

## Security White Paper: Netviewer Admin 6.2

This white paper describes the security mechanisms contained in Netviewer Admin. The first part of the document focuses on the network transport layer. The second part describes the security mechanisms in the application layer.

### Security in the network transport layer

The security mechanisms of the transport layer provide the foundation for secure communication. The following describes how Netviewer protects the channels of communication through mutual authentication and encryption.

#### Encryption methods

Since the various Netviewer servers (Admin Master Server (AMS), Presence Server (PRS), Connection Server (CNS), and Communication Server (CS)) perform different tasks, a variety of methods are used to ensure that communication is secure.

Communication between the clients, the Connection Server, and the Admin Master Server is secured via TLS (standard RFC 2246). A 2048-bit RSA server certificate is used. Client programs authenticate themselves at this level via HTTP Digest Access Authentication (standard RFC 2617).

The pings sent by the host to the PRS are secured via Kerberos security mechanisms (standard RFC 4120).

Communication between clients is secured with AES in CBC mode and 256-bit session keys. Authentication headers (standard RFC 2404) assure data integrity.

The above-mentioned Netviewer servers are independent entities. The flows of signaling data (such as user authentication, key exchange) and session data are logically separated from each other.

### Host installation and computer management

Figure 1 depicts the process of host installation and computer management with Netviewer Admin, including encryption methods. The process is explained below.

1. During installation the host service authenticates itself via license key at the Admin Master Server (AMS) (TLS secured).
2. The AMS provides an authentication token and information about the Presence Server (PRS) (PRS addresses and Kerberos ticket) to the host service (TLS secured).
3. The host service pings the PRS (Kerberos secured). After the ticket expires (24 hours), the host service turns again to the AMS with the authentication token and receives a new Kerberos ticket and PRS information.
4. When the Master client starts, the master user authenticates himself to the connection server (CNS) with his unique ID (e-mail address and password) (TLS-secured).
5. The CNS sends AMS info to the master CM (TLS secured). The AMS info consists of AMS addresses and a ClientContext used to authenticate at the AMS.
6. The master CM pings the AMS in order to retrieve the information that it will display to the user (TLS secured).
7. In order to receive this information, the AMS asynchronously queries the PRS via a Netviewer-secured messaging system in the backend.
8. The AMS sends the information back to the master CM.

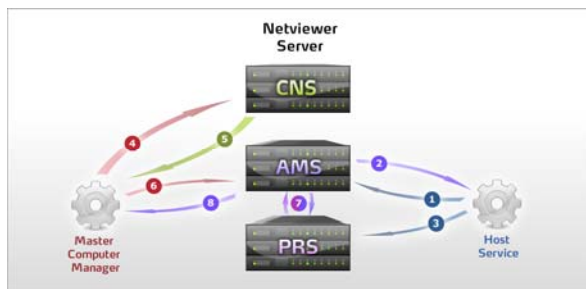


Figure 1

## Establishing a session

The following section describes encryption methods used when establishing a session (visualized in Figure 2).

1. The host service sends a Kerberos-secured ping to the Presence Server (PRS) at regular intervals in order to determine its status and to receive commands.
2. The master user selects from the master Computer Manager (master CM) the host with which he wishes to hold a session; the master CM contacts the Admin Master Server (AMS) with the session request for the target host (TLS secured).
3. The AMS plans a session with the Connection Server (CNS), receives from the CNS a session token and session number via a Netviewer-secured channel.
4. The AMS sends the master CM the session token and number (TLS secured).
5. The AMS transfers to the PRS a task for the relevant target host via a Netviewer-secured channel. This task also contains the session token and number.
6. The next time the target host pings the PRS, the PRS provides the target host with this task (Kerberos secured).
7. The host service starts the Host application, the master CM starts the Master application.
8. The Host and Master applications contact the CNS; the CNS and the relevant application mutually authenticate themselves via TLS handshake and http digest authentication. On the master side, the provided token serves as the authentication and authorization criterion; on the host side, the provided session number serves this purpose.

9. The CNS generates a 256-bit AES key and transfers the AES key and the communication server's (CS) address to the Host and Master applications. The CNS destroys the AES key, the CS does not know this key, the CS cannot decrypt the session data.
10. Host and Master applications contact the CS.
11. CS connects the Master and Host applications; the master transfers its host password over this end-to-end secured data channel; the host service validates the password against its own host password and the session is established.

