Impero® is a registered trademark of Impero Holdings Limited. All other products mentioned in this document are trademarks of their respective manufacturers. Impero Holdings Limited denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice. Copyright (C) 2007-2021 Impero Holdings Limited. All Rights Reserved.
## Contents

1. Introduction .................................................................................................................................................. 7

2. Impero Security Management .................................................................................................................. 8
   2.1. Impero Security Management Overview ............................................................................................. 8
       2.1.1. Impero Security Management Functionality .................................................................................. 8
       2.1.2. Impero Security Management Setup ............................................................................................ 9
       2.1.2.1. Security Database Setup ........................................................................................................... 9
       2.1.2.2. Impero Security Server Setup .................................................................................................. 10
       2.1.3. Impero Security Management Maintenance .................................................................................. 10
   2.2. Load Impero Security Manager ............................................................................................................ 11
       2.2.1. Security Database Wizard ............................................................................................................. 12
   2.3. Impero Security Manager Window ....................................................................................................... 14
       2.3.1. Title Bar ........................................................................................................................................ 14
       2.3.2. Menu Bar ..................................................................................................................................... 14
           2.3.2.1. File Menu .............................................................................................................................. 15
           2.3.2.2. Records Menu ...................................................................................................................... 15
           2.3.2.3. Edit Menu ............................................................................................................................. 15
           2.3.2.4. View Menu ........................................................................................................................... 16
           2.3.2.5. Options Menu ....................................................................................................................... 17
           2.3.2.6. Help Menu ............................................................................................................................ 17
       2.3.3. Toolbar .......................................................................................................................................... 18
       2.3.4. Filter and Fetching Bar .................................................................................................................. 20
       2.3.5. Selection Pane ............................................................................................................................. 21
       2.3.6. Records Pane ............................................................................................................................... 21
       2.3.7. Message Panel ............................................................................................................................... 22
       2.3.8. Status Bar ..................................................................................................................................... 22
   2.4. Manage Security Database Contents .................................................................................................... 22
       2.4.1. Contents Creation Guide ................................................................................................................ 23
           2.4.1.1. Review Security Policies ......................................................................................................... 23
           2.4.1.2. Create Role Assignments ...................................................................................................... 24
           2.4.1.3. View and Manage Data ......................................................................................................... 24
           2.4.1.4. Scheduled Jobs ....................................................................................................................... 25
           2.4.1.5. Security Log ............................................................................................................................ 25
           2.4.1.6. Impero Log ............................................................................................................................. 25
           2.4.1.7. Active Sessions ....................................................................................................................... 26
       2.4.2. Security Settings ............................................................................................................................. 26
           2.4.2.1. Role Assignment ...................................................................................................................... 27
               2.4.2.1.1. New ................................................................................................................................. 28
               2.4.2.1.2. New Batch ....................................................................................................................... 29
               2.4.2.1.3. Edit ................................................................................................................................. 31
               2.4.2.1.4. Delete ............................................................................................................................. 31
               2.4.2.1.5. Clear .............................................................................................................................. 31
           2.4.2.2. Role ......................................................................................................................................... 31
               2.4.2.2.1. New ................................................................................................................................. 34
               2.4.2.2.2. Edit ................................................................................................................................. 35
               2.4.2.2.3. Delete ............................................................................................................................. 35

1
2.4.9.5 Properties .................................................................91
2.4.9 Importing Roles and Definitions ........................................92
2.4.9.1 Impero Definitions ......................................................93
2.4.9.2 Directory Services Definitions .......................................95
2.4.9.3 Windows Definitions ..................................................96
2.4.9.4 RSA SecurID Definitions ..............................................98

2.5 Security Database Tables ....................................................99

| 2.5.1 DWBATH: Scheduled Job ................................................100 |
| 2.5.2 DWCONN: Active Sessions ..............................................101 |
| 2.5.3 DWDOMN: Windows Domain ............................................102 |
| 2.5.4 DWDONE: Security Log ..................................................102 |
| 2.5.5 DWEVNT: Impero Log .....................................................103 |
| 2.5.6 DWGRUH: Impero Host ID Group ......................................103 |
| 2.5.7 DWGRUP: Impero Guest ID Group .....................................103 |
| 2.5.8 DWHOGR: Impero Host ID Group Members ........................104 |
| 2.5.9 DWHOST: Impero Host ID .................................................104 |
| 2.5.10 DWLDAPGRP: Directory Service Group ..............................105 |
| 2.5.11 DWLDAPPROP: Directory Service Properties .....................105 |
| 2.5.12 DWLDAPSERV: Directory Service .....................................106 |
| 2.5.13 DWLDAPUSR: Directory Service User ................................106 |
| 2.5.14 DWLDAPRADIUS: RADIUS settings .................................107 |
| 2.5.15 DWMAIN: Role Assignment .............................................107 |
| 2.5.16 DWNTGR: Windows Group .............................................108 |
| 2.5.17 DWNTUS: Windows User ...............................................108 |
| 2.5.18 DWPOLI: Security Policies .............................................109 |
| 2.5.19 DWPKI: Public/Private Keys ..........................................109 |
| 2.5.20 DWPROP: Impero Properties ..........................................110 |
| 2.5.21 DWROLE: Role ..........................................................110 |
| 2.5.22 DWRSAGRP: RSA SecurID Group ....................................111 |
| 2.5.23 DWRSAPROP: RSA SecurID Properties ..............................111 |
| 2.5.24 DWRSAUSR: RSA SecurID User ......................................112 |
| 2.5.25 DWRSGM: RSA SecurID Group Members ............................112 |
| 2.5.26 DWSERV: Impero Security Servers ...................................112 |
| 2.5.27 DWTODO: Scheduled Job Actions ....................................113 |
| 2.5.28 DWUSER: Impero Guest ID .............................................113 |
| 2.5.29 DWUSGR: Impero Guest ID Group Members .......................114 |
| 2.5.30 DWWKGM: Windows Workstation Group Members ...............115 |
| 2.5.31 DWWKSG: Windows Workstation Group ............................115 |
| 2.5.32 DWWKST: Windows Workstation .....................................115 |

2.6 Impero Security Server Setup ..............................................116

| 2.6.1 Security Server Tab .....................................................117 |
| 2.6.2 Run As Tab ..................................................................117 |
| 2.6.3 Communication Setup ..................................................118 |

2.7 Use Impero Security Management ........................................118

| 2.7.1 Prerequisites ..................................................................118 |
| 2.7.2 Maintenance ..................................................................119 |
| 2.7.3 Security ......................................................................120 |
5.2.6 Programmer Information ..............................................146
  5.2.6.1 NGuestXLib::_INGuestXCtrlEvents ......................146
  5.2.6.2 INGuestXCtrl ..............................................154
  5.2.6.3 INGuestXEventParam .....................................173
  5.2.6.4 INGuestXFont .............................................174
  5.2.6.5 INGuestXRcArea .........................................175
  5.2.6.6 INGuestXShortcut ........................................175
  5.2.6.7 NGuestX Messages ..........................................176
5.3 Impero Scripting ActiveX Control .....................................181
  5.3.1 Create and Delete ..............................................182
  5.3.2 StartGuest, Initialize and Uninitialize .....................182
  5.3.3 Connect and Disconnect .......................................183
  5.3.4 Transfer Files ................................................185
  5.3.5 Examples ......................................................187
  5.3.6 Reference ......................................................189
5.4 Impero Connect Processes and Windows Security .....................196
  5.4.1 Impero Processes ..............................................196
  5.4.2 Main Host Processes ..........................................197
    5.4.2.1 Normal Operation ......................................197
    5.4.2.2 Replace the Local Security Context ..................197
    5.4.2.3 Disable Main Host Processes Security ..............198
  5.4.3 Impero Helper Service .......................................198
    5.4.3.1 Reload Impero Host with Impero Helper Service ....199
  5.4.4 Impero Activity Local Group ..................................199
5.5 Impero Connect Command Line Parameters ..............................199
  5.5.1 Guest parameters .............................................200
  5.5.2 Host parameters ..............................................202
5.6 Impero Connect and URI ..............................................207
5.7 Kerberos authentication ..............................................208

Index .................................................................................210
1 Introduction

This Impero Connect Administrator's Guide supplements the Impero Connect User's Guide and contains the following chapters:

- Impero Security Management
- Impero Gateway
- Impero Name Management
- Advanced Tools
2 Impero Security Management

Impero Security Management provides centralized control of the Guest access privileges of multiple Impero Hosts and extended Hosts.

This main section includes these sections:

- Impero Security Management Overview
- Load Impero Security Manager
- Create or Log On to the Security Database
- Impero Security Manager Window
- Manage Security Database Content
- Security Database Tables
- Impero Security Server Setup
- Use Impero Security Management

2.1 Impero Security Management Overview

Impero Connect can protect computers that run Impero Host or extended Host against unauthorized access and actions from computers that run Impero Guest. Protection can be managed locally on each Impero Host by Guest Access Security and centrally for multiple Impero Hosts by Impero Security Management.


Centrally managed Impero Security Management is explained in this Impero Security Management main section.

This overview section includes the following sections:

- Impero Security Management Functionality
- Impero Security Management Setup

2.1.1 Impero Security Management Functionality

Impero Security Management stores Guest access security data for Guest and Host selections in a central Security Database, which is managed from Impero Security Manager.

Impero Security Server services Host requests for Guest Roles with themselves by managing Guest authentication, querying the central Security Database for security data, determining the applicable Role and returning it to the Host to apply it:

1. A Guest that connects to a Host is requested to identify itself by logon credentials.
2. The Host forwards the Guest credentials to Impero Security Server requesting the Role of the Guest with itself.
4. Based on returned security data, Impero Security Server determines the applicable Role and return it to the Host.
5. The Host applies the received Role to the Guest.

See also

Impero Security Manager
2.1.2 Impero Security Management Setup

Impero Security Management setup falls into three parts:

- **Security Database Setup**
- **Impero Security Server Setup**

2.1.2.1 Security Database Setup

Security Database setup is managed from Impero Security Manager, which is a database client program.

The Security Database can reside in any Open Database Connectivity (ODBC) enabled database. Creating the Security Database creates tables for these data:

- Security Settings including Role Assignments, Roles and Security Policies.
- Scheduling including Scheduled Jobs.
- Impero Definitions including Impero Guest IDs, Impero Guest ID Groups, Impero Host IDs, Impero Host ID Groups and Impero Properties.
- RSA SecurID Definitions including RSA SecurID Users, RSA SecurID Groups and RSA SecurID Properties.

Security Policies specify a Security Server Public Key, lists group members in a Security Server List, specifies a Preferred Guest Type and a Preferred Host Type and specifies Logging Options.

The key element in Impero Security Management is the Role Assignment that specifies a Guest selection, a Host selection and the Role of the Guest selection when connected to the Host selection.

- A Guest selection can be a Impero Guest ID or Impero Guest ID Group, a Windows User or Windows Group, an RSA SecurID User or RSA SecurID Group, a Directory Services User or Directory Services Group or everybody (any Guest).
- A Host selection can be a Impero Host ID or Impero Host ID Group, a Windows User, Windows Group, Windows Workstation, Windows Workstation Group or Windows Domain or everybody (any Host).
- A Role specifies allowed/not allowed/denied Guest actions on the Host and a Host confirm access selection.
- You can create Role Assignments mutually between multiple Windows Groups and with Windows Domain computers in a batch operation.
- You can create other Role Assignments one by one.

Impero Security Manager can retrieve Windows user, workstation, group and domain information from available Windows user and computer management and directory services user and group information from available Directory Services to create Windows Definitions and Directory Services Definitions Role Assignments without previously creating Security Database records.

Impero Definitions and RSA SecurID Definitions records must be created in the Security Database to create Role Assignments with them.
You can modify two of the four built-in Roles and create additional Roles. By group memberships, multiple Role Assignments can be available between each Guest and each Host. The composite of multiple assigned Roles are applied.

Security Database setup is explained in the following sections:

- Load Impero Security Manager
- Create or Log On to the Security Database
- Impero Security Manager Window
- Manage Security Database Content
- Security Database Tables

See also

Impero Security Manager
Security Settings
Role Assignment
Role
Security Policies
Logging
Scheduling
Impero Definitions
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions

2.1.2.2 Impero Security Server Setup

Impero Security Server is an extended Impero Host with the capability to process Host Role requests.

Install Impero Security Server preferably on multiple computers for load balancing and fault tolerance.

Add Impero Security Servers to the Security Server List.

Log Impero Security Servers on to the central Security Database.

Enable Impero Security Server communication with Hosts that use it.

See also

Impero Security Server Setup
Role
Security Database Setup
Security Server List

2.1.3 Impero Security Management Maintenance


Read the Use Impero Security Management section for guidelines.

See also

Security Database Setup
Impero Security Server Setup
Impero Security Management
2.2 Load Impero Security Manager


**NOTE:** To run Impero Security Management with a local test database, install Impero Security Manager and Impero Security Server on the same computer. To run Impero Security Management with a working Security Database, install Impero Security Manager on the workstations of Impero Security Management administrators. Its full functionality is available only if installed on a networked Windows 2003, XP, 2000 or NT computer. The Impero Security Manager program amconfig.exe resides in the directory where Impero Security Manager is installed.

To load Impero Security Manager, select **Start > All Programs > Impero Connect > Security Manager** or run its program file amconfig.exe.

Initially, this window is displayed in front of the Impero Security Manager window:

![Initial window](image)

The pane displays a tip to Impero Security Manager.

**Close:** Click on this button to close the window.

**Next Tip:** Click on this button to show another tip in the pane.

**Show tips on startup:** Leave this box checked to show this window when loading Impero Security Manager. Uncheck to not show it. If suppressed, you can show it from the Help menu Tip of the Day command.

This window is displayed in front of the empty Impero Security Manager window:

![Empty window](image)

It logs on to a data source to create or open a Impero Security Database in it.

**Create local test database:** Check this box to disable the fields below to create a local test database on your computer.

*Note:* If you are loading Impero Security Manager for the first time, we recommend that you create a local test database to try out Impero Security Manager before creating a working Security Database. Creating a local test database requires administrator rights on the computer. Generally, you should not use the local test database as a working Security Database.

**Data source []:** By default, this field displays Impero_Security_Evaluation to log on to the local test database. To create or log on to a working Security Database, specify the data source name (DSN) of the database in which the Security Database shall reside or resides.

**Username []:** Specify in this field the user name required to log on to the database in which the Security Database shall reside or resides. The local test database requires no user name.

**Password []:** Specify in this field the matching password. The local test database requires no password.

**Change...:** Click on this button to show the Windows Select Data Source window to select a data source whose name is displayed in the Data source field.

**Exit:** Click on this button to close the window and the Impero Security Manager window behind it to unload Impero Security Manager.

**Logon:** Click on this button to log on to the specified data source with one of the following results:

- If the specified data source contains Security Database Tables, the Impero Security Manager window is displayed.
- If the Create local test database box was checked before clicking Logon, this window is displayed:
It shows that the local test database with the data source name `Impero_Security_Evaluation` is created in the file `ameval.mdb` that resides in the path `C:\Documents and Settings\All Users\Application Data\Impero\NSS`. Click on **OK** to run the Security Database Wizard to create the local test database.

- If the specified data source contains no Security Database Tables, the Security Database Wizard runs to create them.
- If the specified data source cannot be opened, this window is displayed:

![Error Message]

It indicates that invalid data source credentials were specified or Security Database Tables are corrupted. The Security Database Wizard cannot repair corrupted Security Database Tables. If you cannot repair corrupted Security Database Tables manually, delete them and Load Impero Security Manager to create Security Database Tables with the Security Database Wizard.

See also

- Local test database
- Impero Security Server Setup
- Security Database Setup
- Impero Security Manager window
- Data source
- Create local test database
- Security Database Tables
- Security Database Wizard
- Load Impero Security Manager

2.2.1 Security Database Wizard

If no Security Database Tables exist when logging on to the Security Database, the Security Database Wizard runs:

![Error Message]

The Public Key is used to secure a trusted connection between your Hosts and Security Servers.

Either use the default Public Key or generate a new Public Key. For production environments, it is recommended to generate a new Public Key before deploying your Hosts. Whenever you change the Public Key, you need to also change the Public Key used on your Hosts.

Click on **Next** to show this window:

![Next Window]

As stated in the text in the window, the Group functionality is displayed for compatibility with previous version. It is recommended that you update your Hosts and use Public Key instead.

- **Group Name (Private) []**: By default, Impero is specified in this field. Characters are displayed as dots or asterisks. Leave this name to try out Impero Security Management. To create a working Security Database, specify another private Group name that should be known only among Impero Security Management administrators.

- **Confirm Group Name []**: Re-specify in this field the private Group name for confirmation.

- **Group ID (Public) []**: This field displays the 32-digit hexadecimal checksum generated from the private Group name. This is the Group ID that must be specified on Hosts that use this security server group.

Click on **Next** to show this window:

![Next Window]

It specifies security server group members and enables Impero Access Server compatibility.
To try out Impero Security Management, click on Add to create a record of the Impero Security Manager computer in the pane as shown in the image. To add further members to the group and enable Impero Access Server compatibility, see the Security Server List section.

Click on Next to show this window:

It specifies the type of credentials that Hosts shall request from connecting Guests.

Select one of these options:

- **Guests enter Windows username and password**: Hosts shall request Windows credentials (User name, Password, Domain) (default selection).
- **Guests enter Impero Guest ID and password**: Hosts shall request proprietary Impero credentials (Guest ID, Password).
- **Guests enter RSA SecurID username and passcode**: Hosts shall request RSA SecurID credentials (User name, (password), PASSCODE) if they can.
- **Guests enter Directory Services username and password**: Hosts shall request Directory Services credentials via LDAP (User name, password, Directory Server).

Non-Windows Guests such as Linux or Mac do not support Windows Definitions, RSA SecurID Definitions or Directory Services Definitions and can request only Impero credentials. If Impero Security Management shall support such Guests, Role Assignments based on Guest Impero Definitions must be available in the Security Database.

Click on Next to show this window:

It specifies how Hosts shall identify themselves to the Impero Security Server.

Select one of these options:

- **Windows user if one is logged on, otherwise workstation**: Hosts shall identify themselves by any logged on Windows User or if no user is logged on by the Windows computer name (default selection).
- **Always the workstation**: Hosts shall always identify themselves by the Windows computer name.
- **Impero Host ID**: Hosts shall identify themselves by their Impero Host ID. This is the value defined within the Host application itself. By default, this value matches the computer name.

Non-Windows Hosts such as Linux or mac do not support Windows Definitions and always identify themselves by their Impero Host ID. If Impero Security Management shall support such Hosts, Role Assignments based on their Host Impero Definitions must be available in the Security Database.

Click on Finish to end the Security Database Wizard to show the Impero Security Manager window.

See also

- Security Database Tables
- Security Database Setup
- Security Policies
- Security Server Group Name
- Impero Security Management
- Impero Security Manager window
- Security Server List
- Preferred Guest Type
- Role
- Role Assignment
2.3 Impero Security Manager Window

After logon to the Security Database, this window is displayed:

It contains these elements:
- **Title Bar**
- **Menu Bar**
- **Toolbar**
- **Filter and Fetching Bar**
- **Records panel with a left Selection Pane and a right Records Pane**
- **Message Panel**
- **Status Bar**

**See also**
*Security Database*

2.3.1 Title Bar

This is the Impero Security Manager Window title bar:

It displays the name of the logged on to data source.

**See also**
*Impero Security Manager window*

2.3.2 Menu Bar

This is the Impero Security Manager window menu bar:

It contains these menus:
- **File Menu**
- **Records Menu**
- **Edit Menu**
- **View Menu**
2.3.2.1 File Menu

This is the Impero Security Manager window File menu:

Exit: Select this command or a window control Close control to close the Impero Security Manager window and unload Impero Security Manager.

See also

Impero Security Manager window

2.3.2.2 Records Menu

This is the Impero Security Manager window Records menu:

Expanding commands manage Security Database records as explained in Manage Security Database Contents.

Import data: Select this command to import roles an definitions from an xml file; for more information see Importing Roles and Definitions.

Reset All: Select this command to show a confirmation window to confirm deleting all Security Database Tables and run the Security Database Wizard to create empty Security Database Tables.

EXTREME CAUTION: Selecting this command may waste hours of work and leave Impero Security Servers unable to service Impero modules that depend on them until security data have been re-created. Select this command only if you are absolutely certain that you want to start all over creating security data.

Drop All Tables: Select this command to delete all data in existing database tables. The setup wizard starts automatically upon the next restart.

See also

Impero Security Manager window
Security Database Setup
Security Database Tables
Security Database Wizard
Impero Security Servers

2.3.2.3 Edit Menu

This is the Impero Security Manager window Edit menu:

Copy Ctrl+C: Select text in the Message Panel and select this command or press CTRL+C to copy the selection to the clipboard.

See also
2.3.2.4 View Menu

This is the Impero Security Manager window View menu:

**Toolbar**: This command expands into the commands:

- **No Toolbar**: Select this command to hide the toolbar.
- **Large Toolbar**: Select this command to show large icons in the toolbar.
- **Small Toolbar**: Select this command to show small icons in the toolbar (default selection).
- **Security Settings**: Select this command to check mark/uncheck it to show/hide the Selection Pane Security Settings branch (default: check marked to be shown).
- **Logging**: Select this command to check mark/uncheck it to show/hide the Selection Pane Logging branch (default: check marked to be shown).
- **Scheduling**: Select this command to check mark/uncheck it to show/hide the Selection Pane Scheduling branch (default: check marked to be shown).
- **Impero Definitions**: Select this command to check mark/uncheck it to show/hide the Selection Pane Impero Definitions branch (default: unchecked to be hidden).
- **Windows Definitions**: Select this command to check mark/uncheck it to show/hide the Selection Pane Windows Definitions branch (default: check marked to be shown).
- **RSA SecurID Definitions**: Select this command to check mark/uncheck it to show/hide the Selection Pane RSA SecurID Definitions branch (default: unchecked to be hidden).
- **Directory Services Definitions**: Select this command to check mark/uncheck it to show/hide the Selection Pane Directory Services Definitions branch (default: unchecked to be hidden).
- **Messages**: Select this command to check mark/uncheck it to show/hide the Message Panel (default: check marked to be shown).
- **Clear Messages (CTRL+M)**: Select this command or press CTRL+M to delete the Message Panel contents.
- **Status Bar**: Select this command to check mark/uncheck it to show/hide the Status Bar.

See also

- Impero Security Manager window
- Toolbar
- Selection Pane
- Security Settings
- Logging
- Scheduling
- Impero Definitions
- Windows Definitions
- RSA SecurID Definitions
- Directory Services Definitions
- Message Panel
- Status Bar
2.3.2.5 Options Menu

This is the Impero Security Manager window Options menu:

**Program Options...**: Select this command to show this window:

**Number of records to fetch at a time (0-50, 0=all) []**: Impero Security Manager fetches Security Database records to the Records Pane in batches. Specify in the field a number in the range (default: 50).

**Automatic Refresh**: Leave this box checked to automatically refresh the Records Pane contents whenever a record is changed (default: checked).

**Note**: Refresh discards the Records Pane contents and fetch Security Database records. Refresh manually by clicking the Filter and Fetching Bar Refresh button or pressing F5.

**Confirm Successful Changes**: Check this box to show a window to confirm each successful Records Pane record change (default: unchecked).

**SQL Debug Messages**: Check this box to show SQL debug messages in the Message Panel (default: unchecked).

**Validate LDAP connections at startup**: Leave this box checked to prevent any authentication problems when using Directory Services as your preferred Guest-Type (default: checked).

When this option is selected, any LDAP connections that fail to validate during startup results in a message similar to the one below:

The dialog shows the failed connections and enables you to edit them.

**NOTE**: When using Active Directory with one or more trusted domains, it is essential to use an Encrypted bind under the Credentials tab. The credentials must also be entered using an accepted format as shown in the following table:

<table>
<thead>
<tr>
<th>Encrypted bind</th>
<th>Non-Encrypted bind</th>
</tr>
</thead>
<tbody>
<tr>
<td>username@domain</td>
<td>domain\username</td>
</tr>
<tr>
<td>domain\username</td>
<td>cn=username, ou=container, dc=domain</td>
</tr>
</tbody>
</table>

With Encrypted bind, domain can be NetBIOS or FQDN name.

With Non-Encrypted bind, domain must be NetBIOS name when not using the Distinguished Name

See also

- Impero Security Manager window
- Security Database
- Records Pane
- Security Database Setup
- Filter and Fetching Bar
- Message Panel

2.3.2.6 Help Menu

This is the Impero Security Manager window Help menu:
Online Help: Select this command or press F1 to open the Impero Security Manager Help system on the topic of the currently or most recently shown Records Pane.

Help on Viewing: Select this command to open the Impero Security Manager Help system on the View and Manage Data topic.

Tip of the Day: Select this command to show the Tip of the Day window.

About Impero Security Manager: Select this command to show this window:

This window specifies the Impero Security Manager version and build number (in parentheses).

Note: These numbers are asked for if you request support for Impero Security Manager.

See also

Impero Security Manager window
Records Pane
View and Manage Data
Tip of the Day

2.3.3 Toolbar

From the expanding View menu toolbar command, you can hide/show the Impero Security Manager window toolbar and select two toolbar sizes:

Small Toolbar (default selection):

Large Toolbar:

NOTE: To include Impero Definitions buttons in the toolbar, while the Impero Definitions branch is shown in the Selection Pane select in the View menu Small Toolbar or Large Toolbar.

The toolbar can contain these buttons:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="F2" alt="New Role Assignment" /></td>
<td>Click this button, press F2 or select the Role Assignment menu New command to show the Role Assignment Wizard.</td>
</tr>
<tr>
<td><img src="F3" alt="New Impero Guest ID" /></td>
<td>Click this button, press F3 or select the Impero Guest ID menu New command to show the Impero Guest ID window.</td>
</tr>
<tr>
<td><img src="F4" alt="New Impero Guest ID Group" /></td>
<td>Click this button, press F4 or select the Impero Guest ID Group menu New command to show the Impero Group window.</td>
</tr>
<tr>
<td><img src="F6" alt="New" /></td>
<td>Click this button, press F6 or select the Impero Host ID menu New command to show the Impero Host ID window.</td>
</tr>
<tr>
<td><strong>Impero Host ID (F6)</strong></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>---</td>
</tr>
<tr>
<td><strong>New Impero Host ID Group (F7)</strong></td>
<td>Click this button, press F7 or select the <strong>Impero Host ID Group</strong> menu <strong>New</strong> command to show the <strong>Impero Group</strong> window.</td>
</tr>
<tr>
<td><strong>New Role (F9)</strong></td>
<td>Click this button, press F9 or select the <strong>Role</strong> menu <strong>New</strong> command to show the <strong>Impero Security Role</strong> window.</td>
</tr>
<tr>
<td><strong>New Scheduled Job (F10)</strong></td>
<td>Click this button, press F10 or select the <strong>Scheduled Jobs</strong> menu <strong>New</strong> command to show the <strong>Scheduled Job Wizard</strong>.</td>
</tr>
<tr>
<td><strong>Edit Selected (Ctrl+E)</strong></td>
<td>Select a Records Pane record and click this button, press CTRL+E or select the <strong>Record Type</strong> menu <strong>Edit</strong> command to show the record editing window.</td>
</tr>
<tr>
<td><strong>Delete Selected (Ctrl+D)</strong></td>
<td>Select a Records Pane record and click this button, press CTRL+D or select the <strong>Record Type</strong> menu <strong>Delete</strong> command to show a confirmation window to confirm deleting the record.</td>
</tr>
<tr>
<td><strong>Large Icons</strong></td>
<td>Click this button to make it appear pressed in to show <strong>Records Pane</strong> records as horizontal rows of large icons.</td>
</tr>
<tr>
<td><strong>Small Icons</strong></td>
<td>Click this button to make it appear pressed in to show <strong>Records Pane</strong> records as horizontal rows of small icons.</td>
</tr>
<tr>
<td><strong>List</strong></td>
<td>Click this button to make it appear pressed in to show <strong>Records Pane</strong> records as vertical columns of small icons.</td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>Click this button to make it appear pressed in to show <strong>Records Pane</strong> records in a table with details in columns (default selection).</td>
</tr>
</tbody>
</table>

**See also**

- View Menu
- Toolbar
- Impero Security Manager window
- Small Toolbar
- Large Toolbar
- Impero Definitions
- Selection Pane
- Role Assignment
- Role Assignment Wizard
- Impero Guest ID
- Impero Host ID
- Impero Guest ID Group
- Role
- Scheduled Jobs
- Records Pane
2.3.4 Filter and Fetching Bar

This is the Impero Security Manager window filter and fetching bar:

It can specify a filter criterion and contains a Refresh button and if more records than are shown in the Records Pane are available in the Security Database One More Lot and All Remaining record fetching buttons.

Where: Check this box to enable the drop-down boxes to the right to specify a filter criterion that is applied when fetching records from the Security Database (default: unchecked).

The list of the left drop-down box list contains the Records Pane Details show column names. Select a column name in the list to show it in the field to filter fetched records by the selected name column.

The list of the middle drop-down box contains these operators:

- LIKE: Selects records that in the selected column contain the string of characters that is specified in the right drop-down box field (default selection).
- =: Selects records that in the selected column contain a numerical value that is equal to the numerical value that is specified in the right drop-down box field.
- >: Selects records that in the selected column contain a numerical value that is larger than the numerical value that is specified in the right drop-down box field.
- <: Selects records that in the selected column contain a numerical value that is smaller than the numerical value that is specified in the right drop-down box field.

The list of the right drop-down box contains strings of characters and numerical values that have been specified before (default: none). Select a string or value in the list to show it in the field or specify a new string or value in the field.

NOTE: Strings of characters can contain wildcard characters. Use the wildcard characters specified by the Security Database data source type.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Refresh]</td>
<td>Click on this button or press F5 to discard all Records Pane records and fetch from the Security Database applying any filter criterion specified to the left up to the number of records specified in the Program Options window to the Records Pane.</td>
</tr>
<tr>
<td>![One More Lot]</td>
<td>This button is displayed if more records than are shown in the Records Pane are available in the Security Database. Click it or press CTRL+PAGEDOWN to fetch from the Security Database applying any filter criterion specified to the left up to the number of records specified in the Program Options window to the Records Pane.</td>
</tr>
<tr>
<td>![All Remaining]</td>
<td>This button is displayed if more records than are shown in the Records Pane are available in the Security Database. Click it or press ALT+PAGEDOWN to fetch from the Security Database applying any filter criterion specified to the left all remaining records to the Records Pane.</td>
</tr>
</tbody>
</table>

See also

- Impero Security Manager window
- Records Pane
- Security Database Setup
- One More Lot
- All Remaining
- Program Options window
2.3.5 Selection Pane

This is the Impero Security Manager window records panel left selection pane:

It contains Records Pane commands in a tree structure.

**NOTE:** By default, the Selection Pane is below the Impero Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

Collapse or expand branches by clicking the - + buttons.

Select an expanded branch command to dim its icon and bold its name to show its records in the Records Pane.

**See also**

Impero Security Manager window
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu

2.3.6 Records Pane

This is the Impero Security Manager window records panel right records pane:

It displays records according to the Selection Pane selection. To show another records pane, select it in the Selection Pane.

Click on a toolbar show button to change how records is displayed. Large Icons, Small Icons and List buttons displays the records as icons. The Details button displays the records in a table with details in columns. Column names are Security Database table column names that cannot be changed.

Showing a records pane, records are fetched from the Security Database according to Program Options window and Filter and Fetching Bar settings to become shown in the Records Pane.

The contents of the individual records panes are explained in the Manage Security Database Contents section in the Records menu order.

**See also**

Impero Security Manager window
Selection Pane
Toolbar
Security Database Setup
Program Options window
Filter and Fetching Bar
Manage Security Database Contents
Records Menu
2.3.7 Message Panel

This is the Impero Security Manager window message panel:

It is displayed unless hidden from the View menu Messages command. It displays Impero Security Manager messages and can, if selected in the Program Options window, also show SQL debug messages.

Drag the lower border of the Impero Security Manager window to adjust the height of the message panel. You can scroll the message panel show with its scrollbars.

Select the View menu Clear Messages command or press CTRL+M to delete all message panel messages.

In the message panel, select text or in the message panel context menu select Select All to select the entire message panel contents and in the Edit menu or context menu select Copy or press CTRL+C to copy selected text to the clipboard.

See also
- Impero Security Manager window
- View Menu
- Program Options window
- Edit Menu

2.3.8 Status Bar

This is the Impero Security Manager window status bar:

It is displayed unless hidden from the View menu Status Bar command.

When the mouse pointer is over a menu command or a toolbar button, the left end of the status bar displays a hint to the command or button.

See also
- Impero Security Manager window
- View Menu
- Toolbar

2.4 Manage Security Database Contents

This section explains how to manage the contents of an Impero Security Database from Impero Security Manager. It includes these sections:

- Contents Creation Guide
- Security Settings
- Logging
- Scheduling
- Impero Definitions
- Windows Definitions
- RSA SecurID Definitions
- Directory Services Definitions
If you are new to Impero Security Management, we recommend that you read the Contents Creation Guide before creating Security Database contents.

See also

Security Database Setup
Contents Creation Guide

2.4.1 Contents Creation Guide

This guide introduces you to the main tasks of making your Security Database ready to service Impero Connect modules installed on the computers of your organization. It contains these sections:

- Review Security Policies
- Create Role Assignments
- View and Manage Data
- Scheduled Jobs
- Security Log
- Impero Log
- Active Sessions

See also

Security Database Setup

2.4.1.1 Review Security Policies

Before creating any other Security Database contents, you should review the Security Policies created in the Security Database Wizard to align them with the desired Impero Security Management setup.

The selected Preferred Guest Type and Preferred Host Type determines which basic Guest and Host records must be created.

If Impero Security Management shall run in a Windows domain environment, typically set the Preferred Guest Type to guests to enter Windows user name and password.

If your organization applies a policy of RSA SecurID authentication, set the Preferred Guest Type to guests enter RSA SecurID user name and PASSCODE.

If your organization applies a policy of Directory Services authentication, select the Preferred Guest Type to guests enter Directory Services user name and password.

Regarding Preferred Host Type, in a Windows domain environment typically select Windows user if one is logged on, otherwise workstation to enable applying Host computer user dependent Role Assignments. To apply only Host computer dependent Role Assignments, select Always the workstation.

If you are connecting to non-Windows Hosts such as Linux or Mac, you should use Impero Host ID as preferred Host Type.

See also

Security Database Setup
Security Policies
Security Database Wizard
Preferred Guest Type
Preferred Host Type
AMPLUS.EXE
Role Assignment
2.4.1.2 Create Role Assignments

The main objective of creating Security Database contents is to create mutual Role Assignments between all users and computers that shall be serviced by Impero Security Management.

You can swiftly create Role Assignments mutually between multiple Windows Groups as Guest and Host selection and with Windows Domain computers as Host selection in a batch operation from the Role Assignment menu New Batch command.

You can create Role Assignments one by one between any Guest selection and any Host selection from the Role Assignment menu New command or the toolbar New Role Assignment button.

While Role Assignments with Windows Definitions and Directory Services Definitions records do not require that Guest and Host selection records have been created, Role Assignments with Impero Definitions and RSA SecurID Definitions require that Guest and Host selection records have been created.

Impero Security Manager comes with four built-in Roles of which two can be edited. You can create additional Roles from the Role menu or from the toolbar New Role button.

See also
Security Database Setup
Role Assignment
Windows Groups
Windows Domain
Toolbar
Windows Definitions
Directory Services Definitions
Impero Definitions
RSA SecurID Definitions
AMPLUS.EXE
Role

2.4.1.3 View and Manage Data

Security Database data can be shown in the Impero Security Manager window records panel that contains a left Selection Pane and a right Records Pane. Click an element in the Selection Pane to show its records in the Records Pane.

NOTE: By default, the Selection Pane does not display Impero Definitions, RSA SecurID Definitions and Directory Services Definitions elements. You can show them from the View menu.

Records can be shown as icons (Large Icons, Small Icons or List), but typically they are displayed in a table with Details in columns. Details table contents match the contents of Security Database Tables.

Records are fetched from the security database in lots, the size of which can be set in the Program Options window. If the Security Database contains more records than are currently in the Records Pane, two yellow buttons is displayed next to the Filter and Fetching Bar Refresh button:

Click on the left One More Lot button with a down pointer or press CTRL+PAGEDOWN to fetch another lot into the Records Pane. Click the right All Remaining button with a down pointer and a line or press ALT+PAGEDOWN to fetch all remaining records into the Records Pane.

Click on the Refresh button to clear the Records Pane to fetch a new lot of records. In the Program Options window, you can select to refresh automatically when the Records Pane contents have been changed.
You can sort **Records Pane** data ascending or descending by clicking a column heading. Sorting initiates a new fetching of records from the Security Database.

You can filter **Records Pane** records by specifying a filter criterion in the **Filter** and **Fetching Bar**. Filtering initiates a new fetching of records from the Security Database.

To edit a **Records Pane** record, double-click on it, select the record type menu **Edit** command, click on the toolbar **Edit Selected** button or press CTRL+E.

To delete a **Records Pane** record, select the record type menu **Delete** command, click on the toolbar **Delete Selected** button or press CTRL+D.

**Note:** Other options are available in some record type menus.

**See also**

- **Security Database Setup**
- **Impero Security Manager window**
- **Selection Pane**
- **Records Pane**
- **Impero Definitions**
- **RSA SecurID Definitions**
- **Directory Services Definitions**
- **View Menu**
- **Security Database Tables**
- **Program Options window**
- **Filter and Fetching Bar**
- **Toolbar**

### 2.4.1.4 Scheduled Jobs

**Scheduled Jobs** specify temporary enabling of groups (Windows Groups, Impero Guest ID Groups or Impero Host ID Groups) once or according to a weekly schedule. Create Scheduled Jobs to allow Guest connections to Hosts only in specified time intervals.

**See also**

- **Scheduled Jobs**
- **Windows Groups**
- **Impero Guest ID Groups**
- **Impero Host ID Groups**

### 2.4.1.5 Security Log

Administrator actions from **Impero Security Manager** are logged in the Security Database. You can show these loggings in the **Security Log** to track when changes were made to the Impero Security Management setup. You can clean up the **Security Log** manually from the **Security Log** menu and automatically from the **Logging Options** window.

**See also**

- **Security Database**
- **Security Log**
- **Logging Options**

### 2.4.1.6 Impero Log

Impero modules can log their Impero events in the Security Database. You can show these loggings in the **Impero Log**. You can clean up the **Impero Log** manually from the **Impero Log** menu and automatically from the **Logging Options** window.

**See also**

- **Security Database Setup**
- **Impero Log**
Logging Options

2.4.1.7 Active Sessions

Provided that Hosts log their session events in the Security Database, the Active Sessions Records Pane displays which sessions are currently running with logging Hosts. Active Sessions records refresh automatically every ten seconds. You can refresh manually from the Active Sessions menu or from the Filter and Fetching Bar Refresh button. You can clean up Active Sessions records automatically from the Logging Options window.

See also
Security Database Setup
Active Sessions Records Pane
Filter and Fetching Bar
Logging Options

2.4.2 Security Settings

You can manage Security Settings records from the Records menu Security Settings submenu:

which contains these commands:

- Role Assignment
- Role

You can also manage Security Settings records from the Selection Pane Security Settings branch:

which includes these commands:

- Role Assignments
- Roles
- Security Policies

NOTE: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

See also
Records Menu
Role Assignment
Selection Pane
Security Settings
Security Policies
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
2.4.2.1 Role Assignment

Select the Selection Pane Security Settings branch Role Assignments command to show this Records Pane:

NOTE: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the Role Assignments as named icons or table records. The Details selection displays the table records with these column contents:

- **Guest**: Guest selection icon and name.
- **Host**: Host selection icon and name.
- **Role**: Role icon and name.
- **Enabled**: Check mark (enabled) or red dot with white X (disabled).
- **ID**: Record number (records are numbered starting from 1).
- **Created**: Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- **CreatedBy**: Creator Windows user name.
- **Modified**: Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- **ModifiedBy**: Modifier Windows user name.

Manage Role Assignments from the Records menu Role Assignment submenu:

- or from the matching Role Assignments Records Pane context menu:

It contains these commands:

- **New**
- **New Batch**
- **Edit**
- **Delete**
- **Clear**

NOTE: For a quick start, create Role Assignments between Windows groups and with Windows Domains from the New Batch command.

See also

Selection Pane  
Security Settings  
Records Pane  
Logging  
Scheduling  
Windows Definitions  
Impero Definitions  
RSA SecurID Definitions  
Directory Services Definitions  
View Menu  
Toolbar
Role
Records Menu
Windows groups
Windows Domains

2.4.2.1.1 New

Select the Role Assignment menu New command, click the toolbar New Role Assignment button with a traffic light or press F2 to run the Role Assignment wizard to show this window:

This wizard creates a Role Assignment record.

Click on Back to show an explanation.

Wizard windows displays the options to the left and specifications to the right. Suggested or completed specifications is displayed in black text. Missing specifications is indicated by red text.

This window selects a Guest type (suggested: Windows Group). Select a Guest type option to the left to show it in the right Guest specification after clicking on Next.

If on a Windows 2000+ computer you select Windows User or Windows Group, the matching Windows Select... window is displayed after clicking on Next. When you have selected a Windows account, the Insert <Account type> as Guest is displayed.

If you select Everybody, then the Select Host Type window is displayed after clicking on Next.

Tip: Choosing Directory Services options

If you choose a Guest or Host type which is a Directory Service user, group or organizational unit and your Directory Service connection uses Active Directory, the following dialog box in the wizard shows an LDAP (Lightweight Directory Access Protocol) search field.

Use the filter option to quickly locate the Active Directory object you are looking for rather than browse the entire Active Directory.

Using the filter also improves the ability to locate objects within an Active Directory that has page size limitations. Active Directory controls the maximum number of objects that can be returned in a single search using LDAP and this value is set to 1000 objects, by default.

Otherwise, this window is displayed after clicking on Next:

It specifies a Guest selection.

If a Windows account was selected in a Windows Select... window, disabled left drop-down box fields displays the domain and account and the right Guest specification displays the account name prefixed by its relative identifier number (RID) and the domain name.

Otherwise, enabled selection elements are displayed to the left. Only Windows accounts or names of records that have been created in Impero Security Manager is available for selection. Select actively an element to specify it in the right Guest specification immediately or after clicking on Next.

When you have made a valid selection, click on Next to show this window:
It selects a Host type (suggested: Windows Group). Select a left Host type option to show it in the right Host specification after clicking on Next.

**NOTE:** If Everybody was selected in the Select Guest Type window, all users are disabled in this window. However, if you select Everybody in this window, all users are enabled in the Select Guest Type window.

If on a Windows 2000+ computer you select Windows User or Windows Group, the matching Windows Select... window is displayed after clicking on Next. When you have selected a Windows account, the Insert <Account type> as Host window is displayed.

If you select Everybody, the Insert Role Assignment window is displayed after clicking on Next.

Otherwise, this window is displayed after clicking on Next:

---

It specifies a Host selection.

