Connect

User Guide

Friday, October 29, 2021

Table of Contents

1 Overview

1.1 Connect Modules

Impero Connect is comprised out of the following modules:

- Impero Guest: Enables the computer user to remote control and interact with another computer that runs a Host or an extended Host.
- Impero Host: Enables the computer to be remote controlled and interacted with from a computer that runs a **Guest.**
- Impero WebConnect / 3: A secure web-based service consisting of a Connection Manager that serves as a meeting hub for the Guests and Hosts, and at least one Connection Server that routes the traffic between the Guests and Hosts. The Connection Server is an extended Host. This is available as a hosted service or as an on-premise application. WebConnect 3.0 has an improved security.
- Impero Portal: A management console allowing the users to manage authentication and authorization, view connected devices, do remote sessions and create packages for device enrollment.
- Impero Browser Based Support Console: A browser based interface for the Guest, that allows the supporters to remote control devices, no installation required.
- Impero Security Server: An extended Host that uses a central database to manage Guest authentication and authorization across the network. It also provides centralized logging capabilities and extended authentication methods including RSA.
- Impero Gateway: An extended Host that can route Impero traffic between different communication devices. Gateway can receive Impero communication that uses one communication device and send it using another communication device. This ability enables Gateway to provide communication between Impero modules that use mutually incompatible communication devices, typically to connect Impero modules inside a network or terminal server environment with Impero modules outside a network or terminal server environment.

See also

The Impero Connect Administrator's Guide for more information about the Security Server, the Gateway and the Name Server.
The Impero WebConnect Installation Guide for more information about the WebConnect Connection Server.

1.2 Security

You can prevent changes to the installed **Connect** modules by using a maintenance password. You also can hide the **Host** module from the end user via the stealth mode feature.

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

- Upon connection to the **Host**, the **Guest** can be authenticated against their Windows login credentials.
- Security roles can be defined on the **Host** which dictate what remote control actions the authenticated **Guest** can perform.
- The policy functions can determine how the **Host** behaves before, during and after the remote control session, including notification, confirm access and confirm access via email, and illegal connection attempts.
- The communication between the **Impero** modules can be encrypted using different methods that depend on the environment.
- Audit trails including all the remote control events and physical session recordings can be centrally maintained.

All the **Connect** modules can log **Impero** events locally and centrally in an **Impero** log. You can protect the **Guest** and **Host** setup with a maintenance password.

See also
Guest Access Security
Program Options (Encryption tab and Smart Card tab)
Administrator's Guide

1.3 Communication profiles

To make the **Impero** modules to able to communicate with each other, it is necessary that you define a communication profile. A communication profile is a specific configuration of a communication device.

A communication device is a **Impero** adaptation of a generally available communication protocol or a **Impero** proprietary communication protocol.

A newly installed **Impero** module includes the default communication profiles.

NOTE: Communication profiles are stored in the Impero configuration file (comprof.ndb). The comprof.ndb file is located in the folder:

- `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for the **Guest**
- `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for **Host**-based modules.

Refer to the Impero Knowledge Base, for more information on how to configure **Impero** files.

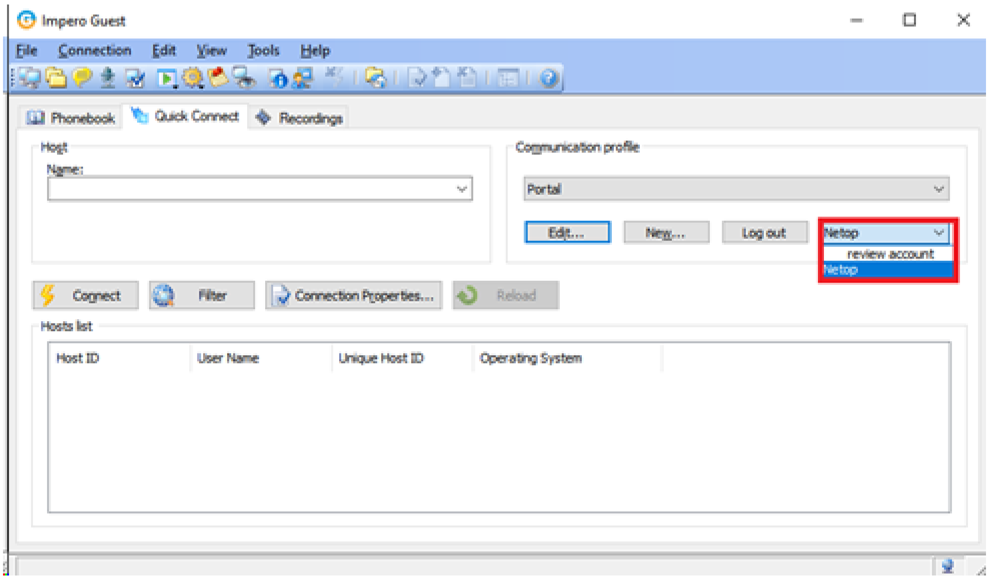
See also

Communication Profiles

2 Managing Hosts

2.1 Multiple Accounts

To switch to secondary accounts in the **Guest**, simply click on the dropdown menu and select the secondary account that you want to switch to.



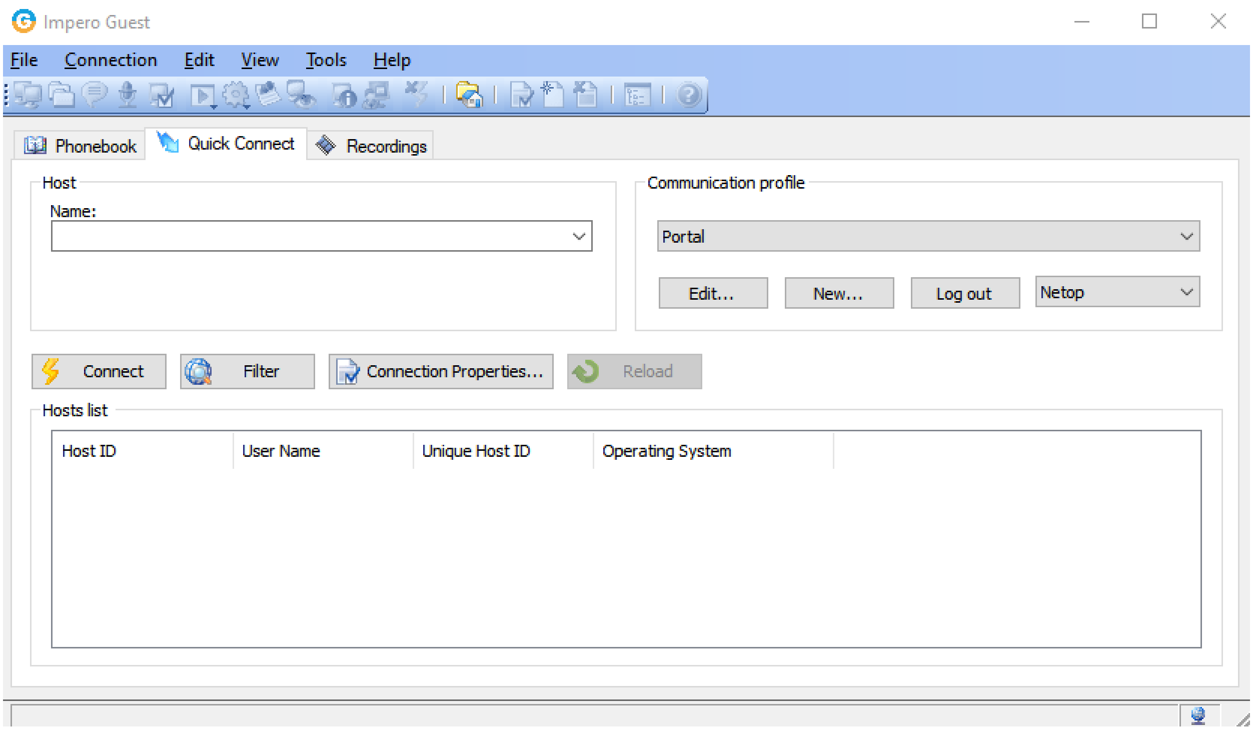
By default, the primary account is the account that the user was first invited to. User settings are not transferred from the primary to any other secondary accounts. As such users can have different permissions, roles, or other settings on other secondary accounts without them interfering with each other.

When removing a user that belongs to multiple accounts from its primary account, the user is deleted from all the accounts.

If Multi-Factor Authentication is enabled for users on the secondary account, users are prompted to enter the MFA code upon logging in when switching to that account.

2.2 Start and end a remote control session

You can connect and start a remote control session in several ways.
Before starting a remote control session, specify a communication profile corresponding to a communication profile (default is TCP/IP = UDP) enabled on the **Host** in the **Communication Profile** section of the **Quick Connect** tab.



Communication profile: Portal

Netop

Host ID	User Name	Unique Host ID	Operating System

To start a remote control session from the Guest window, Quick Connect tab, proceed as follows:

1. In the Quick Connect tab, in the Host section, specify a Host name or address as required by the selected communication profile.

2. Click on the Connect button to connect and start a remote control session. Alternatively, click on a toolbar button or select a command from the Connection menu to connect and start a session. Typically, a Impero logon window is displayed prompting you to log on to the Host.

3. Type your credentials to log on. When you have logged on to the Host, the session starts.

Connections are displayed on the Connections tab. You can change session type or execute action commands by right-clicking on a Host from the Connections tab.

Other ways to connect from the Quick Connect tab

1. Click on the Browse button (Applies only when using profiles that use UDP and WebConnect).

2. Select one or multiple Hosts in the Browse list (Impero Network tab).

3. Click on the Connect button. Alternatively, click on a toolbar button or select a com-

mand on the Connection menu to connect and start a session.

Typically, a Impero logon window is displayed prompting you to log on to the Host.

4. Type your credentials to log on. When you have logged on to the Host, the session starts.

Alternatively:

1. Click on the Windows Network tab at the bottom of the window.
2. In the Windows Network list navigate to and select one or multiple Hosts.
3. Click on the Connect button. Alternatively, click on a toolbar button or select a command on the Connection menu to connect and start a session. Typically, a Impero logon window is displayed prompting you to log on to the Host.
4. Type your credentials to log on. When you have logged on to the Host, the session starts.

To start a remote control session from other Guest window tabs, proceed as follows:

1. In the Phonebook tab, History tab, or Help Request tab, select one or multiple Hosts.
2. Click on a toolbar button or select a command on the Connection menu to connect and start a session. Typically, a Impero logon window is displayed prompting you to log on to the Host.
3. Specify your credentials to log on. When you log in on to the Host, the session starts.

Phonebook	Stores Host records that you have created or saved from the Quick Connect tab or History tab.
History	Stores records of previous Host connections.
Help Request	Displays a list of pending Host help requests.

See also

Save connection information in the phonebook

To end a remote control session, proceed as follows:

In the Remote Control window of the Guest, click on the Disconnect button on the toolbar. Alternatively, click on the Remote Control button from the toolbar.

Alternatively:

In the **Guest** window, select the connection from the **Connections** tab.

Click on the **Disconnect** button from the toolbar.

Alternatively, select the **Disconnect** button from the **Connection** menu.

The **Host** user can also end the session by selecting **Disconnect** in the **Session** menu.

2.3 Use Impero phonebook to manage connections

You can save connection information as records in the **Impero** phonebook for a later use. The phonebook works much like a personal quick-dial telephone directory with the communication profile needed to connect and passwords.

Passwords are encrypted by a secure algorithm.

Phonebook records are saved as files with the extension `*.dwc` in the `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest\PhBook` folder. The dwc files are **`*.xml`** files. You can view the content of these files in any text editor.

From the **Quick Connect** tab

- You can add connection information to the phonebook by right-clicking on a **Host** record in the pane in lower part of the **Guest** window and selecting **Add to Phonebook** after having browsed for **Hosts**.
- In the displayed dialog box select the phonebook folder in which you want to save the information and click on **OK**.

Alternatively:

1. You can copy connection information to the phonebook by right-clicking on a **Host** record in the pane in the lower part of the **Guest** window and selecting **Copy** after you browsed for the **Hosts**.

2. Click on the **Phonebook** tab, right-click on the folder in the left pane in which you want to save the information, and then select **Paste**.

The **Host** record is displayed in the right pane of the **Phonebook** tab.

From the **History** tab

1. You can add connection information to the phonebook, by right-clicking on a **Host** re-

cord in the right pane of the **History** tab and then by selecting **Copy**.

2. Click on the **Phonebook** tab, right-click on the folder in the left pane in which you want to save the information, and select **Paste**.

The **Host** record is displayed in the right pane of the **Phonebook** tab.

Creating phonebook records in the **Phonebook** tab

To create a **Phonebook** record, proceed as follows:

1. Click on the **Phonebook Entry** button from the toolbar.

Alternatively, select **New** > **Phonebook Entry** in the Edit menu.

The **Connection Properties** dialog box is displayed.

2. Fill in the fields in **Connection Properties** with the necessary information and click on **OK**.

See also

Connection Properties

Start and end a remote control session

2.3.1 Edit phonebook records

If you want to edit a phonebook record and change information such as the specified communication profile or the **Host** credentials, you can do that in **Connection Properties**.

To edit a **Phonebook** record, proceed as follows:

1. Select the phonebook record in the right pane of the **Phonebook** tab.

2. Click on the **Connection Properties** button on the toolbar.

Alternatively, select **Connection Properties** from the **Edit** menu. The **Connection Properties** dialog box is displayed.

3. Edit the information and click on **OK**.

You can move phonebook records between the Phonebook root folder and user-created folders using drag-and-drop.

See also

Connection Properties

2.3.2 Protect your phonebook record files with a password

To protect your phonebook record files (`*.dwc`), you can specify a password for each file in **Connection Properties**.

You can specify that the password should be entered every time someone wants to use or edit the file, or you can specify that the password should be entered only to edit the file.

To specify a password for a phonebook record file, proceed as follows:

1. Select the phonebook record in the right pane of the **Phonebook** tab.
2. Click on the **Connection Properties** button from the toolbar.
3. Click on the **Protect Item** tab.
4. Specify a password and confirm it.

If you want the password only to apply to editing, select the **Connect without password** check box.

5. Click on **OK**.

See also
Connection Properties

2.3.3 Organize your phonebook

You can create new folders in the phonebook to organize your connection information and make it easier to find the **Host** that you want to connect to.

To create a new folder, proceed as follows:

1. In the **Edit** menu, select **New** > **Folder**.
2. Enter a name for the folder.
3. Click on **OK**. Alternatively, right-click and create a folder using the shortcut menu.

To create a new subfolder, proceed as follows:

1. In the left pane, select the folder in which you want to create a subfolder.
2. In the **Edit** menu, select **New** > **Folder**.
3. Enter a name for the folder.
4. Click on **OK**. Alternatively, right-click on the folder in which you want to create a sub-

folder, and create a subfolder using the shortcut menu.

You can use drag-and-drop to rearrange your folders.

2.3.4 Export and import phonebook data

You can export and import phonebook data in a `*.csv` (comma separated values) file. This is useful for example if you want to copy phonebook data from one computer to another.

You can also populate the phonebook using existing data from another system, for example by importing data from **Active Directory**.

Scripts can use the phonebook data to call **Hosts**.

To export the phonebook data, proceed as follows:

1. Select a folder in the left pane of the **Phonebook** tab or select one or multiple phonebook records in the right pane.
2. In the **File** menu, select **Export**.
3. In the displayed dialog box, specify the path and name of the `*.csv` file that you want to save the phonebook records to. If you specify only a file name, the export file is saved to the folder in which the **Guest** is installed.
4. Select the **Export Passwords** check box if you want to include passwords for the phonebook records in the `*.csv` file.
5. Click on **OK**.

You cannot export all the **Connection Properties** properties for a phonebook record. This applies to the properties of the **Display** tab, the **Keyboard/Mouse** tab, the **Compression/Encryption** tab, the **Desktop** tab, and the **Record** tab. You can specify these properties when importing.

Csv file syntax

The `*.csv` file is a plain text file. For each phonebook record, the file contains a line of values separated by commas according to this syntax:

```
<Folder path>,<Description>,<Phone number>,<Name>,<Comment>,<Communication profile>,<Host logon name>,<Host logon password>,<Host logon domain>, <Gateway logon name>,<Gateway logon password>,<Gateway logon domain>, <Protect item password>,<Wake on LAN MAC address>,<Logon credentials flags>,<Custom application description>,<Custom application command line>
```

Passwords are encrypted as 64-digit hexadecimal checksums with the prefix ENCRYPTED:.

To import the Phonebook data, proceed as follows:

1. In the File menu, select Import to Phonebook.
2. Specify the path to and name of the `*.csv` file that you want to import.
3. Click on the Connection Properties button if you want to specify the Display tab properties, Keyboard/Mouse tab properties, Compression/Encryption tab properties, Desktop tab properties, and the Record tab properties.
4. Click on OK.

2.3.5 Add a phonebook reference

You can add a phonebook reference in the Guest phonebook. A phonebook reference links to a folder containing phonebook records (`*.dwc` files), for instance a phonebook shared by multiple users.

To add a Phonebook reference, proceed as follows:

1. Right-click in the left pane of the Phonebook tab and select the Add Phonebook reference.
2. In the Add Phonebook Reference dialog box, specify the folder containing phonebook records that you want to link to.
You can browse for the folder by clicking on the button next to the Folder field.
3. Click on OK.
A phonebook reference to a folder containing phonebook records is displayed in the left pane of the Phonebook tab, and the records are displayed in the right pane.
You can edit the phonebook reference by right-clicking on the reference and selecting the Edit Phonebook reference.

2.3.6 Use Remote Desktop from the Netop phonebook

The **Impero** phonebook provides access to using the **Remote Desktop** functionality. This means that you can use one tool for all your remote control sessions.

For information about configuration of RDP (Remote Desktop Protocol), please refer to the Microsoft documentation.

To create a **Remote Desktop** entry in the phonebook, proceed as follows:

1. Right-click in the right pane of the **Phonebook** tab and select **New** > **Remote Desktop Entry**. The **Remote Desktop Connection** dialog box opens.

2. In the **General** tab, specify the logon settings and a `*.rdp` file to be used for the entry.

A **Remote Desktop** entry is created and displayed in the records pane of the **Phonebook** tab together with a pseudo communication profile.

Use the **Remote Desktop** phonebook entry you created to start a remote desktop session.

For information about the use of Remote Desktop, click on the **Help** button in the **Remote Desktop Connection** dialog box.

2.4 Keyboard, mouse and display during remote control

By default, the **Guest** and the **Host** share the keyboard and mouse control during remote control.

If allowed by the **Guest Access Security** settings on the **Host**, you can block the **Host** user from using the keyboard and mouse. To do so, click on the **Lock Keyboard and Mouse** button from the toolbar in the **Remote Control** window.

You can also blank the **Host** screen, if allowed by the **Guest Access Security** settings on the **Host**, so that what is going on on the **Host** computer cannot be seen by anyone. To do so, click on the **Blank Display** button from the toolbar.

NOTE: While **Blank Display** works with most **Host** computers, the design of some display adapters prevents applying it.

Typically, these two functions are used together, for example if you are carrying out maintenance work on an unattended **Host** computer or working on your office computer from home, and you do not want anyone passing by to see what you are doing or to interfere.
In the **Guest Connection Properties**, in the **Startup** tab, you can specify that the **Host** computer screen should be blanked and the keyboard and mouse should be locked in the **Host** computer from the start when you establish a connection to the **Host**.

See also
Guest Access Security
Connection Properties (Keyboard/Mouse tab)

2.5 Generate a Host inventory

If allowed by the **Guest Access Security** settings on the **Host**, you can generate an inventory of the **Host** computer hardware and software. The inventory are displayed on the **Inventory** tab of the **Guest**.

To define what you want the **Host** inventory summary to contain, proceed as follows:
1. In the **Tools** menu, select **Program Options**.
2. Click on the **Inventory** tab, select/clear selection of elements on the **Summary view** list, and click on **OK**.

To generate a **Host inventory**, proceed as follows:
1. On one of the **Guest** window tabs, select the **Host** computer for which you want to generate an inventory.
The **Guest** can connect and generate an inventory from the **Quick Connect** tab, the **Phonebook** tab or the **History** tab.

2. Click on the **Get Inventory** button in the toolbar.

Alternatively, select **Get Inventory** in the **Connection** menu.

Alternatively:
If you are already connected to a **Host**, in the **Remote Control** window, click on the **Get Inventory** button on the toolbar.

The inventory as defined in the **Inventory** tab in **Program Options** is displayed in the **Inventory** tab in the **Guest** window.

See also

Program Options (Inventory tab)
Process Host computer inventory information

2.5.1 Process Host computer inventory information

You can use **Host** computer inventory information to get an overview.

In addition to this you can specify an external program to be executed after an inventory scan has completed. Inventory data is saved in `*.xml` files.

You can also specify custom inventory items that you want to include when generating inventories, that is items not included in the list of inventory items in the **Inventory** tab in **Program Options**.

For example you might want to check what version of a certain program is installed on a number of **Host** computers. If you know the registry key for the program version in question, you can specify a custom inventory item for the registry key. You can then generate inventories telling you what version of the program is installed.

To specify a program to run after inventory scan, proceed as follows:

1. In the **Tools** menu, select **Program Options**.
2. Click on the **Inventory** tab, and click on the **Advanced** button.
3. In the **Advanced inventory** option dialog box, specify whether you want to run a program after generating an inventory for each **Host** or after generating inventories for all the **Hosts** for which you choose to generate the inventories.
4. In the **File** name field, specify the program file name. Click on the **Browse** button to find the program.
5. Then click on **OK**.

When you generate **Host** inventories, the specified program runs automatically afterwards as specified.

Specify custom inventory items

You can retrieve additional information during the inventory scan, such as environment variables, registry keys, file information etc.

1. In the Tools menu, select Program Options.

2. Click on the Inventory tab, and click on the Advanced button.

3. In the Advanced inventory option dialog box, click on the Add button.

4. In the Custom Inventory Items dialog box, enter a name for the custom inventory item.

Select item type on the Item Type list, for example Registry key, and fill in all fields for the selected item type as necessary.

Then click on OK.

The custom inventory item you created is displayed in the Custom Inventory Items pane in the Advanced inventory option dialog box. From here you can edit or delete it.

NOTE: The pane contents are stored in the Impero configuration file **`InvCuItm.xml`**, which is typically located here: `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest`.

2.6 Monitor Hosts

If the Guest Access Security settings on the Hosts allow remote control, the Guest can sequentially monitor the computer screen images of multiple Hosts and toggle between monitor mode and remote control mode.

During monitoring most Guest toolbar buttons are disabled, the Guest has no keyboard and mouse control on the Host computer.

If you discover during monitoring that you need to do something on the Host being monitored, switch to remote control mode using the Monitor/Remote Control toggle button in the monitor toolbox. Not all remote control functionality is available.

Each Host is monitored for a specified number of seconds. Specify the monitor interval in Tools > Program Options > Monitor.

In the Host, monitoring appears as multiple short remote control sessions.

To start monitoring Hosts, proceed as follows:

1. Select Hosts from the Quick Connect tab, the Phonebook tab or the History tab.

2. Click on the Monitor button on the toolbar to start connecting to the first selected Host.

Alternatively, select Monitor in the Connection menu.

3. If prompted by the Host, enter the logon information to log on to the Host.

You see the first Host computer.

4. The monitor toolbox is displayed. Use the tools to control the monitoring.

Button	Description
✖	End monitoring.
▶	Continue countdown after Hold.
⏸	Hold countdown.
⏪	Monitor the previous Host.
⏩	Monitor the next Host.
🖥	Switch between monitor and remote control mode. The button displays a remote control icon in monitor mode and a monitor icon in remote control mode.
⧉	Switch between window and full screen. The button displays a window to full screen icon in window mode and a full screen to window icon in full screen mode.
☰	Display a list of monitored Hosts. Use it to select a specific Host to monitor.

NOTE: The Guest cannot monitor a Host computer with which it runs a remote control session.

2.7 Execute system control commands on a Host computer

If allowed by the **Guest Access Security** settings on the Host, the Guest can execute system control commands on Host computers.

To execute a system control command on a Host computer, proceed as follows:

1. In one of the Guest window tabs, select the Host computer that you want to connect to and execute a system control command on.

The Guest can connect and execute a system control command from the Quick Connect tab, the Phonebook tab or the History tab in the Guest window.

2. Click on the ⚙ Execute Command button on the toolbar.

Alternatively, select the Execute Command from the Connection menu.

or

When already connected, in the Remote Control window, click on the Execute Command button in the toolbar.

Execute Command displays a menu from which you can select the following commands:

Command	Note
Log Off	
Restart	
Shut Down	
Lock Workstation	You can lock only Host computers running on Windows NT and later (2000, XP, 2003, 2008, Vista, and 7) operating systems.
Wake on LAN	Select Wake on LAN to start selected Host computers whose Wake on LAN MAC Address is specified on the Connect tab in the Connection Properties window. NOTE: You can only use this command for Host computers that support this.

See also
Guest Access Security

2.8 Perform Remote Management tasks

If allowed by the Guest Access Security settings on the Host, the Guest can use Remote Management to manage the Host.

For the Host computer you can access the Disk drives, Event Viewer, Task Manager, Registry, Services, Shared Folders, Inventory, Command Console, System Control, Local Users, and Groups.

The window section called Impero Sessions provides access to a few basic remote control session types, Remote Control, File Transfer, Chat, and Audio-Video Chat, which you can use while remote managing the Host.

Other third party programs can be installed in their own window section. In the File menu, click on the Third Party Program Integration button. The first step is to add your own window section, and the next step is to add shortcuts to relevant programs.

To start a remote management session with a Host, proceed as follows:

1. In one of the Guest window tabs, select the Host that you want to connect to and run

a remote management session with.

2. Click on the Remote Management button on the toolbar to start a remote management session with the selected Host.

Alternatively, select Remote Management in the Connection menu.

The Remote Management window is displayed.

Nothing is displayed on the Host computer.

2.8.1 Management pane

When you have started a remote management session with a Host, the Remote Management window is displayed. The Remote Management window contains a pane on the left providing access to available management tools in three or more sections.

Management

The first section provides access to the Management tools. The tools are also available from the Management menu, which is added to the Impero Remote Management menu bar when a remote management session is started.

For details about each tool, refer to the relevant topic below.

Impero Sessions

The second section provides access to Impero Sessions commands. Refer to the Impero Sessions for a brief overview of the command.

Details

The third section is informational only and displays the following information:

- The Host ID
- The Host computer ID or MAC address
- The Guest communication profile
- The encryption type icon and name
- The Host computer operating system
- The remote management session duration in this format: HH:MM:SS.

2.8.2 Disk Drives

Click on Disk Drives from the Management section to display available Host computer disk drives and their properties.

Use the Disk Drives tool to get an overview of the available disk space on a remote controlled computer.

Viewing options are available from the Disk Drives menu and from the shortcut menu that opens when you right-click on the data panel.

2.8.3 Event Viewer

Click on Event Viewer in the Management section to display Windows event logs of the Host computer.

Use the Event Viewer tool to:

- View and change log properties.
- View the properties of an event record and copy them to the clipboard.
- Clear logs.
- Save a log on the Guest or Host computer.
- Open a log saved on the Guest or Host computer to view it.

NOTE: Only Windows NT and later versions (2000, XP, 2003, 2008, Vista, and 7) record event logs. Consequently, the Event Viewer command is enabled only if the Host computer runs on a Windows NT or later operating system.

Like the Windows Event Viewer, the Event Viewer tool includes three categories of information: Application, Security and System.

The File tab can display a saved event log.

The following commands are available from the Event Viewer menu and from the shortcut menu that opens when you right-click on the data panel:

Command	Description
Open	Opens an event log that was previously saved using the Save command. Event log files have the following extension `*.evt`. NOTE: Opening a saved event log overwrites any previous File tab contents.
Save	Saves an event log as a file in a specified location. The file has the

	`*.evt` extension.
Clear	Clears the Application, Security, or System event log from Windows. Before the event log is cleared, you can choose to save the information to a log file. Save the log file saved with `*.evt` extension.
Refresh	Retrieves new data from the Host computer to refresh the tab display.
Log Properties	Opens the properties window for the Application, Security or System log file. You can view and change log size and filter properties.
Event Properties	Displays properties for the selected event. Use the up and down arrows to scroll through the list of events. Click on the Copy button to copy the record properties to the clipboard.

2.8.4 Task Manager

Click on Task Manager in the Management section to display lists of applications and processes that are running on the Host computer.

