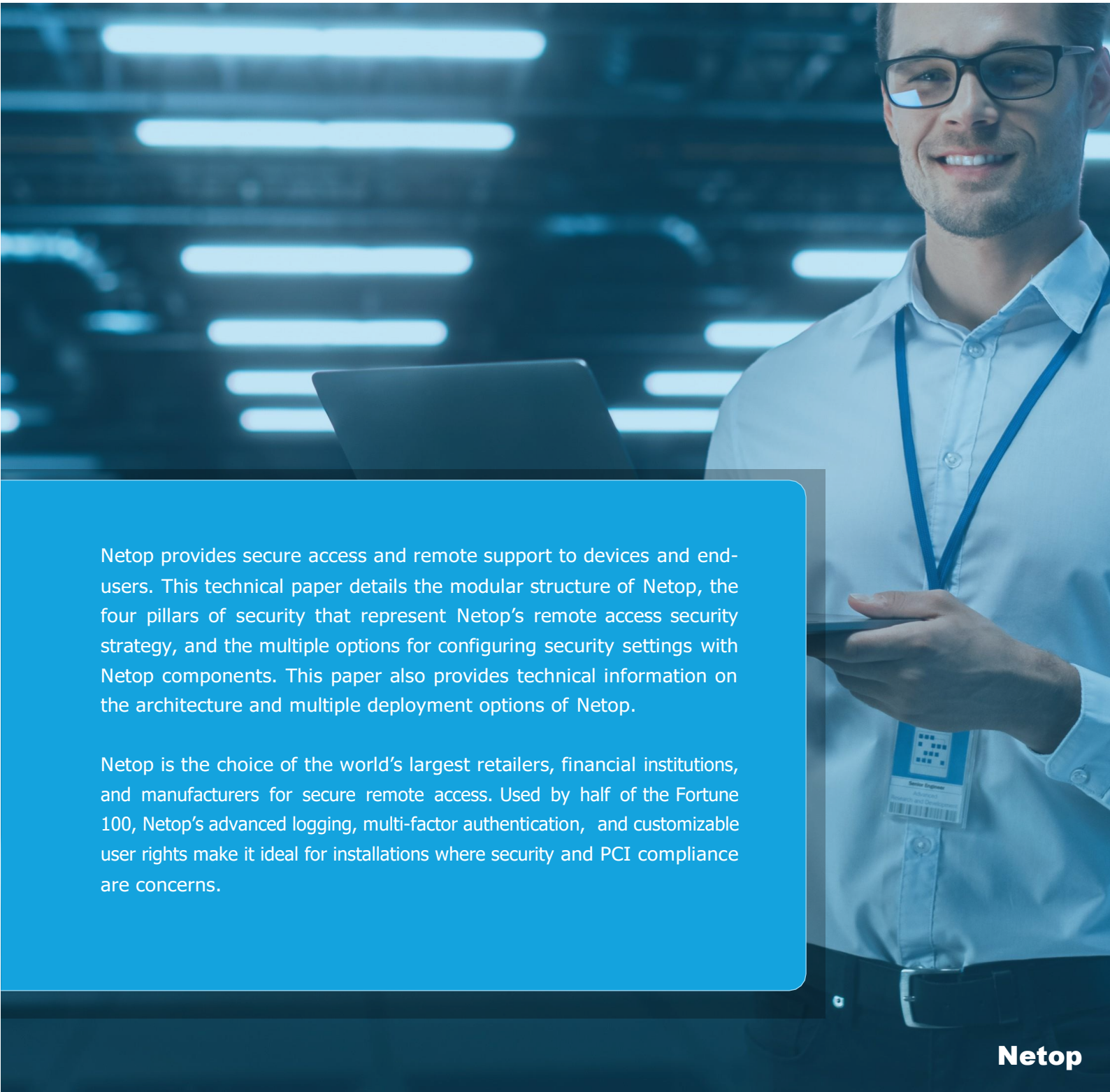
NETOP

Security Paper

A Technical Overview of Netop Security



Netop provides secure access and remote support to devices and end-users. This technical paper details the modular structure of Netop, 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.

Netop 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.

Netop

Table of Contents

Glossary of Terms

AES (Advanced Encryption Standard): A symmetric encryption algorithm used to protect data confidentiality. Netop uses AES with key lengths up to 256 bits to secure data in transit and at rest.

AD FS (Active Directory Federation Services): A Microsoft service that provides Single Sign-On (SSO) by extending on-premises Active Directory capabilities to external systems. Used in Netop for federated authentication via the Portal.

Authentication: The process of verifying the identity of a user or system. Netop supports local, centralized, and multi-factor authentication methods, including Windows credentials, LDAP, RSA SecurID, and RADIUS.

Authorization: The process of determining which actions an authenticated user is permitted to perform. In Netop, this is managed through access privileges and security roles.

Callback: A Netop security feature that allows the Host to call back to a predefined address after a Guest has been authenticated, thereby verifying the physical location of the Guest.

Closed User Groups: A security feature in Netop that restricts Host connections to Guest modules with matching custom serial numbers, rejecting those with retail or trial versions.

Diffie-Hellman: A key exchange algorithm used to securely share cryptographic keys over an untrusted network. Netop uses Diffie-Hellman for secure communication setup.

Guest: The Netop module installed on the technician's machine used to initiate remote support sessions. The Guest connects to the Host to perform remote control operations.

Guest ID: A unique identifier assigned to a Guest module or user. Used for authentication and access **control.**
HMAC (Hash-based Message Authentication Code): A mechanism for verifying data integrity and authenticity, used in Netop for encrypted communications.

Host: The Netop module installed on the remote target machine that is being accessed or controlled. The Host enforces security policies, authenticates Guest users, and logs session data.

LDAP (Lightweight Directory Access Protocol): An open protocol used for accessing and maintaining distributed directory information. Netop integrates with LDAP for user authentication and role management.

MAC/IP Filtering: A feature that restricts Host connections to Guests whose IP or MAC addresses appear in a predefined whitelist.

MFA (Multi-Factor Authentication): A security mechanism requiring two or more forms of identity verification (e.g., password + token). Netop supports MFA using RSA SecurID, RADIUS, and Azure MFA.

Netop Gateway: A proprietary cloud-based service that allows Guest and Host modules to connect over the Internet without opening inbound firewall ports. It provides secure outbound-only connections using TLS encryption.

Netop Portal: A cloud-hosted service that centralizes user management, authentication, and access control. It supports role-based permissions and integrates with AD FS and LDAP.

Netop Security Server: An optional component used for centralized user authentication and access control. It can connect to multiple types of directory services and database engines.
NIS2 Directive: A European Union directive (Directive (EU) 2022/2555) that sets out high common cybersecurity standards across EU member states. It mandates improved risk management, supply chain security, incident

reporting, and accountability for digital service providers. Netop, especially when hosted on AWS, supports NIS2 compliance through encryption, access control, audit logging, and incident response capabilities.

RADIUS (Remote Authentication Dial-In User Service): A protocol that enables centralized Authentication, Authorization, and Accounting (AAA) for remote access. Netop uses RADIUS for integrating with third-party identity providers.

RSA SecurID: A two-factor authentication solution using tokens. Netop integrates with RSA SecurID via the Security Server for MFA enforcement.

Smart Card Authentication: An authentication method using a physical card that stores user credentials. Supported by Netop for high-security environments.

TLS (Transport Layer Security): A cryptographic protocol that ensures data integrity and privacy between communicating applications. Netop uses TLS for all module communications, including Portal.

User Controlled Access: A feature in which the end user at the Host device manually approves or denies incoming remote control session requests from Guests.

Zero Trust: A cybersecurity model based on strict identity verification and least privilege access, assuming no implicit trust within or outside the network. Netop implements Zero Trust principles via strong authentication, role-based access, encryption, and auditing.

1 Overview of Enhanced Security Architecture

Executive Summary

Netop delivers secure access and remote support through a modular system built on four pillars of security: encryption, user access control, privilege management, and comprehensive auditing. In today's evolving threat landscape, this architecture is further reinforced by adherence to Zero Trust principles and alignment with the European Union's NIS2 Directive to ensure secure remote operations and regulatory compliance.

Modern Security Framework Integration

Zero Trust Security Model

Netop's architecture naturally lends itself to a Zero Trust approach: - **Verify explicitly**: Multi-factor authentication (MFA), smart cards, and identity federation (AD FS, LDAP) ensure verification at every connection. - **Use least-privilege access**: Role-based access control (RBAC) and centralized authorization (via Netop Portal or Security Server) restrict user permissions to the bare minimum necessary. - **Assume breach**: Logging, session recording, and centralized audit trails support forensic analysis and detection of abnormal activity post-compromise.

NIS2 Compliance Considerations

The NIS2 Directive mandates robust risk management, incident response, and supply chain security. Netop supports this through: - **Detailed auditing** via logs, screen recordings, and SNMP traps. - **Vendor access control** via Guest authentication, role enforcement, and portal-based third-party session isolation. - **High availability & backup** powered by AWS, with encryption (AES-256), multi-zone redundancy, and patch automation using Chef/OpsWorks.

Pillar 1: Encrypt the Line

All data transmissions are encrypted using: - TLS 1.2+ with strong ciphers (AES-256 GCM preferred). - RSA 2048 or ECDSA 256 for key exchange. - HMAC SHA-256 for data integrity.

Portal integrates AWS Certificate Manager and GlobalSign TLS Certificates. Deprecation of TLS 1.0/1.1 is recommended to comply with current security baselines.

Pillar 2: Manage User Access

Netop provides extensive capabilities: - **Smart Card & MFA support** (Azure MFA, RSA SecurID, RADIUS). - **SSO & Identity Federation**: AD FS/LDAP support for unified authentication. - **Just-In-Time Access**: Temporary users and session-based permissions via Portal.

Enhancing access policies with device-based context awareness or geolocation checks is recommended.

Pillar 3: Manage Access Privileges

Netop offers: - Centralized role management (via Portal or Security Server). - Role assignments mapped to device/user groups. - Compatibility with AD, LDAP, token-based systems.

Security posture can be strengthened by applying dynamic access rights based on session context.

Pillar 4: Document What Happens

Comprehensive logging capabilities include: - **Event logging**: Local, Windows Event Log, SNMP, Portal, and ODBC backends. - **Screen recording**: Tamper-proof format with playback capability. - **Log retention**: Configurable, AES-256 encrypted, 35-day RPO support.

SIEM **Integration** (e.g., with AWS CloudWatch, Splunk) is recommended for advanced alerting and analysis.

Pillar 5: Zero Trust

The Zero Trust Security Model—built on verify explicitly, least privilege access, and assume breach—ensures continuous, granular protection for remote access.

Verify Explicitly: Netop supports strong authentication, including MFA (RSA, RADIUS, Azure MFA), federated identity and SSO, smart cards, and session confirmation, ensuring identity and intent are validated for every request.

Least Privilege Access: Role-based controls define precise user permissions with contextual enforcement, granting only the minimum access necessary and reducing attack surface.

Assume Breach: Continuous monitoring through encrypted channels, detailed logging, segmentation (MAC/IP filtering, closed user groups), and tamper protection enables breach containment and visibility.

AWS Integration: Hosting in AWS adds further Zero Trust alignment with IAM, Certificate Manager, VPC controls, CloudTrail, and Config for secure, compliant cloud infrastructure.

Infrastructure & Hosting

- **Cloud architecture** on AWS, compliant with ISO 27001, SOC 2, PCI DSS, FIPS 140-2.
- **Resiliency**: Multi-region failover, daily backups, incident response.
- **IAM Best Practices**: Least-privilege IAM, CloudTrail-based auditing.

NIS2-aligned practices include layered access control, documented vendor access, and a formal incident response framework.

