

Peregrine | AssetCenter 4.3

Desktop Administration

© Copyright 2004 Peregrine Systems, Inc.
All Rights Reserved.

Information contained in this document is proprietary to Peregrine Systems, Incorporated, and may be used or disclosed only with written permission from Peregrine Systems, Inc. This manual, or any part thereof, may not be reproduced without the prior written permission of Peregrine Systems, Inc. This document refers to numerous products by their trade names. In most, if not all, cases these designations are claimed as Trademarks or Registered Trademarks by their respective companies.

Peregrine Systems[®] and AssetCenter[®] are trademarks of Peregrine Systems, Inc. or its subsidiaries.

This document and the related software described in this manual are supplied under license or nondisclosure agreement and may be used or copied only in accordance with the terms of the agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Peregrine Systems, Inc. Contact Peregrine Systems, Inc., Customer Support to verify the date of the latest version of this document.

The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental.

If you need technical support for this product, or would like to request documentation for a product for which you are licensed, contact Peregrine Systems, Inc. Customer Support by email at support@peregrine.com.

If you have comments or suggestions about this documentation, contact Peregrine Systems, Inc. Technical Publications by email at doc_comments@peregrine.com.

This edition applies to version 4.3 of the licensed program

AssetCenter

Table of Contents

- I. Foreword 11**
 - Introduction (Desktop Administration) 13**
 - Who is the Desktop Administration module intended for? 14
 - What does the Desktop Administration module do? 15
 - Chapter 1. General principles (Desktop Administration) 17**
 - Main concepts used 17
 - Presentation of the applications 18
 - Architecture of the module 22
 - Automation - Detailed architecture 23
 - Encryption and security 25
 - Chapter 2. Setting up the Desktop Administration module 29**
 - Installation 29
 - Configuration 45
- II. Automation 47**
 - Chapter 3. Creating deployment workflows 49**

Creating a deployment workflow	49
Practical case	52
Chapter 4. Using the deployment server	59
Modifying the references in the AssetCenter database	59
Modifying the private key	60
Configuring the Desktop Administration service	60
Modifying the server configuration tool options	60
Restarting the Desktop Administration service automatically	61
Modifying the parameters of a deployment server	61
Obtaining information about how the Desktop Administration service functions	61
Chapter 5. Examples of deployment workflows	63
IDD scan workflow	63
PDI scan workflow	63
WMI scan workflow	64
Registry scan workflow	65
Change the wallpaper workflow	65
InstallShield silent installation workflow	65
Example of temporary agent workflow	66
Software license management	67
Uninstalling software	67
Chapter 6. Examples of deployment wizards	69
Computer deployment wizard	70
Service deployment wizard	70
Location deployment wizard	71
NT-domain computer import wizard	71
NT-domain user import wizard	71
Chapter 7. Glossary (Desktop Administration)	73
Deployment workflow	73
Workflow schema	74
Deployment instances	74
Deployment server	74
Deployment target	74
Workflow activity	75
Workflow event	75
Workflow transition	75
Agent	75

Depot	76
Broadcast signal	76
Chapter 8. References (Desktop Administration)	77
Deployment activities	77
III. Remote control	91
Chapter 9. Remote Control	93
Rapid installation	93
Remote control by the Manager	103
Chapter 10. Control rights	109
Defining control rights	109
Assigning control rights	119
Chapter 11. Using the Manager	121
Starting the Manager module for the first time	122
The interface of the Manager	131
Accessing remote computers	133
Communication protocol settings	137
Managing the list of remote computers	141
Controlling a computer	165
Editing the properties of remote computers	173
Other functions	174
Communicating	177
Managing news	179
Using the Manager from the command line	179
Chapter 12. Using the graphical interface of the agent	183
Configuring the agent	184
Agent options	189
To send a message	193
MyHelp	194
Reading news	195
Protecting your files	196
Chapter 13. Using the Web surveillance agent	199
Using the Web agent	199

Chapter 14. Integrating the Manager with other applications	205
Integrating the Manager with ServiceCenter	206
Integrating InfraTools Desktop Discovery with the Manager	208
Chapter 15. Glossary (Remote control)	211
Remote Control server	211
Web surveillance agent	211
Certificate	212
MyHelp	212
IV. Transversal functions	215
Chapter 16. Departments and employees	217
Organization of departments and employees	217
AssetCenter users	218
AssetCenter administrators	218
Creating departments and employees	218
Defining an employee's user profile	219
Employee groups	220
Chapter 17. Locations	221
Definition of a location	221
Chapter 18. Features	223
Definition of features	223
Description of the features	224
Parameters of a feature	224
Feature classes	226
Managing features	226

List of Figures

1. Desktop Administration - Structure of the module	14
1.1. Desktop Administration module - Architecture	22
1.2. Presentation of the architecture	24
3.1. Launching the deployment - Detail window	55
3.2. Deployment instance - Execution-control window	56
9.1. Manager window	104
9.2. The evaluation-mode dialog box	105
10.1. Window to create rights over files and folders	115
10.2. Window for the creation of rights for keys and for the values of a remote computer's Registry	117
11.1. Main window of the Manager	132
11.2. Manager options window	133
11.3. Using a client gateway	135
11.4. Using a Manager gateway and a client gateway	135
11.5. Using gateways in Remote Management 4.x	138
11.6. List of remote computers	166
11.7. AssetCenter explorer window	170
11.8. Explorer search window	172
12.1. Agent options window	190
14.1. InfraTools Desktop Discovery integration options	209

List of Tables

- 11.1. List of command lines that can be used with the Manager 180
- 18.1. The different data-input constraints applicable to a feature 226



Foreword

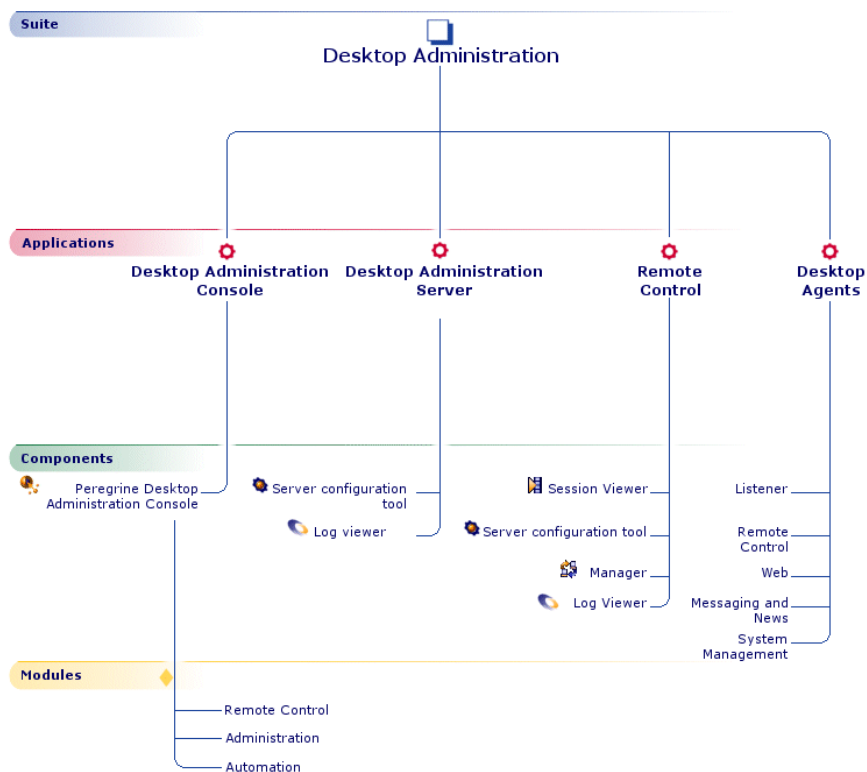
PART

Introduction (Desktop Administration)

PREFACE

The structure of the Desktop Administration module is illustrated in the following diagram.

Figure 1. Desktop Administration - Structure of the module



Who is the Desktop Administration module intended for?

The Desktop Administration module is mainly intended for those in charge of WAN or LAN networked IT-portfolio maintenance and who also want to operate on remote computers.

It is generally implemented by the following persons:

- System administrators
- Network administrators
- IT managers
- IT maintenance technicians



This guide does not explain the technical knowledge related to the domains mentioned above; it is assumed that you are already familiar with it.

What does the Desktop Administration module do?

Desktop Administration is an enterprise-class remote control tool.

The module has two main areas of functionality: Automated administration and remote control.

AssetCenter integrates this functionality via the Remote control and Automation functions. The availability of these functions will depend on the license you have acquired from Peregrine Systems, Inc.

The Desktop Administration function enables you to perform the following tasks:

- Configure remote computers.
- Propagate data to and retrieve data from remote computers.
 - Distribute and deploy software.
 - Verify the implementation of internal security rules on all the computers in your IT portfolio.
 - Prevent the propagation of a virus by stopping the infected computers and servers.
 - And so on.

More generically, this module enables you execute - on a regular or occasional basis - a series of basic tasks on a set of defined computers. The triggering and running of these tasks is determined by a workflow called a deployment workflow.

In a more complex network environment, the Remote Control function enables you to:

- Perform remote administration duties on your servers.
- Resolve problems by taking remote control of an employee's computer.
- Broadcast information rapidly using a message, news, and chat functions.

1 | General principles (Desktop Administration)

CHAPTER

Main concepts used

The Desktop Administration module uses the following notions:

- Deployment workflow [page 73]
- Workflow schema [page 74]
- Deployment instances [page 74]
- Deployment server [page 74]
- Deployment target [page 74]
- Workflow activity [page 75]
- Workflow event [page 75]
- Workflow transition [page 75]
- Agent [page 75]
- Depot [page 76]
- Broadcast signal [page 76]

Presentation of the applications

The Desktop Administration module is comprised of three integrated applications, which can be installed directly from the installation CD-ROM. Each of these applications is made up of several components and/or modules. The following sections give a quick description of each.



The modules available in AssetCenter divide Desktop Administration up into areas of functionality. The availability of these modules depends on the license you have acquired from Peregrine Systems, Inc. If you wish to restrict the functionality available through the graphical interface (for example, to fit the needs of individual users), you may enable or disable the available modules using the **File/ Activate modules** menu item.