The Task Manager tool works like the Windows Task Manager, only on a remote controlled computer. The tool can be used to view and control applications and end processes, and to view the computer load and process threads.

2.8.5 Registry

Click on Registry in the Management section to open the Windows registry on the Host computer.

The Registry tool works like the Windows Registry Editor, only on a remote controlled computer.

About Windows registry

The Windows registry stores the configuration of the Windows operating system in a structured database. The registry is created when Windows is installed on the computer and is automatically modified when applications are installed and used and when users create or change personal settings. Modify the registry settings with caution as erroneous data entries can make the computer malfunction.

Refer to the **Windows Registry Editor** help for details about entries and how to modify them.

2.8.6 Services

Click on **Services** in the **Management** section to display a list of services that are running on the **Host** computer. Services are programs that can run in the background, that is not displaying on the desktop, to support operating system or application functionalities. The **Services** tool enables you to start, stop, pause, resume and restart **Host** computer services, to add and remove services and to change the properties of services.

NOTE: Only Windows NT and later (NT, 2000, XP, 2003, 2008, Vista, and 7) can manage services. Consequently, the **Services** command is enabled only if the **Host** computer runs on a Windows NT or later operating system.

The following commands are available from the **Services** menu and from the shortcut menu that opens when you right-click the data panel:

Command	Description
Add...	Adds a service on the **Host** computer. Follow the instructions in the wizard that opens.
Remove	Deletes a service. When a Services record is deleted, the service status and startup type change to "**Stopped**" and "**Disabled**". When the application that uses the service is unloaded, the record is removed. **NOTE**: If you delete a Services record and you remove the service, affects the dependent services. Dependencies are displayed in the **Dependencies** tab, in the **Properties** dialog box. Right-click and select **Properties** from the shortcut menu.
Restart	Stops and starts the service. **NOTE**: Stopping, pausing or restarting a service can affect dependent services. Dependencies are displayed in the **Dependencies** tab, in the **Properties** dialog box: Right-click and select **Properties** from the shortcut menu.
Refresh	Retrieve new information from the **Host** computer to refresh the displayed information.
Properties	Displays properties for the service on three tab pages.

NOTE: Do not change service properties unless you know exactly what you are doing. Keep notes of changes to enable restoring properties if changes cause an unexpected behavior.

General tab

Use the **Startup type** field to change the way the service starts.

NOTE: If you change the **Startup type** to "**Disabled**", a service which started or paused does not change its status. When it is stopped, it can no longer be started.

Use the **Start**, **Stop**, **Pause** and **Resume** buttons to control the service.

The **Start parameters** field is enabled when a service is "**Stopped**". Specify any parameters like command line options to be used when the service is started.

NOTE: Start parameters are unsaved. A backslash (\) is interpreted as an ESCAPE character. Specify two backslashes for each backslash in a parameter.

Log On tab

Use the **Log on** as options to specify how to log on to a service by using a different account.

Use **Local System** account to log on as a local system account that has extensive rights on the **Host** computer, but no rights on other computers (typically the default selection).

Use **This account to log on** as a specific user and specify the user credentials in the fields.

To specify that the selected Host computer service uses the **Local Service** account, type `NT AUTHORITY\LocalService`. To specify that it uses the Network Service account, specify `NT AUTHORITY\NetworkService`. Do not specify a password for these accounts; both of them have built-in passwords.

Dependencies tab

	Displays dependencies and dependents. You cannot change dependencies on this tab.

2.8.7 Shared Folders

Click on **Shared Folders** in the **Management** section to view and manage agent computer shared resources and view and disconnect shared resource sessions and shared file connections.

Shares tab

Special shares, typically with "$" as the last character in the share name, are created automatically as hidden resources by the operating system for administrative and system use. Typically, you should not delete or change special shares. If you delete or change special shares, they can be restored when the server service is stopped and restarted or when the computer is restarted.

These special shares may appear on the **Shares** tab:

`<Drive letter>$`	Enables **Guests** to connect to the root directory of a drive.
`ADMIN$`	Enables remote administration of a computer. Its path is always the path of the system root directory.
`IPC$`	Enables inter program communication by named pipes. IPC$ is used during remote administration of a computer and when viewing a computer's shared resources and cannot be deleted.
`NETLOGON`	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
`SYSVOL`	Required on domain controllers. Removing it causes a loss of functionality on domain client computers.
`PRINT$`	Used during remote administration of printers.
`FAX$`	A server folder that is used by clients when sending a fax. It stores temporary fax files and fax cover pages.

2.8.8 Inventory

Click on Inventory in the Management section for an overview of the Host computer inventory of hardware and software.

2.8.9 Command Console

Click on the Command Console from the Management section to open a command prompt window on the Host computer. This corresponds to executing Run on the Windows Start menu and typing `cmd` but have the command prompt window display the Host computer, not the Guest.

Before the command prompt window opens, you are required to enter credentials (user name, password and domain) that are valid on the Host computer.

2.8.10 System Control

Click on the System Control in the Management section to control the Host computer status.

System Control allows you to:

- Lock the computer (Windows NT, 2000, XP, 2003, 2008, Vista and 7 only)
- Log off the user
- Restart the computer
- Shut down the computer

Before any of these actions are performed, you can choose to warn the user by displaying a message, for example:

```
Computer updates need to be implemented and you are logged off in a
few minutes. Please save your work and close any open program.
```

Use the Options section to specify whether the user is to be warned and to specify the number of seconds between prompting the user and executing the action selected under Action to Perform.

Allow user to cancel	Generally, you cannot cancel a system control command. However, selecting this option enables the Abort button on

	the pop-up message, and the user is allowed to cancel the command.
Close open programs without saving data	Normally data is saved before the selected system control command is executed. Select this option to close any open programs without saving data.

2.8.11 Local Users and Groups

Click on **Local Users and Groups** in the **Management** section to manage users and groups on the **Host** computer.

With **Local Users and Groups**, you can:

- Add new users and groups
- View and edit properties of existing local users and groups
- Set user passwords
- Rename or delete users and groups

Users tab

The **Users** tab contains the list of users of the **Host** computer.

The shortcut menu has these commands:

Command	Description
New User	Select this command to add a new user. In the **New User** dialog box, specify the appropriate information and select or clear the selection of options related to password and account. Click on **Create**, and then click on **Close**.
Set Password	Select this command to change the selected user's password.
Delete	Select this command to delete the selected user. **NOTE**: When it is necessary for you to remove a user account, it is a good idea to disable the account first. When you are certain that when you disable the account did not cause a problem, you can safely delete it. To disable the account, select **Account is disabled** in the **Properties** dialog box. A deleted user account cannot be recovered. The built-in **Administrator** and **Guest** accounts cannot be deleted.

Rename	Select this command to rename the selected user. Specify a new name and press **Enter** to save. NOTE: Because it retains its security identifier, a renamed user account retains all its other properties, such as its description, password, group memberships, user environment profile, account information, and any assigned permissions and rights. A user name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A user name cannot consist solely of periods (.) or spaces.
Refresh F5	Select this command to retrieve new data from the **Host** computer and refresh the tab display.
Properties	Select this command to view and change properties for a user account. When a user has been created with the **New User** command, the user must be added to a group. This is done on the **Member Of** tab in the **Properties** dialog box. NOTE: Adding users to the Administrators group gives them unlimited access rights.

Groups tab

The **Groups** tab contains the list of groups of the **Host** computer.

The shortcut menu has these commands:

Command	Description
New Group	Select this command to add a new group. In the **New Group** dialog box, type the appropriate information and click on the **Add** button to add existing users to the group button. Click on **Create**, and then click on **Close**. NOTE: A local group name cannot be identical to any other group or user name on the computer being administered. It can contain up to 256 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A group name cannot consist solely of periods (.) or spaces.
Delete	Select this command to delete the selected group. NOTES: • The following built-in groups cannot be deleted: Administrators, Backup Operators, Power Users, Users, Guests, Replicator. • A deleted group cannot be recovered.

	• Deleting a local group removes only the group; it does not delete the user accounts and global groups that were members of that group. • If you delete a group and then create another group with the same group name, make sure to set new permissions for the new group; it does not inherit the permissions that were granted to the old group.
Rename	Select this command to rename the selected group. Specify a new name and press Enter to save. NOTE: Because it retains its security identifier, a renamed group retains all its other properties, such as its description and members. A group name cannot be identical to any other user or group name of the computer being administered. It can contain up to 20 uppercase or lowercase characters, except for the following: " / \ [ ] : ; | = , + * ? < >. A group name cannot consist solely of periods (.) or spaces.
Refresh F5	Select this command to retrieve new data from the Host computer and refresh the tab display.
Properties	Select this command to add and remove users from the group.

2.8.12 Integrate third party applications

If there are applications that you use frequently in connection with remote management, you can create your own section in the left pane of the Remote Management window and add commands to open any third party application.

The user defined section in the left pane of the Remote Management window is added beneath the Management section; see illustration and description in the Management pane. Within the user defined section, the third party applications can be added beneath user-defined group headings like for example Utilities or Tools.

To add a third party application, proceed as follows:

1. In the File menu, click on Third Party Program Integration.

2. Click on the Add Section button to create the section and give it a name, for example My own section.

Note that the section appears after one or more programs have been added.

3. Select a section and click on the Add Program button.

4. In the Add Program dialog box, click on the Browse button to locate the executable. The Working Folder field is updated automatically.

5. Click on OK to add the program and close the dialog box.

Optional parameters

In addition to specifying the name of the executable, optional parameters can also be specified.

Parameter Name	Description
Display Name	Define the program name to be shown in the new section. If this parameter is not set, the name of the executable (for example: excel.exe) is displayed.
Display Name	Define the text to be displayed when the mouse pointer rests on the program name. If this parameter is not set, the name of the executable (for example: excel.exe) is displayed.
Command Line	Define the program parameters to be passed to the program when it is started. The following built-in parameters can be used: • `%%CN` - Host Computer Name • `%%CD` - Host Computer Domain • `%%LU` - Host Logged in User • `%%LD` - Host Logged in Domain • `%%IA` - Host IP Address • `%%MA` - Host MAC Address
Working Folder	Select the folder for the program to store its data. If this parameter is not set, the folder where the executable is located is used.
Run As	Select the folder for the program to store its data. If this parameter is not set, the folder where the executable is located is used.

Select how the program window is displayed: **Normal Window**, **Minimized**, **Maximized**, or **Hidden**.

TIP: Any program that is installed on the **Guest** computer and can react to command line executions can be integrated. To view any necessary command line parameters you can open the program properties dialog box: Right-click on the program from the Windows Start menu and then click on **Properties**.

2.8.13 Impero Sessions

The following commands are available in the Impero Sessions section:

Command	Description
Remote Control	Start/stop a remote control session with the connected Host.
File Transfer	Start/stop a file transfer session with the connected Host.
Chat	Start/stop a chat session with the connected Host.
Audio-Video Chat	Start/stop an audio-video chat session with the connected Host.

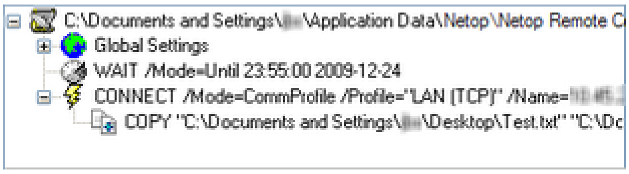
NOTE: Start Audio-Video Chat is disabled if the Guest and Host computers are not both interactive audio enabled or if the Guest is engaged in another audio session. The Guest Access Security settings on the Host can deny a Guest starting a session.

2.9 Create and run a script

A script is a user specified command structure that can execute a task, for example an unattended scheduled file transfer.

You create the script in the Script dialog box as a tree structure consisting of:

- Global Settings, such as overwrite/delete settings, error handling and log file settings etc.
- One or multiple commands, for example a Wait command and a Connect command to connect to a Host.
- One or multiple commands, for example Copy, Delete, Synch, or Inventory, which are executed on the Host after connection.



```
C:\Documents and Settings\[redacted]\Application Data\Netop\Netop Remote C
    Global Settings
    WAIT /Mode=Until 23:55:00 2009-12-24
    CONNECT /Mode=CommProfile /Profile="LAN (TCP)" /Name=[redacted]
        COPY "C:\Documents and Settings\[redacted]\Desktop\Test.txt" "C:\Dc
```

The following example describes how to create a script that copies a file from the Guest to a Host on a specified date and time.

To create this script, proceed as follows:

1. Click on the Script tab to display the tab.

2. In the Edit menu, select New > Script to display the Script dialog box.

3. In the File name field, enter a name for your script, for example "Copy document". If you do not specify a file type extension, the script gets the file type extension `*.dws`.

4. Click on the Open Script button and click on Yes to start a new script.The Global Settings dialog box is displayed.

5. In the Global Settings dialog box, specify settings for the script.To close the dialog box, click on OK.

6. In the Comment field, enter a comment about the script, which is displayed in the Script tab in the Guest window.

7. Select Global Settings in the tree structure in the upper pane of the dialog box, and click on the Add button. Select Wait on the menu.

8. In the Wait dialog box, select Wait until in the Type field.

Specify a date and time for the copying, and click on OK to close the dialog box.

The Wait command is added to the script and displayed in the tree structure.

9. Select Wait in the tree structure, and click on the Add button. Select Connect in the menu.

In the Connect to Host dialog box, specify how you want to connect to the Host, for example using a communication profile.

Select communication profile and specify IP address and logon credentials for the Host.

The Connect command is added to the script and displayed in the tree structure.

10. Select Connect in the tree structure, and click on the Add button. Select Copy in the menu.

The Copy dialog box is displayed.

In the General tab, in the Guest section, specify the file that you want to copy to the Host.

In the Host section, specify the location on the Host that you want to copy the file to, and change any other settings as necessary.

NOTE: You cannot browse, since the Guest is not yet connected to the Host.

Click on OK to close the dialog box.

11. Click on the Save Script button, and click on the Run button to enable the script.

12. Click on Close to close the dialog box.

You have created a script that copies the Test.txt file to one specific **Host** on a specific date and time.

If you want to copy the Test.txt file to a number of **Hosts**, the easiest way to specify this in the script is to first edit the script file (Copy the document.dws file, located in `\\Application Data\Impero\Impero Connect\Guest\script\`) in Notepad and then edit it further in the **Script** dialog box.

Script file contents

```
;Copy document to Host computer
;*************************
Script
SET Copy=G_H
SET Delta=Yes
SET CrashRecovery=Yes
SET OverwriteExisting=Yes
SET OverwriteSystem=No
SET OverwriteReadOnly=No
SET OverwriteHidden=No
SET OnComError=NextHost
SET OnError=NextFile
SET AtEnd=None
SET UnloadGuest=No
SET LogAppend=No
SET Log=SCRIPT.LOG

WAIT Mode=Until 23:55:00 2009-12-24

Connect /Mode=CommProfile /Profile="LAN (TCP)" /Name="10.45.2.33" /LoginCredentials=Yes
COPY "C:\Documents and Settings\user1\Desktop\Test.txt" "C:\Documents and Settings\"
ConnectEnd
ScriptEnd
```

1. Copy the **Connect** command (from Connect /Mode= through ConnectEnd) for as

many Hosts as you want to copy the Test.txt file to.

2. Save and close the Copy document.dws file.

3. Open the Copy document.dws file in the Script dialog box again, and for each Connect command, edit the IP address and logon credentials in accordance with the individual Hosts that you want to copy the `Test.txt` file to.

4. Save the script.

The script you created automatically copies the `Test.txt` file to a specified range of Host computers on the specified date and time.

NOTE: The Guest also contains a couple of slightly more advanced example scripts that you can study to see what you can do with Script. See `example1.dws` and `example2.dws` on the Script tab. You can open them in Notepad to see the contents.

Once the script has been executed, you can check the script log file (`\\Application Data\Impero\Impero Connect\Guest\`) to see if the script was executed successfully.

See also
Script
Global Settings

2.10 Use Intel vPro from Impero Conect

The **Guest** provides access to Intel vPro (sometimes also referred to as IAMT - **I**ntel **A**ctive **M**anagement **T**echnology) functionality which enhances your ability to remote manage enterprise computing facilities.

NOTE: The Guest supports Intel vPro, versions: 2.2 to 1.1. Functionalities introduced after this version are not supported.

The Guest can access Intel vPro even when the computer is turned off, as long as the computer is connected to line power and to a network.

NOTE: Due to a limitation in Intel vPro, it is not possible to establish a connection to Intel vPro on the same computer as the one the Guest is running on.

The Intel Setup and Configuration Service (SCS) provides tools to centrally set up and configure AMT devices. SCS serves as a server for vPro and is also called a provisioning server.

Depending on which permissions the user has, the following SCS realms are relevant when using the vPro Console that the Guest provides access to:

Realm	Comments
General Info	Required
EventLogViewer	If the user has permission to this realm, the Event Management tab is available. The Remove all and Filters and Subscriptions buttons are disabled, so that the user cannot change anything.
Event Management	If the user has permission to this realm, the Event Management tab is enabled and all the buttons are enabled, so that the user can make changes.
Remote Control	If the user has permission to this realm, the Remote Control tab is enabled and the user can execute remote control commands.
Redirection Interface	If the user has permission to this realm, the user can execute serial/IDE redirection commands from the Remote Control tab.

If the user has permissions to neither the Event Management tab nor the Remote Control tab, an "Authentication failed" message box is displayed. This means that either User or Password is wrong or there are no appropriate permissions for the user in question.

NOTE: Even though computers contain Intel vPro technology, the AMT devices are not be operational until they are enabled (also called provisioning) in the vPro BIOS.

Intel vPro enables you to:

- Remotely access BIOS configuration of the managed computer.
- Remotely boot the managed computer from a floppy or CD-ROM image located on the managing computer.
- Retrieve and view the hardware log file of the managed computer.

2.10.1 Log on to the vPro Console

The **Intel vPro** tab is displayed at the bottom of the **Quick Connect** tab pane following the **Windows Network** tab. When you start the **Guest**, the **Intel vPro** pane is empty.

Right-click on the **Intel vPro** pane to display a context menu containing the following commands:

Command	Description
Scan IP range for Intel vPro enabled computers	Select this command to scan for **Intel vPro** enabled computers on your network. You can enter one known IP address to scan for or you can enter an IP range to scan. The computers found during the search is listed in the **Intel vPro** pane by IP address. **NOTE**: You can also use the **Guest Inventory** tab (Summary - Intel vPro State) to find the **Intel vPro** enabled computers on your network.
Retrieve the Intel vPro enabled computers from SCS	Select this command or click on the **Browse** button in the **Quick Connect** tab to retrieve **Intel vPro** enabled computers from Intel SCS. Enter the SCS Web Service URL. **NOTE**: If you do not want to have to enter the SCS Web Service URL every time, go to **Tools** > **Program Options** > **Intel vPro** tab. Select the Connect to SCS check box and enter the SCS Web Service URL in the field below. The address is then saved in the system to avoid entering the address every tome the Retrieve **Intel vPro** Enabled Computers from SCS command is selected.

When you have found one or more **Intel vPro** enabled computers on your network, the above menu is extended with the following commands:

Command	Description
Open Intel vPro Console	Right-click a computer in the list in the **Intel vPro** pane and select this command to open the **vPro Console** from which you can manage the selected computer. Use a user name and password to log on.
Open Intel vPro Web Inter-	Right-click on a computer from the list in the **Intel vPro**

face	pane and select this command to go to the Intel vPro Active Management Technology web page (http) from which you can manage the selected computer. Enter a user name and password to log on to the web page.
Open Intel vPro Web Interface (Secure)	As above, but using secured connection (https).
Add to phonebook	Right-click on a computer (IP address) in the list of the Intel vPro pane and select this command to add the address to the phonebook. NOTE: You can also add Intel vPro entries to the phonebook by right-clicking in the right pane on the Phonebook tab.
Delete	Right-click on a computer in the list in the Intel vPro pane and select this command to remove the computer from the list.
Delete All	Right-click on the Intel vPro pane and select this command to remove all computers from the list in the Intel vPro pane.

To log on to the vPro Console, proceed as follows:

1. Right-click on a computer on the list in the Intel vPro pane and select Open Intel vPro Console.
2. In the Credentials tab of the displayed Impero vPro Console Logon window, select the authentication method:

- Digest authentication
- Kerberos authentication

If you select Digest authentication, enter the user name and password.

Select the Force using secured connection through TLS check box, if you prefer. Normally, Transport Layer Security (TLS) is automatically detected and used when available, but if you select this check box, the Intel vPro Console uses only the secured connection to log on to the AMT device. If the AMT device is not configured to use TLS, you receive an error message and the connection is not established.

If you select **Kerberos authentication**, the tab looks slightly different, and either a current Windows user account or a different user account (user, password, domain) can be used to log on to the AMT device.

In addition to the **Force using secured connection through TLS** check box, you see a **Log on using current Windows account** check box. This check box is selected by default, and as a consequence the **User name**, **Password**, and **Domain** fields are disabled, and the credentials of the current Windows user are used.

NOTE: When using Kerberos authentication the console should be connected to the **Host** using FQDN name (fully qualified domain name). For example, it is not possible to do the Kerberos authentication when connecting to an AMT device using its IP address.

3. If you select the **Force using secured connection through TLS** check box, a client certificate is required to establish the TLS connection when the AMT device is configured for mutual TLS authentication.

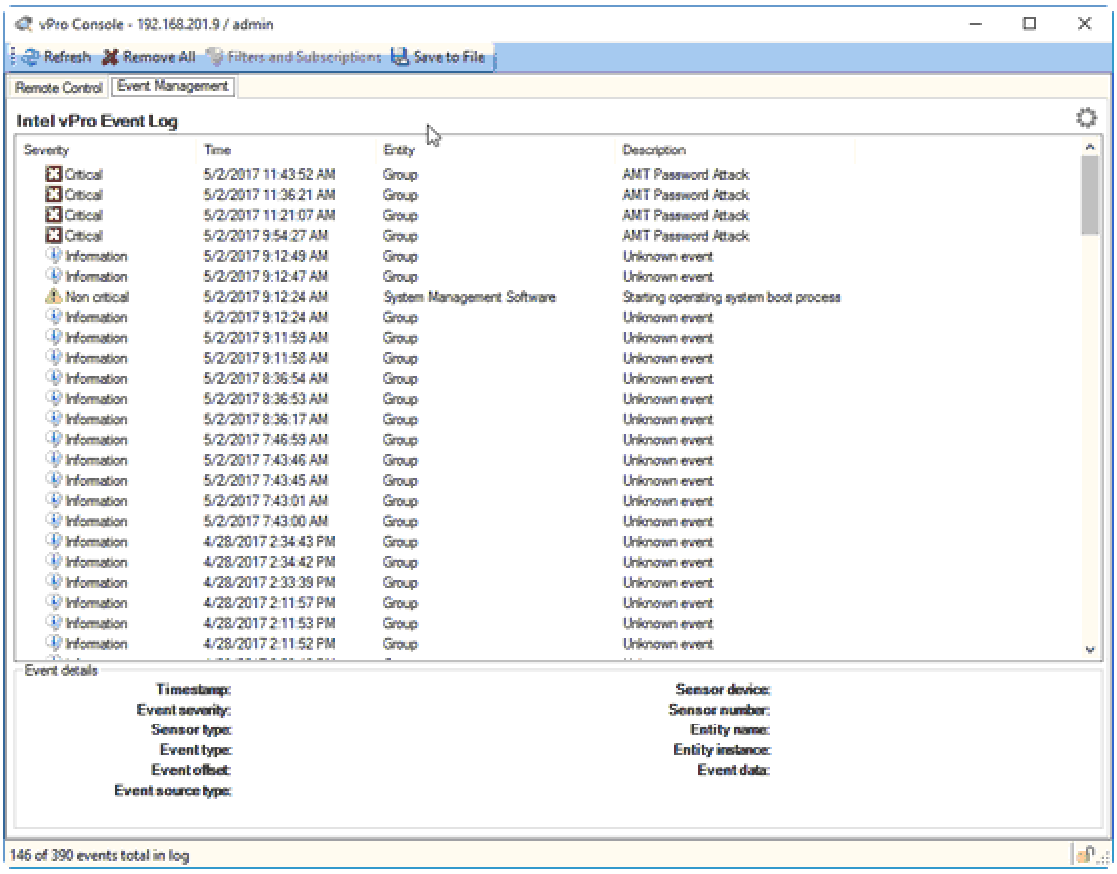
Click on the **Certificate** tab and specify the certificate to be used by first selecting either **Personal Certificate Storage** or **File** in the **Location** list and then selecting the certificate in the Certificate combo box.

4. Click on **Log on** to log on to the **vPro Console**.

When you have logged on, the **vPro Console** window is displayed.

2.10.2 vPro Console

The **vPro Console** window contains a toolbar at the top and two tabs: the **Event Management** tab, on which you can retrieve and view the **Intel vPro Event Log** for the computer being managed, and the **Remote Control** tab, on which you can access the BIOS of the computer, boot from a floppy or CD-ROM image, and manage the power state of the computer remotely.



vPro Console - 192.168.201.9 / admin
Refresh
Remove All
Filters and Subscriptions
Save to File
Remote Control
Event Management

Intel vPro Event Log

Severity	Time	Entity	Description
Critical	5/2/2017 11:43:52 AM	Group	AMT Password Attack
Critical	5/2/2017 11:36:21 AM	Group	AMT Password Attack
Critical	5/2/2017 11:21:07 AM	Group	AMT Password Attack
Critical	5/2/2017 9:54:27 AM	Group	AMT Password Attack
Information	5/2/2017 9:12:49 AM	Group	Unknown event
Information	5/2/2017 9:12:47 AM	Group	Unknown event
Non critical	5/2/2017 9:12:24 AM	System Management Software	Starting operating system boot process
Information	5/2/2017 9:12:24 AM	Group	Unknown event
Information	5/2/2017 9:11:59 AM	Group	Unknown event
Information	5/2/2017 9:11:58 AM	Group	Unknown event
Information	5/2/2017 8:36:54 AM	Group	Unknown event
Information	5/2/2017 8:36:53 AM	Group	Unknown event
Information	5/2/2017 8:36:17 AM	Group	Unknown event
Information	5/2/2017 7:46:59 AM	Group	Unknown event
Information	5/2/2017 7:43:46 AM	Group	Unknown event
Information	5/2/2017 7:43:45 AM	Group	Unknown event
Information	5/2/2017 7:43:01 AM	Group	Unknown event
Information	5/2/2017 7:43:00 AM	Group	Unknown event
Information	4/28/2017 2:34:43 PM	Group	Unknown event
Information	4/28/2017 2:34:42 PM	Group	Unknown event
Information	4/28/2017 2:33:39 PM	Group	Unknown event
Information	4/28/2017 2:11:57 PM	Group	Unknown event
Information	4/28/2017 2:11:53 PM	Group	Unknown event
Information	4/28/2017 2:11:52 PM	Group	Unknown event

Event details

Timestamp:
Event severity:
Sensor type:
Event type:
Event offset:
Event source type:
Sensor device:
Sensor number:
Entity name:
Entity instance:
Event data:

146 of 390 events total in log

Event Management tab

The Event Management tab displays the Intel vPro Event Log for the computer being managed. The events are displayed in the Intel vPro Event Log pane with information about severity, time, and entity together with a description. Select an event in the pane to display further details about the event in the area below the pane.

In the bottom right corner of the **vPro Console** window you see a security indicator, a lock icon. A closed lock indicates that a secured connection is being used, while an open lock indicates that an unsecured connection is being used. In the top right corner you see a network activity indicator that looks like a flower. This icon indicates that the vPro Console is waiting for response from the remote AMT device.

At the top of the vPro Console window you find a toolbar with tools that you can apply to the log. In addition to the Refresh button, the Remove All button, and the Save to File button (save events to a `*.txt` (tab delimited) file or a `*.csv` file), a Filters and Subscriptions button are available.

Remote Control tab

The **Remote Control** tab provides access to the terminal window, which you can use for remote BIOS access and floppy/CD-ROM redirection.

