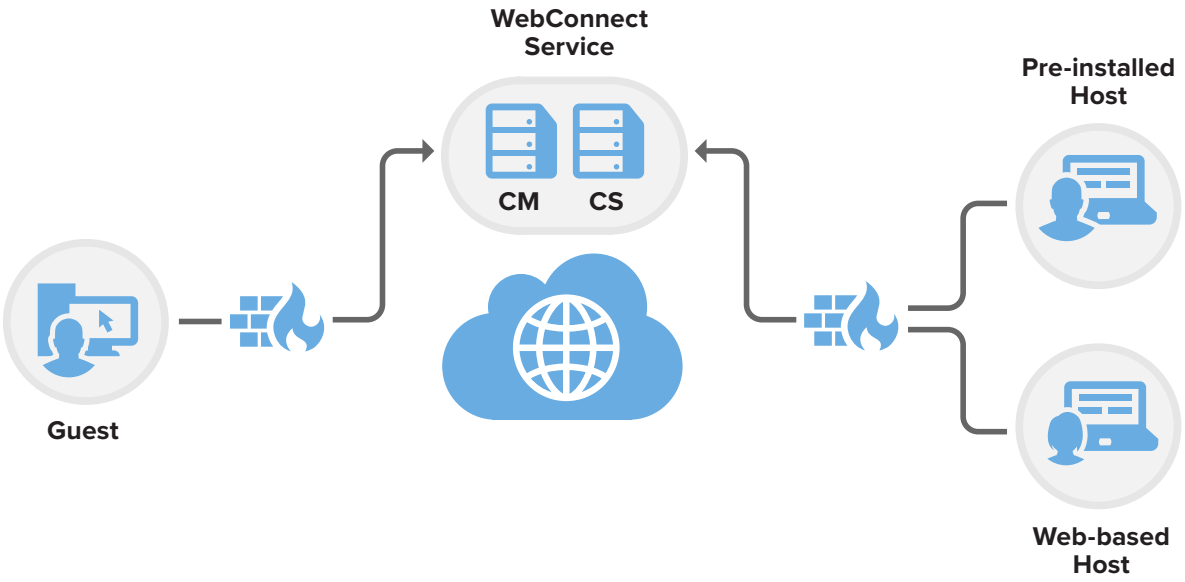


Netop Portal services Host requests for Guest Roles with themselves by managing user authentication, querying the central security database for security data, determining the applicable Role and returning the associated access permissions to the Host to apply them:

1. A user that connects to a Host (from either Browser Based Support Console or an installed Guest) will be requested to identify itself by login credentials.
2. The Host will forward the user credentials to Netop Portal requesting the Role of the user who connected.
3. Netop Portal will manage user authentication and query the security database for security data.
4. Based on returned security data, Netop Portal will determine the applicable Role and return the corresponding access permissions to the Host.
5. The Host will apply the received Role to the user (Browser-Based Support Console or Guest).

4.7. Secure remote access for third-party vendors: self-hosted WebConnect

Netop WebConnect eliminates connectivity problems by creating a new secure meeting ground for applications to meet and communicate over the Internet, unhindered by firewalls.



The Netop WebConnect system consists of a Connection Manager that serves as a meeting hub for Netop Guests and Hosts and multiple Connection Servers that route the traffic.

The Connection Manager is a web service that facilitates connection information and parameters to Netop Guests and Hosts (including OnDemand Hosts and Mobile Hosts) that have a need to meet in relation to remote control sessions. The service directs the applications to a Connection Server.

The Connection Manager uses a Microsoft Internet Information Server and a Microsoft SQL Server for data management.

Connection Servers are capable of connecting Netop modules and routing the traffic.

Data traffic protocols must be allowed outbound through a firewall to the Connection Manager and Connection Server. Outbound communication to the WebConnect Connection Manager is HTTP:80 and/or HTTPS:443. Outbound communication to the WebConnect Connection Servers is TCP:6502 and/or HTTP(TCP encapsulated):80.