The modules are the following:

- **Remote Control:** This module regroups all the functions related to remote control.
 - **Administration:** This module regroups all the functions reserved for advanced users.
 - **Automation:** This module regroups all the functions related to automation (deployment, etc.).
-

Desktop Administration Server

This application contains two components.

Server Configuration Tool

This component enables you to configure the Desktop Administration server. Using this component you can:

- Start and stop the server.
- Declare the connection information to the database.

Log Viewer

The Log Viewer enables you to view the log files produced by different Peregrine Systems, Inc., applications. These files have the **.log** extension.

Remote Control

This application contains four components.

Session viewer

During remote-control sessions between a manager and an agent, the manager can save the remote-control session in the form of an **.rcr** file.

The Log Viewer enables you to read your **.rcr** file(s) and to review the remote-control session.

Manager

The Manager lets its user to take control over a remote computer.

The Manager window is split into three parts. You can view:

- The list of remote computers.
- The screen of the computer you are remotely controlling.
- Messages.

This pane is divided into three tabs that let you view:

- The messages exchanged with the remotely controlled computer.
- The help requests from the remote computer under control (**MyHelp**).
- The status of operations performed on the remote computer. For example: remote control, established connection, launch an explorer, etc.

Whether or not a Manager can take control of a remote computer is conditioned by a certain number of control rights kept in a:

- A certificate saved on the computer where the Manager is located.
- Central database.

The manager can access a distant computer in three different ways:

- Access by network neighborhood

This access method is used for computers that emit broadcast signals indicating their presence. In the Manager window, they appear in the list of remote computers under the **Network Neighborhood** node.

- Access by server

This access uses the information provided by a server. It lets you view the computers and the groups to which they belong. During a remote-control session, the server verifies the identity of the Manager and the specific

control rights the Manager has and authorizes the connection to the remote computer or not.

- Direct access

The direct-access method enables you to create a description of a remote computer and to save its information locally in the Manager's certificate. This is especially useful when an off-site employee cannot access the central server. Such employees could be an off-site maintenance technician needing to take control of a company computer from a personal laptop, for example.

Server Configuration Tool

This component enables you to provide the server with the information necessary for the messaging system and to refresh it. (This information is contained in the database.) Using this console, you can:

- Start and stop the server.
- Select and configure the database.
- Display the computers and groups of connected users.
- Display the number of available news messages.

Log Viewer

The Log Viewer enables you to view the log files produced by different Peregrine Systems, Inc., applications. These files have the **.log** extension.

Desktop Agents

This application contains five components, one of which - the **Listener** - is mandatory. The **Listener** is the principal agent, while the other available agents enable you to expand the capacity of this agent.

 **Important:**

In the corresponding documentation, this application is referred to generically as the **Agent**.

Listener

The Listener is the part of the agent that is installed as a service on the remote computer. This service enables the computer to be controlled by managers at

any given time. In Windows NT, 2000 and XP, a manager can instantly deploy this service on computers using the QuickDeploy! function or a mass deployment workflow.

The Listener service can be used by other Peregrine Systems products in order to:

- Automatically scan remote computers.
- Integrate teledistribution tools.

If you want to use the Listener with other Peregrine products, contract Peregrine Systems, Inc.

System management

This component is necessary to use the automation and remote-control functions.

Remote control

This component enables the remote control of a computer by the Manager and the Desktop Administration server.

Web

Once installed and configured on the remote computer, the **Web** component lets you consult the parameters of the computer from an explorer:

- System information
- Activity
- Process
- Running services
- Application logs, system logs, security logs
- Processor load and memory consumption

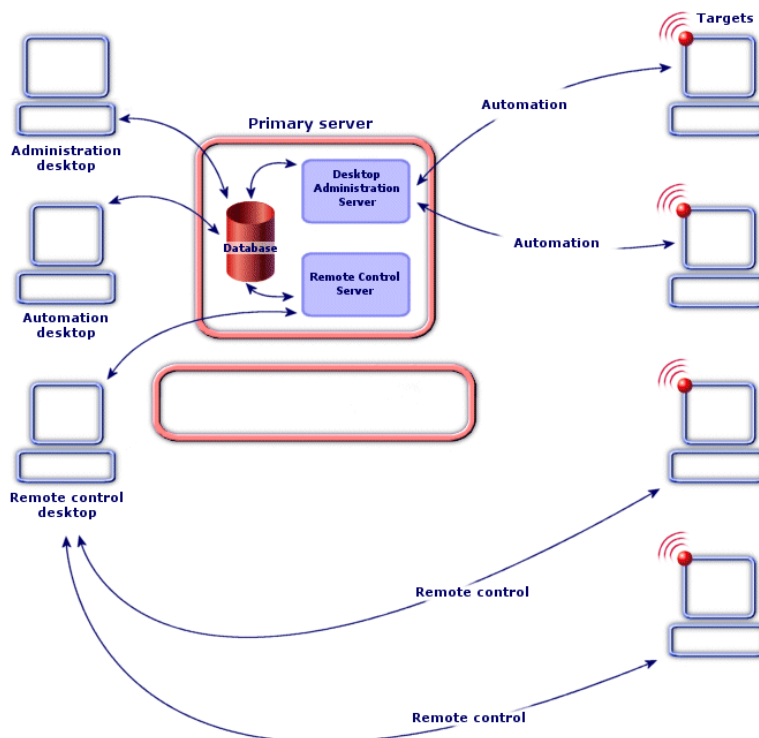
Messaging and News

This component enables you to send and receive messages. You can also receive and consult news if you are set up to receive it.

Architecture of the module

The following diagram outlines the architecture of the module.

Figure 1.1. Desktop Administration module - Architecture



As this diagram shows, there are three main areas to the architecture, which are described later on in this manual:

- The AssetCenter client installed on machines dedicated in whole or in part to the following tasks: Database administration, remote control, automation. It enables you to create deployment workflow schemes, declare the deployment server(s) used and deployment instances. All of these objects are stored in the AssetCenter database.
- The **main server**, where the Desktop Administration server (for automation) and the Remote Control server (for remote control) are installed. The

Desktop Administration server executes the deployment workflow instances on a list of computers stored in the AssetCenter database. It must therefore have access to the AssetCenter database. This access is accomplished via the API layer of AssetCenter.

At the same time, the Remote Control server manages the access rights for remote control (Manager rights) and secures the access to the remote computers, in working with the database.

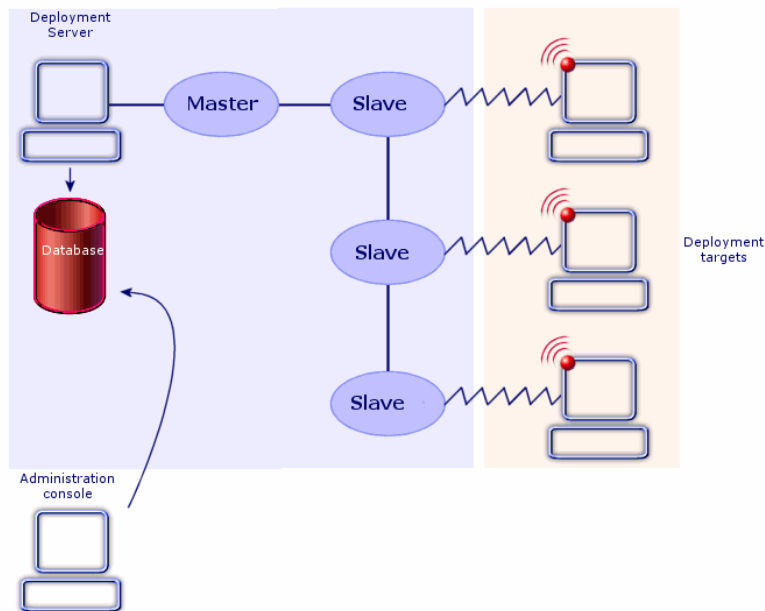
 **Note:**

The architecture presented here is a classic one that regroups the Desktop Administration server and the Remote Control server on the same machine: the main server. You can, however, install each of these servers on a different machine if you wish.

- The deployment targets are computers on which the deployment is carried out. These computers must be declared in the AssetCenter database, in order for the administration console and the deployment server to be able to access them.

Automation - Detailed architecture

The following diagram presents a detailed view of the architecture on which the AssetCenter automation functions are based.

Figure 1.2. Presentation of the architecture

When executing a workflow instance, the server triggers a process that controls the activity in its entirety. This process, called the master process, starts (during the deployment, but not simultaneously) a sub-process, also called a slave process, for each target computer.

You can have multiple deployment servers.

 **Note:**

For server performance reasons, the number of slaves running simultaneously on the server must be limited. This number can be defined by the user of the administration console (at the level of the record in the **Deployment servers** table (amDaServer) that corresponds to the deployment server).

Depending the workflow activities used, a deployment agent can be installed on these computers. Although this is not absolutely necessary, it facilitates the creation, consistency and execution of your deployment workflows.



Note:

Certain functions are available without the remote agent but which require an operating system from the Windows NT family (Windows NT 4.0, Windows 2000 or Windows XP).

For example, when you write a Basic script used in a workflow, the API you use will be different depending on whether you access computers with an agent or not. Consequently, if your IT portfolio contains both computers with an without an agent, you must adopt one of the following solutions.

- Write and maintain two sets for workflows for two lists of target computers,
- Include a test for the agent in your workflows and make them behave accordingly,
- Etc.



Note:

The agent is permanently on stand-by and each computer with an agent can broadcast its presence on the network by sending out an activity signal, also called a broadcast signal.

Encryption and security

Why use security keys?

With the Desktop Administration module, you can:

- Perform tasks remotely on deployment targets
- Retrieve information from the deployment targets.

It is important that such actions be perfectly controlled in order that:

- The modifications performed on the target computers match your expectations.
- The information transmitted over the network stays confidential.

This is why we use security keys.

How do security keys work?

A security key is a text string created using an algorithm that is known only to Peregrine Systems.

The Desktop Administration module uses a double security key for your entire IT portfolio.

- **Public** key: This key is installed on each deployment target using its individual agent.
- **Private** key: This key is installed on each deployment server using the server configuration tool.

The security of the system relies on the extreme difficulty of determining the private key from the public key.

How identification works with automation

Thus, when a Desktop Administration server addresses an order to execute on a target, the modification order is accompanied by the **private** key. This key is confronted by the target's **public** key. If the keys are compatible, the agent will execute the modification order. Otherwise, the order is rejected.