The toolbar for the **Remote Control** tab contains the following buttons:

Button	Description
Remote Control	The menu that opens when you click on the **Remote Control** button down arrow on the toolbar contains the following menu commands: • Normal Reboot • Reboot to BIOS* (If you click the **Remote Control** button instead of the down arrow, this menu command is selected by default) • Boot from Console Floppy • Boot from Console CD When you select menu commands on the **Remote Control** menu, you can see the screen of the computer being booted on the **Remote Control** tab of the vPro Console.
Execute Command	The menu that opens when you click on the Execute Command button down arrow on the toolbar contains the following menu commands: • Normal Reboot* (If you click the Execute Command button instead of the down arrow, this menu command is selected by default) • Boot from Console Floppy • Boot from Console CD When you select menu commands on the **Execute Command** menu, the boot command is executed on the remote computer. The screen of the computer being booted on the **Remote Control** tab of the **vPro Console** is unseen.
Power	The menu that opens when you click on the **Power** button from the toolbar contains the following menu commands, which you can use to manage the power state of the remote computer:

	• Power On • Power Off • Cycle Power Off and On* (default)
Custom command	The menu that opens when you click on the **Custom command** button down arrow on the toolbar contains the following menu commands, which you can use to customize the menus and menu items to the left of the Custom command: • **Send command** - Select this command to open the **Send Custom Command** dialog box, which allows you to specify a custom command and send it immediately. The custom command is not saved. • **Customize** - Select this command to open the **Customize Remote Control Toolbar** dialog box, which allows you to add and specify menus, commands and separators, reorder these elements, and send commands. The changes are saved. You can reset the toolbar again. On the left side in the **Customize Remote Control Toolbar** dialog box a pane containing the menu structure is displayed. If you select a menu, settings for adjusting the menu are displayed to the right of the pane. You can move the menu up and down in the toolbar, change the appearance of the menu and more. If you select a command in the pane, command options are displayed to the right of the pane. Both dialog boxes contain the same command options. Depending on the command you select, different sets of options are enabled. You can specify command type and parameters, CD/floppy redirection and boot options for the command you select.
IDE Redirection Settings	Clicking on the **IDE Redirections Settings** button from the toolbar opens the **IDE Redirections Settings** window where you can select settings for **Floppy redirection** and **CD redirection**, i.e. the drives and image files that are to be used for **Boot from Console Floppy** and **Boot from Console CD**.

Impero vPro Console Settings	Clicking on the **Terminal Settings** button on the toolbar opens the **Impero vPro Console Settings** window where you can edit settings for the following: **Terminal** - Set Font and Emulation. **Keyboard** - Set Special key mode and **Send Esc** button code. **Warnings** - Select the warnings that you want to receive in relation to the Keyboard settings: • Warn if the special key mode cannot be detected automatically • Warn when trying to detect keyboard mode without having Hardware Assets Realm permission

2.11 Tunnel

The **Tunnel** function establishes a secure connection between the **Guest** and **Host**. Through the **Tunnel** application ports are redirected from the **Host** to the **Guest**.

This means that the **Guest** can run local applications while interacting with the connected **Host** without having to control the **Host** machine remotely.

The **Tunnel** is ideally suited, but not exclusive to environments where no traditional desktop is available for use with standard remote control (screen, keyboard and mouse control); however support and system administrative tasks still need to be carried out remotely whilst conforming to industry regulatory standards such as PCI-DSS, HIPAA and FIPS.

Such environments can include embedded Linux systems where operating machinery and hardware contains a streamlined version of a Linux operating system, for example, fuel dispensers and retail systems. Enterprises can also take advantage of the Tunnel for managing and supporting their Linux Desktops and Servers using common applications and services such as Shell clients, HTTP and SFTP.

The **Guest's** ability to use the Tunnel along with the associated ports can be governed by the central **Security Server** solution. This allows organizations to apply granular access privileges. Even when remote systems have a desktop, it may not be required to give Guest users full remote control access on certain machines but limit their ability to use certain application ports through the **Tunnel**.

2.11.1 Predefine local ports for the tunnel

When using the Tunnel capabilities, it is sometimes necessary to configure the local port to a fixed port. This way, when actually tunneling into the machine, the same local port always corresponds to the remote port.

To configure the local ports for the tunnel, proceed as follows:

1. Create the ImperoTunnelPorts.ini file and define the list of local ports and their corresponding remote ones.

The **.ini** file has the following structure:

```
[default]
key = value
[section]
key = value
```

Where section is the Remote IP, key is the remote port and value is the local predefined port.

2. Place the **`*.ini`** file in the C:\windows folder.

It helps identify either the remote port or the remote IP/remote Hostname/remote port pair and assign it a predefined fixed local port that the **Guest** opens when initiating the tunnel.

NOTES:

- In the **`ImperoTunnelPorts.ini`** file you can define the Host by providing either the Host ID or the Host IP Address. When connecting to the Host, the proper definitions are used, otherwise the default definition is applied.
- For the TCP/IP communication profile, there might be a cross Host ID - IP Address compatibility. **.ini** file defined with Host ID works if connection is made with Host IP Address or Host ID. Otherwise, the default definition is used.

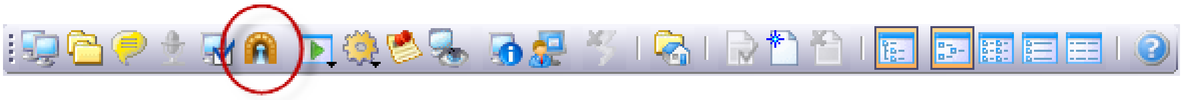
.ini file sample

```
[default]
80=80
8080=8080
8090=8090
[192.168.201.82]
80=90
8080=91
```

```
8090=92
8181=93
[192.168.201.137]
80=94
8080=95
8090=96
8181=97
```

2.11.2 Open tunnel session

The **Guest** can initiate the **Tunnel** session with a **Host** in the same way as any other session:



The **Tunnel** is also available from the context menu on the **Quick Connect** tab, **Phonebook** tab or the **History** tab.

Once the **Guest** is authenticated, the assigned ports are assigned by the **Security Server** and the **Tunnel console** is displayed and confirms which remote ports are available along with the randomly assigned ports that can be used by the **Guest**.

Refer to the separate documentation available on support.imperosoftware.com for more details on how to set up and use the secure tunnel.

2.12 Run a remote program

If allowed by the **Guest Access Security** settings on the **Hosts**, the **Guest** can run a program on one or multiple **Host** computers using the **Run Program** function.

To run a program, proceed as follows:

1. In one of the **Guest** window tabs, select the **Host** computer that you want to connect to and run a program on.

The **Guest** can connect and run a program from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab.

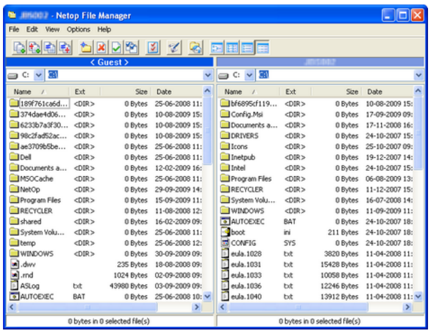
When already connected, the **Guest** can run a program from the **Phonebook** tab, the Quick Connect tab, the Connections tab or the History tab.

2. Click on the Run Program button on the toolbar. Alternatively, from the Connection menu, select the Run Program function.
3. Click on the Browse button.
4. In the Run dialog box, click on the Browse button and select the program that you want to run on the selected Host computer.
When the program file is added in the Local File name field, the global file name with the absolute path replaced by environment variables is also added in the Global File Name field. This is especially useful if your computers are running different Windows platforms.
Select the Global File name option, so that you do not have to consider which operating system version or operating system language the Host computer is using.
If the selected program needs to be started using command line switches, use the Command line switches field to type those. This could for example be starting Internet Explorer with a specific address.
Under Run, define how the program should start. Select Normal, Maximized or Minimized.
5. Click on OK to run the specified program on the selected Host computer.

NOTE: It is necessary that the program file is available on the Host computer in the location specified in the Run dialog box. The program can also be specified on the Tools > Program Options > Run tab. If the program is not available on the Host computer in the specified location, you can use the File Manager to transfer the file to the Host before running it. Refer to the Transfer files section for more information.

2.13 Transfer files

You can use the File Manager to transfer files between a Guest and a Host computer.
If allowed by the Guest Access Security settings on the Host, the Guest can start a file transfer session with a Host to transfer files between the Guest and the Host computer. This includes copying, moving, synchronizing, and cloning files.
You can also use the File Manager to transfer files locally on the Guest computer.



[redacted] - Netop File Manager

< Guest >

C:

Name	Ext	Size	Date
189f761ca6d...	<DIR>	0 Bytes	25-06-2008 11:
374dae4d06...	<DIR>	0 Bytes	10-08-2009 15:
6233b7a3f30...	<DIR>	0 Bytes	10-08-2009 15:
98c2fad52ac...	<DIR>	0 Bytes	10-08-2009 15:
ae3709b5be...	<DIR>	0 Bytes	25-06-2008 11:
Dell	<DIR>	0 Bytes	25-06-2008 11:
Documents a...	<DIR>	0 Bytes	12-02-2009 16:
MSOCache	<DIR>	0 Bytes	25-06-2008 11:
NetOp	<DIR>	0 Bytes	29-09-2009 14:
Program Files	<DIR>	0 Bytes	15-09-2009 11:
RECYCLER	<DIR>	0 Bytes	11-08-2008 12:
shared	<DIR>	0 Bytes	16-02-2009 09:
System Volu...	<DIR>	0 Bytes	25-06-2008 11:
temp	<DIR>	0 Bytes	25-06-2008 12:
WINDOWS	<DIR>	0 Bytes	30-09-2009 09:
.dwv		235 Bytes	18-08-2008 09:
.rnd		1024 Bytes	02-09-2008 09:
ASLog	txt	43980 Bytes	03-09-2009 09:
AUTOEXEC	BAT	0 Bytes	25-06-2008 10:

0 bytes in 0 selected file(s)

[redacted]

C:

Name	Ext	Size	Date
bf6895cf119...	<DIR>	0 Bytes	10-08-2009 15:
Config.Msi	<DIR>	0 Bytes	17-09-2009 09:
Documents a...	<DIR>	0 Bytes	17-11-2008 16:
DRIVERS	<DIR>	0 Bytes	24-10-2007 15:
Icons	<DIR>	0 Bytes	25-10-2007 09:
Inetpub	<DIR>	0 Bytes	19-12-2007 14:
Intel	<DIR>	0 Bytes	24-10-2007 15:
Program Files	<DIR>	0 Bytes	06-08-2009 13:
RECYCLER	<DIR>	0 Bytes	11-12-2007 15:
System Volu...	<DIR>	0 Bytes	16-07-2008 14:
WINDOWS	<DIR>	0 Bytes	11-09-2009 11:
AUTOEXEC	BAT	0 Bytes	24-10-2007 18:
boot	ini	211 Bytes	24-10-2007 18:
CONFIG	SYS	0 Bytes	24-10-2007 18:
eula.1028	txt	3820 Bytes	11-04-2008 11:
eula.1031	txt	15428 Bytes	11-04-2008 11:
eula.1033	txt	10058 Bytes	11-04-2008 11:
eula.1036	txt	12246 Bytes	11-04-2008 11:
eula.1040	txt	13912 Bytes	11-04-2008 11:

0 bytes in 0 selected file(s)

To start a file transfer session, proceed as follows:

1. In one of the **Guest** tabs, select the **Host** to or from which you want to transfer files.

The **Guest** can connect to start a file transfer session from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab, or in response to a help request from a **Help Request** tab.

When already connected, the **Guest** can start and end a file transfer session from the **Phonebook** tab, the **Quick Connect** tab, the **Connections** tab, or the **History** tab.

2. Click on the **File Transfer** button in the toolbar to open the **File Manager**.

NOTE: If the **Host** allows multiple simultaneous **Guest** connections, multiple **Guests** can run separate file transfer sessions.

Copy files

To copy files from one computer to another, proceed as follows:

1. Select files and/or folders in one of the two **File Manager** panes and click on the **Copy File(s)** button from the toolbar.

Alternatively, select files in one of the two **File Manager** panes and select **Copy File(s)** from the File menu.

2. In the **Copy** dialog box, check the location in the **To** field and change the location if necessary.

Click on the **Options** button to view the **Options** dialog box and specify options for the copy process. Refer to the Impero File Manager Options section for more information.

3. To start the copy process, click on **OK**.

NOTE: You can also use drag-and-drop to copy files from one **File Manager** pane to the other.

Move files

To move files from one computer to another, proceed as follows:

1. Select the files and/or folders in one of the two **File Manager** panes and click on the **Move File(s)** button from the toolbar.

Alternatively, select files in one of the two **File Manager** panes and select **Move File(s)** from the File menu.

2. In the **Move** dialog box, check the location in the To field and change the location if necessary.

Click on the **Options** button to view the **Options** dialog box and specify options for the move process. Refer to the Impero File Manager Options for more information.

3. Click on **OK** to start the move process.

Synchronize files

To synchronize files between two computers, proceed as follows:

1. Click on the **Synch File(s)** button on the toolbar. Alternatively, select **Synch File(s)** from the **File** menu.

2. In the **Synchronize** dialog box, check the location in the **To** field and change the location if necessary.

Click on the **Options** button to view the **Options** dialog box and specify options for the synchronize process. Refer to the Impero File Manager Options for more information.

3. Click on **OK** to start the synchronize process.

WARNING! By default, the synchronization process transfers files and folders in both directions, replacing older files and folders with newer files and folders. In the **Transfer** tab of the **Options** dialog, you can change this into **Transfer only if file exists** and **Transfer only one way for the file transfer process**.

Clone Files

To clone files from one computer to another, proceed as follows:

1. Click on the **Clone File(s)** button from the toolbar. Alternatively, select **Clone**

File(s) from the **File** menu.

2. In the **Clone** dialog box, check the location in the **To field** and change the location if necessary.

Click on the **Options** button to view the **Options** dialog box and specify options for the clone process. Refer to the Impero File Manager Options for more information.

3. To start the clone process, click on **OK**.

WARNING! Cloning transfers all the folders and files in the selected pane to the other pane deleting the existing folders and files in it.

TIP: Select all options in the **Confirmation** tab of the **Options** dialog box. Refer to the Impero File Manager Options for more information. A dialog box is displayed when you are about to delete or overwrite a file, allowing you to choose what you want to do with the file.

Transfer files locally on the Guest computer

To transfer files from one location on the **Guest** computer to another, click on the **Local** button from the toolbar in the **File Manager**. The folder structure of the **Guest** computer is displayed in both panes.

Run a script from the File Manager

You can open, edit, and run a script while you are in the **File Manager**.

Click on the **Script Editor** button from the toolbar to open the **Script** dialog box.

Refer to the Create and run a Impero script for more information about using scripts.

2.14 Log events

To support security functions, **Connect** includes an extensive event logging feature that enables you to log session activity and logon attempts to multiple logging destinations.

You can log **Impero** events:

- In an **Impero** log on the local computer.
- In the database of a central **Impero Server**.

- In an SNMP enabled management console (by sending SNMP traps to an SNMP enabled central management console, such as HP OpenView).

To enable logging, proceed as follows:

1. In the **Tools** menu, select **Log Setup**. The **Log Setup** windows is displayed.

2. In the **Log Setup** tab, select where you want to log events.

3. Click on the relevant tab to set up the logging, for example the **Impero Local** tab, if you selected **Log Locally** on the **Log Setup** tab.

4. In the **Impero Local** tab, select the events you want to view in the list of events, all or a specific type of events.

5. On the list of events select the individual events that you want to include in the logging. By default each **Impero** event is written to the local **Impero** log file immediately. Clear the Write to disk for each log entry check box to write **Impero** events to the local **Impero** log file when the **Impero** module is unloaded. This consumes less processor capacity.

6. Click on **OK** to close the dialog box and start logging.

NOTE: The Log file name field displays the (path and) name of the log file (default: IMPERO.LOG). If no path is specified, the log file is located in the **Impero** configuration files folder, typically `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>`. UNC paths are not supported. Only mapped paths are supported. A new local **Impero** log file that is created when the **Impero** module is loaded overwrites the old local **Impero** log file with the same path and file name.

See also

Log Setup

2.15 Record sessions

For documentation purposes you can record the 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 reduces the remote control session transfer speed.

Record sessions for a specific connection

Before connecting to a **Host**

1. In the **Quick Connect** tab, click on **Connection Properties**.

2. In the **Connection Properties** dialog box, click on the **Record** tab and select the **Record remote control session** check box.

3. Click on **OK**.

When you connect to a **Host** every remote control session that you run for that specific connection are recorded.

Record sessions for all connections

To record sessions for all connections, proceed as follows:

1. In the **Tools** menu, select **Program Options**.

2. In the **Program Options** dialog box, click on the **Recording** tab.

3. Select the **Enforce recording** check box to activate session recording. Select other settings as preferred.

4. Click on **OK**. Now sessions are recorded for all connections, until you change these settings again.

See also

Connection Properties
Program Options

2.15.1 Play back session recordings

Session recordings are listed in the **Recordings** tab in the **Guest** window.

To play back a session recording

1. On the **Recordings** tab, select the session recording that you want to play back.

2. On the **Connection** menu, select **Play back session recording** to start playing back the session recording. Alternatively, double-click on the session recording to start playing back the session recording.

In the **Play back recording** window, you can use the following buttons to control the playback:

Button	Description

■	Click on the Stop button to close the window.
⏸	Click on the Pause button to pause playback. Click on this button again to resume playback.
▶	Click on the Play button to start playback or resume playback when paused. When playback has ended, this button is disabled.
⏮	Click on the Back button to return to the beginning of the recording showing a black show area.
⬍ x1	Playback Speed: By default, the spin box field displays x1 indicating true speed. Click on the up/down arrows to change the playback speed by a factor x1 to x20 as displayed in the spin box field.

2.16 Use a skin to see the Host button layout

A Host, typically a CE/Mobile device, can transfer information about its button layout to Guests enabling Guest users to see the button layout by means of a click-able bitmap. This is called a skin.

If you run a remote control session, skins enable you to see the Host device and execute commands on the Host device by clicking buttons on the applied skin. A device may have more than one skin definition depending on its state, for example slide out keyboard, portrait and landscape orientation etc. Every time the device changes state, the Host sends the updated skin information to the Guest.

If the Guest does not have the skin that is necessary for a remote control session with a particular Host, it attempts to collect a suitable skin from the Skin Repository Server. If the necessary skin is not available, the Guest uses a default skin.

The address and port number of the Skin Repository Server that the Guest collects skins from is specified in Program Options on the Skins tab. If you click on the View Models button in the Skins tab, you can also see the skins available on the Skin Repository Server.

To use skins, enable the function in the Guest Connection Properties. Click on the Display tab and select options for the use of skins in the Skin section.

NOTE: You can design additional skins using the Skin Designer and add them to the Skin Repository Server.

See also

Connection Properties (Display tab)
Program Options (Skins tab)

2.17 Multisession Support

Each Windows **Host** supports up to 24 simultaneous sessions, regardless of the communication protocol (TCP, UDP or Web Connect). However, it depends on the session type and the **Host** hardware:

- up to 24 simultaneous sessions for **Remote Control**
- up to 12 simultaneous sessions for **File Transfer** or **Tunnel**

Each Windows **Guest** supports only one session initiated from the same guest instance to the same **Host**.

2.18 Switching between whitelisted applications

While remote controlling a **Host**, if application whitelisting is enabled, only the whitelisted applications are visible and accessible in the **Guest** remote control window. This means that reaching a whitelisted application, which is behind a non-whitelisted application, is more difficult to do. In order to address this problem, there is an easy way to switch between the whitelisted applications by using the dedicated button in the **Guest's** remote control window.

The list includes only the whitelisted applications and allows you to switch to any of those applications, even if they are completely covered by other whitelisted or non-whitelisted applications.

NOTE: In order to use the **Whitelisted Applications switch** button, it is necessary that both the **Guest** and the **Host** are version 12.73 or above.

Refer to the Impero Knowledge Base for more information about whitelisting.

2.19 Multiple monitors support

While in a remote control session, you can dynamically change the **Host** monitor to be displayed on the screen by clicking on the **Monitors** icon from the main menu and selecting the desired monitor.

3 Getting remote support

3.1 Request help

If the **Help Request** function has been enabled on the **Host**, you can request help from a **Guest** that offers help services.

To request help, proceed as follows:

1. Click on the **Request help** button in the toolbar.

Alternatively, in the **Session** menu, select the **Request help** command.

If the **Host** is minimized you can request help by double-clicking on the **Impero Help Request** icon in the notification area.

2. Depending on how the **Help Request** function has been set up, you may now be prompted to enter various information. The Guest user can provide you with the information you need. Specify the necessary information when prompted.

When you have entered the necessary information, your help request is delivered to the help provider, who typically starts a remote control session.

While the help request status is "**Pending**", you can choose to cancel it by clicking on the **Cancel help** button in the toolbar.

See also

Set up Help Request on Guest and Host
Program Options (Help Request tab)
Advanced Help Request Options

3.2 Notification

You may be notified of connecting **Guests** in different ways upon connection, during connection and after connection, depending on the connection notification setup.

Upon connection

You can be notified by a sound being played or a balloon tip or a list of connecting **Guests** being displayed in the notification area in the lower right corner of the screen.

The connection list can be set to disappear after a specified number of seconds, or it can be necessary for you to specify a password to close the history list.

During connection

A sound can be played at certain intervals, the **Guest** name can be displayed in the **Host** title bar, and the **Host** icon in the notification area can be animated.

After connection

You may be notified by a balloon tip or a history list of connections in the notification area when a **Guest** disconnects.

The history list can be set to disappear after a specified number of seconds, or it can be necessary that you need to specify a password to close the history list.

NOTE: You can also be prompted to confirm **Guest access**, if this has been set in the **Guest Access Security** dialog box on the **Guest Access Privileges** tab.

See also

Program Options (Connection Notification tab)
Guest Access Security (Guest Access Privileges tab)

3.3 Communicate with Guest users

Connect offers two ways in which you can communicate with Guest users while receiving remote support.

If allowed by the **Guest Access Security** settings on the **Host**, the **Guest** can start a chat or an audio-video chat with a **Host**, and the **Host** can likewise start a chat or an audio-video chat with the **Guest**.

Chat

To start a chat with a connected **Guest**, proceed as follows:

1. Click on the 💬 **Chat** button in the toolbar. Alternatively, in the **Session** menu, select **Chat**.

2. In the **Chat** dialog box, type your message.

3. Click on the **Send** button.

NOTE: You can save the chat as an `*.rtf` file for documentation purposes.

Multi chat

If the Host allows multiple simultaneous Guest connections, a Guest that the Guest Access Security settings allow to act as multi Guest session administrator can start a multi chat with the Host and all of the connected Guests.

Audio-video chat

Audio-video chat requires audio-video equipment to be installed on both sides.

To start an audio-video chat with a connected Guest, proceed as follows:

Click on the Audio-Video Chat button on the toolbar.

Alternatively, in the Session menu, select Audio-Video Chat.

The Audio-Video Chat dialog box is displayed.

Depending on the hardware available, you can now use your microphone to talk to the Guest user, and if Video is enabled by the Guest user, you can also see each other in the dialog box.

Use the slide bars on the right to control sound and video.

Only the Guest can end the audio-video chat session.

NOTE: Each Guest and each Host can run only one audio session including Transfer Sound at a time.

See also

Guest Access Security
Program Options (Audio-Video Chat tab)

3.4 End a remote control session from a Host computer

If your computer is being remote controlled and you feel that you do not want to continue the session for whatever reason, you can end the session from the Host.

To end a remote control session from the Host, proceed as follows:

Click on the Disconnect button on the toolbar. Alternatively, in the Session menu in the Host window, select Disconnect.

If the **Host** is minimized and only visible as an icon in the notification area in the lower right corner of the screen, you can end the remote control session by right-clicking on the icon and selecting **Disconnect**.

4 Providing remote support

4.1 Set up Help Request on Guest and Host

If you offer help services, the **Help Request** function should be set up on both the **Guest** and **Host** before Host users can request help from your help service.

You also need to specify the communication profile or profiles to use.

To set up the **Help Request** function on the **Guest**, proceed as follows:

1. In the **Tools** menu, select **Program Options**.
2. Click on the **Help Request** tab.
3. Select the **Enable Help Request** check box.
4. In the **Help Service** tab, select the **Enable Help Service** check box.

In one of the **Help Service** fields below, specify the name of your help service. You may have more than one help service.

Setup use of tickets

If you have an extended **Guest**, you see two more sub-tabs on the **Help Request** tab.

Service Tickets tab

The **Service Tickets** tab enables an extended **Guest** to service help requests by a service ticket number. Service tickets are used for **Connect** and **Impero OnDemand** (1.74 and earlier versions).

1. Select the **Enable Service Tickets** check box to enable use of service tickets to service help requests by a service ticket number.
2. In the **Service Ticket Format** field enter a service ticket format using any character plus the control characters #, @, and *.

# produces a number (0-9), @ produces a letter (A-Z), and * produces a number or a letter (0- 9, A-Z), for example @##-****. In the **Help Request** tab in the **Guest** window, this generates service tickets that look like this: JK50-M3SR.

NOTE: The service ticket generated from this can only be used once, after which a new ticket is generated.

3. In the **Number of auto generated Service Tickets** field specify the number (0-3, 0 = manually) of service tickets to be auto-generated.

WebConnect tab

The WebConnect tab enables an extended Guest to service help requests by a WebConnect ticket. WebConnect tickets are used for OnDemand 2.0 and later versions.

1. Select the Enable WebConnect tickets check box to enable use of WebConnect tickets.

2. In the WebConnect Ticket field enter anything that you want to use as a WebConnect ticket for identification purposes during a help request session using WebConnect, for example an email address, a name, or a keyword, for example Security Server.

3. Select a communication profile in the WebConnect Communication Profile list.

The WebConnect communication profile contains the credentials and the Connection Manager URL that are in use for the WebConnect connection.

The profile itself should be defined in the Setup Wizard or in Program Options > Communication Profiles before you can select it here. One or more WebConnect profiles can be defined in Communication Profiles.

4. In the Update interval field, specify how often the Guest should communicate with WebConnect and check for new tickets. Specify an interval in seconds.

5. Click on OK to close the Program Options dialog box.

To set up the Help Request function on the Host, proceed as follows:

1. In the Tools menu, select Program Options.

2. Click on the Help Request tab.

3. In the Help provider field, enter the name of a help service provider.

4. Specify the communication profile that should be used for the connection.

Select one of these options:

Use current Host communication profiles	Select this option to send help requests using communication profiles enabled in Tools > Communication Profiles. If you have enabled more than one communication profile, or if you have enabled only communication profiles using networking communication devices, the Select Help Request Communication Profile dialog box is displayed when requesting help. Select a communication profile.

	You can only use TCP/IP, if the Guest and Host are on the same network. If the Guest and Host are not on the same network, select for example LAN (TCP) or Internet (TCP). Make sure to specify the Guest IP address.
Use specific Communication Profile	Select this option to use a specific communication profile. Select one of the available Host communication profiles in the drop-down list. You can only use TCP/IP, if the Guest and Host are on the same network. If the Guest and Host are not on the same network, select for example LAN (TCP) or Internet (TCP). Make sure to specify the Guest IP address. You can specify the IP address at this point in the Advanced Help Request Options, if you prefer. Otherwise, the Host user is prompted for the IP address when requesting help. The latter allows the Host user to specify different addresses and thereby contact different supporters when requesting help. Advanced Help Request Options 1. Click on the Advanced button. The Advanced Help Request Options dialog box is displayed. 2. In the Phone number or IP address field enter the IP address of the Guest. You can also change the Help request timeout if not answered setting, if necessary. 3. If you request help through a Guest network Impero Gateway, you can specify the gateway logon credentials in the Gateway logon section. Otherwise the Host user is prompted to enter these when requesting help. 4. Select the Use current logon credentials for

	Windows Security authentication check box, if the Host user should log on using the name, password and domain that the user used to log on to Windows on the Host computer. 5. Select the Enable Help Service check box.

4.2 Respond to a help request

If you are using service tickets (extended Guest for OnDemand 1.74 and earlier versions) for help requests, make sure to pass on a service ticket to the Host user by phone or e-mail.

You find the service ticket in the Guest Help Request tab. The service ticket can only be used once, after which a new ticket is generated. The Host user then uses the service ticket to send a help request to you.

If you are using WebConnect tickets (extended Guest for OnDemand 2.0 and later versions), you do not need to do anything.

The WebConnect ticket can either be predefined in the OnDemand Host or the Host user can enter anything, for example a name or a keyword in the OnDemand Host.

All incoming help requests are displayed in the Guest Help Request tab.

Double-click on a help request on the list to start a default session, which is typically remote control.

Alternatively, select a help request and click on a button from the toolbar to start a remote control session or another type of session.

You are prompted to log on to the Host.

Once you have logged on to the Host, you can start helping the Host user using the available remote control functions, and you can communicate with the Host user using the chat for example.