Rules or exceptions may need to be created that allow communication through a proxy server to communicate with the WebConnect Connection Manager and Connection Server modules.

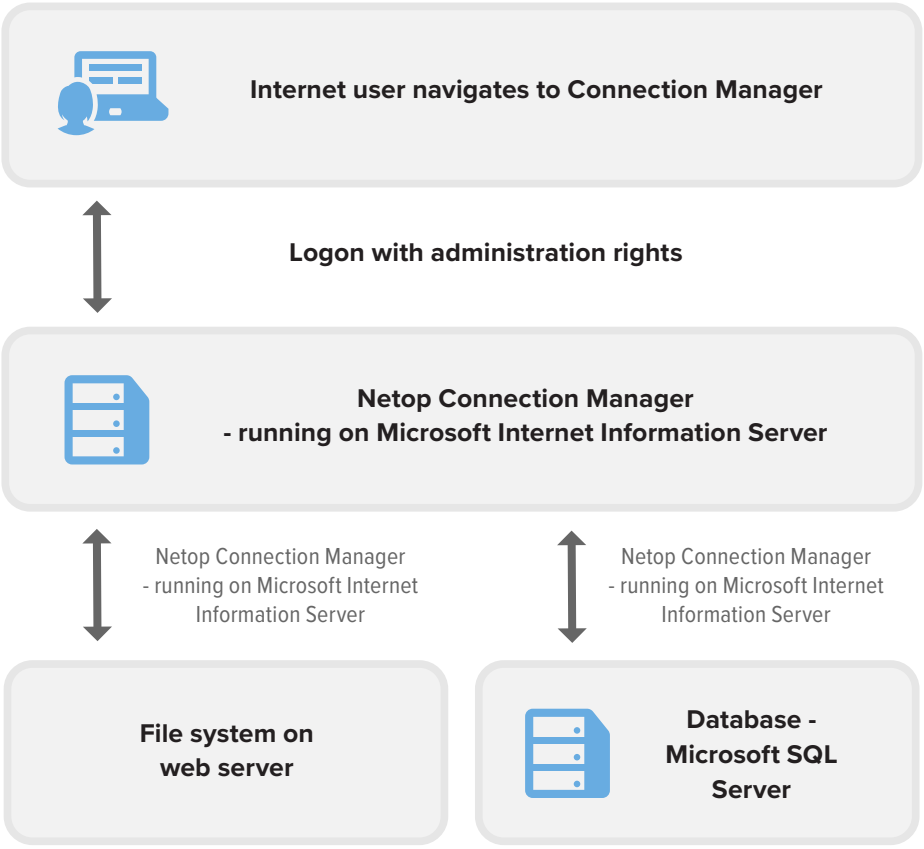
The URL (name resolution) does not impact the firewall setup. When configuring a Windows firewall rule the address of the Connection Manager and Connection Server can be indicated either as IP or name (domain). The rule will work the same.

In the context of HTTPS certificate the name resolution is important. In case the Connection Manager is client hosted it is important that the HTTPS certificate to be issued to the name (domain) of the Connection Manager machine. Also the WebConnect Connection Manager URL should contain the same name (domain) as the HTTPS certificate of the Connection Manager.

In the case of Netop hosted Connection Manager, the Connection Manager's HTTPS certificate is issued to "*.netop.com" (issued by the GlobalSign Domain Validation CA). The WebConnect Connection Manager URL used by the client is "https://webconnect.netop.com/netopcm".

For Firewall and Proxy Server considerations when using Netop WebConnect, read here.