Furthermore, the information transmitted by the targets is encrypted using the **public** key and decrypted using the **private** key.

Security and confidentiality are thus totally assured.

The **public** and **private** security keys are created at the same time - and one time only - using AssetCenter.

How identification works with remote control

The public key is included in the agent's configuration. When the Manager requests to connect to the remote computer, a series of algorithms compare the private key associated with the public key and validate the Manager's connection.

The identification consists of asking the Manager for signature by private key of a phrase selected by the agent when receiving the remote control request. Using this public part, the agent can verify that only the Manager knowing the private part could have provided that signature. The connection is then established for a remote-control session.

The detailed algorithm uses an RSA encoding with 1024-bit keys whose negotiation is done with a simplified Diffie-Helman type algorithm based on a question/response/signature mechanism.

Protecting the confidentiality of the private key

The information guaranteeing the confidentiality and identification during a graphical remote-control session is kept in a file with the private key. This file is generated with the **Generate a double security key** wizard at the same time as the file containing the public key. To assure the confidentiality of the encryption information, we recommend you take the following precautions:

- 1 Place the file with the private key on a media whose access is controlled. For example, you can keep this file on a locked disc or in the directory of a workstation whose access is strictly controlled.
- 2 Generate a certificate of limited validity for your managers. These certificates contain part of the security information in encrypted form and can corrupt the protection of the agents.
- 3 Establish connections between the Remote Control server and the manager that cannot be analyzed. If this constraint is unacceptable, we recommend that you use Microsoft secured-tunnel protocols (PPTV/VPN) in order to establish a secure connection between the Remote Control server and the managers.

In all cases, the usual precautions should be taken at the level of the operating systems and the policies of controlling them. The security of the agent can be compromised if the operating system is easily accessible and if the integrity of the applications can be altered.

2 | Setting up the Desktop Administration module

CHAPTER

Before using the Desktop Administration module you must carry out some preliminary steps, which are described in this chapter.

Installation

We have already seen how the Desktop Administration module is made up of four main elements:

- The module of the AssetCenter package.
- A main deployment or remote control server.
- A manager
- The agents.

You must install these elements being doing anything else.

Automation

Respect the following order:

- 1 Install the AssetCenter package and create of the AssetCenter database.

- 2 Install the deployment server.
- 3 Declare of the deployment server in AssetCenter.
- 4 Install the agents.

Remote control

Depending on your needs, you can use two configuration types when using remote control:

- A simplified configuration for a remote-control session between two computers on the network neighborhood or by direct access (only for remote control).
- A configuration with the server and the database.

Configuration without a database



This type of configuration is only valid for the remote control sessions. It is incapable of automation.

Remote control on a network neighborhood

Desktop Administration is designed with enterprises with extensive networks. In this case, information can be stored centrally in a database, which the Manager can access via a dedicated server.

However, it is possible to use Desktop Administration in simpler environments without having to install a server. In this case, the Manager can automatically detect the active agents on the network by detecting the broadcast signals they send out.

This method is particularly adapted to small, local networks.

Remote control by direct access

In restricted networks for which the manager cannot receive broadcast signals - when agents are on a remote sub-network or when their broadcast option is deactivated, for example - you can create a local description of the computers and populate their connection parameters using a direct access.

The information generated during the creation of a direct access are saved locally in the Manager's certificate.

When the certificate is created, the administrator can authorize the manipulation of the local, direct accesses and even predefine a list of computers in the database. The administrator can thus provide certificates to off-site technicians who cannot access the server while responding to help tickets.

Configuration with a server and a database

We recommend using this mode when you have a large number of computers. It particularly enables you to:

- Provide Managers the list of known computers or computer groups in real time.
- Validate access to the computers according to the control rights set by the administrator.
- Save activity during remote-control sessions for audits or billing.

Desktop Administration uses a multitier configuration that uses a server and a relational database. In this mode, it is possible to manage up to 10,000 computers.

Installing the Desktop Administration module in AssetCenter

The Desktop Administration module is integrated in the main AssetCenter interface.

Whether or not it is activated, though, depends on the license you have received from Peregrine Systems, Inc. For more information on what is included in your license, please contact a sales representative at Peregrine Systems, Inc.




Important:

When installing AssetCenter, make sure the **AssetCenter** package is installed. This package is required for the Desktop Administration module to work correctly.

If you are already using AssetCenter 4.3 (or higher) and you want to acquire the Desktop Administration module, please contact Peregrine Systems, Inc. for a license extension. You will receive a new license file.

To validate your new rights:

- 1 Launch AssetCenter Database Administrator and connect to your database

- 2 Select **Action/ Edit license file**
- 3 Click  and select the new license file
- 4 Click **OK**
- 5 The license file is now registered in the database. The next time your start AssetCenter you will have access to the functionality covered by the license.

 **Important:**

Make sure that the Desktop Administration module is indeed activated in AssetCenter (**File/ Activate modules** menu).

Creating security keys

- 1 Start AssetCenter.
- 2 Execute the **Generate a double security key** wizard via the **Tools/ Actions** menu.
- 3 Populate the following information:

Field	Value
Identity associated with the key	<p>A value of your choice that enables you to name and recognize the key. The identity is stored in the same file storing the public and private keys. Indicate, for example, the name of your company.</p> <p>Note:</p> <p>This identity is only marginally useful at the moment since you do not have a reason to create more than one double security key.</p>
Length of the key	<p>The longer the key, the more complex the encryption algorithm, and the better the security. But the generation and control of the key will also be longer by a few seconds.</p> <p>In most cases, the value 1024 is sufficient.</p>
Private key file	<p>Name of the file that stores the private key. The name proposed by default can be modified.</p>

Field	Value
Public key file	Name of the file that stores the public key. The name proposed by default can be modified.

Installing the deployment server

- 1 Insert the AssetCenter installation CD.
- 2 Select the **Desktop Administration Server** package. The installation program starts automatically.
- 3 Select **Full installation** and indicate the installation path. Then click **OK** to validate.
The following elements are installed:
 - Desktop Administration Server
 - The service associated to the server.
 - The server configuration tool.
- 4 Start the Deployment server configuration tool.
- 5 Select the **Server/ Select private key** menu.
- 6 Select the file that stores the private key (**keypriv.key** by default).
- 7 Click **OK**.



Tip:

After the key is installed, the deployment server no longer needs the **keypriv.key** file.

Install the Remote Control server

- 1 Insert the AssetCenter installation CD.
- 2 Select the **Remote Control** package. The installation program starts automatically.
- 3 Select **Custom Installation**.
- 4 Select **Remote Control Server** and indicate the installation path. Then click **OK** to validate.

Install Remote Control

- 1 Insert the AssetCenter installation CD.
- 2 Select the **Remote Control** package. The installation program starts automatically.
- 3 Select **Custom Installation**.
- 4 Select all components, apart from the **Remote Control server**, specify the installation path and then click **OK** to validate.

The following elements are installed:

- Manager
- Log Viewer
- Session viewer

Creating a certificate

Make sure that the user connected to the database has administrative rights.

To create a certificate:

- 1 Select **Create a Remote Control certificate** from the **Functions and Favorites** menu.
or
- 2 Select the **Tools/ Actions/ Create a Remote Control certificate** menu.
A wizard is displayed. Provide the information required to create the certificate.

Comments on the pages of the Create a certificate wizard

Manager authentication

This page enables you to specify how the manager is authenticated when controlling a computer that is accessed via the secure-access method.

Using the "InfraTools login" option enables you to:

- Identify the manager by associating him with an employee in the InfraTools database.
- Verify that this employee still has the title of manager when controlling a computer.

By removing the title of manager in the table of departments and employees, the administrator immediately revokes the user's control rights over computers via the secure-access method.

Using the "NT login" option enables you to identify the manager in the database using his security identifier and to integrate NT security in the certificate.

The certificate created can be anonymous and issued to several users each identified by their NT login.

NT security

If you select **NT security**, the manager's membership to a specified NT group or domain is verified each time the Manager module is started.

This enables you to increase the security level of remote-control sessions by making sure that users who have been excluded from an NT domain or group can no longer control computers.

Server

Select the servers used by the manager. They will appear in the manager's remote-computer list and indicate the remote computer for which they provide secure access.

Broadcast detectors

A broadcast detector is an agent that listens on a local network to which the manager does not have access. This is the case, for example, with remote sub-networks or networks accessible only by modem. The manager connects to the broadcast detector and, through it, views the list of remote computers transmitting their signal on the network.

Select the broadcast detectors used by the manager. They will appear in the manager's remote-computer list and indicate the agents they have detected on a given network.

Direct accesses

Select the manager's direct accesses (in other words, the remote computers visible by the manager by default).

Depending on the options selected, the Manager can:

- Use direct accesses.
- View direct-access properties.

Without this option, the manager will be able to control agents by the direct-access method but will not be able to see their connection parameters.

- Edit direct accesses

This option is only available if the previous option is selected. This option enables the Manager to:

- Modify the properties of direct accesses.
- Create new direct accesses.

Default parameters

The default parameters are:

- Used by the manager when controlling computers via the broadcast method.
- Assigned to direct accesses created by the manager himself. They can be modified afterward.

Default logon parameters

These parameters are verified by the remote computer each time a remote-control session is opened. The password enables the Manager to be identified by version 4.x, 5.5x, and 6.x agents. The client license, Manager license, and Manager name are only used by the 4.x agents.

Permission to modify default parameters

If you select the **Edit default parameters** option, the Manager can edit the:

- Default logon parameters
- Control options
- Control rights

Validity and generation of the certificate

Validity

Enter a date and time from which the certificate is valid.

Select a calendar in the database or create a calendar manually.

This calendar contains:

- The days and times of the week during which the manager can use the certificate.
- The periods of exception during which the certificate cannot be used.

Add security keys to the certificate

- 1 On this page, integrate the private RSA authentication key used by your company.
This key is obtained when generated the encryption keys in AssetCenter.
For further information, refer to section [Creating security keys](#) [page 32] of this manual.
- 2 If you use a version 5.5x agent, you must integrate the triple DES security key used by your company.

Generate certificate

Enter the name and path of the file to save the certificate.

