




PCI COMPLIANCE Checklist


Concerned about security compliance for your remote access solution?
 Here is how Netop helps you meet even the toughest standards.


PCI SECURITY REQUIREMENTS

- 
Use strong cryptography and security protocols such as secure socket layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. [4.1]

- 
Assign all users a unique ID before allowing them to access system components or cardholder data. [8.1]

- 
In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password or passphrase
 - Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) [8.2]

- 
Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. [8.3]

- 
Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations, and Acronyms). [8.4]

HOW NETOP REMOTE CONTROL MEETS THEM

Industry-Leading Encryption

Encryption

Data transmitted between Windows, Linux, Solaris and Mac OS X modules can be encrypted using the Advanced Encryption Standard (AES) with key lengths up to 256-bits. 7 different levels are available including Netop 6.x/5.x compatible for communication with older Netop modules.

Integrity and message authentication

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.

Centralized 2 and 3 Factor Authentication

Netop Authentication via Security Server

The Netop Security Server verifies the Guest identity against the database service that holds all the pre-defined Guest IDs and passwords.

Windows Authentication via Security Server

The Netop Security Server verifies the Guest identity by letting the Host relay the authentication process to a Windows Domain controller.

Directory Service Authentication via Security Server

The Netop Security Server verifies the Guest identity against a Directory Service via LDAP.

RSA SecurID with 'Triple-factor authentication' via Security Server

The Netop Security Server combines RSA SecurID 'two-factor authentication' with a shadow Netop Guest ID password.

- ✓ Limit access to computing resources and cardholder information only to those individuals whose job requires such access. [7.1]

- ✓ Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities. [7.1.1]

- ✓ Assignment of privileges is based on individual personnel's job classification and function. [7.1.2]

- ✓ Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. [7.2]

- ✓ Ensure that all system components and software have the latest vendor-supplied security patches installed. Deploy critical patches within a month of release. [6.1]

- ✓ Implement automated audit trails for all system components. [10.2]

- ✓ Secure audit trails so they cannot be altered. [10.5]

- ✓ Protect audit trail files from unauthorized modifications. [10.6]

Smart Card Authentication and Tunneling

By using a Smart Card and a Smart Card reader at the Windows Guest, the Windows Host is now able to authenticate the identity of the Guest user via the Security Server that communicates with a Windows server with Microsoft CA installed. If the Host computer demands local logon using Smart Card the Guest user's credentials will be tunneled to the Host in order to provide the information.

Netop Security Role

- A security role is a set of allowed actions.
- The user can create customized roles in addition to the pre-defined roles "Full access" and "View only" or "Deny"
- One or more groups and user accounts can be assigned to each Security Role.
- Total allowed actions are calculated by adding actions from each Security Role the user has membership of.
- Confirmed access is required if it's present in at least one Security Role.

Web Updates

Netop components can be configured to schedule and install automatic updates. This ensures that the latest software updates are made available through a secure and trusted channel using vendor-specific digitally signed certificates. Update directly through Netop hosted services or distribute and control the updates via your own internal web servers.

Netop Logging

Netop can record all sessions verbatim to document the entire remote session. 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.



RSA CERTIFIED



www.netop.com/secure