If a Windows account was selected in a Windows Select... window, disabled left drop-down box fields displays the domain and account and the right Host specification displays the account name prefixed by its relative identifier number (RID) and the domain name.

Otherwise, enabled selection elements are displayed to the left. Only Windows accounts or names of records that have been created in Impero Security Manager are available for selection. Select actively an element to specify it in the right Host specification immediately or after clicking on Next.

**NOTE:** If Impero Guest ID or Impero Guest ID Group was selected in the Select Guest Type window and Impero Host ID Group was selected in the Select Host Type window, the Insert Impero Host ID Group as Host window includes the option Unregistered Host IDs that enables a Role Assignment with Host IDs for which no record exists in Impero Security Manager. Selecting this option that is provided for compatibility with older versions Impero Access Server is not recommended.

When you have made a valid selection, click on Next to show this window:

---

It specifies the Role that applies to the created Role Assignment.

**Enter first character below and select from list []**: In the field, replace * designating any characters by the first letters of a Role name to show in the pane below only Role names that begin with these letters.

**New**: Click on this button to show the Impero Security Role window to create a Role.

In the pane, select a Role name to show it in the right Role specification prefixed by the Role record number.

**Finish**: This button becomes enabled when a valid Role Assignment has been specified. Click on it to end the wizard to create the Role Assignment record.

**See also**
- Role Assignment Toolbar
- Role
- Impero Security Role window

**2.4.2.1.2 New Batch**

Select the Role Assignment menu New Batch command to run the Initial Setup wizard to show this window:
This wizard creates Role Assignments between multiple *Windows Groups* and *Windows Domains* and edit built-in Roles in a batch operation. The left section contains selection drop-down boxes and the right pane contains selection records (initially none).

**Domain []**: The list of this drop-down box contain the names of the Windows domains recognized by the Impero Security Manager computer. Select a domain name in the list to show it in the field.

**Windows Group []**: The list of this drop-down box contains the names of the Windows groups in the domain selected in the *Domain* drop-down box and `<Include access to domain>`. Select a Windows group to create Role Assignments with this Windows Group as Guest and Host selections. Select `<Include access to domain>` to create Role Assignments with the Windows Domain selected in the *Domain* drop-down box as Host selection.

**Note**: `<Include access to domain>` applies to Hosts that identify themselves to Impero Security Server as a workstation, not as a user, see Preferred Host Type.

**Role []**: The list of this drop-down box contains the names of the roles specified in the *Roles* Records Pane. Select a role in the list to show it in the field to apply it to a *Windows Group* drop-down box *Windows Group* selection as *Guest* selection with all *Windows Group* and *Windows Domain* records in the right pane as Host selection. This selection does not apply to a *Windows Group* drop-down box `<Include access to domain>` selection.

**Add**: Click this button to add a selection in the left drop-down boxes as a record in the right pane.

**Del**: Select a record in the right pane and click this button to delete it.

The right pane displays the records of selected *Windows Groups* and *Windows Domains* in a table with these column contents:

- **Windows user**: Group/domain icon and *Windows Group* name or *Domain*.
- **Role**: For a *Windows Group* record the Role record ID and RoleName values. For a *Domain* record the Role 0: To be used as Host.
  
  **Note**: A *Windows Group* record Role applies to the *Windows Group* as Guest selection with all *Windows Group* and *Windows Domain* pane records as Host selection.

- **Domain**: *Windows Group* or *Domain* record *Windows Domain* name.

  **NOTE**: Role Assignment records and selected *Windows Group* and *Windows Domain* records is created in the Security Database if they do not already exist.

Click on **Next** to show this window:

[Next]

In this window, you can review or edit two of the four built-in Roles and select to replace existing Role Assignments.

**Standard Role**: Click on this button to show the *Impero Security Role* window to review or edit the built-in Standard Role.

**Unassigned Hosts’ Role**: Click on this button to show the *Impero Security Role* window to review or edit the built-in Unassigned Hosts’ Role.

**Clear all existing role assignments before making these new ones**: Check this box to replace all existing Role Assignments by those created in the Initial Setup of Guests and Hosts window.

Click on **Back** to return to the Initial Setup of Guests and Hosts window.

Click on **Finish** to end the wizard to apply selections.

See also

- Role Assignment
- Windows Group
- Windows Domain
- Role
- Preferred Host Type
Records Pane
Security Database Setup
Impero Security Role window

2.4.2.1.3 Edit

Select a Role Assignment record and select the Role Assignment menu Edit command, click the toolbar Edit Selected button, press CTRL+E or double-click a Role Assignment record to show this window:

It edits a Role Assignment record.

Guest, Host, Old Role []: These disabled fields display the record Guest selection name, Host selection name and Role name.

New role []: This pane displays the names of available Roles. Select one to replace the record Role.

Record is disabled: Check this box to disable the record (default: unchecked). Impero Security Management does not use a disabled Role Assignment record.

NOTE: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also
Role Assignment Toolbar Role

2.4.2.1.4 Delete

Select Role Assignment records and select the Role Assignment menu Delete command, click the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

NOTE: Role Assignment records of deleted Guest or Host selection records are deleted.

See also
Role Assignment Toolbar

2.4.2.1.5 Clear

Select the Role Assignment menu Clear command to show a confirmation window to confirm deleting all Role Assignment records.

Caution! If no Role Assignment records exist, the Unassigned Hosts' Role applies to all existing Guest and Host selections.

See also
Role Assignment Role

2.4.2.2 Role

Select the Selection Pane Security Settings branch Roles command to show this Records Pane:

NOTE: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero
Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the Roles as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RoleName</td>
<td>Role icon and name.</td>
</tr>
<tr>
<td>Rctl</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Connect (View).</td>
</tr>
<tr>
<td>Keyb</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Use keyboard and mouse.</td>
</tr>
<tr>
<td>Lckm</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Lock keyboard and mouse.</td>
</tr>
<tr>
<td>Blnk</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Blank the screen.</td>
</tr>
<tr>
<td>Clip</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Transfer clipboard.</td>
</tr>
<tr>
<td>Boot</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Execute command.</td>
</tr>
<tr>
<td>Chat</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request chat.</td>
</tr>
<tr>
<td>Audi</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request audio-video chat.</td>
</tr>
<tr>
<td>Vide</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request video.</td>
</tr>
<tr>
<td>Send</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send files to Host.</td>
</tr>
<tr>
<td>Recv</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Receive files from Host.</td>
</tr>
<tr>
<td>RunP</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Run programs.</td>
</tr>
<tr>
<td>Prnt</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Redirect print.</td>
</tr>
<tr>
<td>Mana</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Remote management.</td>
</tr>
<tr>
<td>Inve</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Retrieve inventory.</td>
</tr>
<tr>
<td>Smsg</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send message.</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Mjoi</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Join multi Guest session.</td>
</tr>
<tr>
<td>Madm</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Act as multi Guest session administrator.</td>
</tr>
<tr>
<td>Demo</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Demonstrate</td>
</tr>
<tr>
<td>Tunn</td>
<td>Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Tunnel</td>
</tr>
<tr>
<td>AllowedPorts</td>
<td>(list of allowed ports to be used through tunnel) Allowed Tunnel ports</td>
</tr>
<tr>
<td>BlockedPorts</td>
<td>(list of blocked ports that cannot be used through tunnel) Blocked Tunnel ports</td>
</tr>
<tr>
<td>Conf</td>
<td>Confirm access: No (red X), Yes (check mark) or Yes, with exception (check mark).</td>
</tr>
<tr>
<td>Computer locked</td>
<td>Exception applies (check mark)/Exception does not apply (red X).</td>
</tr>
<tr>
<td>No user logged on</td>
<td>Exception applies (check mark)/Exception does not apply (red X).</td>
</tr>
<tr>
<td>Guest user logged on</td>
<td>Exception applies (check mark)/Exception does not apply (red X).</td>
</tr>
<tr>
<td>Description</td>
<td>Fixed role, Role can be modified, but not deleted or &lt;User specified&gt;.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
</tbody>
</table>

Initially, four built-in Roles exist:

- **Full Control**: Allows all available Guest actions. Fixed Role that can be neither modified nor deleted.
- **No Access**: Allows no Guest actions. Fixed Role that can be neither modified nor deleted.
- **Standard Role**: Allows selected Guest actions (initially Connect (view), Request chat and Receive files from Host). Role can be modified but not deleted.
- **Unassigned Hosts' Role**: Applies if no Role is assigned between existing Security Database records of a Guest selection and a Host selection. Allows selected Guest actions (initially none). Role can be modified but not deleted.

Manage Roles from the Records menu Role submenu:
It contains these commands:

- **New**
- **Edit**
- **Delete**

**See also**
- Selection Pane
- Security Settings
- Records Pane
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions

**2.4.2.2.1 New**

Select the Role menu *New* command, click the toolbar *New Role* button with a padlock or press F9 to show this window:

![New Role Window]

It specifies a Role record.

**Name:** [ ]: This field contains the Role name.

**Description:** [ ]: This field can contain a Role description that is displayed in the Role Records Pane **Description** column.

**Allow:** Check a box to allow the action to a Guest connected to a Host. Uncheck to not allow. *Connect* sub-action check boxes are enabled only if the *Connect (View)* box is checked. If multiple Role Assignments apply, an action being allowed in any applicable Role Assignment overrides this action not being allowed in other applicable Role Assignment.

**Deny:** Check a box to deny the action to a Guest connected to a Host. Uncheck to not deny. *Connect* sub-action check boxes are enabled only if the *Connect (View)* box is unchecked. If multiple Role Assignments apply, an action being denied in any applicable Role Assignment overrides this action being allowed in other applicable Role Assignment.

Click on the Confirm Access tab to finalize the role:

![Confirm Access Tab]

In addition to the *Allow* and *Deny* options you can select the *Enable* check box to enable **Confirm Access** for the role. This means that a user on the Host side of a Connect session must confirm access. When you select the *Enable* check box, the below listed exceptions become available for selection, so that optionally you can modify **Enable - Confirm Access**. You can select **Confirm Access - Except when - Computer locked, No user logged on, and/or Guest user logged on** (same user logged on on both sides).

However, you might belong to various user groups with different roles. The rights of all roles that you belong to applies in combination. If the **Confirm Access - Even if - Computer locked, No user logged on and/or Guest user logged on** options are set in this role, these options then overrides the **Except when** options in all other roles.

If you are for instance an enterprise administrator you want to be able to carry out your work without **Confirm Access**. To override any roles that involve **Confirm Access**, you can select the **Force disable** check box.
NOTE: View the applicable Role of a Guest with a Host in the Who May Connect Whom (Accessible Hosts) and Who May Connect Whom (Permitted Guests) windows.

Click on OK to close the window to create the Role record in the Role Records Pane.

See also
Role Toolbar Records Pane Role Assignment
Who May Connect Whom (Accessible Hosts)
Who May Connect Whom (Permitted Guests)

2.4.2.2.2 Edit
Select a Role record and select the Role menu Edit command, click the toolbar Edit Selected button, press CTRL+E or double-click a Role record to show its properties in the Impero Security Role window to edit them.

NOTE: You cannot edit the built-in Role records Full Control and No Access. Role Assignments apply the edited properties of an edited Role record.

See also
Role Toolbar Impero Security Role window Role Assignment

2.4.2.2.3 Delete
Select Role records and select the Role menu Delete command, click the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

NOTE: You cannot delete the built-in Role records Full Control, No Access, Standard Role and Unassigned Hosts’ Role. Role Assignments that use a deleted Role record are deleted.

See also
Role Toolbar Role Assignments

2.4.2.3 Security Policies
Select the Selection Pane Security Settings branch Security Policies command to show this Records Pane:

NOTE: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the Security Policies as named icons or table records. The Details selection displays the table records in a table with these column contents:

- **Parameter**: Security Policy icon and name/description.
- **Setting**: (Icon and) value.

You cannot sort records.

To manage a Security Policy, double-click its record to show the matching window as explained in
these sections:

- **Security Server Public Key**

  **NOTE:** Group Name functionality has been replaced by Public Key functionality. Group Name has been left in the system for backward compatibility only and we strongly recommend that you use Public Key and update your Impero Hosts.

- **Security Server List**
- **Preferred Guest Type**
- **Preferred Host Type**
- **Logging Options**

**NOTE:** To adopt Security Policy changes, Impero Security Servers must log off from and on to the Security Database.

**See also**
Selection Pane
Security Settings
Records Pane
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Security Policies
Details
Impero Security Server Setup
Security Database Setup

### 2.4.2.3.1 Security Server Public Key

Select this Security Policies record:

and click on the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

From this window you can copy the Public Key to make it available to Hosts. If the Public Key is changed, you must restart Security Servers, reconfigure and restart Hosts.

**See also**
Security Policies
Toolbar
Security Database Wizard

### 2.4.2.3.2 Security Server Group Name (backwards compatibility)

Select this Security Policies record:
and click on the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

![Edit Selected button](image)

As stated in the text in the window, the Group functionality is displayed for compatibility with previous version. It is recommended that you update your Hosts and use Public Key instead.

**Group name (private) []**: By default, **Impero** is specified in this field. Characters are displayed as dots or asterisks. For a working security database, you should specify another private **Group name** that should be known only among Impero Security Management administrators.

**Confirm group name []**: Re-specify in this field the private **Group name** for confirmation.

**Group ID (public) []**: This field displays the 32-digit hexadecimal checksum generated from the private **Group name**. This is the **Group ID** that must be specified on Hosts that use this security server group.

**NOTE**: From this window or from the Security Database Wizard Security Server Group Name window, you can copy the public **Group ID** to make it available to Hosts. If the private **Group name** and consequently the public **Group ID** is changed, Hosts that use this security server group must change their specified **Group ID** accordingly.

See also
- Security Policies
- Toolbar
- Security Database Wizard
- Group name
- Security Server Group Name window
- Group ID

### 2.4.2.3.3 Security Server List

Select this Security Policies record:

![Security Server List](image)

and click on the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

![Add button](image)

It specifies security server group members and Impero Access Server compatibility.

**NOTE**: A similar window is shown in the Security Database Wizard.

The pane displays the records of the security server group Impero Security Servers in a table with these column contents:

- **Servers**: Host icon and Impero Security Server Host ID.
- **Answer Access Server 6.5 Requests**: Traffic light icon and Yes if Impero Access Server compatible, No if not Impero Access Server compatible.
- **Access Server Key**: Access Server key (authentication key) of a Impero Access Server compatible Impero Security Server.

**Add**: The field initially displays the Impero Security Manager computer name. Specify in the field the **Host ID** of a Impero Security Server that shall be a member of the group and click on **Add** to add its record in the pane.

**Remove**: Select a record in the pane and click on this button to remove it.
**Edit**: Select a record in the pane and click on this button to show this window:

It enables Impero Access Server compatibility.

**Enable Impero 6.5 Access Server compatibility**: Check this box to enable Impero Access Server compatibility.

**Note**: Impero Access Server compatibility is required only if Hosts of a version lower than 7.0 must be supported by Impero Security Management.

**Access Server Key []**: Specify in this field the Access Server Key (authentication key) that this Impero Security Server shall use for authenticating Impero Access Server users.

See also

Security Policies
Toolbar
Security Database Wizard

2.4.2.3.4  Preferred Guest Type

Select this Security Policies record:

and click on the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

It has a **Preferred Guest Type** tab and a **Smart Card** tab.

**Preferred Guest Type Tab**
This tab specifies the type of logon credentials that Hosts shall request from connecting Guests if they can.

**NOTE**: A window with the same contents is shown in the Security Database Wizard.

Select one of these options:

**Guests enter Windows user name and password**: Hosts shall request Windows credentials (**User name**, **Password**, **Domain**) if they can (default selection).

**Guests enter Impero Guest ID and password**: Hosts shall request Impero credentials (**Guest ID**, **Password**).

**Guests enter RSA SecurID user name and PASSCODE**: Hosts shall request RSA SecurID credentials (**User Name**, (**Password**), **PASSCODE**) if they can.

**Guests enter Directory Services user name and password**: Hosts shall request directory services credentials (**User Name**, **Password**, **Directory Server**) if they can.

Non-Windows Guests such as Linux and Mac do not support Windows Definitions, RSA SecurID Definitions or Directory Services Definitions and can request only Impero credentials. If Impero Security Management shall support such Guests, Role Assignments based on Guest Impero Definitions must be available in the Security Database.

**Smart Card Tab**

This tab specifies Guest Smart Card logon options.
Windows Security Management

Select one of these options:

**Never log on with Smart Card**: Enable only credentials logon (default selection).

**Always log on with Smart Card**: Enable only Smart Card logon.

**Allow both logon with Smart Card and credentials (name, password and domain)**: Enable credentials and Smart Card logon.

Directory Services

Select one of these options:

**Never log on with Smart Card**: Enable only credentials logon (default selection).

**Always log on with Smart Card**: Enable only Smart Card logon.

**Allow both logon with Smart Card and credentials (name, password and directory server)**: Enable credentials and Smart Card logon.

Select one of these options:

**Subject field**: Retrieve the user identification from the subject field (default selection).

**Subject alternative name field (must be a User Principal Name (UPN))**: Retrieve the user identification from the alternative field.

Specify in the field the directory services attribute type name of the certificate field contents only if different from a user object distinguished name type.

See also

Security Policies
Toolbar
Security Database Wizard
Role Assignment
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
Security Database Setup

2.4.2.3.5 Preferred Host Type

Select this Security Policies record:

and click the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

It specifies how Hosts shall identify themselves to Impero Security Server if they can.

**Note**: A similar window is shown in the Security Database Wizard.

Select one of these options:

**Windows user if one is logged on, otherwise workstation**: If they can, Hosts shall identify themselves by any logged on Windows User or if no user is logged on by the Host computer Windows Workstation (default selection).

**Always the workstation**: If they can, Hosts shall always identify themselves by the Host computer
Windows Workstation.

**Impero Host ID**: Hosts shall identify themselves by their Impero Host ID.

Non-Windows Hosts such as Linux and Mac do not support Windows Definitions and always identify themselves by their Impero Host ID. If Impero Security Management shall support such Hosts, Role Assignments based on their Host Impero Definitions must be available in the Security Database.

**See also**

- Security Policies
- Toolbar
- Security Database Wizard
- Windows User
- Windows Workstation
- Impero Host ID
- Role Assignment
- Windows Definitions
- Role
- Impero Definitions
- Security Database Setup

### 2.4.2.3.6 Logging Options

Select one of these Security Policies records:

![Record](image)

and click the toolbar **Edit Selected** button, press CTRL+E or double-click the record to show this window:

![Edit Selected](image)

It specifies logging options.

**Clean up log entries older than [] days**: Specify in this field a number (default: 7) for the days after which log records shall be deleted.

**Note**: Specify 0 (zero) to not clean up logs automatically.

**Clean up active session entries older than [] hours**: Specify in this field a number (default: 4) for the hours after which Active Sessions records shall be deleted.

**Run Scheduler**: Uncheck this box to disable scheduling including cleanup and Scheduled Jobs (default: checked).

**See also**

- Security Policies
- Toolbar
- Active Sessions
- Scheduled Jobs

### 2.4.3 Logging

You can manage **Logging** records from the **Records** menu **Logging** submenu:

![Records](image)

- or from the Selection Pane Logging branch:
that include these commands:

- Security Log
- Impero Log
- Active Sessions

**NOTE:** By default, the Selection Pane displays the **Logging** branch. You can hide and show it from the **View** menu **Logging** command.

See also

- Records Menu
- Selection Pane
- Logging
- View Menu

### 2.4.3.1 Security Log

Select the Selection Pane **Logging** branch **Security Log** command to show this Records Pane:

**NOTE:** By default, the Selection Pane below the Impero Security Management root element is displayed **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the security database actions as named icons or table records. The **Details** selection displays the table records with these column contents:

- **Created**: Action type icon and time stamp in format `YYYY-MM-DD HH:MM:SS`.
- **CreatedBy**: Creator Windows user or workstation name.
- **Status**: Check mark and **Ok** (success) or red dot with white X and **Err <Number>** (failure).
- **Action**: Action type description and number.
- **Operand**: Record type icon and description (question mark balloon and 0 if not a record).
- **Operator**: Question mark balloon and record number (0 if not a record).
- **P1**: Parameter 1 (action specification).

Manage **Security Log records** from the **Records** menu **Security Log** submenu:

or from the matching **Security Log** Records Pane context menu:

**Delete Older Than...**: Select a **Security Log** record and select this command to show a confirmation window to confirm deleting records older than the selected record.

**Clear Log**: Select this command to show a confirmation window to confirm deleting all **Security Log** records.

**NOTE:** The log is cleaned up automatically according to specified Logging Options.

See also
2.4.3.2 Impero Log

Select the Selection Pane **Logging** branch **Impero Log** command to show this Records Pane:

![Impero Log icon]

**Note**

**Note:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays records of Impero events on Impero modules that log on an Impero Security Server that belongs to the **Security Database Security Server** group. Events can be shown as named icons or table records. The **Details** selection displays the table records with these column contents:

- **Created**: Impero log icon and time stamp in format **YYYY-MM-DD HH:MM:SS**.
- **EventType**: Event code.
- **Host**: Logging Impero module name.
- **Description**: Event arguments. Displays ??? if the event has no arguments.
- **DtlError**: Displays 0 as error logging is not implemented.
- **ProtocolError**: Displays 0 as error logging is not implemented.
- **SerialNo**: Logging Impero module event number.

**Note:** Impero event logging is explained in the **User's Guide**.

Manage Impero Log records from the **Records** menu Impero Log submenu:

![Impero Log icon]

or from the matching Impero Log Records Pane context menu:

![Impero Log icon]

**Delete Older Than...**: Select a Impero Log record and select this command to show a confirmation window to confirm deleting records older than the selected record.

**Clear Log**: Select this command to show a confirmation window to confirm deleting all Impero Log records.

**Note:** The log is cleaned up automatically according to specified Logging Options.

**See also**

Selection Pane
Logging
2.4.3.3 Active Sessions

Select the Selection Pane **Logging** branch **Active Sessions** command to show this Records Pane:

**NOTE:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the **Active Sessions** records based on Impero Log Host session event records.

**NOTE:** **Active Sessions** records are displayed only to the extent that Impero Hosts log session events on a Impero Security Server that belongs to the Security Database Security Server group. If Impero Host session event loggings are incomplete, **Active Sessions** records may be inaccurate.

**Active Sessions** can be shown as named icons or table records. The **Details** selection displays the table records with these column contents:

- **Guest**: Session type icon and Impero Log **Description** column value of a Impero Host session event record.
- **Host**: Impero Log **Host** column value of a Impero Host session event record.
- **SessionType**: Session type name derived from the Impero Log Impero Host session event record.
- **Started**: Session start time stamp in format **YYYY-MM-DD HH:MM:SS**

Manage **Active Sessions** records from the **Records** menu **Active Sessions** submenu:

or from the matching **Active Sessions** Records Pane context command:

**Refresh**: Select this command, press F5 or click on the Filter and Fetching Bar **Refresh** button to retrieve fresh Security Database data to refresh **Active Sessions** records.

**NOTE:** **Active Sessions** records are refreshed automatically every ten seconds and are cleaned up automatically according to specified Logging Options.

See also

**Selection Pane**
**Logging**
**Records Pane**
**Security Settings**
**Scheduling**
**Windows Definitions**
2.4.4 Scheduling

You can manage **Scheduling** records from the **Records** menu **Scheduling** submenu:

that contains this command:

- **Jobs**

You can also manage **Scheduling** records from the Selection Pane **Scheduling** branch:

which includes this matching command:

- **Scheduled Jobs**

  **Note:** By default, the Selection Pane displays the **Scheduling** branch. You can hide and show it from the **View** menu **Logging** command.

**See also**

Records Menu
Selection Pane
Scheduled Job
Scheduling
View Menu

2.4.4.1 Scheduled Job

Select the Selection Pane **Scheduling** branch **Scheduled Jobs** command to show this Records Pane:

**NOTE:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the **Scheduled Job** records that enables a group record temporarily within a specified period, optionally according to a weekly schedule.

**Scheduled Jobs** can be shown as named icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td><strong>Scheduled Job</strong> icon and optionally a description.</td>
</tr>
</tbody>
</table>
### GroupID
Group type icon and name and group record ID column value.

### Domain
Group record Domain column value, if a Windows group.

### StartTime
Start time stamp in format YYYY-MM-DD HH:MM:SS.

### EndTime
End time stamp in format YYYY-MM-DD HH:MM:SS.

### Flags
Weekly schedule hexadecimal number.

### ID
Record number (records are numbered starting from 1).

### Created
Creation date stamp in format YYYY-MM-DD HH:MM:SS.

### CreatedBy
Creator Windows user name.

### Modified
Modification date stamp in format YYYY-MM-DD HH:MM:SS.

### ModifiedBy
Modifier Windows user name.

Manage **Scheduled Job** records from the **Records** menu **Jobs** submenu:

or from the matching **Scheduled Job** Records Pane context menu:

- **New**
- **Details**
- **Edit**
- **Delete**

**See also**
- Selection Pane
- Scheduling
- Records Pane
- Security Settings
- Logging
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions

#### 2.4.4.1.1 New

Select the Jobs menu **New** command, click the toolbar New Scheduled Job button with a clock or press F10 to run the Scheduled Job wizard to show this window:

This wizard creates a Scheduled Job record.
Wizard windows display the options to the left and specifications to the right. Suggested or completed specifications are displayed in black text. User messages are displayed in blue text.

This window specifies an optional Scheduled Job description and selects a group type.

**Description []**: Optionally, specify in this field a Scheduled Job description that is displayed in the Scheduled Job Records Pane **Description** column.

Select one of these options:

- **Windows group**: Create a Windows Group Scheduled Job (default selection).
- **Guest ID group**: Create a Impero Guest ID Group Scheduled Job.
- **Host ID group**: Create a Impero Host ID Group Scheduled Job.

If on a Windows 2000+ computer you select **Windows group**, the Windows **Select Group** window are displayed after clicking on **Next**. When you have selected a Windows group, the **Select <Type> Group** window are displayed.

Otherwise, this window is displayed when you click on **Next**:

- **<Type>**

  It specifies a Scheduled Job group selection.

  If a Windows group was selected in a Windows **Select Group** window, the disabled left drop-down box fields and the right **Windows group** specification displays the domain and group name.

  Otherwise, a drop-down box whose list contains available Security Database group record names are displayed to the left. Actively select a list name to show it in the field to specify it to the right immediately or after clicking on **Next**.

  Click on **Next** to show this window:

- **<Type>**

  It specifies a Scheduled Job start date and time and optionally a weekly schedule.

  Select one of these options:

  - **Once on**: Specify one date and time interval (default selection).
  - **Checked weekdays starting**: Enable the **Every** section to specify a weekly schedule in a date and time interval.
    - **<Date>**: Click on the button of this drop-down box to show a calendar. Select a date in the calendar to show it in the field or edit the date in the field (default: today).
    - **<Time>**: Select time elements and change them with the up/down buttons or edit the time in the field (default: 7:00:00 AM).
  - **Every**: Check weekday boxes to enable at the specified time on checked weekdays.

  Click on **Next** to show this window:

- **<Type>**

  It specifies a Scheduled Job end date and time, if selected in a weekly schedule.

  - **<Date>**: Click on the button of this drop-down box to show a calendar. Select a date in the calendar to show it in the field or edit the date in the field (default: 28 days from today).
  - **<Time>**: Select time elements and change them with the up/down buttons or edit the time in the field (default: 6:00:00 PM).

  **Every**: This section is enabled if a weekly schedule was selected in the **Start Date and Time** window. Check weekdays to disable at the specified time on checked weekdays.

  **Note**: Start Date and Time and End Time window checked weekdays must match. If a valid weekly
schedule has been created, a bar in a lower extension of the window displays it graphically. If your selections are valid, the Finish button is enabled.

Click on Finish to end the wizard to create the specified Scheduled Job record.

See also

Jobs menu
Toolbar
Scheduled Job
Records Pane
Windows Group
Impero Guest ID Group
Impero Host ID Group
Security Database Setup

2.4.4.1.2 Details

Select a Scheduled Job record and select the Scheduled Job menu Details command to show records of the individual Scheduled Job actions. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExecuteAt</td>
<td>Scheduled Job icon and time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>Action</td>
<td>Check mark 7: Enable or red dot with white X 8: Disable.</td>
</tr>
<tr>
<td>Operand</td>
<td>Group record GroupName column value.</td>
</tr>
<tr>
<td>Operator</td>
<td>If Windows group, group record RID column number. If Impero group, group record ID column value.</td>
</tr>
<tr>
<td>P1</td>
<td>Group record GroupName column name.</td>
</tr>
<tr>
<td>P2</td>
<td>If Windows group, group record Domain column value.</td>
</tr>
<tr>
<td>JobID</td>
<td>Scheduled Job record ID column value.</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
</tbody>
</table>

Right-click in the Records Pane and select Back or press CTRL+BACKSPACE to show unexpanded Scheduled Job records.

See also

Scheduled Job
Details
GroupName
RID
ID
Domain
Records Pane
2.4.4.1.3 Edit
Select a Scheduled Job record and select the Scheduled Job menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Scheduled Job record to show the record properties in the **Scheduled Job** wizard to edit them.

**See also**
- Scheduled Job Toolbar
- Scheduled Job wizard

2.4.4.1.4 Delete
Select Scheduled Job records and select the Scheduled Job menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**See also**
- Scheduled Job Toolbar

2.4.5 Impero Definitions
You can manage **Impero Definitions** records from the **Records** menu **Impero Definitions** submenu:

![Impero Definitions](image)

or from the Selection Pane **Impero Definitions** branch:

![Selection Pane](image)

which includes these commands:

- **Impero Guest IDs**
- **Impero Guest ID Groups**
- **Impero Host IDs**
- **Impero Host ID Groups**
- **Impero Properties**

**Note:** By default, the Selection Pane does not display the **Impero Definitions** branch. You can show and hide it from the **View** menu **Impero Definitions** command. Using Impero Definitions, Impero Security Management identifies a connecting Guest by the Impero Guest ID it specifies when logging on to the Host and a connected to Host by the Host ID specified on the Host.

**See also**
- Records Menu
- Selection Pane
- Impero Definitions
- Impero Guest IDs
- Impero Guest ID Groups
- Impero Host IDs
- Impero Host ID Groups
- Impero Properties
- View Menu
2.4.5.1 Impero Guest ID

Click the Selection Pane **Impero Definitions** branch **Guest IDs** command to show this Records Pane:

**Note:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden.

You can hide/show branches by selecting View menu branch name commands.

It displays the **Impero Guest IDs** as icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td><strong>Impero Guest ID</strong> icon and name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>Password</td>
<td>Yellow key and asterisks (password specified) or white key and <strong>No Password</strong> (no password specified)</td>
</tr>
<tr>
<td>ForceChange</td>
<td>Check mark (Guest user must specify a new password at next logon) or nothing (password is OK).</td>
</tr>
<tr>
<td>Callback</td>
<td>White phone and <strong>No callback</strong> (callback is not implemented in Impero Security Management).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>PwdWrong</td>
<td>Number of wrong passwords in last logon attempt.</td>
</tr>
<tr>
<td>PwdNum</td>
<td>Number of recent passwords that cannot be reused.</td>
</tr>
<tr>
<td>PwdChanged</td>
<td>Last password change time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>PwdUsed</td>
<td>Last password use time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional <strong>Impero Guest ID</strong> description.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage **Impero Guest ID** records from the **Records** menu **Guest ID** submenu:

or from the matching **Impero Guest ID** Records Pane context menu:
It contains these commands:

- **New**
- **Edit**
- **Delete**
- **Accessible Hosts**

### See also

- Selection Pane
- Impero Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions
- View Menu
- Details
- Records Menu

#### 2.4.5.1.1 New

Select the Impero Guest ID menu **New** command, click the toolbar **New Impero Guest ID** button with a Impero Guest icon or press F3 to show this window:

**Note:** To show toolbar Impero Definitions buttons, while the Selection Pane shows the Impero Definitions branch select the View menu **Large Toolbar** or **Small Toolbar** command.

This window specifies a Impero Guest ID record. It has two tabs:

- **General** tab
- **Member Of** tab

### General Tab

This tab specifies general Impero Guest ID record properties.

- **[<Impero Guest ID name>]:** If creating a Impero Guest ID record, replace the default **NEW GUEST ID** field contents by the name by which the record Guest shall identify itself. If editing a Impero Guest ID record, you can edit the Impero Guest ID name.

- **Description [ ]:** Optionally, specify in this field a description that is displayed in the Impero Guest ID Records Pane Details show Description column.

- **Callback Number [ ]:** This field is disabled as callback options are currently not implemented in Impero Security Management.

### Callback Mode

- **No callback:** This option is always selected to apply no callback.

### Status

- **Record is disabled:** Check this box to disable the record (default: unchecked).

**Note:** Impero Security Management does not use a Role Assignment record that uses a disabled
Guest or Host selection record.

Password
This section specifies Impero password properties.

**Password []**: If creating an Impero Guest ID record, this field is empty. Optionally, specify a password. Characters are displayed as dots or asterisks. If editing an Impero Guest ID record, this field typically displays dots or asterisks signifying that a password is specified. You can edit the password.

**Confirm []**: Re-specify in this field a new password for confirmation.

**Note**: Impero passwords must satisfy Impero Guest ID Password Properties.

**Change at next logon**: If creating an Impero Guest ID record, this box is checked to request that the Guest user changes the password at next logon after which the box becomes unchecked. You can uncheck and check the box.

**Illegal count []**: This disabled field displays the number of unsuccessful password attempts in the last Guest logon.

**History count []**: This disabled field displays the number of used passwords that cannot be reused.

**Last change []**: This disabled field displays the last time the password was changed.

**Last use []**: This disabled field displays the last time the password was used.

**Member Of Tab**
This tab specifies the Impero Guest ID Group records of which this Impero Guest ID record is a member:

This tab specifies the Impero Guest ID Group records of which this Impero Guest ID record is not a member:

The pane displays the names of Impero Guest ID Group records of which this Impero Guest ID record is a member (initially none).

**Add...**: Click this button to show this window:

It adds this Impero Guest ID record as a member of Impero Guest ID Group records.

The pane displays the names of Impero Guest ID Group records of which this Impero Guest ID record is not a member.

Select in the pane Impero Guest ID Group record names and click on **OK** to close the window to add this Impero Guest ID record as a member of selected Impero Guest ID Group records.

**Remove**: Select Impero Guest ID Group record names in the pane and click this button to remove this Impero Guest ID record as a member of selected Impero Guest ID Group records.

**See also**
- Impero Guest ID
- Toolbar
- Impero Definitions
- Selection Pane
- View Menu
- Records Pane
- Details
- Role Assignment
- Impero Guest ID Password Properties
- Impero Guest ID Group
2.4.5.1.2 Edit
Select a Impero Guest ID record and select the Impero Guest ID menu Edit command, click on the toolbar Edit Selected button, press CTRL+E or double-click a Impero Guest ID record to show its properties in the Impero Guest ID window to edit them.

Note: Role Assignments apply the edited properties of an edited Guest or Host selection record.

See also
- Impero Guest ID
- Toolbar
- Impero Guest ID window
- Role Assignment

2.4.5.1.3 Delete
Select Impero Guest ID records and select the Impero Guest ID menu Delete command, click the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

Note: Role Assignment records that use a deleted Guest or Host selection record are deleted.

See also
- Impero Guest ID
- Toolbar
- Role Assignment

2.4.5.1.4 Accessible Hosts
Select a Impero Guest ID record and select the Impero Guest ID menu Accessible Hosts command to show the Who May Connect Whom (Accessible Hosts) window.

See also
- Impero Guest ID
- Who May Connect Whom (Accessible Hosts) window

2.4.5.2 Impero Guest ID Group
Click the Selection Pane Impero Definitions branch Guest ID Groups command to show this Records Pane:

Note: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Impero Guest ID Groups as icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Impero Guest ID Group icon and name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>Description</td>
<td>Optional Impero Guest ID Group description.</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage **Impero Guest ID Group** records from the **Records** menu **Guest ID Group** submenu:

- or from the matching **Impero Guest ID Group** Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

**See also**

*Selection Pane*
*Impero Definitions*
*Records Pane*
*Security Settings*
*Logging*
*Scheduling*
*Windows Definitions*
*RSA SecurID Definitions*
*Directory Services Definitions*
*View Menu*
*Details*
*Records Menu*
*Members*

### 2.4.5.2.1 New

Select the Impero Guest ID Group menu **New** command, click the toolbar **New Impero Guest ID Group** button with a double Impero Guest icon or press F4 to show this window:

**Note:** To show toolbar Impero Definitions buttons, while the Selection Pane shows the Impero Definitions branch select the **View** menu **Large Toolbar** or **Small Toolbar** command.

This window specifies a Impero Guest ID Group record.

[<Impero Guest ID Group name>]: If creating a Impero Guest ID Group record, replace the default **NEW Impero GUEST ID GROUP** field contents by the desired group name. If editing an Impero Guest ID Group record, you can edit the Impero Guest ID Group name.

**Description []**: Optionally, specify in this field a description that is displayed in the Impero Guest ID Group Records Pane **Details** show **Description** column.
Record is Disabled: Check this box to disable the record (default: unchecked).

**Note:** Enabled group member records remains enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

### See also
- Impero Guest ID Group
- Toolbar
- Impero Definitions
- Selection Pane
- View Menu
- Records Pane
- Details
- Role Assignment

#### 2.4.5.2.2 Edit

Select a Impero Guest ID Group record and select the Impero Guest ID Group menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Impero Guest ID Group record to show its properties in the **Impero Group** window to edit them.

**Note:** Role Assignments apply the edited properties of an edited Guest or Host selection record.

### See also
- Impero Guest ID Group
- Toolbar
- Impero Group window
- Role Assignments

#### 2.4.5.2.3 Delete

Select Impero Guest ID Group records and select the Impero Guest ID Group menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note:** Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

### See also
- Impero Guest ID Group
- Toolbar
- Role Assignments

#### 2.4.5.2.4 Members

Select a Impero Guest ID Group record and select the Impero Guest ID Group menu **Members** command to show this window:

It manages Impero Guest ID Group record Impero Guest ID record members.

The title bar displays the Impero Guest ID Group name.

The pane displays the Impero Guest ID Group record Impero Guest ID record member icons and names.

**Add:** Click on this button to show this window:

It adds Impero Guest ID record members to the selected Impero Guest ID Group record.
The title bar displays the Impero Guest ID Group name.

The pane displays the icons and names of Impero Guest ID records that are not members of the Impero Guest ID Group record.

Select in the pane Impero Guest ID records and click on OK to add them as members of the Impero Guest ID Group record.

Remove: Select in the pane Impero Guest ID records and click this button to remove them as members of the Impero Guest ID Group record.

See also
Impero Guest ID Group
Impero Guest ID

2.4.5.3 Impero Host ID

Click the Selection Pane Impero Definitions branch Host IDs command to show this Records Pane:

Note: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the Impero Host IDs as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostName</td>
<td>Impero Host ID icon and name</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Description</td>
<td>Optional Impero Host ID description.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Impero Host ID records from the Records menu Host ID submenu:

- or from the matching Impero Host ID Records Pane context menu:

It contains these commands:

- New
- Edit
2.4.5.3.1 New

Select the Impero Host ID menu New command, click the toolbar New Impero Host ID button with a Impero Host icon or press F6 to show this window:

![New Impero Host ID window](image)

**Note:** To show toolbar Impero Definitions buttons, while the Selection Pane shows the Impero Definitions branch select the View menu Large Toolbar or Small Toolbar command.

This window specifies a Impero Host ID record. It has two tabs:

- **General** tab
- **Member Of** tab

**General Tab**

This tab specifies general Impero Host ID record properties.

- `<Impero Host ID name>`: If creating a Impero Host ID record, replace the default NEW HOST ID field contents by the Host ID by which the record Host identifies itself to Impero Security Server. If editing a Impero Host ID record, you can edit the Impero Host ID name.

- **Description []**: Optionally, specify in this field a description that is displayed in the Impero Host ID Records Pane Details view Description column.

- **Record is disabled**: Check this box to disable the record (default: unchecked).

**Note:** Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**Member Of Tab**

The functionality of this tab is similar to the functionality of the Impero Guest ID window Member Of tab.
2.4.5.3.2  Edit

Select a Impero Host ID record and select the Impero Host ID menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Impero Host ID record to show its properties in the Impero Host ID window to edit them.

**Note:** Role Assignments apply the edited properties of an edited Guest or Host selection record.

See also
- Impero Host ID
- Toolbar
- Impero Host ID window
- Role Assignments

2.4.5.3.3  Delete

Select Impero Host ID records and select the Impero Host ID menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note:** Role Assignment records that use a deleted Guest or Host selection record are deleted.

See also
- Impero Host ID
- Toolbar
- Role Assignment

2.4.5.3.4  Permitted Guests

Select a Impero Host ID record and select the Impero Host ID menu **Permitted Guests** command to show the **Who May Connect Whom (Permitted Guests)** window.

See also
- Impero Host ID
- Who May Connect Whom (Permitted Guests) window

2.4.5.4 Impero Host ID Group

Click the Selection Pane **Impero Definitions** branch **Host ID Groups** command to show this Records Pane:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Impero Host ID Group icon and name</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>Description</td>
<td>Optional Impero Host ID Group description.</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td><strong>Created</strong></td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td><strong>CreatedBy</strong></td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td><strong>Modified</strong></td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td><strong>ModifiedBy</strong></td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

**Note:** A default Impero Host ID Group named Unregistered Host IDs with ID = 0 is not displayed in the pane. This group that is included for Impero Access Server compatibility enables an old version Access Server enabled Impero Host for which no Impero Host ID record exists to use an Access Server enabled Impero Security Server. You can create Role Assignments with this Impero Host ID Group only with Impero Guest ID and Impero Guest ID Group records. You should not use this Impero Host ID Group for any other purpose than importing an old version Impero Access Server setup, see AMPLUS.EXE.

Manage Impero Host ID Group records from the Records menu Host ID Group submenu:

- or from the matching Impero Host ID Group Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

**See also**

- Selection Pane
- Impero Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions
- View Menu
- Details
- Impero Host ID
- Impero Guest ID Group
- Role Assignment
- AMPLUS.EXE
- Records Menu
- Members
2.4.5.4.1 New

Select the Impero Host ID Group menu New command, click the toolbar New Impero Host ID Group button with a double Impero Host icon or press F7 to show the Impero Group window whose functionality is similar with Impero Guest ID Groups and Impero Host ID Groups.

Note: To show toolbar Impero Definitions buttons, while the Selection Pane shows the Impero Definitions branch select the View menu Large Toolbar or Small Toolbar command.

See also
- Impero Host ID Group
- Toolbar
- Impero Group window
- Impero Guest ID Group
- Impero Definitions
- Selection Pane
- View Menu

2.4.5.4.2 Edit

Select a Impero Host ID Group record and select the Impero Host ID Group menu Edit command, click on the toolbar Edit Selected button, press CTRL+E or double-click a Impero Host ID Group record to show its properties in the Impero Group window to edit them.

Note: Role Assignments apply the edited properties of an edited Guest or Host selection record.