The following illustration shows the security architecture of the WebConnect system:



5. Netop Hosting Environments

Netop created a flexible and secure IT infrastructure using Amazon Cloud, compliant with:

IT Security and Quality Standards

- PCI DSS Level 1
- SOC 1/ISAE 3402
- SOC 2
- SOC 3
- IRAP (Australia)
- ISO 9001:2008
- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- MTCS Tier 3 Certification (Singapore)
- MLPS Level 3 (china)

Industry Specific Standards

- HIPAA
- GxP
- ITAR
- Section 508 / VPAT
- FERPA
- FISMA, RMF and DIACAP
- NIST
- CJIS
- FIPS 140-2
- DoD SRG Levels 2 and 4
- G-Cloud
- IT-Grundschutz
- MPAA
- CSA
- Cyber Essentials Plus

5.1. Logical access and rights

Access to the Netop environment is granted based on:

- Multi-Factor Authentication for console access
- Least privileges access rights
- VPN access to a Bastion Host for connecting to the Netop components.

5.1.1. Multi-Factor Authentication

Netop uses Multi-Factor Authentication to access the Netop Portal environment which is hosted on the AWS.

5.1.2. Least privileges access rights

Netop engineers use AWS Identity and Access Management (IAM) to securely control access to the Netop Portal environment for our users. To manage Netop authentication and authorization, they use least privileges access rights which are managed by the Netop Operations team.

5.1.3. VPN access to a Bastion Host

To access the Netop environment on the Amazon Server, Netop Operations team will need to pass several layers of security:

1. Use a bastion host which only allows access from Netop IP addresses through Virtual Private Network (VPN).

2. Use ssh public and private keys to connect to Netop components

5.2. Logging and audit

5.2.1. Netop Environment Configuration

To continuously monitor configuration changes to the AWS Netop resources, to audit compliance against rules, to analyze security, to dive into configuration details of a resource at any point in time and for troubleshooting purposes, Netop uses the AWS Config.

5.2.2. Logging users access and rights

AWS IAM is integrated with AWS CloudTrail, a service that logs AWS events made by or on behalf of Netop AWS account.

CloudTrail logs authenticated AWS API calls and also AWS sign-in events, and collects this event information. Using information collected by CloudTrail, Netop Operations team can identify which users and accounts called AWS, the source IP address the calls were made from, and when the calls occurred.

5.3. Patch Management

Every Netop Remote Control patch, upgrade or new version is tested first on our staging and beta environments.

To ensure that all our instances operating systems are current with the latest security patches, Netop uses Opsworks which leverages Chef (configuration management software) to automate patches across all environments and components.

5.4. Incident Response

Netop Operations team provide 24x7x365 coverage to detect incidents and to manage the impact and resolution. For more information on Netop product maintenance and support services, see Netop Service Level Agreement.

5.5. AWS Protection

AWS uses a variety of automated monitoring systems to provide high performance services and availability. The tools monitor server and network usage, scan port activities, application usage and unauthorized intrusion attempts. They also allow setting up performance thresholds for unusual activity. Moreover, alarms inform AWS operations and management personnel when warning thresholds are crossed on key operational metrics.

The AWS network provides protection against traditional network security issues: Distributed Denial of Service (DDoS), Man in the Middle (MITM) Attacks, IP Spoofing, port scanning, packet sniffing by other tenants and many more.

5.6. AWS Service-Specific Security

AWS services are architected to work efficiently and securely with all AWS networks and platforms.

To protect sensitive data and applications, Netop uses the following AWS security services:

- Amazon Elastic Compute Cloud (Amazon EC2) Security
- Amazon Elastic Block Storage (Amazon EBS) Security
- Amazon Elastic Load Balancing Security
- Amazon Virtual Private Cloud (Amazon VPC) Security
- Amazon Route 53 Security
- Amazon Web Services
- Amazon Relational Database Service (Amazon RDS) Security
- Amazon ElastiCache Security
- Amazon Simple Email Service (Amazon SES) Security
- Amazon CloudWatch Security
- AWS CloudTrail Security
- AWS OpsWorks Security

Read more about service-specific security on AWS in the AWS Security Whitepaper.

5.7. High availability and scalability

Amazon's load balancing infrastructure has a high level of availability allowing us to deploy a resilient IT architecture.

In case of system or hardware failure, clustered AWS data centers allow automated processes to move customer data traffic to safe load-balanced sites.