Recommendations Summary

Area	Suggested Update
Encryption	Deprecate TLS 1.0/1.1 and mandate TLS 1.2+ with forward secrecy
Zero Trust	Expand with device posture checks and network segmentation
NIS2 Compliance	Highlight existing support and add regular risk assessments & supply chain audits
Log Management	Integrate with centralized SIEM for anomaly detection
Access Control	Enable policy-based access controls and session expiry timers

Note: This document is aligned with evolving global cybersecurity frameworks and standards. It incorporates layered defense principles and operational readiness designed to mitigate current and emerging threats.

2 Compliance and Standards

2.1 The NIS2 Directive: Elevating Cybersecurity Standards Across the EU by Netop on AWS

2.1.1 Introduction

In today's rapidly evolving digital landscape cybersecurity is essential. Some countries have additional security standards and requirements to address security issues in different areas. The new European Union (EU) NIS2 Directive raises cybersecurity standards, requiring enhanced risk management, incident reporting, and governance practices. In this blog, we explore how Netop provides an integrated solution, run on AWS cloud services, that provide customers with NIS2's alignment capabilities. Discover how the partnership between Netop and AWS addresses the challenges of NIS2, supporting cybersecurity resilience across critical sectors within the EU.

2.1.2 What is NIS2?

The NIS2 Directive is an EU legislative framework designed to establishing a high common level of security for network and information systems across vital sectors. Building on the original NIS Directive, NIS2 expands its reach to cover additional sectors, including healthcare, energy, transportation, and digital infrastructure, as well as essential industries like pharmaceuticals, food production, and public administration. The directive introduces stricter requirements in risk management, incident reporting, and supply chain security to mitigate cybersecurity risks that could disrupt essential services.

A key aspect of NIS2 is accent on harmonizing cybersecurity standards across the EU, aiming to create a consistent approach to protecting critical infrastructure. With NIS2, organizations are accountable not only for their cybersecurity but also for the security of their suppliers and third-party vendors. This directive underscores the EU's commitment to strengthening cybersecurity frameworks and reducing vulnerabilities within interconnected networks across vital sectors.

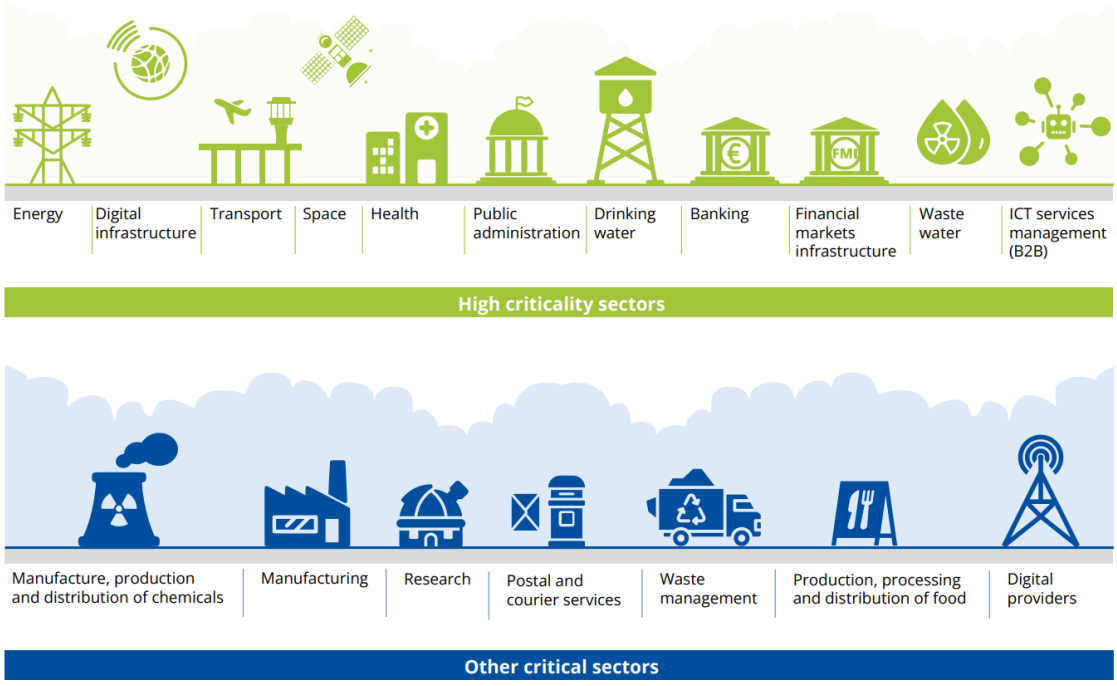


Figure 1. ENISA Infographic on industries and sectors impacted by NIS2

2.1.3 Solution overview:

Netop delivers secure remote access software through an integrated enterprise platform for large private and public organizations in business-critical industries around the world. All types of users, such as employees, experts,

engineers, contractors, subcontractors can start remote control sessions from a distance towards both generic IT devices and industry specific equipment, for troubleshooting sessions or day to day remote working purposes. Leading security focus, real-time operations, broad systems support and global coverage are key attributes for Netop secure remote control software.

NIS2 regulation includes cybersecurity resilience of the supply chain as one of its key focus areas, related to security of remote access for any employees or third-party individuals when they perform remote access interventions inside the organization environment, working from any kind of devices, corporate managed or external. NIS2 defined supply chain translates to all the organizations' suppliers and employees that provide digital services remotely.

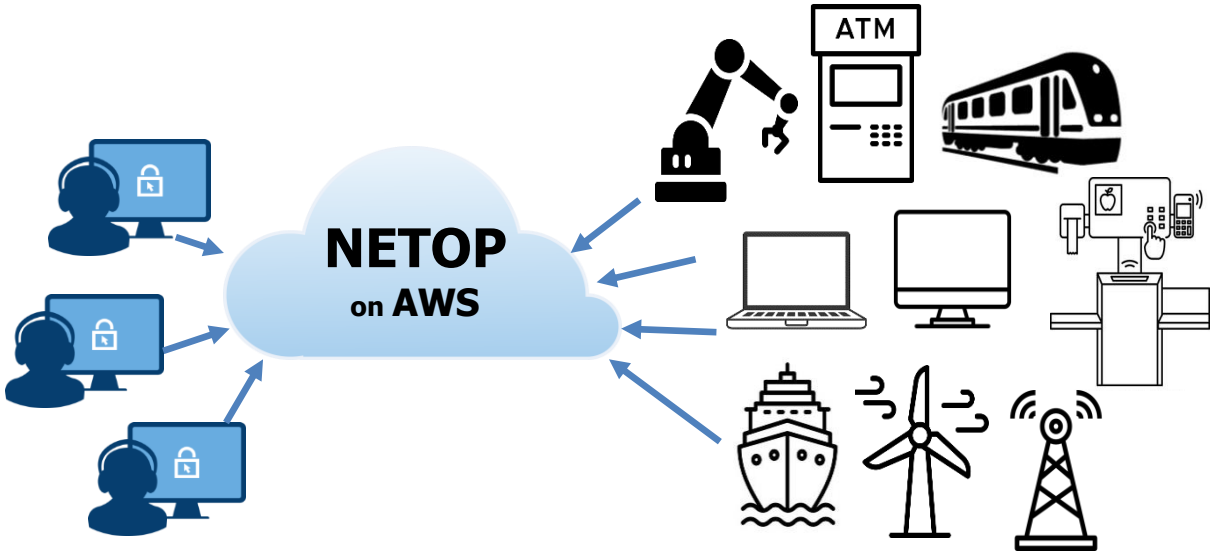


Figure 2. Netop remote access to intelligent devices.

Organizations already using Netop platform on AWS for their secure remote access practice range from all business-critical industries such as retail, banking-finance, insurance, manufacturing, transportation, utilities and city services, healthcare, central and local government bodies, defense and security.

Whether a support technician needs to remote a PC or laptop for troubleshooting purposes, or an outsourced service provider needs to access internal finance systems for data entry operations, an engineer needs to access a production robot to change its settings and configuration, these are only few examples of IT supply-chain resilience scenarios that fall under NIS2 directive.

2.1.4 Netop recommendations towards NIS2 regulation

To address these stringent requirements, Netop is introducing the secure remote access solution applicable to all organizations impacted by NIS2 regulation. By leveraging Netop products and expertise in secure remote access software, organizations can achieve critical NIS2 compliance requirements while fortifying their security posture in the face of growing external cyber-attacks, optimizing their IT infrastructure and reducing response time for remote troubleshooting and connectivity tasks.

The subset of NIS2 measures related to secure remote access practices of the organization, addressed by Netop are listed below.

1. **NIS2 Article 11 – Requirements, technical capabilities and tasks of CSIRTs, Paragraph 3.a**: The

CSIRTs should monitor and analyze cyber threats, vulnerabilities, and incidents at national level while providing support to essential and important entities upon request regarding real-time or near real-time monitoring of their network and information systems.

NETOP recommandations :

a) Use Netop for a real-time remote access dashboard with information on all online/offline endpoints, running remote sessions and connections and active permissions deployed in the environment.

b) Use Netop kill-switch mechanisms for suspicious or rogue sessions as well as mechanisms to deactivate **permissions.**

c) Run a regular secure remote access permissions management assessment

2. Article 21 – Cybersecurity risk-management measures,

The operational and organizational measures required from essential and important entities must follow an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include:

- **Paragraph 2.d:** supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers:

  NETOP recommendations:

  a) Use Netop to provide mechanisms to restrict access to systems, based on grouping principles of both equipment and personnel of service providers, with criteria like: level of criticality, geography, residence, certifications and need-to-know or need-to-perform basis.
  b) Use Netop mechanisms to restrict actions and activities permitted to the supplier, based on criteria such as time-window, work certification, supervision (four-eyes principle).
  c) Provide remote access permissions at application level for Netop sessions performed by suppliers or service providers, on a need-to-know or need-to-perform basis.
  d) Provide human quality control mechanisms on remote access sessions, with Netop session acceptance tools delegated to the security control responsible or supervisor responsible persons. Best practices for acceptance tools are screen pop-up acceptance or email acceptance for incoming remote sessions from supply chain personnel.
  e) Deploy Netop data residency mechanisms for the secure remote access environment, supported by the largest AWS global datacenter infrastructure, such as own customer AWS cloud accounts or Netop managed virtual private cloud accounts located inside the European Union.
  f) Provide IP-fencing (IP range selection) mechanisms for remote access sessions to designated whitelisted supply chain geographies, individual suppliers or personnel contractors.

- **Paragraph 2.e:** security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

  NETOP recommendations:

  a) Make the organization remote access practice, with focus on the supply chain remote access use-cases, a top priority in the organization's cybersecurity policies and framework.
  b) Reduce the attack surface of potential threats, by eliminating point-to-network access (VPN-like or assimilated) and provide alternative point-to-point remote access for remote personnel of the supply chain and entity suppliers.
  c) Implement Netop remote session recording mechanisms, capable to record audio-video evidence (full keyboard, video and mouse events) of all the remote access activity of the supplier personnel;
  d) Block open remote session protocols in the network, including RDP, VNC, Telnet or SSH, to reduce the attack surface and also remove a potential attack's persistence and lateral movement layer;

- **Paragraph 2.h:** policies and procedures regarding the use of cryptography and, where appropriate, encryption;

  NETOP recommendations:

  a) Implement recognized and high-level Netop encryption standards in cloud communication and remote session protocols.
  b) Encrypt with strong Netop mechanisms all remote access sessions data, both for in-transit real-time sessions and at-rest stored data.

- **Paragraph 2.i:** human resources security, access control policies and asset management;

  NETOP recommendations:

a) Provide federated user management directories integration and multi-factor authentication methods for all access and sessions.
b) Identify and eliminate unrestricted remote access practices, remove just-in-time or remote session invite practices performed without prior user identification and authorization of each invitee, even for view-only type of remote sessions.
c) Anonymous access for both employees and external suppliers, even for view-only type of remote sessions, should always be eliminated.