See also
- Impero Host ID Group
- Toolbar
- Role Assignments

2.4.5.4.3 Delete

Select Impero Host ID Group records and select the Impero Host ID Group menu Delete command, click the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

Note: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

See also
- Impero Host ID Group
- Toolbar
- Role Assignments

2.4.5.4.4 Members

Select a Impero Host ID Group record and select the Impero Host ID Group menu Members command to show the Impero Group Members window whose functionality is similar with Impero Guest ID Groups and Impero Host ID Groups.

See also
- Impero Host ID Group
- Impero Group Members window
- Impero Guest ID Groups
2.4.5.5 Impero Properties

Click the Selection Pane **Impero Definitions** branch **Impero Properties** element to show this Records Pane:

*Note:* By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting **View** Menu branch name commands.

It displays the **Impero Properties** as named icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Key icon and property description.</td>
</tr>
<tr>
<td>Setting</td>
<td>Property value.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

*Note:* You cannot sort records.

Manage **Impero Properties** records from the **Records** Menu **Impero Properties** submenu:

- or from the matching **Impero Properties** Records Pane context command:

Select this command, click the toolbar **Edit Selected** button, press CTRL+E or double-click any **Impero Properties** record to show this window:

It specifies Impero password properties.

Impero password syntax

**Minimum password length (0-16) []:** Specify in the field a number in the range for the minimum number of characters in the password (default: 0).

**Password history length (0-10) []:** Specify in the field a number in the range for the number of recent passwords that cannot be reused (default: 0).

**Must begin and end with a character and include a digit:** Check this box to require that the password begins and ends with a letter character and includes a numeral character (default: unchecked).

*Note:* If password syntax requirements are increased, current passwords that do not satisfy the increased requirements remain valid until changed.

**Impero password lifetime**
Password lifetime (0-99 days, 0=infinite) \[\]: Specify in the field a number in the range for the maximum number of days the password can be used before it must be changed (default: 0).

Lock accounts if not used for (0-99 days, 0=infinite) \[\]: Specify in the field a number in the range for the number of days after which a Impero Guest ID record is disabled if not used (default: 0).

Lock accounts after password failures (0-10, 0=never) \[\]: Specify in the field a number in the range for the number of unsuccessful password attempts after which the Impero Guest ID record is disabled (default: 0).

See also

Selection Pane
Impero Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Toolbar
Impero Guest ID

2.4.6 Windows Definitions

You can manage Windows Definitions records from the Records menu Windows Definitions submenu:

- or from the Selection Pane Windows Definitions branch:

that include these commands:

- Windows User
- Windows Group
- Windows Workstation
- Windows Workstation Group
- Windows Domain

Note: By default, the Selection Pane displays the Windows Definitions branch. You can hide and show it from the View menu Windows Definitions command. Using Windows Definitions, Impero Security Management identifies a connecting Guest by the Windows User name it specifies when logging on to the Host and a connected to Host by its computer Windows logon user name if it identifies itself as a user or by its Windows computer name if it identifies itself as a workstation, see Preferred Host Type.

See also

Records Menu
Selection Pane
Windows Definitions
Windows User
Windows Group
Windows Workstation
Windows Workstation Group
View Menu
Preferred Host Type

2.4.6.1 Windows User

Select the Selection Pane Windows Definitions branch Users element to show this Records Pane:

Note: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Windows Users as named icons or table records. The Details selection displays the table records in a table with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RID</td>
<td>Windows User icon and Windows relative identifier number.</td>
</tr>
<tr>
<td>UserName</td>
<td>Windows User name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Windows User domain name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Windows User records from the Records menu Windows User submenu:

- or from the matching Windows User Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Accessible Hosts
Permitted Guests

Note: To create Role Assignments with domain Windows Users, records do not need to exist in the Windows User Records Pane if the Impero Security Manager computer is connected to the Windows User domain network.

See also
Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Accessible Hosts
Permitted Guests
Role Assignments

2.4.6.1.1 New

Select the Windows User menu New command to create Windows User records.

If Impero Security Manager runs on a Windows 2000+ computer, the Windows Select User window is displayed to select a user to create a Windows User record.

If Impero Security Manager runs on another Windows computer, this window is displayed:

It creates Windows User records.

Domain [ ]: The list of this drop-down box contains the names of Windows domains recognized by the Impero Security Manager computer. Select a name in the list to show it in the field.

Username [ ]: The list of this drop-down box contains the names of users in the Windows domain selected in the Domain drop-down box. Select a name in the list to show it in the field.

Record is disabled: Check this box to disable created records (default: unchecked).

Note: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click on this button to create a Windows User record of the user selected in the Username drop-down box.

Insert All Users: Click on this button to create Windows User records of all users in the Windows domain selected in the Domain drop-down box.

See also
Windows User
Domain
Role Assignment
Windows User
Username
2.4.6.1.2 Edit
Select a Windows User record and select the Windows User menu **Edit** command, click on the toolbar **Edit Selected** button, press CTRL+E or double-click a Windows User record to show this window:

It enables editing the properties of the selected Windows User record.

**Domain []**: This disabled field displays the Windows User record **Domain** column value.

**Username []**: This disabled field displays the Windows User record **UserName** column value.

**Record is disabled**: Check this box to disable the record (default: unchecked).

**Note**: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

- Windows User Toolbar
- Role Assignment

2.4.6.1.3 Delete
Select Windows User records and select the Windows User menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note**: Role Assignment records that use a deleted Guest or Host selection record are deleted.

See also

- Windows User Toolbar
- Role Assignment

2.4.6.1.4 Accessible Hosts
Select a Windows User, Impero Guest ID, RSA SecurID User or Directory Services User record and select the matching menu **Accessible Hosts** command to show this window:

**Note**: To show this window for an individual selection for which Role Assignments are available only with group records, create the individual selection record manually.

It displays the Role Assignments of an individual Guest selection record (Windows User, Impero Guest ID, RSA SecurID User or Directory Services User) and its applicable Role rights with any individual Host selection record (Windows User, Windows Workstation or Impero Host ID) with which Role Assignments exist in the security database.

The left pane displays a tree structure with check marked named branches of the selected Guest selection record and the groups of which it is a member. A [+] button indicates that Role Assignments exist in the branch. Click on the [+ ] button, press the right arrow key or double-click the branch name to expand a branch. Click on the [-] button, press the left arrow key or double-click the branch name to collapse a branch. You can move the selection with the up/down arrow keys.

You can expand groups into their individual Host selection records. A fully expanded branch displays the icons and names of individual Host selection records with which Role Assignments exist in the security database.

Select an individual Host selection record to show in the right pane the applicable Role rights of the selected Guest selection record with this Host selection record. Right pane icons and abbreviations
are explained in Role.

**See also**

Windows User  
Impero Guest ID  
RSA SecurID User  
Directory Services User  
Role Assignment  
Role  
Windows Workstation  
Impero Host ID

### 2.4.6.1.5 Permitted Guests

Select a Windows User, Windows Workstation or Impero Host ID record and select the matching menu **Permitted Guests** command to show this window:

![Permitted Guests button](image)

**Note:** To show this window for an individual selection for which Role Assignments are available only with group records, create the individual selection record manually.

It displays the Role Assignments of an individual Host selection record (Windows User, Windows Workstation or Impero Host ID) and the applicable Role rights of any individual Guest selection record (Windows User, Impero Guest ID, RSA SecurID User or Directory Services User) with which Role Assignments exist in the security database.

The left pane displays a tree structure with check marked named branches of the selected Host selection record and the groups of which it is a member. The + button indicates that Role Assignments exist in the branch. Click on the + button, press the right arrow key or double-click the branch name to expand a branch. Click the - button, press the left arrow key or double-click the branch name to collapse a branch. You can move the selection with the up/down arrow keys.

You can expand groups into their individual Guest selection records. A fully expanded branch displays the icons and names of individual Guest selection records with which Role Assignments exist. Select an individual Guest selection record to show in the right pane the applicable Role rights of this Guest record with the selected Host selection record. Right pane icons and abbreviations are explained in Role.

**See also**

Windows User  
Windows Workstation  
Impero Host ID  
Role Assignment  
Role  
Impero Guest ID  
RSA SecurID User  
Directory Services User

### 2.4.6.2 Windows Group

Select the Selection Pane **Windows Definitions** branch **Groups** command to show this Records Pane:

![Groups pane](image)

**Note:** By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.
It displays **Windows Groups** as named icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RID</td>
<td><strong>Windows Group</strong> icon and Windows relative identifier number.</td>
</tr>
<tr>
<td>GroupName</td>
<td><strong>Windows Group</strong> name.</td>
</tr>
<tr>
<td>Domain</td>
<td><strong>Windows Group</strong> domain name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format <code>YYYY-MM-DD HH:MM:SS</code>.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format <code>YYYY-MM-DD HH:MM:SS</code>.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage **Windows Group** records from the **Records** menu **Windows Group** submenu:

- or from the matching **Windows Group** Records Pane context menu:

It contains these commands:

- **New**
- **Edit**
- **Delete**

**Note:** To create Role Assignments with domain Windows Groups, records do not need to exist in the **Windows Group** Records Pane if the Impero Security Manager computer is connected to the domain network.

**See also**

- Selection Pane
- Windows Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions
- View Menu
- Details
- Records Menu
- Role Assignments
2.4.6.2.1 New
Select the Windows Group menu New command to create Windows Group records.

If Impero Security Manager runs on a Windows 2000+ computer, the Windows Select Group window is displayed to select a user group to create a Windows Group record.

If Impero Security Manager runs on another Windows computer, this window is displayed:

It creates Windows Group records.

Domain [:] The list of this drop-down box contains the names of Windows domains recognized by the Impero Security Manager computer. Select a name in the list to show it in the field.

Group [:] The list of this drop-down box contains the names of groups in the Windows domain selected in the Domain drop-down box. Select a user group name in the list to show it in the field.

Record is disabled: Check this box to disable created records (default: unchecked).

Note: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click on this button to create a Windows Group record of the group selected in the Group drop-down box.

Insert All Groups: Click on this button to create Windows Group records of all groups in the domain selected in the Domain drop-down box.

See also
Windows Group
Domain
Role Assignment
Group

2.4.6.2.2 Edit
Select a Windows Group record and select the Windows Group menu Edit command, click the toolbar Edit Selected button, press CTRL+E or double-click a Windows Group record to show this window:

It enables editing the properties of the selected Windows Group record.

Domain [:] This disabled field displays the Windows Group record Domain column value.

Group [:] This disabled field displays the Windows Group record GroupName column value.

Record is disabled: Check this box to disable the record (default: unchecked).

Note: Enabled group member records remains enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also
Windows Group
Toolbar
Role Assignment

2.4.6.2.3 Delete
Select Windows Group records and select the Windows Group menu Delete command, click on the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting records.
Note: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

See also
Windows Group Toolbar Role Assignments

2.4.6.3 Windows Workstation

Select the Selection Pane Windows Definitions branch Workstations command to show this Records Pane:

Note

Note: By default, the Selection Pane below the Impero Security Management root element displays Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays the Windows Workstations as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ComputerName</td>
<td>Windows Workstation icon and Windows computer name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Windows Workstation domain name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Windows Workstation records from the Records menu Workstation submenu:

- or from the matching Windows Workstation Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Permitted Guests
**Note:** To create Role Assignments with domain Windows computers, records do not need to exist in the Windows Workstation Records Pane if the Impero Security Manager computer is connected to the domain network.

**See also**

- Selection Pane
- Windows Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Impero Definitions
- RSA SecurID Definitions
- Directory Services Definitions
- View Menu
- Details
- Records Menu
- Records Pane
- Permitted Guests
- Role Assignment

### 2.4.6.3.1 New

Select the Windows Workstation menu **New** command to create Windows Workstation records.

If Impero Security Manager runs on a Windows 2000+ computer, the Windows **Select Computer** window is displayed to select a Windows computer to create a record of it in the Windows Workstation Records Pane.

If Impero Security Manager runs on another Windows computer, this window is displayed:

![Select Computer Window](image)

It creates Windows Workstation records.

**Domain [ ]:** The list of this drop-down box contains the names of Windows domains recognized by the Impero Security Manager computer. Select a name in the list to show it in the field.

**Workstation [ ]:** The list of this drop-down box contains the names of computers in the Windows domain selected in the **Domain** drop-down box. Select a name in the list to show it in the field.

**Record is disabled:** Check this box to disable created records (default: unchecked).

**Note:** Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**Insert Selected:** Click on this button to create a Windows Workstation record of the workstation selected in the **Workstation** drop-down box.

**Insert All:** Click on this button to create Windows Workstation records of all computers in the domain selected in the **Domain** drop-down box.

**See all**

- Windows Workstation
- Records Pane
- Domain
- Role Assignment
- Workstation
2.4.6.3.2 Edit

Select a Windows Workstation record and select the Windows Workstation menu **Edit** command, click on the toolbar **Edit Selected** button, press CTRL+E or double-click a Windows Workstation record to show this window:

It enables editing the properties of the selected Windows Workstation record.

**Domain []**: This disabled field displays the Windows Workstation record **Domain** column value.

**Workstation []**: This disabled field displays the Windows Workstation record **ComputerName** column value.

**Member of []**: This disabled pane displays the Windows Workstation Group records of which the selected Windows Workstation record is a member.

**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

*Windows Workstation Toolbar*

*Windows Workstation Group Role Assignment*

2.4.6.3.3 Delete

Select Windows Workstation records and select the **Windows Workstation** menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting records.

**Note**: Role Assignment records that use a deleted Guest or Host selection record are deleted.

See also

*Windows Workstation Toolbar Role Assignment*

2.4.6.3.4 Permitted Guests

Select a Windows Workstation record and select the **Windows Workstation** menu **Permitted Guests** command to show the **Who May Connect Whom (Permitted Guests)** window.

See also

*Windows Workstation Who May Connect Whom (Permitted Guests) window*

2.4.6.4 Windows Workstation Group

Select the Selection Pane **Windows Definitions** branch **Workstation Groups** command to show this Records Pane:

**Note**

**Note**: By default, the Selection Pane below the Impero Security Management root element displays
Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Windows Workstation Groups as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Windows Workstation Group icon and Windows computer name.</td>
</tr>
<tr>
<td>Domain</td>
<td>Windows Workstation Group domain name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Windows Workstation Group records from the Records menu Workstation Group submenu:

- or from the matching Windows Workstation Group Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete
- Members

Note: To create Role Assignments with domain Windows computer groups, records do not need to exist in the Windows Workstation Group Records Pane if the Impero Security Manager computer is connected to the domain network. However, Windows Workstation Group records initially have no Windows Workstation record Members.

See also
Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Members
Role Assignments
Windows Workstation

2.4.6.4.1 New
Select the Windows Workstation Group menu New command to create Windows Workstation Group records.

If Impero Security Manager runs on a Windows 2000+ computer, the Windows Select Group window is displayed to select a computer group to create a Windows Workstation Group record.

If Impero Security Manager runs on another Windows computer, this window is displayed:

It creates Windows Workstation Group records.

Domain [-]: The list of this drop-down box contains the names of Windows domains recognized by the Impero Security Manager computer. Select a name in the list to show it in the field.

Group [-]: The list of this drop-down box contains the names of groups in the Windows domain selected in the Domain drop-down box. Select a group name in the list to show it in the field.

Group is disabled for Impero users: Check this box to disable created records (default: unchecked).

Note Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

Insert Selected: Click on this button to create a Windows Workstation Group record of the computer group selected in the Group drop-down box.

Insert All Groups: Click on this button to create Windows Workstation Group records of all groups in the domain selected in the Domain drop-down box.

Note: A Windows Workstation Group record initially have no Windows Workstation record members. You can add members from the Members command.

See also
Windows Workstation Group
Domain
Role Assignment
Group
Windows Workstation
Members

2.4.6.4.2 Edit
Select a Windows Workstation Group record and select the Windows Workstation Group menu Edit command, click the toolbar Edit Selected button, press CTRL+E or double-click a Windows Workstation Group record to show this window::

It enables editing the properties of the selected Windows Workstation Group record.

Domain [-]: This disabled field displays the Windows Workstation Group record Domain column value.

Group [-]: This disabled field displays the Windows Workstation Group record GroupName column value.

Item is disabled with Impero: Check this box to disable the record (default: unchecked).
**Note:** Enabled group member records remain enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**See also**

Windows Workstation Group Toolbar Role Assignment

2.4.6.4.3 Delete

Select Windows Workstation Group records and select the Windows Workstation Group menu Delete command, click on the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note:** Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

**See also**

Windows Workstation Group Toolbar Role Assignments

2.4.6.4.4 Members

Select a Windows Workstation Group record and select the Windows Workstation Group menu Members command to show this window:

It manages Windows Workstation Group record Windows Workstation record members.

The title bar displays the selected Windows Workstation Group record GroupName and Domain column values.

The pane displays Windows Workstation record members identified by their ComputerName and Domain column values.

**Add:** Click on this button to show this window:

It adds domain computers as members of the selected Windows Workstation Group record.

The title bar displays the selected Windows Workstation Group record GroupName and Domain column values.

The left pane displays the icons and names of domains recognized by the Impero Security Manager computer. Select a domain to show its computers in the right pane.

Select domain computers and click on OK to close the window to add selected computers as members of the Windows Workstation Group record.

**Note:** If Windows Workstation records of computers added as members of a Windows Workstation Group do not exist in the Security Database, they are created.

**Remove:** Select Windows Workstation records in the pane and click on this button to remove them as members of the selected Windows Workstation Group record.

**See also**

Windows Workstation Group Windows Workstation Security Database
2.4.6.5 Windows Domain

Select the Selection Pane **Windows Definitions** branch **Domains** command to show this Records Pane:

**Note:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays **Windows Domains** as icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DomainName</td>
<td><strong>Windows Domain</strong> icon and name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage **Windows Domain** records from the **Records** menu **Domain** submenu:

- or from the matching **Windows Domain** Records Pane context menu:

It contains these commands:

- **New**
- **Edit**
- **Delete**

**Note:** To create Role Assignments with Windows domains, records do not need to exist in the Windows Domain Records Pane if the Impero Security Manager computer is connected to the domain network.

**See also**

- **Selection Pane**
- **Windows Definitions**
- **Records Pane**
- **Security Settings**
- **Logging**
- **Scheduling**
- **Impero Definitions**
- **RSA SecurID Definitions**
- **Directory Services Definitions**
2.4.6.5.1 New

Select the **Windows Domain** menu **New** command to show this window:

It creates Windows Domain records.

**Domain []**: The list of this drop-down box contains the names of Windows domains recognized by the Impero Security Manager computer. Select one to show it in the drop-down box field.

**Item is disabled with Impero**: Check this box to disable created records (default: unchecked).

**Note**: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**Insert Selected**: Click on this button to create a Windows Domain record of the domain selected in the **Domain** drop-down box.

**Insert All Domains**: Click on this button to create Windows Domain records of all domains in the **Domain** drop-down box list.

**See also**

Windows Domain
Role Assignment
Domain

2.4.6.5.2 Edit

Select a Windows Domain record and select the **Windows Domain** menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Windows Domain record to show this window:

It enables editing the properties of the selected Windows Domain record.

**Domain []**: This disabled field displaysthe selected Windows Domain record **DomainName** column value.

**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Enabled domain Windows Workstation records remain enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**See also**

Windows Domain
Toolbar
Windows Workstation
Role Assignment

2.4.6.5.3 Delete

Select Windows Domain records and select the **Windows Domain** menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note**: Domain Windows Workstation records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.
You can manage **RSA SecurID Definitions** records from the **Records** menu **RSA SecurID Definitions** submenu:

- or from the Selection Pane **RSA SecurID Definitions** branch:

  ![Image](image.png)

that include these commands:

- **RSA SecurID Users**
- **RSA SecurID Groups**
- **RSA SecurID Properties**

**Note:** By default, the Selection Pane does not show the RSA SecurID Definitions branch. You can show and hide it from the **View** menu **RSA SecurID Definitions** command. Using RSA SecurID Definitions, Impero Security Management identifies a connecting Guest by the RSA SecurID User name it specifies when logging on to the Host.

**R.4.7.1 RSA SecurID User**

Select the Selection Pane **RSA SecurID Definitions** branch **RSA SecurID Users** command to show this Records Pane:

![Image](image.png)

**Note**

**Note:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting **View** menu branch name commands.

It displays **RSA SecurID Users** as named icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td><strong>RSA SecurID User</strong> icon and name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
</tbody>
</table>
ID | Record number (records are numbered starting from 1).
--- | ---
Created | Creation time stamp in format YYYY-MM-DD HH:MM:SS.
CreatedBy | Creator Windows user name.
Modified | Modification time stamp in format YYYY-MM-DD HH:MM:SS.
ModifiedBy | Modifier Windows user name.

Manage RSA SecurID User records from the Records menu RSA SecurID User submenu:

or from the matching RSA SecurID User Records Pane context menu:

It contains these commands:

- **New**
- **Edit**
- **Delete**
- **Accessible Hosts**

See also

- Selection Pane
- RSA SecurID Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- Directory_Services_Definitions
- View Menu
- Details
- Records Menu
- Accessible Hosts

2.4.7.1.1 New

Select the RSA SecurID User menu **New** command to show this window:

It creates or edits an RSA SecurID User record.

**Name [ ]**: Specify in this field the RSA SecurID User name. It becomes the RSA SecurID User record **UserName** column name.

**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

- RSA SecurID User
UserName
Role Assignment

2.4.7.1.2 Edit

Select an RSA SecurID User record and select the **RSA SecurID User** menu **Edit** command, click on the toolbar **Edit Selected** button, press CTRL+E or double-click an RSA SecurID User record to show its properties in the **RSA SecurID User** window to edit them.

**Note:** Role Assignments apply the edited properties of an edited Guest or Host selection record.

**See also**
- RSA SecurID User
- Toolbar
- RSA SecurID User window
- Role Assignments

2.4.7.1.3 Delete

Select RSA SecurID User records and select the **RSA SecurID User** menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note:** Role Assignment records that use a deleted Guest or Host selection record are deleted.

**See also**
- RSA SecurID User
- Toolbar
- Role Assignment

2.4.7.1.4 Accessible Hosts

Select an RSA SecurID User record and select this command to show the **Who May Connect Whom (Accessible Hosts)** window.

**See also**
- RSA SecurID User
- Who May Connect Whom (Accessible Hosts) window

2.4.7.2 RSA SecurID Group

Select the Selection Pane **RSA SecurID Definitions** branch **RSA SecurID Groups** command to show this Records Pane:

**Note:** By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays **RSA SecurID Groups** as named icons or table records. The **Details** selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td><strong>RSA SecurID Group</strong> icon and name.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

**Note:** A built-in RSA SecurID Group named All RSA SecurID Users with ID = 0 are not displayed in the pane.

Manage **RSA SecurID Group** records from the **Records** menu **RSA SecurID Group** submenu:

- or from the matching **RSA SecurID Group** Records Pane context menu:

It contains these commands:

- **New**
- **Edit**
- **Delete**
- **Members**

**Note:** Initially, an RSA SecurID Group record has no RSA SecurID User record members. Add members from the Members command.

**See also**

- Selection Pane
- RSA SecurID Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- Directory Services Definitions
- View Menu
- Details
- ID
- Records Menu
- Members
- RSA SecurID User

2.4.7.2.1 **New**

Select the **RSA SecurID Group** menu **New** command to show this window:

It creates or edits an RSA SecurID Group record.

**Group []:** Specify in this field the RSA SecurID Group name. It becomes the RSA SecurID Group record **GroupName** column name.
**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Enabled group member records remain enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**See also**

- RSA SecurID Group
- Role Assignment

2.4.7.2.2 Edit

Select an RSA SecurID Group record and select the **RSA SecurID Group** menu **Edit** command, click on the toolbar **Edit Selected** button, press CTRL+E or double-click an RSA SecurID Group record to show its properties in the **RSA SecurID Group** window to edit them.

**Note**: Role Assignments apply the edited properties of an edited Guest or Host selection record.

**See also**

- RSA

2.4.7.2.3 Delete

Select RSA SecurID Group records and select the **RSA SecurID Group** menu **Delete** command, click on the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note**: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

**See also**

- RSA SecurID Group
- Toolbar
- Role Assignment

2.4.7.2.4 Members

Select an RSA SecurID Group record and select the **RSA SecurID Group** menu **Members** command to show this window:

It manages RSA SecurID Group record RSA SecurID User record members.

The title bar displays the selected RSA SecurID Group record **GroupName** column name.

The pane displays the RSA SecurID User record members identified by their **UserName** column name.

**Add**: Click this button to show this window:

It adds RSA SecurID User record members to the selected RSA SecurID Group record.

The title bar displays the RSA SecurID Group **GroupName** column name.

The pane displays icons and names of RSA SecurID User records that are not members of the RSA SecurID Group record.

Select in the pane RSA SecurID User records and click **OK** to add them as members of the RSA SecurID Group record.

**Remove**: Select in the pane RSA SecurID User records and click this button to remove them as members of the RSA SecurID Group record.
2.4.7.3 RSA SecurID Properties

Select the Selection Pane RSA SecurID Definitions branch RSA SecurID Properties command to show this Records Pane:

Note: By default, the Selection Pane is below the Impero Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays one RSA SecurID Property as a named icon or a table record. The Details selection displays one table record with these column contents:

- **Property**: RSA SecurID Property icon and Use shadow Impero passwords.
- **Setting**: 0 (disabled) or 1 (enabled).
- **Created**: Creation time stamp in format YYYY-MM-DD HH:MM:SS.
- **CreatedBy**: Creator Windows user name.
- **Modified**: Modification time stamp in format YYYY-MM-DD HH:MM:SS.
- **ModifiedBy**: Modifier Windows user name.

Manage the RSA SecurID Property record from the Records menu RSA SecurID Properties submenu:

or from the matching RSA SecurID Properties Records Pane context command:

Select this command or double-click the RSA SecurID Property record to show this window:

Enable Impero password checking for RSA SecurID users: Leave this box checked to request an Impero password in addition to the RSA SecurID user name and PASSCODE from a connecting Guest to apply triple-factor security (default: checked).

Note: To apply triple factor security authentication, create for each RSA SecurID User record a shadow Impero Guest ID record whose UserName column name is the RSA SecurID User record UserName column name to apply the Impero Guest ID record Password column value for additional RSA SecurID User authentication.

See also

Selection Pane
RSA SecurID Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
Directory Services Definitions
2.4.8 Directory Services Definitions

You can manage Directory Services Definitions records from the Records menu Directory Services Definitions submenu:

- or from the Selection Pane Directory Services Definitions branch:

which contains these commands:

- Directory Services Users
- Directory Services Groups
- Directory Services
- Organizational Units

Note: By default, the Selection Pane does not display the Directory Services Definitions branch. You can show and hide it from the View menu Directory Services Definitions command. Using Directory Services Definitions, Impero Security Management identifies a connecting Guest by the Directory Services User name it specifies when logging on to the Host.

See also

Records Menu
Selection Pane
Directory Services Definitions
Directory Services Users
Directory Services Groups
Directory Services
View Menu

2.4.8.1 Directory Services User

Select the Selection Pane Directory Services Definitions branch Directory Services Users command to show this Records Pane:

Note: By default, the Selection Pane is below the Impero Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Directory Services Users as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN</td>
<td>Directory Services User icon and distinguished name.</td>
</tr>
</tbody>
</table>
Directory Service record **ServiceName** column value.

**Enabled**
Check mark (enabled) or red dot with white X (disabled).

**ID**
Record number (records are numbered starting from 1).

**Created**
Creation time stamp in format **YYYY-MM-DD HH:MM:SS**.

**CreatedBy**
Creator Windows user name.

**Modified**
Modification time stamp in format **YYYY-MM-DD HH:MM:SS**.

**ModifiedBy**
Modifier Windows user name.

Manage **Directory Services User** records from the **Records** menu **Directory Services User** submenu:

or from the matching **Directory Services User** Records Pane context menu:

It contains these commands:

- **New**
- **Edit**
- **Delete**
- **Accessible Hosts**

**Note:** To create Role Assignments with Directory Services Users, records do not need to exist in the Directory Services Users Records Pane if the relevant directory service is specified in the Directory Service Records Pane and is available.

**See also**

- Selection Pane
- Directory Services Definitions
- Records Pane
- Security Settings
- Logging
- Scheduling
- Windows Definitions
- Impero Definitions
- RSA SecurID Definitions
- View Menu
- Details
- Directory Service
- Records Menu
- Accessible Hosts
- Role Assignment

**2.4.8.1.1 New**

Select the **Directory Services User** menu **New** command to show this window:

It creates Directory Services User records.
The pane displays the users in available Directory Services. Select a user and click OK to create a Directory Services User record.

**Item is disabled with Impero:** Check this box to disable the record (default: unchecked).

**Note:** Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**See also**
- Directory Services User
- Directory Services
- Role Assignment

2.4.8.1.2 Edit

Select a Directory Services User record and select the Directory Services User menu Edit command, click the toolbar Edit Selected button, press CTRL+E or double-click a Directory Services User record to show this window:

It enables editing the properties of the selected Directory Services User record.

**Service Name []:** This disabled field displays the Directory Services User record Service column value.

**Name []:** This disabled field displays the Directory Services User record DN column name.

**Item is disabled with Impero:** Check this box to disable the record (default: unchecked).

**Note:** Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

**See also**
- Directory Services User
- Toolbar
- DN
- Role Assignment

2.4.8.1.3 Delete

Select Directory Services User records and select the Directory Services User menu Delete command, click the toolbar Delete Selected button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note:** Role Assignment records that use a deleted Guest or Host selection record are deleted.

**See also**
- Directory Services User
- Toolbar
- Role Assignment

2.4.8.1.4 Accessible Hosts

Select a Directory Services User record and select this command to show the Who May Connect Whom (Accessible Hosts) window.

**See also**
- Directory Services User
- Who May Connect Whom (Accessible Hosts) window
2.4.8.2 Directory Services Group

Select the Selection Pane Directory Services Definitions branch Directory Services Groups command to show this Records Pane:

**Note:** By default, the Selection Pane is below the Impero Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Directory Services Groups as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN</td>
<td>Directory Services Group icon and distinguished name.</td>
</tr>
<tr>
<td>Service</td>
<td>Directory Service record ServiceName column value.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Directory Services Group records from the Records menu Directory Services Group submenu:

or from the matching Directory Services Group Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete

**Note:** To create Role Assignments with Directory Services Groups, records do not need to exist in the Directory Services Group Records Pane if the relevant directory service is specified in the Directory Service Records Pane and is available.

See also

Selection Pane
Directory Services Definitions
Records Pane
Security Settings
Logging
2.4.8.2.1 New

Select the **Directory Services Group** menu **New** command to show this window:

![New Button]

It creates Directory Services Group records.

The pane displays the groups in available Directory Services. Select a group and click on **OK** to create a Directory Services Group record.

**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Enabled group member records remain enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

- Directory Services Group
- Directory Service
- Role Assignment

2.4.8.2.2 Edit

Select a Directory Services Group record and select the **Directory Services Group** menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Directory Services Group record to show this window:

![Edit Button]

It enables editing the properties of the selected Directory Services Group record.

**Service [ ]**: This disabled field displays the Directory Services Group record **Service** column value.

**Name [ ]**: This disabled field displays the Directory Services Group record **DN** column name.

**Item is disabled with Impero**: Check this box to disable the record (default: unchecked).

**Note**: Enabled group member records remain enabled. Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

See also

- Directory Services Group
- Toolbar
- DN
- Role Assignment

2.4.8.2.3 Delete

Select Directory Services Group records and select the **Directory Services Group** menu **Delete** command, click on the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**Note**: Group member records are not deleted. Role Assignments that use a deleted Guest or Host
selection record are deleted.

See also
Directory Services Group
Toolbar
Role Assignment

2.4.8.3 Directory Service

Select the Selection Pane Directory Services Definitions branch Directory Services element to show this Records Pane:

Note: By default, the Selection Pane is below the Impero Security Management root element show Security Settings, Logging, Scheduling and Windows Definitions branches in this order. Impero Definitions, RSA SecurID Definitions and Directory Services Definitions branches are hidden. You can hide/show branches by selecting View menu branch name commands.

It displays Directory Services as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>ServiceName</td>
<td>Directory Service name.</td>
</tr>
<tr>
<td>DnsName</td>
<td>Directory Server DNS name or IP address.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>Port</td>
<td>TCP/IP port number.</td>
</tr>
<tr>
<td>SSL</td>
<td>Check mark (use secure connection) or red X (do not use secure connection).</td>
</tr>
<tr>
<td>BaseDN</td>
<td>Base distinguished name.</td>
</tr>
<tr>
<td>UserDN</td>
<td>Searching user distinguished name.</td>
</tr>
<tr>
<td>Password</td>
<td>Searching user password shown as asterisks.</td>
</tr>
<tr>
<td>UserSearchFilter</td>
<td>User search filter.</td>
</tr>
<tr>
<td>UserAttribFilter</td>
<td>User attribute filter.</td>
</tr>
<tr>
<td>UserBrowseFilter</td>
<td>User browse filter.</td>
</tr>
<tr>
<td>GroupSearchFilter</td>
<td>Group search filter.</td>
</tr>
<tr>
<td>GroupAttribFilter</td>
<td>Group attribute filter.</td>
</tr>
<tr>
<td>GroupBrowseFilter</td>
<td>Group browse filter.</td>
</tr>
<tr>
<td>OuSearchFilter</td>
<td>Organizational unit search filter.</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
</tbody>
</table>
Manage Directory Service records from the Records menu Directory Service submenu:

or from the matching Directory Service Records Pane context menu:

It contains these commands:

- New
- Edit
- Delete

See also

Selection Pane
Directory Services Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
View Menu
Details
Records Menu

2.4.8.3.1 New

Select the Directory Service menu New command to run the Directory Service wizard to create a Directory Service record. This window is displayed:

It specifies the Directory Service connection.

Address []: Specify in this field the Directory Service computer DNS name or IP address.

TCP/IP port number []: Specify in this field 389 for a standard LDAP connection or 686 for a secure LDAP connection (default: 389).

Use a Secure Connection: Check this box to use a secure connection.

Base DN []: Specify in this field the distinguished name from which a search shall start.

Test: Click on this button to test the connection to show a test result message.

Click on Next to show this window:

It specifies Directory Service logon credentials.

Anonymous bind: Check this box to disable the other fields to log on without credentials.
Note: If you log on without credentials, you can typically not search a Directory Service for user and group information.

**Encrypted bind**: When using Active Directory with one or more trusted domains, it is essential to use an Encrypted bind.

**Note:**
The credentials must also be entered using an accepted format as shown in the following table:

<table>
<thead>
<tr>
<th>Encrypted bind</th>
<th>Non-Encrypted bind</th>
</tr>
</thead>
<tbody>
<tr>
<td>username@domain</td>
<td>domain\username</td>
</tr>
<tr>
<td>domain\username</td>
<td>cn=username, ou=container, dc=domain</td>
</tr>
</tbody>
</table>

With Encrypted bind, domain can be NetBIOS or FQDN name.

With Non-Encrypted bind, domain must be NetBIOS name when not using the Distinguished Name.

**User DN []**: Specify in this field the distinguished name by which Impero Security Management shall search for user and group information.

**Password []**: Specify in this field the matching password. Characters are displayed as dots or asterisks.

**Confirm []**: Re-specify in this field the password for confirmation.

**Test**: Click on this button to test Directory Service logon to show a test result message.

Click on **Next** to show this window:

It specifies Directory Service filters that speed up the search for user and group information.

Click on the **Apply Default Values for Specific Service** button to show this window:

The drop-down box list contains names of commonly used Directory Service types. Select a name in the list to show it in the field (default: *Microsoft Active Directory*). Click **OK** to close the window to show the default filters of the selected Directory Service type in the **Filters** window fields. If selecting a Directory Service type does not generate usable filters, specify or modify filters:

**User search filter []**: Specify in this field the user object class.

**User attribute []**: Specify in this field the user logon name attribute.

**User browse filter []**: Specify in this field the user and organizational unit object classes.

**Group search filter []**: Specify in this field the group object class.

**Group member attribute []**: Specify in this field the group member attribute.

**Group browse filter []**: Specify in this field the group and organizational unit object classes.

**OU search filter []**: Specify in this field the organizational unit object class.

Click on **Service Name** to show this window:

This window is used to enable authentication against RADIUS (Remote Authentication Dial In User Service) environments.

RADIUS is a client/server protocol that is often used to centrally validate remote users and authorize their access to existing network resources integrating well with existing technologies including VPN, RAS, Active Directory and Token based authentication solutions.
Using RADIUS with Impero Connect allows the Security Server to authenticate remote support sessions via compatible multi-factor authentication methods, where the Guest user needs to provide their username and password along with a one-time generated passcode that can be derived from a variety of sources including hardware devices or SMS tokens.

**Note:** In order to use the RADIUS implementation the Security Server should be configured to use Directory Services authentication. This requires that the Preferred Guest type is set to ‘Guests enter Directory Services username and password’ in the Security Policies section of the Security Manager.

Also, in order for the Guest to enter their token passcode when authenticating, the **Request Token Passcode** option should be enabled. This is available in a **Properties** section under the Directory Services definitions.

Click on **Next** to show this window:

![Next](image)

It specifies the Directory Service name and status.

- **Name [ ]**: Specify in this field the service name that becomes the Directory Service record **ServiceName** column name.
- **Item is disabled with Impero**: Check this box to disable the record (default: unchecked).
- **Note**: Impero Security Management does not search a Directory Service whose record is disabled.
- **Finish**: Click on this button to end the **Directory Service** wizard to create the Directory Service record.

**See also**

- Directory Service
- 2.4.8.3.2 Edit

Select a Directory Service record and select the **Directory Service** menu **Edit** command, click the toolbar **Edit Selected** button, press CTRL+E or double-click a Directory Service record to show this window:

![Edit](image)

This window has four tabs that match **Directory Service** wizard windows. Edit the tab contents to edit the Directory Service record.

**Note**: Directory Service searches apply the edited properties of a Directory Service record.

**See also**

- Directory Service
- Toolbar
- Directory Service wizard

2.4.8.3.3 Delete

Select Directory Service records and select the **Directory Service** menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

**See also**

- Directory Service
- Toolbar
2.4.8.4 Organizational Units

Under Directory Services Definitions click Organizational Units to show this Records Pane:

It displays Directory Services Organizational Units as named icons or table records. The Details selection displays the table records with these column contents:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN</td>
<td>The DN (Distinguished Name) is the name that uniquely identifies an entry in the directory.</td>
</tr>
<tr>
<td>Service</td>
<td>Directory Service record ServiceName column value.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Check mark (enabled) or red dot with white X (disabled).</td>
</tr>
<tr>
<td>ID</td>
<td>Record number (records are numbered starting from 1).</td>
</tr>
<tr>
<td>Created</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Creator Windows user name.</td>
</tr>
<tr>
<td>Modified</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Modifier Windows user name.</td>
</tr>
</tbody>
</table>

Manage Organizational Units records from the Records menu:

or from the shortcut menu in the pane.

2.4.8.4.1 New

On the Records menu, point to Directory Services Definitions, then Organizational Units and click New.

Browse the domain tree to locate the object you want to add.

2.4.8.4.2 Edit

1. Select the record you want to edit in the Organizational Units pane.
2. On the Records menu, point to Directory Services Definitions, then Organizational Units and click Edit.

2.4.8.4.3 Delete

1. Select the record you want to delete in the Organizational Units pane.
2. On the Records menu, point to Directory Services Definitions, then Organizational Units and click Delete.

2.4.8.5 Properties

Double-click the Request Token Passcode property to open this window:
This option is used with a RADIUS server (Remote Authentication Dial In User Service) and should be enabled in order for the Guest to enter their token passcode when authenticating.

2.4.9 Importing Roles and Definitions

If you find it easier to create roles and definitions outside of the Security Manager, for example if data exists in another system that allows export, you can import data from an external file.

For Impero Definitions role assignments can also be created as part of the import: the import file holds Impero Host information like name, description, type and role and the import creates the Impero Host IDs and subsequently role assignment.

The import file must be in xml format.

To avoid having to edit a raw xml file, you can find a sample xml file named Impero_import.xml in the following directory on the Security Server:

    %programfiles%\Impero\Impero Connect\Security Server

Although it is recommended to use Excel to edit and modify the import file to suit your specific requirements, the import file must be saved in xml format.

About the xml file content

The xml file has 20 fixed headings which must be row headings in the xml file, using rows A through T.

All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import is not successful.

