ADMINISTRATOR'S GUIDE

Connect

Impero

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

2.4.2.3 Security Policies 35
2.4.2.3.1 Security Server Public Key 36
2.4.2.3.2 Security Server Group Name (backwards compatibility) 36
2.4.2.3.3 Security Server List 37
2.4.2.3.4 Preferred Guest Type 38
2.4.2.3.5 Preferred Host Type 39
2.4.2.3.6 Logging Options 40
2.4.3 Logging 40
2.4.3.1 Security Log 41
2.4.3.2 Impero Log 42
2.4.3.3 Active Sessions 43
2.4.4 Scheduling 44
2.4.4.1 Scheduled Job 44
2.4.4.1.1 New 45
2.4.4.1.2 Details 47
2.4.4.1.3 Edit 48
2.4.4.1.4 Delete 48
2.4.5 Impero Definitions 48
2.4.5.1 Impero Guest ID 49
2.4.5.1.1 New 50
2.4.5.1.2 Edit 52
2.4.5.1.3 Delete 52
2.4.5.1.4 Accessible Hosts 52
2.4.5.2 Impero Guest ID Group 52
2.4.5.2.1 New 53
2.4.5.2.2 Edit 54
2.4.5.2.3 Delete 54
2.4.5.2.4 Members 54
2.4.5.3 Impero Host ID 55
2.4.5.3.1 New 56
2.4.5.3.2 Edit 57
2.4.5.3.3 Delete 57
2.4.5.3.4 Permitted Guests 57
2.4.5.4 Impero Host ID Group 57
2.4.5.4.1 New 59
2.4.5.4.2 Edit 59
2.4.5.4.3 Delete 59
2.4.5.4.4 Members 59
2.4.5.5 Impero Properties 60
2.4.6 Windows Definitions 61
2.4.6.1 Windows User 62
2.4.6.1.1 New 63
2.4.6.1.2 Edit 64
2.4.6.1.3 Delete 64
2.4.6.1.4 Accessible Hosts 64
2.4.6.1.5 Permitted Guests 65
2.4.6.2 Windows Group 65

2.4.6.2.1 New 67
2.4.6.2.2 Edit 67
2.4.6.2.3 Delete 67
2.4.6.3 Windows Workstation 68
2.4.6.3.1 New 69
2.4.6.3.2 Edit 70
2.4.6.3.3 Delete 70
2.4.6.3.4 Permitted Guests 70
2.4.6.4 Windows Workstation Group 70
2.4.6.4.1 New 72
2.4.6.4.2 Edit 72
2.4.6.4.3 Delete 73
2.4.6.4.4 Members 73
2.4.6.5 Windows Domain 74
2.4.6.5.1 New 75
2.4.6.5.2 Edit 75
2.4.6.5.3 Delete 75
2.4.7 RSA SecurID Definitions 76
2.4.7.1 RSA SecurID User 76
2.4.7.1.1 New 77
2.4.7.1.2 Edit 78
2.4.7.1.3 Delete 78
2.4.7.1.4 Accessible Hosts 78
2.4.7.2 RSA SecurID Group 78
2.4.7.2.1 New 79
2.4.7.2.2 Edit 80
2.4.7.2.3 Delete 80
2.4.7.2.4 Members 80
2.4.7.3 RSA SecurID Properties 81
2.4.8 Directory Services Definitions 82
2.4.8.1 Directory Services User 82
2.4.8.1.1 New 83
2.4.8.1.2 Edit 84
2.4.8.1.3 Delete 84
2.4.8.1.4 Accessible Hosts 84
2.4.8.2 Directory Services Group 85
2.4.8.2.1 New 86
2.4.8.2.2 Edit 86
2.4.8.2.3 Delete 86
2.4.8.3 Directory Service 87
2.4.8.3.1 New 88
2.4.8.3.2 Edit 90
2.4.8.3.3 Delete 90
2.4.8.4 Organizational Units 91
2.4.8.4.1 New 91
2.4.8.4.2 Edit 91
2.4.8.4.3 Delete 91

2.4.8.5 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

2.7.4 Database Systems 120
2.7.5 Additional Tools 120
2.7.5.1 AMPLUS.EXE 120
2.7.5.2 AMPLUS.ZIP 121
2.7.5.3 IMPEROLOG.ZIP 121
3 Impero Gateway 122
3.1 Impero Gateway Functionality 122
3.1.1 Incoming and Outgoing 122
3.1.2 Outgoing to Incoming 123
3.1.3 Networking to Networking 123
3.1.4 Typically Disabled: Incoming to Outgoing 123
3.2 Impero Gateway Setup 124
3.2.1 Impero Gateway and Firewall 124
3.2.2 Communication Setup 125
3.2.2.1 Device Group 126
3.2.2.2 Impero Net Number 127
3.2.3 Security Setup 128
3.2.3.1 Grant all Guests Default Access Privileges 128
3.2.3.2 Grant Each Guest Individual Access Privileges Using Impero Authentication 129
3.2.3.3 Grant Each Guest Individual Access Privileges Using Windows Security Management ....
3.3 Use Impero Gateway 132
4 Impero Name Management 134
4.1 Impero Name Management Functionality 134
4.2 Impero Name Server Setup 135
4.3 Use Impero Name Server 136
5 Advanced Tools 137
5.1 Impero in Terminal Server Environments (TSE) 137
5.1.1 Installation (TSE) 137
5.1.2 Use (TSE) 137
5.1.2.1 Impero Naming (TSE) 138
5.1.2.2 Impero Communication (TSE) 138
5.1.2.2.1 Impero Gateway Setup (TSE) 138
5.1.2.2.2 Connect out of a TSE 138
5.1.2.2.3 Connect into a TSE 139
5.1.2.2.4 Connect between TSEs 139
5.1.2.3 Impero Module Functionality (TSE) 140
5.1.2.4 Computer Resources Considerations (TSE) 140
5.2 Impero Guest ActiveX Component 140
5.2.1 Requirements (ActiveX) 140
5.2.2 How to Use the Impero Guest ActiveX Component 141
5.2.3 NGuestX Connect Dialog Box 141
5.2.4 NGuestX Connection Properties Dialog Box 142
5.2.4.1 Remote Desktop Tab 142
5.2.4.2 Keyboard Tab 143
5.2.4.3 Mouse Tab 143
5.2.4.4 Compression Tab 144
5.2.4.5 Encryption Tab 144

5.2.4.6 Display Tab 144
5.2.4.7 Host Protection Tab 145
5.2.4.8 About Tab 145
5.2.5 Connection Status Dialog Box 145
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**.

Locally managed Guest Access Security and how Hosts use Impero Security Management is explained in the **User's Guide**.

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.
3. Impero Security Server manages Guest authentication and query the Security Database for security data.
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

Impero Security Server
Security Database
Role

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.
- Logging including Security Log, Impero Log and Active Sessions.
- Scheduling including Scheduled Jobs.
- Impero Definitions including Impero Guest IDs, Impero Guest ID Groups, Impero Host IDs, Impero Host ID Groups and Impero Properties.
- Windows Definitions including Windows Users, Windows Groups, Windows Workstations, Windows Workstation Groups and Windows Domains.
- RSA SecurID Definitions including RSA SecurID Users, RSA SecurID Groups and RSA SecurID Properties.
- Directory Services Definitions including Directory Services Users, Directory Services Groups and Directory Services.

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

After Security Database Setup and Impero Security Server Setup, Impero Security Management can run unattended with very limited maintenance demands.

Read the Use Impero Security Management section for guidelines.

See also

Security Database Setup
Impero Security Server Setup
Impero Security Management

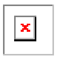
2.2 Load Impero Security Manager

You can install Impero Security Manager from www.Impero.com.

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:



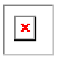
The pane displays a tip to Impero Security Manager.

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:



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.

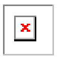
Password []: Specify in this field the matching password. The local test database requires no password.

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:

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:

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:

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:

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.

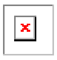
See also

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

Windows Definitions
Impero credentials
Impero Definitions
RSA SecurID credentials
RSA SecurID Definitions
Directory Services credentials
Directory Services Definitions
Windows User
Windows Workstation
Impero Host ID

2.3 Impero Security Manager Window

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



It contains these elements:

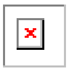
- Title Bar
- Menu Bar
- Toolbar
- Filter and Fetching Bar
- Records panel with a left Selection Pane and a right Records Pane
- Message Panel
- Status Bar

See also

Security Database

2.3.1 Title Bar

This is the Impero Security Manager Window title bar:



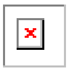
It displays the name of the logged on to data source.

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

- Options Menu
- Help Menu

See also

Impero Security Manager window

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

Impero Security Manager window
Message Panel

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.

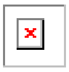
Status Bar: Select this command to check mark/uncheck it to show/hide the Status Bar.

See also

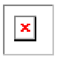
Impero Security Manager window
Toolbar
Selection Pane
Security Settings
Logging
Scheduling
Impero Definitions
Windows Definitions
RSA SecurID Definitions
Directory Services Definitions
Message Panel
Status Bar

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).

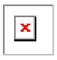
Note: Refresh discards the Records Pane contents and fetch Security Database records. Refresh manually by clicking the **Filter** and **Fetching Bar Refresh** button or pressing F5.

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:

Encrypted bind	Non-Encrypted bind
`username@domain`	`domain\username`
`domain\username`	`cn=username, ou=container,dc=domain`

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

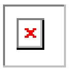
With Non-Encrypted bind, domain must be NetBIOS name when not using the Distinguished Name

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:

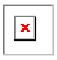


Online Help*:* Select this command or press F1 to open the **Impero Security Manager Help** system on the topic of the currently or most recently shown Records Pane.

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.

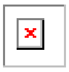
See also

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

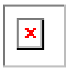
2.3.3 Toolbar

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:

Button	Description
New Role Assignment (F2)	Click this button, press F2 or select the **Role Assignment** menu **New** command to show the **Role Assignment Wizard**.
New Impero Guest ID (F3)	Click this button, press F3 or select the **Impero Guest ID** menu **New** command to show the **Impero Guest ID** window.
New Impero Guest ID Group (F4)	Click this button, press F4 or select the **Impero Guest ID Group** menu **New** command to show the **Impero Group** window.
New	Click this button, press F6 or select the **Impero Host ID** menu **New** command to show the **Impero Host ID** window.