3. Article 22 – Union level coordinated security risk assessments of critical supply chains
NETOP recommendations:

a) Conduct regular penetration testing certifications on remote access tools, including Netop, mitigate vulnerabilities and remove the non-secure remote connection alternatives.

4. Article 23 – Reporting obligations:
NETOP recommendations:

- Implement remote access auditability by extensive use of logging and recording capabilities of Netop remote access sessions, as they can help in preventing attacks and can aid forensic investigations for legal authorities.
- Combine AWS CloudTrail user activity and API usage logging for cloud and hybrid environments with extensive Netop application logging mechanisms that will register all remote access events for connection, session, action, security and configuration. Centralize all secure logging services for a holistic approach to monitoring remote access activities of the digital supply chain.
- Enable Netop mechanisms to encrypt all logging data, cloud-trail activities.
- Log Netop remote access sessions only at entity level (as opposed to logging at the supplier or supply chain personnel level).
- Activate Netop remote session recording mechanisms, capable to record audio-video evidence (full keyboard, video and mouse events) of all the remote access activity of the supply chain personnel.
- Make use of Netop tamper-proof mechanisms for the audio-video recordings, including non-standard and encrypted codecs, remote session interruption in event of recording failure or read-only storage locations, encrypt storage of session recordings.

5. Article 24 – Use of European cybersecurity certification schemes
NETOP recommendations:

- Favor industry-proof and certified remote access software such as Netop, deployed on cloud services for the supply chain security resilience, that provide certified mechanisms, such as ISO27001, SOC2, PCI-DSS, FIPS, HIPAA, NIS2 and various specific industry and equipment manufacturers certifications.
- Provide certified deployments by combining on-premise where required, cloud-based where applicable, or hybrid and multi-cloud architectures into a single Netop secure remote access platform.

2.1.5 Step-by-Step project guidelines for the IT supply chain secure remote access best practice

Step 1 – Determine the supply chain for the organization

- Collect an extensive list with all suppliers, from organization sources, like:
- Accounting: all suppliers active in the last 12 – 36 months
- Purchasing / Supplier Relationship Management: all suppliers active in the last 12 – 36 months
- Contracting / Legal: all suppliers with active contracts in the last 12 – 36 months

Step 2 – determine the list of digital equipment, including IT devices

Any equipment that has a chip, a microcontroller or anything that can be catalogued as artificially intelligent machines, is to be included in the project scope.

Sample sources for equipment list data:

- IT&C Assets: laptops, desktops, networking equipment, communication equipment, servers and datacenter equipment
- Automation projects, such as building automation (access control, audio-video surveillance, building management)

- Industry specific equipment: industrial equipment, robots, sensors, medical equipment, ATM-s, POS-es, kiosks, digital and interactive panels, automation lines, production lines, industrial facilities, transport vehicles or transport lines, city services delivery and fulfilment equipment, etc.…

Step 3 – map digital services of the supply chain towards digital equipment

Supplier centric: which equipment is accessed remote, for what type of services, by each supplier of digital services

In this stage the project team can eliminate the suppliers that do not supply any digital services, for example cleaning services, transport services, furniture, auto, office supplies, or similar.

Device centric: what users are accessing each equipment or equipment type and in what circumstances they access that equipment remotely: from company network, from outside networks, from home, from the world wide web, etc.…

In this stage the project team can eliminate from project scope the equipment that is never accessed remotely, but is only accessed by users in front of the device;

The secure remote access map. Based on the above activities, the project team will define the set of users that access remotely the set of organization devices, into a table format that will become the scope of NIS2 certification project.

Step 4 – Netop is ready to implement your NIS2 secure remote access project

Documentation resulted from the previous phases becomes source for the Netop secure remote access platform implementation project and for NIS2 future audits.

Contact Netop or start a test project in the AWS Marketplace

2.1.6 Conclusion

The NIS2 Directive marks a significant step forward in strengthening cybersecurity across critical infrastructure sectors in the European Union, but compliance can seem daunting without the right tools. By adopting Netop for the company wide enterprise remote access practices, organizations can effectively meet the directive's rigorous requirements while enhancing their overall digital security.

3 Executive Summary

Netop 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 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 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 is provided as connectivity.

Netop supports both physical and virtualized systems. Netop can be run in RDS sessions and connect to other Netop 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:

1. Encrypt the line. Sensitive information is encrypted during transmission over networks to avoid being accessed by malicious individuals.
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.
3. 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.
4. Document what happens. Netop 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 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.

4 Netop Modules

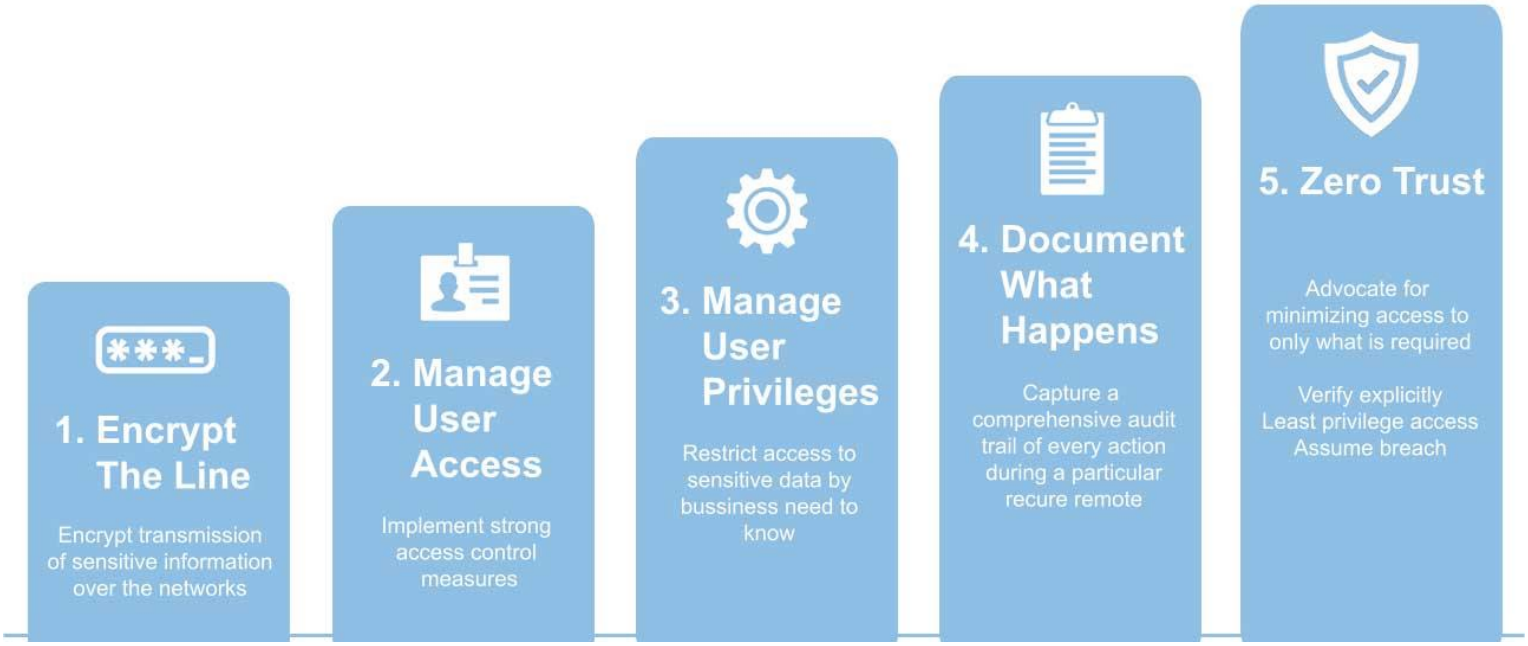
The basic components of Netop consist of two remote control software modules: the Guest installed on the technician's computer and the Host installed on the target machine.

Along with the Guest and Host components, Netop offers a cloud portal for remotely connecting to users' systems.

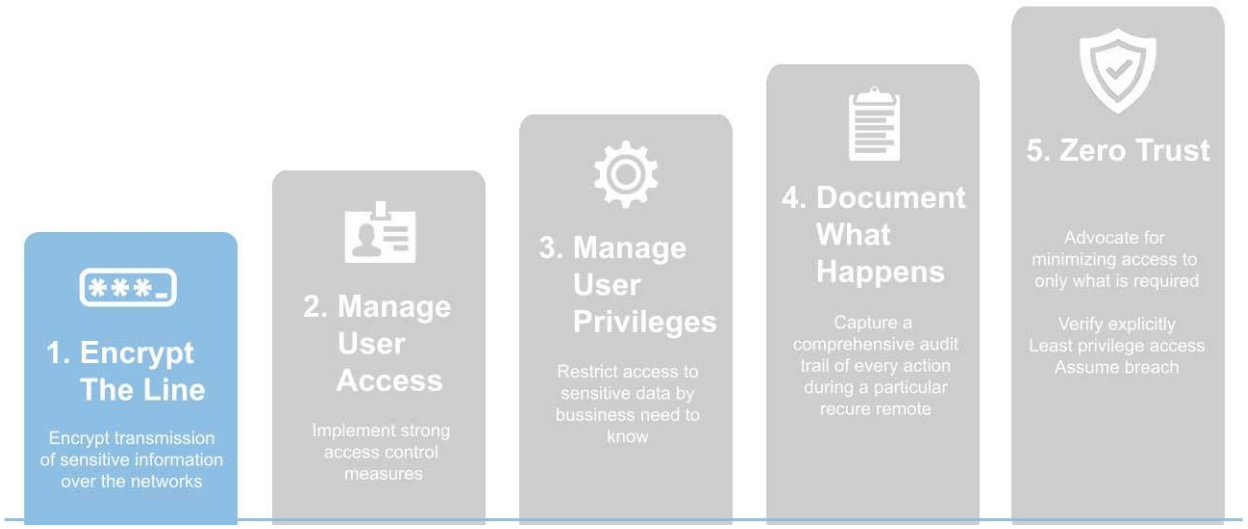
Netop comprises the following modules:

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 Portal's browser based support console.
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.

5 Five Pillars of Security



5.1 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 data environments.

5.1.1 Guest to Host Encryption Options

The security is achieved through multiple modules and components working together.

- Encrypt the line – 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.

5.1.1.1 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.

5.1.1.2 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.

5.1.1.3 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.

5.1.1.4 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.

5.1.1.5 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.

5.1.1.6 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

5.1.2 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.

5.1.3 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).

5.2 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 endpoint 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 user 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 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 Connect 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.