<table>
<thead>
<tr>
<th>Row</th>
<th>Column headings</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Guest Name</td>
</tr>
<tr>
<td>B</td>
<td>Guest Password</td>
</tr>
<tr>
<td>C</td>
<td>Guest RID</td>
</tr>
<tr>
<td>D</td>
<td>Guest Domain</td>
</tr>
<tr>
<td>E</td>
<td>Guest Description</td>
</tr>
<tr>
<td>F</td>
<td>Guest Group Name</td>
</tr>
<tr>
<td>G</td>
<td>Guest Group RID</td>
</tr>
<tr>
<td>H</td>
<td>Guest Group Domain</td>
</tr>
<tr>
<td>I</td>
<td>Guest Group Description</td>
</tr>
<tr>
<td>J</td>
<td>Guest Type</td>
</tr>
<tr>
<td>K</td>
<td>Host Name</td>
</tr>
<tr>
<td>L</td>
<td>Host RID</td>
</tr>
<tr>
<td>M</td>
<td>Host Domain</td>
</tr>
</tbody>
</table>
### 2.4.9.1 Impero Definitions

To import Impero Definitions and create role assignments, specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

Note that Role Assignments are only created when the Role column is populated with a valid entry (the role has to already exist)

**For Impero Guest:**

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>E</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Guest Name</td>
<td>Guest Password</td>
<td>Guest Description</td>
<td>Guest Type</td>
</tr>
<tr>
<td>Value</td>
<td>&lt;Impero Guest name&gt;</td>
<td>&lt;Impero Guest password&gt;</td>
<td>&lt;Impero Guest description&gt;</td>
<td>Impero Guest</td>
</tr>
</tbody>
</table>

**Example**
guest07 SecretPassword01 Guest07 description Impero Guest

**For Impero Guest Group:**

<table>
<thead>
<tr>
<th></th>
<th>F</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Guest Group Name</td>
<td>Guest Group Description</td>
<td>Guest Type</td>
</tr>
<tr>
<td>Value</td>
<td>&lt;Impero Guest group name&gt;</td>
<td>&lt;Impero Guest Group&gt;</td>
<td>Impero Guest Group</td>
</tr>
</tbody>
</table>

**Example**
group17 Group17 description Impero Guest Group
For **Impero Host**:

<table>
<thead>
<tr>
<th></th>
<th>K</th>
<th>N</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Host Name</td>
<td>Host Description</td>
<td>Host Type</td>
</tr>
<tr>
<td>Value</td>
<td>&lt;Impero Host name&gt;</td>
<td>&lt;Impero Host description&gt;</td>
<td>Impero Host</td>
</tr>
</tbody>
</table>

Example

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>us-acc-03</td>
<td>Katie's laptop in US Account Dept</td>
<td>Impero Host</td>
</tr>
</tbody>
</table>

For **Impero Host Group**:

<table>
<thead>
<tr>
<th></th>
<th>O</th>
<th>R</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Host Group Name</td>
<td>Host Group Description</td>
<td>Host Type</td>
</tr>
<tr>
<td>Value</td>
<td>&lt;Impero Host group name&gt;</td>
<td>&lt;Impero Host group description&gt;</td>
<td>Impero Host Group</td>
</tr>
</tbody>
</table>

Example

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>US Accounts</td>
<td>US Account Department</td>
<td>Impero Host Group</td>
</tr>
</tbody>
</table>

**Impero Guest and Group** (inserts Impero Guest, Impero Guest Group and create the Group membership):

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>E</th>
<th>F</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Guest Name</td>
<td>Guest Password</td>
<td>Guest Description</td>
<td>Guest Group Name</td>
<td>Guest Group Description</td>
<td>Guest Type</td>
</tr>
<tr>
<td>Value</td>
<td>&lt;Impero Guest name&gt;</td>
<td>&lt;Impero Guest password&gt;</td>
<td>&lt;Impero Guest description&gt;</td>
<td>&lt;Impero Guest group name&gt;</td>
<td>&lt;Impero Guest group description&gt;</td>
<td>Impero Guest</td>
</tr>
</tbody>
</table>

Example

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>guest07</td>
<td>SecretPassword01</td>
<td>Guest07</td>
<td>description</td>
<td>group17</td>
<td>Group17</td>
</tr>
</tbody>
</table>

**Impero Role** Assignment (inserts Impero Guest, Guest Group, Impero Host, Host Group and create Role Assignments)
2.4.9.2 Directory Services Definitions

To import Directory Services Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

Create one row for each user and one row for each group.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>E</th>
<th>J</th>
<th>K</th>
<th>N</th>
<th>S</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required column</td>
<td>Guest Name</td>
<td>Guest Domain</td>
<td>Guest Type</td>
<td>Host Name</td>
<td>Host Description</td>
<td>Host Type</td>
<td>Role</td>
</tr>
<tr>
<td>Value: user</td>
<td>&lt;Directory Services User DN&gt;</td>
<td>&lt;Directory Services ID&gt;</td>
<td>LDAP User</td>
<td></td>
<td></td>
<td></td>
<td>role (2=full control)</td>
</tr>
<tr>
<td>Value: group</td>
<td>&lt;Directory Services Group DN&gt;</td>
<td>&lt;Directory Services ID&gt;</td>
<td>LDAP Group</td>
<td></td>
<td></td>
<td></td>
<td>role (2=full control)</td>
</tr>
<tr>
<td>Value: OU</td>
<td>&lt;Directory Services Organisational Unit DN&gt;</td>
<td>&lt;Directory Services ID&gt;</td>
<td>LDAP OU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** All headings must be present in the XML file even though you may not be using all sections for the import. If the headings are not complete, the import is not successful.
### Example: user
| cn=john smith, ou=development, ou=dallas, ou=texas, dc=mycompany, dc=local |

1. **LDAP User**

### Example: group
| cn=tx-dallas-development, ou=securitygroups, ou=dallas, ou=texas, dc=mycompany, dc=local |

1. **LDAP Group**

### Example: OU
| ou=texas, dc=mycompany, dc=local |

1. **LDAP OU**

**Note:** All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import is not successful.

### 2.4.9.3 Windows Definitions

To import Windows Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

#### For Windows user, Guest:

<table>
<thead>
<tr>
<th>A</th>
<th>C</th>
<th>D</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required column</strong></td>
<td><strong>Guest Name</strong></td>
<td><strong>Guest RID</strong></td>
<td><strong>Guest Domain</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td><code>&lt;Windows user name&gt;</code></td>
<td><code>&lt;ObjectSID from AD&gt;</code></td>
<td><code>&lt;AD domain&gt;</code></td>
</tr>
</tbody>
</table>

**Example**

| joms | S-1-5-21-2118863332-1524444778-903097961-7496 | mydomain | Windows User |

- OR -

#### For Windows user, Host:

<table>
<thead>
<tr>
<th>K</th>
<th>L</th>
<th>M</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required column</strong></td>
<td><strong>Host Name</strong></td>
<td><strong>Host RID</strong></td>
<td><strong>Host Domain</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td><code>&lt;Windows user name&gt;</code></td>
<td><code>&lt;ObjectSID from AD&gt;</code></td>
<td><code>&lt;AD domain&gt;</code></td>
</tr>
</tbody>
</table>
### For Windows group, Guest:

<table>
<thead>
<tr>
<th>A</th>
<th>C</th>
<th>D</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required column</strong></td>
<td><strong>Guest Name</strong></td>
<td><strong>Guest RID</strong></td>
<td><strong>Guest Domain</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>&lt;Windows user name&gt;</td>
<td>&lt;ObjectSID from AD&gt;</td>
<td>&lt;AD domain&gt;</td>
</tr>
</tbody>
</table>

**Example**

| josm | S-1-5-21-2118863332-1524444778-903097961-7496 | mydomain | Windows Group |

### For Windows group, Host:

<table>
<thead>
<tr>
<th>K</th>
<th>L</th>
<th>M</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required column</strong></td>
<td><strong>Host Name</strong></td>
<td><strong>Host RID</strong></td>
<td><strong>Host Domain</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>&lt;Windows user name&gt;</td>
<td>&lt;ObjectSID from AD&gt;</td>
<td>&lt;AD domain&gt;</td>
</tr>
</tbody>
</table>

**Example**

| development | S-1-5-21-2118863332-1524444778-903097961-16347 | mydomain | Windows Group |

### For Windows workstation (can participate only as Host):

<table>
<thead>
<tr>
<th>K</th>
<th>M</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required column</strong></td>
<td><strong>Host Name</strong></td>
<td><strong>Host Domain</strong></td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>&lt;Workstation name&gt;</td>
<td>&lt;AD domain&gt;</td>
</tr>
</tbody>
</table>
For Windows workstation groups (can participate only as Host):

<table>
<thead>
<tr>
<th>Required column</th>
<th>M</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>&lt;Workstation name&gt;</td>
<td>&lt;AD domain&gt;</td>
</tr>
<tr>
<td>Example</td>
<td>TX-DALLAS-JOSM</td>
<td>mydomain</td>
</tr>
</tbody>
</table>

For Windows domain (can participate only as Host):

<table>
<thead>
<tr>
<th>Required column</th>
<th>M</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>&lt;Workstation name&gt;</td>
<td>&lt;AD domain&gt;</td>
</tr>
<tr>
<td>Example</td>
<td>TX-DALLAS-JOSM</td>
<td>mydomain</td>
</tr>
</tbody>
</table>

Note: All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import is not successful.

2.4.9.4 RSA SecurID Definitions

To import RSA Definitions and create role assignments specific columns must be used. The required columns are listed below along with descriptions of the value each field must have as well as examples of these values.

RSA User (can participate only as Guest):

<table>
<thead>
<tr>
<th>Required column</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>&lt;RSA user name&gt;</td>
</tr>
</tbody>
</table>

Impero Connect Administrator’s Guide
### RSA group (can participate only as Guest):

<table>
<thead>
<tr>
<th>A</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Group Name</td>
<td>Guest Type</td>
</tr>
<tr>
<td>&lt;RSA group name&gt;</td>
<td>RSA Group</td>
</tr>
</tbody>
</table>

**Example**

<table>
<thead>
<tr>
<th>A</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA group 3</td>
<td>RSA Group</td>
</tr>
</tbody>
</table>

### RSA User, RSA Group (can participate only as Guest):

<table>
<thead>
<tr>
<th>A</th>
<th>F</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Name</td>
<td>Guest Group Name</td>
<td>Guest Type</td>
</tr>
<tr>
<td>&lt;RSA user name&gt;</td>
<td>&lt;RSA group name&gt;</td>
<td>RSA User</td>
</tr>
</tbody>
</table>

**Example**

<table>
<thead>
<tr>
<th>A</th>
<th>F</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA user 7</td>
<td>RSA group 3</td>
<td>RSA User</td>
</tr>
</tbody>
</table>

**Note:** All headings must be present in the xml file even though you may not be using all sections for the import. If the headings are not complete, the import is not successful.

### 2.5 Security Database Tables

The Security Database Wizard creates these security database tables:

- DWBATH: Scheduled Jobs
- DWCONN: Active Sessions
- DWDOMN: Windows Domain
- DWDONE: Security Log
- DWEVNT: Impero Log
- DWGRUH: Impero Host ID Group
- DWGRUP: Impero Guest ID Group
- DWHOGR: Impero Host ID Group Members
- DWHOST: Impero Host ID
- DWLDAPGRP: Directory Service Group
See also
Security Database Wizard

2.5.1 DWBATH: Scheduled Job

Security Database Tables store Scheduled Job data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Description</td>
<td>Char (64)</td>
<td>Optional description</td>
</tr>
<tr>
<td>Category</td>
<td>Integer</td>
<td>Group type number</td>
</tr>
</tbody>
</table>
### Security Database Tables

#### 2.5.2 DWCONN: Active Sessions

Security Database Tables store Active Sessions data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>Char (254)</td>
<td>Log record arguments</td>
</tr>
<tr>
<td>Host</td>
<td>Char (254)</td>
<td>Logging Impero module name</td>
</tr>
<tr>
<td>SessionType</td>
<td>Integer</td>
<td>Session type number</td>
</tr>
<tr>
<td>Started</td>
<td>Char (20)</td>
<td>Start time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
</tbody>
</table>
### 2.5.3 DWDOMN: Windows Domain

Security Database Tables store Windows Domain data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>DomainName</td>
<td>Char (254)</td>
<td>Domain name</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

### See also

- Security Database Tables
- Windows Domain

### 2.5.4 DWDONE: Security Log

Security Database Tables store Security Log data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator computer or Windows user name</td>
</tr>
<tr>
<td>Status</td>
<td>Integer</td>
<td>Action result number (0 = OK, 1=Error)</td>
</tr>
<tr>
<td>Action</td>
<td>Integer</td>
<td>Action type number</td>
</tr>
<tr>
<td>Operand</td>
<td>Integer</td>
<td>Action executed on number</td>
</tr>
<tr>
<td>Operator</td>
<td>Integer</td>
<td>Action executed by number</td>
</tr>
<tr>
<td>P1</td>
<td>Char (254)</td>
<td>Parameter 1 (additional action specification)</td>
</tr>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
</tbody>
</table>

### See also

- Security Database Tables
- Security Log
### 2.5.5 DWEVT: Impero Log

Security Database Tables store Impero Log data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format \texttt{YYYY-MM-DD HH:MM:SS}</td>
</tr>
<tr>
<td>EventType</td>
<td>Char (10)</td>
<td>Log record event code</td>
</tr>
<tr>
<td>SerialNo</td>
<td>Integer</td>
<td>Log record event number of each logging Impero module</td>
</tr>
<tr>
<td>DtlError</td>
<td>Integer</td>
<td>DTL error number (0 = no error)</td>
</tr>
<tr>
<td>ProtocolError</td>
<td>Integer</td>
<td>Protocol error number (0 = no error)</td>
</tr>
<tr>
<td>Host</td>
<td>Char (32)</td>
<td>Logging Impero module name</td>
</tr>
<tr>
<td>Description</td>
<td>Char (160)</td>
<td>Log record arguments</td>
</tr>
</tbody>
</table>

**See also**

- Security Database Tables
- Impero Log

### 2.5.6 DWGRUH: Impero Host ID Group

Security Database Tables store Impero Host ID Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GroupName</td>
<td>Char (32)</td>
<td>Impero Host ID group name (UNIQUE)</td>
</tr>
<tr>
<td>Description</td>
<td>Char (64)</td>
<td>Optional description</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format \texttt{YYYY-MM-DD HH:MM:SS}</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format \texttt{YYYY-MM-DD HH:MM:SS}</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

**See also**

- Security Database Tables
- Impero Host ID Group

### 2.5.7 DWGRUP: Impero Guest ID Group

Security Database Tables store Impero Guest ID Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
</tbody>
</table>
### GroupName
<table>
<thead>
<tr>
<th>Char (32)</th>
<th>Impero Guest ID group name (UNIQUE)</th>
</tr>
</thead>
</table>

### Description
<table>
<thead>
<tr>
<th>Char (64)</th>
<th>Optional description</th>
</tr>
</thead>
</table>

### Enabled
<table>
<thead>
<tr>
<th>Integer</th>
<th>0 = Disabled, 1 = Enabled</th>
</tr>
</thead>
</table>

### Created
<table>
<thead>
<tr>
<th>Char (20)</th>
<th>Creation time stamp in format YYYY-MM-DD HH:MM:SS</th>
</tr>
</thead>
</table>

### CreatedBy
<table>
<thead>
<tr>
<th>Char (64)</th>
<th>Creator Windows user name</th>
</tr>
</thead>
</table>

### Modified
<table>
<thead>
<tr>
<th>Char (20)</th>
<th>Modification time stamp in format YYYY-MM-DD HH:MM:SS</th>
</tr>
</thead>
</table>

### ModifiedBy
<table>
<thead>
<tr>
<th>Char (64)</th>
<th>Modifier Windows user name</th>
</tr>
</thead>
</table>

**See also**

[Security Database Tables](#)

**Impero Guest ID Group**

### 2.5.8 DWHOGR: Impero Host ID Group Members

Security Database Tables store Impero Host ID Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostID</td>
<td>Integer</td>
<td>Impero Host ID table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GrpId</td>
<td>Integer</td>
<td>Impero Host ID Group table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

**See also**

[Security Database Tables](#)

**Impero Host ID Group**

### 2.5.9 DWHOST: Impero Host ID

Security Database Tables store Impero Host ID data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>HostName</td>
<td>Char (32)</td>
<td>Impero Host ID name (UNIQUE)</td>
</tr>
<tr>
<td>Description</td>
<td>Char (64)</td>
<td>Optional description</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>
See also

Security Database Tables
Impero Host ID

2.5.10 DWLDAPGRP: Directory Service Group

Security Database Tables store Directory Services Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>DN</td>
<td>Char (254)</td>
<td>Distinguished name (UNIQUE)</td>
</tr>
<tr>
<td>Service</td>
<td>Integer</td>
<td>Directory Service table record number</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Directory Services Group

2.5.11 DWLDAPPROP: Directory Service Properties

Security Database Tables store Directory Service properties data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Setting</td>
<td>Char (254)</td>
<td>Parameter value</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Directory Service
### 2.5.12 DWLDAPSERV: Directory Service

Security Database Tables store Directory Service data in this table that has this key structure:

<table>
<thead>
<tr>
<th><strong>Key</strong></th>
<th><strong>Format</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>ServiceName</td>
<td>Char (32)</td>
<td>Alias name for the service (UNIQUE)</td>
</tr>
<tr>
<td>DnsName</td>
<td>Char (254)</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>Port</td>
<td>Integer</td>
<td>IP port number for the SSL connection</td>
</tr>
<tr>
<td>SSL</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>BaseDN</td>
<td>Char (254)</td>
<td>Base distinguished name</td>
</tr>
<tr>
<td>UserDN</td>
<td>Char (254)</td>
<td>Distinguished name for user object used for searching</td>
</tr>
<tr>
<td>Password</td>
<td>Char (16)</td>
<td>Password for user object used for searching</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>Anonymous bind 0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>UserSearchFilter</td>
<td>Char (60)</td>
<td>Filter to limit search for user objects</td>
</tr>
<tr>
<td>UserAttribFilter</td>
<td>Char (60)</td>
<td>Attribute that holds the user name</td>
</tr>
<tr>
<td>UserBrowseFilter</td>
<td>Char (200)</td>
<td>Filter to limit search for user objects and container objects</td>
</tr>
<tr>
<td>GroupSearchFilter</td>
<td>Char (60)</td>
<td>Filter to limit search for group objects</td>
</tr>
<tr>
<td>GroupAttribFilter</td>
<td>Char (60)</td>
<td>Attribute that holds the group name</td>
</tr>
<tr>
<td>GroupBrowseFilter</td>
<td>Char (200)</td>
<td>Filter to limit search for group objects and container objects</td>
</tr>
<tr>
<td>OuSearchFilter</td>
<td>Char (60)</td>
<td>Filter to limit search for container objects</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format %Y-%m-%d %H:%M:%S</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format %Y-%m-%d %H:%M:%S</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

### See also

- Security Database Tables
- Directory Service

### 2.5.13 DWLDAPUSR: Directory Service User

Security Database Tables store Directory Services User data in this table that has this key structure:

<table>
<thead>
<tr>
<th><strong>Key</strong></th>
<th><strong>Format</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>DN</td>
<td>Char (254)</td>
<td>Distinguished name (UNIQUE)</td>
</tr>
</tbody>
</table>
Service | Integer | Directory Service table record number
--- | --- | ---
Enabled | Integer | 0 = Disabled, 1 = Enabled
Created | Char (20) | Creation time stamp in format YYYY-MM-DD HH:MM:SS
CreatedBy | Char (64) | Creator Windows user name
Modified | Char (20) | Modification time stamp in format YYYY-MM-DD HH:MM:SS
ModifiedBy | Char (64) | Modifier Windows user name

See also
Security Database Tables
Directory Services User

2.5.14 DWLDAPRADIUS: RADIUS settings

Security Database Tables store RADIUS (Remote Authentication Dial In User Service) data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Host</td>
<td>Char (254)</td>
<td>RADIUS host name / IP</td>
</tr>
<tr>
<td>SharedSecr</td>
<td>Char (254)</td>
<td>Shared Secret for the RADIUS server</td>
</tr>
<tr>
<td>Port</td>
<td>Integer</td>
<td>Port used by the RADIUS server</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also
Security Database Tables
Directory Services User

2.5.15 DWMAIN: Role Assignment

Security Database Tables store Role Assignment data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (UNIQUE)</td>
</tr>
<tr>
<td>GuestID</td>
<td>Integer</td>
<td>Guest selection table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GuestType</td>
<td>Integer</td>
<td>Guest selection type number (PRIMARY KEY)</td>
</tr>
<tr>
<td>HostID</td>
<td>Integer</td>
<td>Host selection table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>HostType</td>
<td>Integer</td>
<td>Host selection type number (PRIMARY KEY)</td>
</tr>
<tr>
<td>RoleID</td>
<td>Integer</td>
<td>Roles table record number in</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
</tbody>
</table>
2.5.16 DWNTGR: Windows Group

Security Database Tables store Windows Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>RID</td>
<td>Integer</td>
<td>Domain RID number (UNIQUE)</td>
</tr>
<tr>
<td>GroupName</td>
<td>Char (254)</td>
<td>Windows group name</td>
</tr>
<tr>
<td>Domain</td>
<td>Char (254)</td>
<td>Domain name (UNIQUE)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

- Security Database Tables
- Role Assignment

2.5.17 DWNTUS: Windows User

Security Database Tables store Windows User data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>RID</td>
<td>Integer</td>
<td>Domain RID number (UNIQUE)</td>
</tr>
<tr>
<td>UserName</td>
<td>Char (254)</td>
<td>Windows user name</td>
</tr>
<tr>
<td>Domain</td>
<td>Char (254)</td>
<td>Domain name (UNIQUE)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>
See also

Security Database Tables
Windows User

2.5.18 DWPOLI: Security Policies

Security Database Tables store Security Policies data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Char (32)</td>
<td>Parameter name (PRIMARY KEY)</td>
</tr>
<tr>
<td>Setting</td>
<td>Char (32)</td>
<td>Parameter value</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Security Policies

2.5.19 DWPKI: Public/Private Keys

Security Database Tables store keys for RSA encryption algorithm used in communication handshake mechanism between Impero Security Server and Impero Host in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>PublicKey</td>
<td>MS Access: Memo</td>
<td>Public Key</td>
</tr>
<tr>
<td></td>
<td>Oracle: NChar(1000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2: Varchar(1000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSSQL and UNKNOWN:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Char(1000)</td>
<td></td>
</tr>
<tr>
<td>PrivateKey</td>
<td>MS Access: Memo</td>
<td>Private key</td>
</tr>
<tr>
<td></td>
<td>Oracle: NChar(2000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DB2: Varchar(2000)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSSQL and UNKNOWN:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Char(2000)</td>
<td></td>
</tr>
<tr>
<td>Created</td>
<td>Char(20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char(64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char(20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char(64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Security Policies
### 2.5.20 DWPROP: Impero Properties

Security Database Tables store Impero Properties data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Integer</td>
<td>Parameter name (PRIMARY KEY)</td>
</tr>
<tr>
<td>Setting</td>
<td>Char (254)</td>
<td>Parameter value</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

**See also**

- Security Database Tables
- Impero Properties

### 2.5.21 DWROLE: Role

Security Database Tables store Role data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>RoleName</td>
<td>Char (32)</td>
<td>Role name (UNIQUE)</td>
</tr>
<tr>
<td>Rctl</td>
<td>Integer</td>
<td>Connect value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Keyb</td>
<td>Integer</td>
<td>Use keyboard and mouse value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Blink</td>
<td>Integer</td>
<td>Blank screen value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Lckm</td>
<td>Integer</td>
<td>Lock keyboard value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Boot</td>
<td>Integer</td>
<td>Restart Host value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Clip</td>
<td>Integer</td>
<td>Transfer clipboard value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Send</td>
<td>Integer</td>
<td>Send files to Host value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Recv</td>
<td>Integer</td>
<td>Receive files from Host value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Prnt</td>
<td>Integer</td>
<td>Redirect print value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Chat</td>
<td>Integer</td>
<td>Request chat value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Audi</td>
<td>Integer</td>
<td>Request audio chat value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>RunP</td>
<td>Integer</td>
<td>Run program value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
<tr>
<td>Conf</td>
<td>Integer</td>
<td>Value for confirm: 0 = no, 1 = always, 2 = logged on</td>
</tr>
<tr>
<td>Description</td>
<td>Char (64)</td>
<td>Optional description</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
<tr>
<td>Mana</td>
<td>Integer</td>
<td>Remote management value: 0 = Do not allow, 1 = Allow, 2 = Deny</td>
</tr>
</tbody>
</table>

**See also**

- Security Database Tables
- Impero Properties
Inve | Integer | Inventory scan value: 0 = Do not allow, 1 = Allow, 2 = Deny

Smsg | Integer | Send message value: 0 = Do not allow, 1 = Allow, 2 = Deny

Mjoi | Integer | Join multi Guest session value: 0 = Do not allow, 1 = Allow, 2 = Deny

Madm | Integer | Act as multi Guest session Administrator value: 0 = Do not allow, 1 = Allow, 2 = Deny

See also

Security Database Tables
Role

2.5.22 DWRSAGRP: RSA SecurID Group

Security Database Tables store RSA SecurID Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARKEY)</td>
</tr>
<tr>
<td>GroupName</td>
<td>Char (254)</td>
<td>Group name (UNIQUE)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
RSA SecurID Group

2.5.23 DWRSAPROP: RSA SecurID Properties

Security Database Tables store RSA SecurID Properties data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Integer</td>
<td>Record number (PRIMARKEY)</td>
</tr>
<tr>
<td>Setting</td>
<td>Char (254)</td>
<td>Parameter value</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
RSA SecurID Properties
### 2.5.24 DWRSAUSR: RSA SecurID User

Security Database Tables store RSA SecurID User data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>UserName</td>
<td>Char (254)</td>
<td>User name (UNIQUE)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format $YYYY-MM-DD HH:MM:SS$</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format $YYYY-MM-DD HH:MM:SS$</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

**See also**
- Security Database Tables
- RSA SecurID User

### 2.5.25 DWRSGM: RSA SecurID Group Members

Security Database Tables store RSA SecurID Group RSA SecurID User member data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>Integer</td>
<td>RSA SecurID Users table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GroupID</td>
<td>Integer</td>
<td>RSA SecurID Groups table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format $YYYY-MM-DD HH:MM:SS$</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format $YYYY-MM-DD HH:MM:SS$</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

**See also**
- Security Database Tables
- RSA SecurID Group
- RSA SecurID User

### 2.5.26 DWSERV: Impero Security Servers

Security Database Tables store Security Server List data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>Char (254)</td>
<td>Server name (PRIMARY KEY)</td>
</tr>
</tbody>
</table>
See also
Security Database Tables
Security Server List

2.5.27 DWTODO: Scheduled Job Actions

Security Database Tables store Scheduled Job actions data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>JobID</td>
<td>Integer</td>
<td>Scheduled Job table record number</td>
</tr>
<tr>
<td>ExecuteAt</td>
<td>Char (20)</td>
<td>Execute time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>Action</td>
<td>Integer</td>
<td>Action type number</td>
</tr>
<tr>
<td>Operand</td>
<td>Integer</td>
<td>Record number in group table</td>
</tr>
<tr>
<td>Operator</td>
<td>Integer</td>
<td>Action executed by number</td>
</tr>
<tr>
<td>P1</td>
<td>Char (254)</td>
<td>Parameter 1 (additional action specification)</td>
</tr>
<tr>
<td>P2</td>
<td>Char (254)</td>
<td>Parameter 2 (additional action specification)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
</tbody>
</table>

See also
Security Database Tables
Scheduled Job

2.5.28 DWUSER: Impero Guest ID

Security Database Tables store Impero Guest ID data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>UserName</td>
<td>Char (32)</td>
<td>Impero Guest ID name (UNIQUE)</td>
</tr>
<tr>
<td>Description</td>
<td>Char (64)</td>
<td>Optional description</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
</tbody>
</table>
### Password Management

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Char (32)</td>
<td>Checksum of password</td>
</tr>
<tr>
<td>PwdUsed</td>
<td>Char (20)</td>
<td>Password last use time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>PwdChanged</td>
<td>Char (20)</td>
<td>Password last change time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>PwdWrong</td>
<td>Integer</td>
<td>Number of wrong passwords entered</td>
</tr>
<tr>
<td>PwdNum</td>
<td>Integer</td>
<td>Number of recent passwords that cannot be used</td>
</tr>
<tr>
<td>Pwd0</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd1</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd2</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd3</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd4</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd5</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd6</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd7</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd8</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>Pwd9</td>
<td>Char (32)</td>
<td>Old password checksum</td>
</tr>
<tr>
<td>ForceChange</td>
<td>Integer</td>
<td>0 = password change not required, 1 = password change required</td>
</tr>
<tr>
<td>Callback</td>
<td>Char (254)</td>
<td>Fixed callback phone number</td>
</tr>
<tr>
<td>CBmode</td>
<td>Integer</td>
<td>Callback mode: 0 = No, 1 = Fixed, 2 = Roving</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

### See also

- [Security Database Tables](#)
- [Impero Guest ID](#)

#### 2.5.29 DWUSGR: Impero Guest ID Group Members

Security Database Tables store Impero Guest ID Group Impero Guest ID member data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>UsrID</td>
<td>Integer</td>
<td>Impero Guest ID table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GrpId</td>
<td>Integer</td>
<td>Impero Guest ID Group table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

### See also

- [Security Database Tables](#)
- [Impero Guest ID Group](#)
### 2.5.30 DWWKGM: Windows Workstation Group Members

Security Database Tables store Windows Workstation Group Windows Workstation member data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WkstID</td>
<td>Integer</td>
<td>Windows Workstation table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GrpId</td>
<td>Integer</td>
<td>Windows Workstation Group table record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Windows Workstation Group
Windows Workstation

### 2.5.31 DWWKSG: Windows Workstation Group

Security Database Tables store Windows Workstation Group data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Integer</td>
<td>Record number (PRIMARY KEY)</td>
</tr>
<tr>
<td>GroupName</td>
<td>Char (254)</td>
<td>Windows group name</td>
</tr>
<tr>
<td>Domain</td>
<td>Char (254)</td>
<td>Domain name (UNIQUE)</td>
</tr>
<tr>
<td>Enabled</td>
<td>Integer</td>
<td>0 = Disabled, 1 = Enabled</td>
</tr>
<tr>
<td>Created</td>
<td>Char (20)</td>
<td>Creation time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>CreatedBy</td>
<td>Char (64)</td>
<td>Creator Windows user name</td>
</tr>
<tr>
<td>Modified</td>
<td>Char (20)</td>
<td>Modification time stamp in format YYYY-MM-DD HH:MM:SS</td>
</tr>
<tr>
<td>ModifiedBy</td>
<td>Char (64)</td>
<td>Modifier Windows user name</td>
</tr>
</tbody>
</table>

See also

Security Database Tables
Windows Workstation Group

### 2.5.32 DWWKST: Windows Workstation

Security Database Tables store Windows Workstation data in this table that has this key structure:

<table>
<thead>
<tr>
<th>Key</th>
<th>Format</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

115
See also

Security Database Tables
Windows Workstation

2.6 Impero Security Server Setup


**Note:** To run Impero Security Management with a local test database, install Impero Security Manager and Impero Security Server on the same computer. To run Impero Security Server with a working Security Database, for fault tolerance and load balancing install Impero Security Server preferably on multiple network server computers that run continuously. The Impero Security Server program file NSSW32.EXE resides in the directory where Impero Security Server is installed.

To load Impero Security Server, select **Start > All Programs > Impero Connect > Security Server** or run its program file NSSW32.EXE.

The **Impero Security Server** window:

- resembles the Impero Host window. See the User’s Guide. Set up Impero Security Server as a Host just like Impero Host.

**Note:** The Impero Host Help system is available on-line from the Impero Security Server window.

Select the **Tools** menu **Security Server Setup** command to show this window:

It logs Impero Security Server on to a Security Database.

**ODBC Setup**

Fields are disabled when logged on to a Security Database.

**Data Source Name (DSN): [] [...]**: Specify in this field the path, if applicable, and data source name of the Security Database that you want to log on to (default: Impero_Security_Evaluation, the local test database). Click [...] to display the Windows Select Data Source window to select a data source to show its path and name in the field.

**User ID: []**: Specify in this field the Security Database logon user name. The local test database requires no user name.

**Password: []**: Specify in this field the Security Database logon password. The local test database requires no password.

[Logon.../Logoff...]: Click on this button to log on to/log off from the Security Database.
Information

**Status**: The Security Database logon status is displayed. **Running** means logged on to the Security Database.

**Security Server Group ID**: The 32-digit hexadecimal Security Server Group ID is displayed when Impero Security Server is logged on to the Security Database.

**Note**: You cannot copy the Security Server Group ID from this window but from the Security Server Group Name window.

This section includes these topics:

- Security Server Tab
- Run As Tab
- Communication Setup

**See also**

Local test database
Impero Security Manager
Security Database Setup
Security Server Group Name window

2.6.1 Security Server Tab

The Impero Security Server window tab panel contains an additional Security Server tab:

![Security Server Tab](image)

It displays the Impero Security Server and Impero Security Server Group status.

**Security Server Status []**: This disabled field displays the Impero Security Server Security Database logon status.

The pane displays the records of group security servers in a table with these column contents:

- **Name**: Host ID.
- **Started**: Security Database logon date and time.
- **Status**: Security Database logon status

**Note**: On this tab, Security server running means that the security server is logged on to the security database. It has no relation to the security server communication status that is displayed in the title bar.

**See also**

Impero Security Server window
Impero Security Server Setup
Impero Security Server Group
Security Database Setup
Communication Setup

2.6.2 Run As Tab

If Impero Security Server runs on a computer on which no user is logged on, which is typically the case with server computers, it has no rights to query a domain controller for Windows user and group information. To achieve these rights, Impero Security Server must run as a Windows account with these rights.

Click the toolbar Program Options button or select the Tools menu Program Options command to show the Program Options window. Select the Run As tab:
It enables running Impero Security Server as a specified Windows account.

**Enable**: Check this box to enable the fields below (default: unchecked).

**User name**: Specify in this field a Windows user name.

**Password**: Specify in this field the matching password.

**Domain**: Specify in this field the matching domain.

**Automatically change to random password every week**: Check the box to randomly change the password immediately and on a weekly basis to automatically satisfy a password change policy.

**Caution!** Do not check this box if the specified Windows user name is used by a person, as the person does not know the randomly generated password. Typically, create a Windows user account exclusively for this purpose.

**See also**

Impero Security Server Setup

2.6.3 Communication Setup

Impero Hosts can request security roles for connecting Guests from Impero Security Server by networking communication devices (TCP/IP, IPX or NetBIOS).

To respond to such requests, communication profiles that match the communication profiles used by requesting Hosts must be enabled on Impero Security Server.

In a typical setup, the **TCP/IP** communication profile that by default is enabled satisfies this demand.

Manage Impero Security Server communication profiles from the toolbar **Communication Profiles** button or **Tools** menu **Communication Profiles** command **Communication Profile Setup** window. See the **User's Guide**.

**Note**: The Impero Host Help system is available on-line from the Impero Security Server window.

**See also**

Impero Security Server Setup

Impero Security Server window

2.7 Use Impero Security Management

This main section includes these sections:

- **Prerequisites**
- **Maintenance**
- **Security**
- **Database Systems**
- **Additional Tools**

2.7.1 Prerequisites

To use Impero Security Management, this must be in place:

1. You must configure a Security Server Database with a Public Key. This is used to generate a Private Key to help secure a trusted connection between your Hosts and Security Servers.

2. At least one Impero Security Server must be in the Security Server List and if also Impero Access Server enabled Hosts shall be serviced, at least one Impero Security Server in the group must be
Access Server enabled.

3. Role Assignments for all relevant Guests with all Hosts that use Impero Security Server must exist in the security database.

4. If using Windows Definitions, Impero Security Servers with no user logged on to the computer must run as a Windows user account.

5. Impero Security Servers must be logged on to the Security Database.

6. Impero Security Server communication status must be Running using communication profiles that match the communication profiles used by the Hosts using it.

7. Hosts must select Use Impero Security Server and specify the Public Key specified in the Security Database.

When this is in place, Impero Security Management can run unattended to service security role requests from Hosts.

See also
Security Database Wizard
Security Server Public Key
Impero Security Server Setup
Security Server List
Access Server enabled
Role Assignment
Windows Definitions
Run As Tab
Security Database Setup
Communication Status

2.7.2 Maintenance

When installing a new Impero Connect version or build, follow this update instruction:


2. Reinstall all Impero Security Managers and Impero Security Servers without loading them.

3. Load one Impero Security Manager to automatically update security database tables.

4. Load and start all Impero Security Servers.

Note: Do not enable scheduled Web Update on Impero Security Servers.

All cooperating Impero Security Managers and Impero Security Servers should use the same version and build to avoid database conflicts.

Administrators should frequently test Impero Security Management performance to see if any settings need to be adjusted.

From time to time, administrators must work with Impero Security Manager to manage Scheduled Jobs and adjust Role Assignments with organizational changes.

See also
Impero Security Manager
Impero Security Server Setup
Scheduled Jobs
Role Assignment
2.7.3 Security

Impero Security Servers should be adequately protected against unauthorized direct and remote access.

The Security Database should also be adequately protected. Advanced database systems typically have their own security schemes.

The connection between Hosts and Security Servers is secured by using a unique Public Key. The Public Key must be generated in the Security Manager and implemented on the Hosts before deployment.

Impero Security Servers generally need only read access to Security Database Tables. However, all Impero Security Servers must have write access to DWDONE: Security Log and DWEVNT: Impero Log tables to log events and to DWUSER: Impero Guest ID to apply password changes.

Impero Security Management administrators need rights to change the contents of Security Database Tables, in particular the right to delete records from DWDONE: Security Log and DWEVNT: Impero Log tables to clean up logs.

See also

[Impero Security Server Setup](#)
[Security Database Setup](#)
[Security Database Tables](#)
[DWDONE: Security Log](#)
[DWEVNT: Impero Log](#)
[DWUSER: Impero Guest ID](#)

2.7.4 Database Systems

Impero Security Management has been tested only with a limited range of database systems. Therefore, it may be that administrators can experience problems if implementing Impero Security Management with a database system with which it was not tested.

Although Impero’s responsibility ends with the ODBC interface, we are interested in learning about difficulties in implementing Impero Security Management with different database systems so that we can assist users that encounter similar problems.

2.7.5 Additional Tools

Impero Security Management includes these additional tools:

- **AMPLUS.EXE**
- **AMPLUS.ZIP**
- **ImperoLOG.ZIP**

2.7.5.1 AMPLUS.EXE

**AMPLUS.EXE** can import a Impero Access Server setup into a Security Database.

From the **Impero Access Server Configuration** window **Main Setup** window, you can export Guests, Hosts and Access Profiles into these comma separated values (csv) configuration files:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Record Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST.TXT</td>
<td>&lt;Host ID&gt;,&lt;Comment&gt;,&lt;Host ID Group&gt;</td>
</tr>
<tr>
<td>GUEST.TXT</td>
<td>&lt;Guest ID&gt;,&lt;Comment&gt;,&lt;Guest ID Group&gt;,&lt;Password&gt;,&lt;Administrator Y/N&gt;,</td>
</tr>
<tr>
<td></td>
<td>&lt;Enabled Y/N&gt;,&lt;ForceChange Y/N&gt;</td>
</tr>
<tr>
<td>PROFILE.TXT</td>
<td>&lt;Guest ID Group&gt;,&lt;Host ID Group&gt;,&lt;Rctl Y/N&gt;,&lt;Keyb Y/N&gt;,&lt;Lckm Y/N&gt;,&lt;Boot Y/N&gt;,</td>
</tr>
</tbody>
</table>
AMPLUS.EXE can import Impero Definitions structured like this into the Security Database by using this command syntax:

```
AMPLUS -F <Import file name>
```

Specify the import file like this:

```
LOGON <ODBC data source name> <User name> <Password>
IMPORT
LOGOFF
EXIT
```

Save the import file as e.g. AMPLUS.IMP.

Place the import file and the GUEST.TXT, HOST.TXT and PROFILE.TXT configuration files in the Impero Security Server program directory where AMPLUS.EXE resides and run this command:

```
AMPLUS -F AMPLUS.IMP
```

This imports the Impero Definitions into the Security Database.

See also

Security Database Setup
Impero Definitions

2.7.5.2 AMPLUS.ZIP

Impero Security Server and Impero Security Manager use the same interface to the database.

AMPLUS.ZIP contains the C++ source for use with this API.

2.7.5.3 IMPEROLOG.ZIP

ImperoLOG.ZIP contains tools for creating your own Impero logging DLL file.
3 Impero Gateway

This main section explains the functionality of Impero Gateway.

Impero Gateway is a Impero Host with the added capability of routing Impero communication between different communication devices.

This main section contains these sections:

- Impero Gateway Functionality
- Impero Gateway Setup
- Use Impero Gateway

3.1 Impero Gateway Functionality

Impero Gateway can receive Impero communication that uses one communication device and send it using another communication device. This ability enables Impero 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.

Impero Gateway functionality categorizes communication devices into these groups:

- **Inside** communication devices:
  - Networking communication devices can communicate among multiple computers in a network or terminal server environment by analogy with communication among people in a conference. Impero supports the Networking communication devices TCP/IP, IPX, NetBIOS and Terminal Server.

- **Outside** communication devices:
  - Point-to-point communication devices can communicate between two computers that are connected by a telephone connection or another type of one-to-one communication link such as infrared. Impero supports the Point-to-point communication devices ISDN (CAPI), Windows modem, Serial and Infrared (IrDA).
  - Network point-to-point communication devices can communicate between two computers across a network. Impero supports the Network point-to-point communication devices TCP/IP (TCP) and TCP/IP (TCP IPv6).

*Note:* Impero communication devices are explained in the User's Guide.

This section includes these sections:

- Incoming and Outgoing
- Outgoing to Incoming
- Networking to Networking
- Typically Disabled: Incoming to Outgoing

See also

- Impero Gateway
- Impero in Terminal Server Environments

3.1.1 Incoming and Outgoing

Impero Gateway on a network computer can route Impero communication between a network computer or terminal server environment Impero module that uses an inside communication devices and a Impero Gateway connected Impero module that uses an outside communication device:
You can edit each Impero Gateway communication profile that uses an outside communication device to support only incoming (outside to inside) communication or only outgoing (inside to outside) communication or in some cases also both at the same time.

See also
- Impero Gateway
- Impero in Terminal Server Environments
- Inside Communication Device
- Outside Communication Device
- Communication Setup

3.1.2 Outgoing to Incoming

Two Impero Gateways that communicate by an outside communication device can route communication between Impero modules on separate networks or in separate terminal server environments. Impero Gateway at one end routes outgoing communication and Impero Gateway at the other end routes the incoming communication.

This setup is typically used between geographically separated corporate entities that communicate by a secure connection directly or across the Internet.

See also
- Impero Gateway
- Outside Communication Device
- Impero in Terminal Server Environments
- Outgoing
- Incoming

3.1.3 Networking to Networking

Impero Gateway can route Impero communication between Impero modules that use mutually incompatible Networking communication devices.

See also
- Impero Gateway
- Networking

3.1.4 Typically Disabled: Incoming to Outgoing

Typically, Impero Gateway cannot route Impero communication between two outside communication devices on the same Impero Gateway or through two Impero Gateways on a network.

This ability is intentionally disabled, as it can cause an uncontrolled propagation of network communication (broadcast storm).

You can apply Impero.ini file DTL section settings that enables Impero Gateway incoming communication to be routed outgoing through another network Impero Gateway.

See also
- Impero Gateway
- Outside Communication Device
- Settings
- Incoming and Outgoing
3.2 Impero Gateway Setup


If the network is protected by a perimeter firewall, to avoid compromising firewall security install Impero Gateway in the firewall demilitarized zone.

To load Impero Gateway, select Start > All Programs > Impero Connect > Gateway or run its program file NGW32.EXE.

The Impero Gateway window:

- resembles the Impero Host window. See the User’s Guide. Set up Impero Gateway as a Host just like Impero Host.

Note: The Impero Host Help system is available on-line from the Impero Gateway window.

To enable Impero Gateway Functionality, set up communication and security as explained in these sections:

- Communication Setup
- Security Setup

See also

Impero Gateway
Impero Gateway and Firewall
Impero Gateway Setup
Impero Gateway Functionality

3.2.1 Impero Gateway and Firewall

Networks are typically protected by a perimeter firewall. To avoid compromising firewall security, Impero Gateway must be installed in the firewall demilitarized zone (DMZ) as illustrated in the example below:

The outside Impero Guest with IP address 192.168.0.1 listens on receive port 1234 with the communication devices TCP/IP (TCP) and/or TCP/IP (UDP).

Impero Gateway is installed on a computer in the firewall DMZ with two IP addresses, 192.168.16.3 that listens on receive port 5678 with the communication devices TCP/IP (TCP) and TCP/IP (UDP), and 192.168.20.4 that listens on receive port 6789 with the communication device TCP/IP (UDP).

The inside Impero Host with IP address 192.168.20.5 listens on receive port 7890 with the communication device TCP/IP (UDP).

Firewall Rules

Referring to this setup, these firewall rules must be implemented:

1. Routing shall be allowed between 192.168.0.1:1234 and 192.168.16.3:5678 using TCP or UDP.
2. Routing shall be allowed between 192.168.20.4:6789 and 192.168.20.5:7890 using UDP.

Firewall Setup

Implement firewall rule 1 and test it by connecting from the outside Impero Guest to Impero Gateway.
Implement firewall rule 2 and test it by unloading Impero Gateway, loading Impero Guest on the
Impero Gateway computer and connecting from the Impero Gateway computer Impero Guest to the
inside Impero Host.