Installing the agents

To install the agent on one single deployment target

- 1 Insert the AssetCenter installation CD.
- 2 Select the **Agent** package. The installation program starts automatically.
- 3 Select **Full installation** and then click **OK** to validate.
- 4 Start the agent.
- 5 Select the **Tools/ Configuration** menu.
- 6 Select the **Security** tab.
- 7 Select the **Public key** option.
- 8 Select the file that stores the public key (**keypub.key** by default).
- 9 Click **OK**.

After the key is installed, the agent no longer needs the **keypub.key** file.

Important:

For more information about the agents, refer to the Remote Control 5.5.3 **User's guide**, chapter **Using the agent's graphical interface**.

To install the agent on several deployment targets

If you have a large number of agents to install, we recommend performing one of the following solutions:

- Perform a silent installation.
- You can also use the **Mass Deploy** deployment workflow (provided with the line-of-business data) if the target computers use Windows NT, 2000 or XP.
- Use the QuickDeploy! program

Silent installation

Silent installation enables you to quickly install the agent from a DOS prompt.

To perform a silent installation, you must follow these two steps:

- 1 Create an **.ans** file (answer file).
- 2 Launch the silent installation on each deployment target using the **.ans** file as parameter file.

Step 1: Create an answer file (agent.ans file).

Start by installing and configuring an agent on one deployment target. You will use this as a model.



Note:

You must enter a password when configuring the agent to avoid unwanted remote-control sessions.

You must also install the public key, which is encrypted.

After the agent model is created:

- 1 Select the **Tools/ Configuration** menu.
- 2 Click **Save**.
- 3 Enter the name of an answer file (**agent.ans**).

You then need to copy the **agent.ans** file and place its copy next to the **setupl.exe** program in the installation folder. This installation file is usually located on a network drive that the agents can access.

Example of answer file used for silent installation of the agent:

```
[Install]
Type=custom
Packages=ifltsnr,iftmsg,iftrc,iftsys
ListeningAddress=INet::1738
Broadcast=INet:255.255.255.255:1738
BroadcastDelay=60000
Collection=INet::1738
CollectionMax=1000
```

```
NewIdentity=Company
NewKey=LS0tLS1CRUdJTiBQVUJMSUMGS0VZLS0tLS0
ServerAddress=INet:fdacprod:1739
AgentPassword=mH2lUx6sMGpZ98AtMCCc7437DCNK
```

Important:

For more information about the answer files, refer to the Remote Control 5.5.3 **User's guide**, chapter **Customized silent installation**, section **Creating an answer file**.

Step 2: Launch the installation on the deployment targets

To launch the silent installation, execute the following command line on the computers in your NT domain:

```
setup1.exe -a:agent.ans
```

Installing agents with MassDeploy workflow

AssetCenter enables you to install agents on remote computers using the **MassDeploy** workflow.

This workflow is part of the line-of-business data provided with AssetCenter.

To use this workflow, you must:

- 1 Copy the **deploy** folder installed during the Desktop Administration Server installation (by default **c:\Program Files\Peregrine\DA\deploy**) in the deployment server's file depot.
- 2 Edit the impersonation activities of the **MassDeploy** workflow by specifying the authentication information in the **Impersonation** tab (**Deployment/Deployment workflows** menu).

The scripts associated with the **MassDeploy** workflow are documented at the level of the workflow itself.

Note:

Otherwise, you can run the deployment server on an administrator account of the domain.

- 3 Launch the **MassDeploy** workflow.

The workflow schema performs the following actions:

- 1 Connects to a remote computer using an **Impersonate** activity.

- 2 Stops services and the listener if they are already present on the computer.
- 3 Copies files in the **deploy** folder to the remote computer.
- 4 Installs and launches the listener as a service.
- 5 Stops and uninstalls temporary services.

Installing agents with QuickDeploy!

The Remote Control Manager module enables you to remotely install the Agent module on one or more computers. These computers must be registered in one of the domains to which the computer supporting the Manager module has access (Windows NT, Windows 2000 or Windows XP).

Before you install the agent on your remote computers, make sure that:

- You have administrator rights on the target computer(s).
- The Server service is started on the remote computer(s).
- You have access to the c\$ folder as an administrator.

QuickDeploy! can be used in three different ways:

- Selecting the computers from one of the domains to which you have access.
- Using a file that contains the list of computers in a domain.
- Entering manually the name of the computers.

Remotely installing in a domain

To install an agent remotely on one or more computers in a domain to which the Manager has access:

- 1 Launch the Manager.
- 2 Select the **File/Launch QuickDeploy** menu.
- 3 Wait for the **Administrator credentials on remote computers** window to appear.
- 4 Populating the **Account**, **Domain** and **Password** fields enables you to have advanced administration rights on the domain of the computer(s) on which you want to install the agent.
- 5 If the computers in your network have been scanned by InfraTools Network Discovery, you can select the computer(s) on which you want to install an agent from the scan.

Select **Import from an IND scan**.

- 6 Populate the **Server address**, **Account** and **Password** fields to access the InfraTools Network Discovery server.

- 7 If you want to select the computers from your NT domain, choose the **Select an NT domain** option.
 - 8 Click **Next** to go to the **Select an NT domain** page.
 - 9 Select the NT domain where the computer or computers on which you want to install the Agent module are registered.
 - 10 Click **Next** to go to the **Select computers** page.
 - 11 Select the computer(s) on which you want to remotely install the Agent module.
 - 12 Click **Next** to go to the **Confirmation** page.
This page displays the name of the computer(s) on which you want to install the agent.
 - 13 Click **Next** to go to the **Start Deployment** page.
 - 14 Click **Start** to launch the remote installation of the agent.
The length of time it takes to deploy the Agent module depends on the number of computers selected. You can stop the deployment process at any time by clicking **Stop**.
-



Note:

The **Stop** command will never interrupt the current operation, but will impede the triggering of the following operation.

- 15 Click **Finish** after the deployment process has terminated (the status bar will indicate that it is 100% completed).
- 16 Click **Next** to go to the **Deployment results** page.
The **Deployment results** page tells you if the installation of an agent failed on a computer or computers.
By selecting the **Save the list of computes for which deployment failed** option, you can enter the name of a text file in the **File** field. If the deployment failed, you can use this text file later by relaunching a new installation procedure from a text file.

Remotely installing from a text file

In order for the text file to enable the installation of an Agent module on the computers of an NT domain, this file must contain the list of computers. In this file, the name of each computer must be placed on its own line. The name of this computer can be its:

- NetBIOS identifier

- IP address
- Full name

 **Warning:**

In this list of computers:

- The NetBIOS identifier cannot have more than 30 characters.
- No spaces are allowed in the computer name. (Example: You cannot remotely install an Agent module on a **PARIS Server** computer. The computer must be named **PARIS_Server** instead.)

Example of a text file:

```
#Headquarters computers
NTSRV1
NTSRV2
JDUPONT1
ADUPONDnt4
#NY computers
SERV1
SERV2
SERV3
ADMIN1
```

To launch the remote installation of an Agent module from a text file:

- 1 Launch the Manager.
- 2 Select the **File/Launch QuickDeploy** menu.
- 3 Wait for the **Administrator credentials on remote computers** window to appear.
- 4 Populating the **Account**, **Domain** and **Password** fields enables you to have advanced administration rights on the domain of the computer(s) on which you want to install the agent.
- 5 Select the Import from file option.
- 6 Populate the **Choose a file** field with the full path and the name of the text file that contains the list of computers.
- 7 Click **Next** to go to the **Confirmation** page.
This page displays the name of the computer(s) on which you want to install the agent.
- 8 Click **Next** to go to the **Start Deployment** page.
- 9 Click **Start** to launch the remote installation of the agent.

The length of time it takes to deploy the Agent module depends on the number of computers selected. You can stop the deployment process at any time by clicking **Stop**.

 **Note:**

The **Stop** command will never interrupt the current operation, but will impede the triggering of the following operation.

- 10 Click **Finish** after the deployment process has terminated (the status bar will indicate that it is 100% completed).
- 11 Click **Next** to go to the **Deployment results** page.
The **Deployment results** page tells you if the installation of an agent failed on a computer or computers.
By choosing the **Save the list of computers for which deployment failed** option, you can enter the name of the text file in the **File** field. You can use this text file later in relaunching a new installation procedure from a text file.

Remotely installing on computers for which the name is entered manually

To launch the remote installation of an Agent module from a text file:

- 1 Launch the Manager.
- 2 Select the **File/Launch QuickDeploy** menu.
- 3 Wait for the **Administrator credentials on remote computers** window to appear.
- 4 Populating the **Account**, **Domain** and **Password** fields enables you to have advanced administration rights on the domain of the computer(s) on which you want to install the agent.
- 5 Select the Manual entry option.
- 6 Populate the **Computers** field with the names of the computers on which you want to install the Agent module. Each name must be separated by a comma. The computer names can be:
 - NetBIOS identifier
 - IP address
 - Full name

 **Warning:**

In this list of computers:

- The NetBIOS identifier cannot have more than 30 characters.
- No spaces are allowed in the computer name. (Example: You cannot remotely install an Agent module on a **PARIS Server** computer. The computer must be named **PARIS_Server** instead.)

Example of a text file:

```
#Headquarters computers
NTSRV1
NTSRV2
JDUPONT1
ADUPONDnt4
#NY Computers
SERV1
SRV2
SERV3
ADMIN1
```

- 7 Click **Next** to go to the **Confirmation** page.

This page displays the name of the computer(s) on which you want to install the agent.

- 8 Click **Next** to go to the **Start Deployment** page.
- 9 Click **Start** to launch the remote installation of the agent.

The length of time it takes to deploy the Agent module depends on the number of computers selected. You can stop the deployment process at any time by clicking **Stop**.

 **Note:**

The **Stop** command will never interrupt the current operation, but will impede the triggering of the following operation.

- 10 Click **Finish** after the deployment process has terminated (the status bar will indicate that it is 100% completed).
- 11 Click **Next** to go to the **Deployment results** page.

The **Deployment results** page tells you if the installation of an agent failed on a computer or computers.

By choosing the **Save the list of computers for which deployment failed** option, you can enter the name of the text file in the **File** field. You can use

this text file later in relaunching a new installation procedure from a text file described in the previous section.