NOTE: To be able to service help requests make sure to set up the communication profiles and the Help Request options on both the Guest and Host. Refer to the Set up Help Request on Guest and Host for more information.

4.3 Run a multi Guest session

If allowed in the General tab of the Host Program Options, multiple Guests can connect to the same Host in a multi Guest session.

For example, if you need help from another supporter while providing support to a Host user, other Guests can join your session by connecting to the same Host.

In a multi Guest remote control session, one Guest at a time can have keyboard and mouse control. The Guest that has keyboard and mouse control can execute all actions allowed to it by the Guest Access Security settings on the Host.

Guests that do not have keyboard and mouse control can execute only a limited range of actions.

The Host window title bar displays the name of the Guest that has keyboard and mouse control. Other connected Guests are indicated by +<Number of other connected Guests>.

Example: Connected [User1]+1

Guests that the Guest Access Security settings allow to act as multi Guest session administrator can manage a multi Guest session. This means that these Guests can:

- Show a connection list of connected Guests
- Suspend further connections
- Disconnect all other Guests
- Start a multi chat session with all connected the Guests and the Host.

Guests with no rights to act as a multi Guest session administrator cannot carry out these actions.

See also

Communicate with Host users

Guest Access Security

4.4 Send special keystrokes

During remote control you can send various keystroke combinations to the Host computer using the Send Keystrokes command on the title bar menu of the Remote Control window.

You also find the most commonly used commands as toolbar buttons in the Remote

Control window.

CAUTION! Using these keystroke combinations from the keyboard can have undesired effects.

Keystroke combination	Description
Send CTRLI+ESC	Select this command to send the keystroke combination CTRL+ESC to the Host. Alternatively, click on the Send CTRL+ESC button on the toolbar. This keystroke combination displays the Start menu on a Windows Host computer or the Window List on an OS/2 Host computer.
Send CTRL+ALT+DEL	Select this command to send the keystroke combination CTRL+ALT+DEL to the Host. Alternatively, click on the Send CTRL+ALT+DELbutton on the toolbar. This keystroke combination displays the security dialog box on a Windows 2000/XP/2003/2008/Vista/7 Host computer or restarts an OS/2 Host computer. NOTE: Send CTRL+ALT+DEL is disabled with a Windows ME, 98 or 95 Host computer. Select Restart Host PC to re-start the Host computer.
Send ALT+TAB	Select this command to send the keystroke combination ALT+TAB to the Host. This keystroke combination switches the active window clockwise on the Host computer screen.
Send ALT+SHIFT+TAB	Select this command to send the keystroke combination ALT+SHIFT+TAB to the Host. This keystroke combination switches the active window counter-clockwise on the Host computer screen.
Send Print Screen	Select this command to send a PRINT SCREEN command to the Host. This copies an image of the entire Host computer screen to

	the Host computer clipboard.
Send ALT+PRINT SCREEN	Select this command to send an ALT+PRINT SCREEN command to the Host. This copies an image of the active window on the Host computer screen to the Host computer clipboard.

NOTE: The Send Keystrokes command is disabled if the Guest Access Security settings on the Host do not allow use of keyboard and mouse.

4.5 Use clipboard commands

During remote control you can use the clipboard.

You access the clipboard commands from the Clipboard command in the title bar menu of the Remote Control window. You also find these commands as toolbar buttons in the Remote Control window.

Command	Description
Send to Host	Select this command to send the Guest computer clipboard content to the Host computer clipboard. Alternatively, click on the Send Clipboard button from the toolbar. NOTE: This command is disabled if the Guest Access Security settings on the Host do not allow Transfer clipboard.
Retrieve from Host	Select this command to retrieve the Host computer clipboard content to the Guest computer clipboard. Alternatively, click on the Retrieve from Host button from the toolbar. NOTE: This command is disabled if the Guest Access Security settings on the Host do not allow Transfer clipboard.
Save Screen to Clipboard	Select this command to capture the Host computer screen image to the Guest computer clipboard. Alternatively, click on the Save Screen to Clipboard button from the toolbar.
Save Screen to File	Select this command to capture the Host computer screen im-

	age and save it as a bitmap file with the name `<Host name>-<Date>-<Time>.bmp` in the SnapShot folder. You can change the file name and folder before saving. Alternatively, click on the Save Screen to File button from the toolbar.

4.6 Communicate with Host users

Connect offers a number of ways in which you can communicate with the Host users while providing remote support.

If allowed by the Guest Access Security settings on the Host, the Guest can start a chat or an audio-video chat with a Host, or the Guest can send a message to the Host.

Chat

To start a chat, when already connected to a Host, proceed as follows:

1. In the Remote Control window, click on the Chat button from the toolbar.
2. In the Chat dialog box, type your message.
3. Click on the Send button.

To start a chat, if not already connected to a Host, proceed as follows:

1. In the Guest window, select the Host.
2. Click on the Chat button from the toolbar. Alternatively, select Chat in the Connection menu.
3. In the Chat dialog box, type your message.
4. Click on the Send button.

The Host user can reply, and the chat session remains open until either you or the Host user close it by clicking on the End chat button. A Host can also request a chat with the Guest.

NOTE: You can save the chat as an ***.rtf** file for documentation purposes.

Multi chat

If the Host allows multiple simultaneous Guest connections, a Guest that the Guest Access Security settings allow to act as multi Guest session administrator can start a multi chat with the **Host** and all the connected **Guests**. Refer to the Run a multi Guest Session section for more information.

A **Start Multi Chat** button is displayed in the toolbar in the **Remote Control** window of the **Guest** that is a multi **Guest** session administrator. Click on this button to start a chat with the **Host** and all other connected **Guests** at the same time.

Audio-video chat

The **Guest** can start an audio-video chat session with a **Host**, if that audio-video equipment is installed on both sides. Also the **Host** can request an audio-video chat session with the **Guest**, if they are already connected.

To start an audio-video chat, when already connected to a **Host**, proceed as follows:

In the **Remote Control** window, click on the **Audio-Video Chat** button from the toolbar.
The **Audio-Video Chat** dialog box is displayed.

To start an audio-video chat, if not already connected to a **Host**, proceed as follows:
1. In the **Guest** window, select the **Host** that you want to chat with.

2. Click on the **Audio-Video Chat** button from the toolbar. Alternatively, select **Audio-Video Chat** on the **Connection** menu.
The **Audio-Video Chat** dialog box is displayed.
Depending on the hardware available, you can use your microphone to talk to the Host user, and if **Video** is enabled, you can also see each other in the dialog box.
Use the toolbar buttons at the top and the slide bars on the right to control sound and video.

Only the **Guest** can end the audio-video chat session by clicking on the **Stop Audio-Video Chat** button from the toolbar.

NOTE: Each **Guest** and each **Host** can run only one audio session including Transfer Sound at a time.

Message

To send a message to a **Host**, when already connected, proceed as follows:

1. In the **Remote Control** window, click on the **Send Message** button from the toolbar.

2. Type the text you want to send and click on the **Send Message** button from the toolbar.

To send a message to a **Host**, if not already connected, proceed as follows:

1. Select the **Host**.
2. Click on the **Send Message** button from the toolbar. Alternatively, select **Send Message** in the **Connection** menu.
3. Type the text you want to send and click on the **Send Message** button from the toolbar.

The message is displayed on the **Host** computer. The Host user cannot reply or send a new message. If you want the Host user to reply, use one of the chat options.

See also
Guest Access Security
Program Options (Audio-Video Chat tab)

4.7 Send or receive print jobs

You can send a **Guest** computer print job to a **Host** computer printer (remote printer). Host users can likewise send a print job to a **Guest** computer printer.

It is necessary that an **Impero** printer and the correct remote printing device driver are installed on the computer sending the print job.

To add an **Impero** printer on the **Guest** computer, proceed as follows:

1. In the **Tools** menu, select **Options**.
2. Click on the **Remote Printing** tab.
3. Click on the **Add** printer button. The **Add printer guidelines** window is displayed.
4. Read the guidelines and click on the **Ready** button to start adding an **Impero** printer using the **Add Printer Wizard**.

The **Add printer guidelines** window remains on the screen while you go through the wizard.

Send a print job to a remote printer

Once you have added the Impero printer on the Guest computer, you can send a print job to the remote printer in question.

Example: If you want to print a Word document on the remote printer, activate the print job as you normally would in Word. Make sure that you choose the Impero printer that you added.

4.7.1 Redirect a print job

You can redirect a print job sent from the Host computer to the Guest computer to any printer specified on the Guest computer.

To redirect a print job, proceed as follows:

1. In the Tools menu, select Options.
2. Click on the Remote Printing tab.
3. In the Redirect print to section, select one of the following options:

Option	Description
Default printer	Redirect the print job to the default Guest computer printer.
Prompt with a list of available printers	Select this option and click on the Browse button to display the Select Print Redirection Printer dialog box. The dialog box contains the names of Guest computer printers. Select a name and click on OK to specify the printer name in the field. Incoming Impero print jobs are then redirected to this printer.

4.8 Share your screen

When providing support you might want to demonstrate a procedure to a Host user.

If allowed by the Guest Access Security settings on the Host, you can start a demonstrate session with a Host. This enables you to display the Guest computer screen image on the Host computer while you are carrying out a particular procedure.

To start a demonstrate session, proceed as follows:

When already connected, in the **Remote Control** window, click on the **Demonstrate** button on the toolbar.

If you are not are not already connected, you can connect and run a demonstrate session from the **Phonebook** tab, the **Quick Connect** tab, or the **History** tab.

1. In one of the these tabs, select the **Host** computer that you want to connect to and and run a demonstrate session with.

2. Then click on the **Demonstrate** button in the toolbar in the **Guest** window.

When you start the demonstrate session, and before anything is displayed on the **Host** computer, the **Mask Windows** dialog box is displayed. This dialog box enables you to mask **Guest** computer screen elements that you do not want the Host user to see. These elements are displayed as black rectangles on the **Host** computer screen.

To mask/unmask a screen element, proceed as follows:

1. Select the element in the pane.

2. Click on the **+** (plus) or **-** (minus) button at the bottom of the dialog box to mask or unmask the element.

Select the **New screen** window warning check box to have the **New window** dialog box displayed if a new screen element that does not belong to a masked application element opens on the **Guest** computer screen.

Select what you want to mask.

3. Click on **OK**.

The **Impero Demonstration** window is displayed on the selected **Host** computer screen.

During a demonstrate session, a small toolbox is displayed on the **Guest** computer screen. It allows you to stop the demonstration or display the **Mask windows** dialog box, if you want to make changes to the masking.

4.9 Impero Screen Video

Impero Screen Video is a tool for recording the actions you take and the commands you click.

To start **Screen Video**, proceed as follows:

In the Windows **Start** menu, point to **All Programs**, **Impero Connect**, **Tools** and then click on **Screen Video**.

Use the tool to create a video within an area of the screen or of the entire screen.

To capture a screen video

1. Set up the tool according to your preferences.

In the **Region** menu, select the area you want to capture.

TIP: Typically **Full Screen** is selected.

In the **Options** menu, select recording options and define settings.

TIP: It is often a good idea to hide the program when recording starts, and to define keyboard shortcut keys to start and stop the recording.

These settings are saved and can be used the next time you want to capture a screen video.

2. To start the recording, click on the **Record** button

3. Stop recording by pressing the shortcut key you defined. Alternatively, you can right-click on the **Screen Video** icon in the notification area and click on the **Stop** button on the shortcut menu.

Overview of the Options menu

Option	Description
Video Options	Change the encoder to be used for the video recording. For the configurable encoders, click on **Configure** to set for example compression. Move the Quality slider to the right to increase quality. Note that a higher quality video file is larger. You can let **Screen Video** automatically adjust frame rates: Leave the **Auto Adjust** check box selected. Or you can clear the **Auto Adjust** check box and set the options yourself: Max frame rate left end represents recording 200 frames/

<table>
<tr><td></td><td>second and Max frame rate right end represents recording 1 frame/minute. When you move the slider, the Set Key Frames Every, Capture Frames Every and Playback Rate fields are automatically adjusted:
<table>
<tr><th>Recording frame rate</th><th>Set Key Frames Every</th><th>Capture Frame Every</th><th>Playback Rate</th></tr>
<tr><td>200 - 1 frames/ second</td><td>Second</td><td>0.005 - 1 second</td><td>Recording frame rate</td></tr>
<tr><td>60 - 1 frames/ minute</td><td>20 frames</td><td>1 - 60 seconds</td><td>20 frames/ second</td></tr>
</table>
NOTE: Playback is synchronized at each key frame. A large number of frames makes a large file.</td></tr>
<tr><td>Cursor Options</td><td>Define whether the mouse pointer should be included in the recording, and define the pointer appearance.</td></tr>
<tr><td>Audio Options</td><td>Define options for recording sound as well as video.</td></tr>
<tr><td>Autopan Speed</td><td>Setting autopan speed is relevant when Enable Autopan has been selected (command above in the same menu). Automatic panning means that the recording region center is automatically moved towards the mouse pointer position while recording. When Enable Autopan is not selected, the recording region center does not move.
Autopan Speed defines how fast the recording region center is moved.</td></tr>
<tr><td>Recording Thread Priority</td><td>Recording Thread Priority means that a priority is set for use of computer resources for Screen Video as compared to other program running at the same time.
General guideline: If the video recording does not play smoothly, computer resources may be too scarce and it might help to raise the Recording Thread Priority.</td></tr>
<tr><td>Keyboard Shortcuts</td><td>Define keyboard keys to control the recording.</td></tr>
</table>

4.10 Impero Marker Utility

Use the Impero Marker Utility to draw and write or magnify something on the Host computer screen during a remote control session.

The tool can be used by both the Guest computer and the Host computer. Note, though, that the Host user cannot initiate this feature. It only opens if the Host is remote controlled and the Guest user decides to start the Marker Utility.

The texts and lines created using the Marker Utility 'float' over the desktop. If other applications are opened, texts and lines remain on top.

The Marker Utility includes tools for drawing shapes like circles and rectangles and for writing text or magnifying a part of the screen.

To start the Marker Utility from the Guest, proceed as follows:

1. Connect to the Host.
2. In the Remote Control window, click on the Marker Mode button in the toolbar.

The Marker Utility opens and you can start using the tools. Place the mouse pointer on a toolbar button for a description of the tool.

To close the Marker Utility from the Guest, proceed as follows:

In the Remote Control window, click on the Marker Mode button in the toolbar.

Alternatively, in the title bar menu of the Remote Control window, select the Marker Mode command.

5 Dialog box help

5.1 Guest dialog boxes

5.1.1 Advanced audio settings

Use the **Advanced audio settings** dialog box to specify preferred audio playback and recording devices to be used in connection with audio-video chat.

Playback

The **Preferred device** drop-down list contains the names of audio playback devices found by Windows. Select your preferred audio playback device from the list.

Record

The **Preferred device** drop-down list contains the names of audio recording devices found by Windows. Select your preferred audio recording device in the list.

NOTE: If multimedia devices are connected to the computer, the <Use any available device> selection may select a connected device instead of the computer sound system. In that case, select the computer sound system.

Audio Compression

The Try audio compression codecs in the following order pane contains a Windows prioritized list of mono audio compression codecs available on the **Guest** computer.

Use the **Up/Down** buttons to move a codec up or down in the prioritized list. You can restore the default codec priority by clicking on the **Use defaults** button.

The highest prioritized **Guest** computer codec that is also available on the **Host** computer is used.

See also

Program Options (Audio-Video Chat tab)

5.1.2 Advanced Help Service

Use the **Advanced Help Service** dialog box to specify actions to be executed when a help request arrives.

Option	Description
Action	Select an action in the list. The list contains the following options: • **None**: No action. • **Send message**: Run a local program if specified and send a message to the **Host**. The fields below are enabled. • **Run local program**: Run a local program if specified. The fields below, except **Send message**, are enabled.
Command line	Specify the command line of a **Guest** computer program, typically a helpdesk program to register the help request. Click on the **[...]** button to select a program file. You can add the following arguments to the command: • %H: Help request Host name. • %T: Help request time. • %P: Help request problem description.
Timeout	Specify a number of seconds (default: 5, range 0-9999, 0 = no timeout). The command specified above times out (cancels if unsuccessful) after the specified number of seconds.
Send message	Specify the path and name of an **`*.rtf`** file to send a message with the **`*.rtf`** file content to the **Host** requesting help. See also Communicate with Host users (Message). Click on the **[...]** button to open an *.rtf file.
Clear help request	Select this check box to delete the help request record in the **Help Request** tab when the actions specified above have been executed successfully. **NOTE**: Deleting the **Help Request** tab record does not cancel the help request.
Display a notification	Select this check box to be notified when a help request arrives.

message when new help request arrives	The notification message contains the help request **Host** name, time and, if specified, problem description.

See also

Set up Help Request on Guest and Host
Respond to a help request
Program Options (Help Request tab)

5.1.3 Advanced inventory option

Use the **Advanced inventory option** dialog box to specify inventory processing and custom inventory items.

Run program after inventory scan

You can specify an inventory processing program to automatically process each newly retrieved Host computer inventory. Select one of these options:

Option	Description
Disable	Disable running the program specified below.
Run for each Host	Run the program specified below when a **Host** computer inventory is retrieved.
Run after all scans have completed	Run the program file specified below when a batch of **Host** computer inventories is retrieved.
File name	Specify an inventory processing program file path and name including required command line switches. Click on the **Browse** button to open an inventory processing program file. The path and name of the file is displayed in the field.

Custom inventory items

To add custom inventory items, click on the **Add** button. The **Custom Inventory Items** dialog box is displayed. Refer to the Custom Inventory Items for more information.

To edit a custom inventory item after adding it, click on the **Edit** button if you want.

When you generate **Host** inventories, the inventories contains the custom inventory item that you defined.

See also

Program Options (Inventory tab)

5.1.4 Advanced TCP/IP Configuration

Use the **Advanced TCP/IP Configuration** dialog box to set advanced options for the TCP/IP communication profile.

Bindings

Option	Description
Use all available IP addresses	Select this check box to use all available IP addresses. If the computer has multiple IP addresses and only one of them is to be used for **Impero** communication, clear the check box to enable the IP address field or interface list.
IP address	Specify the IP address that is to be used for **Impero** communication.
Use an interface	Specify which network interface is to be used for **Impero** communication.

Specify Port Numbers

Option	Description
Use default port numbers	Select this check box to use the default **Impero** port number **6502** for **Receive port** and **Send port**. Port number **1970** is officially registered to **Connect**. However, port number **6502** is the preferred default port number for compatibility with older **Impero** versions.
Receive port	If the **Use default port numbers** check box is selected, the port number **6502** is displayed. If the **Use default port numbers** check box is not selected, the number is editable. You can specify a number in the range **1025–65535**.

Send port	If the **Use default port numbers** check box is selected, the number **6502** is displayed. If the **Use default port numbers** check box is not selected, the number is editable. You can specify a number in the range **1025–65535**. The **Send port** number of the source module should correspond to the **Receive port** number of the destination module.

Options

Select the **Use TCP for session if possible** check box to connect by TCP/IP, but if available on the **Guest** and **Host**, switch to TCP/IP (TCP) when connected for high speed session communication.

See also

Communication Profile Edit

5.1.5 Advanced Video

To set advanced video options, use the **Advanced Video** dialog box.

Select the driver to use for video in the drop-down list. If a video camera is installed, the field contains its driver name, and the image frame displays the image captured by the camera.

To display the **Windows Video Format** dialog box and format the video capture image, click on the **Format** button.

To display the **Windows Video Source** dialog box and change video source properties, click on the **Properties** button .

To disable video data compression, select the **Disable compression** check box.

5.1.6 Communication Profile Edit

Use the **Communication Profile Edit** dialog box to create or edit a communication profile.

Communication information

Option	Description
Description of the communication profile	Enter a communication profile name. The name should be unique. If the field already contains a communication profile name, you can edit the field contents. NOTE: You can create multiple differently named communication profiles that use the same communication device.
Communication device	Specify the name of the communication device to be used by the communication profile. Select a communication device on the drop-down list.
Use dial-up networking	This check box is enabled only if a TCP/IP family communication device is selected from the **Communication device** field. Select the check box to expand the **Communication Profile Edit** dialog box with a **Dial-up network connection** section.

Dial-Up Network Connection

Option	Description
Dial-up network profile	On the list of available dial-up network profiles, select a profile to use to connect to a network.
Dialing from Calling card	The dialing properties of the selected dial-up network profile is displayed here.
Configure	Click on this button to display the Dial-up Connection dialog box and configure the dial-up connection.
Dialing properties	Click on this button to display the **Phone and Modem Options** dialog box and edit the dialing properties of the selected dial-up network profile.
Add profile	Click on this button to display the **Network Connection Wizard**, which helps you add a dial-up network profile.

[Communication profile name]

The lower dialog box section is named according to the communication device displayed in the **Communication device** field.

In this section, you can specify the configuration of the communication device that should apply to the communication profile. The options vary depending on the communication device.

For more information about the most commonly used communication devices see the list below.

TCP/IP

Max packet size (MTU)	Specify the maximum packet size (range `512- 5146`, default: `2600`). A high MTU increases the communication speed and a low MTU can contribute to solving communication problems.
Optimize for Internet communication	Select this check box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Advanced	Click on this button to display the **Advanced TCP/IP Configuration** dialog box. See Advanced TCP/IP Configuration.
IP Broadcast list	Click on this button to display the **IP Broadcast List** dialog box. See IP Broadcast List.

General information about Impero TCP/IP

Impero TCP/IP is a UDP based communication device that connects by UDP and optionally communicate by TCP/IP (TCP) during a session.

Each communication profile that uses TCP/IP can support multiple **Impero** connections.

TCP/IP offers three connect options:

- IP address
- Name response
- Name resolution

IP address

You can connect by IP address across segmented IP networks including the Internet. It is necessary that the source module port number matches the destination module port number, see Advanced TCP/IP Configuration.

If you connect from outside a network protected by a network address translation (NAT) firewall or proxy server to a **Impero** module on a network computer, specify the firewall or proxy server public IP address with the port number assigned to the network computer, for example `192.168.20.51:1234`.
Ask the firewall or proxy server administrator which port number is assigned to a specific network computer.

Name response

Name response broadcasts a name, the first characters of a name or without a name, requesting **Impero** modules with a corresponding enabled name to respond. The following name response options are available:

- If a **Guest** connects or browses using the Host name qualifier H::, the **Host** can respond by its enabled Name type name.
- If a **Guest** connects or browses using the Host name qualifier U::, the **Host** can respond by its enabled LAN User type name.
- If a **Host** requests help, the **Guest** can respond by its enabled Help service names.

NOTE: A broadcast reaches only computers on the local network segment and computers whose IP address or DNS name is specified in the communication profile **IP Broadcast List**.

Name resolution

Name resolution resolves a specified name into its corresponding IP address. These name resolution options are available:

- In the Advanced TCP/IP Configuration dialog box, select the **Use Impero Name Server** check box and specify the **Impero Name Servers** to use.
  Under **Program Options** > **Host Name** > **Impero Name Server**, specify the **Name Space ID** used by the Impero modules you want to connect to.

Connect by any enabled destination module name, for a **Host** help request a Guest Help service name.

Name Server resolves the name into the corresponding IP address and connect by it across segmented IP networks including the Internet. You can also browse for **Hosts** using the **Name Server**.

- If a **Guest** connects by a name using the Host name qualifier DNS::, a domain name server interprets the name as a DNS name and attempt to resolve it into a corresponding IP address, so the **Guest** can connect by it across segmented IP networks, including the Internet.

NOTE: In most cases, if the Host name qualifier H:: is used, a domain name server interprets the name as a DNS name and attempt to resolve it into a corresponding IP address.

- If a **Guest** connects by a name using the Host name qualifier LDAP::, the **Guest** searches directory services specified on the **Directory Services** tab in the **Program Options** dialog box for a user with this name and connect by the corresponding address attribute, which is typically an IP address.

You can also browse for Hosts using directory services.

See also

Program Options (Host Name tab)

Connect problems

In case of connect problems, verify that an IP connection is available from a command prompt by typing:

```
PING <Impero module IP address>
```

The PING utility sends four data packets requesting a reply. If you receive the replies, an IP connection is available.

If an IP connection is available and connectivity problems persist, consult your network/ system administrator or submit a support request to **Impero Support**.

TCP/IP (TCP)

Option	Description
Optimize for Internet	Select this check box to apply settings (MTU, data compression,

communication	etc.) optimized for communicating across the Internet.
Encapsulate in HTTP	Select this check box to wrap data packets as HTTP packets to ease firewall passage. This is also known as HTTP-tunneling.
Use Proxy Settings	If you select **Encapsulate in HTTP**, the **Use Proxy Settings** check box becomes available for selection. If you select this check box, proxy authentication is activated in the used communication profile. The application uses the proxy settings defined in Windows.
Advanced	Click on this button to display the **Advanced TCP/IP Configuration** dialog box. See Advanced TCP/IP Configuration.

Impero TCP/IP (TCP) is a TCP based communication device.

Each communication profile that uses TCP/IP (TCP) can support one **Impero** connection. To support multiple **Impero** connections, you can create multiple communication profiles that use TCP/IP (TCP).

To connect, specify a computer IP address.

If you connect from outside a network protected by a network address translation (NAT) firewall or proxy server to a **Impero** module on a network computer, specify the firewall or proxy server public IP address with the port number assigned to the network computer, for example `192.168.20.51:1234`.

Ask the firewall or proxy server administrator which port number is assigned to a specific network computer.

- If a **Guest** connects directly to a **Host**, specify the **Host** computer IP address.
- If a **Guest** connects through a remote network **Gateway** to a **Host**, specify the IP address of the gateway computer and optionally the **Host** name.
- If a **Host** requests help, a **Guest** connected to directly or on a remote **Gateway** network can respond by its enabled Help service names.

TCP/IP (TCP IPv6)

Option	Description
Optimize for Internet	Check this box to apply settings (MTU, data compression, etc.) op-

communication	timized for communicating across the Internet.
Advanced	Click on this button to display the Advanced TCP/IP Configuration dialog box. See Advanced TCP/IP Configuration.

Impero TCP/IP (TCP IPv6) is a TCP IPv6 based communication device.

Each communication profile that uses TCP/IP (TCP IPv6) can support one Impero connection. To support multiple Impero connections, you can create multiple communication profiles that use TCP/IP (TCP IPv6).

You can use TCP/IP (TCP IPv6) only between computers connected to an IPv6 network.

To connect, specify a computer IPv6 address.

- If a Guest connects directly to a Host, specify the Host computer IPv6 address.
- If a Guest connects through a remote network Gateway to a Host, specify the Gateway computer IPv6 address and optionally the Host name.
- If a Host requests help, a Guest connected to directly or on a remote Gateway network can respond by its enabled Help service names.

WebConnect

Option	Description
Address	Specify the URL of the WebConnect / WebConnect 3 service, i.e. the Connection Manager, that facilitates the WebConnect / WebConnect 3 connection.
Account	Specify a WebConnect / WebConnect 3 service recognized account.
Password	Specify the password corresponding to the WebConnect / WebConnect 3 service recognized account
Domain	Specify the domain corresponding to the WebConnect /WebConnect 3 service recognized account.
Optimize for Internet communication	Select this check box to apply settings (MTU, data compression, etc.) optimized for communicating across the Internet.
Advanced	Click on this button to display the Advanced TCP/IP Configuration

	dialog box. See Advanced TCP/IP Configuration.
Test	Click on the **Test** button to verify the WebConnect Service URL.

WebConnect is a **Impero** proprietary communication device that enables networked **Impero** modules to connect easily over the Internet through a **Impero** connection service called **WebConnect** without the need to open firewalls for incoming traffic. All of the traffic is outgoing.

NOTE: **WebConnect 3** service has improved security.

Impero Portal

Option	Description
Address	Specify the address of the **Portal**: connect.backdrop.cloud.
Live Update (Guest only)	Select this check box to see the available hosts in real-time.
Enrollment Key (Host only)	This is retrieved from the **Portal** under **Account** > **Deployments**. It is a string which is associated to a deployment package. The **Host** is enrolled into the **Portal** with the predefined settings from the specific deployment package. For more details on deployment packages and enrollment keys, see the Impero Portal User's Guide.
Test	Click on the **Test** button to verify the **Portal** address and credentials.

The **Portal** is a service which provides connectivity across the internet. It does not require direct visibility between end points.