Impero Host ID (F6)	
☒ *New Impero Host ID Group (F7)*	Click this button, press F7 or select the **Impero Host ID Group** menu **New** command to show the **Impero Group** window.
☒ *New Role (F9)*	Click this button, press F9 or select the **Role** menu **New** command to show the **Impero Security Role** window.
☒ *New Scheduled Job (F10)*	Click this button, press F10 or select the **Scheduled Jobs** menu **New** command to show the **Scheduled Job Wizard**.
☒ *Edit Selected (Ctrl +E)*	Select a Records Pane record and click this button, press CTRL+E or select the **Record Type** menu **Edit** command to show the record editing window.
☒ *Delete Selected (Ctrl +D)*	Select a Records Pane record and click this button, press CTRL+D or select the **Record Type** menu **Delete** command to show a confirmation window to confirm deleting the record.
☒ *Large Icons*	Click this button to make it appear pressed in to show **Records Pane** records as horizontal rows of large icons.
☒ *Small Icons*	Click this button to make it appear pressed in to show **Records Pane** records as horizontal rows of small icons.
☒ *List*	Click this button to make it appear pressed in to show **Records Pane** records as vertical columns of small icons.
☒ *Details*	Click this button to make it appear pressed in to show **Records Pane** records in a table with details in columns (default selection).

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.

Button	Description
Refresh	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**.
One More Lot	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**.
All Remaining	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**.

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**.

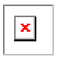
The contents of the individual records panes are explained in the Manage Security Database Contents section in the **Records** menu order.

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.

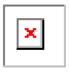
In the message panel, select text or in the message panel context menu select **Select All** to select the entire message panel contents and in the Edit menu or context menu select **Copy** or press CTRL +C to copy selected text to the clipboard.

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 a 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

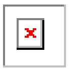
2.4.1.3 View and Manage Data

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
Role
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.

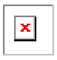
The right pane displays the records of selected **Windows Groups** and **Windows Domains** in a table with these column contents:

- **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:



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.

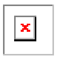
See also

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.

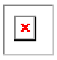
Caution! If no Role Assignment records exist, the Unassigned Hosts' Role applies to all existing Guest and Host selections.

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:

Column	Description
RoleName	Role icon and name.
Rctl	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Connect (View).
Keyb	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Use keyboard and mouse.
Lckm	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Lock keyboard and mouse.
Blnk	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Blank the screen.
Clip	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Transfer clipboard.
Boot	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Execute command.
Chat	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request chat.
Audi	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request audio-video chat.
Vide	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Request video.
Send	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send files to Host.
Recv	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Receive files from Host.
RunP	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Run programs.
Prnt	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Redirect print.
Mana	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Remote management.
Inve	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Retrieve inventory.
Smsg	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Send message.

Mjoi	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Join multi Guest session.
Madm	Allow (check mark)/Do not allow (red X)/Deny (red dot white X) Act as multi Guest session administrator.
Demo	Allow (check mark)/Do not allow (red X/Deny (red dot white X) Demonstrate
Tunn	Allow (check mark)/Do not allow (red X/Deny (red dot white X) Tunnel
AllowedPorts	(list of allowed ports to be used through tunnel) Allowed Tunnel ports
BlockedPorts	(list of blocked ports that cannot be used through tunnel) Blocked Tunnel ports
Conf	Confirm access: No (red X), Yes (check mark) or Yes, with exception (check mark).
Computer locked	Exception applies (check mark)/Exception does not apply (red X).
No user logged on	Exception applies (check mark)/Exception does not apply (red X).
Guest user logged on	Exception applies (check mark)/Exception does not apply (red X).
Description	Fixed role, Role can be modified, but not deleted or <User specified>.
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.
ID	Record number (records are numbered starting from 1).

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:

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

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
View Menu
Details
Security Database Setup
Records Menu

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:

It specifies a Role record.

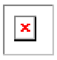
Name: []: This field contains the Role name.

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 aree 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:



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

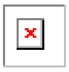
NOTE: To adopt Security Policy changes, Impero Security Servers must log off from and on to the Security Database.

See also

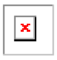
Selection Pane
Security Settings
Records Pane
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Security Policies
Details
Impero Security Server Setup
Security Database Setup

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:



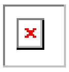
From this window you can copy the Public Key to make it available to Hosts. If the Public Key is changed, you must restart Security Servers, reconfigure and restart Hosts.

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:

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:

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

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.
- **Running***:* Security server status: Question mark: Unknown, Check mark: Logged on to the security database, Red dot with white X: Not logged on to the security database.
- **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 Gusts, 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.

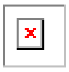
Specify in the field the directory services attribute type name of the certificate field contents only if different from a user object distinguished name type.

See also

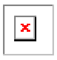
Security Policies
Toolbar
Security Database Wizard
Role Assignment
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
Security Database Setup

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:

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

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).

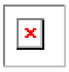
See also

Security Policies
Toolbar
Active Sessions
Scheduled Jobs

2.4.3 Logging

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

- or from the Selection Pane Logging branch:



that include these commands:

- Security Log
- **Impero Log**
- **Active Sessions**

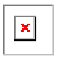
NOTE: By default, the Selection Pane displays the **Logging** branch. You can hide and show it from the **View** menu **Logging** command.

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:

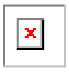


NOTE: By default, the Selection Pane below the Impero Security Management root element is displayed **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches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

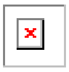
It displays the security database actions as named icons or table records. The *Details* selection displays the table records with these column contents:

- **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

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

2.4.3.2 Impero Log

Select the Selection Pane **Logging** branch **Impero Log** 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 records of Impero events on Impero modules that log on a 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:

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

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

Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Security Database Setup
Security Server group
Details
Records Menu
Logging Options

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.

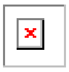
See also

Selection Pane
Logging
Records Pane
Security Settings
Scheduling
Windows Definitions

Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Impero Log
Security Database Setup
Security Server group
Details
Records Menu
Filter and Fetching Bar
Logging Options

2.4.4 Scheduling

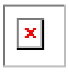
You can manage **Scheduling** records from the **Records** menu **Scheduling** submenu:



that contains this command:

- **Jobs**

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



which includes this matching command:

- **Scheduled Jobs**

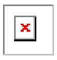
Note: By default, the Selection Pane displays the **Scheduling** branch. You can hide and show it from the **View** menu **Logging** command.

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:

Column	Description
Description	**Scheduled Job** icon and optionally a description.

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:

It contains these commands:

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

See also

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

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 displays 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:

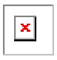
Windows group: Create a Windows Group Scheduled Job (default selection).

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**:

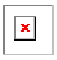


It specifies a Scheduled Job group selection.

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:



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

Select one of these options:

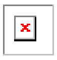
Once on*:* Specify one date and time interval (default selection).

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:



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:

Column	Description
ExecuteAt	Scheduled Job icon and time stamp in format `YYYY-MM-DD HH:MM:SS`.
Action	Check mark **7: Enable** or red dot with white X **8: Disable**.
Operand	Group record **GroupName** column value.
Operator	If Windows group, group record **RID** column number. If Impero group, group record **ID** column value.
P1	Group record **GroupName** column name.
P2	If Windows group, group record **Domain** column value.
JobID	Scheduled Job record **ID** column value.
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.

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

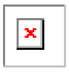
Select Scheduled Job records and select the Scheduled Job menu **Delete** command, click the toolbar **Delete Selected** button or press CTRL+D to show a confirmation window to confirm deleting them.

See also

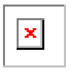
Scheduled Job
Toolbar

2.4.5 Impero Definitions

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



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



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:

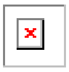
Note: By default, the Selection Pane below the Impero Security Management root element displays **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are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

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

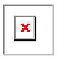
- **New**
- **Edit**
- **Delete**
- **Accessible Hosts**

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 a 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 a 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.

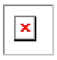
History count []: This disabled field displays the number of used passwords that cannot be reused.

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

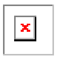
This tab specifies the Impero Guest ID Group records of which this Impero Guest ID record is a member:



This tab specifies the Impero Guest ID Group records of which this Impero Guest ID record is 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

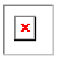
Select a Impero Guest ID record and select the Impero Guest ID menu **Accessible Hosts** command to show the **Who May Connect Whom (Accessible Hosts)** window.

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:

Column	Description
GroupName	**Impero Guest ID Group** icon and name.
Enabled	Check mark (enabled) or red dot with white X (disabled).
Description	Optional **Impero Guest ID Group** description.

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 **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.

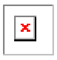
Note: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

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:

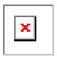


It manages Impero Guest ID Group record Impero Guest ID record members.

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:

Column	Description
HostName	**Impero Host ID** icon and name
Enabled	Check mark (enabled) or red dot with white X (disabled).
ID	Record number (records are numbered starting from 1).
Description	Optional **Impero Host ID** description.
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 **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**

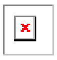
- **Delete**
- **Permitted Guests**

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
Permitted Guests

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:



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.

See also

Impero Host ID
Toolbar
Impero Definitions
Selection Pane
View Menu
Records Pane
Details
Role Assignment

Impero Guest ID window

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:

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 *Impero Host ID Groups* as named icons or table records. The *Details* selection displays the table records with these column contents:

Column	Description
GroupName	**Impero Host ID Group** icon and name
Enabled	Check mark (enabled) or red dot with white X (disabled).

Description	Optional **Impero Host ID Group** description.
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.

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
Impero Group window
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:

Column	Description
Property	Key icon and property description.
Setting	Property value.
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.

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`).

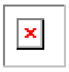
Lock accounts after password failures (0-10, 0=never) []*:* Specify in the field a number in the range for the number of unsuccessful password attempts after which the Impero Guest ID record is disabled (default: `0`).

