



## Release notes – version 9.0

Danware is proud to introduce NetOp Remote Control 9.0 as the coming shipping version. It will also be available as a commercial upgrade to our existing customers using version 8.0 or earlier.

## What's new in version 9.0?

This is the new features in headlines grouped by function. Later in the document detailed information about each new feature has been included.

The product in general contains all functions and platforms support available in NetOp Remote Control version 8.0 except the ones listed under the section "Discontinued functions and platforms".

## Windows Operating Systems

### Security

- ✓ **Smart Card authentication** – allows the Host to verify the Guest identity via Security Server.
- ✓ **Password length** – allow NetOp modules to work with Windows passwords up to 64 bytes.
- ✓ **Disconnect password** – optional password to prevent the Guest user from closing the session.
- ✓ **Switch to window mode password** – optional password to prevent the Guest user leaving full screen mode.
- ✓ **Active Directory computer support** – new Host object type for authorization in the Security Server.
- ✓ **Confirm Access enhancements** – New flexible options to adjust the user accept.

### Installation

- ✓ **Windows Installer** – full support for MSI installation including customized transform files.
- ✓ **Transform file Editor** – configure installation and Host settings and save all changes in a MST file.
- ✓ **Deploy MSI packages** – NDU can now also remote install NetOp MSI packages.

### Multi Guest Session

- ✓ **Auto Take Control** – Guest can automatically withdraw keyboard and mouse control from another Guest computer by using the keyboard or clicking the mouse – mouse movements do not activate this.
- ✓ **Retain state for remaining Guest** – Enhanced security using Multi Guest Session.

### Communication

- ✓ **Connection Attempts** – number of retries used to connect, default 1, 0 means infinity.
- ✓ **Auto reconnect** – in case an unintended disconnect occurs or the other end disconnects the module can reconnect automatically.

### Enhanced feature set

- ✓ **Monitor mode** – connect and view a group of Hosts one at a time.
- ✓ **Video support** – use web cams for a new session to view the remote user.
- ✓ **Snapshot** – allows the Guest to save the current Host desktop image as a file.

# NetOp Remote Control



- ✓ **Service Ticket request help** – allows the Host to seek for a specific Guest.
- ✓ **Scheduled cleanup** – the Security Server must at a fixed schedule delete Active Session entries older than x hours. A corresponding entry is inserted in the NetOp Log to balance the session start. An option in the Security Manager can manually clear the Active Session.
- ✓ **Sort Comment column** – the Guest Phonebook can now be sorted by this field.
- ✓ **Hide Guest main interface** – For use in third party products the Guest application and notification area icon can be hidden.
- ✓ **XML based address book** – New format for Connection properties

## Discontinued functions and platforms

The following have been discontinued:

- ✓ **Windows CE platforms** have been moved from NetOp Remote Control to a new product line called NetOp Mobile & Embedded.

## Detailed information

### Security

- ✓ **Smart Card authentication**  
A new authentication method using Smart Card has been introduced. It allows the Host to verify the Guest identity by prompting the Guest user to insert a Smart Card into the Guest computer's card reader and type the corresponding PIN code. The authentication may be performed locally on the Host or it may be performed via Security Server.

The Guest connects to the Host. The Host contacts the Security Server and receives the message that the Preferred Guest Type is defined as "Guests enter Smart Card and PIN". The Security Server generates a random string called a challenge and transmits this to the Host which forwards the challenge and the Smart Card Logon requirement to the Guest. The Guest user enters PIN to activate the authentication process.

The Smart Card digitally signs the challenge with Guest user's private key. The Guest user's username, the signed challenge and the certificate containing the public key are transmitted to the Host. NetOp encrypts the transmission of the login data with 256-bit AES encryption unless all encryption methods except NetOp 6.x comp. are disabled.

The Host forwards username, signed challenge and certificate to the Security Server. NetOp encrypts the transmission of the login data with 256-bit AES encryption unless all encryption methods except NetOp 6.x comp. are disabled. The Host also forwards details about the Host identity to the Security Server. From its certificate store the Security Server uses the server certificate that issued the Guest user's Smart Card certificates to confirm the genuineness of the forwarded Guest user certificate and also checks that it has not been revoked.

The Security Server now authenticates the Guest user identity by checking the signed challenge using the Guest user's public key. Failing the authentication will make the Host re-prompt the Guest user until exceeding the maximum number of login retries. The error dialog box will not reveal what values that contained invalid information to prevent hacking. Entering invalid login data will create a

# NetOp Remote Control



NetOp log event, if activated. If the certificate and the signed challenge data supplied for the authentication were valid, the Security Server first checks the Guest user's Windows group memberships at a Windows Domain controller.

The public key certificate contains the Guest user's domain information. Then the Security Server performs an SQL query against the Security Server database with the found Guest user identities (Windows username, Windows Domain name and Windows group memberships) and Host identities (depending on the Preferred Host Type). Depending on the query result, the Guest user access is allowed or denied.