5.2.1 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)*

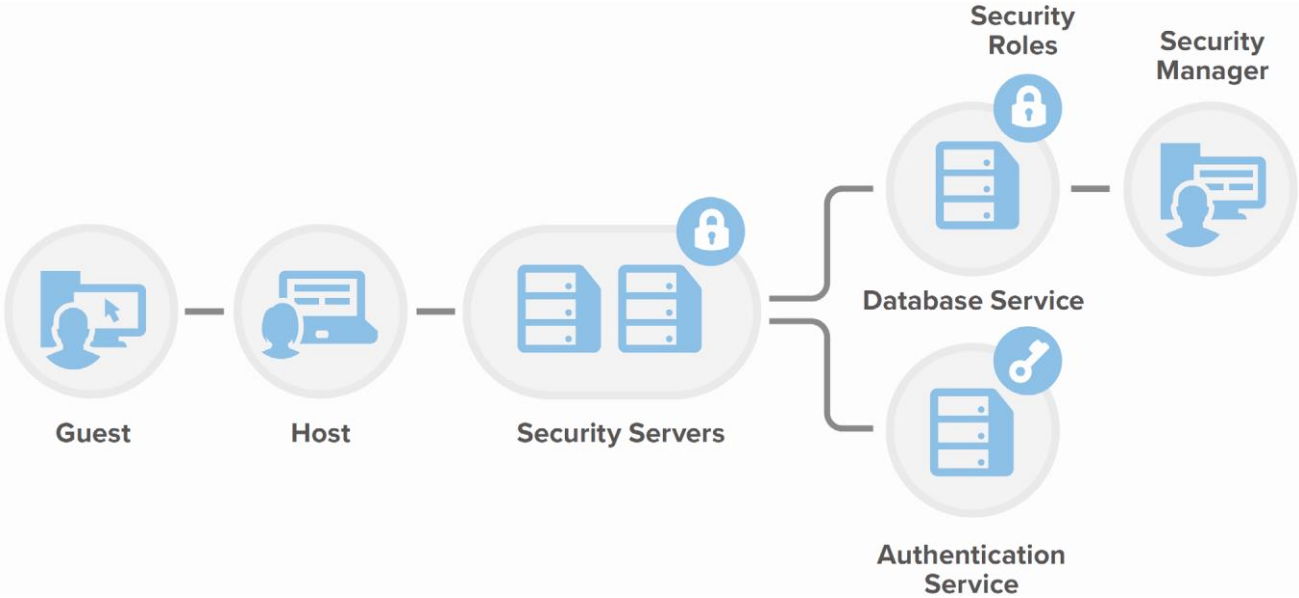
5.2.1.6 Smart Cards

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 to use smart card authentication, either by working with Netop Security Server or directly on the Connect Host, see Netop Smart card Integration.

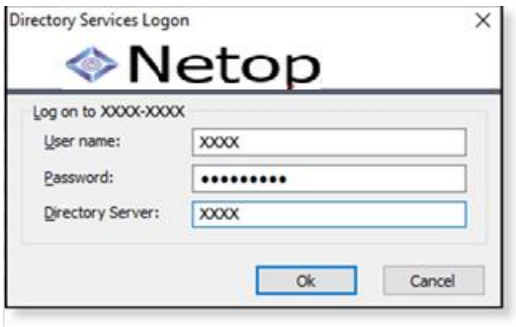


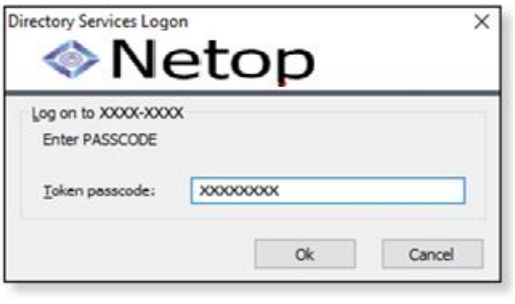
5.2.1.7 Multi-factor authentication

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 offers extended security with Windows Azure and Remote Authentication Dial-In User Service (RADIUS) multifactor 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.

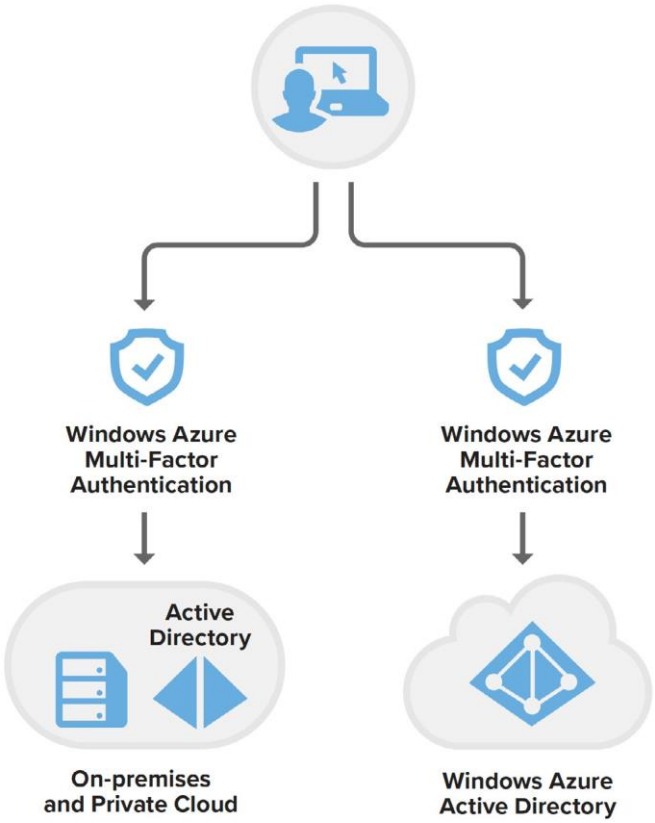
Using RADIUS with Netop allows the Security Server to authenticate remote support sessions via compatible multifactor authentication methods, where the Guest user needs to provide their user name and password initially, followed by a one-time generated pass code that can be derived from a variety of 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 provides integration to this service. Companies can use their own Windows Azure Multi- Factor Authentication in Netop.



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.

5.2.1.8 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.

5.2.1.9 Centralized Authentication

Netop offers a totally centralized security regime using the Windows NT SAM database, Microsoft Active Directory, Directory Services via LDAP, Netop Portal or Connect Security Server.

For example, using Microsoft Active Directory, each Guest is authenticated against an Active Directory Service such as that provided by Windows Server 2022. 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.

Connect Security Server Authentication

The Connect Security Server is a special Host module that can answer queries from other Connect 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 Connect 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 Connect Security Server.

To achieve Connect authentication the Connect Security Server verifies the Guest identity against the database service that holds all the predefined Guest IDs and passwords. To achieve Windows authentication the Connect 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 Connect 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 Netop 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 Connect 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 Connect 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 Connect 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 Connect 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 Connect Portal User's Guide.

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

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 Connect Portal.

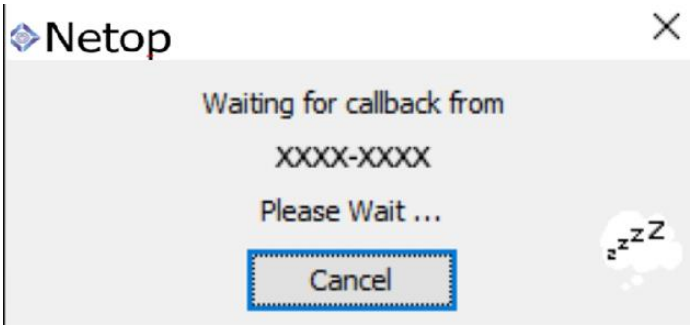
Instead of manually filling in information for every user, the AD FS integration will allows using data from the company's user store (Single-Sign On authentication extending enterprise identity beyond the firewall). This also means that data from the Connect Portal is synced with the company's data 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 Connect 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 Connect Portal User's Guide.

5.2.2 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.

5.2.3 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.

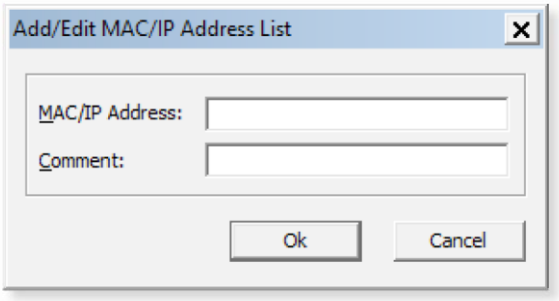
With closed user groups, companies can obtain a custom serial number to the software used by service desk representatives and target devices. In fact, when an application is installed, a license is requested. From this license an embedded legacy license is extracted. This embedded legacy license has encoded the features available for the application installed. One of this feature is Closed User Group, meaning that it can communicate with other application that has this feature. Thus, 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.

5.2.4 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:



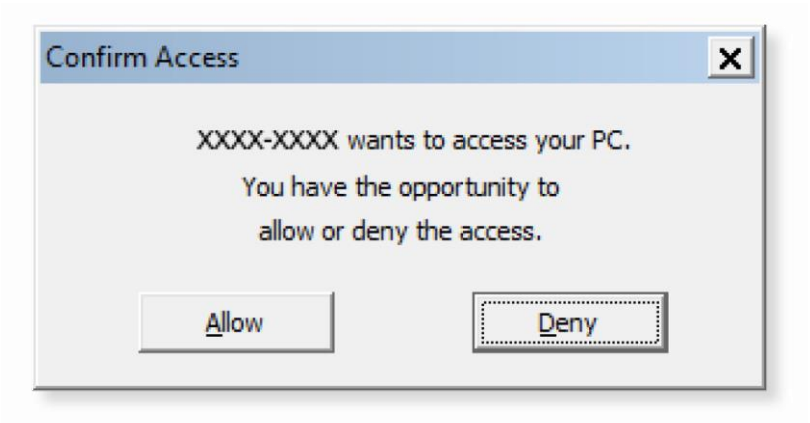
When this feature is enabled, the Host only communicates with Guest computers if their addresses are listed in the predefined list. This feature is designed to use the original MAC/IP address (or the NAT address) of the Guest.

5.2.5 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.

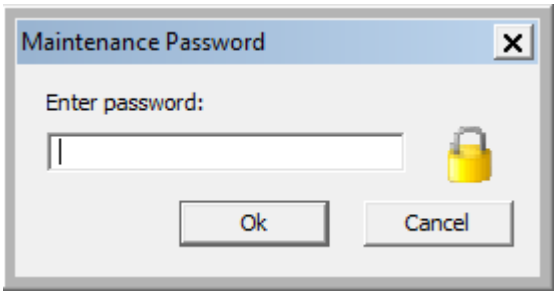


There is an option to bypass the Confirm Access dialogue box if there is no user logged on to the computer. With Netop, you can also customize the message that appears on the Host computer.

5.2.6 Tamper proofing the Host configuration

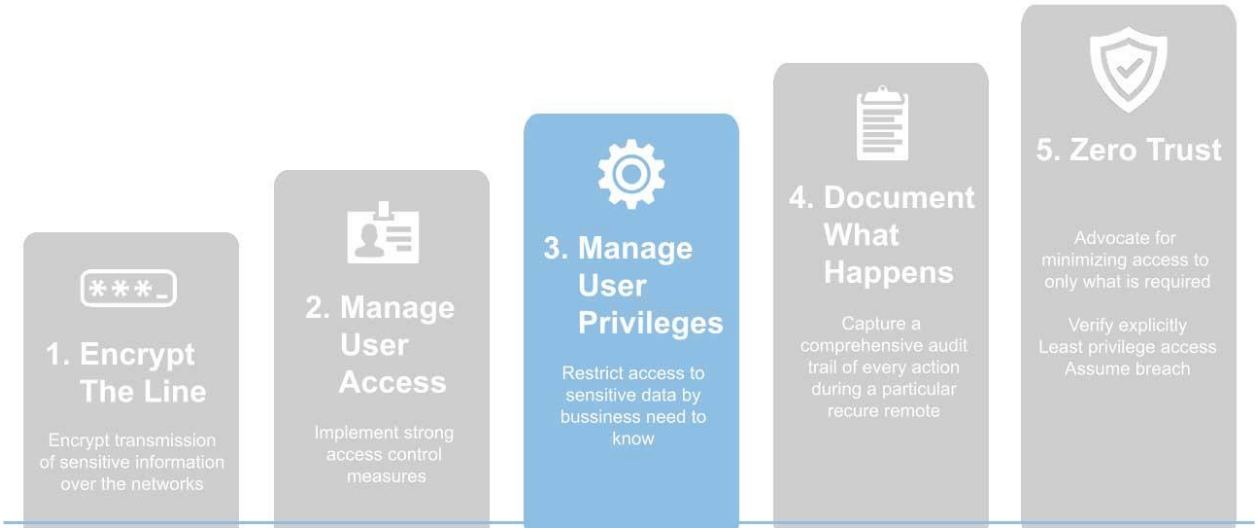
The Host module has a maintenance password feature that can protect the Host configuration under all platforms.