See also

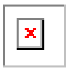
Selection Pane
Impero Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Toolbar
Impero Guest ID

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:

Column	Description
RID	**Windows User** icon and Windows relative identifier number.
UserName	**Windows User** name.
Domain	**Windows User** domain 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 **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

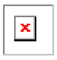
Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Accessible Hosts
Permitted Guests
Role Assignments

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:

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

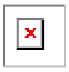
Select the Selection Pane **Windows Definitions** branch **Groups** command to show this Records Pane:

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.

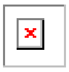
It displays **Windows Groups** as named icons or table records. The **Details** selection displays the table records with these column contents:

Column	Description
RID	**Windows Group** icon and Windows relative identifier number.
GroupName	**Windows Group** name.
Domain	**Windows Group** domain 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 **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:

Column	Description
ComputerName	**Windows Workstation** icon and Windows computer name.
Domain	**Windows Workstation** domain 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 **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

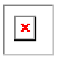
Selection Pane
Windows Definitions
Records Pane
Security Settings
Logging
Scheduling
Impero Definitions
RSA SecurID Definitions
Directory Services Definitions
View Menu
Details
Records Menu
Records Pane
Permitted Guests
Role Assignment

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:



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.

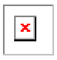
Insert All*:* Click on this button to create Windows Workstation records of all computers in the domain selected in the **Domain** drop-down box.

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

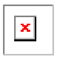
Select a Windows Workstation record and select the **Windows Workstation** menu **Permitted Guests** command to show the **Who May Connect Whom (Permitted Guests)** window.

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:

Column	**Description**
GroupName	**Windows Workstation Group** icon and Windows computer name.
Domain	**Windows Workstation Group** domain 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 **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

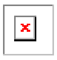
Details
Records Menu
Members
Role Assignments
Windows Workstation

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 Grouprecord.

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.

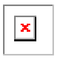
Note: A Windows Workstation Group record initially have no Windows Workstation record members. You can add members from the Members command.

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.

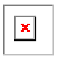
Note: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

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:

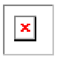


It manages Windows Workstation Group record Windows Workstation record members.

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:

Column	Description
DomainName	**Windows Domain** 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 **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

View Menu
Details
Records Menu
Role Assignments

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.

See also

Windows Domain
Toolbar
Windows Workstation
Role Assignments

2.4.7 RSA SecurID Definitions

You can manage **RSA SecurID Definitions** records from the **Records** menu **RSA SecurID Definitions** submenu:

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

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.

See also

Records Menu
Selection Pane
RSA SecurID Definitions
RSA SecurID Users
RSA SecurID Groups
RSA SecurID Properties
View Menu

2.4.7.1 RSA SecurID User

Select the Selection Pane *RSA SecurID Definitions* branch *RSA SecurID Users* 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 **RSA SecurID Users** as named icons or table records. The *Details* selection displays the table records with these column contents:

Column	Description
UserName	**RSA SecurID User** 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 **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

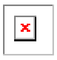
Select an RSA SecurID User record and select this command to show the **Who May Connect Whom (Accessible Hosts)** window.

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.

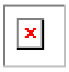
It displays **RSA SecurID Groups** as named icons or table records. The **Details** selection displays the table records with these column contents:

Column	Description
GroupName	**RSA SecurID Group** icon and name.
Enabled	Check mark (enabled) or red dot with white X (disabled).

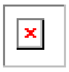
ID	Record number (records are numbered starting from 1).
Created	Creation time stamp in format `YYYY-MM-DD HH:MM:SS`.
CreatedBy	Creator Windows user name.
Modified	Modification time stamp in format `YYYY-MM-DD HH:MM:SS`.
ModifiedBy	Modifier Windows user name.

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**

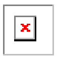
Note: Initially, an RSA SecurID Group record has no RSA SecurID User record members. Add members from the Members command.

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 I

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.

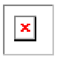
Note: Group member records are not deleted. Role Assignments that use a deleted Guest or Host selection record are deleted.

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:

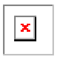


It manages RSA SecurID Group record RSA SecurID User record members.

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.

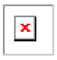
Remove*:* Select in the pane RSA SecurID User records and click this button to remove them as members of the RSA SecurID Group record.

See also

RSA SecurID Group
RSA SecurID User

2.4.7.3 RSA SecurID Properties

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

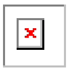


Note: By default, the Selection Pane is below the Impero Security Management root element show **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and D**irectory Services Definitions** branches are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

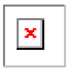
It displays one **RSA SecurID Property** as a named icon or a table record. The **Details** selection displays one table record with these column contents:

- **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.

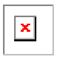
Manage the **RSA SecurID Property** record from the **Records** menu **RSA SecurID Properties** submenu:



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 a 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

View Menu
Details
Records Menu
RSA SecurID User
Impero Guest ID
UserName
Password

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:

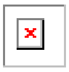
Note: By default, the Selection Pane is below the Impero Security Management root element show **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are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

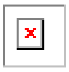
Column	Description
DN	**Directory Services User** icon and distinguished name.

Service	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**

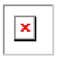
Note: To create Role Assignments with Directory Services Users, records do not need to exist in the Directory Services Users Records Pane if the relevant directory service is specified in the Directory Service Records Pane and is available.

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).

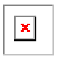
Note: Impero Security Management does not use a Role Assignment record that uses a disabled Guest or Host selection record.

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:

Column	Description
DN	**Directory Services Group** icon and distinguished name.
Service	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 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

Scheduling
Windows Definitions
Impero Definitions
RSA SecurID Definitions
View Menu
Details
Directory Service
Records Menu
Role Assignment
Directory Services Group

2.4.8.2.1 New

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

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:

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:

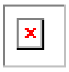
Note: By default, the Selection Pane is below the Impero Security Management root element show **Security Settings**, **Logging**, **Scheduling** and **Windows Definitions** branches in this order. **Impero Definitions**, **RSA SecurID Definitions** and **Directory Services Definitions** branches are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

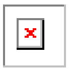
Column	Description
ID	Record number (records are numbered starting from 1).
ServiceName	**Directory Service** name.
DnsName	Directory Server DNS name or IP address.
Enabled	Check mark (enabled) or red dot with white X (disabled).
Port	TCP/IP port number.
SSL	Check mark (use secure connection) or red X (do not use secure connection).
BaseDN	Base distinguished name.
UserDN	Searching user distinguished name.
Password	Searching user password shown as asterisks.
UserSearchFilter	User search filter.
UserAttribFilter	User attribute filter.
UserBrowseFilter	User browse filter.
GroupSearchFilter	Group search filter.
GroupAttribFilter	Group attribute filter.
GroupBrowseFilter	Group browse filter.
OuSearchFilter	Organizational unit search filter.
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 Service** records from the **Records** menu **Directory Service** submenu:



or from the matching **Directory Service** Records Pane context menu:



It contains these commands:

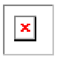
- **New**
- **Edit**
- **Delete**

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.

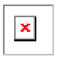
TCP/IP port number []: Specify in this field `389` for a standard LDAP connection or `686` for a secure LDAP connection (default: `389`).

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:

Encrypted bind	Non-Encrypted bind
`username@domain`	`domain\username`
`domain\username`	`cn=username, ou=container,dc=domain`

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

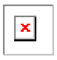
User DN []: Specify in this field the distinguished name by which Impero Security Management shall search for user and group information.

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.

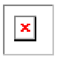
Test*:* Click on this button to test Directory Service logon to show a test result message.

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.

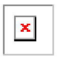
Group search filter []: Specify in this field the group object class.

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.

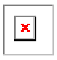
RADIUS is a client/server protocol that is often used to centrally validate remote users and authorize their access to existing network resources integrating well with existing technologies including VPN, RAS, Active Directory and Token based authentication solutions.

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:



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.

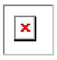
Finish*:* Click on this button to end the **Directory Service** wizard to create the Directory Service record.

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:



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

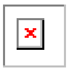
2.4.8.4 Organizational Units

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:

Column	Description
DN	The DN (Distinguished Name) is the name that uniquely identifies an entry in the directory.
Service	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.

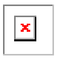
Manage **Organizational Units** records from the **Records** menu:



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

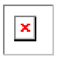
1. Select the record you want to edit in the Organizational Units pane.
2. On the **Records** menu, point to **Directory Services Definitions**, then **Organizational Units** and click **Edit**.

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.

Column headings

Row	Column headings
A	Guest Name
B	Guest Password
C	Guest RID
D	Guest Domain
E	Guest Description
F	Guest Group Name
G	Guest Group RID
H	Guest Group Domain
I	Guest Group Description
J	Guest Type
K	Host Name
L	Host RID
M	Host Domain

Row	Column headings
N	Host Description
O	Host Group Name
P	Host Group RID
Q	Host Group Domain
R	Host Group Description
S	Host Type
T	Role

The following sections describe which columns are used for each authentication method.

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**:

	A	B	E	J
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Type**
Value	<Impero Guest name>	<Impero Guest password>	<Impero Guest description>	Impero Guest
Example	guest07	SecretPassword01	Guest07 description	Impero Guest

For **Impero Guest Group**:

	F	I	J
Required column	**Guest Group Name**	**Guest Group Description**	**Guest Type**
Value	<Impero Guest group name>	<Impero Guest Group	Impero Guest Group
Example	group17	Group17 description	Impero Guest Group

For **Impero Host**:

	K	N	S
Required column	**Host Name**	**Host Description**	**Host Type**
Value	<Impero Host name>	<Impero Host description>	Impero Host
Example	us-acc-03	Katie's laptop in US Account Dept	Impero Host

For **Impero Host Group**:

	O	R	S
Required column	**Host Group Name**	**Host Group Description**	**Host Type**
Value	<Impero Host group name>	<Impero Host group description>	Impero Host Group
Example	US Accounts	US Account Department	Impero Host Group

Impero Guest and Group (inserts Impero Guest, Impero Guest Group and create the Group membership):

	A	B	E	F	I	J
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Group Name**	**Guest Group Description**	**Guest Type**
Value	<Impero Guest name>	<Impero Guest password>	<Impero Guest description>	<Impero Guest group name>	<Impero Guest group description>	Impero Guest
Example	guest07	SecretPassword01	Guest07 description	group17	Group17 description	Impero Guest

Impero Role Assignment (inserts Impero Guest, Guest Group, Impero Host, Host Group and create Role Assignments):

	A	B	E	J	K	N	S	T
Required column	**Guest Name**	**Guest Password**	**Guest Description**	**Guest Type**	**Host Name**	**Host Description**	**Host Type**	**Role**
Value: Guest	<Impero Guest name>	<Impero Guest password>	<Impero Guest description>	Impero Guest	<Impero Host name>	<Impero Host description>	Impero Host	role (2=full control)
Value: Guest Group	<Impero Guest group name>		<Impero Guest group description>	Impero Guest Group	<Impero Host group name>	<Impero Host group description>	Impero Host Group	role (2=full control)
Example: Guest	guest07	SecretPassword01	Guest07 description	Impero Guest	us-acc-03	Katie's laptop in US Account Dept	Impero Host	2
Example: Guest group	group17		Group17 description	Impero Guest Group	US Accounts	US Account Department	Impero Host Group	2

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.