On the Impero Gateway computer, unload Impero Guest and reload Impero Gateway. Test both
connections by connecting from the outside Impero Guest to the inside Impero Host.

To connect by TCP, use the relevant communication profile that uses TCP. To connect by UDP,
enable the relevant communication profile that uses UDP at loading and connect using the
communication profile <Any initialized communication> to request that Impero Gateway routes
the communication to enabled networking communication profiles.

Test that you cannot connect from the outside Impero Guest to the inside Impero Host if Impero
Gateway is stopped (communication is disabled).

WebConnect 2 enabled Gateway

If connecting through the Gateway using WebConnect 2, no incoming ports need to be open in the
firewall, no firewall rules apply.

Outbound communication to the WebConnect 2 service is TCP:443 and/or HTTP:80.

See also

Impero Gateway

3.2.2 Communication Setup

Impero Gateway communicates with other Impero modules through communication hardware
connected to the Impero Gateway computer. To service Impero modules on network computers, the
Impero Gateway computer must have at least one network connection. To service Impero modules
on computers communicating through Point-to-point connections, matching communication
equipment must be connected to the Impero Gateway computer.

If multiple external modem connections are demanded for availability and load balancing, multiple
Impero Gateways with each one or multiple modems is typically installed on larger networks.

Click the toolbar Communication Profiles button or select the Tools menu Communication
Profiles command to show this window:

This window is explained in the User's Guide.

Impero Gateway automatically assigns to each enabled communication profile a Impero Net Number
that is displayed to the right.

You can create or edit communication profiles in the Impero Gateway Communication Profile Edit
window:

The upper and lower sections of this window are explained in the User's Guide. The middle
Gateway settings section is included only with Impero Gateway.

Gateway settings

Device group: [ ]: This field is disabled if an inside communication device is selected in the
Communication information section Communication device drop-down box or if Incoming
connections only is selected in the Connection direction section. Otherwise, it displays the Device
Group name of the communication profile selected in the Communication Profile Setup window
when the Communication Profile Edit window was showed, initially GATEWAY. You can specify
another device group name in the field (max. 10 characters).

Note: Device Group names should identify the outside communication profile type to users that
connect to Impero Gateway from the network or the terminal server environment.

**Impero net (10..127): []**: This field is empty unless a communication profile that was assigned a Impero Net Number is being edited. Optionally, specify in the field a number in the specified range to assign this Impero Net Number to the communication profile. If unspecified, Impero Gateway automatically assigns an unused Impero Net Number to the communication profile when selected to become enabled in the Communication Profile Setup window.

**Note**: Rules apply to assigning Impero Net Number to communication profiles.

Connection direction

This section is disabled if an inside communication device is selected in the Communication information section Communication device drop-down box.

Select one of these options:

**Incoming and outgoing connections**: Select this option to allow incoming as well as outgoing connections (default selection unless TCP/IP (TCP) or TCP/IP (TCP IPv6), see the note below).

**Note**: This option is disabled if TCP/IP (TCP) or TCP/IP (TCP IPv6) is selected in the Communication information section Communication device drop-down box.

**Incoming connections only**: Select this option to allow only incoming connections (default selection if TCP/IP (TCP) or TCP/IP (TCP IPv6), see the note above).

**Outgoing connections only**: Select this option to allow only outgoing connections.

To enable Impero Gateway incoming communication to be routed outgoing through another network Impero Gateway, add this section to the Impero.ini file:

```
[DTL]
GWRestrictedBroadcast=0
GWAllowFullBroadcast=1
```

This section includes these sections:

- **Device Group**
- **Impero Net Number**

See also

- Impero Gateway
- Point-to-point
- Impero Net Number
- Inside communication
- Device Group
- Outside communication
- Terminal Server Environment
- Incoming and Outgoing

3.2.2.1 Device Group

Specify a **Device Group** name to identify a Impero Gateway outside communication profile to enable network Impero modules to connect outgoing through a network Impero Gateway by this communication profile. You can specify any unique name of up to 10 characters, typically the name of the communication device used by the communication profile. If different Impero Gateway outside communication profiles available on the same network use the same communication device, add further distinctions to each **Device Group** name.

**Note**: Specify the same Device Group name for multiple functionally identical Impero Gateway outside communication profiles on the same network to enable connecting through any available Impero Gateway. Typically, network administrators specifies which Device Group names shall be used.

Network Impero modules can specify or browse for and select a **Device Group** name to use any available network Impero Gateway with an outgoing communication profile with the desired
functionality.

**Example**

Functionally identical analog modems are connected to multiple Impero Gateway computers on a network. Network administrators decide that these connections shall form a Device Group named **Analog** to assign the Device Group name **Analog** to the communication profiles of all these connections:

![Diagram](image)

A network Impero module that using a communication profile that uses the Gateway communication device specifies or selects the Device Group Analog connects through the first found Impero Gateway that has an outside communication profile with the Device Group name Analog available.

**See also**

Device Group
Impero Gateway
Outside
Incoming and Outgoing

3.2.2.2 Impero Net Number

Impero assigns Impero net numbers to Impero Gateway communication profiles to distinguish them from each other. If Impero Gateway runs on multiple computers on a network, these rules apply:

1. The Impero net number assigned to any Impero Gateway communication profile that uses a specific configuration of a networking communication device must be the same on the entire network.

2. The Impero net number assigned to any Impero Gateway communication profile that uses an outside communication device must be unique on the entire network and different from the Impero net number assigned to any Impero Gateway communication profile that uses a networking communication device.

**Note:** If the Impero net numbers assigned manually or automatically do not satisfy these rules, they must be changed to satisfy the rules.

**Example**

Network administrators have decided on these networking communication profile Impero net numbers:

- 100: TCP/IP
- 101: IPX
- 102: NetBIOS

All network Impero Gateways must use these networking communication profile Impero net numbers and any network Impero Gateway communication profile that uses an outside communication device must use a unique Impero net number that is different from these numbers.

![Diagram](image)

**Note:** The Impero Gateway window tab panel Communication tab has an additional Net column that displays the Impero net numbers of enabled communication profiles.

**See also**

Impero net
Impero Gateway
Networking
Outside
3.2.3 Security Setup

Impero Gateway security can protect the network against unauthorized access through an Impero Gateway on which incoming communication profiles are enabled. Impero Gateway security applies not only to Impero Guests that connect to start a session or execute an action with a network Impero Host but also to Impero Hosts that connect to request help from a network Impero Guest.

You can set up Impero Gateway security in the Guest Access Security window that on Impero Gateway in addition to the usual tabs includes a Gateway Access Privileges tab:

**Note:** The Guest Access Security window is explained in the User's Guide.

This tab specifies Impero Gateway security settings.

**Gateway access method**

The list of the drop-down box contains these options:

- **Grant all Guests default access privileges** (default selection)
- **Grant each Guest individual access privileges using Impero authentication**
- **Grant each Guest individual access privileges using Windows Security Management**

Select an option in the list to show it in the field. With each selection, the section below has different contents that are explained in the sections linked to above.

**See also**

Impero Gateway

Incoming and Outgoing

### 3.2.3.1 Grant all Guests Default Access Privileges

With this selection on the Impero Gateway Guest Access Security window Gateway Access Privileges tab, this Default access privileges assigned section is displayed:

**Note:** Clear both fields to disable password protection.

**Call back**

Select one of these options:

- **No call back:** Do not apply call back (default selection).

**Call back to:** Specify in the field a telephone number or IP address to make the Impero Gateway disconnect and connect to the specified telephone number or IP address.

**Note:** Call back to a specified telephone number or IP address enables connections only from the specified Impero module address. Other Impero module address restriction options are explained in
Roving call back: This selection requests that the connecting Impero module specifies a telephone number or IP address to call back to. When received, the Impero Gateway disconnects and connects to the specified telephone number or IP address.

**Note:** Roving call back is typically used to make connection costs payable by the Impero Gateway organization, e.g. when a traveling employee connects to the home computer.

When a Impero module connects through a Impero Gateway on which *Grant all Guests default access privileges* is selected, if a password is specified Impero Gateway requests it. If no password is required or if the connecting Impero module specifies the correct password, Impero Gateway routes the connection.

**See also**

- Impero Gateway
- Gateway Access Privileges
- Security Role

### 3.2.3.2 Grant Each Guest Individual Access Privileges Using Impero Authentication

With this selection on the Impero Gateway **Guest Access Security** window **Gateway Access Privileges** tab, this *Individual Guest access privileges assigned* section is displayed:

It contains a pane, buttons and sections.

The pane displays the Security Role folders that expand into records of Guest Profiles that have been assigned the Security Role.

By default, the pane displays the Security Role folder **Allow routing** that does not expand into any Guest Profile records. In the image above, a Guest Profile record has been added to the **Allow routing** Security Role folder for illustration. Double-click a Security Role folder to close (collapse) or open (expand) it to show records of Guest Profiles that have been assigned this Security Role. You can move Guest Profile records up and down, also between Security Role folders, by drag and drop.

If you select a Security Role folder, the **Allow Guest to** section is displayed to the right.

If you select a Guest Profile record, the **Password** and **Call back** sections is displayed to the right. In these sections, you can change these properties of the selected Guest Profile record.

Right-click in the pane to show this context menu:

**Note:** Add Security Role is included in the menu only if a Security Role folder is selected.

### Add Security Role

Select this command or click the **Add Security Role** button below to show this window:

It specifies the properties of a Security Role.

**Name of Security Role:** [ ]: Specify in this field the Security Role name.

**Allow Guest to:** This section always contains a disabled checked box that is labeled *Be routed via the Gateway* signifying that this Security Role property always applies.

**Note:** To organize Guest Profile records in different Security Role folders, you may want to create differently named Security Roles. However, all Impero Gateway Security Roles have the same property.
Add Guest
Select this command or click on the Add Guest button below to show this window:

It specifies the properties of a Guest Profile.

**Guest ID:** Specify in this field the name by which the connecting Impero module identifies itself to the Impero Gateway.

**Note:** Even a Impero Host or extended Host that requests help through a Impero Gateway must identify itself by a Guest ID.

**Password:** See Password.

**Delete:** Select in the pane a Security Role folder or a Guest Profile record and select this command or click on the Delete button below to show a confirmation window to confirm deleting it.

**Caution!** Deleting a Security Role folder deletes all Guest Profile records into which it expands.

**Rename:** Select in the pane a Security Role folder or a Guest Profile record and select this command to show this window:

**Rename security role/Guest:** You can edit the name in the field to rename the selected Security Role folder or Guest Profile record.

When a Impero module connects through a Impero Gateway that uses Grant Each Guest Individual Access Privileges Using Impero Authentication, Impero Gateway requests Impero credentials (Guest ID and Password). If the returned credentials match the credentials of a Guest Profile, Impero Gateway routes the connection.

See also

**Impero Gateway**
**Gateway Access Privileges**
**Security Role**
**Allow Guest to**
**Password**
**Call back**

3.2.3.3 Grant Each Guest Individual Access Privileges Using Windows Security Management

With this selection on the Impero Gateway **Guest Access Security** window Gateway Access Privileges tab, this Individual Guest access privileges assigned section is displayed:

It contains a pane, buttons and sections.

The pane displays the Security Role folders that expand into records of Windows Groups and Users that have been assigned the Security Role.

By default, the pane displays the Security Role folder Allow routing that does not expand into any Windows Group or User records. In the image above, one Windows Group record and one Windows User record have been added to the Allow routing Security Role folder for illustration. Double-click a Security Role folder to close (collapse) or open (expand) it to display the records of Windows Groups and Users that have been assigned this Security Role. You can move Windows Group and User records up and down, also between Security Role folders, by drag and drop.

If you select a Security Role folder, the Allow Guest to section is displayed to the right.

If you select a Windows Group or User record, the Domain, RAS and Call back sections and the Windows User Manager button is displayed to the right.
Right-click in the pane to show this context menu:

Note: Add Security Role and Rename are included in the menu only if a Security Role folder is selected.

Add Security Role
Select this command or click the Add Security Role button below to show the Security Role window to add a Security Role folder in the pane.

Note: To organize User and Group records in different Security Role folders, you may want to create differently named Security Roles. However, all Impero Gateway Security Roles have the same property.

Add User
Select this command or click the Add User button below to show on a Windows 2000+ computer the Windows Select Users window to select one or multiple Windows users of which records are added to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

On a Windows NT or 9x computer, this window is displayed:

Which domain is the account in: []: The list of this drop-down box displays the names of the domains recognized by the Impero Gateway computer. Select one in the list to show it in the field.

Select the account to add: []: The list of this drop-down box contains the names of the Windows users in the domain whose name is shown in the Which domain is the account in drop-down box field. Select one in the list to show it in the field.

Click on OK to add a record of the selected Windows user to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

Add Group
Select this command or click the Add Group button below to show on a Windows 2000+ computer the Windows Select Groups window to select one or multiple Windows groups of which records are added to the selected Security Role folder or the Security Role folder of the selected Windows User or Group record.

On a Windows NT or 9x computer, the Choose Account window showing groups instead of users is displayed to add a Group record in the pane.

Delete: Select a Security Role folder or a User or Group record in the pane and select this command or click on the Delete button below to show a confirmation window to confirm deleting the selected folder or record.

Caution! Deleting a Security Role folder deletes all User and Group records in it.

Rename: Select a Security Role folder and select this command to show the Rename window to rename it.

Domain
This section displays a description the domain of the selected Windows User or Group record.

RAS
This section is included only if Impero Gateway runs on a Windows 2003, XP, 2000 or NT operating system computer.

Get call back information from Windows NT Remote Access Service (RAS): Check this box to use call back information stored in Windows NT Remote Access Service (default: unchecked).
Call back

This section is not included if the RAS section box is checked. See Call back.

**Windows User Manager**: This button is included only if the Impero Gateway runs on a Windows 2003, XP, 2000 or NT operating system computer. Click it to show the Windows user manager window according to the rights of the user logged on to Windows on the Impero Gateway computer to manage Windows users and groups.

When a Impero module connects through a Impero Gateway that uses *Grant Each Guest Individual Access Privileges Using Windows Security Management*, Impero Gateway requests the Windows credentials (*User name*, *Password* and *Domain*). Impero Gateway queries Windows Security Management for validation of the returned credentials and for information on the group memberships of the identified user. If the identified user matches a User or Group record, Impero Gateway routes the connection.

See also

- Impero Gateway
- Gateway Access Privileges
- Security Role
- Allow Guest to
- Rename

### 3.3 Use Impero Gateway

Communication Setup is straightforward if only one Impero Gateway is available on the network. Name Device Groups to enable network users to select the right communication device for their outgoing connections.

If multiple Impero Gateways are available on a network, pay attention to selecting valid Impero Net Numbers.

To protect the network against unauthorized access through Impero Gateway, create a Security Setup.

The *Impero Gateway* window tab panel includes a **Routing** tab:

It displays only incoming routing through Impero Gateway.

The pane contains the table records with these column contents:

- **Time**: Connect icon, date and time.
- **User Name**: Connect logon user name if authenticated, otherwise empty.
- **Status**: **Authenticating** if Security Setup specified authentication is incomplete, otherwise **Routing**.
- **Communication Profile**: Outside communication profile name.

Impero Gateway capacity is limited by the number of enabled outside communication profiles, as each outside communication profile can support only one connection at a time.

Running a remote support session through a Gateway using WebConnect 2

**Note**: To achieve a remote support session via a gateway using WebConnect, the Guest and the Gateway need to be configured with credentials from the same account.

To achieve a remote support session from the Impero Guest through a gateway, the Guest user needs to:

1. Select the specific Gateway and click on the **Browse Gateway** button.
The **Gateway browse list** displays the list of Hosts behind the gateway.

2. To connect to a specific host available through the selected Gateway, either double-click on the specific Host or select the Host in the list and click on **Connect**.

**See also**

- Communication Setup
- Impero Gateway
- Device Groups
- Incoming and Outgoing
- Impero Net Numbers
- Security Setup
- Impero Gateway window
- Outside
4 Impero Name Management

This main section explains Impero Name Management and Impero Name Server functionality. Impero Name Server is an Impero Host with the added capability of resolving Impero names into IP addresses.

This main section contains these sections:
- Impero Name Management Functionality
- Impero Name Server Setup
- Running Impero Name Server

4.1 Impero Name Management Functionality

Impero Name Management enables swift Impero connections across large segmented networks including the Internet.

Using the communication device TCP/IP, Impero Name Management enables connecting across large segmented networks by easily remembered Host names or Host user names instead of hard-to-remember IP addresses or by creating elaborate IP broadcast lists.

Note: The TCP/IP communication device is explained in the User's Guide.

Impero Name Management uses one or for load balancing and fault tolerance preferably two Impero Name Servers to resolve Impero names into IP addresses that can be used for connecting across any TCP/IP network including the Internet.

Using Impero Name Management, you can connect by these Impero module names:
- Computer IP address
- Impero Host name (Host ID), if specified
- Impero Host user Windows or network logon name, if enabled
- Impero Guest help service name (help provider name), if enabled
- Impero School class name
- Impero School Student name

Impero users select to use Impero Name Server in communication profiles that use the TCP/IP communication device by specifying one or two Impero Name Servers. See the User's Guide, Dialog box help, Guest dialog boxes, Advanced TCP/IP Configuration. If selected, a yellow pages icon is displayed in the Impero module window status bar.

Impero Name Servers store name information in name spaces. A name space is a virtually private segment of the Impero Name Server database that is available only to Impero modules that specify the matching Name Space ID. Users that want to connect to each other by using Impero Name Management must agree to specify the same Name Space ID on the Program Options window Host Name tab. See the User's Guide.

When communicating, Impero modules that use Impero Name Server automatically identify themselves to their specified Impero Name Servers by all their available names and their specified Name Space ID.

When a Impero module that uses Impero Name Server connects by specifying a Impero name (automatically accompanied by a Name Space ID), one of the selected Impero Name Servers resolves the specified name, if found in the specified name space, into the matching IP address and return it to the connecting Impero module to automatically connect by the resolved IP address.

Impero Name Servers request, at a specified Client refresh rate, that the Impero modules that use it refresh stored name information. Stored name information that has not been refreshed within a specified Server life time is automatically deleted. This ensures that the stored name information is current at all times except for Impero modules that changed names or stopped communicating since their name information was last refreshed.
Impero offers the free service of two Impero Name Servers that are accessible across the Internet. Impero Name Server is also available for local installation for the exclusive use by an organization.

4.2 Impero Name Server Setup


To load Impero Name Server, select Start > All Programs > Impero Connect > Name Server or run its program file NNSW32.EXE.

The Impero Name Server window:

- resembles the Impero Host window. See the User's Guide. Set up Impero Name Server as a Host just like Impero Host.

Note: The Impero Host Help system is available on-line from the Impero Name Server window.

To edit Impero Name Server properties, in the Program Options window select the Impero Name Server tab:

It specifies Impero Name Server settings.

Make this Host a Impero Name Server: Leave this box checked to enable Impero Name Server functionality and the commands below (default: checked).

Client refresh rate: [] Minutes: Specify in this field a number in the range 1 to 99 (default: 5).

Server life time: [] Minutes: Specify in this field a number in the range 1 to 99 (default: 6).

Note: The Client refresh rate value determines the interval at which Impero modules must refresh their name data. The Server life time value determines the maximum age of name data. The Server life time value should be slightly larger than the Client refresh rate value.

Clear database upon startup: Leave this box checked to delete all name data when Impero Name Server is restarted (default: checked).

Note: The Impero Name Server database uses a Impero proprietary format. You cannot access the database separately.

To communicate with Impero modules, at least one communication profile that uses the TCP/IP communication device must be enabled. You can enable multiple differently named communication profiles that use different configurations of the TCP/IP communication device to accommodate Impero modules that use different configurations of the TCP/IP communication device.

Note: The TCP/IP communication device is explained in the User's Guide.

The Impero Name Server window tab panel includes a Name Server tab:

It displays the Impero Name Server status.

Name Server status []: This disabled field displays Running if the Make this Host a Impero Name Server box is checked and Stopped if unchecked.

Number of registered names []: This disabled field displays the number of names currently stored in the Impero Name Server database.
4.3 Use Impero Name Server

When set up and started (communication enabled), Impero Name Server can operate fully automatically and unattended.

The **Number of registered names** field contents provide an indication of the condition of the Impero Name Server.

Each Impero module may account for multiple names, e.g. for Impero Guest multiple help service names and for Impero Host its Host ID and its Windows or network logon user name. IP addresses is not counted as names.

If you restart Impero Name Server with the **Clear database upon startup** box checked, the name count should increase from zero and stabilize after the time set for **Client refresh rate**.

If users have problems connecting to Impero modules in remote network segments, check that the same Impero Name Servers are used and that exactly the same **Name Space ID** is specified at both ends and that communication profiles match between the Impero modules and with the specified Impero Name Servers.

**Firewall Problems**

To connect through a firewall, the firewall must allow communication through the TCP/IP ports used by Impero Name Server communication.

Some firewalls change the port number of outgoing communication to a random port number to protect network computers against unwanted incoming communication. Consequently, Impero Name Server receives and stores an invalid port number.

In that case, on Impero modules in the **Advanced TCP/IP Configuration** window check the **Ignore port information from Name Server** box and in the **Use port** field specify the port number that shall be used for connecting.

**Note:** The **Advanced TCP/IP Configuration** window is explained in the **User’s Guide**.

**See also**

- Impero Name Server Setup
- Number of registered names
- Clear database upon startup
- Client refresh rate
5 Advanced Tools

This main section explains advanced tools for Impero Connect running on Windows operating systems.

It contains these sections:

- Impero in Terminal Server Environments (TSE)
- Impero Guest ActiveX Component
- Impero Scripting ActiveX Control
- Impero Connect Processes and Windows Security

5.1 Impero in Terminal Server Environments (TSE)

Microsoft Windows Terminal Server enable terminal users to log on to the terminal server and run installed applications in a terminal server session.

Impero Connect can be run in terminal server sessions and connect to other Impero Connect modules running in sessions on the same terminal server, another terminal server, or other networked computers.

This section contains these sections:

- Installation (TSE)
- Use (TSE)

5.1.1 Installation (TSE)

On a terminal server, you must install Impero Connect from the Control Panel utility Add or Remove Programs. To avoid problems, any already installed Impero modules should be unloaded during installation.

You can install Impero Guest, Impero Host and Impero Gateway. If Impero modules should communicate with Impero modules outside the TSE, you must install Impero Gateway.

You cannot install Impero Security Server or Impero Name Server on a terminal server.

See also

Impero Gateway
Impero Security Server Setup
Impero Name Server Setup

5.1.2 Use (TSE)

In most respects, TSE Impero modules work like network computer Impero modules that communicate by a networking communication device. However, there are important differences because TSE elements reside on the same computer and share the same computer resources.

This section includes these sections:

- Impero Naming (TSE)
- Impero Communication (TSE)
- Impero Host Functionality (TSE)
- Computer Resources (TSE)

See also

Networking
5.1.2.1 Impero Naming (TSE)

In a TSE, the terminal server console and client sessions share the terminal server computer name and network address.

Impero Host is not allowed to start communicating if another Impero Host communicates by the same name. Therefore, Impero Hosts should not be named by the Windows computer name (the default selection that is recommended for a network computer Impero Host), but preferably by the USERNAME environment variable that names Impero Host by the user name. See the User’s Guide, Host dialog box help, Program Options, Host Name tab.

Client session Impero Guests should also use different Guest IDs because using the same may under certain circumstances cause communication mix-up. See the User’s Guide, Dialog box help, Guest dialog boxes, Program Options, Logon tab.

5.1.2.2 Impero Communication (TSE)

Impero modules communicate inside a TSE by the Terminal Server communication device that is available only on terminal servers. See the User’s Guide, Dialog box help, Guest dialog boxes, Communication Profile Edit.

Between a client session Impero module and a Impero module running on a computer outside the TSE, the preferred communication mode is through a Impero Gateway running on the terminal server.

This section contains these sections:

- Impero Gateway Setup (TSE)
- Connect out of a TSE
- Connect into a TSE
- Connect between TSEs

See also
Impero Gateway

5.1.2.2.1 Impero Gateway Setup (TSE)

To enable communication between TSE Impero modules and Impero modules on computers outside the TSE, load and start Impero Gateway on the terminal server console.

For inside communication, enable a communication profile that uses the Terminal Server communication device.

For outside communication, enable communication profiles that match the communication profiles used by outside Impero modules.

Be aware of the Impero Gateway Communication Setup and Security Setup requirements.

See also
Impero Gateway
Communication Setup
Security Setup

5.1.2.2.2 Connect out of a TSE

To connect from a Impero Guest to an outside Impero Host through a Impero Gateway:

- On Impero Guest, enable the Terminal Server communication profile.

- On Impero Gateway, enable for example the TCP/IP communication profile for outside communication in addition to the Terminal Server communication profile for inside communication.

- On Impero Host, enable the same communication profile as the Impero Gateway outside communication profile, i.e. TCP/IP.
Connect from Impero Guest using *<Any initialized communication>*.

You can also connect directly out of the TSE using a communication profile that uses a point-to-point communication device, for example TCP.

See also

*Impero Gateway*

*Networking*

5.1.2.2.3  Connect into a TSE

You can connect to Impero modules in a TSE only through a terminal server console *Impero Gateway*.

Connect by a communication profile that matches the *Impero Gateway* outside communication profile.

**Connect from Impero Guest to Impero Host**

To connect by networking communication devices:

- On Impero Guest, enable for example the TCP/IP communication profile.
- On Impero Gateway, enable the same communication profile, i.e. TCP/IP, for outside communication in addition to the *Terminal Server* communication profile for inside communication.
- On Impero Host, enable the *Terminal Server* communication profile.
- Connect from Impero Guest using *<Any initialized communication>*.

**Send a help request from Impero Host to Impero Guest**

To connect by networking communication devices:

- On Impero Host, enable for example the TCP/IP communication profile.
- On Impero Gateway, enable the same communication profile, i.e. TCP/IP, for outside communication in addition to the *Terminal Server* communication profile for inside communication.
- On Impero Guest, enable the *Terminal Server* communication profile.
- Connect from Impero Host using *<Any initialized communication>*.

5.1.2.2.4  Connect between TSEs

Connecting between Impero modules in different TSEs combines the requirements of Connect out of a TSE and Connect into a TSE.

The following *Impero.ini* file DTL section settings that enables incoming to outgoing communications must be applied on all Gateways:

```
[DTL]
GWAllowFullBroadcast=1
GwRestrictedBroadcast=0
```

See also

*Connect out of a TSE*

*Connect into a TSE*

*Impero Gateways*

*Networking*

*Enable incoming to outgoing communication*
5.1.2.3 Impero Module Functionality (TSE)

TSE client session Impero modules have mostly the same functionality as a network computer Impero modules. However, certain functionalities are different because Impero modules run on the same computer.

**Blank Display** cannot be implemented the Impero way in a TSE and is therefore disabled.

If implemented, **Restart Host PC** would restart the terminal server computer, which would in most cases be most undesirable. Therefore, this functionality is disabled.

These **Guest Access Security** window **Guest Policy** tab settings can restart the Impero Host computer:
- In the **Password** section selecting **Restart Windows**.
- In the **Disconnect** section selecting **Restart Windows**.

On a TSE client session Impero Host, both of these settings causes the client session user to be logged off from the terminal server.

Remote printing features make little sense in a TSE and are disabled.

**Note:** Client session Impero configuration files are stored in user profile directories.

5.1.2.4 Computer Resources Considerations (TSE)

The terminal server console and client session Impero modules share the same computer resources, namely the terminal server computer resources, limited only by restrictions applied to the users logged on to the terminal server.

This applies to files, installed programs and peripherals such as outside connections and printers. Consider this carefully, particularly when specifying **Guest Access Security** and **Maintenance Password** settings for TSE Impero modules.

5.2 Impero Guest ActiveX Component

The Impero Guest ActiveX component allows programmers to add Impero Guest Connect functionality to an area in a file.

This section includes the following sections:
- **Requirements (ActiveX)**
- **How to Use the Impero Guest ActiveX Component**
- **ImperoX Connect Dialog Box**
- **ImperoX Connection Properties Dialog Box**
- **Programmer Information**

5.2.1 Requirements (ActiveX)

To run the Impero Guest ActiveX component on a computer that uses a Microsoft Windows operating system, these system requirements apply:
- Computer: Pentium
- Memory: 32 MB
- Platform: Windows 2000 SP 4 or later
5.2.2 How to Use the Impero Guest ActiveX Component

To use the Impero Guest ActiveX component, it must be embedded in a graphical area in a file that can be displayed in a container application. Users with ActiveX programming skills can embed Impero Guest ActiveX component in a file based on the included Programmer Information.

The Impero Guest ActiveX component is delivered with a demo that shows you how the Impero Guest ActiveX component works. Run the register.bat file and then the NGuestX-demo.exe file to start the demo:

The Impero Guest ActiveX component is embedded in the white area.

1. Click anywhere in the white area to display the NGuestX Connect dialog box.
2. Click the Properties button to display the ImperoX Connection Properties dialog box.

Note: You can also open the ImperoX Connection Properties dialog box by right-clicking anywhere in the white area.

3. Click the About tab, click the Change button and specify a license key.
4. Click OK in the NGuestX License dialog box and the NGuestX Connection Properties dialog box to close these.

You are now ready to connect to a Host from the NGuestX Connect dialog box.

See also
NGuestX Connect Dialog Box
NGuestX Connection Properties Dialog Box
Programmer Information

5.2.3 NGuestX Connect Dialog Box

Click an area that contains Impero Guest ActiveX component to display this dialog box:

From this dialog box you can connect to a Impero Host on a remote computer.

Remote IP address or computer name: Specify the Impero Host IP address or Host name.

Connect via Impero Gateway: To connect via a Impero Host network Impero Gateway, select this check box and specify the Impero Gateway computer IP address in the field.

Communication
The options available in the Communication section vary depending on the communication profile you select.

Communication profile: Select the communication profile you want to use:
- TCP
- HTTP
- UDP
- WebConnect

Use custom port number: Connection port address. When the Connect via Impero Gateway check box is selected, the port is used for gateway. Enter a number between 1 and 65535. If the check box is not selected, the port number is used for connecting to a remote Host. When the communication profile is changed, the port is automatically updated with the default value for the selected communication profile:
• TCP – 6502
• UDP – 6502
• HTTP – 80

Use HTTP Proxy: This check box is available only when the communication profile is HTTP. Select to use HTTP Proxy. Specify the IP address or Host name of the HTTP profile in the field below the check box.

WebConnect Service URL: This specifies the address of the WebConnect service, i.e. the Connection Manager that facilitates the WebConnect connection. In the credentials fields below specify the credentials by which the Impero module should identify itself when connecting to the Impero WebConnect service. Specify a WebConnect service recognized account and the corresponding password and domain.

Properties: Click this button to display the ImperoX Connection Properties dialog box.

When you click OK, a logon dialog box is displayed. Specify the credentials required by Impero Host.

When connected, the clicked area is replaced by the Impero Host computer screen image.

See also
Area
Impero Guest ActiveX Component
ImperoX Connection Properties Dialog Box

5.2.4 NGuestX Connection Properties Dialog Box

Use the NGuestX Connection Properties dialog box to change properties for either the current connection when connected, or for the next connection, if not connected.

Right-click an area that contains the Impero Guest ActiveX component, or in another NGuestX dialog box, click the Properties button to display this dialog box:

It contains the following tabs:
• Remote Desktop
• Keyboard
• Mouse
• Compression
• Encryption
• Display
• Host Protection
• About

Apply: This button is enabled if property changes have not been saved. Click on the button to save property changes without closing the dialog box.

See also
Area

5.2.4.1 Remote Desktop Tab

This is the NGuestX Connection Properties dialog box Remote Desktop tab:
Desktop

Select your preferred graphic mode for connections:

**Command mode**: Select this option to transfer the Host screen image as commands. Host screen transfer stores the screen image in cache memory and transfers only image changes to save transmission bandwidth and optimize update speed.

**Accelerated bitmap**: Select this option to transfer the Host screen image as accelerated bitmap. The transfer is slower than command mode, but details are displayed with more accuracy.

**Normal bitmap**: Select this option to transfer the Host screen image as bitmap. The transfer is slower than accelerated bitmap mode, but you can use this mode if accelerated bitmap mode causes problems. You can limit the number of display colors to save transmission bandwidth by selecting a setting on the drop-down list.

Optimizations

Increase the performance by disabling Host desktop features:

**Full optimization**: Select this option to disable every feature under **Custom optimization** for the current or next connection.

**Custom optimization**: Select this option to disable/enable features to customize the optimization.

5.2.4.2 Keyboard Tab

This is the NGuestX Connection Properties dialog box **Keyboard** tab:

Use the **Keyboard** tab to select keyboard mode and customize shortcuts for special keystrokes.

**Keyboard mode**

Select a keyboard mode option.

Note that selecting the **Remote keyboard** option may have undesired effects on the Host computer, as special keystroke combinations is also sent to the Host computer.

If Guest and Host computer keyboard layouts are different, you should also select the **Use Guest keyboard layout** check box to avoid problems.

**Key mappings**

You can customize special keystroke combinations.

Assign desired keystroke combinations by selecting check boxes and selecting a character in the drop-down list.

By default, CTRL+Z is assigned to Zoom in and out (switch between the Connect window and full screen).

5.2.4.3 Mouse Tab

This is the NGuestX Connection Properties dialog box **Mouse** tab:

Use the **Mouse** tab to select mouse mode, i.e. which mouse events should be sent to the Host computer. Sending fewer mouse events saves transmission bandwidth.

Select the **Show remote mouse events** check box to display Host computer mouse movements on the Guest computer screen. The Guest computer mouse pointer must be in the Connect window.
5.2.4.4 Compression Tab

This is the **NGuestX Connection Properties** dialog box **Compression** tab:

![Compression Tab]

The Impero ActiveX Guest can compress transmitted data to speed up transmission across slow communication links. However, data compression takes time.

Select one of these options:

- **Automatic compression (Recommended)**: Selects the compression based on the properties of the used communication profile. In most cases, this provides the fastest transmission.
- **No compression**: Typical selection for fast communication links.
- **Low compression**: Typical selection for medium fast communication links.
- **High compression**: Typical selection for slow communication links.

5.2.4.5 Encryption Tab

This is the **NGuestX Connection Properties** dialog box **Encryption** tab:

![Encryption Tab]

The communication between Impero modules can be protected by encrypting transmitted data. Select preferred encryption type.

Communicating Impero modules automatically negotiates to encrypt communication by an encryption type that is enabled on both modules. Impero modules on which no common encryption type is enabled cannot communicate.

5.2.4.6 Display Tab

This is the **NGuestX Connection Properties** dialog box **Display** tab:

![Display Tab]

Remote screen area

Select an option for how large an area of the Host screen should be displayed. Display the entire Host screen or specify a limited area of the Host screen.

In case of more than one Host monitor, specify which monitor should be displayed.

Host screen display properties

- **Fit window to Host screen**: Resize the Connect window to fit the 1:1 scale Host screen image within its display panel. If the Host screen image has more pixels than the maximized Connect window display panel, the display panel has scrollbars.

- **Fit Host screen to window**: Scale the Host screen image to fit within the Connect window display panel.

- **Do not fit**: Display the part of the 1:1 scale Host screen image that fits within the Connect window display panel. If the Host screen image has fewer pixels than the display panel, it is surrounded by black borders. If the Host screen image has more pixels than the display area, the display panel has scrollbars.

- **Enable auto scroll**: Scroll the Host screen image automatically when the mouse pointer comes
close to the window borders.

5.2.4.7 Host Protection Tab
This is the NGuestX Connection Properties dialog box Host protection tab:

Lock Host
Select options to prevent Host users and other Guest users from interfering with ongoing Connect sessions.

Auto take control
Select the Take keyboard and mouse control automatically check box to allow all Guests to take over keyboard and mouse control automatically during multi Guest sessions by using the keyboard or mouse.

5.2.4.8 About Tab
This is the NGuestX Connection Properties dialog box About tab:

In addition to viewing the version and build of the Impero Guest ActiveX component and copyright information, you can change the license and interface language of the component from the About tab.

5.2.5 Connection Status Dialog Box
Click the Impero Host computer screen image and press the Connection Status Dialog hotkey (default: CTRL+ALT+END) to display the following dialog box:

General Tab
The General tab displays general connection information and contains the following buttons:

Start chat: Click this button to start a chat with the Host user. You can save the chat from the Chat dialog box for documentation purposes.

Disconnect: Click this button to disconnect from the Host.

Properties: Click this button to display the NGuestX Connection Properties dialog box and edit remote desktop, keyboard, mouse, compression, encryption, display and Host protection properties and change the license key or language. See NGuestX Connection Properties Dialog Box.

Save log: Click this button to save a communication log.

Session administration tab
Use the Session administration tab to manage multi Guest sessions:

Guests: The field displays the total number of Guests connected to the Host.

Suspend further connections: Click the Suspend button to prevent further connections to the Host. Click the Resume button to allow further connections to the Host again.
**Disrupt Guests**: Click the **Disrupt Guests** button to disconnect all other Guests from the Host.

**Take keyboard and mouse control**: Click the **Take control** button to take control of the keyboard and mouse on the Host computer.

### 5.2.6 Programmer Information

This section includes the following sections:

- `NGuestXLib::_INGuestXCtrlEvents`
- `INGuestXEventParam`
- `INGuestXFont`
- `INGuestXRcArea`
- `INGuestXShortcut`
- `NGuestX Messages`

#### 5.2.6.1 NGuestXLib::_INGuestXCtrlEvents

Event handler interface for INGuestX class.

**Public member functions**

**HRESULT NGuestXLib::_INGuestXCtrlEvents::OnOpenPre ()**

Fired when the NGA instance is about to open by `INGuestXCtrl::Open()` method. The event is not fired when the instance is already opened when `INGuestXCtrl::Open()` is called. The event is always followed by `OnClosePost()` event.

When the event is fired, the `INGuestXCtrl::IsOpen` property is always `false`.

**HRESULT _INGuestXCtrlEvents::OnOpenPost ([in] VARIANT_BOOL Ok)**

Fired when the NGA instance has been opened by `INGuestXCtrl::Open()` method.

When the event is fired, `INGuestXCtrl::IsOpen` property is true if the instance was opened successfully. It is safe to call the `INGuestXCtrl::Close()` in response to `OnOpenPost(true)`.

**Parameters:**

- **Ok** - status of `Open` request
  - `true` - the NGA was opened successfully
  - `false` - failed to open NGA instance.

**HRESULT NGuestXLib::_INGuestXCtrlEvents::OnClosePre ()**

Fired when the NGA instance is about to close by `INGuestXCtrl::Close()` method. The event is not fired when the instance is already closed when `INGuestXCtrl::Close()` is called.

There is the `OnClosePost()` event fired for each `OnClosePre()` event.

When the event is fired, `INGuestXCtrl::IsOpen` is always `true`.

**HRESULT NGuestXLib::_INGuestXCtrlEvents::OnClosePost ([in] VARIANT_BOOL Ok)**

Fired when the NGA instance has been closed by `INGuestXCtrl::Close()` method.
When the event is fired, INGuestXCtrl::IsOpen property is false if the instance was closed successfully. It is safe to call the INGuestXCtrl::Open() in response to OnClosePost(true).

**Parameters:**

Ok - status of Close() request
- true - the NGA was closed successfully
- false - failed to close NGA.

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnConnectPre ()**

Fired if a new connection should be established in response to INGuestXCtrl::BeginSession() function.

The event is fired before any long lasting network operations started.

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnConnectPost ([in] VARIANT_BOOL Ok)**

Fired after OnConnectPre() when a connection was established successfully or NGA failed to establish a new connection.

**Parameters:**

Ok - operation status
- true - the connection established successfully
- false - failed to establish a connection

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnDisconnectPre ()**

Fired after OnEndSessionPre() in response to EndSession() if the connection should be terminated because there is no more active session.

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnDisconnectPost ()**

Fired after OnDisconnectPre() method when NGA has been disconnected from Host.

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnBeginSessionPre ([in] LONG Type)**

The very first event that can be fired in response to INGuestXCtrl::BeginSession() before any long lasting network operations started.

**Parameters:**

Type - session type
- INGuestXCtrl::SessionType_RemoteControl - Connect
- INGuestXCtrl::SessionType_Chat - Text chat

**HRESULT NGuestXLib::_NGuestXCtrlEvents::OnBeginSessionPost ([in] LONG Type, [in] VARIANT_BOOL Ok)**

Fired after OnBeginSessionPre() when a session was established successfully or NGA failed to establish a new session.

When a new connection is created after INGuestXCtrl::BeginSession(), after having OnBeginSessionPre() event, the authentication event should be expected (e.g. OnLoginPassword, OnLoginImpero, etc).

It is safe to open a new session of another type in response to this event only if a INGuestXCtrl::BeginSession() was called with active connection. Otherwise it is safe to start a session only after authentication, i.e. in response to OnSessionStarted() event.

**Parameters:**
Type - session type
- INGuestXCtrl::SessionType_RemoteControl - Connect
- INGuestXCtrl::SessionType_Chat - Text chat

Ok - status of BeginSession request
- true - the session established successfully
- false - failed to establish a session

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre ([in] LONG Type)
Fired when NGA was requested to close a session by INGuestXCtrl::EndSession() method before any long lasting network operations started.

Parameters:
Type - session type
- INGuestXCtrl::SessionType_RemoteControl - Connect
- INGuestXCtrl::SessionType_Chat - Text chat

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost ([in] LONG Type, [in] VARIANT_BOOL Ok)
Fired after OnEndSessionPre() when the session was closed by INGuestXCtrl::EndSession(). It is safe to open a new session of the same type in response to this event.

Parameters:
Type - session type
- INGuestXCtrl::SessionType_RemoteControl - Connect
- INGuestXCtrl::SessionType_Chat - Text chat

Ok - status of EndSession request
- true - the session closed successfully
- false - failed to close a session

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted ([in] LONG Type)
Fired after the session went into the running state after having established a new connection.

Parameters:
Type - session type
- INGuestXCtrl::SessionType_RemoteControl - Connect
- INGuestXCtrl::SessionType_Chat - Text chat

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEndedByHost ()
Fired when a session and connection was ended by Host. OnErrorMsg() event is fired with message #?? after this event.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectionLost ()
Fired after connection was lost. OnErrorMsg() event is fired with message #?? after this event.
HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginPassword ([in] LONG Reason, [in] INGuestXEventParam * EventParam)
Fired when Impero password should be sent to Host.

Default action:
Built-in dialog is displayed to prompt password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginPassword() method.
To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:
- Reason - The why this prompt is needed
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

Fired when Impero Guest ID and password should be sent to Host.

Default action:
Built-in dialog is displayed to prompt for ID and password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginImpero() method.
To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:
- Reason - The why this prompt is needed
- bNss - If the Host is configured for Impero Security Server authentication. When a Host is configured for Nss authentication Guest can change by sending new password with INGuestXCtrl::SendLoginImpero() method.
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginWindows ([in] LONG Reason, [in] INGuestXEventParam * EventParam)
Fired when Windows logon, domain and password should be sent to Host.

Default action:
Built-in dialog is displayed to prompt for logon, domain and password. Event handler can suppress the built-in logon dialog and send password with INGuestXCtrl::SendLoginWindows() method.
To cancel logon INGuestXCtrl::EndSession() function can be called.