To remote control a **Host** using the **Portal** authentication and authorization you need to:

1. Make sure that you have a **Portal** account.
2. On the **Host** create a **Portal** communication profile using the portal address and the enrollment key.
3. On the **Guest** select the **Portal** communication profile. When initializing the **Portal** communication profile for the first time, you are prompted to specify the **Portal** credentials

4. Select the **Host**.

5. Click on the **Connect** button.

Gateway

Option	Description
Access Gateway via communication profile	In the drop-down list, select the communication profile that should be used to access the local network **Gateway**. Select <Any initialized communication> to connect to or browse for **Gateway** device groups using any enabled communication profile that uses a networking communication device. Select another communication profile to connect or browse using only that communication profile, which does not need to be enabled. Select **Terminal Server** only if your **Impero** module is located on a terminal server client.
Gateway device group	Gateway device groups are administrator specified names of available outgoing communication on local network **Impero Gateways**. Select one of these options: Use device group: Select this option to specify a Gateway device group name in the field. Browse for device groups: Select this option to display the Gateway Device Group List dialog box when connecting.

Gateway is an **Impero** proprietary communication device that enables a network **Impero** module to connect through a local network **Gateway**.

Each communication profile that uses **Gateway** can support only one **Impero** connection.

To connect, specify a modem telephone number or computer IP address according to the selected device group type. The device group type is selected in the **Gateway Device Group List** dialog box.

- If a Guest connects through a local network Gateway directly to a Host, specify the modem telephone number or computer IP address of the Host computer.
- If a Guest connects through a local network Gateway through a remote network Gateway to a Host, specify the Gateway computer modem telephone number or computer IP address and optionally the Host name.
- If a Host requests help through a local network Gateway, a Guest connected to directly or on a remote Gateway network can respond by its enabled Help service names.

Resources

To use Gateway, make sure that one or multiple outgoing Gateways run on the local network.

Terminal Server

Terminal Server is an Impero proprietary communication device that enables Impero modules running in a terminal server environment to communicate.

Each communication profile that uses Terminal Server can support multiple Impero connections.

To connect, specify a name by which the destination Impero module can respond:

- If a Guest connects or browses using the Host name qualifier H::, the Host can respond by its enabled Name type name.
- If a Guest connects or browses using the Host name qualifier U::, the Host can respond by its enabled LAN User type name.
- If a Host requests help, a Guest can respond by its enabled Help service names.

If the Gateway runs on the terminal server console, terminal server Impero modules and Impero modules outside the terminal server environment can connect through it. Refer to the Administrator's Guide for more information.

5.1.7 Communication Profile Setup

For Impero modules to be able to communicate with each other, it is necessary for you to define a communication profile. A communication profile is a specific configuration of a communication device.

A communication device is a Impero adaptation of a generally available communication protocol or an Impero proprietary communication protocol.

A newly installed Impero module includes default communication profiles. You typically need to modify the default communication profiles or create communication profiles to optimize communication in your environment.

Use the Communication Profile Setup dialog box to enable/disable, create, edit and delete communication profiles.

Select check boxes in the Communication Profile List to enable communication profiles at Impero module loading.

Click on the New button to create a communication profile. The Communication Profile Edit dialog box is displayed.

If you want to edit a communication profile, select the communication profile and click on the Edit button. The Communication Profile Edit dialog box is displayed.

NOTE: To apply changes to enabled communication profiles, reload the Guest.

See also
Communication Profile Edit

5.1.8 Connect to Host

Use the Connect to Host dialog box to add or edit a Connect command.

Select how you want to connect in the Connect using list:

Option	Description
Phonebook file	Connect to a Host using its Impero phonebook file.
Communication profile	Connect to a Host using a communication profile and a Host name and/or a Host computer telephone number or IP address.
Local	Connect locally to the Guest computer.

The dialog box changes depending on what you select in the Connect using list.

- If you select **Phonebook** file, you can specify a phonebook file by browsing for it or entering the path and name of a file in the **Phonebook** file field.
- If you select **Communication profile**, specify the following:

Option	Description
Communication profile	Select a communication profile in the drop-down list which contains available **Guest** communication profiles.
<Host connect information>	Specify **Host** connect information in one or two fields according to the communication profile selection above. In a field in which you can specify an IP address, you can also specify an IP address range, e.g. `192.168.1.1-192.168.1.5`, to connect to multiple **Host** computers from one script. In this case the logon information below must be the same for all the Hosts that you specify.
Logon name	Specify any logon name required by the **Host**.
Logon password	Specify the corresponding password.
Logon domain	Specify the corresponding domain or directory server.
Use current logon credentials for Windows Security authentication	Select this check box to log on to the **Host** by the Windows logon user credentials of the **Guest** computer user.

- If you select Local, no further specification is required.

Click on **OK** to add the **Connect** command in the upper pane of the **Script** dialog box.

See also
Script
Create and run a script

5.1.8.1 Connection Properties

Use the **Connection Properties** dialog box to set a number of properties to optimize **Host** connections according to user preferences. The properties are applied individually to **Host** connections.

Connect tab

Host PC Information

Option	Description
Description	Identifies the Host record. The field can be empty. You can leave it empty to automatically specify the applicable Host name or phone number/IP address in it when creating the Host record. You can edit the field contents.
Phone number/IP address	This field is included if the communication profile selected in the Communication section uses a point-to-point, gateway, or network point-to-point communication device. Specify the Host telephone number or IP address if connecting directly to the Host, otherwise the telephone number or IP address of the network connecting Impero Gateway for the Host.
Name	If the field label does not include "(optional with Gateway)", specify the name by which the Host should respond. If the field label includes "(optional with Gateway)", you can either leave the field empty to browse for Hosts or specify the name by which the Host should respond.
Comments	Specify a comment to be displayed in the Comment column of the right pane of the Phonebook tab or the History tab.

Communication

Option	Description
Communication profile	Specifies the selected communication profile name. You can change the communication profile name by selecting another communication profile in the drop-down list.
Wake on LAN MAC address	If Wake on LAN is enabled, you can specify the MAC address of the Host computer network card to be able to start the Host computer by connecting to the Host.

NOTE: The Connect tab is only included if you open the Connection Properties dialog box from the Phonebook tab or the History tab.

Logon tab

Use the Logon tab to specify the Host and Host network connecting Gateway logon credentials in order to connect without being prompted for logon credentials.

Depending on the Guest Access Method defined on the Host, define the credentials as follows:

Guest access method	Logon name	Logon password	Logon domain
Default access privileges	Empty	Password	Empty
Impero authentication	Guest ID	Password	Empty
Windows security management*	Domain\Username	Password	Empty
Directory services	Username	Password	Directory Service Name
Impero Portal**	N/a	N/a	N/a
NSS - Windows username & password	Domain\Username	Password	Empty
NSS - Impero Guest ID & Password	Guest ID	Password	Empty
NSS - RSA	N/a	N/a	N/a
NSS - Directory services	Username	Password	Directory Service Name

*When authenticating to a Host configured to use Windows authentication, the domain is now integrated in the username field and is only needed if authenticating to a domain. The domain field is inferred from the username when a "\" character is provided, otherwise the local computer is assumed. Examples of accepted entries in a username field are:

Username field	Host in a domain	Host NOT in a domain
Domain\username	Login OK	Login Error
Computer\username	Login OK	Login OK
.\username	Login OK	Login OK
\username	Login OK	Login OK
username	Login Error	Login OK

**: If the Guest and Host are version 12.60 or higher and the communication profile used is based on the Portal, the logon credentials do not work.

Select the Use current logon credentials for Windows Security authentication check box to log in using the Windows logon user name, password and domain of the Guest computer user.

NOTE: The Logon tab is not included if you open the Connection Properties dialog box from the Remote Control window.

Protect Item tab

Use the Protect Item tab to protect a Host record and file with a password.

Password characters are displayed as asterisks or dots. Leave fields empty to disable password protection.

Select the Connect without password checkbox if you want the Guest user to be able to use a phonebook record without knowing the password. The password protection is applied to the contents of the connection properties, so that these are protected against being changed unintentionally.

NOTE: The **Protect Item** tab is only included if you open the Connection Properties dialog box from the Phonebook tab or the History tab.

Startup tab

Use the Startup tab to set startup properties for remote control sessions.

Host window startup size

Option	Description
Windowed	Display the Host screen image in a Remote Control window. If Fit window to Host screen is selected on the Display tab, the window can be resized to its maximized size.
Full screen	Display the Host screen image in full screen to cover the entire Guest computer screen.
Maximized	Display the Host screen image in a maximized Remote Control window covering the entire Guest computer screen except the Windows taskbar.
Minimized	Display the Remote Control window as a button on the Windows taskbar.

Monitors

This section allows you to select which monitors are displayed before connecting to the Host.

Option	Description
All monitors	Displays all the Host monitors. This is the default setting; if you do not select which Host monitor to display, when remote controlling the Host, all Host monitors are displayed on the screen.
Primary monitor	Displays the Host monitor which is set as the primary monitor.
Monitor: <monitor number>	Monitor: `<monitor number>`

Displays the selected Host monitor. If the <monitor number> is higher than the number of monitors available on the Host, when remote controlling the Host All monitors are displayed on the screen.

Remote control window startup size

Option	Description
Enable	Select this check box to enable the elements below and apply their values at startup. Leave unchecked to apply the last displayed Remote Control window position and size.
x	Specify the horizontal offset in pixels of the upper left corner of the Remote Control window from the upper left corner of the Guest computer screen at startup.
y	Specify the vertical offset in pixels of the upper left corner of the Remote Control window from the upper left corner of the Guest computer screen at startup.
Width	Specify the width in pixels of the Remote Control window at startup.
Height	Specify the height in pixels of the Remote Control window at startup.

Actions

Option	Description
Lock Host keyboard and mouse	Select this check box to disable the Host computer keyboard and mouse at startup.
Blank Host display	Select this check box to display a black screen image to the Host user at startup.

Transfer sound	Select this check box to transfer Host computer application sound at startup.
Suspend other Guests from connecting to Host	Select this check box to deny further Guests access to the Host at startup.

NOTE: The Startup tab is not included if you open the Connection Properties dialog box from the Remote Control window.

Display tab

Use the Display tab to set display properties for the Host screen image.

Host window fit

Option	Description
Fit window to Host screen	Resize the Remote Control window to fit the **1:1** scale Host screen image. If the Host screen image has more pixels than the display area of the maximized Remote Control window, the Remote Control window has scrollbars.
Fit Host screen to window	Scale the Host screen image to fit within the Remote Control window.
Do not fit	Display the part of the **1:1** scale Host screen image that fits within the Remote Control window. If the Host screen image has fewer pixels than the display area, black borders surround it. If the Host screen image has more pixels than the display area, the Remote Control window has scrollbars.

Limit number of colors in bitmap mode

Option	Description
No, use actual number of colors	Display true colors. Consumes the most transmission bandwidth.
Max 256 colors	Displays reduced palette colors. Consumes less transmission bandwidth.
Max 16 colors	Displays crude colors.

	Consumes little transmission bandwidth.
Max 2 colors	Displays black and white colors. Consumes a of minimum transmission bandwidth.

DOS Box Font

During remote control, if you start a command prompt window on the **Host** computer, the command prompt window characters are by default displayed on the **Guest** computer using the default font of the **Guest** computer system. You can change the font used.

Clear the **System default** check box to allow selection of another font.

Click on the **Select Font** button to select the command prompt window font. The font change is only seen when displaying the command prompt window in full screen.

Skin

In the **Display** tab of the **Guest Connections Properties** you can define how you want the **Guest** to use skins on connection.

Option	Description
Automatic	Select this option to enable automatic use of skin. The **Host** device, typically a CE/Mobile device, sends a string ID to the Guest, and the **Guest** contacts the **Skin Repository Server** to get the corresponding skin. If the **Guest** does not find the corresponding skin on the Skin Repository Server a default skin is used.
Do not use skin	Select this option not to use skins for remote control sessions.
Use specific skin model	Select this option, if you want to overrule the Automatic option and use a specific skin model. If you select this option, the **Select Model** button is activated. Click on the **Select Model** button to open the **Skin Models** window and select the skin that you want to use. In the **List of Models**, select the skin and then click on **OK**.
Show as transparent window	The skin is displayed as a transparent window without frame or background, showing only the device itself (default). If you clear the check box, you see a normal window with

	frame and a white background behind the device.

See also

Use a skin to see the Host button

Program Options (Skins tab)

Keyboard/Mouse tab

Use the **Keyboard/Mouse** tab to set keyboard and mouse control properties for remote control sessions.

Keyboard

Option	Description
Remote keyboard (Send all keystrokes to Host)	Send all **Guest** computer keystrokes to the **Host** computer.
Local keyboard (Don't send special keystrokes)	Send the **Guest** computer keystrokes except **Send Keystrokes** keystroke combinations to the **Host** computer. Send Send Keystrokes keystroke combinations to the **Guest** computer.
No keyboard control	Send all the **Guest** computer keystrokes to the **Guest** computer.
Use Guest keyboard layout	If the **Guest** and **Host** computer keyboard layouts are different, some **Guest** computer keystrokes can come out wrong on the Host computer. To avoid this, select the **Use Guest keyboard layout** check box.
Don't transfer Host Num Lock, Scroll Lock, Insert and Caps Lock	With some display adapters, enabling these **Host** computer keyboard options may cause the **Guest** computer keyboard lights to flash. To avoid this, select the Don't transfer Host Num Lock, Scroll Lock, Insert and Caps Lock check box.

Mouse

Option	Description

Remote mouse (send all mouse events)	Send all **Guest** computer mouse events (clicks, drags and moves) to the **Host** computer.
Local mouse (Only send clicks and drags)	Send only **Guest** computer mouse clicks and drags to the **Host** computer to save transmission bandwidth.
No mouse control	Send no **Guest** computer mouse events to the **Host**.
Display Host mouse movements	Move the **Guest** computer mouse pointer in accordance with **Host** computer mouse pointer movements.

NOTE: To suppress **Guest** computer mouse pointer movements induced by the **Host** computer, press and hold the **CTRL** key.

Compression/Encryption tab

Use the **Compression/Encryption** tab to set data transmission properties.

Compression level

Connect can compress transmitted data to speed up transmission across slow communication links. However, data compression takes time.

Option	Description
Automatic	Selects compression based on the properties of the applied communication profile. In most cases this provides the fastest transmission.
No compression	Typical selection for fast communication links.
Low	Typical selection for medium fast communication links.
High	Typical selection for slow communication links.

Host screen transfer

Option	Description
Transfer Host screen as commands	Typically faster, but with some **Host** computer display adapters some **Host** screen image details can be lost or corrupted.
Transfer Host screen as bitmap	Typically slower, but transfers Host screen image details correctly. When this option is selected the slider below becomes available.

	The slider has three options that range from better accuracy (Quality) to better performance (Speed). The middle option is a combination of the two. The default option is set to best quality. Here is how you use the slider: • **Quality**: More accuracy using an enhanced compression algorithm. • **Center**: Less accuracy but better performance using a TurboJPEG high compression ratio of 80. • **Speed**: Much less accuracy but much better performance using a TurboJPEG high compression ratio of 50.

NOTE: This section is disabled if you open the **Connection Properties** dialog box from the **Remote Control** window.

Cache

Command mode **Host** screen transfer stores the screen image in cache memory and transfers only image changes. This saves transmission bandwidth and optimizes update speed.

The **Cache size** field displays the selected cache memory size. You can select Automatic and values from None to 10240 kb on the drop-down list.

Automatic selects the cache memory size based on the properties of the used communication profile. In most cases, this provides the optimum.

NOTE: This section is disabled if you open the **Connection Properties** dialog box from the **Remote Control** window.

Total **Impero** cache memory sharing and size is specified on the **Cache** tab in the **Program Options** window.

Preferred Encryption Type

The field displays the encryption type preferred by the **Guest**. You can select another encryption type on the drop-down list.

If the preferred encryption type is enabled on both **Guest** and **Host**, then it is applied.

If Netop 6.x/5.x Compatible is the preferred encryption type and not enabled on both

Guest and Host, select a higher encryption level.

If another encryption type is preferred and this encryption type is not enabled on the Host, an encryption type that is enabled on both Guest and Host is applied.

If no common encryption type is enabled on Guest and Host, enable additional encryption types on the Encryption tab in the Program Options dialog box to achieve a match.

NOTE: The icon of the encryption type used in a remote control session are displayed on the status bar.

Desktop tab

Use the Desktop tab to specify transfer properties for Host computer desktop features.

Optimize screen transfer

Advanced Host computer desktop features slow down the Host screen transfer in command mode and are typically unimportant to the Guest user. Therefore, Connect by default transfers the Host screen image without advanced desktop features.

However, you can change this and select which advanced desktop features to transfer.

Option	Description
Always	Always transfer without advanced desktop features.
Only when high compression	Transfer without advanced desktop features only with high compression, see Compression/Encryption tab.
Never	Never transfer without advanced desktop features.

Optimization parameters

Option	Description
Full optimization	Transfer without the desktop features listed below.
Custom optimization	Select to enable the Custom options section below. You can then clear the selection of specific custom options to enable transfer of these advanced desktop features. Custom options: • Disable wallpaper • Disable screen saver • Disable animation gimmicks • Disable full window drag

	• Disable Windows Aero By default, all check boxes are selected.

Record tab

Use the Record tab to enable remote control session recording.

Select the Record remote control session check box to record a remote control session.

Recording a remote control session creates a record on the Recordings tab. You can play back the recording from the Recordings tab.

If you select the Enforce recording check box on the Program Options window Recording tab, remote control sessions are recorded regardless of the selection on the Record tab.

NOTE: The Record section is disabled if you open the Connection Properties dialog box from the Remote Control window. Recording reduces the remote control session transfer speed.

Custom tab

Use the Custom tab to specify the properties of a custom application command.

Option	Description
Description	Specify a custom application name that is added as a command to the Host record context menu.
Command line	Specify the custom application command line (program file path, name and switches.) Click on the Browse button to open a program file and specify its path and name in the field.

NOTE: The Custom tab is only included if you open the Connection Properties dialog box from the Phonebook tab or the History tab.

5.1.9 Inventory

When you add an Inventory command to a script, the Inventory dialog box is displayed allowing you to specify what should happen to the inventory that is generated.

Option	Description
Inventory step	Select an Inventory step option in the drop-down list: • **One Step**: Generate, retrieve, copy and complete a **Host** computer inventory. • **Generate**: Generate inventory on the **Host** computer. • **Retrieve**: Save the generated inventory to the `%TEMP%\si_out.xml` file on the **Host** computer. **NOTE**: To make the retrieved inventory available for completion on the **Guest** computer, it must be copied by a file transfer **Copy** command from the **Host** computer to the **Guest** computer, typically to the `%TEMP%` directory. • **Complete**: Move a **Host** computer inventory file copied to the **Guest** computer to the inventory directory to enable displaying it on the Inventory tab. The inventory directory is located in the **Impero** configuration files directory, typically `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest\inventory`.
Inventory file path	This field is enabled only if Complete is displayed in the Inventory step field. Specify the **Guest** computer path and name of the inventory file to be completed.

See also

Script
Create and run a script
Generate a Host inventory

5.1.10 Name Not Found

The **Name Not Found** dialog box advises you on how to overcome connect problems.

Here is some additional advice:

- Verify that communication can physically reach the **Host** computer:

If communicating across an IP network, execute this command in a Windows command prompt window:

```
PING <Host computer IP address>
```

This command sends four data packets to the specified IP address requesting replies. If positive replies are received, communication can physically reach the **Host** computer. If negative replies are received, check your network setup or consult your network/system administrator.

If communicating across a modem connection using Windows Modem, the setup of your modem in Windows may not satisfy **Impero** requirements. Try setting up your modem using Serial instead.

- In the **Host** window, on the **Names** tab, verify that the **Host** responds to the specified name or address with the selected communication profile. See Communication Profile Edit for further information about the characteristics of the communication device used by the selected communication profile.
- Try connecting to other **Hosts** starting with **Hosts** close to you. Try using other communication profiles and other **Host** names or addresses.
- Consult your network/system administrator.
- As a last resort, submit a support request to Impero Customer & Product Support.

5.1.11 Custom Inventory Items

Use the **Custom Inventory Items** dialog box to define additional inventory items that should be retrieved during an inventory scan.

Option	Description
Name	Enter a name for the custom inventory item.
Item type	Select an item type, for example Registry key, and fill in all fields for the selected item type as necessary.

The custom inventory item you created is displayed in the **Custom Inventory Items** pane in the **Advanced inventory option** dialog box.

NOTE: The pane contents are stored in the Impero configuration file `InvCuItm.xml`, which is typically located here: `C:\Users\<User name>\AppData\Roaming\Danware`

`Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest.`

When you generate **Host** inventories, the inventories contain the custom inventory item that you defined.

See also

Advanced inventory option
Program Options (Inventory tab)
Process Host computer inventory information

5.1.12 Global Settings

Use the **Global Settings** dialog box to specify the script global settings that should apply as default settings for the subsequent script commands. The dialog box is displayed when you create a script.

To edit the global settings of a script, in the **Script** dialog box upper pane, select the **Global Settings** element and click on **Edit**.

General tab

Use the **General** tab to specify the global file transfer direction.

Option	Description
From	Select **Guest** or **Host** in the drop-down list. Displays the global source **Impero** module name.
To	Displays the receiving Impero module, i.e. the **Impero** module name that has not been selected in the From drop-down list. The field cannot be edited.

Transfer tab

Use the **Transfer** tab to specify global file transfer settings.

Option	Description
Use delta file transfer	Select this check box to compare source files with destination files and transfer only the difference between source files and destination files. This saves transmission bandwidth.
Enable crash recovery	Select this check box to transfer files in a way so that they can be recovered after a computer or network crash during transfer.

Overwrite/Delete tab

Use the **Overwrite/Delete** tab to specify global overwrite and delete settings.

Option	Description
Allow overwriting/deleting existing files/folders	Select this check box to allow overwriting and deleting files and folders on the destination computer.
Allow overwriting/deleting system files	Select this check box to allow overwriting and deleting system files on the destination computer.
Allow overwriting/deleting read-only files	Select this check box to allow overwriting and deleting read-only files on the destination computer.
Allow overwriting/deleting hidden files	Select this check box to allow overwriting and deleting hidden files on the destination computer.

Advanced tab

Use the **Advanced** tab to specify global error handling and the log file settings.

Error Handling

Option	Description
On communication error	Specifies the action in case of a communication error. Select an option in the drop-down list: • Exit: End the script. • Next Host: Proceed to the next Host specified in the script. • Retry 1 time: Retry the failed command once. • Retry 2 times: Retry the failed command twice. • etc.
On transfer error	Specifies the action in case of a file transfer error. Select an option in the drop-down list: • Exit: End the script. • Next Host: Proceed to the next **Host** specified in the script. • Next File: Proceed to the next file specified in the script. • Retry 1 time: Retry the failed command once. • Retry 2 times: Retry the failed command twice. • etc.

Log File

Option	Description
Generate log file	Select this check box to generate a log file when running the script.
Append if log exists	Select this check box to append the log to an existing log file with the specified name. Clear the selection to overwrite. The field below the check box specifies the log file path and name (default: `SCRIPT.LOG`). Click on the **Browse** button to open a different log file. If no path is specified, the log file is located in the **Impero** configuration files folder, typically `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest\`.

Option	Description
Restart script when finished	Select this check box to restart the script at script end.
Close Guest when finished	Select this check box to unload the **Guest** at script end.

See also

Script
Create and run a script

5.1.13 IP Broadcast List

For TCP/IP broadcast communication to reach computers on remote network segments when **Impero** Name Management is not used, make sure that the IP addresses or DNS names are listed in the IP Broadcast List. For further information about Impero Name Management, see the Administrator's Guide.

Click on the **Add** button to open a dialog box allowing you to add a DNS name or IP addresses.

Specify an IP address, for example `192.168.102.57`, an IP address range, for example `192.168.102.20 -192.168.102.30`, or a DNS name, for example MAIL_SVR, to add it to the IP Broadcast List, and click on **OK**.

NOTE: Specifying an IP address range makes each broadcast send a number of data packets corresponding to the number of IP addresses in the range. To avoid excessive network traffic, do not specify larger IP address ranges than justified.

Select the **Disable local subnet broadcast** check box to disable broadcast communication to local network segment computers.

See also

Communication Profile Edit

5.1.14 Log Setup

Log Setup tab

Use the **Log Setup** tab to specify where to log.

Log events

Option	Description
Log locally	Select this check box to log **Impero** events in a log file on the computer.
Log on Impero server	Select this check box to log **Impero** events in the database log of a central Security Server.
Log to Windows event log	Select this check box to log **Impero** events in the Windows event log of the computer and/or of another Windows NT/2000/XP/2003/2008/Vista/7 computer.
Log using SNMP traps	Select this check box to log **Impero** events by sending **SNMP** messages to a management information system.
Custom Host Name for all log events	Select this check box to identify logged events by a customized **Host** name. The left field specifies the customized **Host** name composed from components and keyboard characters on the

	drop-down list to the right. Select a component on the drop-down list to add it in the left field. The following components are available: • %A: IP/MAC address • %I: Host ID • %C: Computer name • %L: Windows logon user name

Custom Guest name for Connection and Session log events	Select this check box to identify **Guests** engaged in Connection and Session log events by a customized name.
	The left field specifies the customized **Guest** name composed from components and keyboard characters on the drop-down list to the right. Select a component from the drop-down list to add it in the left field.
	The following components are available:
	• %A: IP/MAC address
	• %U: Authenticated user name
	• %I: Guest ID
	• %C: Computer name
	• %L: Windows logon user name
	Example of a custom Host and Guest name local Impero log
	`20080903,14:10,Host1+User1,0,00000,00000,HCON+,`
	`20080903,14:10,Host1+User1,1,00000,00000,HSES+,User2@192.168.1.2`
	`20080903,14:10,Host1+User1,2,00000,00000,HSESRC +,User2@192.168.1.2`
	`20080903,14:10,Host1+User1,3,00000,00000,HSESFXFER+,User2@192.168.1.2`
	`20080903,14:10,Host1+User1,4,00000,00000,HSESCHAT +,User-`

	2@192.168.1.2 20080903,14:10,Host1 +User1,5,00000,00000,HSESAUDIO+,User- 2@192.168.1.2 20080903,14:10,Host1 +User1,6,00000,00000,HSESAUDIO-,User- 2@192.168.1.2 20080903,14:10,Host1 +User1,7,00000,00000,HSESCHAT -,User- 2@192.168.1.2 20080903,14:11,Host1 +User1,8,00000,00000,HSESFXFER-,User- 2@192.168.1.2 20080903,14:11,Host1 +User1,9,00000,00000,HSESRC -,User- 2@192.168.1.2 20080903,14:11,Host1+User1,10,00000,00000,HSES -,User2@192.168.1.2 The **Host** name was customized as %C+%L. The **Guest** name was customized as %U@%A. The **Host** was started and the **Guest** started a remote control session, a file transfer session, a chat session and an audio-video chat session and ended sessions in reverse order.

Security Server has an additional check box:

Act as log server: Select this check box to enable logging other **Impero** modules' **Impero** events in the security database **Impero** Log.

Impero Local tab

Use the **Impero Local** tab to specify which **Impero** events should be logged and the local **Impero** log file.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: • Connection • Session • Action • Security • Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See Available Impero log event codes and arguments - Guest.

Log File

This section is only enabled if the **Log locally** check box has been selected on the **Log Setup** tab.

Option	Description
Log file name	Displays the (path and) name of the log file (default: `IMPERO.LOG`). If no path is specified, the log file is located in the **Impero** configuration files folder, typically: • `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for the **Guest** • `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for **Host**-based modules.
Write to disk for each log entry	Select this check box to write each **Impero** event to the local **Impero** log file immediately. Clear the check box to write **Impero** events to the local **Impero** log file when the **Impero** module is unloaded, which consumes less processor capacity. **NOTE**: A new local **Impero** log file that is created when the **Impero** module is loaded overwrites an old local **Impero** log file with the

	same path and file name.

Impero Server tab

Use the **Server** tab to specify which **Impero** events should be logged and the Host ID of the logging server.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: • Connection • Session • Action • Security • Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See Available Impero log event codes and arguments - Guest.

Host ID for Log Server

This section is only enabled if the **Log on Impero server** check box has been selected on the **Log Setup** tab.

Specify the Host ID of the **Impero** server on which **Impero** events should be logged. Click on the **Browse** button to browse the network for available logging **Impero** servers.

NOTE: If the **Use Impero Security Server** option (in Guest Access Security) is selected on a **Host** or extended **Host**, leave the Host ID for Log Server field empty to log in the database log of the specified security server.

Windows Event Log tab

Use the **Windows Event Log** tab to specify which **Impero** events should be logged and Windows event logs.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: • Connection • Session • Action • Security • Configuration

Events to log

In the Events to log list, select the events you wish to log.