2.4.9.2 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.

	A	D	J
Required column	**Guest Name**	**Guest Domain**	**Guest Type**
Value: user	<Directory Services User DN>	<Directory Services ID>	LDAP User
Value: group	<Directory Services Group DN>	<Directory Services ID>	LDAP Group
Value: OU	<Directory Services Organisational Unit DN>	<Directory Services ID>	LDAP OU

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:

	A	C	D	J
Required column	**Guest Name**	**Guest RID**	**Guest Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows User
Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows User

- OR -

For Windows user, Host:

	K	L	M	J
Required column	**Host Name**	**Host RID**	**Host Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows User

	K	L	M	J
Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows User

For Windows group, Guest:

	A	C	D	J
Required column	**Guest Name**	**Guest RID**	**Guest Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows Group
Example	josm	S-1-5-21-2118863332-1524444778-903097961-7496	mydomain	Windows Group

- OR -

For Windows group, Host:

	K	L	M	J
Required column	**Host Name**	**Host RID**	**Host Domain**	**Guest Type**
Value	<Windows user name>	<ObjectSID from AD>	<AD domain>	Windows Group
Example	development	S-1-5-21-2118863332-1524444778-903097961-16347	mydomain	Windows Group

For Windows workstation (can participate only as Host):

	K	M	S
Required column	Host Name	Host Domain	Host Type
Value	<Workstation name>	<AD domain>	Windows Workstation

	K	M	S
Example	TX-DALLAS-JOSM	mydomain	Windows Workstation

For Windows workstation groups (can participate only as Host):

	K	M	S
Required column	Host Name	Host Domain	Host Type
Value	<Workstation name>	<AD domain>	Windows Workstation Group
Example	TX-DALLAS-JOSM	mydomain	Windows Workstation Group

For Windows domain (can participate only as Host):

	K	M	S
Required column	Host Name	Host Domain	Host Type
Value	<Workstation name>	<AD domain>	Windows Domain
Example	TX-DALLAS-JOSM	mydomain	Windows Domain

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):

	A	J
Required column	Guest Name	Guest Type
Value	<RSA user name>	RSA User

	A	J
Example	RSA user 7	RSA User

RSA group (can participate only as Guest):

	A	J
Required column	**Guest Group Name**	**Guest Type**
Value	<RSA group name>	RSA Group
Example	RSA group 3	RSA Group

RSA User, RSA Group (can participate only as Guest):

	A	F	J
Required column	**Guest Name**	**Guest Group Name**	**Guest Type**
Value	<RSA user name>	<RSA group name>	RSA User
Example	RSA user 7	RSA group 3	RSA User

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

- DWLDAPPROP: Directory Service Properties
- DWLDAPSERV: Directory Service
- DWLDAPUSR: Directory Service User
- DWMAIN: Role Assignment
- DWNTGR: Windows Group
- DWNTUS: Windows User
- DWPOLI: Security Policies
- DWPKI: Public/Private Keys
- DWPROP: Impero Properties
- DWROLE: Roles
- DWRSAGRP: RSA SecurID Group
- DWRSAPROP: RSA SecurID Properties
- DWRSAUSR: RSA SecurID User
- DWRSGM: RSA SecurID Group Members
- DWSERV: Impero Security Servers
- DWTODO: Scheduled Job Actions
- DWUSER: Impero Guest IDs
- DWUSGR: Impero Guest ID Group Members
- DWWKGM: Members of Workstation Groups
- DWWKSG: Workstation Groups
- DWWKST: Workstations

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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Description	Char (64)	Optional description
Category	Integer	Group type number

GroupID	Integer	Record number in group table
Domain	Char (254)	Domain name (if applicable)
StartTime	Char (20)	Start time stamp in format `YYYY-MM-DD HH:MM:SS`
EndTime	Char(20)	End time stamp in format `YYYY-MM-DD HH:MM:SS`
Flags	Integer	Weekly settings number
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
Scheduled Job

2.5.2 DWCONN: Active Sessions

Security Database Tables store Active Sessions data in this table that has this key structure:

Key	Format	Explanation
Guest	Char (254)	Log record arguments
Host	Char (254)	Logging Impero module name
SessionType	Integer	Session type number
Started	Char (20)	Start time stamp in format `YYYY-MM-DD HH:MM:SS`

See also

Security Database Tables
Active Sessions

2.5.3 DWDOMN: Windows Domain

Security Database Tables store Windows Domain data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DomainName	Char (254)	Domain name
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
Windows Domain

2.5.4 DWDONE: Security Log

Security Database Tables store Security Log data in this table that has this key structure:

Key	Format	Explanation
Created	Char (20)	Creation time stamp in format `YYYY-MM-DD HH:MM:SS`
CreatedBy	Char (64)	Creator computer or Windows user name
Status	Integer	Action result number (0 = OK, 1=Error)
Action	Integer	Action type number
Operand	Integer	Action executed on number
Operator	Integer	Action executed by number
P1	Char (254)	Parameter 1 (additional action specification)
ID	Integer	Record number (PRIMARY KEY)

See also

Security Database Tables
Security Log

2.5.5 DWEVNT: Impero Log

Security Database Tables store Impero Log data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Created	Char (20)	Creation time stamp in format `YYYY-MM-DD HH:MM:SS`
EventType	Char (10)	Log record event code
SerialNo	Integer	Log record event number of each logging Impero module
DtlError	Integer	DTL error number (0 = no error)
ProtocolError	Integer	Protocol error number (0 = no error)
Host	Char(32)	Logging Impero module name
Description	Char (160)	Log record arguments

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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (32)	Impero Host ID group name (UNIQUE)
Description	Char (64)	Optional description
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)

GroupName	Char (32)	Impero Guest ID group name (UNIQUE)
Description	Char (64)	Optional description
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
Impero Guest ID Group

2.5.8 DWHOGR: Impero Host ID Group Members

Security Database Tables store Impero Host ID Group Impero Host ID member data in this table that has this key structure:

Key	Format	Explanation
HostID	Integer	Impero Host ID table record number (PRIMARY KEY)
GrpId	Integer	Impero Host ID Group table record number (PRIMARY KEY)
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
Impero Host ID Group
Impero Host ID

2.5.9 DWHOST: Impero Host ID

Security Database Tables store Impero Host ID data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
HostName	Char (32)	Impero Host ID name (UNIQUE)
Description	Char (64)	Optional description
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DN	Char (254)	Distinguished name (UNIQUE)
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 Group

2.5.11 DWLDAPPROP: Directory Service Properties

Security Database Tables store Directory Service properties data in this table that has this key structure:

Key	Format	Explanation
Property	Integer	Record number (PRIMARY KEY)
Setting	Char (254)	Parameter value
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 Service

2.5.12 DWLDAPSERV: Directory Service

Security Database Tables store Directory Service data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
ServiceName	Char (32)	Alias name for the service (UNIQUE)
DnsName	Char (254)	Domain Name System
Port	Integer	IP port number for the SSL connection
SSL	Integer	0 = Disabled, 1 = Enabled
BaseDN	Char (254)	Base distinguished name
UserDN	Char (254)	Distinguished name for user object used for searching
Password	Char (16)	Password for user object used for searching
Enabled	Integer	Anonymous bind 0 = Disabled, 1 = Enabled
UserSearchFilter	Char (60)	Filter to limit search for user objects
UserAttribFilter	Char (60)	Attribute that holds the user name
UserBrowseFilter	Char (200)	Filter to limit search for user objects and container objects
GroupSearchFilter	Char (60)	Filter to limit search for group objects
GroupAttribFilter	Char (60)	Attribute that holds the group name
GroupBrowseFilter	Char (200)	Filter to limit search for group objects and container objects
OuSearchFilter	Char (60)	Filter to limit search for container objects
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 Service

2.5.13 DWLDAPUSR: Directory Service User

Security Database Tables store Directory Services User data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
DN	Char (254)	Distinguished name (UNIQUE)

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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
Host	Char (254)	RADIUS host name / IP
SharedSecret	Char (254)	Shared Secret for the RADIUS server
Port	Integer	Port used by the RADIUS server
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

2.5.15 DWMAIN: Role Assignment

Security Database Tables store Role Assignment data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (UNIQUE)
GuestID	Integer	Guest selection table record number (PRIMARY KEY)
GuestType	Integer	Guest selection type number (PRIMARY KEY)
HostID	Integer	Host selection table record number (PRIMARY KEY)
HostType	Integer	Host selection type number (PRIMARY KEY)
RoleID	Integer	Roles table record number in
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
Role Assignment

2.5.16 DWNTGR: Windows Group

Security Database Tables store Windows Group data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RID	Integer	Domain RID number (UNIQUE)
GroupName	Char (254)	Windows group name
Domain	Char (254)	Domain name (UNIQUE)
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
Windows Group

2.5.17 DWNTUS: Windows User

Security Database Tables store Windows User data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RID	Integer	Domain RID number (UNIQUE)
UserName	Char (254)	Windows user name
Domain	Char (254)	Domain name (UNIQUE)
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
Windows User

2.5.18 DWPOLI: Security Policies

Security Database Tables store Security Policies data in this table that has this key structure:

Key	Format	Explanation
Parameter	Char (32)	Parameter name (PRIMARY KEY)
Setting	Char (32)	Parameter value
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
PublicKey	MS Access: Memo Oracle: NChar(1000) DB2: Varchar(1000) MSSQL and UNKNOWN: Char(1000)	Public Key
PrivateKey	MS Access: Memo Oracle: NChar(2000) DB2: Varchar(2000) MSSQL and UNKNOWN: Char(2000)	Private key
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
Security Policies

2.5.20 DWPROP: Impero Properties

Security Database Tables store Impero Properties data in this table that has this key structure:

Key	Format	Explanation
Property	Integer	Parameter name (PRIMARY KEY)
Setting	Char (254)	Parameter value
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
Impero Properties

2.5.21 DWROLE: Role

Security Database Tables store Role data in this table that has this key structure:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
RoleName	Char (32)	Role name (UNIQUE)
Rctl	Integer	Connect value: 0 = Do not allow, 1 = Allow, 2 = Deny
Keyb	Integer	Use keyboard and mouse value: 0 = Do not allow, 1 = Allow, 2 = Deny
Blnk	Integer	Blank screen value: 0 = Do not allow, 1 = Allow, 2 = Deny
Lckm	Integer	Lock keyboard value: 0 = Do not allow, 1 = Allow, 2 = Deny
Boot	Integer	Restart Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Clip	Integer	Transfer clipboard value: 0 = Do not allow, 1 = Allow, 2 = Deny
Send	Integer	Send files to Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Recv	Integer	Receive files from Host value: 0 = Do not allow, 1 = Allow, 2 = Deny
Prnt	Integer	Redirect print value: 0 = Do not allow, 1 = Allow, 2 = Deny
Chat	Integer	Request chat value: 0 = Do not allow, 1 = Allow, 2 = Deny
Audi	Integer	Request audio chat value: 0 = Do not allow, 1 = Allow, 2 = Deny
RunP	Integer	Run program value: 0 = Do not allow, 1 = Allow, 2 = Deny
Conf	Integer	Value for confirm: 0 = no, 1 = always, 2 = logged on
Description	Char (64)	Optional description
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
Mana	Integer	Remote management value: 0 = Do not allow, 1 = Allow, 2 = Deny

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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (254)	Group name (UNIQUE)
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
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:

Key	Format	Explanation
Property	Integer	Record number (PRIMARY KEY)
Setting	Char (254)	Parameter value
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
UserName	Char (254)	User name (UNIQUE)
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
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:

Key	Format	Explanation
UserID	Integer	RSA SecurID Users table record number (PRIMARY KEY)
GroupID	Integer	RSA SecurID Groups table record number (PRIMARY KEY)
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
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:

Key	Format	Explanation
ServerName	Char (254)	Server name (PRIMARY KEY)

ServerType	Integer	0 = Security Server only, 1 = Access Server compatible, 999 = Security Server group
ASkey	Char (32)	Access Server key (if applicable)
IsRunning	Integer	0 = not running, 1 = running
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
JobID	Integer	Scheduled Job table record number
ExecuteAt	Char (20)	Execute time stamp in format `YYYY-MM-DD HH:MM:SS`
Action	Integer	Action type number
Operand	Integer	Record number in group table
Operator	Integer	Action executed by number
P1	Char (254)	Parameter 1 (additional action specification)
P2	Char (254)	Parameter 2 (additional action specification)
Created	Char (20)	Creation time stamp in format `YYYY-MM-DD HH:MM:SS`
CreatedBy	Char (64)	Creator Windows user name

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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
UserName	Char (32)	Impero Guest ID name (UNIQUE)
Description	Char (64)	Optional description
Enabled	Integer	0 = Disabled, 1 = Enabled

Password	Char (32)	Checksum of password
PwdUsed	Char (20)	Password last use time stamp in format `YYYY-MM-DD HH:MM:SS`
PwdChanged	Char (20)	Password last change time stamp in format `YYYY-MM-DD HH:MM:SS`
PwdWrong	Integer	Number of wrong passwords entered
PwdNum	Integer	Number of recent passwords that cannot be used
Pwd0	Char (32)	Old password checksum
Pwd1	Char (32)	Old password checksum
Pwd2	Char (32)	Old password checksum
Pwd3	Char (32)	Old password checksum
Pwd4	Char (32)	Old password checksum
Pwd5	Char (32)	Old password checksum
Pwd6	Char (32)	Old password checksum
Pwd7	Char (32)	Old password checksum
Pwd8	Char (32)	Old password checksum
Pwd9	Char (32)	Old password checksum
ForceChange	Integer	0 = password change not required, 1 = password change required
Callback	Char (254)	Fixed callback phone number
CBmode	Integer	Callback mode: 0 = No, 1 = Fixed, 2 = Roving
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
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:

Key	Format	Explanation
UsrID	Integer	Impero Guest ID table record number (PRIMARY KEY)
GrpId	Integer	Impero Guest ID Group table record number (PRIMARY KEY)
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
Impero Guest ID Group

Impero Guest ID

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:

Key	Format	Explanation
WkstID	Integer	Windows Workstation table record number (PRIMARY KEY)
GrpId	Integer	Windows Workstation Group table record number (PRIMARY KEY)
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
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:

Key	Format	Explanation
ID	Integer	Record number (PRIMARY KEY)
GroupName	Char (254)	Windows group name
Domain	Char (254)	Domain name (UNIQUE)
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
Windows Workstation Group

2.5.32 DWWKST: Windows Workstation

Security Database Tables store Windows Workstation data in this table that has this key structure:

Key	Format	Explanation

ID	Integer	Record number (PRIMARY KEY)
ComputerName	Char (254)	Workstation name (UNIQUE)
Domain	Char (254)	Domain name (UNIQUE)
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
Windows Workstation

2.6 Impero Security Server Setup

You can install Impero Security Server from www.Impero.com.

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:

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:

1. Unload all Impero Security Managers and security server group Impero Security Servers.
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:

File Name	Record Syntax
`HOST.TXT`	`<Host ID>,<Comment>,<Host ID Group>`
`GUEST.TXT`	`<Guest ID>,<Comment>,<Guest ID Group>,<Password>,<Administrator Y/N>, <Enabled Y/N>, <ForceChange Y/N>`
`PROFILE.TXT`	`<Guest ID Group>,<Host ID Group>,<Rctl Y/N>,<Keyb Y/N>,<Lckm Y/ N>,<Boot Y/N>,`

	<Blnk Y/N>,<Prnt Y/N>,<Clip Y/N>,<Chat Y/N>,<Audi Y/N>,<Send Y/ N>,<Recv Y/N>, <Conf Y/N/L>,<RunP Y/N>,<Mana Y/N>,<Inve Y/N>,<Smsg Y/N>,<Mjoi Y/N>, <Madm Y/N>

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:

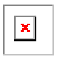
- Incoming and Outgoing
- Outgoing to Incoming
- Networking to Networking
- Typically Disabled: Incoming to Outgoing

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:



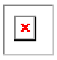
You can edit each Impero Gateway communication profile that uses an outside communication device to support only incoming (outside to inside) communication or only outgoing (inside to outside) communication or in some cases also both at the same time.

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

You can install Impero Gateway from www.Impero.com.

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 `NGWW32.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

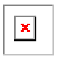
Impero Gateway

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.

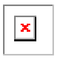
Click the toolbar **Communication Profiles** button or select the **Tools** menu **Communication Profiles** command to show this window:



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

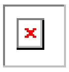
Specify a **Device Group** name to identify a Impero Gateway outside communication profile to enable network Impero modules to connect outgoing through a network Impero Gateway by this communication profile. You can specify any unique name of up to 10 characters, typically the name of the communication 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:



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.

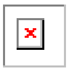
Note: If the Impero net numbers assigned manually or automatically do not satisfy these rules, they must be changed to satisfy the rules.

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.



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 a 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:

It contains these sections:

Allow Guest to

Be routed via the Gateway: This box is checked and disabled signifying that this Security Role property always applies.

Password

Password: []: Specify in this field a password of up to 16 characters to enable password protection (default: none). Characters are displayed as dots or asterisks.

Confirm password: []: Re-specify in this field the password for confirmation.

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 the **User's Guide**.

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.

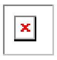
When a Impero module connects through a Impero Gateway on which *Grant all Guests default access privileges* is selected, if a password is specified Impero Gateway requests it. If no password is required or if the connecting Impero module specifies the correct password, Impero Gateway routes the connection.

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.

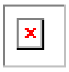
The pane displays the Security Role folders that expand into records of Guest Profiles that have been assigned the Security Role.

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.

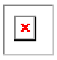
Right-click in the pane to show this context menu:



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.

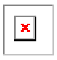
Name of Security Role: []: Specify in this field the Security Role name.

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.

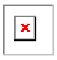
Note: Even a Impero Host or extended Host that requests help through a Impero Gateway must identify itself by a Guest ID.

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.

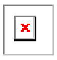
When a Impero module connects through a Impero Gateway that uses **Grant Each Guest Individual Access Privileges Using Impero Authentication**, Impero Gateway requests Impero credentials (**Guest ID** and **Password**). If the returned credentials match the credentials of a Guest Profile, Impero Gateway 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.

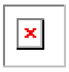
The pane displays the Security Role folders that expand into records of Windows Groups and Users that have been assigned the Security Role.

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

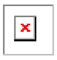
Select this command or click the **Add Security Role** button below to show the **Security Role** window to add a Security Role folder in the pane.

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

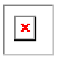
3.3 Use Impero Gateway

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.

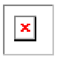
Impero Gateway capacity is limited by the number of enabled outside communication profiles, as each outside communication profile can support only one connection at a time.

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 a 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

You can install Impero Name Server from www.Impero.com.

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)

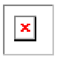
To run the Impero Guest ActiveX component on a computer that uses a Microsoft Windows operating system, these system requirements apply:

- 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.

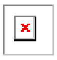
You are now ready to connect to a Host from the **NGuestX Connect** dialog box.

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 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:

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:

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:

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.