Netop took advantage of AWS infrastructure including multiple data centers, which are redundantly connected to multiple tier-1 transit providers, and in order to remain resilient in front of failures, our engineers have distributed the Netop Portal servers across multiple availability zones in the following regions:

- US East (N. Virginia)
- US West (Oregon)
- US West (N. California)
- EU (Ireland)
- EU (Frankfurt)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Asia Pacific (Seoul)
- South America (Sao Paulo)

Each region is completely independent, achieving the greatest possible fault tolerance and stability Each Availability Zone is isolated, but the Availability Zones in a region are connected through low-latency links.

5.8. Backup and restoring

We take advantage of Amazon RDS automated backups by creating a storage volume snapshot of Netop Portal and Netop Authenticate Services (NAS) database.

This process is backing up the entire database instance and not just individual databases.

All backup data is encrypted using the industry standard AES-256 encryption algorithm.

The backup retention period is set to the maximum of 35 days to maintain compliance.

In case of data corruption we use daily snapshots to restore the full database.

The retention period of 35 days gives the possibility to restore the database instance to any specific point in time during this retention period and to meet our RPO objectives.

6. FAQ

Where should the Security Servers be installed and what network access is required?

Because Netop Security Server is the focal point for authenticating your Guest users, it should be installed on a server based operating system for maximum availability. The server does not need to be dedicated and can run Windows Server 2000, 2003, 2008, 2012 or 2012 R2 (32-bit and 64-editions including 2008 R2) including virtual environments.

You will require a UDP connection via your chosen port (6502 by default) between your Hosts and Security Servers.

Does Netop Security Server have failover capabilities?

Yes. Multiple Security Servers can exist to provide a fault-tolerant environment with maximum availability. Should one server fail, the remaining servers will seamlessly handle the authentication and authorization process.

What type of databases are supported by Netop Security Server?

Netop Security Server follows the SQL92 Standard (ODBC-compliant) and is known to support the following databases: DB2, MS JetEngine, MS SQL and Oracle.

Note: Netop does not support MySQL, because it does not use ‘named primary key’, which is a requirement for Netop Security Server.

What if my Host users have concerns over remote access to their systems?

Using Netop Security Server or the Netop Portal means that only authenticated Guests are allowed to access specific Host machines. This does not mean that once authenticated, the Guest will have complete control over the Host system. There are many different levels of control and notification features that can be made available to the Host users including Confirm Access dialogs, notification features and disconnect hotkeys.

All remote support activity can also be logged and therefore audited including the actual remote session allowing organizations to trace and deal with any unauthorized access attempts.

7. About Netop

Netop builds market-leading software for remotely accessing and supporting devices, managing classroom technology and serving customers online. Used by half of the Fortune 100, Netop's secure remote access and live chat solutions help businesses provide better customer service, reduce support costs and meet security and compliance standards. In addition, Netop's Vision Classroom Management software empowers schools and teachers to maximize the use of technology for improved student achievement. Netop is headquartered in Denmark and has offices in the United States, China, Romania and Switzerland. The company sells its solutions directly and through Netop business partners to public and private clients in more than 80 countries.

8. References

http://www.windowsecurity.com/articles-tutorials/windows_os_security/Windows_Terminal_Services.html

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

https://technet.microsoft.com/en-us/library/cc782486%28v=ws.10%29.aspx

http://searchsecurity.techtarget.com/tip/Security-token-and-smart-card-authentication

https://msdn.microsoft.com/en-us/library/windows/desktop/aa363652(v=vs.85).aspx

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html

http://aws.amazon.com/compliance/pci-dss-level-1-faqs/

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

https://aws.amazon.com/certificate-manager/

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-examples.html

http://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

https://www.citrix.com/glossary/vdi.html

http://www.infoworld.com/article/2661685/vdi/application-and-desktop-virtualization-under-the-hood.html

http://blog.parallels.com/2014/05/20/vdi-vs-rds/