Configuration

Configuring the deployment server

The deployment server must have access to the AssetCenter database. This database contains all the data needed for the deployment: target computers, deployment workflows, etc. Configuring the server essentially consists in declaring the database connection information.

Configuring the deployment server is carried out by the server configuration tool. This tool automatically detects the computer on which the server is installed.

You must declare the database to which the server must connect:

- 1 Launch the configuration tool.
- 2 Stop the service (**Service/ Stop** menu).
- 3 Select your server (**Server/ Configure the database** menu).

The **Deployment servers** table in the AssetCenter database is populated automatically.

- 4 Start the service (**Service/ Start** menu).

The information relating to the server appears in a few seconds.

The deployment server is executed as an NT service.

Configuring AssetCenter.

To configure a deployment server:

- 1 Start AssetCenter.
- 2 Select **Deployment/ Deployment servers**.
- 3 Select the record that was automatically created when you configured the deployment server.
- 4 Complete the information listed in the table below:

Field	Description
Name	Name of the deployment server.
Computer	Computer on which the deployment server runs. This computer must be in the list of computers in the database.
Depot	<p>The path of the depot folder on the deployment server. This folder stores the files that are exchanged between the server and the deployment targets. This folder is located in the installation folder of Desktop Administration Server.</p> <p>Example: C:\Program Files\Peregrine\Desktop Administration Server\depot.</p> <p>Note:</p> <p>This folder is essential for any file-transfer operation between the server and the deployment targets. By default, the path is relative to the installation folder.</p>
Broadcast detection	<p>List of addresses used by a deployment workflow for which the Start on broadcast option is selected (Properties tab).</p> <p>These addresses are the server's listening addresses for the computers transmitting broadcast signals.</p> <p>The address uses the INET format and has the following syntax:</p> <pre>INET::port1; INET::port2;</pre>
Maximum number of slaves	<p>Maximum number of slave processes that the server can start at a time.</p> <p>Reduce the default value if the server's performances are insufficient.</p>
Default server	Check this box in order for the declared server to be default deployment server.

5 Click **Create** to validate your information.



Automation

PART

3 | Creating deployment workflows

CHAPTER

Creating a deployment workflow

The first step is the creation of a workflow that details the successive steps performed during a deployment for a deployment target. This deployment workflow plays the role of a template for the instances that will be executed on the deployment targets.

Creating a deployment workflow consists of defining:

- Activities
- Activity output events that enable you to activate transitions.
- Transitions that trigger activities.

You can access the list and the detail of deployment workflows via the **Deployment/ Deployment workflows** menu. The **Activities** tab of the window that appears is divided into two panes:

- The left pane gives you a tree view of the structure of a workflow.
- The right pane gives you a graphical view of the workflow. This pane also enables you to edit the deployment workflow in a user-friendly and graphical manner.

- The starting of each workflow is defined in the **Properties** tab, which contains the **Start on broadcast** option.

This option tells the deployment server not to try starting the workflow on a computer until the computer is announced on the network by a broadcast message.

In order for this option to work, the server needs to have been configured to receive such messages, and the computers must have an installed and configured agent in order to transmit such messages.

This option enables you to, for example, reliably launch a deployment on laptop computers or computers that are shut off during the day.

This section explains how to use this graphical editor to create, modify or delete the elements of workflow:

- Activities
- Events
- Transitions

Activities

To create an activity, right-click in an empty zone of the **Activities** tab, then select an activity in one of the available categories. The table below lists the available activities according to their category:

Activity category	Available activities
Core activities	<ul style="list-style-type: none"> • Success • Failure • Retry • Jump • Empty activity • Synchronization • Wait
System management	<ul style="list-style-type: none"> • Impersonate • Execution • Shutdown • Wake on LAN • Registry

Activity category	Available activities
File management	<ul style="list-style-type: none"> • Upload files • Download files • Move files • Copy files • Rename • Delete files • Create folders • Delete folders
Script	Script
Action	Action
Messaging	Messaging

The detail of an activity and its properties are automatically displayed when you select an activity.

To delete an activity:

- You can either select the activity by clicking on it with the mouse, then pressing "Delete" on the keyboard.
- Or you can select the activity, right-click and select **Delete** from the shortcut menu that appears.



Note:

You can also perform all selections, creations and deletions from the tree-list view of the workflow.

The set of available activities in Desktop Administration: ► [References \(Desktop Administration\)](#) [page 77].

Events

Events are the outputs of activities. They enable the activation of transitions, which trigger other activities. The available events vary depending on the nature of the activity:

For example:

- A **File management** type activity has **OK** and **Error** for events by default. But you can access additional events **No file**.

To add an event to an activity:

- 1 Select the concerned activity and right-click.
- 2 Select the event to add: **Error, OK, Return value, No file**, etc.

Transitions

To create a transition:

- 1 Select the event that enabled the transition by clicking it with the mouse.
- 2 Hold the mouse button down and drag the event all the way to the destination activity.

To delete a transition:

- You can either select the transition by clicking on it with the mouse, then pressing "Delete" on the keyboard.
- Or you can select the transition, right-click and select **Delete** from the shortcut menu that appears.

To modify the source and/or destination of a transition:

- 1 Select the transition.
- 2 Drag the extremity you want to modify.

Practical case

This section describes the steps necessary for executing a deployment on a set of targets. For the example, we will use one of the deployment workflows available in the demonstration database. We will also assume that the server and deployment targets are all declared in the database and that the records corresponding to these targets (in the Computers table) have all been correctly populated. The typical procedure breaks down in to the following steps:

- 1 Create a deployment workflow (not dealt with in this section; a demonstration database is used).
- 2 Create a workflow instance.
- 3 Launch the deployment.
- 4 Verify the execution of the deployment.

Creating a deployment workflow

For this example we are using the **Registry inventory** deployment workflow, provided with the software.

Creating a deployment instance

To create a deployment instance, you must:


- Select a deployment workflow.
- Select a set of targets on which this deployment workflow will be launched.

To create a deployment instance:

- 1 Select **Deployment/ Deployment instances**.
- 2 Click **New**.
- 3 Populate the fields listed in the table below and then click **Create**.

Field	Value
Original workflow	Registry inventory
Deployment server	Select a declared deployment server. Note that if you leave this field empty, AssetCenter will use the deployment server for which you have selected the Default server option.
Start	Date the workflow started by the server.
Stop	Date the workflow stopped by the server. When this date is reached, the server stops deploying on the computers still pending.

Now select the deployment targets. To do this:

- 1 Click  next to the list of computers displayed in the **General** tab of the detail of a deployment workflow instance.
- 2 AssetCenter triggers a wizard that proposes a list of deployment targets. Make your selection and click **OK**.

 **Note:**

Because the Computers table is hierarchic, you can deploy a workflow on a group of computers or even select all the computers one by one. In this last case, you can only select up to 99 computers on which to deploy a workflow.

Creating a deployment-type action

AssetCenter enables you to create a deployment-instance type action.

This is a contextual action on the Computers table (amComputer). It applies to a selection of one or multiple records.

To create a deployment instance type action:

- 1 Tools/ Actions/ Edit menu
- 2 Create a new action and populate the **Type** field with the value **Deployment**
- 3 Populate the **Deployment** tab with the name of the deployment workflow (**Deployment workflow** field)

To use a deployment-type action on the Computers table, right-click on the desired record and select the created action.

Creating a deployment-type action enables you to:

- Launch the workflow without having to use the Deployment instance menu.
- Use the deployment action via an **action** type action.

This action enables you to define a list of target computers via an AQL query. If you do not define a query, all records from the Computers table will be processed.

- Call another workflow from within the workflow by using an action type activity to execute a deployment action.

Launching a deployment

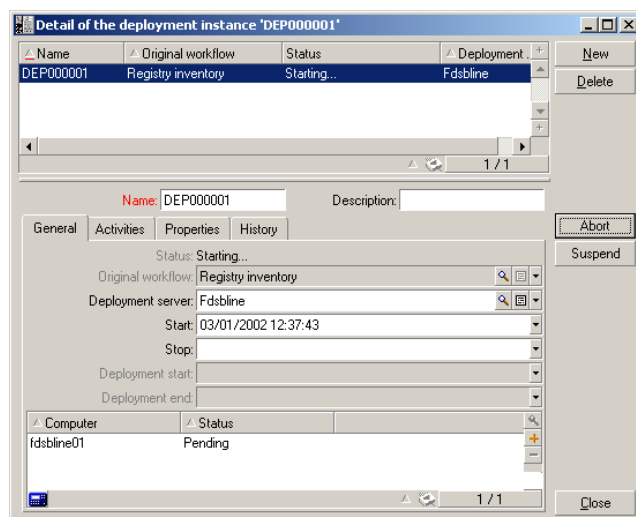
In the detail of the deployment instance, click **Start**. AssetCenter attempts to trigger the deployment on the selected targets. The **Status** of the workflow becomes **Starting**.



Note:

Use the F5 key regularly to refresh the displayed workflow status. Whether or not the **Start**, **Abort**, **Suspend** and **Resume** buttons are displayed depends on the status of the workflow.

Figure 3.1. Launching the deployment - Detail window




You can abort or suspend the deployment at any time by clicking **Abort** or **Suspend**.

If the workflow fails, the **Retry** button copies the original workflow and just executes it for those deployment targets that have failed.

The **Activities** tab contains a copy of the workflow of the deployment instance. If you modify a workflow instance in progress, the modifications will only be taken into account when the workflow is restarted.

Verifying the execution of the deployment

To monitor the status and progress of a running deployment:

- 1 Select a deployment target from the list in the **General** tab of the deployment workflow instance detail.
- 2 Click 
- 3 The window that opens displays the activity being executed as well as the deployment log.
 - The dates and times indicate when the workflow activities are processed.
 - The colored arrow indicates the current progress of the workflow.