See Available Impero log event codes and arguments - Guest.

Use Windows event log

This section is enabled only if the **Log to Windows event log** check box is selected on the **Log Setup** tab.

Option	Description
Local	Select this check box to log **Impero** events in the Windows event log of the computer.
Remote	Select this check box to log **Impero** events in the Windows event log of a remote Windows NT/2000/XP/2003/2008/Vista/7 computer. Specify the Windows name of the remote computer.

SNMP Traps tab

Use the **SNMP Traps** tab to specify which **Impero** events to log in a management information system.

Select Events to view in list

Option	Description
View all Events	Display all available events in the Events to log list.
View Selected	Select event types to display in the Events to log list: • Connection • Session

	• Action • Security • Configuration

Events to log

In the **Events to log** list, select the events you wish to log.

See Available Impero log event codes and arguments - Guest.

If the **Log using SNMP Trapsbox** is selected on the **Log Setup** tab, a **S**imple **N**etwork **M**anagement **P**rotocol (SNMP) message is sent when a selected **Impero** event occurs.

NOTE: **Impero SNMP** events are defined in the `danware.mib` file located in the folder where the **Impero** module is installed.

5.1.14.1 Available Impero log event codes and arguments - Guest

The **Guest** can log the following **Impero** log events:

Connection

Event Name	Event Code	Arguments
Con: Call Host	GCONCALL	Host name
Con: Disconnect Host	GCONHNGUP	Host name
Con: Connection lost	*CONLOST	Host name
Con: User authenticated	GCONUSER	(none)
Ses: Remote control started	GSESRC +	Host name

Session

Event Name	Event Code	Arguments
Ses: Remote control stopped	GSESRC -	Host name
Ses: File transfer started	GSESFXFER+	(none)
Ses: File transfer stopped	GSESFXFER-	(none)
Ses: Chat started	GSESCHAT +	(none)
Ses: Chat stopped	GSESCHAT -	(none)
Ses: Audio started	GSESAUDIO+	(none)
Ses: Audio stopped	GSESAUDIO-	(none)
Ses: Remote Management started	GSESRM +	Host name
Ses: Remote Management stopped	GSESRM -	Host name

Action

Event Name	Event Code	Arguments
Act: Help service start	GACTHLPSV+	(none)
Act: Help service stop	GACTHLPSV-	(none)
Act: Help request received	GACTHLPRQ+	Host name
Act: Help request canceled	GACTHLPRQ-	Host name
Act: File received	*ACTFILE +	File path and name
Act: File Sent	*ACTFILE -	File path and name
Act: Host Rebooted	*ACTBOOT	Host name
Act: Session recording started	GACTREC +	Recording file path and name
Act: Session recording stopped	GACTREC -	Recording file path and name
Act: Windows event logging failed	*ACTWIN !	(none)
Act: SNMP trapping failed	*ACTSNMP !	(none)
Act: Received Clipboard	*ACTCLPB +	(none)
Act: Sent Clipboard	*ACTCLPB -	(none)
Act: Received Print Job	*ACTPRINT+	(none)
Act: Sent Print Job	*ACTPRINT-	(none)
Act: Communication Profile Started	GACTCOMPR+	Communication profile name
Act: Communication Profile Stopped	GACTCOMPR-	[Communication profile name]
Act: Inventory received	GACTINV	Host name
Act: Message sent	GACTMSG	Host name

Security

Event Name	Event Code	Arguments
Sec: Password rejected	*SECPW!	Host name
Sec: Confirm access granted	*SECCA (10 characters, 4 blank spaces at the end)	Host name
Sec: Confirm access denied	*SECCA !	Host name
Sec: Security Server logon	GSECACSRV+	Logon name
Sec: Security Server logoff	GSECACSRV-	(none)

Configuration

Event Name	Event Code	Arguments
Cfg: Help service name defined	GCFGHLPSV+	Help service name
Cfg: Help service name deleted	GCFGHLPSV-	Help service name
Cfg: Local logging turned on	*CFGLLOC +	Log file name
Cfg: Local logging turned off	*CFGLLOC -	Log file name
Cfg: Local logging filename changed	*CFGLFILE*	New log file name
Cfg: Server logging turned on	*CFGLSRV +	Log server name
Cfg: Server logging turned off	*CFGLSRV -	Log server name
Cfg: Windows event logging turned on	*CFGLWIN +	If remote: computer name
Cfg: Windows event logging turned off	*CFGLWIN -	If remote: computer name
Cfg: Sending SNMP traps turned on	*CFGLSNMP+	(none)
Cfg: Sending SNMP traps turned off	*CFGLSNMP-	(none)
Cfg: Security Server password changed	GCFGACPW*	Impero Guest ID
Cfg: Web update check	*CFGWUCHK	Old build, new build, [timeout error]
Cfg: Web update download	*CFGWUDL	File name, [timeout error]
Cfg: Web update install	*CFGWUINST	(none)
Cfg: Web update success	*CFGWU *	Old build, new build
Cfg: Web update failed	*CFGWU !	Old build, error message

5.1.14.2 Available Impero log event codes and arguments - Host

The Host or extended Host can log the following Impero log events:

Connection

Event Name	Event Code	Arguments
Con: Host started	HCON +	(none)
Con: Host stopped	HCON -	(none)
Con: Callback	HCONCALLB	Callback number
Con: Connection lost	*CONLOST	(none)
Con: Name Server started	HCONNNS +	(none)
Con: Name Server stopped	HCONNNS -	(none)
Con: Security Server started	HCONNSS +	(none)

Con: Security Server stopped	HCONNSS -	(none)
Con: Gateway started	HCONGW +	(none)
Con: Gateway stopped	HCONGW -	(none)

Session

Event Name	Event Code	Arguments
Ses: Session started	HSES +	Guest name
Ses: Session stopped	HSES -	Guest name
Ses: Remote control started	HSESRC +	Guest name
Ses: Remote control stopped	SESRC -	Guest name
Ses: File transfer started	HSESFXFER+	Guest name
Ses: File transfer stopped	HSESFXFER-	Guest name
Ses: Chat started	HSESCHAT +	Guest name
Ses: Chat stopped	HSESCHAT -	Guest name
Ses: Audio started	HSESAUDIO+	Guest name
Ses: Audio stopped	HSESAUDIO-	Guest name
Ses: Remote Management started	HSESRM +	Guest name
Ses: Remote Management stopped	HSESRM -	Guest name
Ses: Maintenance password for confirm access wrong. Guest access denied	SESACCTR!	Guest name
Ses: Maintenance password for confirm access ok. Guest allowed access	SESACCTR	Guest name

Action

Event Name	Event Code	Arguments
Act: Help request sent	HACTHLPRQ+	Help service name, problem description
Act: Help request canceled	HACTHLPRQ-	(none)
Act: File received	*ACTFILE +	File path and name
Act: File sent	*ACTFILE -	File path and name
Act: Host reboot	*ACTBOOT	(none)
Act: Run Program	HACTRUN	Program name
Act: Execute Command	HACTEXE	Command name
Act: Windows event logging failed	*ACTWIN !	(none)
Act: SNMP trapping failed	*ACTSNMP !	(none)
Act: Received clipboard	*ACTCLPB +	(none)
Act: Sent clipboard	*ACTCLPB -	(none)
Act: Received print job	*ACTPRINT +	(none)
Act: Sent print job	*ACTPRINT -	(none)

Act: Keyboard and mouse assigned	HACTKBDMS+	Guest name
Act: Keyboard and mouse revoked	HACTKBDMS-	Guest name
Act: Keyboard locked	HACTKBD -	(none)
Act: Keyboard unlocked	HACTKBD +	(none)
Act: Screen blanked	HACTSCR -	(none)
Act: Screen unblanked	HACTSCR +	(none)
Act: Host user logged off	HACTLOFF	(none)
Act: Gateway logon	HACTGW +	Connecting module name
Act: Inventory sent	HACTINV	Guest name
Act: Message received	HACTMSG	Guest name

Security

Event Name	Event Code	Arguments
Sec: Individual security enabled or changed	HSECINDIV+	Guest access method
Sec: Individual security disabled	HSECINDIV-	Guest access method
Sec: Security role added	HSECROLE +	Security role name
Sec: Security role deleted	HSECROLE -	Security role name
Sec: Security role changed	HSECROLE *	Security role name
Sec: Guest added to role	HSECGUEST+	Guest name
Sec: Guest deleted from role	HSECGUEST-	Guest name
Sec: Guest changed in role	HSECGUEST*	Guest name
Sec: Password enabled	HSECPW +	If individual: Guest name
Sec: Password disabled	HSECPW -	If individual: Guest name
Sec: Password changed	HSECPW *	If individual: Guest name
Sec: Callback enabled (default only)	HSECCALLB+	(none)
Sec: Callback disabled (default only)	HSECCALLB-	(none)
Sec: Callback changed (default only)	HSECCALLB*	(none)
Sec: Confirm access enabled	HSECCA +	If individual: security role name
Sec: Confirm access disabled	HSECCA -	If individual: security role name
Sec: Password rejected	*SECPW!	Guest name
Sec: Confirm access granted	*SECCA (10 characters, 4 blank spaces at the end)	(none)
Sec: Confirm access denied	*SECCA !	(none)
Sec: Illegal password limit reached	HSECPWLIM	(none)
Sec: Timeout limit exceeded	HSECTMOUT	AC (inactivity), AU (authentication) or CA (confirm access)

Configuration

Event Name	Event Code	Arguments
Cfg: Local logging started	*CFGLLOC +	Log file name
Cfg: Local logging stopped	*CFGLLOC -	Log file name
Cfg: Local logging filename changed	*CFGLFILE*	New log file name
Cfg: Server logging started	*CFGLSRV +	Log server name
Cfg: Server logging stopped	*CFGLSRV -	Log server name
Cfg: Windows event logging started	CFGLWIN +	If remote: computer name
Cfg: Windows event logging stopped	*CFGLWIN -	If remote: computer name
Cfg: Sending SNMP traps started	*CFGLSNMP+	(none)
Cfg: Sending SNMP traps stopped	*CFGLSNMP-	(none)
Cfg: Option change: Start at load	HCFGOWAIT*	ON/OFF
Cfg: Option change: Load with OS	HCFGOLOAD*	ON/OFF
Cfg: Option change: Minimize at startup	HCFGOMIST*	ON/OFF
Cfg: Option change: Stealth mode	HCFGOSTLT*	ON/OFF
Cfg: Option change: Minimize on connection	HCFGOMICO*	ON/OFF
Cfg: Option change: On top	HCFGOTOP *	ON/OFF
Cfg: Option change: Show file transfer	HCFGOSFX *	ON/OFF
Cfg: Option change: Send keep alive	HCFGOALIV*	ON/OFF
Cfg: Option selected: Boot after disconnect	HCFGOBOOT+	(none)
Cfg: Option selected: Logoff after disconnect	HCFGOLOGO+	(none)
Cfg: Option selected: Lock after disconnect	HCFGOLOCK+	(none)
Cfg: Option selected: Nothing after disconnect	HCFGONOTH+	(none)
Cfg: Option change: Naming method	HCFGONAME*	(none)
Cfg: Option change: Public Host name	HCFGOPUBN*	ON/OFF
Cfg: Option change: Enable user name	HCFGOUSRN*	ON/OFF
Cfg: Option change: Connec-	HCFGONOTI *	(none)

tion notification		
Cfg: Option change: Help Request description	HCFGOHRD *	(none)
Cfg: Option change: Help Request provider	HCFGOHRP *	(none)
Cfg: Option change: Help Request communication	HCFGOHRC *	(none)
Cfg: Option change: Help Request phone/IP	HCFGOHRPI *	(none)
Cfg: Option change: Help Request show icon	HCFGOHRSI *	ON/OFF
Cfg: Option change: Audio full duplex	HCFGOAUFD*	ON/OFF
Cfg: Option change: Audio silence level	HCFGOAUSL*	(none)
Cfg: Option change: Audio line hold	HCFGOAULH*	(none)
Cfg: Option change: Name space ID	HCFGONSID*	(none)
Cfg: Maintenance requiry changed for Guest	HCFGMRQG*	(none)
Cfg: Maintenance requiry changed for Gateway	HCFGMRQGW*	(none)
Cfg: Maintenance requiry changed for other	HCFGMRQO *	(none)
Cfg: Maintenance requiry changed for exit/stop	HCFGMRQEX*	(none)
Cfg: Protect files changed	HCFGPROTS*	(none)
Cfg: Maintenance password changed	HCFGMTPW *	(none)
Cfg: Guest access allow to changed (default only)	HCFGGALLW*	(none)
Cfg: MAC/IP address list changed	HCFGMACIP*	(none)
Cfg: File transfer disable changed	HCFGFX *	(none)
Cfg: Security Server group ID changed	HCFGSSG *	(none)
Cfg: Web update check	*CFGWUCHK	Old build, new build, [timeout error]
Cfg: Web update download	*CFGWUDL	File name, [timeout error]
Cfg: Web update install	*CFGWUINST	(none)
Cfg: Web update success	*CFGWU *	Old build, new build
Cfg: Web update failed	*CFGWU !	Old build, error message
Cfg: Maintenance password for confirm access enabled	HCFGACCTR+	(none)
Cfg: Maintenance password for confirm access disabled	HCFGACCTR-	(none)

Gateway can log these **Impero** log special **Gateway** events:

Event Name	Event Code	Arguments
GW Gateway access allowed	HGWACCES+	(none)
GW Gateway callback	HGWCALLB	Callback number
GW Gateway callback changed (default only)	HGWCALLB*	(none)
GW Gateway callback disabled (default only)	HGWCALLB-	(none)
GW Gateway callback enabled (default only)	HGWCALLB+	(none)
GW Gateway group defined	HGWGROUP+	Security role name
GW Gateway group deleted	HGWGROUP-	Security role name
GW Gateway Guest added	HGWGUEST+	Guest name
GW Gateway Guest changed	HGWGUEST*	Guest name
GW Gateway Guest deleted	HGWGUEST-	Guest name
GW Gateway individual security disabled	HGWINSEC-	(none)
GW Gateway individual security enabled (or changed)	HGWINSEC+	(none)
GW Gateway NSS GID changed	HGWSSGID*	(none)
GW Gateway password changed (default only)	HGWPW*	(none)
GW Gateway password disabled (default only)	HGWPW-	(none)
GW Gateway password enabled (default only)	HGWPW+	(none)
GW Gateway password rejected	*SECGWPW!	Connecting module name

5.1.15 Impero File Manager Options

Use the **Options** dialog box to set up how file transfer should work.

You can set up synchronization options, general transfer options, options for display of confirmation dialog boxes in relation to deleting/overwriting files during file transfer, **File Manager** layout options, and options for logging during file transfer.

Transfer tab

Synchronize

Option	Description
Transfer only if file ex-	Select this check box to synchronize files only if they exist in the

ists	unselected pane.
Transfer only one way	Select this check box to synchronize files only from the selected pane to the unselected pane.

General Transfer

Option	Description
Include subfolders	Select this check box to transfer also the contents of subfolders of selected folders.
Use delta file transfer	Select this check box to compare source files with corresponding destination files and transfer only differences between source and destination files. This saves transmission bandwidth.
Enable crash recovery	Select this check box to transfer files so that they can be recovered after a computer or network crash during file transfer.
Close dialog when finished	Select this check box to close the **Transfer Status** window when a file transfer is finished.
End session when finished	Select this check box to end the file transfer session when a file transfer is finished.

Confirmation tab

Confirm when...

Option	Description
Delete non-empty folders	Select this check box to display a confirmation dialog box if you are about to delete a folder containing folders or files. The confirmation dialog box allows you the following choices with regard to the deletion: • **Skip**: Click on this button to skip deleting the specified folder. • **Delete**: Click on this button to delete the specified folder. • **Advanced**: Click on this button to change your delete confirmation selections for this file transfer only. • **Cancel**: Click on this button to cancel the file transfer at this point. You cannot undo executed file transfer actions.
Overwriting/deleting	Select this check box to display a confirmation dialog box if you

files	are about to overwrite or delete files. The confirmation dialog box allows you the following choices with regard to the overwriting/deletion: • Skip: Click on this button to skip overwriting the specified file. • Overwrite: Click on this button to overwrite the specified file. • Advanced: Click on this button to change your overwriting confirmation selections for this file transfer only.
Overwriting/deleting read-only files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete read-only files.
Overwriting/deleting hidden files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete hidden files.
Overwriting/deleting system files	Select this check box to display a confirmation dialog box if you are about to overwrite/delete system files.
Drag and drop (copying files with the mouse)	Select this check box to display a confirmation dialog box before executing a drag and drop file transfer.

Layout tab

Screen

Option	Description
Show toolbar	Select this check box to display the toolbar of the File Manager window.
Show status bar	Select this check box to display a status bar at the bottom of the two panes in the File Manager window.
Save session path at exit	Select this check box to display the same pane contents when starting a file transfer session with the same Host the next time. Uncheck it to always display the system drive contents when starting a file transfer session.

Keyboard

Option	Description
Use system hotkey layout	Select this option to use the operating system hotkey layout, see the table below.
Use Impero hotkey	Select this option to use the Impero hotkey layout, see the table

layout	below.

Function	Windows hotkey	Impero hotkey
Copy Files		F3
Move Files		F6
New Folder		F7
Delete	DELETE	F8
Rename	F2	
Close	ALT+F4	F10
Properties	ALT+ENTER	SHIFT+F1
Select All	CTRL+A	
Select by		+
Deselect by		-
Invert selection		*
Arrange Icons By Name		CTRL+F3
Arrange Icons By Type		CTRL+F4
Arrange Icons By Size		CTRL+F6
Arrange Icons By Date		CTRL+F5
Refresh	F5	CTRL+R
Select the left record panel		ALT+F1
Select the right record panel		ALT+F2
Help	F1	F1

Icons

Option	Description
Local associated and Host 'exe' icons	Display file icons in the **File Manager** window panes according to **Guest** file associations, but display Host exe file icons according to **Host** file associations.
Local associated icons	Display file icons in the **File Manager** window panes according to **Guest** file associations. This saves transmission bandwidth.
Default icons	Display the same default icon for all files in the **File Manager** window panes. This saves transmission bandwidth and processor capacity.

Logging tab

Option	Description
Generate log file	Select this check box to generate a file transfer log file when ending a file transfer session.
Append if log file exists	Select this check box to append new log entries to an existing log file. If you do not select it, any existing log file is overwritten.
Filename	This field specifies the log file (path and) name. The default name is `NFM.LOG`. The file is located in the Impero configuration files folder, typically `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest`. Click on the **Browse** button to specify another log file path and name.

See also

Transfer files

5.1.16 Modem

Use the **Modem** dialog box to manage the modem database.

NOTE: The modem database is stored in the Impero configuration file modems.ndb, which is typically located in the directory:

- `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for the **Guest**.
- `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>` for **Host**-based modules.

In the **Modem List** the first _Modem Database YYYYDDD record specifies the modem database update year and day number. You can download and install the newest available update from the Impero Knowledge Base, see the Download Updates subsection.

NOTE: Downloading and installing **`modems.ndb`** overwrites your current **`modems.ndb`**.

Other records represent modem configurations created by Impero Support or added by a user.

You can create, edit and delete modem configurations using the buttons at the bottom of the dialog box.

To base a new modem configuration on an available modem configuration, select the modem configuration in the pane before clicking on the **New** button.

See also

Modem Configuration

5.1.17 Modem Configuration

Use the **Modem Configuration** dialog box to create or edit a modem configuration in the modem database.

With some modem configurations, some or all fields are disabled to protect the original modem configuration. If you select a modem configuration in the **Modem** dialog box and click on **New**, the properties of the selected modem configuration are displayed in the **Modem Configuration** dialog box with all fields enabled.

The **Name** field contains the modem configuration name, which must be unique within the modem database. You can edit the field contents.

Modem command strings

These fields specify the modem AT command strings. Consult with your modem manual or the modem manufacturer website to find the AT command strings required by your modem.

Max data rate

In the Max data rate drop-down list, select a data rate applicable to your modem and the modem you want to connect to.

Settings

Option	Description
RTS/CTS Flow control	Select this check box to use Return To Send/Clear To Send flow control.
Ignore carrier signal	Normally, no carrier signal indicates an error. However, in some

	situations there may not be any carrier signal, without this being an error. Select this check box to not wait for a carrier signal.

See also

Modem

5.1.18 Novell Network Numbers

Unless a network list is created, the IPX communication reaches only the Impero modules on the local network. You can extend the communication to remote networks.

In the **Novell Network Numbers** dialog box you can add, edit, and delete network numbers using the buttons on the right side of the network list.

The pane displays the 8-digit hexadecimal network numbers of the selected remote networks.

See also

Communication Profile Edit

5.1.19 Program Options

Layout tab

Use the **Layout** tab to specify layout options for the **Guest** window.

Enable

Option	Description
Tool bar	Clear the selection of this check box to remove the toolbar.
Status line	Clear the selection of this check box to remove the status bar.
Menu hints	Clear the selection of this check box to disable the display of menu command and toolbar button hints in the status bar.
Add Guest icon to tray	Clear the selection of this check box to display no **Guest**

	icon in the notification area in the lower right screen corner when the Guest is loaded.
Hide Guest from taskbar when minimized	This option is only available if the **Add Guest icon to tray** check box is selected. Clear the selection of this check box to display the minimized Guest as an icon in the taskbar at the bottom of the screen. If selected, the minimized Guest is displayed only as a Guest icon in the notification area in the lower right corner of the screen.
Save Guest minimize state on exit	Select this check box to load the Guest minimized if minimized when the Guest last unloaded.
Stealth mode (hide Guest when started)	Select this check box to load the Guest hidden to the computer user. To uncover the Guest when loaded in stealth mode, execute **`showgst.exe`**, which is located in the directory in which the Guest was installed.

Use the Menu and Toolbar Theme list to select color theme for the menu and toolbar.

Tab layout

Use the Tab layout option to enable/disable tab panel tabs and rearrange the order of the tabs.

The pane contains a list of available tab panel tab names.

Remove the selection of a check box to remove the tab in question from the tab panel.

The order of the tab names in the pane from top to bottom controls the order of the tab panel from left to right. Select a tab name and click on one of the Up/Down buttons to move it.

NOTE: For the changes to take effect, make sure to restart the Guest.

General tab

Use the General tab to specify general connect options.

Option	Description

<table>
<tr><td>Host session default mode</td><td colspan="2">Select a session to start when connecting to a Host. Remote control is the default session.</td></tr>
<tr><td>Inactivity</td><td colspan="2">In the Inactivity timeout field, specify a number of minutes after which to disconnect if there has been no Guest user keyboard or mouse activity within the specified number of minutes (default: 0, range 0-999).</td></tr>
<tr><td>Keep Alive</td><td colspan="2">Select the Send keep alive message check box to send a data packet at intervals while connected to alert the Guest if the connection is lost.

NOTE: To maintain an ISDN (CAPI) connection during short periods of inactivity, select the Short-hold mode check box in the Edit dialog box for the ISDN (CAPI) communication profile.</td></tr>
<tr><td>Confirm when</td><td colspan="2">Select the Exiting Guest while connected check box to display a warning if you attempt to unload the Guest while being connected to a Host. You are prompted to confirm if you want to unload the Guest anyway.</td></tr>
<tr><td rowspan="3">Connection</td><td><b>Option</b></td><td><b>Description</b></td></tr>
<tr><td>Connection attempts</td><td>Specify a number of connection attempts in the range 1-999 that the Guest should automatically make to connect to a Host.</td></tr>
<tr><td>Auto reconnect</td><td>In the list, select the reconnect option that should apply if a connection is lost:
• Never: Never reconnect.
• Abnormal disconnect only: Reconnect only if the connection is lost by an abnormal event.
• Host disconnect only: Reconnect only if the Host disconnected.
• Always: Always reconnect.</td></tr>
<tr><td rowspan="2">Impero Portal settings</td><td>Certificate...</td><td>You can modify the following options:
• Connection allowed when using an invalid certificate
• Display invalid certificate warning (enabled by default)</td></tr>
<tr><td>Proxy...</td><td>By default, no proxy is used when initializing the Portal communication profile. This setting can be changed, to either attempt to detect and use the current proxy settings of the system.
Available options:
• no proxy
• use system proxy settings (enabled by default); when enabled, it automatically detects the proxy configuration of the system from the Internet Options</td></tr>
</table>

		- use custom proxy settings NOTE: It is necessary that you specify at least the address (IP/DNS name) and port.

Cache tab

Use the Cache tab to specify disk cache options for the remote control screen image.

When the Guest remote controls a Host in command mode, the Guest stores the Host screen image in disk cache memory to transfer only image changes. This speeds up Host screen image update and saves transmission bandwidth.

Host screen command transfer disk cache

Option	Description
Use separate cache file for each Host	Select this option to reserve a disk cache section for each connected and disconnected Host. If you connect to many different Hosts, a large total disk cache size is required to achieve high update and reconnect speed.
Use shared cache file for all Hosts	Select this option to share the available disk cache among connected and disconnected Hosts. Total disk cache size demand is typically lower.
Don’t save cache between sessions	Select this option to share the available disk cache only among connected Hosts. Total disk cache demand is lowest, but reconnects are slower.
Limit total disk cache size to	In this field, specify a disk cache size in the range 200 - 64000 (default: 10000). The number should typically be larger than default if you regularly run command mode remote control sessions with many different Hosts.

Logon tab

Use the Logon tab to specify Guest logon and name options.

Guest ID

The contents of the Guest ID field specify the name by which the Guest identifies itself when communicating (default: computer name).

You can edit the field content.

If the field is empty, the Guest identifies itself by its computer address, typically IP address or network card MAC address.

NOTE: If the Guest runs on a network computer, we recommend naming it by its computer name. If the Guest runs on a terminal server client, we recommend naming it by its user logon name. See the Administrator's Guide, Advanced Tools, Impero Naming in a TSE.

Authentication

Select the Cache logon passwords check box to store the most recently used logon credentials in cache memory and apply them when connecting.

Cached logon credentials are lost when the Guest is unloaded.

Access Server 6.x/5.x

Option	Description
Use Access Server on Guest side	Select this check box to enable Guest side authentication with Hosts that are Guest side authentication enabled on an older version of Access Server. NOTE: Security Server (version 7+ only) does not support Guest side authentication.
Ignore if access to Host cannot be authenticated	Select this check box to ignore Guest side authentication with Hosts that are not Guest side authentication enabled on a Access Server.

Host Name tab

Use the Host Name tab to specify Host name.

Default Host name qualifier

Impero interprets a name specified in the Quick Connect tab, in the Host section Name field as a certain type of name according to this default Host name qualifier or a prefixed Host name qualifier (shown in parentheses below).

Option	Description
Host ID (H::)	Interprets a **Host** name without a prefix as a Host ID.
User name (U::)	Interprets a **Host** name without a prefix as a user name.
DNS name (DNS::)	Interprets a **Host** name without a prefix as a Domain Name Server name.
LDAP name (LDAP::)	Interprets a **Host** name without a prefix as a directory services user attribute value. See Directory Services tab.

Duplicate names

If connecting by a networking communication device, multiple **Hosts** may respond by the same name, for instance if the same user is logged on to multiple computers. By default, the **Guest** connects to the first responding **Host**.

Select the **Check for duplicate names before connecting** check box to wait a few seconds for **Host** responses and display a **Multiple Host Names found** window if multiple Hosts respond. The window prompts you to select a **Host**.

See also

Communication Profile Edit
Administrator's Guide, Impero Name Management.

Directory Services tab

Use the **Directory Services** tab to specify directory services to enable the **Guest** to connect to and browse for **Hosts** using the LDAP:: Host name qualifier.

General

Option	Description
Directory Server	Specify the directory server IP address or DNS name.
Port	Specify the port through which to connect to the directory server (default: 389, the Lightweight Directory Access Protocol (LDAP) port). Select the **Use secure connection** check box to connect to the directory server by a secure connection. The LDAP secure connection port number is 636.

Base DN	Specify the directory services distinguished name from which a search should start.

Credentials tab

Specify the credentials by which the **Guest** should log on to the directory server. The credentials determine the user rights by which directory services information is available.

Option	Description
Anonymous bind	Select this check box to search the directory service with anonymous user rights. Clear the selection to enable the fields below.
User DN	Specify a directory service user distinguished name to search the directory service with the rights of this user. Make sure to specify the corresponding password.

Settings tab

Specify the settings for searching directory services for user attribute values to return corresponding name and address attribute values.