Parameters:
- Reason - The why this prompt is needed
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginLdap ([in] LONG Reason, [in] INGuestXEventParam * EventParam)
Fired when LDAP server name, logon and password should be sent to Host.

Default action:
Built-in dialog is displayed to prompt for server name, logon and password. Event handler can
suppress the built-in logon dialog and send password with `INGuestXCtrl::SendLoginLdap()` method.

To cancel logon `INGuestXCtrl::EndSession()` function can be called.

**Parameters:**
- Reason - The why this prompt is needed
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

Fired when logon name, RSA SecurID passcode and password should be sent to Host.

**Default action:**
Built-in dialog is displayed to prompt for logon, RSA passcode and password. Event handler can suppress the built-in logon dialog and send password with `INGuestXCtrl::SendLoginRsa()` method.

To cancel logon `INGuestXCtrl::EndSession()` function can be called.

**Parameters:**
- Reason - The why this prompt is needed
- Shadow - 1 if a Impero password is required in addition to the RSA SecurID PASSCODE.
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginFailed ([in] LONG Reason)
Fired when the logon has been failed.

**Is it safe to open a new session.**

**Parameters:**
- Reason - the reason why logon has failed.

Fired when the server side requires RSA SecurID pin code.

**Default action:**
Built-in dialog is displayed to prompt RSA SecurID pin code. Event handler can suppress the built-in logon dialog and send password with `INGuestXCtrl::SendLoginRsaPin()` method.

**Parameters:**
- Reason - The why this prompt is needed
- Mode - 0 = fixed, 1,2 = selectable (2 has no suggestion).
- SuggestedPin - The suggested pin code if any. May be NULL.
- MinLen - The minimum length for a valid pin code.
- MaxLen - The maximum length for a valid pin code.
- AllowNonNumeric - True if characters other than 0-9 are allowed
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.
HRESULT NGuestXLib::_INGuestXCtrlEvents::OnHostScreenSizeInfo ([in] LONG Width, [in] LONG Height)
Fired when the size of the remote screen is changed.

Parameters:

- Width - new width of the remote screen
- Height - new height of the remote screen

Fired when multi Guest parameters have been updated on Host.

Parameters:

- Event - bitwise combination of the MultiguestEvent_t flags:
  - INGuestXCtrl::MultiguestEvent_InputAssigned - This Guest is assigned input control
  - INGuestXCtrl::MultiguestEvent_InputRevoked - This Guest is revoked input control
  - INGuestXCtrl::MultiguestEvent_InputDenied - This Guest requested input control but it was denied. See error for optional error code.
  - INGuestXCtrl::MultiguestEvent_ConnectionsChanged - Number of session changed
  - INGuestXCtrl::MultiguestEvent_MultiSessionsSuspended - More sessions suspended
  - INGuestXCtrl::MultiguestEvent_MultiSessionsAllowed - More sessions allowed
  - INGuestXCtrl::MultiguestEvent_MultiSessionsDenied - Change of sessions denied

- NumGuest - new number of connected Guest (only on INGuestXCtrl::MultiguestEvent_ConnectionsChanged event)
- Error - additional information (only for INGuestXCtrl::MultiguestEvent_InputDenied and INGuestXCtrl::MultiguestEvent_MultiSessionsDenied events).

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEraseBackground ([in] LONG hWnd, [in] LONG hDC, [in] INGuestXEventParam * EventParam)
Fired when NGA control background should be erased.

Default action: If there is an RC session the background is erased by black color. When there is no RC session the default NGA bitmap is shown.

Parameters:

- hWnd - NGA window handler
- hDC - device context for erase background windows message
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

Fired on incoming chat message.

Default action:
Show the message in the chat dialog if the one is opened.

Parameters:

- Msg - received chat message
**EventParam** - event parameter object. Handler can change its property Handled to true to suppress the default action.

```c
```

Fired on outgoing chat message.

The event fired after INGuestXCtrl::SendChatMessage() was called. The message can be different from one passed to INGuestXCtrl::SendChatMessage() method because "<PC Name>" string is inserted.

**Default action:**

Show the message in the chat dialog if the one is opened.

**Parameters:**

- **Msg** - received chat message
- **EventParam** - event parameter object. Handler can change its property Handled to true to suppress the default action.

```c
```

Fired before any NGA error message is shown.

**Default action:**

Built-in error message box is shown. Event handler can suppress the message box.

**Parameters:**

- **MsgNo** - id of message format string
- **Message** - message to be shown
- **EventParam** - event parameter object. Handler can change its property Handled to true to suppress the default action.

```c
```

Fired before any NGA information message is shown.

**Default action:**

Status changed in the built-in window if the window is open.

**Parameters:**

- **MsgNo** - id of message format string
- **Message** - message to be shown
- **EventParam** - event parameter object. Handler can change its property Handled to true to suppress the default action.

```c
HRESULT NGuestXLib::_INGuestXCtrlEvents::OnConnectWindow ([in] INGuestXEventParam * EventParam)
```

Fired when user left clicks on ActiveX area when there is no active connection.

**Default action:**

Built-in dialog is displayed to setup a new connection. Event handler can suppress the built-in dialog.

**Parameters:**
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnStatusWindow ([in] INGuestXEventParam * EventParam)
Fired when user pressed the keyboard shortcut for connection status window when there is an active connection.

**Default action:**
Built-in Connection Status dialog is displayed. Event handler can suppress the built-in dialog.

**Parameters:**
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnPropertyWindow ([in] INGuestXEventParam * EventParam)
Fired when user right clicks on ActiveX area when there is no active connection.

**Default action:**
Built-in Connection Properties dialog is displayed. Event handler can suppress the built-in dialog.

**Parameters:**
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatUIStart ([in] INGuestXEventParam * EventParam)
Fired when a Chat UI should be shown.

**Default action:**
Show the chat window.

**Parameters:**
- EventParam - event parameter object. Handler can change its property Handled to true to suppress the default action.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatUIEnd ()
Fired when a Chat UI should be hidden.

NGA hides the chat window if the one is opened.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnInfoWindow ([in] LONG Reason, [in] INGuestXEventParam * EventParam)
Fired when an info window should be shown.

**Default action:**
Open the modal info window to show info messages.

**Parameters:**
- Reason - one of the INGuestXCtrl::InfoWindowReason_t constants

Fired when current license does not allow to start the connection initiated either via GUI or BeginSession() method.
Default ActiveX handler shows the License GUI window. Default GUI can be suppressed by setting the property Handled of the param object to TRUE in application event handler.

This event is fired continuously until either the license is accepted by the ActiveX or the connection is canceled by setting the property Canceled of the param object to TRUE.

**Default action:**

Open the modal license dialog window to enter the license.

**Parameters:**

- **MsgNo** - id of message format string
- **Message** - Either contains the description that a license is required for non web connect connections or the Sentinel error why current license key cannot be used.
- **EventParam** - event parameter object. Handler can change its property Handled to true to suppress the default action. Handler can change its property Canceled to true to terminate connection process. Property Canceled is checked only if Handled was set to true.

### 5.2.6.2 INGuestXCtrl

Impero Guest ActiveX Interface.

**Member enumeration**

```cpp
enum INGuestXCtrl::CommProfile_t
{
    CommProfile_TCP = 0, "LAN (TCP)" profile.
    CommProfile_HTTP = 1, "HTTP" profile.
    CommProfile_UDP = 2, "UDP" profile.
    CommProfile_WebConnect = 3, "WebConnect" profile.
}
```

**Enumerator:**

- CommProfile_TCP 0 - "LAN (TCP)" profile.
- CommProfile_HTTP 1 - "HTTP" profile.
- CommProfile_UDP 2 - "UDP" profile.
- CommProfile_WebConnect 3 - "WebConnect" profile.

```cpp
enum INGuestXCtrl::SessionType_t
{
    SessionType_RemoteControl = 1, Connect Session.
    SessionType_Chat = 4, Chat Session.
}
```

**Enumerator:**

- SessionType_RemoteControl 1 - Connect Session.
- SessionType_Chat 4 - Chat Session.

```cpp
enum INGuestXCtrl::MouseMode_t
{
    MouseMode_Local = 0, Only send click and drag to Host.
    MouseMode_Remote = 1, Send all mouse events to Host.
    MouseMode_None = 2, Do not send mouse events to Host.
}
```

**Enumerator:**

- MouseMode_Local 0 - Only send click and drag to Host.
- MouseMode_Remote 1 - Send all mouse events to Host.
- MouseMode_None 2 - Do not send mouse events to Host.
KeyboardMode_Local  0 - Do not send special keystrokes.
KeyboardMode_Remote  1 - Send all keystrokes to Host.
KeyboardMode_None   2 - No keyboard control.

enum INGuestXCtrl::StretchMode_t
Remote desktop stretch mode.

   Enumerator:
Stretch_FitWindowToHost  0 - Do not stretch, show in actual size.
Stretch_FitHostToWindow  1 - Stretch Host window to fit control.
Stretch_FitNone        2 - Do not stretch.

enum INGuestXCtrl::GraphicsMode_t
Graphics mode.

   Enumerator:
GraphicsMode_Hook  0 - Command (hook) mode.
GraphicsMode_AccBitmap  1 - Accelerated bitmap.
GraphicsMode_NormalBitmap  2 - Normal bitmap.

enum INGuestXCtrl::MaxColors_t
The limits of colors bitmap graphic modes.

   Enumerator:
MaxColors_Actual  0 - Actual Colors.
MaxColors_256     1 - 256 colors.
MaxColors_16      2 - 16 colors. MaxColors_2  3 - 2 colors.

enum INGuestXCtrl::CompressionLevel_t
The connection compression level.

   Enumerator:
CompressionLevel_Auto  0 - Compression level selected automatically.
CompressionLevel_None  1 - None.
CompressionLevel_Low   2 - Low.
CompressionLevel_High  3 - High.

enum INGuestXCtrl::EncryptionLevel_t
The connection encryption level.

   Enumerator:
EncryptionLevel_Compatible  0 - Compatible.
EncryptionLevel_None        1 - None.
EncryptionLevel_DataIntegrity  2 - DataIntegrity.
EncryptionLevel_Keyboard    3 - Keyboard.
EncryptionLevel_DataIntegrityAndKeyboard  4 - DataIntegrityAndKeyboard.
EncryptionLevel_High  5 - High.
EncryptionLevel_VeryHigh  6 - Very High.

enum INGuestXCtrl::DesktopOptimization_t
The remote desktop optimization flags.

Enumerator:
DesktopOptimization_DisableEverything  0x00000001 - Disable everything.
DesktopOptimization_DisableWallpaper   0x00000002 - Disable wallpaper.
DesktopOptimization_DisableScreenSaver  0x00000004 - Disable screen saver.
DesktopOptimization_DisableAnimation   0x00000008 - Disable animation.
DesktopOptimization_DisableFullWindowDrag  0x00000010 - Disable full window drag.
DesktopOptimization_DisableMenuAnimation  0x00000020 - Disable menu animation / not supported by current API.
DesktopOptimization_DisableComboboxAnimation  0x00000040 - Disable combobox animation / not supported by current API.
DesktopOptimization_DisableSmoothScrolling  0x00000080 - Disable smooth scrolling / not supported by current API.
DesktopOptimization_DisableGradientCaption  0x00000100 - Disable gradient caption / not supported by current API.
DesktopOptimization_DisableActiveDesktop  0x00000200 - Disable active desktop.
DesktopOptimization_DisableMenuFade     0x00000400 - Disable menu fade / not supported by current API.
DesktopOptimization_DisableSelectionFade  0x00000800 - Disable selection fade / not supported by current API.
DesktopOptimization_DisableTooltipFade   0x00001000 - Disable tooltip fade / not supported by current API.
DesktopOptimization_DisableMenuDropShadowEffect   0x00002000 - Disable drop shadow effect on menus / not supported by current API.
DesktopOptimization_DisableFontSmoothing  0x00004000 - Disable font smoothing feature / not supported by current API.
DesktopOptimization_DisableVistaAero    0x00008000 - Disable Windows Vista Aero / not supported by current API.
DesktopOptimization_DisableOverlappedContent   0x00010000 - Disable overlapped content / not supported by current API.
DesktopOptimization_DisableVistaAnimations   0x00020000 - Disable all animations on Vista / not supported by current API.

enum INGuestXCtrl::Language_t
User interface languages.

Enumerator:
Language_English  1033 - English.
Language_French   1036 - French.
Language_German   1031 - German.
Language_Spanish  1034 - Spanish.
enum INGuestXCtrl::LicenseType_t
License type.

**Enumerator:**
- LicenseType_None 0 - No license.
- LicenseType_Network 1 - Network license.
- LicenseType_Standalone 2 - Standalone license.
- LicenseType_File 3 - Standalone license from file.

anonymous enum

**Enumerator:**
- NGA_UNKNOWN -1 - Unknown property value

enum INGuestXCtrl::MultiguestEvent_t
Multi Guest event flags.

**Enumerator:**
- MultiguestEvent_InputAssigned 0x00000001 - This Guest is assigned input control
- MultiguestEvent_InputRevoked 0x00000002 - This Guest is revoked input control
- MultiguestEvent_InputDenied 0x00000004 - This Guest requested input control but it was denied.
- MultiguestEvent_ConnectionsChanged 0x00000008 - Number of session changed
- MultiguestEvent_MultiSessionsSuspended 0x00000010 - More sessions suspended
- MultiguestEvent_MultiSessionsAllowed 0x00000020 - More sessions allowed
- MultiguestEvent_MultiSessionsDenied 0x00000040 - Change of sessions denied

enum INGuestXCtrl::SessionStatus_t
Session status.

**Enumerator:**
- SessionStatus_Idle 0 - Idle
- SessionStatus_Connecting 1 - Connection started
- SessionStatus_Opening 2 - Connected, opening a session
- SessionStatus_Authenticating 3 - Session can be opened, authenticating
- SessionStatus_Starting 4 - Authenticated, initializing RC/Chat
- SessionStatus_Running 5 - Session initialized
- SessionStatus_Closing 6 - Closing

enum INGuestXCtrl::InfoWindowReason_t
Info window reason.

**Enumerator:**
- InfoWindowReason_Connecting 1 - Starting a new connection
- InfoWindowReason_Connected 2 - When info window was closed for gateway authentication and now it should be reopened to display the progress of connecting to a Host behind the gateway.
- InfoWindowReason_CancelLogin 3 - Cancel logon button is pressed
- InfoWindowReason_Disconnecting 4 - Disconnecting from Host
enum INGuestXCtrl::ErrorCode_t

Error codes.

**Enumerator:**

- **NGA_OK** 0 - Ok
- **NGA_ERROR** 1 - General error (NSDK Dw::Error code)
- **NGA_ERR_BASE** 0x1000 - Base for NGA errors
- **NGA_ERR_INVALID_PARAMETER** 0x1001 - Invalid parameter
- **NGA_ERR_INVALID_STATUS** 0x1002 - A session or instance cannot be opened or closed because of the current status
- **NGA_ERR_NOT_OPENED** 0x1003 - The NGA instance is not opened
- **NGA_ERR_PERMISSION_DENIED** 0x1004 - User does not have the right to complete the operation
- **NGA_ERR_NO_SESSION** 0x1005 - There is no session of appropriate type to complete the operation

**Member functions**

**HRESULT INGuestXCtrl::Open ([out, retval] LONG * result)**
Opens NGA control instance.

Opens NGA control instance and change IsOpen property if opened successfully. Instance should be open to create sessions.

This method is synchronous.

**The method fires the following events:**

- **NGuestXLib::_INGuestXCtrlEvents::OnOpenPre()**
- **NGuestXLib::_INGuestXCtrlEvents::OnOpenPost()**

**NGuestXLib::_INGuestXCtrlEvents::OnOpenPre** event is always followed by **NGuestXLib::_INGuestXCtrlEvents::OnOpenPost()** event.

The events are not fired if the instance is already opened.

**Returns:**

- 0 - opened successfully (NGA_OK)
- 1 - failed to open instance (NGA_ERROR)
- **NGA_ERR_INVALID_STATUS** - the instance is already opened

**HRESULT INGuestXCtrl::Close ([out, retval] LONG * result)**

Close NGA control instance.

Ends all active sessions, disconnects from the Host, closes the NGA control instance and changes IsOpen property if closed successfully.

This method is synchronous.

**The method fires the following events:**

- **NGuestXLib::_INGuestXCtrlEvents::OnClosePre()**
- **NGuestXLib::_INGuestXCtrlEvents::OnClosePost()**

**NGuestXLib::_INGuestXCtrlEvents::OnClosePre** event is always followed by **NGuestXLib::_INGuestXCtrlEvents::OnClosePost()** event.
The events are not fired if the instance is already closed.
After having the Close() method called, the Open() method can be called once again.
This method is called automatically when ActiveX window is being destroyed.

**Returns:**
- 0 - closed successfully (NGA_OK)
- 1 - failed to close the instance. The instance is not closed and cannot be opened.
- NGA_ERR_INVALID_STATUS - the instance is already closed

**HRESULT INGuestXCtrl::BeginSession ([in] LONG SessionType,  [out, retval] LONG * result)**
Initiates a new session.

This function can be used to start a chat session or to resume an RC session when the connection is active or to start a new connection with chat or RC session.

When there is no active connection, the new connection is established with a Host specified by HostAddress, PortNumber, GatewayAddress, HttpProxyAddress, CommProfile properties.

If there is already an active connection, this function either opens a new chat session or resumes an RC session.

The function is asynchronous. The following events can be fired during and after calling this method:

1. NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre()
2. NGuestXLib::_INGuestXCtrlEvents::OnConnectPre()
3. NGuestXLib::_INGuestXCtrlEvents::OnConnectPost()
4. NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost()
5. NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted()

NGuestXLib::_INGuestXCtrlEvents::OnConnectPre(),
NGuestXLib::_INGuestXCtrlEvents::OnConnectPost() and
NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted() are fired only when a new connection is established.

When there was an active connection, only
NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre() and
NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost() events are fired.
NGuestXLib::_INGuestXCtrlEvents::OnConnectPre() is always followed by
NGuestXLib::_INGuestXCtrlEvents::OnConnectPost().

There is always NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost() for each
NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPre().

None of these events may be produced if the BeginSession() returns an error.

It is safe to call this function only in certain states:

- When there is no connection (session status: idle). For example, it is safe to call
  BeginSession() in response to the last connection
  NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() event. A new connection is created.

- When there is a running Rc or chat session (session status: running) to open a session of another type. For example, it is safe to call BeginSession(chat) in response to
  NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted(rc) or
  NGuestXLib::_INGuestXCtrlEvents::EndSessionPost(chat, true). A new Rc or Chat session is opened using the current connection.

In other cases such as when a connection is closing, or when a connection is starting, or when Host requested authentication this function returns an error.
For example in the following code:

```c
nga->Open();
nga->BeginSession(Rc);
nga->BeginSession(Chat);
```

the `BeginSession(Chat)` in most cases returns error because connection and Rc session is not established yet.

**Parameters:**

- **SessionType** - a session to open:
  - `SessionType_RemoteControl` - Connect (SU_RemoteControl)
  - `SessionType_Chat` - Text chat (SU_Chat)

**Returns:**

- 0 - success (NGA_OK).
- 1 - failed to start session (NGA_ERROR).
- `NGA_ERR_INVALID_PARAMETER` - either some of the connection properties or the parameter are invalid.
- `NGA_ERR_INVALID_STATUS` - session of this type is already opened
- `NGA_ERR_NOT_OPENED` - the NGA instance is not opened with Open() method.
- `NGA_ERR_PERMISSION_DENIED` - a second session cannot be opened because the user has no permissions on Host to open a session of the given type.

**HRESULT INGuestXCtrl::EndSession ([in] LONG SessionType,   [out, retval] LONG * result)**

Ends an active session of the given type.

If there is no more active session, this function disconnects the NGA instance from Host.

The function is asynchronous. The following events can be produced after calling this method:

1. `NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre()`  
2. `NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre()`  
3. `NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost()`  
4. `NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost()`  

NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre() and NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost() are fired only when the instance is disconnected from Host.

When there is still an active connection, only  
NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPre() and  
NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() events are fired.

NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPre() is always followed by  
NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost().

There is always NGuestXLib::_INGuestXCtrlEvents::OnEndSessionPost() for each  
NGuestXLib::INGuestXCtrlEvents::OnEndSessionPre().

None of these event can be produced if the function returns an error.

It is safe to call this function only in certain states:

- There is an active connection and running session of the given type (session status: running). For example in response to the `NGuestXLib::_INGuestXCtrlEvents::OnSessionStarted()` event.
There is already an active connection but the session is not authenticated yet (session status: authenticating). For example in response to NGuestXLib::_INGuestXCtrlEvents::OnBeginSessionPost event.

In other states (e.g. connecting, closing) the function returns an error.

For example in the following code:

```c++
// nga is not connected yet
if (nga->BeginSession(Rc) == 0) // start new connection
    nga->EndSession(Rc)
```
the EndSession(Rc) returns an error because the Rc session wasn’t opened yet.

**Parameters:**

- **SessionType** - a session to open
  - `SessionType_RemoteControl` - Connect (SU_RemoteControl)
  - `SessionType_Chat` - Text chat (SU_Chat)

**Returns:**

- 0 - success (NGA_OK)
- 1 - failed to close session (NGA_ERROR)
- `NGA_ERR_INVALID_PARAMETER` - the parameter is invalid
- `NGA_ERR_INVALID_STATUS` - the parameter is invalid
- `NGA_ERR_NOT_OPENED` - the NGA instance is not opened with Open() method.

**HRESULT INGuestXCtrl::SendLoginPassword ([in] BSTR Pwd, [out, retval] LONG * result)**

Sends the password credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginPassword() event.

The function is asynchronous.

**Parameters:**

- **Pwd** - The password must not be NULL and not longer than 16 characters.

**Returns:**

- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- `NGA_ERR_INVALID_PARAMETER` - the parameter is invalid
- `NGA_ERR_NOT_OPENED` - the NGA instance is not opened with Open() method.
- `NGA_ERR_INVALID_STATUS` - the authentication cannot be sent at this moment.


Sends the Impero credentials to Host.

This function shall only be called on NGuestXLib::_INGuestXCtrlEvents::OnLoginImpero() event.

The function is asynchronous.
Parameters:
- **GuestId** - The user ID must not be NULL and not longer than 32 characters.
- **Pwd** - The password must not be NULL and not longer than 16 characters.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

```cpp
```
Sends Windows system credentials to Host.

This function shall only be called on NGuestXLib::INGuestXCtrlEvents::OnLoginImpero() event.

The function is asynchronous.

Parameters:
- **UserId** - The user ID must not be NULL and not longer than 512 characters.
- **Domain** - The domain must not be NULL and not longer than 512 characters.
- **Pwd** - The password must not be NULL and not longer than 512 characters.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

```cpp
```
Sends LDAP credentials to Host.

This shall only be called on NGuestXLib::INGuestXCtrlEvents::OnLoginLdap() event.

The function is asynchronous.

Parameters:
- **Server** - The server ID must not be NULL and no longer than 512 characters.
- **User** - The user ID must not be NULL and no longer than 512 characters.
- **Pwd** - The password must not be NULL and no longer than 512 characters.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid
NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.


Sends RSA credentials to Host.

This function shall only be called on NGuestXLib::INGuestXCtrlEvents::OnLoginRsa() event.

The function is asynchronous.

Parameters:
- UserId - The user ID must not be NULL and no longer than 32 characters.
- Pco - The RSA SecurID passcode must not be NULL and no longer than 16 characters.
- Pwd - The optional password. May be be NULL. Must be no longer then 16 characters.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::SendLoginRsaPin ([in] BSTR Pin, [out, retval] LONG * result)

Sends RSA SecurID pin code to Host.

Sends an RSA SecurID pin code. This shall only be called on NGuestXLib::INGuestXCtrlEvents::OnEnterRsaPincode() event.

The function is asynchronous.

Parameters:
- Pin - The pin code.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - a parameter is invalid.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be sent at this moment.

HRESULT INGuestXCtrl::CancelLogin ([out, retval] LONG * result)

Cancels the authentication on a Gateway or Host.

Can be used to cancel the authentication on a gateway or Host. When canceling the authentication on Host, the NGuestXLib::INGuestXCtrlEvents::OnLoginFailed() is fired.

This function should be called on in response to OnLogin events:

- NGuestXLib::INGuestXCtrlEvents::OnLoginPassword()
- NGuestXLib::INGuestXCtrlEvents::OnLoginImpero()
- NGuestXLib::INGuestXCtrlEvents::OnLoginWindows()
- NGuestXLib::INGuestXCtrlEvents::OnLoginLdap()
- NGuestXLib::INGuestXCtrlEvents::OnLoginRsa()
NGuestXLib::_INGuestXCtrlEvents::OnEnterRsaPincode()

**Returns:**
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.
- NGA_ERR_INVALID_STATUS - the authentication cannot be canceled at this moment.

HRESULT INGuestXCtrl::SendRefreshScreen ([out, retval] LONG * result)
Forces the Host to resend its screen.
This function forcefully refreshes RC screen.

**Returns:**
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_STATUS - there is no running Rc session.

HRESULT INGuestXCtrl::SendCtrlAltDel ([out, retval] LONG * result)
Sends Ctrl-Alt-Del keystroke to Host.
This function sends both key down and up scancodes.

**Returns:**
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendCtrlEsc ([out, retval] LONG * result)
Sends Ctrl-Esc keystroke to Host.
This function sends both down and up scancodes.

**Returns:**
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

HRESULT INGuestXCtrl::SendAltTab ([in] VARIANT_BOOL bSendAltUp, [out, retval] LONG * result)
Sends Alt+Tab keystroke to Host.
Function sends scancodes for Alt-Tab key down and key up. To prevent the function from sending Alt key up scancode the bSendAltUp parameter can be set to FALSE.

**Parameters:**
- bSendAltUp - when false the function does not send Alt up scancode.

**Returns:**
 HRESULT INGuestXCtrl::SendAltShiftTab ([in] VARIANT_BOOL bSendAltUp, [out, retval] LONG * result)
Sends Alt-Shift-Tab keystroke to Host.

Function sends scancodes for Alt-Shift-Tab key down and key up. To prevent the function from sending Alt key up scan code the bSendAltUp parameter can be set to FALSE.

Parameters:
UpDown - If TRUE, send down+up scancodes, otherwise only down.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

 HRESULT INGuestXCtrl::SendAltUp ([out, retval] LONG * result)
Sends Alt key up scan code to Host.

This function can be use to send a key up scan code for Alt button to Host when the Alt up scan code was not sent by SendAltTab() or SendAltShiftTab().

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_NO_SESSION - there is no running Rc session.
- NGA_ERR_NOT_OPENED - the NGA instance is not opened with Open() method.

 HRESULT INGuestXCtrl::SendGoSolo ([out, retval] LONG * result)
Sends the Go Solo command to Host.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command.
- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence don't have the right for this command.

 HRESULT INGuestXCtrl::RequestKeyboardAndMouseControl ([out, retval] LONG * result)
Sends Request Keyboard And Mouse Control command to Host.

Returns:
- 0 - success (NGA_OK)
1 - failed to send a command.

- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence doesn't have the right to this command.

HRESULT INGuestXCtrl::SendGuardHost ([in] VARIANT_BOOL Guard,  [out, retval] LONG * result)
Sends Guard command to Host.

Parameters:
- Guard true - to prevent further Guest connections false - to enable further Guest connections

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send the command (NGA_ERROR)
- NGA_ERR_NOT_OPENED - NGA instance is not opened
- NGA_ERR_NO_SESSION - there is no session of the appropriate type.
- NGA_ERR_PERMISSION_DENIED - returned when the Guest is not an Administrator (Power User) and hence doesn't have the right to this command.

HRESULT INGuestXCtrl::SendChatMessage ([in] BSTR Message,  [out, retval] LONG * result)
Sends chat message to Host.

Parameters:
- Message - a chat message to send to Host.
- Font - a font of chat message

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command.
- NGA_ERR_NOT_OPENED - NGA instance is not opened.
- NGA_ERR_NO_SESSION - there is no chat session.

HRESULT INGuestXCtrl::SetCustomString ([in] LONG StringId,  [in] BSTR Str,  [out, retval] LONG * result)
Overrides the given GUI string.

Parameters:
- StringId - The Id of GUI string to override.
- Str - New GUI string. Passing a NULL string removes the overridden string.

Returns:
- 0 - success (NGA_OK)
- 1 - failed to send a command (NGA_ERROR)
- NGA_ERR_INVALID_PARAMETER - unknown string id
HRESULT INGuestXCtrl::GetKeyboardShortcut ([in] LONG ShortcutType, [out, retval] INGuestXShortcut ** result)

Keyboard shortcut interface.

This method can be used to set/get ActiveX keyboard shortcuts, for example "Send Alt-Ctrl-Del to Host", "Send Ctrl-Esc to Host", etc.

**Parameters:**

- ShortcutType - the ID of the shortcut to return (one of the INGuestXShortcut::ShortcutType_t constants)

**Returns:**

button assignments for the given shortcut. See INGuestXShortcut for more details.

**Properties**

LONG INGuestXCtrl::CurrentCommProfile [get]

The communication profile of the current connection, read only.

When there is no active connection the NGA_UNKNOWN is always returned.

BSTR INGuestXCtrl::CurrentHostAddress [get]

The Host address of the current connection, read only.

When there is no connection, the empty string is returned.

LONG INGuestXCtrl::CurrentPortNumber [get]

The port number of the current connection, read only.

The value 0 means that default port for current communication profile should be used.

When there is no active connections, NGA_UNKNOWN is returned.

BSTR INGuestXCtrl::CurrentGatewayAddress [get]

The address of the gateway for the current connection, read only.

When there is no active connection, the empty string is returned.

BSTR INGuestXCtrl::CurrentHttpProxyAddress [get]

The address of HTTP proxy for the current connection, read only.

When there is no connection, the empty string is returned.

LONG INGuestXCtrl::CurrentGraphicsMode [get]

The graphic mode of the current connection, read only.

One of the GraphicsMode_t constant can be assigned to this property.

When there is no active connection, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::CurrentGraphicsMaxColors [get, set]

The limit of bitmap mode colors for the current connection, read/write.

One of the MaxColors_t constant can be assigned to this property.

Used only for bitmap modes (e.g. when GraphicsMode property is either GraphicsMode_AccBitmap or GraphicsMode_NormalBitmap).

When there is no active connection, the NGA_UNKNOWN is returned.
LONG INGuestXCtrl::CurrentCompressionLevel [get, set]
The compression level of the current connection, read/write.
One of the CompressionLevel_t constants can be assigned to this property.
When there is no active connection, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::CurrentEncryptionPreferred [get]
The encryption level of the current connection, read/write.
One of the EncryptionLevel_t constants can be assigned to this property.
When there is no active connection, the NGA_UNKNOWN is returned.

VARIANT_BOOL INGuestXCtrl::IsOpen [get]
Whether the instance of NGA was opened successfully by Open() function, read only.

VARIANT_BOOL INGuestXCtrl::IsConnected [get]
Whether the instance of NGA is connected to remote Host, read only.
Property is true when there is an active session (chat or RC).

LONG INGuestXCtrl::SessionStatus [get]
Current status of RC session, read only.

Status:
Can be one of the SessionStatus_t constants. When the NGA instance is not open, status is SessionStatus_Idle.

LONG INGuestXCtrl::HostScreenWidth [get]
The current width of the remote desktop, read only.
When there is no active RC session, the NGA_UNKNOWN is returned.

LONG INGuestXCtrl::HostScreenHeight [get]
The current height of the remote desktop, read only.
When there is no active RC session, the NGA_UNKNOWN is returned.

VARIANT_BOOL INGuestXCtrl::IsMultiguestAdminOnHost [get]
Whether the current RC session has multi Guest admin role on Host, read only.
When there is no active session, the false is returned.

LONG INGuestXCtrl::NumGuestsOnHost [get]
The number of Guests connected to Host, read only.
When there is no active session, the NGA_UNKNOWN is returned.

INGuestXFont INGuestXCtrl::ChatFont [get]
Get chat font interface, read only.

LONG INGuestXCtrl::CommProfile [get, set]
Communication profile for a next connection.
One of the CommProfile_t constants can be assigned to this property.
**Default value:** CommProfile_TCP
BeginSession() method uses this profile when establishing a new connection.

BSTR INGuestXCtrl::HostAddress [get, set]
The address of remote Host for a next connection.
BeginSession() method uses this address when establishing a new connection.

**Default value:** empty string

LONG INGuestXCtrl::PortNumber [get, set]
Port number for a next connection.
The value 0 means that default port for current communication profile should be used.
BeginSession() method uses this property when establishing a new connection.

**Default value:** 0

BSTR INGuestXCtrl::GatewayAddress [get, set]
Address of gateway for a next connection.
When empty string is specified the gateway is not used. This property is ignored when UDP communication profile is selected.
BeginSession() method uses this address when establishing a new connection.

**Default value:** empty string

BSTR INGuestXCtrl::HttpProxyAddress [get, set]
Address of HTTP proxy for a next connection.
The proxy address is ignored when UDP or TCP communication profile is selected.
BeginSession() method uses this address when establishing a new connection.

**Default value:** empty string

LONG INGuestXCtrl::CompressionLevel [get, set]
The compression level for a next connection.
One of the CompressionLevel_t constants can be assigned to this property.
BeginSession() method uses this mode when establishing a new connection.

**Default value:** CompressionLevel_Auto - select compression level automatically

LONG INGuestXCtrl::EncryptionPreferred [get, set]
The encryption level for a next connection.
One of the EncryptionLevel_t constants can be assigned to this property.
BeginSession() method uses this mode when establishing a new connection.

**Default value:** EncryptionLevel_Compatible - Impero 6.5 compatible encryption

LONG INGuestXCtrl::GraphicsMode [get, set]
The graphic mode for a next connection.
One of the GraphicsMode_t constant can be assigned to this property.
BeginSession() method uses this mode when establishing a new connection.
LONG INGuestXCtrl::GraphicsMaxColors [get, set]
The limit of bitmap mode colors for a next connection.
One of the MaxColors_t constant can be assigned to this property.
Used only for bitmap modes (e.g. when GraphicsMode property is either GraphicsMode_AccBitmap
or GraphicsMode_NormalBitmap).
BeginSession() method uses this mode when establishing a new connection.

**Default value:** MaxColors_Actual - use actual colors

VARIANT_BOOL INGuestXCtrl::LockHostKeyboardOnConnect [get, set]
Keyboard locking mode for a next connection.
BeginSession() method uses this mode when establishing a new connection.

**Default value:** FALSE (do not lock)

VARIANT_BOOL INGuestXCtrl::BlankHostScreenOnConnect [get, set]
Host screen blanking mode for a next connection.
BeginSession() method uses this mode when establishing a new connection.

**Default value:** FALSE (do not blank)

VARIANT_BOOL INGuestXCtrl::GuardHostOnConnect [get, set]
Host guard settings for a next connection.
BeginSession() method uses this mode when establishing a new connection.

**Default value:** FALSE (do not guard)

LONG INGuestXCtrl::DesktopOptimizeMask [get, set]
Desktop optimization mask for the current and next connection.
A bitwise OR of the DesktopOptimization_t constants can be assigned to this property.
Changing this property affects current RC session immediately. Same setting is used for the next RC session.

**Default value:** DesktopOptimization_DisableEverything - disable everything

LONG INGuestXCtrl::StretchToFitWindow [get, set]
Remote desktop stretch mode.
Property indicates how the remote desktop image is displayed inside NGA control. Changing this property with active RC session redraws the NGA control.
One of the StretchMode_t constants can be assigned to this property.

**Default value:** Stretch_FitWindowToHost

VARIANT_BOOL INGuestXCtrl::AutoScroll [get, set]
Auto scroll mode.
The scroll is done when the mouse enters a hot zone close to the border (1/10 of the width or height in each side (left/right/top/bottom) of the RC window.

**Default value:** TRUE (enabled)
LONG INGuestXCtrl::ScrollPositionX [get, set]
The horizontal position of the remote desktop image inside NGA control.
**Default value:** 0

LONG INGuestXCtrl::ScrollPositionY [get, set]
The vertical position of the remote desktop image inside NGA control.
**Default value:** 0

INGuestXRcArea INGuestXCtrl::RcArea [get]
Rc area interface (read only property).
This property can be used to set/get the Connect area to be shown in the control. Changing this property does not affect the Connect area of the current connection, settings are used for next connections.
See [INGuestXRcArea](#) for more details.

LONG INGuestXCtrl::MouseMode [get, set]
Mouse mode of current and next RC session.
One of the [MouseMode_t](#) constants can be assigned to this property.
**Default value:** MouseMode_Remote

VARIANT_BOOL INGuestXCtrl::ShowRemoteMouseMovements [get, set]
Gets or sets the value of remote mouse movements property.
When this property is true, the remote desktop mouse movements are shown when the control is focused.
**Default value:** false (do not show remote mouse movements)

LONG INGuestXCtrl::KeyboardMode [get, set]
The keyboard mode of the current and next RC session.
One of the [KeyboardMode_t](#) constants can be assigned to this property.
**Default value:**
KeyboardMode_Local

VARIANT_BOOL INGuestXCtrl::UnicodeKeyboardMode [get, set]
Indicates whether keyboard events are sent as unicode characters or as scan codes.
**Returns:**
false - NGA sends scancodes true - NGA sends unicode characters
**Default value:**
false (Send scan codes)

VARIANT_BOOL INGuestXCtrl::RemoteCursor [get, set]
The remote cursor display mode.
When 'true', NGA mouse cursor has the shape of the Host mouse cursor when displayed in the NGA control. The shape of the cursor is not stretched when the remote desktop mode is stretched to fit the screen.
**Default value:** true
VARIANT_BOOL INGuestXCtrl::AutoTakeControl [get, set]
Gets or sets the auto take control property.
When several Guests are connected to the same Host, only one of these Guests controls the Host's keyboard and mouse. When this option is enabled, Guest requests the control over Host keyboard and mouse automatically on keyboard or mouse hit.

**Default value:** true

LONG INGuestXCtrl::Language [get, set]
Gets or sets the language used for build-in dialogs.
One of the Language_t constants can be assigned to this property.
When attempting to assign unsupported language value, the current UI language is not changed.

**Default value:** selected in accordance with system locale. If the current system locale is not supported, the Language_English language is used.

LONG INGuestXCtrl::LicenseType [get, set]
Sentinel license type (network, standalone, etc).
One of the LicenseType_t constants can be assigned to this property.
When attempting to assign unsupported license type value, the current License type is not changed.

**Default value:** LicenseType_None

BSTR INGuestXCtrl::LicenseKey [get, set]
The Sentinel license key.
ActiveX uses this property when the license type is standalone. The string property contains the license key (not the file name).

**Default value:** empty string

BSTR INGuestXCtrl::LicenseServer [get, set]
The IP/hostname of the Sentinel license server.
ActiveX uses this property when the License Type is network.

**Default value:** empty string

BSTR INGuestXCtrl::LicenseFile [get, set]
The Sentinel license file.
ActiveX uses this property when the license type is standalone file. The string property contains the full path to the license file.

**Default value:** empty string

VARIANT_BOOL INGuestXCtrl::LicenseAutoSave [get, set]
The Sentinel license properties autosave flag.
ActiveX checks this property when some license property is changed and if flag is `TRUE`, property value is saved to registry. The setting of this flag affects only properties changed after flag was set.

**Default value:** TRUE
BSTR INGuestXCtrl::WebConnectAddress [get, set]
Gets or sets the WebConnect address for a next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** empty string

BSTR INGuestXCtrl::WebConnectCredentialsAccount [get, set]
Gets or sets the WebConnect credentials account for a next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** empty string

BSTR INGuestXCtrl::WebConnectCredentialsPassword [get, set]
Gets or sets the WebConnect credentials password for a next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** empty string

BSTR INGuestXCtrl::WebConnectCredentialsDomain [get, set]
Gets or sets the WebConnect credentials domain for a next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** empty string

BSTR INGuestXCtrl::WebConnectProvidedTicket [get, set]
Gets or sets the WebConnect provided ticket for next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** empty string

BSTR INGuestXCtrl::WebConnectNameQualifier [get, set]
Gets or sets the WebConnect name qualifier for next connection.
This property is ignored when a communication profile other than WebConnect is selected.
BeginSession() method uses this address when establishing a new connection.
**Default value:** "HST"

5.2.6.3 INGuestXEventParam
Auxiliary parameter interface for INGuestX events.
This is internal interface and cannot be created via CoCreateInstance() function. Scripting languages can change Handled property provided in this interface to indicate that an event was handled successfully and default NGuestX action should be suppressed.

Example of using this property from javascript language:
function nguestx_OnLoginPassword(reason, eventparam)
{
    nguestx.SendLoginPassword("1");
    eventparam.Handled = 1; // Set event handled
}

Properties

VARIANT_BOOL INGuestXEventParam::Handled [get, set]
Indicates that an event has been handled by an application.
Event handler can set this property to true to suppress default NGuestX action.

VARIANT_BOOL INGuestXEventParam::Canceled [get, set]
Indicates that an action should be canceled.
Event handler can set this property to true to indicate that processing should not continue.

5.2.6.4 INGuestXFont
Chat font interface.

Member enumeration

enum INGuestXFont::FontEffect_t
Font effect.

Enumerator:
FontEffect_Italic 1 - Italic
FontEffect_StrikeOut 2 - Strike out

Properties

LONG INGuestXFont::Height [get, set]
Font height.

LONG INGuestXFont::Weight [get, set]
Font weight.

LONG INGuestXFont::CharSet [get, set]
Font character set.

LONG INGuestXFont::Effects [get, set]
Font effects.
The bitwise OR of the FontEffect_t constants.

VARIANT_BOOL INGuestXFont::Underline [get, set]
Font underline.

LONG INGuestXFont::FgColor [get, set]
Font foreground color.

LONG INGuestXFont::BgColor [get, set]
Font background color.
BSTR INGuestXFont::Name [get, set]
Font name property.

5.2.6.5 INGuestXRcArea
RC area interface.

Member enumeration

enum INGuestXRcArea::RcAreaMode_t
RC area modes.

**Enumerator:**
- RcAreaMode_None 0 - None
- RcAreaMode_Rect 1 - Rectangle
- RcAreaMode_Monitor 2 - Monitor

**Properties**

LONG INGuestXRcArea::Mode [get, set]
RC area mode:
- 0 (RcAreaMode_None) - Show entire Connect screen.
- 1 (RcAreaMode_Rect) - Show only rectangular area specified by Top, Left, Width, Height properties.
- 2 (RcAreaMode_Monitor) - Show only Host monitor specified by Monitor property.

LONG INGuestXRcArea::Monitor [get, set]
RC area monitor.

LONG INGuestXRcArea::Top [get, set]
RC area rectangle top.

LONG INGuestXRcArea::Left [get, set]
RC area rectangle left side coordinate.

LONG INGuestXRcArea::Width [get, set]
RC area rectangle width.