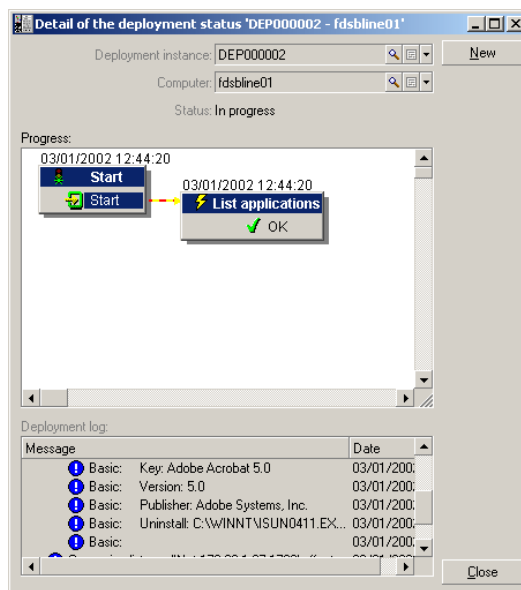


Note:

Use the F5 regularly to refresh the information shown on the workflow and to see the current progress of the activities.

- 4 The deployment log describes the stages in the processing of the workflow, in particular Basic messages containing "PRINT" instructions.

Figure 3.2. Deployment instance - Execution-control window



Verification of the connection address

When you launch a deployment workflow, you might need to connect to a server.

The server determines the connection address using the information contained in the database (**amComputer** and **amIftAgent** tables).

Connection process

A connection process is launched on each address.

The connection address is determined by the information in the database:

- The IP name and port of the agent (**amIftAgent.tcpiphostname** et **amIftAgent.sPortNumber**)
- In case of failure, it is the name of the computer (**amComputer.TcpIpHostName**) and default port.
- In case of failure, it is the IP address of the computer (**amComputer.TcpIpAddress**) and default port.

Configuration of the connection to a listener

You can choose to not take the default connection parameters into account by defining a context variable **Computer.ForceConnection**.

This variable defines the connection parameters to use to connect to a remote agent.

Syntax

```
INET:<Computer name>:<Port number>
```

Example

```
DaSetContext "Computer.ForceConnection", "INET:"&DaContext("Computer.N  
ame")&":1739"
```

This script enables the deployment server to connect to the TCP/IP port 1739 instead of connecting to the default port 1738.

For more information about the commands used in this script, refer to the **Programmer's reference** guide.

4 Using the deployment server

CHAPTER

With section [Configuring the deployment server](#) [page 45], you will have learned how to use the server configuration tool at installation time.

This chapter tells you more about the day-to-day use of the server configuration tool.

Modifying the references in the AssetCenter database

To modify the references in the AssetCenter database containing the deployment workflows and the description of the deployment targets:

- 1 Start Desktop Administration Server's Server configuration tool.
- 2 Select the **Server/ Configure the database** menu.
- 3 Modify the information relating to the database connection.
- 4 Validate the new parameters by clicking **OK**.
- 5 If the **Desktop Administration** service is already started, select the **Server/ Reload configuration** menu.

Modifying the private key

- 1 Create new security keys.
 - ▶ Creating security keys [page 32]
- 2 Start Desktop Administration Server's Server configuration tool.
- 3 Select the **Server/ Modify the private key** menu.
- 4 Indicate the full path of the file that stores the new private key.
- 5 Validate the new parameters by clicking **OK**.

Configuring the Desktop Administration service

When you installed Desktop Administration Server, a service was created.

To modify the parameters of the Desktop Administration service

- 1 Start Desktop Administration Server's Server configuration tool.
- 2 Select the **Service/Configure** menu.
- 3 Validate the new parameters by clicking **OK**.

To start, stop or restart the Desktop Administration service:

- 1 Start Desktop Administration Server's Server configuration tool.
- 2 Select the **Service/Stop**, **Service/Start** or **Service/Restart** menu.

Modifying the server configuration tool options

- 1 Start Desktop Administration Server's Server configuration tool package.
- 2 Select the **File/Options** menu.
- 3 Modify the options.
- 4 Validate the new parameters by clicking **OK**.

For more information option parameters, refer to the AssetCenter **Interface** guide, chapter **Customizing a client workstation**, section **AssetCenter interface options**.

Restarting the Desktop Administration service automatically

To have the server configuration tool attempt automatically and regularly restarting the **Desktop Administration** service whenever it stops:

- 1 Start Desktop Administration Server's Server configuration tool.
 - 2 Select the **File/ Watchdog mode** menu.
-

 **Note:**

When the automatic restart option is activated, a mark appears in front of the **Watchdog mode** entry of the **File** menu.

You cannot adjust the frequency of attempts to restart the service.

Modifying the parameters of a deployment server

- 1 Start AssetCenter.
- 2 Select **Deployment/ Deployment servers**.
- 3 Select the deployment server to modify.
- 4 Update the deployment server's parameters.
- 5 Validate the new parameters by clicking **Modify**.
- 6 Start Desktop Administration Server's Server configuration tool package.
- 7 If the **Desktop Administration** service is already started, select the **Server/Refresh caches** menu.

If the **Desktop Administration** service is not yet started, select the **Service/Restart** menu.

Obtaining information about how the Desktop Administration service functions

- 1 Display the user interface of Desktop Administration Server's Server configuration tool package.
- 2 Select the **File/Refresh** menu.
- 3 Consult the **Server information** section in the workspace.

- 4 For more details, select the **Service/ Display log** menu.

To learn more about how the Log viewer program works, refer to the AssetCenter **Administration** guide, chapter **Consulting the log (.log) files**.

5 | Examples of deployment workflows

CHAPTER

This chapter describes some of the deployment workflows that are part of the **line-of-business data** installed with AssetCenter.

It also gives you some examples of deployment workflows that you can create yourself.

IDD scan workflow

This workflow launches a Desktop Inventory scan on a remote computer and copies the InfraTools Desktop Discovery scan files to AssetCenter.

You can then import the scan data to your database using a Connect-It workflow.

PDI scan workflow

This workflow launches a Desktop Inventory scan on a remote computer and copies the Desktop Inventory scan files to AssetCenter.

This workflow differs from the **IDD scan** workflow by the type of **.xml.gz** files generated.

To work correctly, the script used by the scan executable must have the **/o** parameter. This is so it doesn't account for the default values of the scan executable, but instead accounts for those of the workflow.

For example:

```
c:\scanW32.exe /o:C:\[Computer.Name]
```

The path indicated is the one of the scan executable's folder. And each scan file generated will be saved in a file having the same name as the computer.

WMI scan workflow

This workflow is an example of how using the API to access the Windows Management Instrumentation.

This workflow enables you to retrieve the information relating to the scan data of a remote computer:

- Processor
- RAM
- BIOS
- Video card
- Sound card
- Operating system
- And so on.

Required configurations

The WMI service is installed by default for Windows XP and Windows 2000. For Windows NT4.0, you need to have already installed the Service Pack 4, as well as WMI Core 1.5.

WMI Core 1.5 is available on the Microsoft Web site.

Registry scan workflow

This workflow establishes a list of all the applications on a remote computer visible from the Control Panel (**Add/Remove programs**).

This information is stored in the **Automated Desktop Administration Tracking** table (amDaTracking) in the AssetCenter database.

Change the wallpaper workflow

This workflow:

- 1 Searches for and displays the folder storing the computer's wallpapers.
- 2 Copies a bitmap file of the server to the remote computer.
- 3 Configures the copied file as the Windows default wallpaper on the deployment target.
- 4 Connects to the remote sever as a referenced user (impersonation).
- 5 Configures the user's wallpaper.

InstallShield silent installation workflow

This workflow is a deployment example of a program based on the InstallShield installation engine.

The command parameters are defined in the **Execution** tab of the **RunSetup** activity.

The parameters in this workflow show how to use the silent installation method via the **-s** parameter and an answer file **.iss**.

The creation of this answer file is done using the **-r** parameter.

For more information about InstallShield, refer to the documentation provided with this program.

Example of temporary agent workflow

This workflow addresses the security requirements of certain companies to not install an agent that will run permanently on a computer (server, etc.). An agent is installed temporarily to execute a task and is then uninstalled.

This workflow uses NT security and requires you to have NT administrator security privileges.

The example workflow is as follows:

- 1 Impersonation of the remote computer.
- 2 Installation of the listener on a remote computer in a temporary folder: Installation of the **iftlsnr.exe**, **iftagt.exe** and **iftsys.exe** files.
- 3 Creation and launching of the temporary **iftlsnr.exe** service on a listening port different from the standard port.
- 4 Addition of activities via the listener.
- 5 Stopping the listener and uninstalling the temporary folder.

The command line to launch the service is the following:

```
iftlsnr.exe -temp -listen:INET::1740 -svc
```

- **-svc**: This parameter indicates that the program is launched as a service.
- **-temp**: This parameter indicates that the .INI files or the Registry or not read from or written to.
- **-listen:INET::1740**: This parameter indicates that the program **iftlsnr.exe** uses port 1740 instead of port 1738 (the default port) to avoid conflicts with an agent already installed.

To indicate that the deployment server uses a different port, the following command line is used:

```
DaSetContext "Computer.ForceConnection", "INET:"&DaContext("Computer.N  
ame")&":1740"
```

- The context variable **Computer.ForceConnection** enables you to specify the port number by using the following syntax: INET:<Name of the computer or IP address>:<Port number>.

For more information about the syntax used, refer to the **Programmer's reference** guide.

Software license management

AssetCenter enables you to manage the software licenses in your IT portfolio by creating the appropriate workflow.

The example workflow is as follows:

- 1 Launch a scan of the installed applications (using a WMI scan, Registry inventory, InfraTools Desktop Discovery).
- 2 Compare the installed applications with the purchased license files.
- 3 Generate an electronic form to be sent to users asking them to list the applications they use.
- 4 Uninstall the unused applications.
- 5 Compare the number of used applications to the license files and issue purchase requests for more licenses if this number does not match.

Uninstalling software

AssetCenter enables you to uninstall an application on all remote computers using the appropriate workflow.

The example workflow is the following:

- 1 Perform a query on the name of the application.
- 2 Determine the number of computers on which this application exists.
- 3 Uninstall the application.

6 Examples of deployment wizards

CHAPTER

Wizards are used to automate the execution of deployment workflows.

A wizard enables you to, for example, select a list of deployment targets and execute a deployment workflow on each selected target.