For guidance on filling in the **User search filter** and **User attribute** fields, click on the **Default** button to display the **Display Directory Service** dialog box. Select a directory service name in the list of available directory services and click on **OK**.

Selecting a directory service, for example Active Directory, populates the User search filter and User attribute fields with default values for the selected directory service. You can edit the values if you have customized your directory service and require different values.

Attributes

Option	Description
Name attribute	Specify or edit the name attribute.
Address attribute	Specify or edit the address attribute designation.
Search name prefix	Specify or edit any prefix (e.g. cn=) that should be added before search values.

Remote Control tab

Use the Remote Control tab to specify general remote control session options.

NOTE: You can specify individual remote control session options for each Host connection in the Connection Properties dialog box, which you can access either by clicking the Connection Properties dialog box on the Quick Connect tab, or in a running remote control session, by clicking on the Connection Properties button from the toolbar.

Enable

Option	Description
Toolbar	Select this check box to display the Remote Control window toolbar.
Toolbox in full screen	Select this check box to display the Remote Control full screen display toolbox.
Full screen toolbox roll-up	Select this check box to reduce the Remote Control full screen display toolbox to the corresponding title bar when not in use.
Status line	Select this check box to display the Remote Control window status bar.

Hot keys assignment

You can assign hotkeys (keystroke combinations) to specified actions. By default, **CTRL +Z** is assigned to Zoom in and out (switch between Remote Control window and full screen). Assign desired hotkeys by selecting check boxes and specifying a character in the last field.

Remote control window

Option	Description
Host window auto scroll	Select this check box to enable automatic Host screen image scroll when the mouse pointer approaches Remote Control window borders.
Show full screen as topmost window	Select this check box to display the Remote Control full screen display in front of any other window.
Show full screen on all monitors	Select this check box to display the Remote Control full screen display on all available monitors.

Auto take control	Select this check box to enable acquiring multi **Guest** session keyboard and mouse control by a keystroke or mouse click.
Switch to window mode password	Specify a password that should be requested to switch from full screen to window. The field displays password characters as dots or asterisks.
Disconnect password	Specify a password that should be requested to disconnect. The field displays the password characters as dots or asterisks.

Clipboard tab

Use the **Clipboard** tab to specify remote control clipboard transfer options.

Automatic clipboard transfer

Option	Description
Automatically transfer clipboards below	Select this check box to enable contents placed on the **Guest** computer or **Host** computer clipboard during a remote control session to automatically become the clipboard contents of both computers if smaller than the number of kilobytes specified in the field.
Show progress dialog during transfer	Select this check box to display a small window with a progress bar while clipboard contents are being transferred from one computer to the other.

Monitor tab

Use the **Monitor** tab to specify monitor options.

Option	Description
Monitor interval	Specify a number of seconds in the range 1-999 after which to switch to the next **Host** after monitoring a **Host** (default: 15).
Start Monitor in full screen	Select this check box to initially display monitored **Host** screen images in full screen mode. If unchecked, **Host** screen images are initially shown in window mode.

Audio-Video Chat tab

Use the **Audio-Video Chat** tab to specify audio and video chat options.

Audio-video chat settings

Option	Description
Start audio chat when conference is started	Select this check box to enable sound transfer at session start.
Start video when conference is started	Select this check box to enable image transfer at session start.

Audio Chat

Select the **Enable full-duplex audio** check box to enable sound transfer in both directions at the same time.

NOTE: Some computer sound systems do not support full-duplex audio.

Microphone sensitivity

Option	Description
Silence level	Drag the slider bar to specify the microphone sound input level below which no sound data should be transferred.
Line hold	Drag the slider bar to specify the time period in which sound data should continue to be transferred after the microphone sound input level has dropped below the silence level. TIP: Try out different Silence level and Line hold settings to optimize sound transfer.
Check sound system	Click on this button to check the computer sound system. A result message is displayed.
Advanced	Click on this button to display the **Advanced audio settings** dialog box. See Advanced audio settings.

Video

Option	Description
Capture size	Select a video capture frame size on the list. The size is displayed in pixels

	(default: 160 x 120).
Advanced	Click on this button to display the **Advanced Video** dialog box. See Advanced Video.

Remote Printing tab

Use the **Remote Printing** tab to specify remote **Impero** printers and incoming print job redirection.

Remote Impero printers

You can add an **Impero** printer on the **Guest** computer to enable sending a **Guest** computer print job to a **Host** computer printing device (remote printer).

Click on the **Add printer** button and following the instructions in the displayed **Add printer guidelines** window. Click on the **Ready** button to start adding a **Impero** printer.

The **Remote Impero printers** pane displays the names of **Impero** printers in the Windows Printers folder on the **Guest** computer.

NOTE: You can also add an **Impero** printer on a **Host** computer to enable sending a **Host** computer print job to a **Guest** computer printing device. You can remove a **Impero** printer by selecting the printer in the pane and clicking on the **Remove printer** button.

If you are connected to multiple **Hosts** while sending a print job to a **Impero** printer, a dialog box prompting you to select the **Host** to which you want to send the print job is displayed.

NOTE: Special instructions for remote printing from DOS applications are available in the Impero Knowledge Base.

Redirect print to

You can redirect a print job sent from the **Host** computer to the **Guest** computer to any printer specified on the **Guest** computer.

Option	Description
Default printer	Select this option to redirect the print job to the default **Guest** computer printer.
Prompt with a list of available printers	Select this option and click on **Browse** to display the **Select Print Redirection Printer** dialog box. **From the Select**

	Print Redirection Printer dialog box, you can select a printer from a list of available printers.

See also

Send a print job to a remote printer

Recording tab

Use the **Recording** tab to specify remote control session recording options.

Options

Option	Description
Use compatible mode	Remote control session recording was improved in **Impero Connect** version 8. Older **Guest** versions cannot play back version 8+ recordings. Select this check box to make older version compatible recordings.
Enforce recording	Select this check box to record all remote control sessions even if the Record remote control session check box is not selected (**Connection Properties** > **Record** tab).
Disconnect if recording fails	Select this check box to disconnect if recording a remote control session fails.

Recording

A **Recordings** tab record and recording file name will identify the remote control session **Guest**. Select one of these identity options:

Option	Description
Guest ID	Identify by the Guest ID. See **Logon** tab for further information.
Guest user	Identify by the **Guest** computer Windows or network logon user name.

See also

Record sessions

Sounds tab

Use the **Sounds** tab to specify sounds played upon selected events.

Select an event check box to play a sound upon the event. Clear the selection to suppress playing a sound upon the event.

Select an event and click on **Select Sound** to open a sound file with the extension `*.wav` to replace the current sound. The event is marked with an asterisk (*). Select an event marked (*) and click on **Default Sound** to reassign the default sound to the event and remove the (*) mark.

If you want to listen to the sound while editing the sound settings, select an event and click on **Play** to play the sound assigned to the event.

Help Request tab

Use the **Help Request** tab to set up use of help request.

Select the **Enable help request** check box to enable the **Guest** to receive help requests.

Click on the **Advanced** button to display the **Advanced Help Service** dialog box allowing you to specify actions that are to be executed when a help request arrives. See Advanced Help Service.

Help Service tab

The **Guest** can receive **Host** help requests only if the **Enable help request** and **Enable help services** check boxes are selected, at least one Help service name is specified and communication profiles are enabled at **Guest** loading.

The **Host** uses the term help provider for a help service name.

Option	Description
Enable help services	Select this check box to enable the help services specified below.
Help service 1-3	In these fields, specify the names of the help services that this **Guest** is to offer.

Service Ticket tab

The extended **Guest** also has a **Service Tickets** tab that enables it to service help requests by service ticket numbers. Service tickets are used for both **Connect** and **OnDemand** (1.74 and earlier versions).

Option	Description

Enable service tickets	Select this check box to enable the use of service tickets to service help requests through a service ticket number.
Service ticket format	Enter a service ticket format using any character plus the control characters #, @, and * (# produces a number (0-9), @ produces a letter (A-Z) and * produces a number or a letter (0-9, A-Z)), for example @##-****. The service ticket generated from this can only be used once, after which a new ticket is generated.
Number of auto generated service tickets	Enter the number (0-3, 0 = manually) of service tickets to be auto-generated.

WebConnect tab

The extended **Guest** also has a **WebConnect** tab that enables it to service help requests by **WebConnect** tickets. **WebConnect** tickets are used for **OnDemand** 2.0 and later versions.

Option	Description
Enable WebConnect tickets	Select this check box to enable use of **WebConnect** tickets.
WebConnect ticket	Enter anything that you want to use as a **WebConnect** ticket for identification purposes during a **OnDemand** remote control session using **WebConnect**, for example an email address, a name, or a keyword, for example **Security Server**.
WebConnect profile	Select a **WebConnect** profile in the list. The **WebConnect** profile contains the credentials and the **Connection Manager URL** to be used for the **WebConnect** connection. The profile itself should be defined in the **Setup Wizard** before you can select it here. You can also set up the profile in **Communication Profiles**. One or more **WebConnect** profiles can be defined in **Communication Profiles**. See Communication Profile Edit for more information.
Update interval	Enter an interval in seconds to specify how often the **Guest** should communicate with **WebConnect** and check for new

	tickets.

See also

Set up Help Request on Guest and Host

Run tab

Use the **Run** tab to specify programs to include in the **Run Program** drop-down menu on the **Guest** window and **Remote Control** window toolbars.

The pane displays specified programs as records in a table with a description and the program file path and name.

NOTE: Table contents are stored in the runprog.ndb **Impero** configuration file: `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Guest`.

Click on the **Add** button to add a program to the pane. The **Run** dialog box in which you can specify a program to run is displayed. See Run.

To see the properties of a record in the pane, select the record and click on the **Properties** button. The **Run** dialog box is displayed, and you can edit the properties specified.

To delete a record again, select it in the pane and click on the **Delete** button.

See also

Run a program on one or multiple Hosts

Encryption tab

Use the **Encryption** tab to enable encryption types.

The communication between **Impero** modules is protected by encrypting transmitted data.

A range of encryption types is available on **Connect** modules.

Communicating **Impero** modules automatically negotiate to encrypt communication by an encryption type that is enabled on both modules. See Connection Properties (**Compression/Encryption** tab). **Impero** modules on which no common encryption type is enabled cannot communicate.

Select the check boxes next to the various encryption types to enable them.

To see encryption details about the individual encryption types, select an encryption type and click on the **Show Details** button.

Inventory tab

Use the **Inventory** tab to specify what inventories should contain and how the contents should be displayed in the **Guest** window Inventory tab.

Summary view

The pane contains a list of available inventory details. Select the check boxes to specify the inventory details of the **Guest** window Inventory tab summary, which is displayed in the details pane on the right when a folder is selected in the contents pane on the left.

The pane top-to-bottom order of selected inventory details determines the left-to-right order of details pane columns.

Use the Up/Down, **Select All**, **Deselect All** buttons to arrange the contents of the pane.

Click on the **Advanced** button to specify inventory processing and custom inventory items. The **Advanced inventory** option dialog box is displayed. See Advanced inventory option.

See also

Generate a Host inventory

Smart Card tab

Use the **Smart Card** tab to specify the **Smart Card** reader whose reading applies to the **Smart Card** authentication.

Smart Card Reader

Option	Description
Select Smart Card reader	In the drop-down list, select the **Smart Card** reader that you want to use. The list contains Default and the names of connected **Smart Card** readers found by Windows.
Support Remote Smart Card Logon	Select this check box to enable remote **Smart Card** logon. This means that using a local **Smart Card** reader you can log directly into remote enterprise and application systems using a **Smart Card** for authentication and authorization.

Intel vPro tab

Use the Intel vPro tab to specify the address of the SCS Web Service.

Select the Connect to SCS check box and enter the SCS Web Service URL in the field below.

The address is then saved in the system, so that every time you select the Retrieve Intel vPro Enabled Computers from SCS command on the context menu for the Intel vPro tab pane on the Quick Connect tab, you aren't prompted to enter the address.

See also

Use Intel vPro from Impero Remote Control

Skins tab

If you run a remote control session, skins enable you to see the Host device and execute commands on the Host device by clicking the buttons on the applied skin. A device may have more than one skin definition depending on its state, for example slide out keyboard, portrait and landscape orientation etc. Every time the device changes state, the Host sends updated skin information to the Guest.

If the Guest does not have the skin that is needed for a remote control session with a particular Host, it attempts to collect a suitable skin from the Skin Repository Server. If the necessary skin is not available, the Guest uses a default skin.

On the Skins tab, the address and port number of the **Skin Repository Server** are displayed.

Click on the View Models button if you want to see the available skin models.

Web Update tab

Use the Web Update tab to specify web update options to automatically update the Guest installation.

Option	Description
Update server	Specify the web address of the server from which to download Guest update files (default: update.netop.com, the Impero manufacturer web update server). NOTE: To update many Impero installations in an organization, we recommend publishing new updates to an internal web update

	server (select **Publish New Updates** on the **Tools** menu).
HTTP Proxy	Specifying a HTTP proxy is typically not required. Before specifying a HTTP proxy, click on **Update now** to test the web update connection. If you receive a message indicating connection to the update server, specify no HTTP proxy. If **Update now** yields no connection, click on the **Detect** button to make **Impero** attempt to detect the HTTP proxy server and display its name and port number in the **HTTP Proxy** field. Click on **Update now** to test the connection. If unsuccessful, consult your network/system administrator about what to specify in the **HTTP Proxy** field (format: `<Server name>:<Port number>`).
Update now	Click on this button to connect to the update server specified in the **Update server** field. A web update message notifies you if the connection to the update server fails, if no updates are available or if updates are available, and in the latter case ask you if you want to download and install updates.
Schedule	Click on this button to display the **Web Update Schedule** dialog box and specify a schedule of checks for updates including download and installation of available update files.

5.1.20 Run

Use the **Run** dialog box to specify a program file to run using the **Run Program** function and how the program should start.

File

Type a descriptive text in the **Description** field. This text appears on the menu.

File name

Make sure that the Local file name option has been selected and then click on the **Browse** button to locate the program `.exe` file.

When the program file is added to the **Local file name** field, the global file name is automatically added to the **Global file name** field. The absolute path is replaced with environment variables. This is especially helpful if your computers are running different Windows platforms.

Example of a local file name and the corresponding global file name:

```
C:\Program Files\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
%ProgramFiles%\Adobe\Acrobat 6.0\Reader\AcroRd32.exe
```

TIP: Once you have added a program to the **Local file name** field and the global file name has been added automatically to the **Global file name** field, select the **Global file name** option, so that you do not have to consider which operating system version or operating system language **Host** computers are using.

If the selected program needs to be started using command line switches, use the **Command line switches** field to type those. This could for example be starting Internet Explorer with a specific address or for Adobe Acrobat Reader, the name of the document to read.

Run

Under **Run**, select **Normal**, **Maximized** or **Minimized** to define how the program should start when opened from the **Run Program** button in the toolbar or from the **Run Program** command on the **Connection** menu.

5.1.21 Script

A script is a user specified command structure that can execute a task, typically an unattended scheduled file transfer.

Use the **Script** dialog box to create and edit scripts in a graphical tree structure.

Option	Description
Filename	Specify a script file name. If you do not specify a file extension and a path, the script file gets the extension .dws and is located in the **Impero** configuration files folder, typically `C:\Users\<User name>\AppData\Roaming\Danware Data\C\Program Files (x86)\Netop\Netop Re-`

	`mote Control\Guest\script\.` If you create a new script, you are prompted for confirmation. Click on **Yes**. The **Global Settings** dialog box is then displayed.
Open Script	Click on this button to open a script file.
Comment	Enter a comment about the script. The comment is displayed in the **Comments** column in the **Script** tab (Optional).
Save Script	Click on the **Save Script** button to save a new or edited script.
Add	Click on the **Add** button to add a script command in the upper pane under the selected script command. See **Commands list** below.
Edit	Select a script command in the upper pane and click on the **Edit** button to display the corresponding editing window.
Run Script	Click on this button to run the script.
Delete	Select a script command in the upper pane and click on the **Delete** button to delete it, including the command sub tree under it.

Commands list

To specify the first command of a script, in the upper pane of the **Script** dialog box, select the **Global Settings** element and click on the **Add to display** a drop-down menu.

This menu contains script commands that can execute on the **Guest**:

Connect	Select the **Connect** command to add a **Connect** command, which connects to a **Host**.
Wait	Select the **Wait** command to add a **Wait** command, which delays script execution.
Run	Select the **Run** command to add a **Run** command.

A **Connect** command branches the script into commands that execute with or on the connected Host computer or in case of a local **Connect** command on the **Guest** computer.

In the upper pane, click on the **+** (plus) button next to a **Connect** command to expand it and select the expanded **Connect** command or a command below it.

Click on **Add** to display the following menu, which contains script commands that can execute with a connected **Host** or a **Guest** connected locally to itself:

Copy	Select one of these commands to display a <File transfer> dialog box and add a **File Transfer** command.
Move	
Synch	
Clone	
Delete	
Wait	Select this command to display the **Wait** dialog box and add a **Wait** command to delay script execution.
Run	Select this command to display the **Run Program** dialog box and add a **Run** command to execute a program on the connected to computer. You can schedule scripts to be ran from the **Guest** on the **Host** by using elevated privileges; select **Use a different account** and enter the credentials of a user with elevated privileges on the **Host** machine.
Logoff	Select one of these commands to add an **Action** command to execute an action on the connected to computer.
Restart	
Poweroff	
Lock	
Inventory	
Send Message	

See also

Create and run a script
Global Settings
Impero File Manager Options

5.1.22 Send Message

When you add a **Send Message** command to a script, the **Send Message** dialog box is displayed allowing you to specify how the message should be sent.

Option	Description
	Select a Send Message step option in the drop-down list:

	• **One Step**: Select this option to copy a message file on the **Guest** computer to the Messages directory on the **Host** computer and display it in a **Send Message** window on the **Host** computer screen. NOTE: Create and save the message file in the **Message** window. • **Display Message**: Select this option to display a message file located on the **Host** computer in the Messages directory in a Message window on the **Host** computer screen.
Message path	Specify the **Guest** computer (**One Step**) or **Host** computer (**Display Message**) path and name of the message file to (copy and) display. Click on the **Browse** button to open a message file on the **Guest** computer and display its path and name in the field. NOTE: The **Host** computer Messages directory, which is located in the **Impero** configuration files directory, typically `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Host\Messages`, is identified by the environment variable `%RootConfig%Messages`. To display in the Message window on the **Host** computer screen, the message file name must use the syntax `<Date>T<Time>;<Sender>.rtf` with the date format YYYY-MM-DD and the time format HH-MM-SS.

See also

Script
Create and run a script
Communicate with Host users

5.2 Host dialog boxes

5.2.1 Advanced Help Request Options

Communication

Option	Description
Phone number or IP address	If requesting help by a communication profile that uses a point-to-point or network point-to-point communication device other than Infrared (IrDA), a telephone number or IP address should be specified.

	If not specified in this field, the **Connect to Help Provider** dialog box is displayed when requesting help, and you can specify the telephone number or IP address there.
Help request timeout if not answered	Specify a number in the range to cancel the help request if not responded to by a help provider within the specified number of minutes (default: 0, i.e. the help request does not get canceled).

Gateway logon

If requesting help by a communication profile that uses a point-to-point or network point-to-point communication device through a **Guest** network **Gateway**, it may request logon.

Specify **Gateway logon** name, password and domain in this section.

If valid **Gateway logon** credentials are not specified here, a **Gateway** logon dialog box may be displayed when requesting help, and you can specify the credentials there.

Select the **Use current logon credentials for Windows Security authentication** check box to log on by the name, password and domain of the user logged on to Windows on the **Host** computer.

See also

Program Options (Help Request tab)
Request help

5.2.2 Allowed ISDN Numbers

If **Guest ISDN number check** is enabled in the **Communication Profile Edit** dialog box for ISDN, a **Host** and a connecting **Gateway** can allow connections by ISDN (CAPI) communication only from telephone numbers in the **Allowed ISDN Numbers** list.

The **Allowed Network Numbers** dialog box displays allowed ISDN telephone numbers. You can add, edit and delete ISDN telephone numbers in the dialog box.

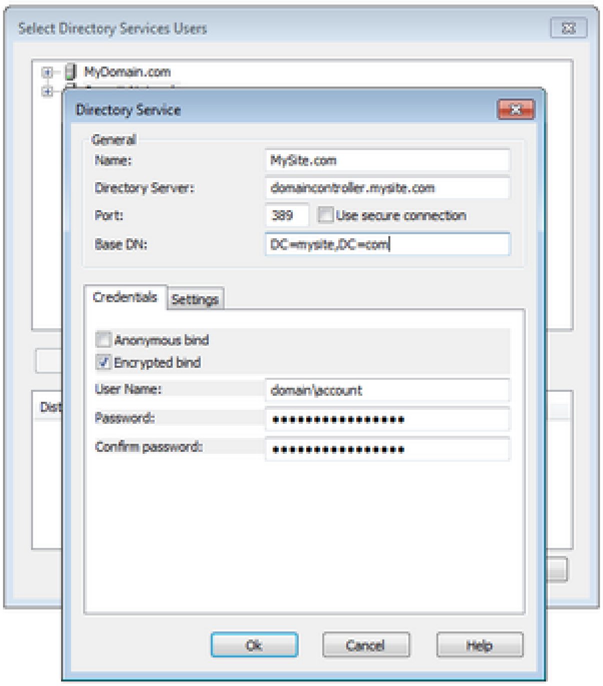
NOTE: Allowed ISDN numbers are stored in the **Impero** configuration file anumlist.ndb, which is typically located in the directory `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>`.

See also

Communication Profile Edit

5.2.3 Directory Service

Use the **Directory Service** dialog box to specify a directory service.



Name: MySite.com

Directory Server: domaincontroller.mysite.com

Port: 389 □ Use secure connection

Base DN: DC=mysite,DC=com

□ Anonymous bind

☑ Encrypted bind

User Name: domain\account

Password: ****************

Confirm password: ****************

General

Option	Description
Name	Specify the name that should identify the directory service in **Directory Services** tab pane.
Directory server	Specify the directory server IP address or DNS name.
Port	Specify the port through which the **Host** should connect to this directory server (default: 389, the Lightweight Directory Access Protocol (LDAP) port). Select the **Use secure connection** check box to connect to the directory server by a secure connection. The LDAP secure connection port number is 636.
Base DN	Specify the directory service distinguished name from which a search should start.

Credentials tab

Use the **Credentials** tab to specify the credentials by which the **Host** should log on to the directory server. The credentials determine what directory service information is available to the **Host**.

Option	Description
Anonymous bind	Select this check box to search the specified directory service with anonymous user rights, which are typically very limited.
User DN	Specify a directory service user distinguished name to search the directory service with the rights of this user.
Password/Confirm password	Specify the corresponding password and confirm it.

Settings tab

Use the **Settings** tab to specify the search criteria that should be applied to retrieve the properties of a connecting Guest user. Initially, the fields are empty.

Click on the **Default** button to display the **Select Directory Service** dialog box.

The drop-down list contains names of commonly used directory services such as Microsoft Active Directory. Select a directory service type in the drop-down list. If the directory service type of the directory server specified in the **Directory Server** field of the **Directory Service** dialog box is available in the list, select this in the list.

Click on the **OK** button to close the dialog box and specify the default settings of the selected directory service type in the **Settings** tab fields.

NOTE: If the **Settings** tab fields are filled in when you select a directory service type in the **Select Directory Service** dialog box, you typically do not need to edit their contents.

Option	Description
User search filter	Optionally (recommended), specify a search filter to limit the search for user attributes to a certain object class.
User attribute	Specify the type designation of the searched for user attribute.
User browse filter	Optionally (recommended), specify a user browse filter to limit the browse for user attributes to certain object classes.

Group search filter	Optionally (recommended), specify a search filter to limit the search for group attributes to a certain object class.
Group attribute	Specify the type designation of the searched for group attribute.
Group browse filter	Optionally (recommended), specify a group browse filter to limit the browse for group attributes to certain object classes.
OU search filter	Optionally (recommended), specify a search filter to limit the search for organizational unit attributes to a certain object class.

See also

Program Options (Directory Services tab)

5.2.4 Guest Access Security

Guest Access Privileges tab

Use the **Guest Access Privileges** tab to select the **Guest Access Method** to apply to connecting **Guests**.

Select a method from the **Guest Access Method** list:

Grant all Guests default access privileges	This selection means that the **Guests** share the same privileges and use the same password to log on to the **Host**. When a **Guest** connects, the **Host** requests a password. If the **Guest** returns the password set up for the default user, the **Host** grants the **Guest** the privileges set up for the default security role. **Setup** In the left pane, select **Default Security Role** to display the access privileges of this security role, i.e. what **Guests** are allowed to do when connecting to the **Host**, in the right pane. The **Confirm access** section in the right pane specifies whether and when access to the Host computer needs confirmation. NOTE: For practical reasons, the **Impero message** and **Get**

inventory functions are exempted from Confirm access security, as these are often used when there is no user present on the Host side.

The Whitelisted applications section in the right pane specifies whether the Remote Control sessions for this role are limited solely to the whitelisted applications defined in the **whitelisted.txt** file, found in the Impero configuration files folder: `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\<Module name>`.

NOTE: Refer to the Impero Knowledge Base for more information about whitelisting.

Select Default User in the left pane to set password and call back options. In the right pane, specify a password of max. 64 characters to enable shared password authentication.
To disable shared password authentication and request no password from a connecting Guest, clear both password fields. This, however, leaves the Host without Guest access authentication, and any Guest can then connect to the Host. Unless suppressed, a security warning is displayed when the Host starts communicating.
The Call back section below the Password section specifies whether or not to use call back.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address to enable connections only from a

<table>
<tr><td></td><td></td><td>Guest on a computer with this telephone number or IP address.</td></tr>
<tr><td></td><td>Roving call back</td><td>Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device.
When the Host receives this information, it disconnects and reconnects to the specified telephone number or IP address.
Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.</td></tr>
<tr><td>Grant each Guest individual access privileges using Impero authentication</td><td colspan="2">This selection means that each Guest has its own privileges and password to log on to the Host.
When a Guest connects, the Host requests the Impero credentials, i.e. ID and password, defined for that specific Guest. When the Guest returns the required information, the Host grants the Guest the privileges set up for the specific Guest.

Setup
Each security role specifies what is allowed to the Guest and the selected confirm access option. Each Guest profile specifies Guest logon credentials and the selected call back option.
Initially, the left pane contains the security role folders Full access, View only, Inventory only and Remote Management only. You can add a security role by clicking on the Add security role button and defining the new security role by clearing the check boxes in the right pane.
The Confirm access section in the right pane specifies whether and when access to the Host computer needs confirmation.</td></tr>
</table>

	NOTE: For practical reasons, the **Impero** message and **Get inventory** functions are exempted from **Confirm access security**, as these are often used when there is no user present on the **Host** side. The Whitelisted applications section in the right pane specifies whether the Remote Control sessions for this role are limited only to whitelisted applications defined in the whitelisted.txt file, found in the Impero configuration files folder: `C:\ProgramData\Danware Data\C\Program Files (x86)\Impero\Impero Connect\<Modulename>` folder. You can add **Guests** to a security role by selecting it and clicking on the **Add Guest** button. In the displayed **Guest Profile** dialog box, specify the **Guest** name, password and call back option. See Guest Profile. Select a **Guest profile** element in the left pane to display its **Password** section and the **Call back** section to the right.
Grant each Guest individual access privileges using Windows Security Management	This selection means that each **Guest** has its own privileges and logs on to the **Host** by its Windows logon user credentials. When a **Guest** connects, the **Host** requests the Windows user name, password and domain. If a match is found in **Windows Security Management**, the **Host** grants the **Guest** the privileges of the security role assigned to the Windows account object. A **Guest** user who is assigned different security roles individually and as a member of groups is allowed what is allowed by any of the applicable security roles, i.e. the sum of privileges of the applicable security roles. **Setup** Each security role specifies what is allowed to the **Guest** and

the selected confirm access option.

Initially, the left pane contains the security role folders **Full access**, **View only**, **Inventory only** and **Remote Management** only. Select a security role folder to display the privileges in the right pane. You can add a security role by clicking on the **Add security** role button and defining the new security role by clearing check boxes in the right pane.

The **Confirm access** section in the right pane specifies whether and when access to the **Host** computer needs confirmation.

NOTE: For practical reasons, the **Impero** message and **Get inventory** functions have been exempted from Confirm access security, as these are often used when there is no user present on the **Host** side.