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.

5.3 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.

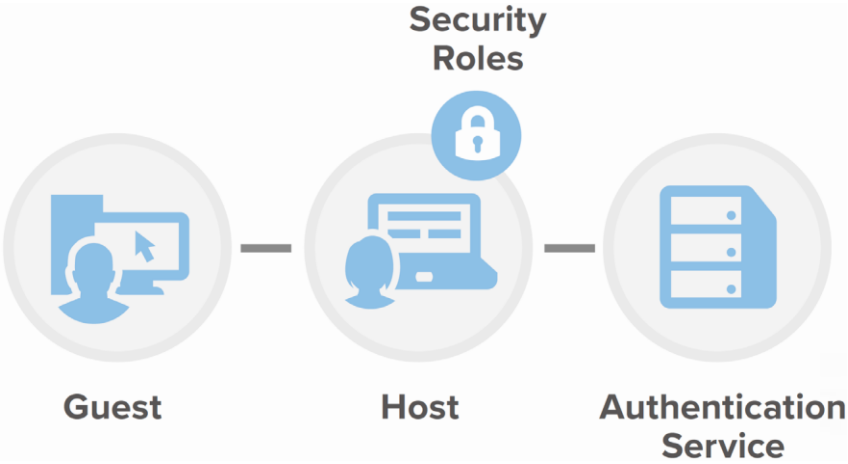
The Host user has to confirm access if the Guest user is present in at least one security role. Security roles can be managed locally for all supported platforms or centrally via the Netop Security Server or via the Netop Portal.

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.

5.3.1 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.

5.3.2 Centralized Access Privileges

Access privileges define **what actions an authenticated user (Guest) is permitted to perform** on a target machine (Host). These privileges ensure that users can only perform operations appropriate to their role or authorization level, helping organizations enforce **least privilege access** and maintain a secure remote control environment. In modern deployments, **centralized authorization** means that permissions and roles are not configured individually on each Host, but instead managed centrally through systems like the **Netop Portal** or **Netop Security Server**.

The **Netop Portal** acts as a cloud-native, centralized control plane that defines security roles, manages user identity and permissions, and applies them dynamically to support sessions.

For environments requiring local control or integration with existing infrastructure, the **Netop Security Server** provides a centralized on-premises mechanism for managing access privileges. It integrates with database services (Oracle, MS SQL Server, MS Access, DB2) and checks Guest identity and group membership to authorize session permissions.

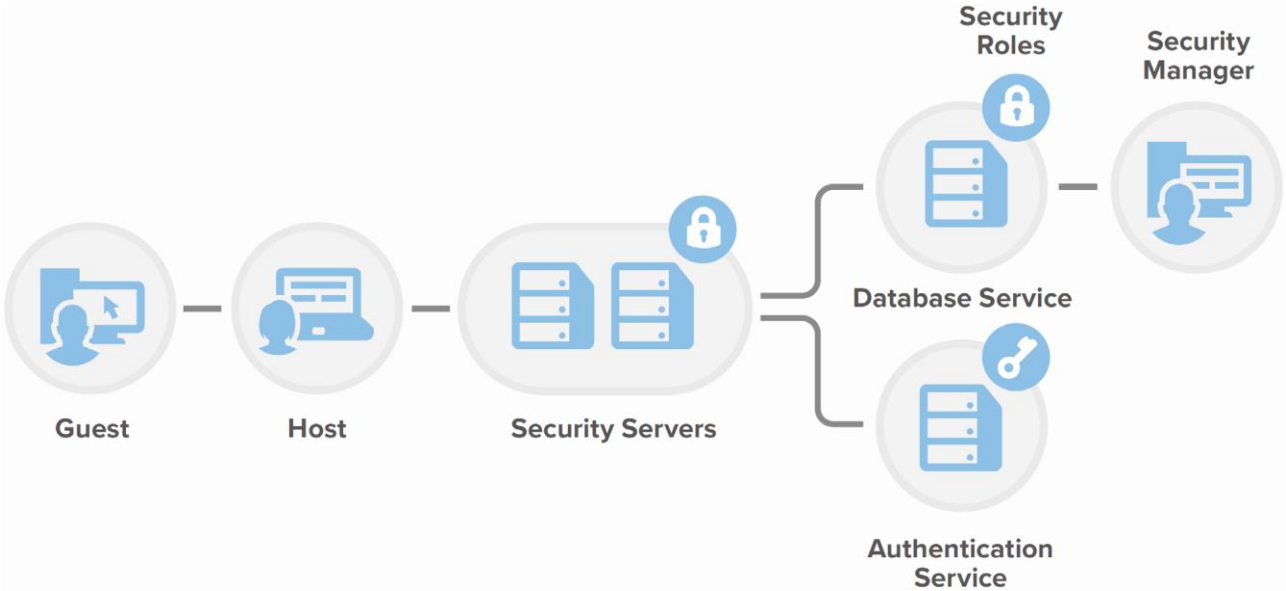
In brief, centralized authorization means that information about security roles is available in a database on a shared remote computer.

5.3.2.1 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.

5.3.2.2 Netop Portal centralized authentication and authorization

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

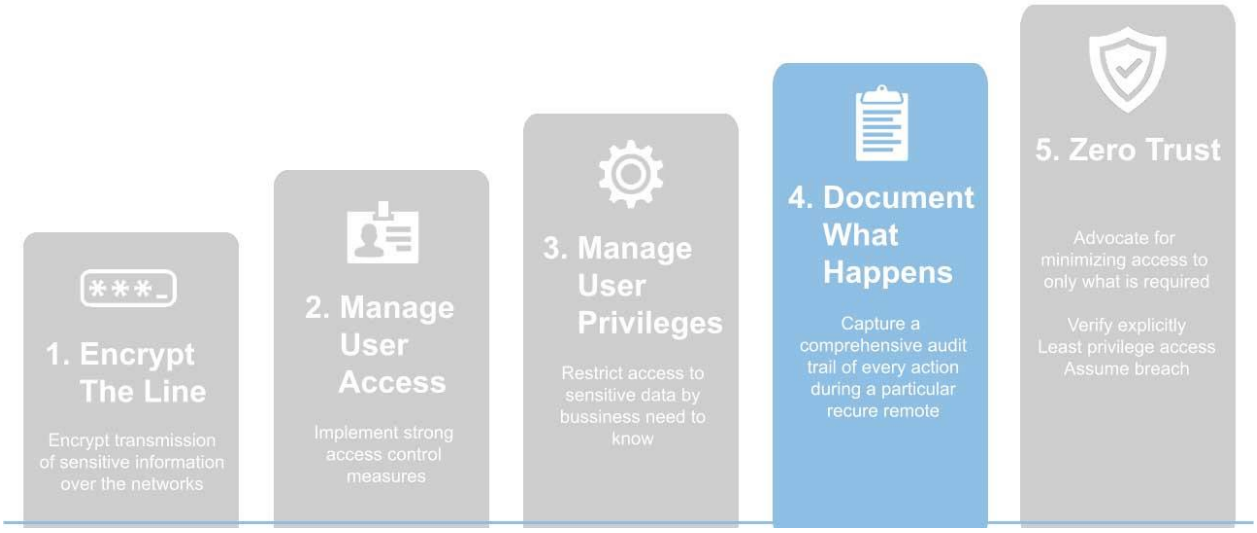
Centralized authorization means that access permissions for each remote support session can be defined using security roles via the Netop Portal. These permissions can be easily managed using the Netop Portal and offers great flexibility with different levels of control depending on the Guest users'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

5.4 Pillar of Security #4: Document what happens



Netop 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 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 User Guide. Event codes and their definitions can be found in Netop 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

5.4.1 Netop Logging

To support security functions, Netop 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 Logging, see the Netop 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 User's guide, section 5.1.15 Log Setup.

5.4.1.1 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\<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.

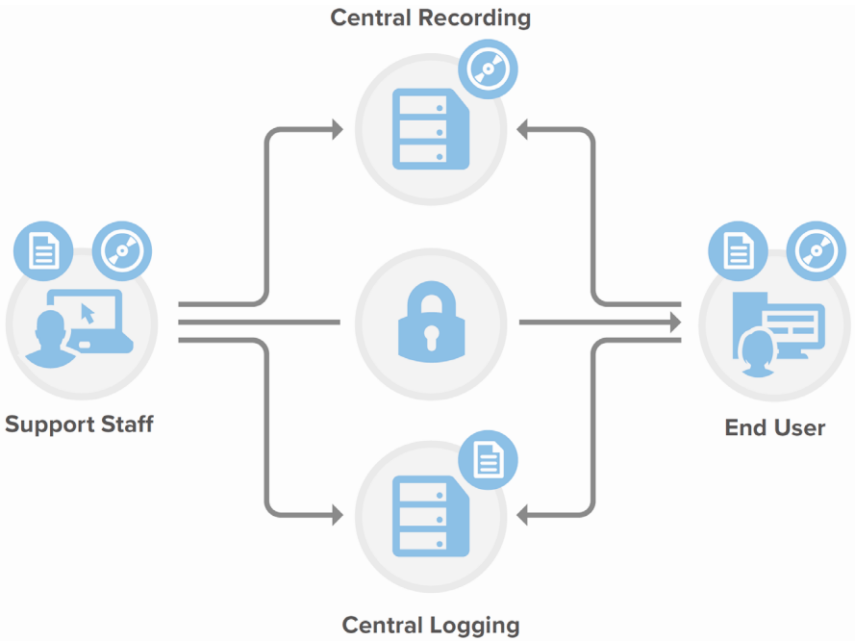
5.4.1.2 Windows Event Logging

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

5.4.1.3 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.



5.4.1.4 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 User Guide.

5.4.1.5 SNMP logging

In Netop 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, read How to set up SNMP for Netop.

5.4.1.6 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.

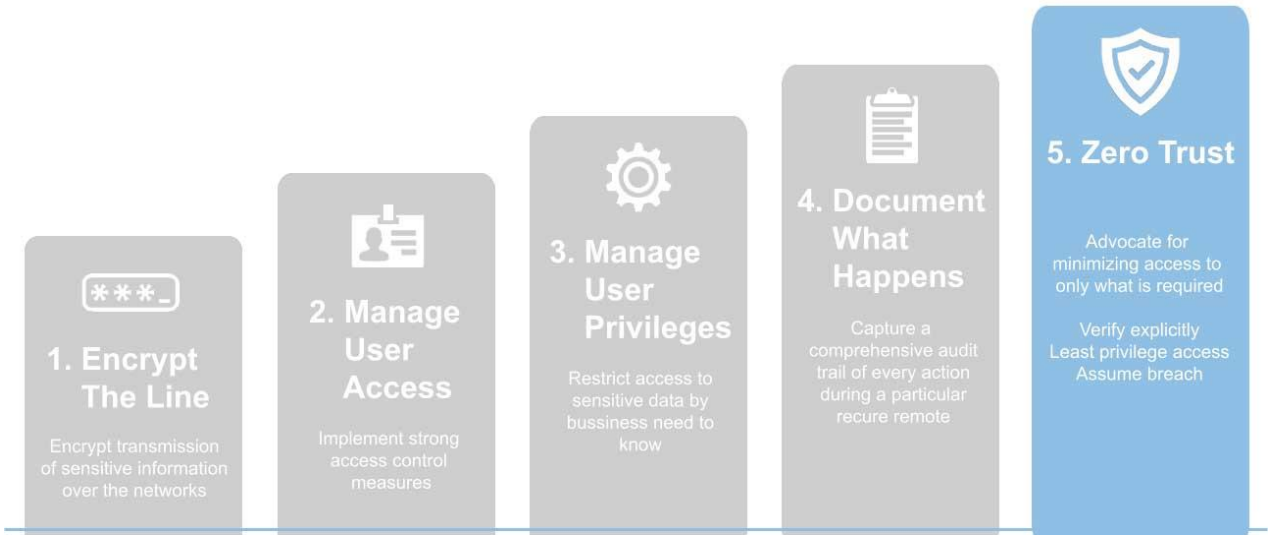
For documentation purposes you can record remote control sessions. You can choose to record sessions for a specific connection, or you can choose to record sessions for all connections.