**LONG INGuestXRcArea::Height [get, set]**
RC area rectangle height.

5.2.6.6 INGuestXShortcut
Keyboard shortcut interface. Defines the button assignments for a shortcut returned by INGuestXCtrl::GetKeyboardShortcut() method.

Member enumeration

enum INGuestXShortcut::ShortcutType_t
Keyboard shortcut types.
**Enumerator:**

<table>
<thead>
<tr>
<th>ShortcutType</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AltCtrlDel</td>
<td>0 - Send ALT + CTRL + DEL to Host</td>
</tr>
<tr>
<td>CtrlEsc</td>
<td>1 - Send CTRL + ESC to Host</td>
</tr>
<tr>
<td>AltTab</td>
<td>2 - Send ALT + TAB to Host</td>
</tr>
<tr>
<td>Status</td>
<td>3 - Connection Status Dialog</td>
</tr>
</tbody>
</table>

**Properties**

VARIANT_BOOL INGuestXShortcut::Alt [get, set]

**ALT usage in shortcut:**
- TRUE - ALT is used.
- FALSE - ALT is not used.

VARIANT_BOOL INGuestXShortcut::Ctrl [get, set]

**CTRL usage in shortcut:**
- TRUE - CTRL is used.
- FALSE - CTRL is not used.

LONG INGuestXShortcut::VkCode [get, set]

**VK code that should be used in shortcut.**

**Allowed VK codes are:**
- A-Z, 0-9, F1-F12, VK_INSERT, VK_HOME, VK_END, VK_PRIOR (Page Up), VK_NEXT (Page Down), VK_UP, VK_DOWN, VK_LEFT, VK_RIGHT.
- To disable the shortcut, set this property to -1.

**5.2.6.7 NGuestX Messages**

**NGuestX Info Messages**

<table>
<thead>
<tr>
<th>ID</th>
<th>Message Text</th>
<th>Type</th>
<th>Parameter %1</th>
<th>Parameter %2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>Connection %1 is listening</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>Connection %1 is calling %2</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td>Connection address</td>
</tr>
<tr>
<td>2003</td>
<td>Connection %1 is opening</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>Connection %1 could not find %2</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td>Connection address</td>
</tr>
<tr>
<td>2005</td>
<td>Connection %1 failed.</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>Connection %1 connected to %2 ok</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td>Connection address</td>
</tr>
<tr>
<td>2007</td>
<td>Connection %1: %2</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td>Connection address</td>
</tr>
</tbody>
</table>
Now connected

<table>
<thead>
<tr>
<th>Year</th>
<th>Message Text</th>
<th>Type</th>
<th>Parameter %1</th>
<th>Parameter %2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>Connection %1 connected ok</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>Connection %1 disconnected</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Connection %1 closed ok</td>
<td>OnInfoMsg</td>
<td>Connection name (com. profile)</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>Name server %1 found</td>
<td>OnInfoMsg</td>
<td>Name server address</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Name server %1 not found.</td>
<td>OnInfoMsg</td>
<td>Name server address</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Name server(s) activated: %1 %2</td>
<td>OnInfoMsg</td>
<td>Primary Nns</td>
<td>Secondary Nns</td>
</tr>
<tr>
<td>2016</td>
<td>Gateway not found.</td>
<td>OnInfoMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td>Opening %1...</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td>Opened %1 ok</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>Comm error with %1.</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2023</td>
<td>Authenticating on %1...</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2024</td>
<td>Authenticated on Impero Host OK</td>
<td>OnInfoMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2025</td>
<td>Waiting for host to confirm access</td>
<td>OnInfoMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2027</td>
<td>Access allowed by host</td>
<td>OnInfoMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2028</td>
<td>Closing %1 ...</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2029</td>
<td>Closed %1 ok</td>
<td>OnInfoMsg</td>
<td>Connection address</td>
<td></td>
</tr>
<tr>
<td>2046</td>
<td>Session ended by Host.</td>
<td>OnInfoMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2084</td>
<td>Authenticated on connection server. Waiting %1!d! sec</td>
<td>OnInfoMsg</td>
<td>Seconds left to wait.</td>
<td></td>
</tr>
</tbody>
</table>

NGuestX Error Messages

<table>
<thead>
<tr>
<th>ID</th>
<th>Message Text</th>
<th>Type</th>
<th>Parameter %1</th>
<th>Parameter %2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1225</td>
<td>The Host does not allow %1.</td>
<td>OnErrorMsg</td>
<td>Connect/Chat</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Out of memory.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Message</td>
<td>Error Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------------------------------</td>
<td>---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>Host and Guest can't agree on encryption.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>Host does not allow 6.5 compatible. Try another encryption.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2026</td>
<td>Access denied by host.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2031</td>
<td>Impero Security Server: Unknown Guest.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2032</td>
<td>Impero Security Server: Not authorized.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2033</td>
<td>Impero Security Server: Unknown Host.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2034</td>
<td>Impero Security Server: Guest ID was disabled.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2035</td>
<td>Password too long.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2036</td>
<td>Impero Guest ID too long.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2037</td>
<td>Username too long.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2038</td>
<td>Directory Service alias name too long.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2039</td>
<td>No access. Closed user group.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2041</td>
<td>Alter authentication method or update host.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2042</td>
<td>Invalid credentials, please retry.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2043</td>
<td>Too many invalid credentials entered.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2045</td>
<td>No response from %1.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2047</td>
<td>Unsupported authentication method.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2049</td>
<td>Directory Service open error.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2050</td>
<td>Directory Service group not found.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2051</td>
<td>Directory Service user not found.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error Code</td>
<td>Message</td>
<td>Message Text</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2052</td>
<td>Logon to Directory Service failed.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2053</td>
<td>No Distinguished Name could be found for this logon name.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2054</td>
<td>Directory Service object not found.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2055</td>
<td>Secure Sockets Layer (SSL) is required by this Directory Service.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2056</td>
<td>Directory Services: Unsupported authentication method.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2057</td>
<td>The Directory Service failed to authenticate.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2058</td>
<td>Directory Services: Insufficient rights.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2059</td>
<td>Directory Service not found.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2060</td>
<td>Could not connect to Directory Service.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2061</td>
<td>Directory Services: Unsupported feature.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2062</td>
<td>Directory Services error.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2063</td>
<td>Impero Security Server service not available.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2064</td>
<td>New password rejected. It was used before, is too short, or needs to include a digit.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2065</td>
<td>Impero Security Server connect error %1.</td>
<td>OnErrorMsg</td>
<td>Error code</td>
<td></td>
</tr>
<tr>
<td>2066</td>
<td>RSA SecurID server failed to validate credentials.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2067</td>
<td>RSA SecurID pincode changed ok.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2068</td>
<td>RSA SecurID next PASSCODE required.</td>
<td>OnErrorMsg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2069</td>
<td>RSA SecurID Server connect error %1.</td>
<td>OnErrorMsg</td>
<td>Error code</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Default message</td>
<td>Internal ReasonId</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Impero Security Server: Guest ID was disabled.</td>
<td>MessageAccessServerGuestLocked</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Invalid credentials, please retry.</td>
<td>MessageInvalidPassword</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Please enter a new password.</td>
<td>MessageMustChangePassword</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Directory Service open error.</td>
<td>MessageLdapServiceError</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Directory Service group not found.</td>
<td>MessageLdapGroupNotFound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Directory Service user not found.</td>
<td>MessageLdapUserNotFound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Logon to Directory Service failed.</td>
<td>MessageLdapServerLoginFailed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>No Distinguished Name could be found for this logon name.</td>
<td>MessageLdapLoginNameNotResolved</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Directory Service object not found.</td>
<td>MessageLdapNoObject</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Secure Sockets Layer (SSL) is required by this Directory Service.</td>
<td>MessageLdapSslRequired</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>The Directory Service failed to authenticate.</td>
<td>MessageLdapAuthenticationError</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Directory Services: Insufficient rights.</td>
<td>MessageLdapInsufficientRights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Directory Service not found.</td>
<td>MessageLdapServerNotFound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>Could not connect to Directory Service.</td>
<td>MessageLdapServerConnectError</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>Directory Services: Unsupported feature.</td>
<td>MessageLdapUnsupportedFeature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Directory Services error.</td>
<td>MessageLdapError</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>New password rejected. It was used before, is too short, or needs to include a digit.</td>
<td>MessageNssNonConformingPassword</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>RSA SecurID server failed to validate credentials.</td>
<td>MessageRsaValidationFailed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>RSA SecurID pincode changed ok.</td>
<td>MessageRsaPincodeChanged</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.3 Impero Scripting ActiveX Control

The object control extension `NFMSCRPT.OCX` is installed in your Windows system32 directory when you install Impero Guest. It allows you to access the Guest's scripting capabilities from any programming or scripting tool that supports ActiveX automation.

A commonly used tool is Microsoft Visual Basic (VB). The OCX is tested with VB, and examples in this section are written mostly in VB. An example of a VBscript using an excerpt of the commands available is:

```vbnet
Rc = Script.Initialize()
Rc = Script.Call("MyDesktop")
Rc = Script.IncludeSubdirectories(True)
Rc = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
Rc = Script.Hangup()
Rc = Script.Uninitialize()
```
Scripts as simple as this are more easily created and executed with the script editor in the Impero Guest program. Say, however, that you wish to retry all or parts of your operations repeatedly until they have all succeeded, you must make a more complex algorithm that this editor is not designed for. With \texttt{NFMSCRPT.OCX} you can improve the above script to for example:

\begin{verbatim}
Rc = Script.Initialize()
CallAgain:
Rc = Script.Call("MyDesktop")
Rc = Script.IncludeSubdirectories(True)
RcSync = Script.Synchronize("c:\MyDocuments\*.*", "c:\MyDocuments\*.*")
Rc = Script.Hangup()
if (RcSync<>0) Then
    WriteLog ("Failed. Trying again in 30 seconds")
    WaitSeconds(30)
    GoTo CallAgain:
End If
Rc = Script.Uninitialize()
\end{verbatim}

This section contains these topics:
- Creation and Deletion
- \texttt{StartGuest, Initialize and Uninitialize}
- Connect and Disconnect
- Transferring Files
- Examples
- Reference

5.3.1 Create and Delete

An \texttt{NFMscript} object is created and eventually destroyed with the means of the programming tool. With VB, you can use the visual way by right-clicking the object toolbar (the one on the left side), and choose Components. A dialog with all available OCXs appears. Check the box with Impero File Manager Script, and click \texttt{OK}. A script icon is added to your toolbar. Click on this icon, then click the location in the form where you want the NFM script object placed, and drag it out. The default visual representation is a tree view showing commands as they execute, so even though the control initially shows up blank, it may be an idea to give it a reasonable size.

Assume you have named your \texttt{NFMScript} object \texttt{Script}. \texttt{Script.ClearLog()} can be used to clear the treeview log window. If you do not want any visual feedback, you can make the script invisible. You can also choose another reporting mode than \texttt{ReportLog()}.

\begin{verbatim}
Set Script.Visible = False
Rc = Script.ReportSilent()
Rc = Script.ReportStatus()
Rc = Script.ReportLog()
\end{verbatim}

The OCX can handle any number of simultaneous \texttt{NFMscript} objects, but the Impero Guest limits you to a maximum of 10 active objects at a time. The 11th and all further objects can be created but always returns error codes from all methods.

5.3.2 \texttt{StartGuest, Initialize and Uninitialize}

\texttt{NFMSCRPT.OCX} is only another way of wrapping up the Impero Guest. Therefore, the Impero Guest program has to be running when the OCX executes. The simplest way is to start it manually before starting the program or script you are writing using \texttt{NFMSCRPT.OCX}.

You may, however, want to hide the Impero Guest program and consider it an invisible service that
is needed to run with your application. If you wish that, you can call the `StartGuest()` function.

In VB you would typically do that in the `Form_Load()` function for your initial form:

```vba
Sub Form_Load()
    Dim Rc As Long
    Again:
    Rc = Script.StartGuest(True)
    If (Rc < -12 Or Rc > -11) Then
        MsgBox("Can’t start Impero Guest, please exit Host")
        GoTo Again
    End If
End
```

If Impero is installed and is working properly, the most likely reason for not being able to start the Guest program is that the Host is running. You must manually stop the Host. When the Guest has started, you can send commands to it from any NFMscript object you have created. The first command any object should send is the `Initialize` command that creates connection between the object and the Guest. This typically happens as a reaction to the click of a button.

```vba
Sub Button_Click()
    Rc = Script.Initialize()
    If (Rc <> 0) Then
        MsgBox("No connect. Is Impero Guest Running?")
        GoTo EndButtonClick
    End If
    ' <... do your stuff...>
    Rc = Script.Uninitialize()
EndButtonClick:
End
```

One reason `Initialize` might fail and return nonzero might be that the Guest program could not start. It is good practice to call `Uninitialize()` when you are returning from your subroutine. This way you free the connection to the Guest to be used for others. If you forget `Uninitialize()`, it is done implicitly for you if you call `Initialize()` again, but you are blocking 1 out of 10 connections to your Guest in the meanwhile.

`Uninitialize()` returns 0 on success and a nonzero code on error. You need not take any specific action, if an error is returned. When your application exits, it is good practice to call `FreeGuest()` that does all the needed clean up. Your program works OK without a call to `FreeGuest()`, but you are relying on the program exit to clean everything up.

**Note:** If you are writing a script for browser use (e.g. Internet Explorer), do not call `FreeGuest()`, as you are not the one to decide when Internet Explorer exits.

```vba
Sub StopButton_Click()
    Rc = Script.FreeGuest()
    Stop
End
```

### Summary

- `StartGuest()` may be called once at program start, no matter how many NFMscript objects you wish to create. `FreeGuest()` should be called on exit, and never in browser scripts. `Initialize()` must be called before any other command. The one exception is `StartGuest()`.
- After `Uninitialize()`, no other commands but `FreeGuest()` succeeds until the next `Initialize()`. You can have any number of `Initialize().Uninitialize()` sessions on the same object.

#### 5.3.3 Connect and Disconnect

The next thing you have to do is to connect to an Impero Host program running on another computer. The `Call()` command establishes this connection for you. If it fails, it returns a nonzero error code. If it succeeds, it returns 0. The argument to `Call()` is a string that is the name of the Impero phonebook (.dwc) file. In this file is stored the name of a computer and the parameters for
how to connect to it. The phonebook files are the ones shown on the Impero Guest program Phonebook tab. Say you have a phonebook file named Venus.dwc:

```vbscript
Sub Button_Click()
Rc = Script.Initialize()
Rc = Script.Call("Venus")
if (Rc <> 0) Then
    MsgBox("Venus not responding")
    GoTo EndButtonClick
End If
'... do your stuff...>
Rc = Script.Hangup()
Rc = Script.Uninitialize()
EndButtonClick:
End
```

It is good practice to call `Hangup()` before you make your next `Call()`. If you happen to make a new `Call()` before `Hangup()`, on the first one it is hunged up automatically. One good reason not to omit calling `Hangup()` is to save money on your telephone bill. You can make as many `Call()`s and `Hangup()`s you want on the same object.

Please be aware that the argument to `Call()` is NOT the name of the computer you wish to connect to. It is the name of a phonebook file. As such files often reside in the Impero phonebook directory, you need not specify a path if you have the file there. As the Impero default for phonebook filename extension is `.dwc`, you need neither pass that, so the three calls below do the same, but the two last are independent of where Impero is installed.

```vbscript
Script.Call("C:\program files\Impero Connect\phbook\venus.dwc")
Script.Call("venus.dwc")
Script.Call("venus")
Script.Call("*")
```

The fourth call does not know which phonebook file it wants to use. The "*" parameter causes a file selection box to pop up, where the end user can select a *.dwc file in the phonebook directory.

### Traversing the Phonebook

If you want a control that makes the phonebook files available, other than the independent popup file selection box made with `Script.Call("*")`, you can traverse the phonebook directory like for example below, where a combo box is used:

```vbscript
Sub Combo1_Dropdown()
Dim More As Boolean
More = Script.PhonebookSetFirst()
Do While (More)
    Combo1.Add(Script.PhonebookGetName())
    More = Script.PhonebookGetName()
Loop
End Sub
Sub Combo1_Click()
    Script.Call(Combo1.Value)
    Script.Hangup()
End Sub
```

If you wish to traverse only a subset of all your phonebook connections, place the ones you want to expose in a sub folder named for example `offices`, using the Phonebook tab control in the Impero Guest program, then use:

```vbscript
Script.PhonebookSetSubfolderFirst("offices")
```

### Summary

`Call()` must be called to connect to a Host. After a successful `Call()`, you can execute other commands. Do `Call("*")` to enable dynamic selection.

When done with the Host, call `Hangup()`. After a `Hangup()`, no commands that need Host access...
You can have any number of Call().Hangup() connections on the same object.

### 5.3.4 Transfer Files

After a Call() and before a Hangup(), you can call the file transfer commands that are:

- `Script.CopyFromHost (RemoteFileFilter, LocalDirectory)`
- `Script.CopyToHost (LocalFileFilter, RemoteDirectory)`
- `Script.CloneFromHost (RemoteDirectory, LocalDirectory)`
- `Script.CloneToHost (LocalDirectory, RemoteDirectory)`
- `Script.Synchronize (LocalDirectory, RemoteDirectory)`
- `Script.SynchronizeOneway (LocalDirectory, RemoteDirectory, Direction)`

Remote indicates files on the remote computer where Impero Host runs, Local is the computer where your NFMScript application and Impero Guest run.

File filters must be legal Windows file filters like `C:\winnt\*.exe`. The name of one single file like `C:\config.sys` is also a legal file filter. Blanks are allowed in names. The functionality of these commands is explained in Impero Script.

The dialogs of Impero are not shown during the execution of the commands, unless the command needs its end user to take a decision, for example whether a file should be overwritten or not. But if you call for example `CopyToHost()` on a very large file via a slow telephone line, your application is not locked. In your script program:

- All events are still processed, so any button can be pressed
- Progress of commands can be caught and monitored
- Cancelling commands is built-in, and can even be customized

**Important!** The methods in an NFMScript object are not re-entrant. In order to keep your application alive and responsive, all messages are processed while the method waits for Impero to finish processing the method. This makes it possible for you to call the same method again while the first call you made has not returned yet. Such a call cannot work correctly, but return a busy code. It is your application's responsibility to ensure that methods in the NFMScript objects are not re-entered into. One very useful exception to this rule is the three cancel methods.

**Cancel**

If you have chosen to have your NFMScript visible in your application, your end user can press the escape key in the script log window. This fires the internal `OnCancel()` event. The built-in action on that event is that a message box pops up with an option of four actions:

- Continue (Action 0)
- Cancel Command (Action 1)
- Cancel Call (Action 2)
- Cancel Script (Action 3)

Selecting Continue causes the script to continue as if nothing has happened. In fact, Impero Guest is never notified.

All three other NFMScript cancel replies sends a Cancel() command to Impero. Impero promptly cancels the last command it received from your script, and that script function returns with an error. What happens next is different for each of the three cancel replies.

Selecting Cancel Command causes the next script command to be issued to Impero. Only one single script command is canceled. Cancel Command should be used when for instance one large irrelevant file blocks a useful transfer of many files.

Selecting Cancel Call causes all further script commands to be ignored until the next Hangup() command. All commands from the current command until the next Hangup() command simply returns successfully without doing anything. Cancel Call addresses the situation where you for instance picked the wrong computer to connect to.

Cancel Script works the same way, but until the next Uninitialize() command. It should be used when you want to stop everything and evaluate what to do next.
If you want your own interface for canceling, you can use the three equivalent cancel commands from the script interface. Since all events are still being processed during the execution of a command like `CopyToHost()`, all buttons respond at any time. From your own cancel button, call:

```
Script.CancelCommand()
or
Script.CancelCall()
or
Script.CancelScript()
```

For instance like this, if you designed a button named CancelButton:

```
Sub CancelButton_Click()
    Script.CancelCall()
End Sub
```

If you want to use the internal cancel event but construct your own actions on that event, fill in the `OnCancel()` event that the OCX fires on your script application before putting up its message box.

You can for instance do like the following to make the user dialog less complex by allowing only `CancelScript`:

```
Private Sub Script_OnCancel(Action As Long)
    rc = MsgBox("Cancel?", vbYesNo)
    If rc = vbYes Then Action = 3
    If rc = vbNo Then Action = 0
End Sub
```

In the parameter `Action`, you return 0 for `Continue`, 1 for `Cancel Command`, 2 for `Cancel Call` and 3 for `Cancel Script`. Action arrives to you with a value of -1. If you do not change that value, the built-in message box above pops up, otherwise not.

Add an Option Dialog

In parallel with `OnCancel()`, you find `OnRButtonDown()`. A difference is that this event has no default action. It only does what you program. The parameter is available to allow for future extensions. For forwards compatibility, return a zero for no action.

```
Private Sub Script_OnRButtonDown(Action As Long)
    rc = MsgBox("Include Subdirectories", vbYesNo)
    If rc = vbYes Then Script.SetIncludeSubdir(True)
    If rc = vbNo Then Script.SetIncludeSubdir(False)
    Action = 0
End Sub
```

Monitor Progress

You can at any time query the progress of a script command. It is however your application’s responsibility to find a suitable place in your code to do it from. The NFMscript exposes the `Script.GetProgress()` function.

- that returns a percentage between 0 and 100. To use this from VB, instance a timer and a progress bar. You can for instance get the progress bar from one of the Microsoft common controls OCXs:

```
Sub Button_Click()
    rc = Script.Call(..)
    Timer1.Interval = 500
    rc = CopyToHost(....)
    Timer1.Interval = 0
    Script.Hangup()
End Sub
Sub Timer1_Timer()
    ProgressBar1.Value = Script.GetProgress()
End Sub
```

Settings

Impero Script has many parameters for the file transfer commands. All of these have been made
available as methods named Set<NameOfItem>() in the OCX. They are:

- SetOverwriteReadonly(BOOL YesNo)
- SetOverwriteHidden(BOOL YesNo)
- SetOverwriteSystem(BOOL YesNo)
- SetOverwriteExisting(BOOL YesNo)
- SetRetriesOnTransferError(long Retries)
- SetRetriesOnConnectError(long Retries)
- SetDeltaFileTransfer(BOOL YesNo)
- SetCrashRecovery(BOOL YesNo)
- SetCompression(long Level)
- SetConnected(BOOL conn)
- SetIncludeEmptyDir(BOOL YesNo)
- SetIncludeSubDir(BOOL YesNo)
- SetIncludeHiddenAndSystem(BOOL YesNo)
- SetIncludeOnlyNewer(BOOL YesNo, DATE DateTime)
- SetIncludeOnlyExisting(BOOL YesNo)

You may ask why these are methods and not properties, since all they seem to do is to set the value of a variable. The reason is that some of them must be implemented as sending real commands to Impero, while others just set a value to be used as an option for another command. For consistency, all settings are implemented as methods.

Execute

Many methods in NFMSCRPT.OCX correspond to commands in the Impero Script command language. This is the syntax you see in the Impero Guest’s script editor dialog and also in the OCX log window. If you want, you can send commands directly in that command language using:

```vba
Rc = Script.Execute(String Command),
```

The purpose of this OCX is however to relieve you of the burden of a lot of string formatting and event handling, so this entry is only published as an extra service for unforeseen circumstances.

5.3.5 Examples

In the directory where Impero Guest is installed, you find a file named examples.zip. Unzip this file to get the source code and executables for the examples Hello World Script, Visit all Hosts Script and Keep Synchronized Script.

Hello World Script

HelloWorldScript.exe is the simplest possible example. When you press the Start button, it copies a file to a Host computer. The Visual Basic project HelloWorldScript.vbp is included.

```vba
Private Sub Command1_Click()
    Dim Rc As Long
    Rc = HelloScript.Initialize
    Rc = HelloScript.Call("*")
    'Move some arbitrary file across. This one is always there
    Rc = HelloScript.CopyToHost(HelloScript.GetInstallDir() + "\Impero.fac", "c:\*.*")
    Rc = HelloScript.Hangup
    Rc = HelloScript.Uninitialize
End Sub
Private Sub ExitButton_Click()
    HelloScript.FreeGuest
    Stop
End Sub
Private Sub Form_Load()
    HelloScript.StartGuest(True)
End Sub
```

Visit All Hosts Script

This example has more features. In the beginning, we declare a logical variable, and we start Impero
Guest when the program starts up. Next, we cycle through the available phonebook files in the phonebook root directory and write their names in the log. Our intention is to visit all of these hosts one by one.

```vbscript
Dim More As Boolean
Private Sub Form_Load()
    Script.StartGuest True
    More = Script.PhonebookSetFirst
Do While More
    Script.WriteLog "Will visit " + Script.PhonebookGetFilename
    More = Script.PhonebookSetNext
Loop
End Sub
```

There is a button labeled Start Visit. When this button is clicked, we show a dialog in which we display what we are doing with the Host while executing a `CopyToHost()` operation. When we are finished, we stop the dialog and hide it:

```vbscript
Private Sub StartButton_Click()
    StartButton.Enabled = False
    StopButton.Enabled = True
    Script.Initialize
    More = Script.PhonebookSetFirst
Do While More
    rc = Script.Call(Script.PhonebookGetFilename)
    VisitDialog.Show
    Script.CopyToHost Script.GetInstallDir + "\Impero.fac", "c:\*.*"
    VisitDialog.Animation1.AutoPlay = False
    VisitDialog.Timer1.Interval = 0
    Script.Hangup
    VisitDialog.Hide
    More = Script.PhonebookSetNext
Loop
    StopButton.Enabled = False
    StartButton.Enabled = True
    Script.Uninitialize
End Sub
```

The dialog shows the `.AVI` file with the filecopy animation that also explorer does. The dialog has a timer that updates a progress bar:

```vbscript
Private Sub Form_Load()
    Caption = VisitForm.Script.PhonebookGetFilename
    Timer1.Interval = 100
    Animation1.Open "d:\Impero\v60\filecopy.avi"
    Animation1.AutoPlay = True
End Sub
Private Sub CancelButton_Click()
    VisitForm.Script.CancelCall
    Hide
End Sub
Private Sub Timer1_Timer()
    ProgressBar1.Value = VisitForm.Script.GetProgress
    ProgressBar1.Refresh
End Sub
```

Keep Synchronized Script

This is an example that shows timing and repetition using the `Wait...()` functions.

Initially, the Guest is started, and the initial parameters for the interface and the internal variables are set:

```vbscript
Dim Rc As Long
Dim TryAgain As Boolean
Private Sub Form_Load()
    Script.StartGuest (True)
```
TryAgain = True
StartTime.Value = Now
StartDate.Value = Today
End Sub

In the following section, the \texttt{WaitUntil()} function holds execution until the date and time are entered into the Microsoft DTPicker controls \texttt{StartDate} and \texttt{StartTime}. \texttt{Call(""')} leaves it up to the end user to pick a phonebook file in a \texttt{FileDialog}, then \texttt{Synchronize()} synchronizes the contents of two directories. If the interface's checkbox is checked, the program tries to repeat the \texttt{Call()} and \texttt{Synchronize()} periodically, until you actively stop it. While inactive, the program hides itself.

Private Sub StartButton_Click()
    Rc = Script.Initialize
    Rc = Script.WaitUntil(StartDate.Value, StartTime.Value)
    Again:
        Rc = Script.Call("*")
        If (Rc <> 0) Then GoTo Done
        Rc = Script.Synchronize("C:\reports\*.*", "c:\reports\*.*")
        If (Rc <> 0) Then MsgBox("This example assumes a directory C:\REPORTS")
        Rc = Script.Hangup
        If (Repeat.Value = Checked And TryAgain) Then
            If (MsgBox("Now sleep: " + CStr(Interval.Value), vbOKCancel) = vbCancel) Then GoTo Done
            KeepInSyncForm.Hide
            Script.Wait (Interval.Value)
            KeepInSyncForm.Show
            GoTo Again
        End If
    End If
    Done:
    Rc = Script.Uninitialize
End Sub

The button labeled \textbf{Stop} will cancel the repeating cycles:

Private Sub StopButton_Click()
    Script.CancelScript
    TryAgain = False
End Sub

The button labeled \textbf{Clear} will clear the log. This can be useful if it becomes very long.

Private Sub ClearButton_Click()
    Script.ClearLog
    Script.WriteLog("Ready")
End Sub

The \textbf{Exit} button will free the Guest and stop the program.

Private Sub ExitButton_Click()
    Script.FreeGuest
    Stop
End Sub

If you hold down the right mouse button, you can clear the log.

Private Sub Script_OnRbuttonDown(Action As Long)
    If (MsgBox("Clear Log?", vbYesNo) = vbYes) Then
        ClearButton_Click
        Action = 0
    End If
End Sub

5.3.6 Reference

This table explains all the Impero Scripting ActiveX Control API methods.

\textbf{Note:} All \texttt{NFMscript} methods that return a \texttt{Long}, return zero for success (Unless otherwise specified).
<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call (Filename As String) As Long</td>
<td>Call a phonebook entry. See also Hangup() and CancelCall(). If Initialize() was not called, it is called implicitly. That in turn calls StartGuest() if the Guest is not already running. If another Call() is currently active, it is hunged up. If you want two simultaneous Call()s, you must use two NFMscript objects.</td>
</tr>
<tr>
<td>CancelCall () As Long</td>
<td>Cancel the Call() that is currently active. Typically called asynchronously from a separate button. The current method (e.g. CopyFromHost()) is canceled and return an error code. All following methods returns immediately with no error, until your program executes the next Hangup() or Call() method.</td>
</tr>
<tr>
<td>CancelCommand () As Long</td>
<td>Cancel the method call that is currently active. Typically called asynchronously from a separate button. The current method (e.g. CopyFromHost()) is canceled and return an error code. All following methods executes as if nothing had happened.</td>
</tr>
<tr>
<td>CancelScript () As Long</td>
<td>Cancel the Call() that is currently active. Typically called asynchronously from a separate button. The current method (e.g. CopyFromHost()) is canceled and return an error code. All following methods returns immediately with no error, until your program executes the next Uninitialize() or Initialize() method.</td>
</tr>
<tr>
<td>ClearLog () As Long</td>
<td>Clears the script object's log window.</td>
</tr>
<tr>
<td>CloneFromHost (RemoteDir As String, LocalDir As String) As Long</td>
<td>Clones the RemoteDir directory to the LocalDir directory. A Call() must be open to the computer with the RemoteDir.</td>
</tr>
<tr>
<td></td>
<td>• RemoteDir - A directory on the remote computer where Impero Host runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td></td>
<td>• LocalDir - A directory on the local computer where Impero Guest runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td>CloneToHost (LocalDir As String, RemoteDir As String) As Long</td>
<td>Clones the LocalDir directory to the RemoteDir directory. A Call() must be open to the computer with the RemoteDir.</td>
</tr>
<tr>
<td></td>
<td>• RemoteDir - A directory on the remote computer where Impero Host runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td></td>
<td>• LocalDir - A directory on the local computer where Impero Guest runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td>CopyFromHost (RemoteFilter As String, LocalDir As String) As Long</td>
<td>Clones the files matching RemoteFilter to the LocalDir directory. A Call() must be open to the computer with the RemoteFilter.</td>
</tr>
<tr>
<td></td>
<td>• RemoteFilter - A valid file filter on the remote computer where Impero Host runs. An example could be &quot;C:\DATA*.XLS&quot;.</td>
</tr>
<tr>
<td></td>
<td>• LocalDir - A directory on the local computer where Impero Guest runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td>CopyToHost (LocalFilter As String, RemoteDir As String) As Long</td>
<td>Clones the files matching LocalFilter to the RemoteDir directory. A Call() must be open to the computer with the RemoteDir.</td>
</tr>
<tr>
<td></td>
<td>• LocalFilter - A valid file filter on the local computer where Impero Guest runs. An example could be &quot;C:\DATA*.XLS&quot;.</td>
</tr>
<tr>
<td></td>
<td>• RemoteDir - A directory on the remote computer where Impero Host runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>DirGetName () As String</td>
<td>Returns the name of the current subdirectory from DirSetFirst/Next().</td>
</tr>
<tr>
<td>DirSetFirst (Directory As String) As Boolean</td>
<td>Initializes the directory search entries, so that the next call to DirGetName() returns the name of the first subdirectory of &quot;Directory&quot; on the remote computer. A Call() must be open to the remote computer. If there are no such subdirectories, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>DirSetNext () As Boolean</td>
<td>Advances to the next directory search entry, so that the next call to DirGetName() returns the name of the next subdirectory. If there are no more subdirectories, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>DriveGetName () As String</td>
<td>Returns the name of the current disk drive from DriveSetFirst/Next().</td>
</tr>
<tr>
<td>DriveSetFirst () As Boolean</td>
<td>Initializes the disk drive entries, so that the next call to DriveGetName() returns the name of the first disk drive on the remote computer that you currently have made a Call() to. If there are no disk drives, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>DriveSetNext () As Boolean</td>
<td>Advances to the next disk drive entry, so that the next call to DriveGetName() returns the name of the next disk drive. If there are no more drives, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>Execute (Command as String) As Long</td>
<td>Execute a script editor command. The format of these commands resemble the NFMscript methods.</td>
</tr>
<tr>
<td>FileGetAccessed () As Date</td>
<td>Returns the last access date for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetArchive () as Boolean</td>
<td>Returns the archive flag for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetCreated () As Date</td>
<td>Returns the create date for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetHidden () As Boolean</td>
<td>Returns the hidden flag for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetModified () As Date</td>
<td>Returns the modified date for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetName () As Date</td>
<td>Returns the name of the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileGetReadonly () As Boolean</td>
<td>Returns the read only flag for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>Function Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FileGetSize () As Long</td>
<td>Returns the size of the file selected with FileGetFirst/Next(). If the size is above 2GB, -1 is returned.</td>
</tr>
<tr>
<td>FileGetSystem () As Boolean</td>
<td>Returns the system flag for the file selected with FileGetFirst/Next().</td>
</tr>
<tr>
<td>FileSetFirst (FileFilter As String) As Boolean</td>
<td>Initializes the file entries, so that the next call to FileGet…() returns a property of the first file on a remote computer matching the given file filter. If there are no entries, the return value is False. On success, the return value is True. There must be an open Call() on the remote computer.</td>
</tr>
<tr>
<td>FileSetNext () As Boolean</td>
<td>Advances to the next file entry, so that the next call to FileGet…() returns the name of the next remote file. If there are no more files, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>FreeGuest () As Long</td>
<td>Frees connection to Impero Guest DLLs and does other clean up. Not mandatory, but it is good practice to call this before your application exits. Do not use this method in conjunction with browser scripts.</td>
</tr>
<tr>
<td>GetInstallDir () As String</td>
<td>Returns the Impero install directory on the local computer where the Impero Guest program runs.</td>
</tr>
<tr>
<td>GetPhonebookDir () As String</td>
<td>Returns the phonebook directory. The Impero.INI PHONEBOOKPATH and DATAPATH settings are respected.</td>
</tr>
<tr>
<td>GetProgress () As Long</td>
<td>Get the progress of the current method. Typically only useful with Copy, Clone and Synchronize methods. Returns the percentage 0-100 where 100 means done. Useful if you place it in a timer and feed the result into a progress bar.</td>
</tr>
<tr>
<td>Hangup () As Long</td>
<td>Disconnect the current Call().</td>
</tr>
<tr>
<td>Initialize () As Long</td>
<td>Initializes a Impero Guest session. Check that the return code is 0 (zero) before calling other methods. See also Uninitialize(). If the Impero Guest is not already running, StartGuest() is called implicitly.</td>
</tr>
<tr>
<td>PhonebookGetFilename () As String</td>
<td>Returns the name of the current phonebook file. If there are none, the string returned is “No Phonebook Entries or Error”.</td>
</tr>
<tr>
<td>PhonebookSetFirst () As Boolean</td>
<td>Initializes the phonebook entries, so that the next call to PhonebookGetFilename() returns the name of the first phonebook file. If there are no entries, the return value is False. On success, the return value is True.</td>
</tr>
<tr>
<td>PhonebookSetNext () As Boolean</td>
<td>Advances to the next phonebook entry, so that the next call to PhonebookGetFilename() returns the name of the next phonebook file. If there are no more files, the return value is False. On success, the return value is True. Can be used with both PhonebookSetFirst() and PhonebookSetSubfolderFirst().</td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>PhonebookSetSubfolderFirst (Folder As String) As Boolean</td>
<td>Initializes the phonebook entries, so that the next call to PhonebookGetFilename() returns the name of the first phonebook file in a specific subdirectory of the phonebook directory. If there are no entries, the return value is False. On success, the return value is True.</td>
</tr>
</tbody>
</table>
| RunLocal (Command As String) As Long | Runs an operating system executable file with parameters on your local computer.  
- **Command** - The name of a BAT, COM or EXE file. If you want to use shell commands, you must give the name of the shell executable. For NT and Win95 it is "cmd.exe", so you can use "cmd /c dir c:\*.*" or "cmd /k rename autoexec.bat autoexec.old". |
| RunRemote (Command As String) As Long | Runs an operating system executable file with parameters on a remote computer. A Call() must be open to that computer. Please note that the outcome of this depends on the setup of the remote computer environment, and is 100 % independent of your local computer.  
- **Command** - The name of a BAT, COM or EXE file. If you want to use shell commands, you must give the name of the shell executable. For NT and Win95 it is "cmd.exe", so you can use "cmd /c dir c:\*.*" or "cmd /k rename autoexec.bat autoexec.old". |
| SetCompression (Level As Long) As Long | Set the compression level.  
- **Level** - An integer number. 0 means no compression, >0 means compression. |
| SetCrashRecovery (YesNo As Boolean) As Long | Instructs Impero whether to apply crash recovery. If a Call() is interrupted, a partial file can be kept on the target disk. Only useful if SetDeltaFileTransfer is on, so this method implicitly sets SetDeltaFileTransfer to True.  
- **YesNo** - If True, partial files are kept on the target disk, and SetDeltaFileTransfer is set, so the valid part does not need to be retransmitted when you come back. If False, partial files are cleaned up automatically if the connection is lost. |
| SetDeltaFileTransfer (YesNo As Boolean) As Long | Instructs Impero whether to apply the Delta File Transfer method for minimizing the amount of data transfer. True is also set by SetCrashRecovery(True), but not cleared by SetCrashRecovery(False).  
- **YesNo** - If True, Delta File Transfer is applied when feasible. If False, all file transfers unconditionally transfer all bytes in all files. |
| SetIncludeEmptyDir (YesNo As Boolean) As Long | Instructs Impero whether to include empty directories in file transfer operations.  
- **YesNo** - If True, empty directories are included. If False, they are not included. |
| SetIncludeHiddenAndSystem (YesNo As Boolean) As Long | Instructs Impero whether to include hidden and system files in file transfer operations.  
- **YesNo** - If True, hidden and system files are included. If False, they are not included. |
<table>
<thead>
<tr>
<th>Method Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetIncludeOnlyExisting</td>
<td>Instructs Impero whether to include only files that already exist with the same name on the target computer in file transfer operations.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, only files that already exist with the same name on the target computer are transferred. If False, all files are transferred.</td>
</tr>
<tr>
<td>SetIncludeOnlyNewer</td>
<td>Allows you to set a limit to how old files you want to include in file transfer operations.</td>
</tr>
<tr>
<td>(YesNo As Boolean, Date As Date) As Long</td>
<td>- YesNo - If True, only files that are newer than Date are transferred. If False, all files are transferred.</td>
</tr>
<tr>
<td></td>
<td>- Date - Files with a modify date older than this are excluded if YesNo is True.</td>
</tr>
<tr>
<td>SetIncludeSubDir</td>
<td>Instructs Impero whether to include subdirectories of the directories/file filters given as source in file transfer operations.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, subdirectories are included. If False, subdirectories are excluded.</td>
</tr>
<tr>
<td>SetOverwriteExisting</td>
<td>Set the action you want when trying to overwrite existing files.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, existing files are overwritten without warning. If False, existing files cause a prompt in a dialog.</td>
</tr>
<tr>
<td>SetOverwriteHidden</td>
<td>Set the action you want when trying to overwrite hidden files.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, hidden files are overwritten without warning. If False, hidden files cause a prompt in a dialog.</td>
</tr>
<tr>
<td>SetOverwriteReadonly</td>
<td>Set the action you wish when trying to overwrite read only files.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, read only files are overwritten without warning. If False, read only files cause a prompt in a dialog.</td>
</tr>
<tr>
<td>SetOverwriteSystem</td>
<td>Set the action you wish when trying to overwrite system files.</td>
</tr>
<tr>
<td>(YesNo As Boolean) As Long</td>
<td>- YesNo - If True, system files are overwritten without warning. If False, system files cause a prompt in a dialog.</td>
</tr>
<tr>
<td>SetReportLog () As None</td>
<td>Make the logging of events in the object's log window be the default treeview representation.</td>
</tr>
<tr>
<td>SetReportSilent () As None</td>
<td>Disable the logging of events in the object's log window.</td>
</tr>
<tr>
<td>SetRetriesOnConnectError</td>
<td>Set the number of times you want the file call method to automatically retry making the connection before returning.</td>
</tr>
<tr>
<td>(Retries As Long) As Long</td>
<td>- Retries - An integer number between 0 and 9 inclusive.</td>
</tr>
<tr>
<td>SetRetriesOnTransferError</td>
<td>Set the number of times you want the file transfer method to automatically retry an operation before returning.</td>
</tr>
<tr>
<td>(Retries As Long) As Long</td>
<td>- Retries - An integer number between 0 and 9 inclusive.</td>
</tr>
<tr>
<td>StartGuest (Minimized As Boolean) As Long</td>
<td>Starts the Impero Guest executable. If it is already started, StartGuest() returns with no error. If Impero Host is running, StartGuest() returns an error code.</td>
</tr>
</tbody>
</table>
- **Minimized** - If True, the Guest attempts to start up minimized.
- **Return Codes:**
  - -11 and -12 mean success.
  - -11: Started OK.
  - -12: Already started.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Synchronize (LocalDir As String, RemoteDir As String) As Long</strong></td>
<td>Synchronizes two directories. A Call() must be open to the remote computer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LocalDir</strong> - A directory on the local computer where the Impero Guest runs. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td></td>
<td>- <strong>RemoteDir</strong> - A directory on the remote computer where the Impero Host runs. Must end with &quot;*.*&quot;.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SynchronizeOneWay (SourceDir As String, TargetDir As String, ToHost As Boolean) As Long</strong></td>
<td>Synchronizes two directories, but moves files one way only. A Call() must be open to the remote computer.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SourceDir</strong> - The directory from where the files originate. It can be local or remote depending on ToHost. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td></td>
<td>- <strong>TargetDir</strong> - The directory to which the files are moved. It can be local or remote depending on ToHost. Must end with &quot;*.*&quot;.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ToHost</strong> - If True, files are moved only from Guest to Host. If False, files are moved only from Host to Guest.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uninitialize () As Long</strong></td>
<td>Uninitializes a Impero Guest session. After Uninitialize(), Initialize() must be called before calling other methods. Uninitialize is not mandatory, but good practice.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wait (Period As Date) As Long</strong></td>
<td>Waits a number of hours, minutes and seconds and then returns.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Period</strong> - The number of hours, minutes and seconds that you want the method to wait before returning. Use WaitSeconds() to specify the period as seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If using AM-PM time notation, 12:00:01 AM causes a wait of 1 second, not 12 hours and 1 second.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WaitSeconds (Period As Long) As Long</strong></td>
<td>Waits a number of seconds and then returns.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Period</strong> - The number of seconds that you want the method to wait before returning.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WaitUntil (Date As Date, Time As Date) As Long</strong></td>
<td>Waits until a specified local date and time and then returns. For use with the Microsoft DTPicker object, this method has two parameters, one for date and one for time.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Date</strong> - The date you want the method to wait until before returning. If this variable has a time part, it is ignored.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Time</strong> - The time of the above date when the method shall return. If this variable has a date part, it is ignored.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WaitUntilAnyDay (Time As Date) As Long</strong></td>
<td>Waits until the next occurrence of a specified local time and then returns. This method is intended for applications that repeat an operation at the same time every day.</td>
</tr>
</tbody>
</table>
5 Advanced Tools

Impero Connect Administrator's Guide

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time of any date when the method returns. If this variable has a date part, it is ignored.</td>
</tr>
<tr>
<td>WriteLog (Text As String) As Long</td>
<td>Writes a text in the script object's log window, if it is in the default SetReportLog() status.</td>
</tr>
<tr>
<td></td>
<td>Text - A string that shall be appended to the current treeview item in the log.</td>
</tr>
</tbody>
</table>

See also

Impero Scripting ActiveX Control

5.4 Impero Connect Processes and Windows Security

This section explains the Windows access rights and privileges granted to Impero processes, which is not related to Impero Host Guest Access Security by Windows Security Management.