Disconnect Guests: Click the **Disconnect 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::_INGuestXCtrlEvents::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::_INGuestXCtrlEvents::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::_INGuestXCtrlEvents::OnDisconnectPre ()

Fired after `OnEndSessionPre()` in response to `EndSession()` if the connection should be terminated because there is no more active session.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnDisconnectPost ()

Fired after `OnDisconnectPre()` method when NGA has been disconnected from Host.

HRESULT NGuestXLib::_INGuestXCtrlEvents::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::_INGuestXCtrlEvents::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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginImpero ([in] LONG Reason, [in] VARIANT_BOOL bNss, [in] INGuestXEventParam * EventParam)

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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLoginRsa ([in] LONG Reason, [in] LONG Shadow, [in] INGuestXEventParam * EventParam)

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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnEnterRsaPincode ([in] LONG Reason, [in] LONG Mode, [in] BSTR SuggestedPin, [in] LONG MinLen, [in] LONG MaxLen, [in] VARIANT_BOOL AllowNonNumeric, [in] INGuestXEventParam * EventParam)

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

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnHostMultiGuestInfo ([in] LONG Event, [in] LONG NumGuests, [in] LONG Error)

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_MultiSessionsDeninied` - 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_MultiSessionsDeninied` 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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatMessageIn ([in] BSTR Msg, [in] INGuestXFont * Font, [in] INGuestXEventParam * EventParam)

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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnChatMessageOut ([in] BSTR Msg, [in] INGuestXFont * Font, [in] INGuestXEventParam * EventParam)

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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnErrorMsg ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

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.

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnInfoMsg ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

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.

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

HRESULT NGuestXLib::_INGuestXCtrlEvents::OnLicenseRequired ([in] LONG MsgNo, [in] BSTR Message, [in] INGuestXEventParam * EventParam)

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

enum INGuestXCtrl::CommProfile_t

Communication profile.

Enumerator:

`CommProfile_TCP` 0 - "LAN (TCP)" profile.

`CommProfile_HTTP` 1 - "HTTP" profile.

`CommProfile_UDP` 2 - "UDP" profile.

`CommProfile_WebConnect` 3 - "WebConnect" profile.

enum INGuestXCtrl::SessionType_t

Session types.

Enumerator:

`SessionType_RemoteControl` 1 - Connect Session.

`SessionType_Chat` 4 - Chat Session.

enum INGuestXCtrl::MouseMode_t

Mouse mode.

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.

enum INGuestXCtrl::KeyboardMode_t

Keyboard mode.

Enumerator:

`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_MultiSessionsDeninied` 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

`InfoWindowReason_Closing` 5 - Closing ActiveX instance

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:

```
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
- no session can be started at this moment
- `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:

```
// 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`
- there is no opened session of specified type
- session can not be finished at this moment
- `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.

HRESULT INGuestXCtrl::SendLoginImpero ([in] BSTR GuestId, [in] BSTR Pwd, [in] BSTR NewPassword, [out, retval] LONG * result)

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.

HRESULT INGuestXCtrl::SendLoginWindows ([in] BSTR UserId, [in] BSTR Domain, [in] BSTR Pwd, [out, retval] LONG * result)

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.

HRESULT INGuestXCtrl::SendLoginLdap ([in] BSTR Server, [in] BSTR User, [in] BSTR Pwd, [out, retval] LONG * result)

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.

HRESULT INGuestXCtrl::SendLoginRsa ([in] BSTR UserId, [in] BSTR Pco, [in] BSTR Pwd, [in] BSTR NewPassword, [out, retval] LONG * result)

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:

- 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::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 scancode 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 compartible 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:

`ShortcutType_AltCtrlDel` 0 - Send ALT + CTRL + DEL to Host

`ShortcutType_CtrlEsc` 1 - Send CTRL + ESC to Host

`ShortcutType_AltTab` 2 - Send ALT + TAB to Host

`ShortcutType_Status` 3 - Connection Status Dialog

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

ID	Message Text	Type	Parameter %1	Parameter %2
2001	Connection %1 is listening	OnInfoMsg	Connection name (com. profile)	
2002	Connection %1 is calling %2	OnInfoMsg	Connection name (com. profile)	Connection address
2003	Connection %1 is opening	OnInfoMsg	Connection name (com. profile)	
2004	Connection %1 could not find %2.	OnInfoMsg	Connection name (com. profile)	Connection address
2005	Connection %1 failed.	OnInfoMsg	Connection name (com. profile)	
2006	Connection %1 connected to %2 ok	OnInfoMsg	Connection name (com. profile)	Connection address
2007	Connection %1: %2	OnInfoMsg	Connection name (com.	Connection address

	now connected		profile)	
2008	Connection %1 connected ok	OnInfoMsg	Connection name (com. profile)	
2009	Connection %1 disconnected	OnInfoMsg	Connection name (com. profile)	
2010	Connection %1 closed ok	OnInfoMsg	Connection name (com. profile)	
2011	Name server %1 found	OnInfoMsg	Name server address	
2012	Name server %1 not found.	OnInfoMsg	Name server address	
2013	Name server(s) activated: %1 %2	OnInfoMsg	Primary Nns	Secondary Nns
2016	Gateway not found.	OnInfoMsg		
2020	Opening %1...	OnInfoMsg	Connection address	
2021	Opened %1 ok	OnInfoMsg	Connection address	
2022	Comm error with %1.	OnInfoMsg	Connection address	
2023	Authenticating on %1...	OnInfoMsg	Connection address	
2024	Authenticated on Impero Host OK	OnInfoMsg		
2025	Waiting for host to confirm access	OnInfoMsg		
2027	Access allowed by host	OnInfoMsg		
2028	Closing %1 ...	OnInfoMsg	Connection address	
2029	Closed %1 ok	OnInfoMsg	Connection address	
2046	Session ended by Host.	OnInfoMsg		
2084	Authenticated on connection server. Waiting %1!d! sec	OnInfoMsg	Seconds left to wait.	

NGuestX Error Messages

ID	Message Text	Type	Parameter %1	Parameter %2
1225	The Host does not allow %1.	OnErrorMsg	Connect/Chat	
2015	Out of memory.	OnErrorMsg		

2017	Host and Guest can't agree on encryption.	OnErrorMsg		
2018	Host does not allow 6.5 compatible. Try another encryption.	OnErrorMsg		
2026	Access denied by host.	OnErrorMsg		
2031	Impero Security Server: Unknown Guest.	OnErrorMsg		
2032	Impero Security Server: Not authorized.	OnErrorMsg		
2033	Impero Security Server: Unknown Host.	OnErrorMsg		
2034	Impero Security Server: Guest ID was disabled.	OnErrorMsg		
2035	Password too long.	OnErrorMsg		
2036	Impero Guest ID too long.	OnErrorMsg		
2037	Username too long.	OnErrorMsg		
2038	Directory Service alias name too long.	OnErrorMsg		
2039	No access. Closed user group.	OnErrorMsg		
2041	Alter authentication method or update host.	OnErrorMsg		
2042	Invalid credentials, please retry.	OnErrorMsg		
2043	Too many invalid credentials entered.	OnErrorMsg		
2045	No response from %1.	OnErrorMsg	Connection address	
2047	Unsupported authentication method.	OnErrorMsg		
2049	Directory Service open error.	OnErrorMsg		
2050	Directory Service group not found.	OnErrorMsg		
2051	Directory Service user not found.	OnErrorMsg		

2052	Logon to Directory Service failed.	OnErrorMsg		
2053	No Distinguished Name could be found for this logon name.	OnErrorMsg		
2054	Directory Service object not found.	OnErrorMsg		
2055	Secure Sockets Layer (SSL) is required by this Directory Service.	OnErrorMsg		
2056	Directory Services: Unsupported authentication method.	OnErrorMsg		
2057	The Directory Service failed to authenticate.	OnErrorMsg		
2058	Directory Services: Insufficient rights.	OnErrorMsg		
2059	Directory Service not found.	OnErrorMsg		
2060	Could not connect to Directory Service.	OnErrorMsg		
2061	Directory Services: Unsupported feature.	OnErrorMsg		
2062	Directory Services error.	OnErrorMsg		
2063	Impero Security Server service not available.	OnErrorMsg		
2064	New password rejected. It was used before, is too short, or needs to include a digit.	OnErrorMsg		
2065	Impero Security Server connect error %1.	OnErrorMsg	Error code	
2066	RSA SecurID server failed to validate credentials.	OnErrorMsg		
2067	RSA SecurID pincode changed ok.	OnErrorMsg		
2068	RSA SecurID next PASSCODE required.	OnErrorMsg		
2069	RSA SecurID Server connect error %1.	OnErrorMsg	Error code	

2070	Connect disallowed.	OnErrorMsg		

OnLoginXXX Reason Values

ID	Default message	Internal ReasonId
12	Impero Security Server: Unknown Guest.	MessageAccessServerGuestNotDefinedOnServer
13	Impero Security Server: Not authorized.	MessageAccessServerGuestNotAllowedToRcHost
15	Impero Security Server: Guest ID was disabled.	MessageAccessServerGuestLocked
23	Invalid credentials, please retry.	MessageInvalidPassword
25	Please enter a new password.	MessageMustChangePassword
31	Directory Service open error.	MessageLdapServiceError
32	Directory Service group not found.	MessageLdapGroupNotFound
33	Directory Service user not found.	MessageLdapUserNotFound
34	Logon to Directory Service failed.	MessageLdapServerLoginFailed
35	No Distinguished Name could be found for this logon name.	MessageLdapLoginNameNotResolved
36	Directory Service object not found.	MessageLdapNoObject
37	Secure Sockets Layer (SSL) is required by this Directory Service.	MessageLdapSslRequired
38	Directory Services: Unsupported authentication method.	MessageLdapUnsupportedAuthenticationMethod
39	The Directory Service failed to authenticate.	MessageLdapAuthenticationError
40	Directory Services: Insufficient rights.	MessageLdapInsufficientRights
41	Directory Service not found.	MessageLdapServerNotFound
42	Could not connect to Directory Service.	MessageLdapServerConnectError
43	Directory Services: Unsupported feature.	MessageLdapUnsupportedFeature
44	Directory Services error.	MessageLdapError
46	New password rejected. It was used before, is too short, or needs to include a digit.	MessageNssNonConformingPassword
48	RSA SecurID server failed to validate credentials.	MessageRsaValidationFailed
49	RSA SecurID pincode changed ok.	MessageRsaPincodeChanged

50	RSA SecurID next PASSCODE required.	MessageRsaNextPasscodeRequired

OnLicenseRequired event messages

ID	Message text	Parameter %1
2402	No appropriate license was found. Without a license only WebConnect connections are allowed. You may enter your license here.	
2409	License validation error: license expiration date was reached.	
2410	License validation error: no necessary feature is available in license.	
2411	License validation error: license server is not running on the specified machine.	
2412	License validation error: invalid license key.	
2413	License validation error: all licensing tokens are already in use.	
2414	License validation error: %1	Error message from license library (unlocalizable)
2415	License validation error: failed to resolve the server host.	
2421	License validation error: no valid license was found in specified file.	
2422	License validation error: license file was not found.	
2425	License validation error: license server with valid license was not found.	