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

5.4.2 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.

5.5 Pillar of Security #5: Adopt a Zero Trust Security Model



In today's complex and hybrid IT environments, traditional perimeter-based security is no longer sufficient. Organizations must evolve toward a ***Zero Trust Security Model****, which assumes that threats can exist both outside and inside the network. The Zero Trust model enforces the principle:* ***"Never trust, always verify."***
This model is built on three main pillars:

- ***Verify explicitly***
- ***Use least privilege access***
- ***Assume breach***

Netop Remote Control, combined with cloud-hosted infrastructure such as AWS, aligns well with the Zero Trust approach and enables organizations to implement granular, dynamic, and secure access control mechanisms for remote support.

5.5.1 Verify Explicitly: Strong Authentication and Session Integrity

Netop supports a broad range of authentication methods that fulfill Zero Trust requirements for strong identity verification before any access is granted.

- **Multi-Factor Authentication (MFA):** Netop integrates with RSA SecurID, RADIUS, and Windows Azure MFA. This ensures access is based on something the user knows (credentials) and something the user has (e.g., a token or one-time code).
- **Federated Identity and Single Sign-On (SSO):** Netop Portal supports **Active Directory Federation Services (AD FS)** and **LDAP** integration. This centralizes identity control and facilitates audit logging while reducing credential sprawl.
- **Smart Card Authentication:** Government-grade smart card access is supported, providing physical token-based identity validation.
- **Session Confirmation and Callbacks:** Netop allows for real-time confirmation by the Host user, validating identity and intent for every remote session request.

These features support the **explicit verification of every user and device**, regardless of network location.

5.5.2 Least Privilege Access: Role-Based Security Controls

The Zero Trust model advocates for minimizing access to only what is required. Netop achieves this through detailed, role-based access control mechanisms:

- **Security Roles:** Actions available to each authenticated user can be controlled via **local or centralized roles**, configured in the Netop Security Server or the Netop Portal.
- **Granular Privileges:** Roles define what a Guest user can see or do on the Host, ensuring only the necessary permissions are granted for a session.
- **Contextual Access Enforcement:** Access rights can differ based on group membership, authentication method, or device classification, supporting least-privilege enforcement aligned with the principle of **just-enough access (JEA)**.

By minimizing unnecessary access, Netop significantly reduces the attack surface and potential for privilege escalation.

5.5.3 Assume Breach: Continuous Monitoring and Segmentation

Zero Trust frameworks are designed around the assumption that attackers may already be inside the network. Netop addresses this by logging, monitoring, and segmenting communication across its modules.

- **Encrypted Channels:** All communication between Guest and Host, and between internal Netop components, is **encrypted using modern standards** such as AES-256, TLS 1.2+, and HMAC-based integrity checks.
- **Logging and Auditing:** Detailed logs of access attempts, session activity, and configuration changes are recorded and can be sent to centralized log servers for auditing and alerting.
- **Closed User Groups and MAC/IP Filtering:** Segmentation is enforced by limiting which machines can communicate using unique serial numbers and address-based whitelisting.
- **Tamper-Protection:** The Host module supports **tamper-resistant configuration** options and prevents unauthorized stopping or reconfiguration during active sessions.

Together, these features support a posture of **assumed breach containment** and real-time visibility.

5.5.4 Supporting Zero Trust with AWS Infrastructure

When hosted in AWS, Netop can leverage native cloud security features that align directly with Zero Trust principles:

- **AWS Certificate Manager:** Manages TLS certificates to ensure all communication is authenticated and encrypted.
- **Identity and Access Management (IAM):** Enforces access policies at every layer of the AWS stack used by Netop modules.
- **CloudTrail and Config:** Provide immutable logs and compliance tracking across Netop Portal.
- **VPC Controls and PrivateLink:** Enable secure, isolated communication channels without traversing public networks.

*These integrations ensure that Netop's cloud-hosted components are protected by **Zero Trust-aligned security controls at the infrastructure level**, in addition to the application level.*

5.5.5 Summary: Zero Trust as a Security Pillar

*By embedding Zero Trust principles within its authentication, encryption, access control, and auditing mechanisms, **Netop Remote Control** ensures that each session is:*

- **Explicitly verified**
- **Minimally privileged**
- **Continuously monitored**

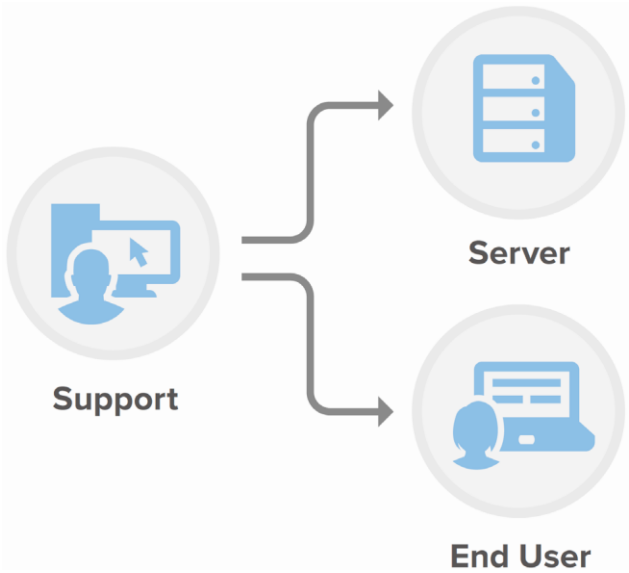
*Whether deployed on-premises or in the cloud, Netop provides the architectural and operational foundations needed to support **a Zero Trust strategy** for secure remote access and support environments.*

6 Netop Architecture

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

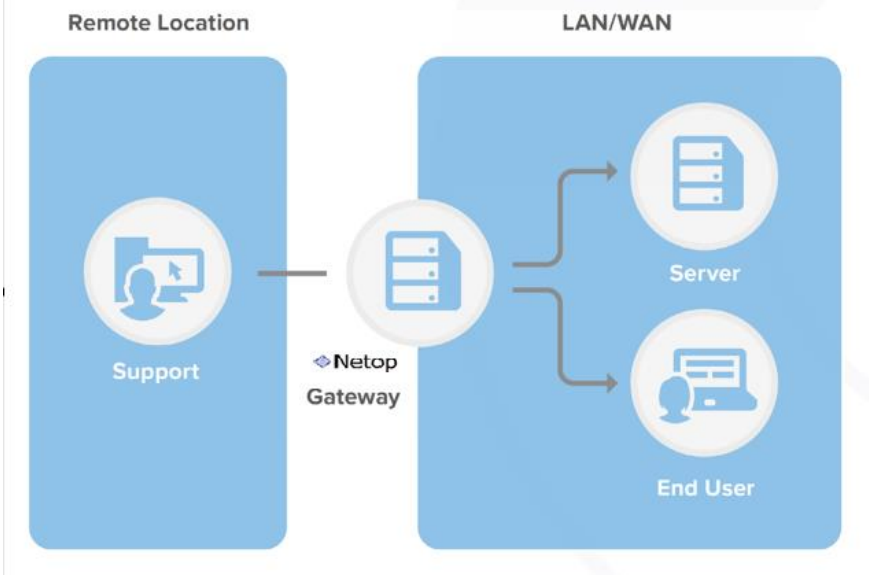
6.1 LAN/WAN Remote Access

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



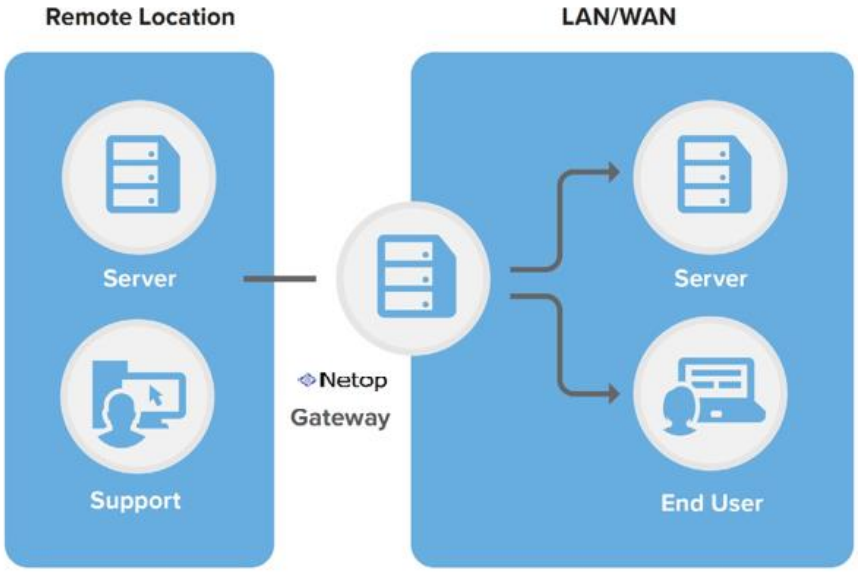
6.2 External Access to LAN/WAN Systems

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



6.3 Security Privileges for External Access to LAN/WAN Systems

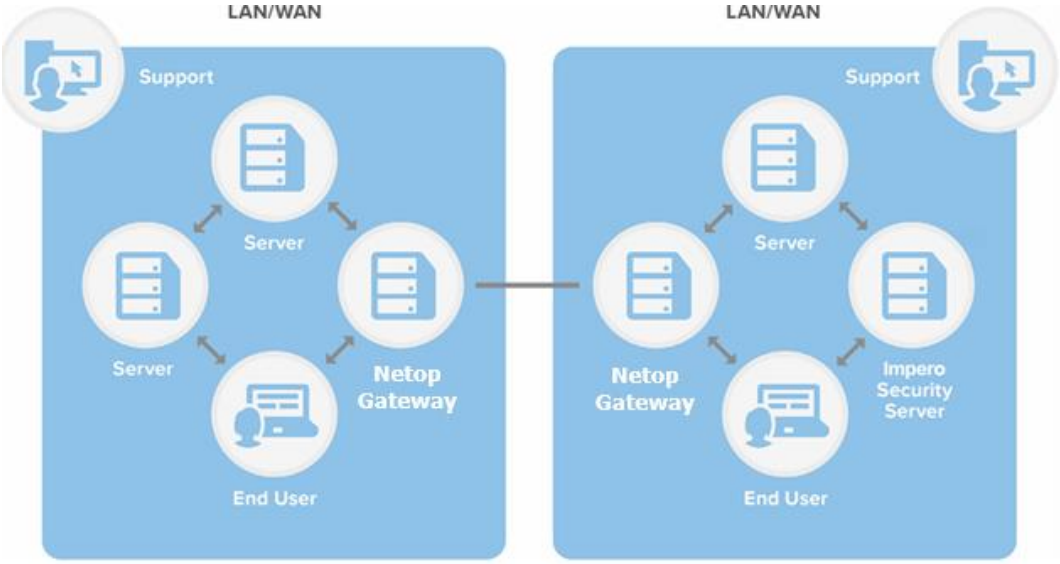
Organizations may need to manage permissions for hundreds to thousands of users while complying with security regulations and implemented policies. Security Server works with your existing infrastructure and integrates with Directory Services, RSA SecurID and Smart Cards.



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

6.4 Network Bridging

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



6.5 Virtualized Environments

Netop supports physical systems and virtualized systems.

6.5.1 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 data center. It enables fully personalized desktops for each user.

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

6.5.2 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.