It includes these sections:

- Impero Processes
- Main Host Processes
- Impero Helper Service
- ImperoActivity Local Group

5.4.1 Impero Processes

Impero Connect processes can be grouped in three categories by the security context in which they run, that is the Windows access token assigned to the processes.

Main Host Processes

Main Host processes include the Impero Host or extended Host executable program (NHSTW32.EXE etc.) and some of the internal utility programs run by them.

Because Impero Connect is a Connect product rather than a traditional server service, these processes and Guest induced operations such as file transfer are performed in a context nearly identical to the context of the logged on user, rather than in a context derived from the identity (if any) stated when establishing the connection.

For more details, see Main Host Processes.

Impero User Programs

Impero user programs include Impero Guest (NGSTW32.EXE), Impero Security Manager (AMCONFIG.EXE), Impero Installation programs (SETUP.EXE and NDU.EXE), etc.

These are ordinary user programs that run in the security context of the logged on user. They are not treated any different than e.g. NOTEPAD.EXE.

Impero Helper Service

Impero helper service includes only NHOSTSVC.EXE and only some of its running instances (some other running instances of NHOSTSVC.EXE run as Host processes or Impero user programs).

Impero helper service is the only Impero process that runs in the privileged LocalSystem context performing selected privileged operations on behalf of Impero.

For more details, see Impero Helper Service.
5.4.2 Main Host Processes

This section includes these sections:

- Normal Operation
- Replace the Local Security Context
- Disable Main Host Processes Security

5.4.2.1 Normal Operation

The main Host processes include the Host or extended Host executable program (NHSTW32.EXE, NSSW32.EXE, NGWW32.EXE or NNSW32.EXE), utility programs run by the Host (NLDRW32.EXE, NUTIL32B.EXE, VITAWRAP.EXE, some instances of NHOSTSVC.EXE and RUNDLL32.EXE), and in some rare situations the Guest or Student programs (NGSTW32.EXE or NSTDW32.EXE). Programs started by Run Program may also run as main Host processes.

These processes form the bulk of the Impero Connect Host functionality. They run in the security context of the interactively logged on user, but modified so that the access token also lists membership of the ImperoActivity Local Group. This extra group membership applies only to operations on the same computer. Network operations and a few other system operations ignores it.

When no user is logged on or the logged on user cannot be determined, main Host processes run in this synthesized local security context:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Anonymous logon (S-1-5-7) (Windows NT or 2000) or Local Service (S-1-5-19) (Windows XP or later).</td>
</tr>
<tr>
<td>Groups</td>
<td>ImperoActivity, EveryOne (S-1-1-0), INTERACTIVE (S-1-5-4), Users (S-1-5-32-545, Windows 2000 and later only), S-1-5-1333028174-1801727600-1093862016-1001, S-1-5-1333028174-1801727600-1093862016-1024 and S-1-5-1333028174-1801727600-1093862018-1024</td>
</tr>
<tr>
<td>Privileges</td>
<td>SeChangeNotifyPrivilege (Traverse folders) and SeShutdownPrivilege (allows reboot or shutdown through Impero).</td>
</tr>
<tr>
<td>Default owner</td>
<td>ImperoActivity, in a few cases Anonymous logon (S-1-5-7)</td>
</tr>
<tr>
<td>Default group</td>
<td>ImperoActivity</td>
</tr>
<tr>
<td>Default ACL</td>
<td>LocalSystem – Full Access, ImperoActivity – Full Access</td>
</tr>
<tr>
<td>Network credentials</td>
<td>None</td>
</tr>
</tbody>
</table>

Depending on system configuration, Impero may be running in this local context all the time and impersonate the logged on user, or it may run as the logged on user and impersonate the local context.

See also

ImperoActivity Local Group

5.4.2.2 Replace the Local Security Context

The local security context described in Normal Operation can be replaced by an actual local or domain account by the Run As feature. See the User’s Guide > Dialog box help > Guest dialog boxes > Program Options > Run As tab.
5. Advanced Tools

Impero Connect Administrator’s Guide

5.4.2.3 Disable Main Host Processes Security

In some cases, Impero may refuse to function as it should because overzealous security settings do not grant some needed permission to neither EveryOne, INTERACTIVE nor ImperoActivity. To diagnose if this is the cause of a problem, you can temporarily disable the security restrictions on the main Host processes.

In the Windows Registry, find the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Impero Host for NT Service \SecurityLevel

Change the LowLevel key value from 0 to 1.

**Caution!** Changing this setting requires administrative privileges and creates an obvious security hole, so it should be returned to its default value 0 as soon as the cause of a problem has been identified.

Reload Impero Host with Impero Helper Service. The main Host processes runs with full LocalSystem rights and privileges rather than in the restricted context described in Normal Operation. This gives no network access rights. Also if the Impero Host program is started manually by a user, it may arbitrarily choose to run as either LocalSystem or that user. To make it run as LocalSystem, on the Program Options window General tab check the Load Host at Windows Startup box, then Reload Impero Host with Impero Helper Service.

The typical resolution of problems that need this setting is to grant the ImperoActivity Local Group read permission to some file, directory or registry key that is needed by Windows to perform a task requested by Impero.

Please inform Impero Support about any general permissions needed so that we can update the list of permissions granted by default, see ImperoActivity Local Group.

See also

Impero Helper Service
Normal Operation
Reload Impero Host with Impero Helper Service
ImperoActivity Local Group

5.4.3 Impero Helper Service

This small service has been carefully designed for extra high security. It is the only component of a running Impero Connect installation that runs in the powerful LocalSystem context. The sole purpose and functionality of Impero Helper Service is to perform selected privileged operations on behalf of the other Impero processes so that these larger processes can be run with safer more restricted privileges. Impero Helper Service is designed to resist attempts to use it for any other purpose.

Impero Helper Service must be configured to run under the LocalSystem account with permission to interact with the desktop. Any other configuration is going to probably fail or actually reduce overall security. Several of the tasks performed by Impero Helper Service are permitted only for the LocalSystem account and have no administrative option to grant similar permission to a dedicated service account.

Impero Helper Service is located entirely in the program file NHOSTSVC.EXE, but not all processes running in this program file are part of Impero Helper Service or run in LocalSystem context. Additionally, Impero Helper Service sometimes runs sub-tasks using RUNDLL32.EXE from the system32 directory, but only some of these run with LocalSystem privileges.

Notice that the bulk of Impero Connect runs in a much more restricted context. See Main Host Processes.
Note: The major part of the NHOSTSVC.EXE file is error and log messages, not program code.

5.4.3.1 Reload Impero Host with Impero Helper Service

If you stop Impero Helper Service from the Windows Control Panel > NT Server Manager > Microsoft Management Console or other administrative tools, the service unloads the Host or extended Host before the service stops. This action is logged in the Windows Application event log.

If you start or restart Impero Helper Service using the same tools, it executes the actions it normally executes when Windows starts on the computer. Stopping and starting Impero Helper Service is therefore a useful method for reloading a Host or extended Host remotely or through a batch file such as:

```plaintext
NET STOP "Impero Host for NT Service"
NET START "Impero Host for NT Service"
```

Notice that the registry name of Impero Helper Service is Impero Host for NT Service for compatibility with older Impero versions.

See also
Impero Helper Service

5.4.4 Impero Activity Local Group

The installation of Impero Host or an extended Host creates a Windows local group named ImperoActivity.

The purpose of the ImperoActivity local group is to contain the permissions required by Impero Host and extended Hosts to function properly on the computer. It has been carefully designed to serve only this purpose.

The ImperoActivity local group intentionally has no members.

Caution! Do not add any members to ImperoActivity local group, as this compromises the computer system security and integrity.

When Impero Host or an extended Host loads on the computer, Impero Helper Service determines which permissions in addition to those granted to ImperoActivity local group by default are required for the Impero module to function properly on the computer. These permissions are granted to ImperoActivity local group, if available. Impero Helper Service log sevents of permissions granted persistently to ImperoActivity local group in the Windows event log.

The permissions of the ImperoActivity local group are available to a Impero Host or extended Host loaded on the computer.

A list of the default permissions granted to ImperoActivity local group is published in the Impero KnowledgeBase. It is revised from time to time based on user input and the developments in Windows operating systems.

Note: Do not confuse the Windows permissions of ImperoActivity local group with the Windows Security Management access privileges granted to Impero Guests on Impero Hosts or extended Hosts. These Guest Access Privileges are explained in the User's Guide.

See also
Impero Helper Service

5.5 Impero Connect Command Line Parameters

As an alternative to starting Impero Guest or Impero Host from Windows' Start menu or directly from the folder where NGSTW32.EXE or NHSTW32.EXE is installed, you can start the executable from a command line and add parameters to have full control of what happens on startup.
In a command line window, type the full path to the .exe file followed by a space and then one or more of the available parameters, for example:

```
C:\Program Files\Impero\Impero Connect\Guest\ngstw32.exe /C:WebConnect /H:myhost
```

This connects to a Host machine called myhost using the WebConnect communication profile. By default, this also establishes a Connect session. The full lists of parameters are given below.

### 5.5.1 Guest parameters

Impero Guest accepts maximum 9 command line parameters in the following format:

```
ngstw32.exe [commands...] [additional_parameter]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/A:</td>
<td>Start an Audio-Video Chat session with the connected Host.</td>
</tr>
<tr>
<td>/B:&lt;FileName&gt;</td>
<td>Play back session recording file.</td>
</tr>
<tr>
<td></td>
<td>Do not combine this switch with other parameters.</td>
</tr>
<tr>
<td>/C:&lt;Communication profile&gt;</td>
<td>Connect by &lt;Communication profile&gt; to the Host specified by the switch /H: or /P:.</td>
</tr>
<tr>
<td>/CC:&lt;ProfileName&gt; &amp;&amp;&lt;CMURL&gt;&amp;&amp;&lt;User name&gt;&amp;&amp;&lt;Password&gt;&amp;&amp;&lt;Domain&gt;</td>
<td>Create the specified Webconnect profile.</td>
</tr>
<tr>
<td>/CD:&lt;ProfileName&gt;</td>
<td>Delete the specified webconnect profile.</td>
</tr>
<tr>
<td>/D:</td>
<td>Disconnect from the connected Hosts.</td>
</tr>
<tr>
<td></td>
<td>Do not combine this parameter with other parameters.</td>
</tr>
<tr>
<td>/DT:&lt;SessionId&gt;</td>
<td>Disconnect tunnel session from external program by &lt;SessionId&gt;</td>
</tr>
<tr>
<td>/E:&lt;PhoneBookFileName&gt;</td>
<td>Show the Connection Properties of &lt;Phonebook file path and name&gt; or, if combined with a session parameter (/A:, /F:, /G:, /R: or /V:), start this session with the &lt;Phonebook file path and name&gt; Host.</td>
</tr>
<tr>
<td>/F:</td>
<td>Start a File Transfer session with the connected to Host.</td>
</tr>
<tr>
<td>/G:</td>
<td>Start a Remote Management session with the connected to Host.</td>
</tr>
<tr>
<td>/H:&lt;DisplayHostName&gt;</td>
<td>Connect to &lt;DisplayHostName&gt; Host by a communication profile or the one specified by /C:</td>
</tr>
<tr>
<td>/I:</td>
<td>Start Get Inventory session.</td>
</tr>
<tr>
<td>/J:</td>
<td>Start Demo session.</td>
</tr>
<tr>
<td>/LGD:&lt;LoginDomain&gt;</td>
<td>Specify login domain for connecting to a Gateway.</td>
</tr>
<tr>
<td>/LGN:&lt;LoginID&gt;</td>
<td>Specify login name when connecting to a Gateway.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>LGP:&lt;LoginPassword&gt;</td>
<td>Specify login password for connecting to a Gateway.</td>
</tr>
<tr>
<td>LGEP:&lt;EncryptedLoginPassword&gt;</td>
<td>Specify encrypted login password for connecting to a Gateway.</td>
</tr>
<tr>
<td>LHD:&lt;LoginDomain&gt;</td>
<td>Specify login domain for connecting to a Host.</td>
</tr>
<tr>
<td>LHN:&lt;LoginID&gt;</td>
<td>Specify login name when connecting to a Host.</td>
</tr>
<tr>
<td>LHP:&lt;LoginPassword&gt;</td>
<td>Specify login password for connecting to a Host.</td>
</tr>
<tr>
<td>LHEP:&lt;EncryptedLoginPassword&gt;</td>
<td>Specify encrypted login password for connecting to a Host.</td>
</tr>
<tr>
<td>M:[&lt;FileName&gt;]</td>
<td>Record Connect session to <code>&lt;FileName&gt;</code>. Only works in conjunction with <code>/P:</code> or <code>/H:</code>. Combine this parameter with <code>/R:</code> to record the Connect session. If no <code>&lt;Recording file path and name&gt;</code> is specified, a recording file named <code>&lt;Time stamp&gt;-&lt;Guest ID&gt;-&lt;Host ID&gt;.dwr</code> is saved in the Impero Configuration Files record directory.</td>
</tr>
<tr>
<td>P:&lt;HostPhoneNr&gt;</td>
<td>Connect to <code>&lt;HostPhoneNr&gt;</code> Host by a dynamic communication profile or the one specified by <code>/C:</code></td>
</tr>
<tr>
<td>R:</td>
<td>Start a Connect session with the connected Host.</td>
</tr>
<tr>
<td>S:&lt;FileName&gt;</td>
<td>Run script <code>&lt;FileName&gt;</code>. Do not combine this parameter with other parameters.</td>
</tr>
<tr>
<td>TUN:</td>
<td>Start Tunnel session with hidden tunnel console.</td>
</tr>
<tr>
<td>TUC:</td>
<td>Start Tunnel session.</td>
</tr>
<tr>
<td>V:</td>
<td>Start a Chat session with the connected Host.</td>
</tr>
<tr>
<td>X:&lt;Number of pixels from left screen border&gt;[,&lt;Number of pixels from upper screen border&gt;][,&lt;Number of pixels width&gt;][,&lt;Number of pixels height&gt;]]</td>
<td>Connect window position and size. Combine this parameter with <code>/R:</code> to specify a non-default position and size of the Connect window.</td>
</tr>
<tr>
<td>YD:&lt;ServiceTicketId&gt;</td>
<td>Delete Help Service/Service ticket <code>&lt;ServiceTicketId&gt;</code>.</td>
</tr>
<tr>
<td>YT:&lt;TicketId&gt;</td>
<td>Add Service ticket <code>&lt;TicketId&gt;</code>.</td>
</tr>
</tbody>
</table>
The above parameters can also be used to start or control Impero Guest from another application.

**Examples**
The examples should be on one line and are broken in two lines for formatting reasons only.

```
<Impero Guest program path and file>
/E:“C:\ProgramData\Impero\Impero Connect\Guest\John.dwc” /R: /M:

**Explanation:** Load Guest and connect to the Host of the phonebook entry file John.dwc that is located in the C:\ProgramData\Impero\Impero Connect\Guest directory to start a Connect session with it and record the session storing the recording file in its default location with its default name.

```

```
<Impero Guest program path and file> /C:TCP/IP /H:Peter /F:

**Explanation:** Load the Guest and using the communication profile TCP/IP connect to the Host named Peter to start a file transfer session with it.

```

```
<Impero Guest program path and file> /S:“C:\SCRIPTS\MY SCRIPT.DWS”

**Explanation:** Load the Guest and run the C:\SCRIPTS\MY SCRIPT.DWS script file.

**Note:** Parameter paths and file names that contain spaces and special characters must be enclosed by double quotes.

### 5.5.2 Host parameters

Impero Host accepts maximum 9 command line parameters in the following format:

```
nhstw32.exe [commands...] [host_name]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/C:&lt;communication profile&gt;</td>
<td>Enable &lt;communication profile&gt; in addition to other selected Communication Profiles. The setting is not stored.</td>
</tr>
<tr>
<td>/I:&lt;Inventory file path and name&gt;</td>
<td>Generate and retrieve Host computer inventory to store it in &lt;Inventory file path and name&gt;.</td>
</tr>
<tr>
<td>/R:&lt;HostName&gt;</td>
<td>Set the Host ID. The setting is stored.</td>
</tr>
</tbody>
</table>
### /W: [+/-]
- /W: Start Host at loading.
- /W:+ Start Host at loading. Save the setting to **Program Options**.
- /W: Do not start Host at loading. Save the setting to **Program Options**.

### /Q:
Close program after successful connection.

### /resetperm /mpass: [Maintenance password]
Resets permissions on the Host to default permissions, the permissions you had initially configured on the connected Host, the ones located on the Host in the `.ndb` files.

Prerequisites for this command to work:
- On the Host machine go to **Tools > Maintenance Password**, set a maintenance password and select the Guest access security check box.
- Enter the correct maintenance password in the `/mpass:` [Maintenance Password] command line option.

### /restart /mpass: [Maintenance password]
Restarts the Host.

Prerequisites for this command to work:
- On the Host machine go to **Tools > Maintenance Password**, set a maintenance password and select the **Unload and Stop** check box.
- Enter the correct maintenance password in the `/mpass:` [Maintenance Password] command line option.

If user interaction is needed (e.g.: "are you sure you want to restart, because..."), the command is not successful.

### /restart:force /mpass: [Maintenance password]
Restart the Host forcefully. The command bypasses any user interaction.

Prerequisites for this command to work:
- On the Host machine go to **Tools > Maintenance Password**, set a maintenance password and select the **Unload and Stop** check box.
- Enter the correct maintenance password in the `/mpass:` [Maintenance Password] command line option.

### /setperm:[permission]=on|off /mpass: [Maintenance password]
Sets the permissions for existing connections to the host. To see the list of permissions and associated codes, click here.

The permissions can be enabled or disabled by using on or off.

The `/setperm` parameter can be used multiple times in order to define more permissions in the same command line.

Here is an example:

```
"C:\Program Files (x86)\Impero\Impero Connect\Host\nowutil.exe" /h /setperm:2.1.2=off /setperm:2.1.3=off /mpass:a
```

The permissions are changed on-the-fly, no host restart is needed.
Prerequisites for this command to work:

- On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Guest access security check box.
- Enter the correct maintenance password in the /mpass: [Maintenance Password] command line option.

/start

Starts the Host. If user interaction is needed (e.g.: "are you sure you want to start, because...")

/start:force

Starts the host forcefully, bypassing any user interaction.

/stop /mpass:[Maintenance password]

Stops the Host.
Prerequisites for this command to work:

- On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Unload and Stop check box.
- Enter the correct maintenance password in the /mpass: [Maintenance Password] command line option

If user interaction is needed (e.g.: "are you sure you want to stop, because...")

/stop:force /mpass:[Maintenance password]

Stops the Host forcefully. The command bypasses any user interaction.
Prerequisites for this command to work:

- On the Host machine go to Tools > Maintenance Password, set a maintenance password and select the Unload and Stop check box.
- Enter the correct maintenance password in the /mpass: [Maintenance Password] command line option

/T:<TimeOut>

Close program after timeout <TimeOut> minutes.

/ZH:<SerialComHandle>

Sets handle for serial communication.

/ZZTOP

Enables DTL log.

/Wizard

Displays the Program Options dialog.

/WizardOnly

Displays the Setup Wizard.

Request Help by using one or more of these parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/R:R</td>
<td>Initiates a help request from the Host.</td>
</tr>
<tr>
<td>/R:C</td>
<td>Cancels the help request from the Host.</td>
</tr>
<tr>
<td>/HD:&lt;HelpCommentBuffer&gt;</td>
<td>Specifies a help request problem description.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Function</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/HP:&lt;HelpProvider&gt;</td>
<td>Specifies a help provider (help service name or service ticket number).</td>
</tr>
<tr>
<td>/HC:&lt;SpecificComProfName&gt;</td>
<td>Specifies a help request communication profile.</td>
</tr>
<tr>
<td>/HA:&lt;PhoneNumber or TCP/IP Address&gt;</td>
<td>Specifies a help provider address (Guest address or Connection Manager URL. The Connection Manager URL can be omitted if specified in the used WebConnect communication profile). Save the setting to Program Options &gt; Advanced Help Request Options.</td>
</tr>
<tr>
<td>/HW:</td>
<td>Must be included with a help request via WebConnect.</td>
</tr>
<tr>
<td>/HS:</td>
<td>In case no help provider is found, the help request fails silent.</td>
</tr>
<tr>
<td>/HT:</td>
<td>Enables service tickets. Setting saved to Program Options &gt; Advanced Help Request Options.</td>
</tr>
</tbody>
</table>

Cancel a pending help request by this parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/HH:</td>
<td>Cancels a pending help request.</td>
</tr>
</tbody>
</table>

Log on to a Guest network connecting Impero Gateway by these parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>/LGN:&lt;HelpReqLoginID&gt;</td>
<td>Specifies a Gateway login name. The setting is saved to Program Options &gt; Advanced Help Request Options.</td>
</tr>
<tr>
<td>/LGP:&lt;HelpReqLoginPassword&gt;</td>
<td>Specifies a Gateway login password. The setting is saved to Program Options &gt; Advanced Help Request Options.</td>
</tr>
<tr>
<td>/LGD:&lt;HelpReqLoginDomain&gt;&gt;</td>
<td>Specifies a Gateway login domain. The setting is saved to Program Options &gt; Advanced Help Request Options.</td>
</tr>
<tr>
<td>/LGC:</td>
<td>Specifies that help request gateway login uses current credentials for Windows Security authentication. The setting is saved to Program Options &gt; Advanced Help Request Options.</td>
</tr>
</tbody>
</table>

Examples
The examples should be on one line and are broken in two lines for formatting reasons only.

<Impero Host program path and file> /R:John C:/TCP/IP /W:
Explanation: Load Host with the Host name John, start the Host (do not store) enabling TCP/IP and other selected communication profiles.

<Impero Host program path and file> /R:Peter /W:+
Explanation: Load Host with the Host name Peter, start the Host (store) enabling selected
<Impero Host program path and file> /HD:“Nothing works” /HP:“Windows Help” /HC:TCP4 /HA:192.168.102.58

**Explanation:** Load the Host and send a help request with the problem description "Nothing works", help provider Windows Help, communication profile TCP4 and IP address 192.168.102.58.

**Note:** Parameters that contain spaces or special characters must be enclosed by double quotation marks.

### Connect Permissions

This is the list of Connect permissions and associated codes:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>View remote screen</td>
<td>2.1.1</td>
</tr>
<tr>
<td>Use keyboard and mouse</td>
<td>2.1.2</td>
</tr>
<tr>
<td>Lock keyboard and mouse</td>
<td>2.1.3</td>
</tr>
<tr>
<td>Blank the screen</td>
<td>2.1.4</td>
</tr>
<tr>
<td>Transfer clipboard</td>
<td>2.1.5</td>
</tr>
<tr>
<td>Execute command</td>
<td>2.1.6</td>
</tr>
<tr>
<td>Request chat</td>
<td>2.1.7</td>
</tr>
<tr>
<td>Request audio chat and transfer sound</td>
<td>2.1.8</td>
</tr>
<tr>
<td>Request video</td>
<td>2.1.9</td>
</tr>
<tr>
<td>Send files to host</td>
<td>2.1.10</td>
</tr>
<tr>
<td>Receive files from host</td>
<td>2.1.11</td>
</tr>
<tr>
<td>Run programs</td>
<td>2.1.12</td>
</tr>
<tr>
<td>Redirect print</td>
<td>2.1.13</td>
</tr>
<tr>
<td>Remote Manage</td>
<td>2.1.14</td>
</tr>
<tr>
<td>Retrieve inventory</td>
<td>2.1.16</td>
</tr>
<tr>
<td>Send message</td>
<td>2.1.17</td>
</tr>
<tr>
<td>Demonstrate</td>
<td>2.1.18</td>
</tr>
<tr>
<td>Join multi Guest session</td>
<td>2.1.19</td>
</tr>
<tr>
<td>Act as multi Guest session Administrator</td>
<td>2.1.20</td>
</tr>
<tr>
<td>Select remote monitor</td>
<td>2.1.21</td>
</tr>
</tbody>
</table>
5.6 Impero Connect and URI

Starting with Impero Connect 12.5 you can launch Impero Guest from a web page and easily perform an action by using Uniform Resource Identifiers (URIs).

What is URI?

URI is a string of characters used to identify a resource enabling interaction with representations of the resource over a network.

The syntax of the URI is:

```
scheme:[//host][/]path?query#[fragment]
```

Where:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme</td>
<td>Identifies the custom protocol to the OS. In this case it is nrc. It is mandatory.</td>
</tr>
<tr>
<td>host</td>
<td>This is the Impero Host unique identifier. Based on the communication profile this is just a string containing an IP, hostname or unique identifier.</td>
</tr>
<tr>
<td>path</td>
<td>The main operation descriptor, or sub-operations encoded in the path hierarchy. It can have the following values: &quot;remote-control&quot;, &quot;file-transfer&quot;, &quot;remote-management&quot;, &quot;chat&quot; and &quot;inventory&quot;.</td>
</tr>
</tbody>
</table>
| query     | This is used mainly for integration with the Impero Portal and it allows the Guest to use a pre-authenticated Portal communication profile when performing the action described by path. 

query is in the format url=[url]

url is the address of the Impero Portal, for instance: portal.Impero.com. If there is no existing communication profile with the same URL, a new Portal communication profile is automatically created, otherwise the existing communication profile is used. If there is a Portal communication profile and it is authenticated, a connection is established. If the profile is not authenticated, a Impero Portal login window is displayed and after a successful authentication, the connection is established. 

**NOTE:** query was added in NRC 12.70. |
| fragment  | The communication profile type. 

When the #direct command is entered as the fragment for a URI, the Guest is directed to open, connect to the specified host, begin the action specified by the path (Connect, file transfer, remote management, chat, inventory), and use the first communication profile from the list of communication profiles on the Guest, containing a TCP/IP (TCP) communication device. If no fragment is specified, or if the #portal command is entered, the default communication profile selected for the session is the one which has an imperio Portal communication device. |

Examples of URI

<table>
<thead>
<tr>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 5 Advanced Tools

**Impero Connect Administrator's Guide**

<table>
<thead>
<tr>
<th>nrc:</th>
<th>Opens the Guest.</th>
</tr>
</thead>
<tbody>
<tr>
<td>nrc://</td>
<td>Opens the Guest.</td>
</tr>
<tr>
<td>nrc://MY-COMPUTER/remote-control</td>
<td>Opens the Guest in a Connect session with the specified Host ID (in this case specified by Host ID: MY-COMPUTER). The communication profile is not specified; therefore, in order for the Connect session to work, you should have created a Impero Portal communication profile on the Guest.</td>
</tr>
<tr>
<td>nrc://192.168.200.30/remote-control/#direct</td>
<td>Opens the Guest in a Connect session with the Host (in this case specified by IP: 192.168.200.30) using the first communication profile of type &quot;direct&quot; (that has the Communication Device set to TCP/IP (TCP)).</td>
</tr>
<tr>
<td>nrc://localhost1/file-transfer</td>
<td>Opens the Guest in a file transfer session with the specified Host using a Impero Portal communication profile on the Guest.</td>
</tr>
<tr>
<td>nrc://hostname/inventory</td>
<td>Opens the Guest in a request inventory session with the specified Host and if allowed by the Guest Access Security settings on the Host, it generates an inventory of Host computer hardware and software.</td>
</tr>
<tr>
<td>nrc://hostname/remote-control?url=portal.Impero.com</td>
<td>Opens the Guest in a Connect session with the specified Host using a Impero Portal communication profile with the given URL.</td>
</tr>
</tbody>
</table>

**How to use URI with the Impero Guest?**

On the machine where the Impero Guest resides, open a web browser and enter the URI corresponding to the action you want to perform: open the Guest, Connect, file transfer, remote management, chat or inventory. Based on the browser and operating system, it might be needed to have an actual HTML file including a URI link and use that link instead of using the URI directly in the browser.

### 5.7 Kerberos authentication

In some Windows Active Directory environments, it is not possible to communicate between Impero applications using the traditional NTLM authentication methods when the Host is configured to use Windows Security Management as the preferred authentication type. This would be the case in an Active Directory environment where multiple Domains existed with the same NetBIOS name. For example,

<table>
<thead>
<tr>
<th>Parent Domain</th>
<th>Child Domain</th>
<th>NetBIOS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain1.local</td>
<td>Sales.domain1.local</td>
<td>Sales</td>
</tr>
<tr>
<td>Domain2.local</td>
<td>Sales.domain2.local</td>
<td>Sales</td>
</tr>
</tbody>
</table>

In this example, each child domain has a unique FQDN (Fully Qualified Domain Name) but uses the same NetBIOS Domain name.

In order for the Guest to connect to Hosts in such environments, the following should be added to the Impero.INI file on the Guest machine:

```
[DANWARE]
ForceKerberosAuthentication=1
```
Restart the Guest application for the changes to take effect. When connecting to Hosts using this method, the FQDN of the Host should be used. The Guest should also supply the FQDN for the Domain name at the authentication stage. Kerberos authentication is not backwards compatible with older Hosts and cannot be used with Hosts that do not require Kerberos authentication.

**Notes:**

- Use the FQDN (Fully Qualified Domain Name) as the connection name on the Guest.
- When authenticating, use the FQDN in the **Domain** field.
A

About Netop Security Manager window 18
About tab
  ActiveX Guest 145
Accessible Hosts 52, 64, 78, 84
Active Sessions 43
Add Group command 131
Add Netop Guest ID to Netop Guest ID Group window
Add User command 131
Additional Tools 120
Advanced Tools 137
All Remaining button 20
Allow Guest to section 128
Always the workstation selection 13, 39
AMPLUS.EXE 120
AMPLUS.ZIP 121
Answer Access Server 6.5 Requests 37
authentication
  kerberos 208

C

Call back section 128, 132
chatting, NGuestX 145
Choose Account window 131
Clear 31
Clear database upon startup check box 135
Clear Messages command 16
Client refresh rate field 135
Communication Setup 118, 125
compressing transmitted data 144
Compression tab
  ActiveX Guest 144
Computer Resources Considerations (TSE) 140
ComputerName column 68
Connect and Disconnect 183
Connect between TSEs 139
Connect into a TSE 139
Connect out of a TSE 138
Connection direction section 126
Connection Properties
  ActiveX Guest 142
  ActiveXGuest 142, 143, 144, 145
Connection Status dialog box
  Disconnect 145
  Disconnect Guests 145
  Properties 145
  Save log 145
  Start chat 145
  Suspend further connections 145
  Take keyboard and mouse control 145
Container application 141
Contents Creation Guide 23
Copy command 15
Create and Delete 182
Create local test database check box 11
Create Role Assignments 24
Credentials window 88

D

Data source field 11
Database Systems 120
Default access privileges assigned section 128
Delete 31, 35, 48, 52, 54, 57, 59, 64, 67, 70, 73, 75, 78,
80, 84, 86, 90
Delete Selected button 19
Description column 33, 42, 44, 49, 52, 55, 58
Details 47
Details button 19
Device Group 126
Device group field 125
Directory Service 87
Directory Service window 90
Directory Service wizard 88
Directory Services credentials selection 13
Directory Services Definitions 82
Directory Services Definitions branch 82
Directory Services Definitions command 16
Directory Services Group 85
Directory Services Group window 86
Directory Services User 82
Directory Services User window 84
Disable Main Host Processes Security 198
disconnecting from Host, NGuestX 145
Display tab
  ActiveX Guest 144
Index

DN column 82, 85
Domain column 62, 66, 68, 71
Domain drop-down box 30, 63, 67, 69, 72, 75
Domain section 131
DomainName column 74
DWBATH: Scheduled Jobs 100
DWCONN: Active Sessions 101
DWDOMN: Windows Domain 102
DWDONE: Security Log 102
DWEVNT: Netop Log 103
DWGRUH: Netop Host ID Group 103
DWGRUP: Netop Guest ID Group 103
DWHOGR: Netop Host ID Group Members 104
DWHOSET: Netop Host ID 104
DWLDAPGRP: Directory Service Group 105
DWLDAPPROP: Directory Service Properties 105
DWLDAPSERV: Directory Service 106
DWLDAPUSR: Directory Service User 106
DWMAIN: Role Assignment 107
DWNTGR: Windows Group 108
DWNTUS: Windows User 108
DPKI: Public/Private Keys 109
DWPOLI: Security Policies 109
DWPROPI: Netop Properties 110
DWROLE: Roles 110
DWRSAGRP: RSA SecurID Group 111
DWRSAPROP: RSA SecurID Properties 111
DWRSASUR: RSA SecurID User 112
DWRSNG: RSA SecurID Group Members 112
DWSERV: Netop Security Servers 112
DWTOD: Scheduled Actions 113
DUSER: Netop Guest IDs 113
DWHITEGR: Netop Guest ID Group Members 114
DWWKGM: Members of Workstation Groups 115
DWWKSG: Workstation Groups 115
DWWKST: Workstations 115

E

Edit 31, 35, 48, 52, 54, 57, 59, 64, 67, 70, 72, 75, 78, 80, 84, 86, 90
Edit Menu 15
Edit Selected button 19
Enable incoming to outgoing communication 126
encrypted bind 17
Encryption tab
  ActiveX Guest 144
End Time window 46
Examples 187
F

File Menu 15
Filter and Fetching Bar 20
Filters window 89
Full Control 33
G

Gateway Access Privileges tab 128
Gateway settings section 125
General tab 50, 56
Grant All Guests Default Privileges 128
Grant Each Guest Individual Access Privileges Using Netop Authentication 129
Grant Each Guest Individual Access Privileges Using Windows Security Management 130
Group drop-down box 67, 72
Group ID (public) field 37
Group ID public field 12
Group name (private) field 12, 37
GroupName (private) field 52, 71
Guest Profile window 130
Guests enter Directory Services user name and password selection 38
Guests enter Netop Guest ID and password selection 38
Guests enter RSA SecurID user name and password selection 38
Guests enter Windows user name and password selection 38
H

Hello World Script 187
Help Menu 17
Host column 42
Host Protection tab
  ActiveX Guest 145
How to Use Netop Guest ActiveX Component 141
I

ID column 33, 45, 53, 58
Incoming and Outgoing 122
Incoming connections only selection 126

Individual Guest access privileges assigned section 130
Initial Setup of Guests and Hosts window 29
Initial Setup of Roles window 30
Initial Setup wizard 29
Insert <Account type> as Guest window 28
Insert <Account type> as Host window 29
Insert Directory Services Group window 86
Insert Directory Services User window 83
Insert Reference to Domain window 75
Insert Role Assignment window 29
Insert Windows Group (Workstation) window 72
Insert Windows Group window 67
Insert Windows User window 63
Insert Workstation window 69

Inside 122
Inside communication 138
Installation (TSE) 137
Introduction 7

Jobs menu 45

Keep Synchronized Script 188
kerberos 208
keyboard mode 143
Keyboard tab
  ActiveX Guest 143

Large Icons button 19
Large Toolbar command 16
LDAP 17
List button 19
Load Netop Security Manager 11
Locate window 88
Logging 40
Logging branch 41
Logging command 16
Logging Options 40
Logging Options window 40
logging, NGuestX 145
Logon button 11
Logon to Database window 11
Logon to Database window 11

Main Host Processes 197
Maintenance 119
Make this Host a Netop Name Server check box 135
Manage Security Database Contents 22
managing multi Guest sessions, NGuestX 145
Member Of Tab 51, 56
Members 54, 59, 73, 80
Menu Bar 14
Messages command 16
Messages Panel 22
Mouse tab
  ActiveX Guest 143

Netop Communication (TSE) 138
Netop credentials selection 13
Netop Definitions 48
Netop Definitions branch 48
Netop Definitions command 16
Netop Gateway 122
Netop Gateway and Firewall 124
Netop Gateway Communication Profile Edit window 125
Netop Gateway Communication Profile Setup window 125
Netop Gateway Functionality 122
Netop Gateway Setup 124
Netop Gateway Setup (TSE) 138
Netop Gateway window 124
Netop Group Add Members window 54
Netop Gateway Membership window 54
Netop Group window 53
Netop Guest ActiveX Component 140
Netop Guest ID 49
Netop Guest ID Group 52
Netop Guest ID Password Properties window 60
Netop Guest ID window 50
Netop Helper Service 198
Netop Host computer screen image 142
Netop Host Functionality (TSE) 140
Netop Host ID 55
Index

Netop Host ID Group 57
Netop Host ID selection 13, 40
Netop Host ID window 56
Netop in Terminal Server Environments 137
Netop Log 42
Netop Name Management 134
Netop Name Management Functionality 134
Netop Name Server 134
Netop Name Server Setup 135
Netop Name Server tab 135
Netop Name Server window 135
Netop Naming (TSE) 138
Netop net field 126
Netop Net Number 127
Netop Processes 196
Netop Properties 60
Netop Properties for Domain window 75
Netop Properties for Role Assignment window 31
Netop Properties for Windows (Workstation) Group window 73
Netop Properties for Windows Group window 67
Netop Properties for Windows User window 64
Netop Properties for Workstation window 70
Netop Remote Control Processes and Windows Security 138
Netop RSA SecurID Properties window 81
Netop Scripting ActiveX Control 181
Netop Security Management 8
Netop Security Management flowsheet 8
Netop Security Management Functionality 8
Netop Security Management Overview 8
Netop Security Management Setup 9
Netop Security Manager Window 14
Netop Security Role window 34
Netop Security Server Setup 10, 116
Netop Security Server Setup window 116
Netop Security Server window 116
NetopActivity Local Group 199
NETOLOG.ZIP 121
NetopX Connect window 141
NetopX Connection Properties dialog box 142
NetopX graphical area 141
Network_point-to-point 122
NetopLog 42
Networking 122
Networking to Networking 123
New 28, 34, 45, 50, 56, 59, 63, 67, 69, 72, 75, 77, 79, 83, 86, 88
New Batch 29
New Netop Guest ID button 18
New Netop Guest ID Group button 18
New Netop Host ID button 18
New Netop Host ID Group button 19
New Role Assignment button 18
New Role button 19
New Scheduled Job button 19
NGuestX Connect window
   Communication profile 141
   Gateway 141
   Host name 141
   IP address 141
No Access 33
No Toolbar command 16
ODBC Microsoft Access Setup window 11
One More Lot button 20
Options Menu 17
Outgoing to Incoming 123
Outside 122
Outside communication 138
Password column 49
Password section 128
Permitted Guests 57, 65, 70
Point-to-point 122
Preferred Guest Type 38
Preferred Host Type 39
Prerequisites 118
Program Options window 17
Programmer Information 146
protecting transmitted data 144
protected transmission 144
pruning 118
P
R

RAS section 131
Records Menu 15
Records Pane 21
Reference 189
Refresh button 20
Reload Netop Host with Netop Helper Service 199
Remote Desktop tab
  ActiveX Guest 142
Rename window 130
Replace the Local Security Context 197
Requirements (ActiveX) 140
Review Security Policies 23
Role 31
Role Assignment 27
Role Assignment wizard 28
RoleName column 32
RSA SecurID credentials selection 13
RSA SecurID Definitions 76
RSA SecurID Definitions branch 76
RSA SecurID Definitions command 16
RSA SecurID Group 78
RSA SecurID Group Members Add window 80
RSA SecurID Group Members window 80
RSA SecurID Group window 79
RSA SecurID Properties 81
RSA SecurID User 76
RSA SecurID User window 77
Run As Tab 117
Running Netop Security Management 10

S

Scheduled Job wizard 45
Scheduled Jobs 44
Scheduling 44
Scheduling branch 44
Scheduling command 16
Security 120
Security Database Setup 9
Security Database Tables 99
Security Database Wizard 12
Security Database Wizard Preferred Guest Type window 13
Security Database Wizard Security Server Group Name window 12
Security Database Wizard Security Server List window 12
Security Log 41
Security Policies 35
Security Policies Preferred Guest Type Tab 38
Security Policies Preferred Host Type window 39
Security Policies Security Server List window 37
Security Policy Security Server Group Name window 36, 37
Security Role window 129
Security Server Group Name 36
Security Server List 37
Security Server Public Key 36
Security Server Tab 117
Security Settings 26
Security Settings branch 26
Security Settings command 16
Security Setup 128
Security_Policies Smart Card Tab 38
Select <Type> Group window 46
Select Guest Type window 28
Select Host Type window 28
Selection Pane 21
Server Properties window 38
Service column 83, 85
Service Name window 90
Small Icons button 19
Small Toolbar command 16
special keystrokes
  mapping 143
speeding up transmission 144
Standard Role 33
Start Date and Time window 46
StartGuest, Initialize and Uninitialize 182
Status Bar 22
Status Bar command 16

T

Temporary Access window 45
Tip of the Day window 11
Title Bar 14
Index

Toolbar 18
Toolbar command 16
Transferring Files 185
Typically Disabled: Incoming to Outgoing 123

U

Unassigned Hosts’ Role 33
Use (TSE) 137
Use Netop Gateway 132
Use Netop Name Server 136
Use Netop Security Management 118
Username column 49, 62, 66, 76, 78
Username drop-down box 63

V

validate LDAP 17
Via Netop Gateway check box 141
View and Manage Data 24
View Menu 16
Visit All Hosts Script 187

W

Who May Remote Control Whom (Accessible Hosts) window 64
Who May Remote Control Whom (Permitted Guests) window 65
Windows credentials selection 13
Windows Definitions 61
Windows Definitions branch 61
Windows Definitions command 16
Windows Domain 74
Windows Group 65
Windows Group drop-down box 30
Windows group selection 46
Windows User 62
Windows user if one is logged on, otherwise workstation selection 39
Windows User Manager button 132
Windows user/workstation selection 13
Windows Workstation 68
Windows Workstation Group 70
Windows Workstation Group Members Add window 73
Windows Workstation Group Members window 73
Workstation drop-down box 69