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:

```
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 NFMSCRPT.OCX you can improve the above script to for example:

```
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()
```

This section contains these topics:

- Creation and Deletion
- Startguest, Initialize and Uninitialize
- Connect and Disconnect
- Transferring Files
- Examples
- Reference

5.3.1 Create and Delete

An 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 **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 NFMScript object Script. 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 ReportLog().

```
Set Script.Visible = False
Rc = Script.ReportSilent()
Rc = Script.ReportStatus()
Rc = Script.ReportLog()
```

The OCX can handle any number of simultaneous 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 StartGuest, Initialize and Uninitialize

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 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:

```
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.

```
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.

```
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 a 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`:

```
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.

```
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:

```
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:

```
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 succeed.

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 responds 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:

```
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.

```
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.

```
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:

```
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:

```
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:

```
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 `WaitUntil`() function holds execution until the date and time are entered into the Microsoft DTPicker controls `StartDate` and `StartTime`. `Call(“*”)` leaves it up to the end user to pick a phonebook file in a `FileDialog`, then `Synchronize`() synchronizes the contents of two directories. If the interface’s checkbox is checked, the program tries to repeat the `Call`() and `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
Done:
Rc = Script.Uninitialize
End Sub
The button labeled Stop will cancel the repeating cycles:
Private Sub StopButton_Click()
  Script.CancelScript
  TryAgain = False
End Sub
```

The button labeled 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 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.

Note: All `NFMscript` methods that return a `Long`, return zero for success (Unless otherwise specified).

Method	Description
`Call (Filename As String) As Long`	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.
`CancelCall () As Long`	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.
`CancelCommand () As Long`	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.
`CancelScript () As Long`	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.
`ClearLog () As Long`	Clears the script object's log window.
`CloneFromHost (RemoteDir As String, LocalDir As String) As Long`	Clones the `RemoteDir` directory to the `LocalDir` directory. A `Call`() must be open to the computer with the `RemoteDir`. • `RemoteDir` - A directory on the remote computer where Impero Host runs. Must end with "`\*.*`". • `LocalDir` - A directory on the local computer where Impero Guest runs. Must end with "`\*.*`".
`CloneToHost (LocalDir As String, RemoteDir As String) As Long`	Clones the `LocalDir` directory to the `RemoteDir` directory. A `Call`() must be open to the computer with the `RemoteDir`. • `RemoteDir` - A directory on the remote computer where Impero Host runs. Must end with "`\*.*`". • `LocalDir` - A directory on the local computer where Impero Guest runs. Must end with "`\*.*`".
`CopyFromHost (RemoteFilter As String, LocalDir As String) As Long`	Clones the files matching `RemoteFilter` to the `LocalDir` directory. A `Call`() must be open to the computer with the `RemoteFilter`. • `RemoteFilter` - A valid file filter on the remote computer where Impero Host runs. An example could be "`C:\DATA\*.XLS`". • `LocalDir` - A directory on the local computer where Impero Guest runs. Must end with "`\*.*`".
`CopyToHost (LocalFilter As String, RemoteDir As String) As Long`	Clones the files matching `LocalFilter` to the `RemoteDir` directory. A `Call`() must be open to the computer with the `RemoteDir`. • `LocalFilter` - A valid file filter on the local computer where Impero Guest runs. An example could be "`C:\DATA\*.XLS`". • `RemoteDir` - A directory on the remote computer where Impero

	Host runs. Must end with "*.*".
DirGetName () As String	Returns the name of the current subdirectory from DirSetFirst/ Next().
DirSetFirst (Directory As String) As Boolean	Initializes the directory search entries, so that the next call to DirGetName() returns the name of the first subdirectory of "Directory" 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. • Directory - A directory on the currently Call()ed remote computer.
DirSetNext () As Boolean	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.
DriveGetName () As String	Returns the name of the current disk drive from DriveSetFirst/ Next().
DriveSetFirst () As Boolean	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.
DriveSetNext () As Boolean	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.
Execute (Command as String) As Long	Execute a script editor command. The format of these commands resemble the NFMscript methods. • Command - The command to execute.
FileGetAccessed () As Date	Returns the last access date for the file selected with FileGetFirst/Next().
FilGetArchive () as Boolean	Returns the archive flag for the file selected with FileGetFirst/ Next().
FileGetCreated () As Date	Returns the create date for the file selected with FileGetFirst/ Next().
FileGetHidden () As Boolean	Returns the hidden flag for the file selected with FileGetFirst/ Next().
FileGetModified () As Date	Returns the modified date for the file selected with FileGetFirst/ Next().
FileGetName () As Date	Returns the name of the file selected with FileGetFirst/Next().
FileGetReadonly () As Boolean	Returns the read only flag for the file selected with FileGetFirst/ Next().

`FileGetSize () As Long`	Returns the size of the file selected with `FileGetFirst/Next()`. If the size is above 2GB, -1 is returned.
`FileGetSystem () As Boolean`	Returns the system flag for the file selected with `FileGetFirst/Next()`.
`FileSetFirst (FileFilter As String) As Boolean`	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. • `FileFilter` - A legal file filter on the remote computer, e.g. "`C:\*.*`".
`FileSetNext () As Boolean`	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`.
`FreeGuest () As Long`	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.
`GetInstallDir () As String`	Returns the Impero install directory on the local computer where the Impero Guest program runs.
`GetPhonebookDir () As String`	Returns the phonebook directory. The `Impero.INI PHONEBOOKPATH` and `DATAPATH` settings are respected.
`GetProgress () As Long`	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.
`Hangup () As Long`	Disconnect the current `Call()`.
`Initialize () As Long`	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.
`PhonebookGetFilename () As String`	Returns the name of the current phonebook file. If there are none, the string returned is "`No Phonebook Entries or Error`".
`PhonebookSetFirst () As Boolean`	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`.
`PhonebookSetNext () As Boolean`	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`().

`PhonebookSetSubfolderFirst (Folder As String) As Boolean`	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`.
`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.

`SetIncludeOnlyExisting (YesNo As Boolean) As Long`	Instructs Impero whether to include only files that already exist with the same name on the target computer in file transfer operations. • `YesNo` - If `True`, only files that already exist with the same name on the target computer are transferred. If `False`, all files are transferred.
`SetIncludeOnlyNewer (YesNo As Boolean, Date As Date) As Long`	Allows you to set a limit to how old files you want to include in file transfer operations. • `YesNo` - If `True`, only files that are newer than `Date` are transferred. If `False`, all files are transferred. • `Date` - Files with a modify date older than this are excluded if `YesNo` is `True`.
`SetIncludeSubDir (YesNo As Boolean) As Long`	Instructs Impero whether to include subdirectories of the directories/file filters given as source in file transfer operations. • `YesNo` - If `True`, subdirectories are included. If `False`, subdirectories are excluded.
`SetOverwriteExisting (YesNo As Boolean) As Long`	Set the action you want when trying to overwrite existing files. • `YesNo` - If `True`, existing files are overwritten without warning. If `False`, existing files cause a prompt in a dialog.
`SetOverwriteHidden (YesNo As Boolean) As Long`	Set the action you want when trying to overwrite hidden files. • `YesNo` - If `True`, hidden files are overwritten without warning. If `False`, hidden files cause a prompt in a dialog.
`SetOverwriteReadonly (YesNo As Boolean) As Long`	Set the action you wish when trying to overwrite read only files. • `YesNo` - If `True`, read only files are overwritten without warning. If `False`, read only files cause a prompt in a dialog.
`SetOverwriteSystem (YesNo As Boolean) As Long`	Set the action you wish when trying to overwrite system files. • `YesNo` - If `True`, system files are overwritten without warning. If `False`, system files cause a prompt in a dialog.
`SetReportLog () As None`	Make the logging of events in the object's log window be the default treeview representation.
`SetReportSilent () As None`	Disable the logging of events in the object's log window.
`SetRetriesOnConnectError (Retries As Long) As Long`	Set the number of times you want the file call method to automatically retry making the connection before returning. • `Retries` - An integer number between 0 and 9 inclusive.
`SetRetriesOnTransferError (Retries As Long) As Long`	Set the number of times you want the file transfer method to automatically retry an operation before returning. • `Retries` - An integer number between 0 and 9 inclusive.
`StartGuest (Minimized As Boolean) As Long`	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.

	• Minimized - If True, the Guest attempts to start up minimized. • Return Codes: o -11 and -12 mean success. o -11: Started OK. o -12: Already started.
Synchronize (LocalDir As String, RemoteDir As String) As Long	Synchronizes two directories. A Call() must be open to the remote computer. • LocalDir - A directory on the local computer where the Impero Guest runs. Must end with "\*.*". • RemoteDir - A directory on the remote computer where the Impero Host runs. Must end with "\*.*".
SynchronizeOneWay (SourceDir As String, TargetDir As String, ToHost As Boolean) As Long	Synchronizes two directories, but moves files one way only. A Call() must be open to the remote computer. • SourceDir - The directory from where the files originate. It can be local or remote depending on ToHost. Must end with "\*.*". • TargetDir - The directory to which the files are moved. It can be local or remote depending on ToHost. Must end with "\*.*". • ToHost - If True, files are moved only from Guest to Host. If False, files are moved only from Host to Guest.
Uninitialize () As Long	Uninitializes a Impero Guest session. After Uninitialize(), Initialize() must be called before calling other methods. Uninitialize is not mandatory, but good practice.
Wait (Period As Date) As Long	Waits a number of hours, minutes and seconds and then returns. • Period - The number of hours, minutes and seconds that you want the method to wait before returning. Use WaitSeconds() to specify the period as seconds. **Note:** If using AM-PM time notation, 12:00:01 AM causes a wait of 1 second, not 12 hours and 1 second.
WaitSeconds (Period As Long) As Long	Waits a number of seconds and then returns. • Period - The number of seconds that you want the method to wait before returning.
WaitUntil (Date As Date, Time As Date) As Long	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. • Date - The date you want the method to wait until before returning. If this variable has a time part, it is ignored. • Time - The time of the above date when the method shall return. If this variable has a date part, it is ignored.
WaitUntilAnyDay (Time As Date) As Long	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.

	- Time - The time of any date when the method returns. If this variable has a date part, it is ignored.
WriteLog (Text As String) As Long	Writes a text in the script object's log window, if it is in the default SetReportLog() status. - Text - A string that shall be appended to the current treeview item in the log.

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:

Item	Value
User ID	Anonymous logon (S-1-5-7) (Windows NT or 2000) or Local Service (S-1-5-19) (Windows XP or later).
Groups	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
Privileges	SeChangeNotifyPrivilege (Traverse folders) and SeShutdownPrivilege (allows reboot or shutdown through Impero).
Default owner	ImperoActivity, in a few cases Anonymous logon (S-1-5-7)
Default group	ImperoActivity
Default ACL	LocalSystem – Full Access, ImperoActivity – Full Access
Network credentials	None

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**.

See also

Normal Operation

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:

```
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]
```

Parameter	Function
/A:	Start an Audio-Video Chat session with the connected Host.
/B:<FileName>	Play back session recording file. Do not combine this switch with other parameters.
/C:<Communication profile>	Connect by <Communication profile> to the Host specified by the switch /H: or /P:.
/CC:<ProfileName>&&<CMURL>&&<Username>&&<Password>&&<Domain>	Create the specified Webconnect profile.
/CD:<ProfileName>	Delete the specified webconnect profile.
/D:	Disconnect from the connected Hosts. Do not combine this parameter with other parameters.
/DT:<SessionId>	Disconnect tunnel session from external program by <SessionId>
/E:<PhoneBookFileName>	Show the Connection Properties of <Phonebook file path and name> or, if combined with a session parameter (/A:, /F:, /G:, /R: or /V:), start this session with the <Phonebook file path and name> Host.
/F:	Start a File Transfer session with the connected to Host.
/G:	Start a Remote Management session with the connected to Host.
/H:<DisplayHostName>	Connect to <DisplayHostName> Host by a communication profile or the one specified by /C:
/I:	Start Get Inventory session.
/J:	Start Demo session.
/LGD:<LoginDomain>	Specify login domain for connecting to a Gateway.
/LGN:<LoginID>	Specify login name when connecting to a Gateway.

/LGP:<LoginPassword>	Specify login password for connecting to a Gateway.
/LGEP:<EncryptedLoginPassword>	Specify encrypted login password for connecting to a Gateway.
/LHD:<LoginDomain>	Specify login domain for connecting to a Host.
/LHN:<LoginID>	Specify login name when connecting to a Host.
/LHP:<LoginPassword>	Specify login password for connecting to a Host.
/LHEP:<EncryptedLoginPassword>	Specify encrypted login password for connecting to a Host.
/M:[<FileName>]	Record Connect session to <FileName>. Only works in conjunction with /P: or /H: Combine this parameter with /R: to record the Connect session. If no <Recording file path and name> is specified, a recording file named <Time stamp>-<Guest ID>-<Host ID>.dwr is saved in the Impero Configuration Files record directory.
/P:<HostPhoneN>	Connect to <HostPhoneNr> Host by a dynamic communication profile or the one specified by /C:
/R:	Start a Connect session with the connected Host.
/S:<FileName>	Run script <FileName>. Do not combine this parameter with other parameters.
/TUN:	Start Tunnel session with hidden tunnel console.
/TUC:	Start Tunnel session.
/V:	Start a Chat session with the connected Host.
/X:<Number of pixels from left screen border>[,<Number of pixels from upper screen border>[,<Number of pixels width>[,<Number of pixels height>]]]	Connect window position and size. Combine this parameter with /R: to specify a non-default position and size of the Connect window.
/YD:<ServiceTicketId>	Delete Help Service/Service ticket <ServiceTicketId>.
/YT:<TicketId>	Add Service ticket <TicketId>.

/YS:<ServiceName>	Add Help Service <ServiceName>.
/ZI:<ExtNotificationInstance>	Set external Instance to receive session events notifications.
/ZH:<SerialComHandle>	Set handle for serial communication.
/ZW:<hWndExtNotification>	Set external HWND to receive session events notifications.
/ZZTOP	Enable the DTL log.

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]
```

Parameter	Function
/C:<communication profile>	Enable <communication profile> in addition to other selected Communication Profiles. The setting is not stored.
/I:<Inventory file path and name>	Generate and retrieve Host computer inventory to store it in <Inventory file path and name>.
/R:<HostName>	Set the Host ID. The setting is stored.

`/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..."), the command is not successful.
`/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..."), the command is not successful.
`/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:

Parameter	**Function**
`/R:R`	Initiates a help request from the Host.
`/R:C`	Cancels the help request from the Host.
`/HD:<HelpCommentBuffer>`	Specifies a help request problem description.

/HP:<HelpProvider>	Specifies a help provider (help service name or service ticket number).
/HC:<SpecificComProfName>	Specifies a help request communication profile.
/HA:<PhoneNumber or TCP/ IP Address>	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** > **Advanced Help Request Options**.
/HW:	Must be included with a help request via WebConnect.
/HS:	In case no help provider is found. the help request fails silent.
/HT:	Enables service tickets. Setting saved to **Program Options > Advanced Help Request Options**.

Cancel a pending help request by this parameter:

Parameter	Function
/HH:	Cancels a pending help request.

Log on to a Guest network connecting Impero Gateway by these parameters:

Parameter	Function
/LGN:<HelpReqLoginID>	Specifies a Gateway login name. The setting is saved to **Program Options** > **Advanced Help Request Options**.
/LGP:<HelpReqLoginPassword>	Specifies a Gateway login password. The setting is saved to **Program Options** > **Advanced Help Request Options**.
/LGD:<HelpReqLoginDomain>>	Specifies a Gateway login domain. The setting is saved to **Program Options** > **Advanced Help Request Options**.
/LGC:	Specifies that help request gateway login uses current credentials for Windows Security authentication The setting is saved to **Program Options > Advanced Help Request Options.**

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 communication profiles.

```
<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:

Permission	Code
View remote screen	2.1.1
Use keyboard and mouse	2.1.2
Lock keyboard and mouse	2.1.3
Blank the screen	2.1.4
Transfer clipboard	2.1.5
Execute command	2.1.6
Request chat	2.1.7
Request audio chat and transfer sound	2.1.8
Request video	2.1.9
Send files to host	2.1.10
Receive files from host	2.1.11
Run programs	2.1.12
Redirect print	2.1.13
Remote Manage	2.1.14
Retrieve inventory	2.1.16
Send message	2.1.17
Demonstrate	2.1.18
Join multi Guest session	2.1.19
Act as multi Guest session Administrator	2.1.20
Select remote monitor	2.1.21

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:

Parameter	Description
Scheme	Identifies the custom protocol to the OS. In this case it is `nrc`. It is mandatory.
host	This is the Impero Host unique identifier. Based on the communication profile this is just a string containing an IP, hostname or unique identifier.
path	The main operation descriptor, or sub-operations encoded in the path hierarchy. It can have the following values: "remote-control", "file-transfer", "remote-management", "chat" and "inventory".
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 diplayed 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 a Impero Portal communication device.

Examples of URI

URI	Description

`nrc:`	Opens the Guest.
`nrc://`	Opens the Guest.
`nrc://MY-COMPUTER/remote-control`	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.
`nrc://192.168.200.30/remote-control/#direct`	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 "`direct`" (that has the Communication Device set to TCP/IP (TCP)).
`nrc://localhost1/file-transfer`	Opens the Guest in a file transfer session with the specified Host using a Impero Portal communication profile on the Guest.
`nrc://hostname/inventory`	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.
`nrc://hostname/remote-control?url=portal.Impero.com`	Opens the Guest in a Connect session with the specified Host using a Impero Portal communication profile with the given URL.

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,

Parent Domain	Child Domain	NetBIOS Name
Domain1.local	Sales.domain1.local	Sales
Domain2.local	Sales.domain2.local	Sales

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 51
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

DWHOST: 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

DWPKI: Public/Private Keys 109

DWPOLI: Security Policies 109

DWPROP: Netop Properties 110

DWROLE: Roles 110

DWRSAGRP: RSA SecurID Group 111

DWRSAPROP: RSA SecurID Properties 111

DWRSAUSR: RSA SecurID User 112

DWRSGM: RSA SecurID Group Members 112

DWSERV: Netop Security Servers 112

DWTODO: Scheduled Actions 113

DWUSER: Netop Guest IDs 113

DWUSGR: 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 column 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 129, 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

J

- Jobs menu 45

K

- Keep Synchronized Script 188
- kerberos 208
- keyboard mode 143
- Keyboard tab
  - ActiveX Guest 143

L

- 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

M

- 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

N

- 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 Group Members 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 72

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 196

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

NETOPLOG.ZIP 121

NetopX Connect window 141

NetopX Connection Properties dialog box 142

NetopX graphical area 141

Network_point-to-point 122

Networking 122

Networking to Networking 123

New 28, 34, 45, 50, 53, 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

non-encrypted bind 17

Normal Operation 197

NSM data source cannot be opened window 12

Number of registered names field 135

O

ODBC Microsoft Access Setup window 11

One More Lot button 20

Options Menu 17

Outgoing to Incoming 123

Outside 122

Outside communication 138

P

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

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 Preferred Host 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