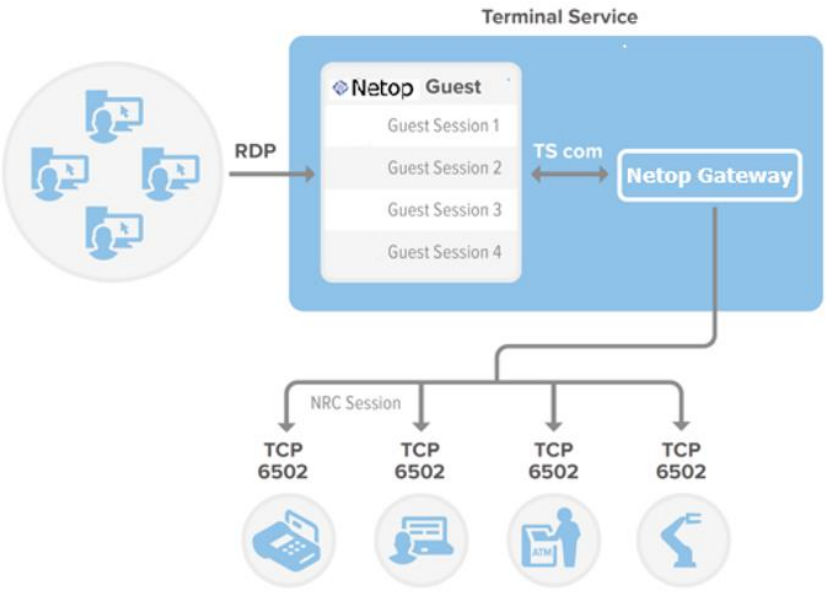
Netop can be run in RDS sessions and connect to other Netop modules running in sessions on the same RDS, another RDS, or other networked computers.

Since Netop modules running on RDS are required to communicate with Netop 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.

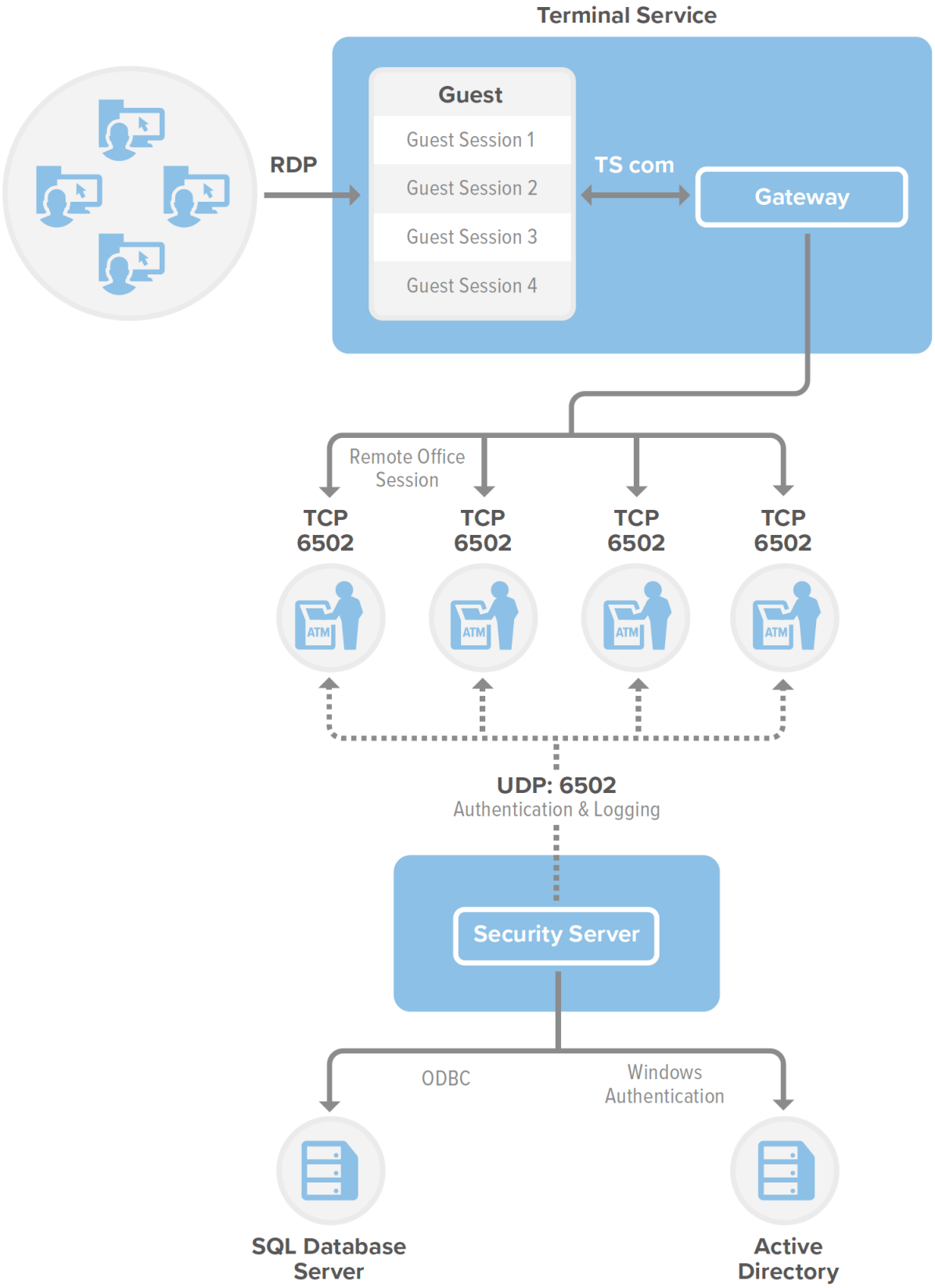
6.5.2.1 Guest running on RDS, Host outside the RDS

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.



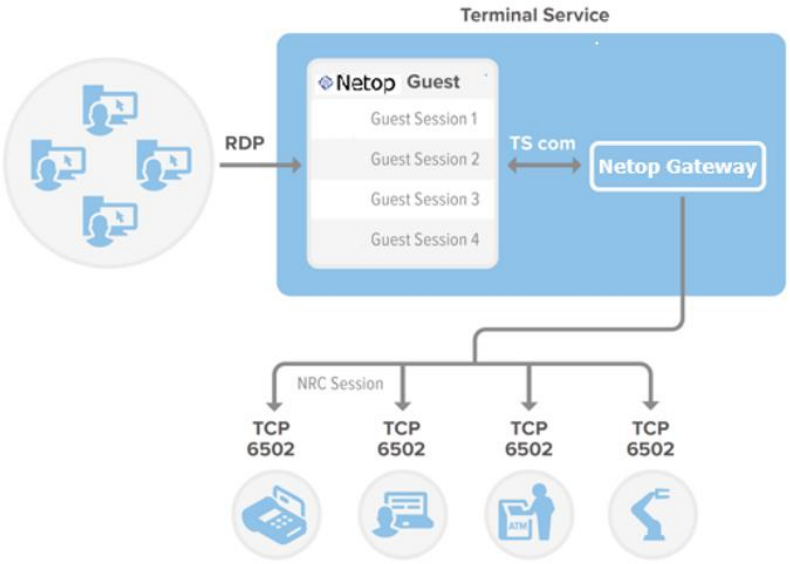
Guest to Host via Netop Security Service

Using Netop Security Server provides centralized security, administration authentication and authorization of all Connect 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.

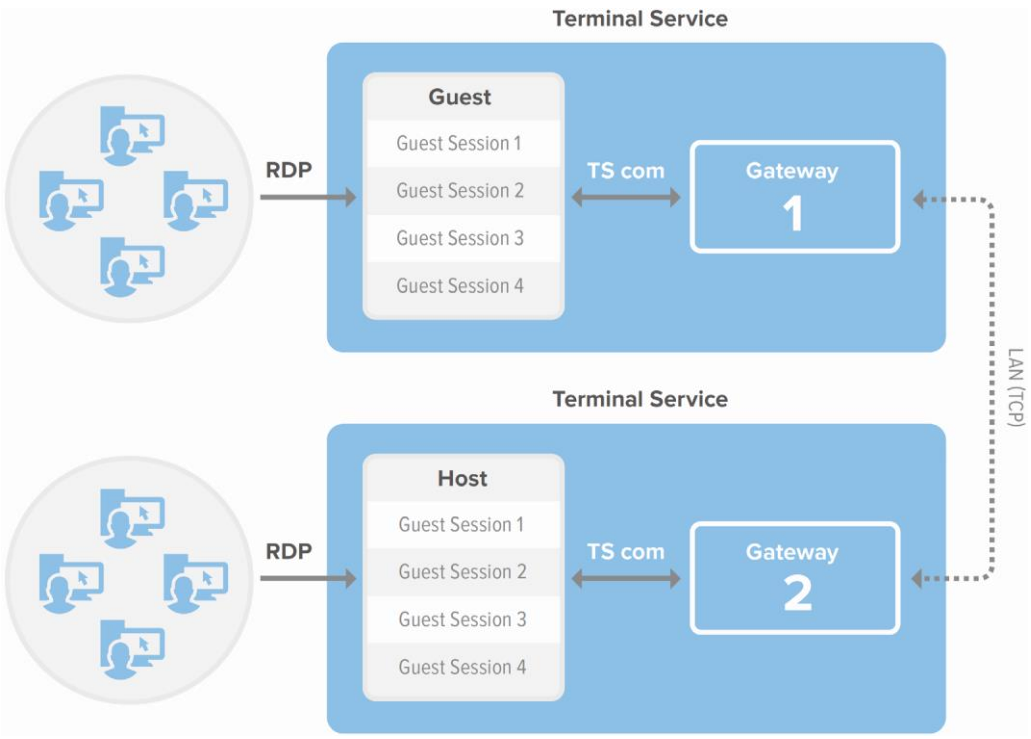


6.5.2.2 Guest outside the RDS, Host running on RDS

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.



6.5.2.3 Guest Running on RDS, Host running on a different RDS

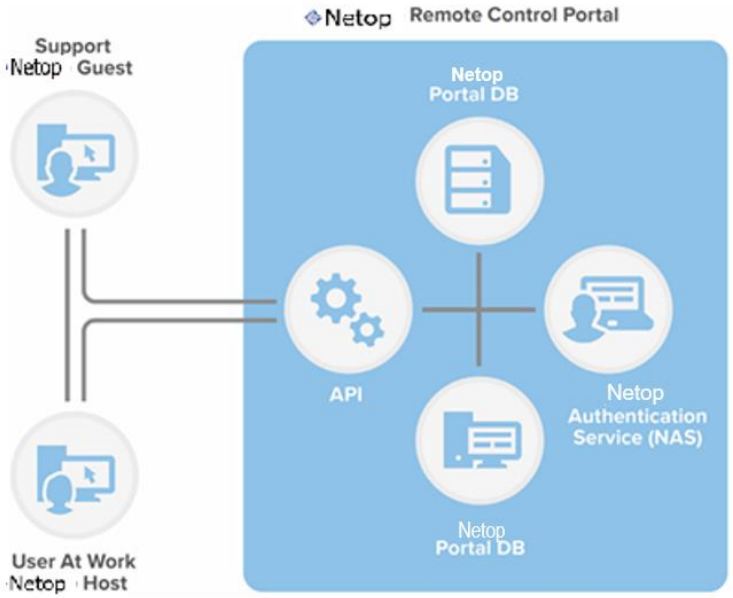


6.6 Secure remote access for third-party vendors: Cloud hosted Portal access

Netop for third-party vendors is now browser based as well, it's easy to use and easy to manage. Using the Netop 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 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 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