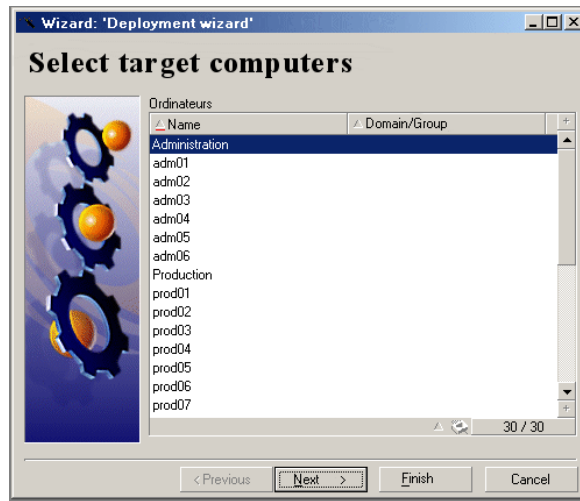
You can access AssetCenter's wizards via the **Tools/ Actions** menu.

The following wizards are provided with the AssetCenter demonstration database.

For more information about creating a wizard, refer to the **Administration** guide in the chapter **Wizards**.

Computer deployment wizard

This wizard enables you to deploy a workflow on one or more computers recorded in the **amComputer** table.



Deployment is limited to 99 computers in multiple selection.

We recommend creating computer groups. A group can be made up of as many items as required.

When you create a computer group, the deployment takes into account the members of this groups. It is possible for this operation to be recursive because the Computers table (**amComputer**) is hierarchic.

Service deployment wizard

This wizard enables you to deploy a workflow on one or more services recorded in the **amEmplDept** table.

The wizard searches for the computers used by the employees of the selected departments (**amEmplDept**).

Location deployment wizard

This wizard enables you to deploy a workflow on one or more locations recorded in the **amLocation** table.

The wizard searches for the computers linked to the selected locations.

NT-domain computer import wizard

This wizard enables you to:

- 1 Select an NT network.

The **Extract list from domain controller** option enables you to choose between information coming from the master explorer or those coming from the domain controller.

If you selected this option, make sure you have network administrator rights.

If you cleared this option, the information about the local computer on which you executed the wizard will not be retrieved.

- 2 Retrieve the list of computers on this network.
- 3 Create the corresponding records in the **amComputer** table.

The wizard retrieves the **Name** and **First** (First name) data depending on the customizations made to the operating system. You must therefore update the wizard script if the data to retrieve does not follow the "Name, First" order defined in the NT account manager.

NT-domain user import wizard

This wizard enables you to:

- 1 Choose a Windows NT network.
- 2 Retrieve the list of users that have a login on this Windows NT network.
- 3 Create the corresponding records in the **amEmplDept** table and populate the **First name** and **Last name** fields.



The information about the local computer on which you executed the wizard will not be retrieved.

7 Glossary (Desktop Administration)

CHAPTER

Deployment workflow

The deployment workflow is the formalization and/or automation of the deployment procedures.

For example, the following processes can be modeled and automated using workflow methods:

- The deployment of an application on an IT portfolio.
- The periodic execution of a hardware and software scan.
- Etc.

AssetCenter enables you to define deployment workflow schemas and manage their procedures.

Warning:

The deployment workflows differ from the classic workflows available in AssetCenter. In principal, they are the same, but their functionality and interfaces are different from one workflow to the next.

Workflow schema

Creating a workflow schema involves defining:

- Activities
- Activity output events that enable you to activate transitions.
- Transitions that trigger activities.

Deployment instances

A deployment instance is a single occurrence of an execution of a workflow schema. It is transmitted to the deployment server to be processed and executed. You can look as a deployment workflow instance as one unit of elementary work for a deployment server.



The deployment instance is thus a copy of the deployment workflow that you initially created. You can thus modify the original deployment workflow as you wish during the execution of a deployment instanced based on this workflow.

Deployment server

The deployment server the core of this Desktop Administration module. It executes the deployment instances on a list of the machines stored in the database.

You may use one or more deployment servers.

Deployment target

A deployment target is a machine on which is deployment is performed. Targets are declared in the Computers table of the AssetCenter database.

Workflow activity

A workflow activity is made up of:

- A task to perform.
- Events that trigger transitions to other activities.

The administration console proposes a series of typical activities, such as downloading, execution, etc.

Workflow event

Workflow events are the outputs of activities. They enable the activation of transitions, which trigger other activities.

Workflow transition

A workflow transition enables you to go from one activity to another. This is triggered by the occurrence of an event.

An event can be associated with several transitions.

Agent

The agent is a program that enables the computer on which it is installed to be controlled by the deployment server.

The agent is made up of two parts:

- The **Listener**: An executable installed as a service on the computer. This service, running on permanent stand-by on the network, enables the computer to be controlled by the deployment servers.
- A **graphical interface**: It has numerous functions, but it notably enables the user of a controlled computer to chat with the deployment server, send messages, refuse to accept remote-control sessions, etc.

Depot

Sub-folder of the Desktop Administration Server administration folder that regroups the following folders:

- **deploy**
This folder contains the scan executables used by the **MassDeploy** workflow.
- **idd**
This folder contains the scan executables used by the **IDD scan** workflow.
- **pdi**
This folder contains the scan executables used by the **PDI scan** workflow.
- **wallpaper**
This folder is used by the **Change the wallpaper** workflow.

Broadcast signal

Each agent is identified on the network by an activity signal called the **broadcast signal**. This signal is recognized by the deployment servers.

8 References (Desktop Administration)

CHAPTER

Deployment activities

This section provides an exhaustive preview of all the available deployment activities, which are classified by category.

Core activities

This category regroups all the activities inherent in a workflow, such as its entry point (the **Start** activity created by default for all new workflows) or its different output points (**Failure** or **Success**, for example).

Most activities transmit two kinds of output messages: **OK** or **Error**. We recommend that you process these messages with a **Success** or **Failure** type activity.

Success

End-of-workflow activity that was correctly executed.

Stops the workflow and interrupts the activities in progress.

Failure

End-of-workflow activity that could not be executed.
Stops the workflow and interrupts the activities in progress.

Retry

End-of-workflow activity that triggered the same workflow another time.
The workflow is restarted from the **Start** activity.

Jump

Workflow activity that jumped to another named activity. To define the target activity, select an activity in the **To** field of the activity detail.
This activity enables you to reduce the transitions in a workflow schema and make reading it easier.

Empty activity

Workflow activity provoking a single output message: OK.
This activity is used if there are not an identical number of workflow-event activities that must be synchronized.

For example:

- The **Send** workflow activity uses three events: OK, no file, error.
- The **Execution** workflow activity uses two events: OK, error.

To synchronize these two activities, you must create an empty activity for the **Send** activity that processes the 'OK' and 'no file' events.

Synchronization

This activity provokes a successful output (the output event is validated) if all the input events are validated. In practice, several transitions are connected to this activity. The activity verifies all the transitions, and if it cannot verify them, it waits until it can do so. A workflow can only result from this activity after all the input transitions are verified.

Wait

This activity pauses the deployment workflow. The duration of this pause is defined in the **Duration** field of the activity detail.

System management

This category groups together those activities that act directly on the system.

Impersonate

This activity enables you to perform tasks on a remote computer to:

- Perform an action in the place of the named user.

You can therefore have access to the same:

- Objects, with the same rights as the named user.
- Environment variables as the named user.
- Preference folders and Registry as the named user.

An impersonating activity does not have any immediate results. It modifies the behavior of other activities such as:

- Execution
- Edition of the Registry
- RPC/ WMI

The impersonation parameters are populated in the **Impersonate** tab of the activity detail:

- **User:** Login of the user you want to impersonate.

The **@LoggedOnUser** instruction makes it possible to use the identity of the currently logged user. If no user is logged, the activity fails.

The **@LocalSystem** instruction enables you to use the default system account (all local rights on the machine).

Important:

The **@LoggedOnUser** and **@LocalSystem** instructions are only valid for the activities involving the agent. For the RPC/WMI activities, these instructions are meaningless, because authentication is performed via NT security.

Note:

If a user is never physically logged on, the preferences relating to this user are not saved.

- **Domain:** User domain.
-



Note:

To specify a local account of the machine, you must specify the name of the machine, for example using the following syntax:

[Computer.Name]

- **Password:** Password associated with the user login.
 - **Test:** This operation opens a DOS box on the remote computer and verifies the validity of the populated parameters (login, domain, password).
In order to work, this test requires a listener on the remote computer.
-



Note:

Do not perform several **impersonating** activities at the same time in the same workflow.

This activity does not work with Windows 9.x operating systems. In Windows NT 3.51, the functions are limited.

Execution

This activity executes a program stored on the deployment target. All the execution parameters are stored in the **Execution** tab of the activity detail.

- **Command:** Name of the program to execute and parameters.
 - If you do not specify a path, the program to execute must be located in your operating system's **Path** environment variable.
 - If you specify a path, it must be the absolute path. Par example
C:\temp\sample.exe
- **Path:** Current folder of the program to execute. This parameter is not mandatory.
- **Synchronous:** Select this option for the execution to be synchronous. The activity does not let the user control the computer until the program is executed.
- **Log:** Select the option that best suits you for the information to enter into the log file.
- **Visibility:** This option enables you to either force the display of graphical interface of the executed program or hide it.
 - **By default:** Only the operating system decides on the interface's display.

- **Force display:** interface displayed.
- **Hide:** interface hidden.

Shutdown

This activity shuts down a deployment target. You can choose whether to restart or shut down the target by selecting the corresponding option in the **Method** field of the activity detail.

Wake on LAN

This activity sends a wake on LAN signal to a deployment target. It wakes up the target machine.

The **Wake on LAN** activity only works in the following cases:

- The target computer has a motherboard and a network card that support this function.
- The target computer is declared in the database and the **Physical address** field is populated for the computer. This address is the computer's MAC address.

Registry

This activity enables you to perform operations on the Registry using a script in the **Edit script** tab of the activity detail. This script calls on specific functions in the Registry, which are detailed in the **Programmer's reference** guide.



Note:

Warning: This script is not an AssetCenter or Basic script but a series of operations to be performed on the Registry.

For example, [Hkey_Local_Machine\Software\Microsoft]? to verify a Registry key or [Hkey_Local_Machine\Software\Microsoft] to create it.

General information on the Registry

The Registry stores essential information related to the configuration of the operating system..

 **Warning:**

Errors in manipulating the Registry can provoke major dysfunctions with the computer. Be extremely prudent when making changes to the Registry.