- ✓ **Password length**  
NetOp modules are now able to work with Windows passwords up to 64 bytes in length to fully comply with Windows password/account policies.
- ✓ **Disconnect password (Kiosk mode)**  
An optional password to prevent the Guest user from closing the session has been added. This is part of a number of new Kiosk Mode features.
- ✓ **Switch to window mode password (Kiosk Mode)**  
An optional password to prevent the Guest user leaving full screen mode has been added. This is part of a number of new Kiosk Mode features.
- ✓ **Active Directory computer support**  
To the Security Server the computer name has been added as a new Host object type for authorization in Active Directory.
- ✓ **Confirm Access enhancements**  
New flexible options to adjust the user accept has been introduced. It is now possible to define Confirm Access with the following exceptions:
  - Computer locked
  - No user logged on
  - Guest user logged on (this Host)

## Installation

- ✓ **Windows Installer**  
The support for MSI installation has been enhanced to include customizable transform files and each NetOp module now uses its own installation file (msi). The interactive windows Installer setup wizard is designed according to Microsoft MSI recommendations and handles Installation, Modification, Upgrade and Removal.
- ✓ **Transform file Editor**  
A Transform Editor is now available. It is used to create transform files (.mst) that contain information needed to deploy and install NetOp modules with a user defined configuration using Windows Installer.
- ✓ **Deploy MSI packages**  
NetOp Deployment Utility can now also remote install NetOp MSI packages. The configuration for MSI installations is done using the Transform Editor and NDU is only used for deployment and installation. NDU still handles configuration, deployment and installation of InstallShield packages.

# NetOp Remote Control



## Multi Guest Session

### ✓ **Auto Take Control (Kiosk Mode)**

Guest can automatically withdraw keyboard and mouse control from another Guest computer by using the keyboard or clicking the mouse – mouse movements do not activate this. The feature is especially useful for industrial use on large machinery, where one person needs to be able to control the central machine computer from different terminals placed around the machine. This is part of a number of new Kiosk Mode features.

### ✓ **Retain state for remaining Guest**

The Host module now has an extra checkbox in Program options under General to prevent a Guest without multi Guest session administrator rights to automatically obtain the right to take keyboard and mouse control once he is the last remaining Guest connected to the Host.

The effect is that the automatic enabling of the Take Control icon in the remaining Guest toolbar is disabled, if the check box *Retain state for remaining Guest* on the Host is set AND the Guest does not have Multi Guest Session administrator rights.

## Communication

### ✓ **Auto reconnect (Kiosk Mode)**

In case an unintended disconnect occurs or the Host end disconnects the Guest can reconnect automatically. This is part of a number of new Kiosk Mode features.

### ✓ **Connection Attempts (Kiosk Mode)**

The number of retries used to connect can now be defined. Default is 1, 0 means infinite number of retries. This is part of a number of new Kiosk Mode features.

## Enhanced feature set

### ✓ **Monitor mode**

Connect to and view a group of Hosts one at a time. The feature causes the Guest to cycle through the selected Hosts thus making it easy to use for surveillance and monitoring. The cycling can be paused for remote control of current Host and resumed afterwards.

### ✓ **Video Chat**

The existing audio chat session has been expanded in order to support video. Using web cams at Guest and Host enables transfer of the video signal from the camera to the opposite end of the connection.

### ✓ **Snapshot**

Two buttons on the tool bar allow the Guest user to save the current Host desktop image either to the Guest clipboard or as a file locally on the Guest. Depending on a setting on the Guest the image will be either the full Host desktop or the part of the Host desktop currently visible on the Guest.

### ✓ **Service Ticket request help**

This allows the Host to seek for a specific Guest (Help Provider) that matches the Service Ticket number supplied to the helpdesk by the Host (user) in order to route the Request Help from the Host to the correct Guest.

### ✓ **Scheduled cleanup**

The Security Server must at a fixed schedule delete Active Session entries older than x hours. A corresponding entry is inserted in the NetOp Log to balance the session start. An option in the

# NetOp Remote Control



Security Manager can manually clear the Active Session. This may be needed in order to neutralize mismatch in the log due to broken remote control sessions that are prevented from reporting end of session to the Security Server in the normal way.

✓ **Sort Comment column**

The Guest Phonebook can now be sorted by the Comment field.

✓ **Hide Guest main interface**

When the Guest functionality is used in help desk or system management environments like Remedy, SMS or HP OpenView, it's often a requirement that the Guest main interface is invisible and the functionality works as a hidden service activated by calling the module with command line switches and variables like IP address and protocol.

The Guest main interface can be hidden by selecting the Stealth mode check box found in Tools /Program options / Layout. Next time the Guest module starts, it will be hidden.

To reveal the Guest main interface again the command line program ShowGuest.exe must be run while the Guest is loaded. This will enable the main interface until the Guest is unloaded and loaded again. To keep the Guest in visible mode, the check box must be unchecked.

The ShowGuest.exe is a part of the Guest installation and can as a feature be deselected to prevent the Guest user from retrieving the Guest main interface.

✓ **XML based address book –**

For easier import/export and integration with other systems the address book files (.dwc) holding connection properties are now in xml format.