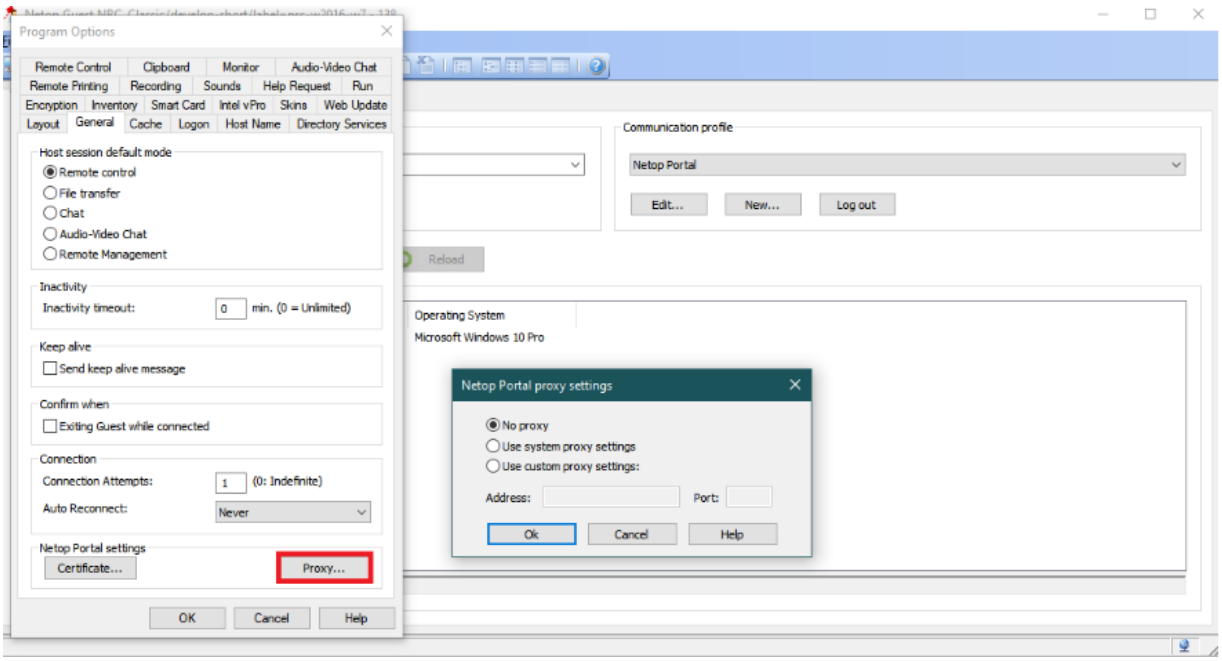
6.7 Netop Remote Control through Netop Portal – Network whitelisting

When you configure Netop Remote Control to use the **Netop Portal** communication, there are situations when access must be allowed through a company's proxy server and/or firewall. Rules or exceptions may need to be created that allow communication through a proxy server or firewall to communicate with the **Netop Portal** service.

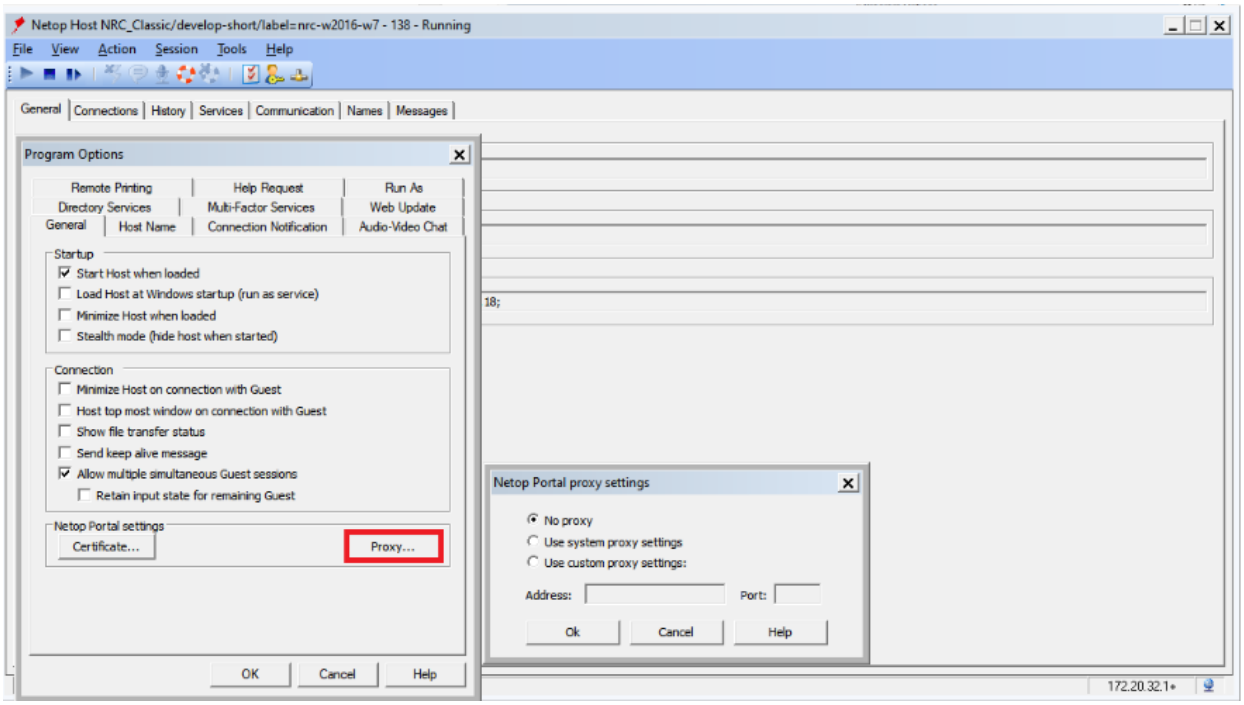
Proxy settings

A proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.
The Proxy settings can be defined on both Guest and Host, from Tools – Program Options – General – Proxy.
By default, no proxy is used when initializing the Netop Portal communication profile. This setting can be changed, to either attempt to detect and use the current proxy settings of the system (usually they can be seen by opening Internet Options – Connections – LAN Settings from Windows) or to manually specify a proxy server address and port to be used.
NOTE: Proxy authentication is not yet supported in this version.

- **Guest**



- **Host**



For the **Netop Portal** service, the following communication needs to be allowed:

NOTE: The **Netop Hosts** connect to the **Netop Portal** by using the **Netop** domains. Please refer to the **TCP netop.com** domains down below.

Outbound HTTPS (for SSL certificate validation):

- **GlobalSign ROOT CA R1**
  - *.globalsign.com
- **Amazon Root CA1**
  - ***.**amazontrust.com
- **Digicert**
  - ***.digicert.com**

netop.com domains

Outbound HTTPS (Port 443):

- accounts.netop.com[1]
- deviceapi.netop.com[1]
- portal.netop.com[1]
- portalapi.netop.com[1]
- portal-dl.netop.com[1]
- secure.netop.com[1]
- get.netop.com[2]
- remote.netop.com[2]
- nas.netop.com[3]
- wc-eu-wcs.netop.com[3]

TCP (Port 443)3

- wc-eu-cm.netop.com
- Ireland:
  - cs-eu-west.netop.com:443 | 52.211.129.227 (static IP);
  - s1-wcs-eu-west-1.netop.com | 18.203.12.45 (static IP);
  - s2-wcs-eu-west-1.netop.com | 52.214.177.66 (static IP);
- Frankfurt: cs-eu-central.netop.com:443 | 52.28.221.32 (static IP);
- Singapore:
  - cs-ap-southeast.netop.com:443 | 52.74.247.93 (static IP);
  - s1-wcs-ap-south-1.netop.com | 13.126.31.199 (static IP);
  - s2-wcs-ap-south-1.netop.com | 65.1.183.153 (static IP)
- Tokyo:
  - cs-ap-northeast.netop.com:443 | 54.64.34.84 (static IP) ;
  - s1-wcs-ap-northeast-2.netop.com | 3.34.222.89 (static IP);
  - s2-wcs-ap-northeast-2.netop.com | 3.35.80.48 (static IP);
- Sao Paolo:
  - cs-sa-east.netop.com:443 | 54.232.255.105 (static IP);
  - s1-wcs-sa-east-1.netop.com | 18.231.9.29 (static IP);
  - s2-wcs-sa-east-1.netop.com | 54.94.75.28 (static IP);
- N Virginia:
  - cs-us-east.netop.com:443 | 54.164.69.65 (static IP);
  - s1-wcs-us-east-1.netop.com | 54.89.190.50 (static IP);
  - s2-wcs-us-east-1.netop.com | 54.145.155.159 (static IP);
- Oregon: cs-us-west.netop.com:443 | 54.148.245.185 (static IP);
- Bahrain:
  - cs-me-south.netop.com | 157.175.10.43 (static IP);
  - s1-wcs-me-south-1.netop.com | 15.184.106.141 (static IP);
  - s2-wcs-me-south-1.netop.com | 15.185.152.47 (static IP);
- Cape Town:
  - cs-af-south.netop.com:443 | 13.245.250.222 (static IP);
  - s1-wcs-af-south-1.netop.com | 13.245.254.74 (static IP);
  - s2-wcs-af-south-1.netop.com | 13.245.148.178 (static IP);

WebSockets Secure (Port 443)

wss.netop.com[1]

TCP & UDP[2]:

- portal-ice-ap-northeast-v2.netop.com | 3.34.203.149
- portal-ice-ap-south-v2.netop.com | 13.126.197.58
- portal-ice-eu-west-v2.netop.com | 52.228.62.188
- portal-ice-us-east-v2.netop.com | 54.157.42.39

Outbound HTTPS (for SSL certificate validation):

- **GlobalSign ROOT CA R1**
  - *.globalsign.com
- **Amazon Root CA1**
  - ***.**amazontrust.com

If you protect your computer using a local firewall, make sure that you configure the firewall so that you allow the following Netop Portal executable files to run and be accessed from outbound LAN/internet access:

- nhstw32.exe (Host)
- ngstw32.exe (Guest)
- Netop Ondemand.exe

For assistance with your firewall configuration, please contact the firewall software provider.

Mass Deployment

To mass deploy the **Host** application when using the **Portal** communication profile, refer to the following link.

NOTE:
1 Services required by Netop Remote Control and Netop OnDemand.
2 Services required by Netop OnDemand.
3 Services required by Netop Remote Control.

7 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)
- SO 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

7.1 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.

7.1.1 Multi-Factor Authentication

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

7.1.2 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.

7.1.3 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.

7.2 Logging and audit

7.2.1 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.

7.2.2 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.

7.3 Patch Management

Every Netop 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.

7.4 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.

7.5 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.

7.6 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

7.7 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 tier1 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.

7.8 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.

8 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.

9 About Netop

About Netop

Netop sets the standard for secure remote control. Built for industries where there's no margin for error, it delivers the strongest security in its class — whether running in the cloud, on-premise, or in fully isolated networks. It speaks every language of technology, from the latest platforms to decades-old systems, and works out-of-band with Intel® vPro® to solve problems before anyone is on site. The result: fewer truck rolls, faster recovery, and complete confidence that your most critical systems are always within reach.

Our Story

Founded in Denmark, Netop quickly became a trusted name in remote access for organizations where security and uptime are paramount. Over the years, our solutions have been adopted by half of the Fortune 100, along with schools, governments, and enterprises in more than 90 countries.

Today, we're re-building the Netop brand with a renewed focus on innovation, modern security standards, and seamless integration into complex IT environments. Our mission is simple: empower IT teams to connect, control, and support any device, anywhere — without compromise.

Netop operates globally and is active in Germany, Finland, Denmark, the United Kingdom, Romania, the Philippines, Australia, Colombia, and the United States. Netop continues to partner directly with technical teams and enterprise leaders to solve their most pressing remote access challenges. As we look ahead, our vision is to lead the industry in secure, versatile, and future-proof remote-control solutions that give our customers total control and complete peace of mind.

10 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/