The Whitelisted applications section in the right pane specifies whether the Remote Control sessions for this role are limited only to whitelisted applications defined in the whitelisted.txt file, found in the **Impero** configuration files folder: `C:\ProgramData\Danware Data\C\Program Files (x86)\Impero\Impero Connect\<Modulename>`.

You can add a user or group to a security role by selecting it and clicking on the **Add User** or **Add Group** button. In the Select Users or Select Groups dialog box, specify the users or groups you want to add.

Select a Windows user or group element to display its Domain section, RAS section and Call back section to the right.

The Domain section displays the domain of the selected Windows user or group.

The RAS section is only included if the Host computer runs on a Windows NT, 2000, XP, 2003, 2008, Vista or 7 operating system. Select the **Get call back information from Windows**

NT Remote Access Service (RAS) check box to use call back information stored in Windows NT Remote Access Service.

The Call back section is displayed only if the check box in the RAS section is not selected.

Specify whether or not to use call back.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the Host disconnect and reconnect to the specified telephone number or IP address, if a Guest connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address enables connections only from a Guest on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a Guest that connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the Host receives this information, it disconnects and reconnects to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.

The Windows User Manager button is included only if the

	Host computer runs on a Windows NT, 2000, XP, 2003, 2008, Vista or 7 operating system. Click on this button to display the Windows user manager window according to the administrator rights of the user logged on to Windows on the Host computer to manage users and groups.
Grant each Guest individual access privileges using Directory services	This selection means that each Guest has is own privileges and logs on to the Host by directory services user credentials. When a Guest connects, the Host requests the directory service user name, password and directory server for that specific Guest. If a match is found on the directory server, the Host grants the Guest the privileges of the security role assigned to the directory services account element. A Guest user who is assigned different security roles individually and as a member of groups is allowed what is allowed by any of the applicable security roles, i.e. the sum of privileges of the applicable security roles. Setup Each security role specifies what is allowed to the Guest and the selected confirm access option. Initially, the left pane contains the security role folders Full access, View only, Inventory only and Remote Management only. Select a security role folder to display the privileges in the right pane. You can add a security role by clicking on the Add security role button and defining the new security role by clearing check boxes in the right pane. The Confirm access section in the right pane specifies whether and when access to the Host computer needs confirmation. NOTE: For practical reasons, the Impero message and Get inventory functions have been exempted from Confirm access security, as these are often used when there is no user present on the Host side.

The Whitelisted applications section in the right pane specifies whether the Remote Control sessions for this role are limited only to whitelisted applications defined in the whitelisted.txt file, found in the **Impero** configuration files folder: `C:\ProgramData\Danware Data\C\Program Files (x86)\Impero\Impero Connect\<Modulename>`.

You can add a user or group to a security role by selecting it and clicking on the **Add User** or **Add Group** button. In the displayed **Select Directory Services Users** or **Select Directory Services Groups** dialog box, specify the users or groups you want to add.

Select a directory services user or group element to display its Directory service section and Call back section to the right.

The **Directory Service** section displays the directory service name and the selected directory services user or group element distinguished name (dn).

Specify whether or not to use call back:

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the **Host** disconnect and reconnect to the specified telephone number or IP address, if a **Guest** connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address enables connections only from a **Guest** on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a **Guest** that

	connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the Host receives this information, it disconnects and reconnects to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the Host organization, e.g. when a traveling employee connects to the home computer.
Use the Impero Security Server	This selection means that the Host uses the Security Server to authenticate each connecting Guest and assign a security role to it. When a Guest connects, the Host requests logon credentials according to Security Management preferences. Refer to the Administrator's Guide for further information about Security Management. The Host forwards returned credentials to Security Server for validation and compilation of the security role that is to be assigned to the Guest according to the security data stored in the security database. The Host applies the resulting security role to the Guest. Setup The Public Key field is used to secure a trusted connection between your Hosts and Security Servers. NOTE: In production environments, we recommend that you replace the default Public Key with a newly generated Public Key using the Security Manager. The Public Key should be copied to the Hosts exactly as it is

	shown in the **Security Manager**. It is recommended that you change the **Public Key** before deploying your **Hosts**. Refer to the **Security Management** section in the Administrator's Guide for more information about generating a **Public Key** from the **Security Manager**.
Use the Impero Portal access rights	This selection means that the **Host** uses the **Portal** to authenticate each connecting **Guest** and assign permissions to it. When a **Guest** connects, the **Host** requests logon credentials according to the **Portal** account. Refer to the Impero Connect User's Guide for more information about the **Portal**. The **Host** forwards returned credentials to **Portal** for validation and compilation of the security permissions that are to be assigned to the **Guest**. The **Host** applies the resulting security permissions to the **Guest**.

Guest Policy tab

Use the **Guest Policy** tab to specify **Guest** access security policies. The policy functions determine how the **Host** behaves before, during and after the remote control session.

Password

Option	Description
Maximum invalid password attempts	Specify a number in the range 0 - 9 for the number of logon attempts that can be allowed to a **Guest** before the action selected in the drop-down list below is executed.
Action if maximum attempts are exceeded	In the drop-down list, select what should happen if maximum password attempts are exceeded: • **Disconnect**: Disconnect the **Guest**. • **Disable Host**: Make the **Host** reject any connection attempt.

	• Restart Windows: Restart Windows on the Host computer, which - depending on the Host setup - may load and start the Host and make it available for connection.

Disconnect

Option	Description
Action after disconnect	In the drop-down list, select what should happen after disconnect: • None: No action. • Lock computer: Lock the Host computer. The Windows Computer Locked window is displayed. The Host keeps running and is available for connection. • Log off Windows: Log off the Host computer user from Windows. The Welcome to Windows window is displayed. The Host keeps running and is available for connection. • Restart Windows: Restart Windows on the Host computer, which - depending on the Host setup - can load and start the Host and make it available for connection.
System-wide disconnect hotkey	Select any of the first four check boxes and optionally specify a character in the last check box to compose a keystroke combination that disconnects all connected Guests whether the Host window is active or not.

File Transfer

Select the Disable file transfer before local logon check box to disable file transfer if no user is logged on to the Host computer.

Record Sessions

Option	Description
Enable	Select this check box to enable Host recording of remote control sessions. If you enable the Record Sessions function, you can document any unauthorized procedures that a Guest could carry out on the

	Host.
Folder	Specify the path of the directory in which to save the session recording files. Click on the **Browse** button to select a folder.
Disconnect if recording fails	Select this check box to disconnect if session recording fails. **NOTE**: Session recording files are named `<Time stamp>-<Guest ID>-<Host ID>.dwr`. You can only play back session recording files on a **Guest**.

Timeout

Option	Description
Confirm Access	Specify a number in the range `1 - 9999` to disconnect if the Host user has not confirmed Guest access within the specified number of seconds.
Authentication	Specify a number in the range `1 - 9999` to disconnect if **Guest** authentication has not completed within the specified number of seconds.
Inactivity	Specify a number in the range `1 - 9999` to disconnect if there has been no **Guest** keyboard or mouse activity within the specified number of seconds.

MAC/IP Address List Setup tab

MAC/IP Address List

Select the **Enable MAC/IP address** check check box to limit the network addresses from which a **Guest** can connect to the addresses specified in the pane.

Click on the **Add** button to specify MAC/IP addresses.

MAC addresses are applied if they communicate by NetBIOS or IPX. IP addresses apply if they communicate by TCP/IP or TCP/IP (TCP).

Encryption tab

The communication between **Impero** modules is protected by encrypting transmitted data.

A range of encryption types is available on Connect modules.

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

Select the check boxes next to the various encryption types to enable them.

To see encryption details about the individual encryption types, select an encryption type and click on the Show Details button.

Smart Card

Use the Smart Card tab to specify Smart Card logon options to use Smart Card for authentication with Windows Security Management or Directory Services.

Windows Security Management

If you have selected the Guest access method Grant each Guest individual access privileges using Windows Security Management on the Guest Access Privileges tab, select an option in this section.

Option	Description
Never log on with Smart Card	Enable only credentials logon.
Always log on with Smart Card	Enable only Smart Card logon.
Allow both logon with Smart Card and credentials (name, password, and domain)	Enable both credentials and Smart Card logon.

Directory Services

If you have selected the Guest access method Grant each Guest individual access privileges using Directory services on the Guest Access Privileges tab, select an option in this section.

Option	Description
Never log on with Smart Card	Enable only credentials logon.
Always log on with Smart Card	Enable only Smart Card logon.
Allow both logon with Smart Card and credentials (name, password and server)	Enable both credentials and Smart Card logon.

Subject Field	Retrieve the user identification from the Subject field of the Smart Card certificate.
Subject Alternative Name Field (must be a User Principal Name (UPN))	Retrieve the user identification from the Subject Alternative Name field of the Smart Card certificate.
The Certificate Field matches this Directory Services Attribute	Specify the directory services attribute compatible with the Smart Card certificate field contents. This is necessary only if different from a user object distinguished name. For Directory Services Smart Card logon to succeed, make sure that Host can resolve the Smart Card certificate user identification into a Directory Services user identification. If the Smart Card certificate user identification and Directory Services user identifications are incompatible, Smart Card logon fails. To find the available Smart Card certificate user identifications, insert the Smart Card and in Internet Explorer click on the Internet Options command on the **Tools** menu to display the **Internet Options** dialog box. On the **Content** tab, click on **Certificates** to display the **Certificates** dialog box. On the **Personal** tab, double-click on the appropriate certificate record to display the **Certificate** dialog box. The **Details** tab displays the contents of available certificate fields including **Subject** and **Subject Alternative Name**.

See also
Program Options (Smart Card tab)

5.2.5 Guest Profile

Use this dialog box to create a **Guest** profile element in the security role folder that you selected on the **Guest Access Privileges** tab.

Guest name

In the **Guest ID** field, specify the name that a **Guest** is using this **Guest** profile should specify to log on to the **Host**. This is the name that identifies the **Guest** profile.

NOTE: A **Guest** is not limited to logging on by the name that identifies the **Guest**. The **Guest** logon does not verify **Guest** identity but validates the **Guest** credentials.

Password

In the **Password** section, specify a password of max. 64 characters to enable password authentication.

Call back

In the **Call back** section specify whether or not to use callback.

Option	Description
No call back	Do not apply call back.
Call back to	Specify a telephone number or an IP address to make the **Host** disconnect and reconnect to the specified telephone number or IP address, if a **Guest** connects by a communication profile that uses a point-to-point or network point-to-point communication device. Call back to a specified telephone number or IP address enable connections only from a **Guest** on a computer with this telephone number or IP address.
Roving call back	Select this option to request a call back telephone number or IP address from a **Guest** that connects by a communication profile that uses a point-to-point or network point-to-point communication device. When the **Host** receives this information, it disconnects and reconnects to the specified telephone number or IP address. Roving call back is typically used to make connection costs payable by the **Host** organization, for example when a traveling employee connects to the home computer.

See also

Guest Access Security (Guest Access Privileges tab)

5.2.6 Help Providers

In connection with a help request, if help providers are found, but no problem description and/or no Help provider was specified in the **Program Options** dialog box in the **Help Request** tab, the **Help Providers** dialog box is displayed.

Specify a problem description and a help provider:

Option	Description
Problem description	This field displays any problem description specified in the **Program Options** dialog box in the **Help Request** tab. You can leave the field empty or specify or edit a problem description.
Help providers	Names of help providers found (on **Impero Guest** named help services) are displayed in the **Help providers** pane. Select one and click on **Select** to deliver the help request to the selected help provider.

5.2.7 Help Request

Select one of these options:

Option	Description
Use the help service to search for help providers	Select this option to request help from a help service.
Use service ticket to connect to a specific help provider	Select this option to request help by a received service ticket number. Selecting this option enables the following fields: • Service ticket: In this field, specify the service ticket number. • Problem description: In this field, you can describe your problem.

NOTE: This dialog box displays only the service ticket fields if **Enable Service Tickets** is selected in the **Program Options** dialog box in the **Help Request** tab. An **OnDemand**

enabled **Guest** can issue service ticket numbers and forward a service ticket number to you to enable you to return a help request.

See also

Set up Help Request on Guest and Host

Program Options (Help Request tab)

5.2.8 Maintenance Password

You can protect the **Host** setup with a maintenance password, so that no unauthorized people can make changes to the **Host** setup.

Use the **Maintenance Password** dialog box to specify a maintenance password, what it protects, and Host configuration files (`*.ndb`) protection.

Click on the **Change Maintenance Password** button to display the **Change Maintenance Password** dialog box, where you can specify the maintenance password (max. 64 characters), change it, or disable it by deleting it.

Specify what the maintenance password should apply to and when:

Maintenance password required for

Option	Description
Guest access security	Select this check box to apply maintenance password protection to the **Guest Access Security** command on the **Tools** menu and the **Guest Access Security** button on the toolbar.
All other configuration	Select this check box to apply maintenance password protection to all other setup commands on the **Tools** menu and other tool buttons on the toolbar.
Unload and Stop	Select this check box to apply maintenance password protection to unloading the **Host** and stopping the **Host**. Apply Unload and Stop maintenance password protection to prevent **Host** stop or unload that make it unavailable for connection and/or to protect security configuration files.
Confirm access	Select this check box to require the user to enter the maintenance password before the remote session can begin. Using **Confirm access**, the local user on the **Host** machine has the ability to allow or deny the remote session. In some situations, such as large industrial environments or senior executives within a

	large organization, the maintenance password is often known by the local Host user. As an extra level of security and to help prevent unauthorized users from allowing the remote support session, the local user on the Host machine can now enter the maintenance password in the Confirm Access Password dialog box before the remote session can begin.

Protect security configuration files

Option	Description
Protect by maintenance password only (if applies)	Protect Host setup only by any applied maintenance password protection. This does not protect Host configuration files (default selection).
Protect files when connected	Protect Host configuration files and disable setup commands on the Tools menu when the Host status is "Connected" to prevent a connected Guest from changing Host setup.
Protect files when connected and running	Protect Host configuration files and disable setup commands on the Tools menu when the Host status is "Connected", "Help requested" or "Running" to prevent a Host computer user from changing the Host setup. Combined with the Unload and Stop option, the maintenance password protection also prevents the Host user from stopping and unloading the Host and then changing the Host security configuration files.

NOTE: Host configuration files (`*.ndb`) are located in the Impero configuration files folder, typically `C:\ProgramData\Danware Data\C\Program Files (x86)\Netop\Netop Remote Control\Host`.

If maintenance password protection is enabled, a dialog box prompting you to enter the maintenance password is displayed when you select a protected command or click a protected button.

There is no limit to the number of maintenance password attempts.

5.2.9 Program Options

General Tab

Use the **General** tab to specify startup and connection options.

Startup

Option	Description
Start Host when loaded	Select this check box to start the Host and enable communication when loaded.
Load Host at Windows startup (run as service)	Select this check box to load the Host when Windows starts on the computer. NOTE: Loading the Host at Windows startup and starting the Host when loaded makes the Host ready for connection when the Host computer is started, even if no user is logged on to Windows.
Minimize Host when loaded	Select this check box to minimize the Host to a Host icon when loaded.
Stealth mode (hide Host when started)	Select this check box to load the Host hidden to the Host computer user. If hidden, nothing on the screen indicates that the Host is loaded. NOTE: To display a hidden Host, execute the **showhost.exe** file. The **showhost.exe** file is located in the folder where the Host is installed.

Connection

Option	Description
Minimize Host on connection with Guest	Select this check box to minimize the Host window to a Host icon when a Guest connects.
Host top most window on connection with Guest	Select this check box to display the Host window in front of any other window when a Guest connects.
Show file transfer status	Select this check box to display the File Transfer Status window when a Guest starts a file transfer session.
Send keep alive message	Select this check box to send a data packet at intervals

	while connected to alert the Host user if the connection is lost. NOTE: To maintain an ISDN (CAPI) connection during short periods of inactivity, do not select this check box. Instead select the Short-hold mode check box in the Edit dialog box for the ISDN (CAPI) communication profile.
Allow Multiple Simultaneous Guest Sessions	Select this check box to allow multiple Guest connections to the Host at the same time.

Host Name tab

Use the Host Name tab to specify Host naming, name options and the Name Server name space ID.

Naming

This section specifies the name by which the Host identifies itself when communicating.

To communicate by a communication profile that uses a networking communication device (NetBIOS, IPX, TCP/IP, Terminal Server), it is necessary that each Host use a unique name. A Host that uses a name that is already used by another communicating Host is denied communication.

Select one of these options:

Option	Description
Enter name or leave name field blank	Select this option to display a field below. Specify a name in the field or leave the field blank to name the Host by the specified name or leave it without a name.
Use environment variable	Select this option to display a field below. Specify an environment variable name in the field to name the Host by the value of the specified environment variable. NOTE: Do not name a network computer Host by the environment variable `USERNAME` if it is set up to load at Windows startup. If you do that, the Host loads before a user logs on to Windows to get the name `%USERNAME%` and retains this name until reloaded while a user is logged on to get the name `<Windows logon user name>`. Of multiple Hosts named `%USERNAME%`, only one can communicate.

	Name a terminal server session Host typically by the environment variable USERNAME. See the Administrator's_Guide, Impero Naming (TSE). To display available Windows environment variables, in a command prompt window type set and press ENTER.
Use Windows computer name	Name the **Host** by the **Host** computer Windows name. **NOTE**: Name a network computer **Host** typically by the Windows computer name. Do not name a terminal server session **Host** by the Windows computer name. Terminal server session **Hosts** share the Windows computer name of the terminal server computer. Of multiple Hosts named by the terminal server computer name, only one can communicate. Select the **Prefix with computer workgroup name** check box to add a prefix to the **Host** computer name to ensure **Host** name uniqueness across multiple domains and workgroups. The prefix can be its domain or workgroup name. Use the **Separate with** field to specify the separator character. The default character is a back slash (\), but you can replace it by any other character.
Name	The **Host** name according to the selection above.

Name options

Option	Description
Public Host name	Select this check box to respond to **Guests** that browse for **Hosts** by the **Host** name. **NOTE**: If the **Host** computer is connected directly to a public network like the Internet, you may want to clear the selection of this check box to not invite hacking attempts.
Enable user name	Select this check box to enable the name of a user logged on to the **Host** computer to enable connections by the user name. **NOTE**: If this check box is selected, the user name appears on the **Names** tab of the **Host** window. You may want to clear the selection of this check box on a server **Host** to disable connecting by the name

	of a temporarily logged on user or the user as which the Host runs to acquire the computer rights of the user.

Impero Name Server

In the Name Space ID field specify the name space ID specified on Guests with which the Host should be able to communicate by using Name Server. The default name space ID is PUBLIC.

The name space ID applies only if the Host communicates through a communication profile that uses the TCP/IP communication device and for which the Use Impero Name Server check box in the Advanced TCP/IP Configuration window is selected and Name Servers are specified.

NOTE: For the changes to the naming or name space ID to take effect, make sure to restart the Host.

Connection Notification tab

Use the Connection Notification tab to specify options for connection notification upon, during and after connection.

Upon connection

Option	Description
Play sound	Select this check box to play a sound when a Guest connects. The sound file StartHRC.wav is located in the Media folder of the folder in which the Host is installed.
Display Connection List	Select this check box to display the Connection List window when a Guest connects. Specify in the field to the right the number of seconds that this window should be displayed. Default is 6. The value 0 makes the Connection List window remain on the screen.
Password to close Connection List	Select this check box and specify a password in the field below to make the Connection List window remain on the screen until closed manually. Characters are displayed as dots or asterisks. To close the Connection List window, you are prompted to enter the specified password.

Display balloon tip	Select this check box to display a balloon tip from the **Host** icon when a **Guest** connects.

During connection

Option	Description
Play sound	Select this check box to play a sound during **Guest** connection at this interval. In the Interval field specify a number in the range for the interval between sounds in seconds. The sound file ContHRC.wav is located in the Media folder of the folder in which the **Host** is installed.
Display Guest name (if available) in the title bar	Select this check box to display the connected keyboard and mouse control **Guest** name in the title bar, the Windows taskbar **Host** icon and the **Host** icon tool tip.
Animate icon	Select this check box to animate the **Host** icon double corner lines during **Guest** connection.

After connection

Option	Description
Display History List	Select this check box to display the **History List** window when a **Guest** disconnects. Specify in the field to right the number of seconds this window should be shown. Default is 0. The value 0 makes the **History List** window remain on the screen.
Password to close History List	Select this check box and specify a password in the field below to make the **History List** window remain on the screen until closed manually. Characters are shown as dots or asterisks. To close the **History List** window, enter the specified password.
Display balloon tip	Select this check box to display a balloon tip from the **Host** icon when a **Guest** disconnects.

Audio-Video Chat tab

Use the **Audio-Video Chat** tab to specify audio and video settings.

Audio Chat

General

Select the **Enable full-duplex audio** check box to enable sending audio data between **Guest** and **Host** in both directions at the same time.

NOTE: Some computer audio systems do not support full-duplex audio.

Microphone sensitivity

Option	Description
Silence level	Drag the slider bar to specify the microphone sound input level below which no sound data should be transferred.
Line hold	Drag the slider bar to specify the time period in which sound data should continue to be transferred after the microphone sound input level has dropped below the silence level. **TIP**: Try out different Silence level and Line hold settings to optimize sound transfer.

Click on the **Check sound system** button to test the computer sound system.

Click on the **Advanced** button to display the **Advanced audio settings** dialog box.

See Advanced audio settings.

Video Chat

Click on the **Advanced** button to display the **Advanced Video** dialog box.

See Advanced Video.

Remote Printing tab

Use the **Remote Printing** tab to specify remote **Impero** printers.

Click on the **Add Printer** button to add a remote printer. Follow the guidelines in the displayed **Add printer guidelines** dialog box. Click on the **Ready** button to start adding a remote **Impero** printer.

The remote printers that you add, are displayed in the **Remote Impero printers** pane.

You can remove an **Impero** printer by selecting it in the pane and clicking on the **Remove Printer** button.

To send a **Host** computer print job to a **Guest** printing device while the **Guest** is connected, print to a **Host** computer remote **Impero** printer that specifies the **Guest** printing device.

NOTE: Special instructions for remote printing from DOS applications are available in the Impero Knowledge Base.

See also

Send a print job to a remote printer

Help Request tab

Use the **Help Request** tab to specify general help request options. If unspecified, the **Host** user can specify individual options with each help request.

Optional help information

Option	Description
Problem description	To always specify the same problem description, specify it in this field. If the field is left empty, the **Help Providers** window is displayed when requesting help, allowing you to specify a problem description for the individual help request.
Help provider	To always request help from the same help provider (help service), specify its name in this field. If the field is left empty, the **Help Providers** window is shown when you request help, allowing you to specify a help provider for the individual help request.

Communication

Communication profile

Option	Description
Use current Host communication profiles	Select this option to send help requests by enabled communication profiles. Unless only one communication profile or only communication profiles that use networking communication devices are enabled, the **Select Help Request Communication Profile** dialog box is displayed when requesting help.
Use specific Communication Profile	Select this option and select one of the available **Host** communication profiles in the drop-down list to use a specific communication profile.

Click on the **Advanced** button to display the **Advanced Help Request Options** dialog box. See Advanced Help Request Options.

Options

Option	Description
Add Help Request icon to the tray	Select this check box to add a help request icon (a life belt) to the notification area in the lower right corner of the screen. If this icon is added, the Host computer user can request help even if the **Host** is hidden. To request help, double-click on the icon or right-click on the icon and select **Request Help**.
Enable Help Service	Select this check box to enable help request by a help service.
Enable Service Tickets	Select this check box to enable help request by a service ticket.

See also

Request help
Set up Help Request on Guest and Host

Run As tab

Use the **Run As** tab to enable running the Host with the rights of a Windows user account if no user is logged on to the **Host** computer, the **Host** runs with extensive **Host** computer rights but no network computer rights. See the Administrator's Guide, **Impero** Connect Processes and Windows Security. If a user is logged on to the **Host** computer, the **Host** runs with the rights of the logged on user.

Run Host as specific user

Option	Description
Enable	Select this check box to always run the **Host** as a specific Windows user account.
User name	Specify the Windows user account name.
Password	Specify the corresponding password.
Domain	Specify the corresponding domain. **CAUTION!** Consider carefully in each case the benefits and drawbacks including security risks of always running the **Host** as a specific Windows user account. In some cases, run the **Host** as a Windows user account created exclusively for this purpose.
Automatically change to random password every week	Select this check box to change the password of the credentials specified above immediately and every week into a random password to automatically satisfy a password change policy. **CAUTION!** Do not select this check box if the credentials specified above belong to a user person, as the user person cannot know the random password.

Directory Services tab

Use the **Directory Services** tab to specify directory services to enable authenticating connecting **Guests**.

Click on the **Add** button to add a directory service. The **Directory Service** dialog box in which you can specify the directory service that you want to use is displayed. See Directory Service.

The name of the directory service and the directory server IP address or DNS name is displayed in the pane on the **Directory Services** tab.

To edit the properties of the directory service record, select the record in the pane and click on the **Edit** button.

To remove the directory service, select the record in the pane and click on the **Delete** button.

See also

Guest Access Security(Grant Each Guest Individual Access Privileges Using Directory Services tab).

Multi-Factor Services tab

Use the **Multi-Factor Services** tab to enable multi-factor authentication when connecting **Guests**.

Click on the **Add** button to add the corresponding Multi-Factor service. The **Multi-Factor Service** dialog box in which you can specify the multi-factor service that you want to use is displayed.

Multi-Factor Service Settings

Option	Description
Name	Specify a name for the multi-factor service to be defined.
Multi-Factor Service Type	The list of services which help safeguard access to data and applications. **Connect** currently provides integration to Windows Azure Multi-Factor Authentication.
Client Certificate	Click on the **Choose certificate...** button and browse for the Windows Azure certificate to be used for the Windows Azure Multi-Factor Authentication.
LDAP Phone No Attribute	The LDAP attribute identifying the user's telephone number. It will be used to send user the token to be used for multi-factor authentication.
Apply to all roles	Select this check box to apply the current multi-factor authentication service to all roles defined in the Directory Services.

	NOTE: Multi-factor authentication applies to all roles only if the Guest Access Method selected from **Tools** > **Guest Access Security** is either Grant each Guest individual access privileges using Windows Security Management or Grant each Guest individual access privileges using Directory services.

To edit the properties of the Multi-Factor service record, select the record in the pane and click on the **Edit** button.

To remove the multi-factor service, select the record in the pane and click on the **Delete** button.

In case there are multiple roles which can apply for a specific authenticating user, each potentially with a different multi-factor authentication services, the multi-factor authentication service to be chosen is the one with the highest priority from the list. Order in the list dictates the priority, top items having the highest priority.

See also

Guest Access Security (Grant Each Guest Individual Access Privileges Using Directory Services tab).

Web Update tab

Use the **Web Update** tab to specify web update options to automatically update the **Host** installation.

Web Update Settings

Option	Description
Update server	Specify the web address of the server from which to download **Host** update files (default: update.netop.com, the **Impero** manufacturer web update server). **NOTE**: To update the **Impero** installations in an organization, we recommend publishing new updates to an internal web update server (select Publish New Updates on the Tools menu).
HTTP Proxy	Specifying a HTTP proxy is typically not required. Before specifying a HTTP proxy, click on the Update now button to test the web update connection. If you receive a message indicating connection to the update server, specify no HTTP proxy. If **Update now** yields no connection, click on the **Detect** button to make

	Impero attempt to detect the HTTP proxy server and display its name and port number in the HTTP Proxy field. Click on the Update now button to test the connection. If unsuccessful, consult your network/system administrator about what to specify in the HTTP Proxy field (format: `<Server name>:<Port number>`).
Update now	Click on this button to connect to the update server specified in the Update server field. A web update message notifies you if the connection to the update server fails, if no updates are available or if updates are available, and in the latter case ask you if you want to download and install updates.
Schedule	Click on this button to display the Web Update Schedule dialog box and specify a schedule of checks for updates including download and installation of available update files.

5.2.10 Select Directory Services Users or Groups

The Select Directory Services Users dialog box and the Select Directory Services Groups dialog box are similar.

The directory services users or groups that you add here are added to the security role selected in the Guest Access Security dialog box on the Guest Access Privileges tab.

The upper pane displays directory services specified in the Program Options dialog box on the Directory Services tab.

Users or groups are displayed below the individual directory services in the pane.

Select a user or group in the upper pane and click on the Add button. The user or group is added to the lower pane. They are displayed by their distinguished name, for example the directory path and common name of the user/group, and the directory service name as specified in the Program Options dialog box on the Directory Services tab.

See also

Guest Access Security (Guest Access Privileges tab)
Directory Service

Index