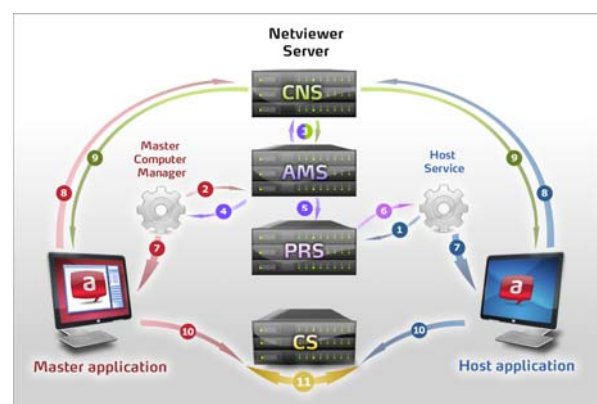


Figure 2

## Security in the application layer

In the application layer, Netviewer utilizes a variety of technological and process-supported security mechanisms:

- The Master and Host software are signed with a certificate provided by VeriSign, an independent certification body.
- When starting the Master program, the administrator must authenticate himself using his e-mail address and a self-chosen password.
- Access rights management in the computer manager prevents users from gaining unauthorized access to hosts for which they do not have access rights.
- If an additional host password has been defined at the host installation, the master user will be required to enter this following successful user authentication in order to access a specific host. This host password is stored only on the host computer and is not known to Netviewer AG.

- It is possible to display a wait screen while the master works on the host computer. This is useful if the master is performing confidential tasks such as entering license keys.
- The communication server is at no time able to access session data because these are encrypted end-to-end.

When the administrator connects to a host, the host may be in one of the following states:

- a) A user is signed on to the host computer.
- b) The host computer is blocked.
- c) The host computer is signed off.

These three scenarios are described below:

- a) A user is signed on to the host computer.

If the administrator starts a Netviewer Admin session while a user is signed on to the host computer, this user must explicitly permit access to his computer. Screen transmission and remote control will be available to the administrator only after the user of the host computer has given his approval. Until this occurs, the administrator will see only a black screen.

The administrator has the same authorizations and limitations as the signed on user. The administrator can switch the Windows user account during the session in order to receive additional rights, such as the right to access certain files.

The user who is signed on to the host can end the Netviewer Admin session at any time.

- b) The host computer is blocked.

The entire screen is visible, but the host computer must first be unlocked. The administrator can sign on using his administrator account or the account of the user who is currently signed on. The user account will determine the administrator's authorizations.

- c) The host computer is signed off.

The Windows login dialog is visible on the screen. The administrator can sign on using his administrator account or the account of a local

user. The user account will determine the administrator's authorizations.

### Logging and recording

At the end of the session, the Master program generates a TXT file that logs the duration of the session and the number of transferred bytes, among other things. In addition, all statistical session data are logged at the server.

All session data, including video and audio data, can be recorded and stored in Netviewer's proprietary NVL format.

### Summary

The security of Netviewer Admin and the integrity of transferred data are ensured through the use of several different security mechanisms:

- Netviewer Admin is signed with the Netviewer certificate, which was issued by VeriSign, an independent certification body.
- TLS is used for mutual authentication and for encryption between the client, connection server, and Admin Master Server.
- A 256-bit AES key is used to encrypt the session data.
- The master and the host use the optional three-character (or longer) host password as additional access limitation. The unique host password is defined during installation of the host and is stored only on the host computer.
- The various Netviewer servers are independent entities.
- The communication server does not know the temporary 256-bit AES key used to encrypt the session data.
- The user authenticates himself to the Master program with a self-defined password and his e-mail address.
- Access rights management prevents unauthorized host access.
- All sessions are encrypted end-to-end.
- All session data can be recorded for later review.



Version 1.0 January 2011

© 2011 Netviewer AG. Netviewer Support, Meet, Admin, Webinar, Enterprise Server, Standard Server, and das Netviewer logo are registered trademarks of Netviewer AG. All rights reserved. All other brands are the property of their respective owners.