A Registry key is made up of four items:

- A full name uniquely identifying the key in the tree structure of the Registry.
- A name for each key entry.
- A value for this entry.
- A type for the data stored in the value of the entry. The list of types is summarized in the table below:

Data type	Description
REG_BINARY	Raw binary data. It is represented in hexadecimal format in the operating system's Registry editor utility.
REG_DWORD	4-bit number. This data is represented in binary, decimal or hexadecimal format in the operating system's Registry editor utility.
REG_EXPAND_SZ	Interpreted character string of variable length. Data of this type is used to store environment variables whose values are interpreted when a program or service is executed.
REG_MULTI_SZ	List of character strings. In general, the strings are separated by spaces or commas.
REG_SZ	Character string.

 **Note:**

For further information on the Registry, please consult the documentation of your operating system.

Description of the format

The syntax and the format used by the **Edit script** are similar to those used in the **.reg** files created by the RegEdit application in Microsoft Windows. Apart from certain proprietary extensions in Desktop Administration, both formats remain compatible. The specific extensions are available in the form of operators

entered directly after the name of a key or an entry. The operators, which are incompatible with the classic **.reg** format are listed below:

- +
- -
- ?
- !
- >
- :

The **Edit script** supports the following operations:

- Creating a Registry key,
- Deleting a key,
- Creating or assigning a value to an entry for a key.

Empty lines or lines starting with the ' character are ignored. The first line, if it is not valid, is also ignored.

Each line describes an operation to be performed on a Registry key, an operation on an entry or the definition of a sub-key:

- [**<Name of the key>**] or [**<Name of the key>**]+: Creates a key (if it does not already exist)
- [**<Name of the key>**]-: Deletes an existing key
- [**<Name of the key>**]?: Makes the activity fail if the key is not found
- [**<Name of the key>**]!: Makes the activity fail if the key is found
- [**<Name of the key>**]>: Extracts the full contents of the key. This type of operation is generally used in conjunction with the **DaRegExec()** and **DaGetRegOutputValue()** functions (which enable you to execute a script on the Registry and recover the output of the previous function respectively). For further information, refer to the **Programmer's Reference** provided with AssetCenter.

As soon as a key is defined, the values of the entries can be manipulated using the following operations:

- **<Entry>=<Value>**: Defines an entry and a corresponding value for a key,
- **<Entry>:<Value>**: Defines an entry (if it has not already been defined),
- **<Entry>-**: Deletes an existing entry,
- **<Entry>?**: Makes the activity fail if the entry is not found,
- **<Entry>!**: Makes the activity fail if the entry is found,
- **<Entry>>**: Extracts the full contents of the key. This type of operation is generally used in conjunction with the **DaRegExec()** and

DaGetRegOuputValue() functions (which enable you to execute a script on the Registry and recover the output of the previous function respectively). For further information, refer to the **Programmer's Reference** provided with AssetCenter.

<**Entry**> may contain either a string in double quotes ("), or the @ character to define the default value of a key.

<**Value**> can contain:

- A character string. Example:

```
"C:\Program Files\Test"
```

- A 4-byte number (dword). Example:

```
dword:000004da
```

- A binary block in hexadecimal format. Example:

```
hex:44,55,d4,56,40
```

File management

This category groups together those activities that act on files and folders.

Upload files

This activity sends files to a deployment target.

The parameters of this activity are available in the **Files** tab of the activity detail:

- **Source folder:** Path of the files to copy on the deployment target. It is a relative path depending on the path of the file depot on the deployment server.
- **Destination folder:** Absolute path of the files copied to the deployment target.
- **Filter(s):** Set of file names (wildcard characters authorized) that are separated by a semi-colon. For example:

```
*.gif; iftmsgr.exe
```

If this field is not populated, all the files in the specified folder will be taken into account.

You can also select the following options:

- **Recursive:** If this option is selected, the copy is recursive.
Copies all files and sub-folders in the current folder.

- **Replace:** If this option is selected, the copy will overwrite any files with the same name in the destination folder of the target.
- **Force:** If this option is selected, the copy will not take into account the read-only protections on the target.
- **Resume:** If this option is selected, the activity tries to resume sending files in case of a transfer interruption.

Download files

This activity copies files from the deployment target to the deployment server. The parameters of this activity are available in the **Files** tab of the activity detail:

- **Source folder:** Path of the files to copy to the depot of the deployment server. It is an absolute path on the deployment target.
- **Destination folder:** Relative path (depending on the path of the file depot) of the files copied to the deployment server.
- **Filter(s):** Set of file names (wildcard characters authorized) that are separated by a semi-colon. For example:

```
*.gif; iftmsgr.exe
```

If this field is not populated, all the files in the specified folder will be taken into account.

You can also select the following options:

- **Recursive:** If this option is selected, the copy is recursive.
- **Replace:** If this option is selected, the copy will overwrite any files with the same name in the destination folder of the target.
- **Force:** If this option is selected, the copy will not take into account the read-only protections on the server.
- **Resume:** If this option is selected, the activity tries to resume receiving files in case of a transfer interruption.

Move files

This activity moves files locally to the server or the deployment target. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the Files tab of the activity detail:

- **Source folder:** Source path of the elements to move. Depending on how the function operates, it is either a path relative to the file depot (in the case

of a local move to the deployment server) or an absolute path (in the case of a local move to the deployment target).

- **Destination folder:** Destination path of the elements to move. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local move to the deployment server) or an absolute path (in the case of a local move to the deployment target).
- **Filter(s):** Set of file names (wildcard characters authorized) that are separated by a semi-colon. For example:

```
*.gif; iftmsgr.exe
```

If this field is not populated, all the files in the specified folder will be taken into account.

You can also select the following options:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.
- **Recursive:** If this option is selected, the move is recursive.
Moves all files and sub-folders from the current folder.
- **Replace:** If this option is selected, the move will overwrite any files with the same name in the destination folder of the target.
- **Force:** If this option is selected, the copy will not take into account the read-only protections on the target or the server.

Copy files

This activity copies files locally on the server or the deployment target. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the Files tab of the activity detail:

- **Source folder:** Source path of the elements to copy. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local copy to the deployment server) or an absolute path (in the case of a local copy to the deployment target).
- **Destination folder:** Destination path of the elements to copy. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local copy to the deployment server) or an absolute path (in the case of a local copy to the deployment target).
- **Filter(s):** Set of file names (wildcard characters authorized) that are separated by a semi-colon. For example:

```
*.gif; iftmsgr.exe
```

If this field is not populated, all the files in the specified folder will be taken into account.

You can also select the following options:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.
- **Recursive:** If this option is selected, the copy is recursive.
Copies all files and sub-folders in the current folder.
- **Replace:** If this option is selected, the copy will overwrite any files with the same name in the destination folder of the target.
- **Force:** If this option is selected, the copy will not take into account the read-only protections on the target or the server.

Rename

This activity renames files locally on the server or the deployment target. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the Files tab of the activity detail:

- **Current name:** Full source path of the file to rename. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local renaming in the deployment server) or an absolute path (in the case of a local renaming in the deployment target).
- **New name:** This parameter contains the new file name.

You can also select the following options:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.
- **Replace:** If this option is selected, the copy will overwrite any files with the same name in the destination folder of the target.
- **Force:** If this option is selected, the copy will not take into account the **read-only** option on the target or the server.

Delete files

This activity deletes files locally on the server or the deployment target. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the Files tab of the activity detail:

- **Folder:** Path of the elements to delete. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local deletion from the deployment server) or an absolute path (in the case of a local deletion from the deployment target).
- **Filter(s):** Set of file names (wildcard characters authorized) that are separated by a semi-colon. For example:

```
*.gif; iftmsgr.exe
```

If this field is not populated, all the files in the specified folder will be taken into account.

You can also select the following options:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.
- **Recursive:** If this option is selected, the deletion of files is recursive. Deletes all files and sub-folders from the current folder.
- **Force:** If this option is selected, the copy will not take into account the **read-only** option on the target or the server.

Create folders

This activity creates files locally and recursively on the server or the deployment target or the server. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the **Files** tab of the activity detail:

- **Folder(s):** Path of the folder to create. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local creation in the deployment server) or an absolute path (in the case of a local creation in the deployment target).

You can also select the following option:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.

Delete folders

This activity deletes files locally from the server or the deployment target. The way in which it works is determined by the **Perform the operation on the server** option.

The parameters of this activity are available in the **Files** tab of the activity detail:

- **Folder(s):** Path of the folder to delete. Depending on how the function operates, it is either a path relative to the file depot (in the case of a local deletion from the deployment server) or an absolute path (in the case of a local deletion from the deployment target).

You can also select the following option:

- **Perform the operation on the server:** If this option is selected, the activity operates on the deployment server and not the target.
- **Recursive:** If this option is selected, the deletion is recursive.
- **Force:** If this option is selected, the copy will not take into account the read-only protections on the target or the server.

Script

This activity enables you to define a script that will be executed on the deployment target. This script uses functions that are detailed in the **Programmer's reference** guide.

You can access a script editor with syntax highlighting and line numbers by pressing **F4** while in the detail of a script.



Note:

All workflow activities are available in API form via this script-type activity. Certain other functions (API, RPC) are only available from a script.

Action

This activity enables you to execute an action (in the sense given by AssetCenter) contextually on a database table. The **Action** tab regroups the parameters of this activity:

- **Action:** SQL name of the action to be executed.
Because the action is contextual, only those tables relating to the deployment target are available.
- **Table:** Select one of the tables on which the action is executed.

Messaging

This activity enables you to execute a messaging type action.

AssetCenter lets you manage two types of messages:

- Messages issued from AssetCenter and sent to the AssetCenter database via its internal messaging system.
- Messages created in AssetCenter and sent via an external messaging system.

The workflow's sending parameters are defined in the **Messaging** tab.

In order for a messaging-type activity to be corrected executed, you need to have already configured the messaging system according the protocols you use, as well as the deployment server.

For more information about configuring the messaging system, refer to the "Administration" guide, chapter "Messaging".



Remote control

PART

9 Remote Control

CHAPTER

Rapid installation

This explains how to rapidly install and configure the Manager and Agent components of Desktop Administration so that a Manager can control the computers on which the agent is installed.

By following the procedures described in this chapters, you can discover the general layout and functions of Remote Control in evaluation mode. This mode is **valid for a 30-day period**, and it enables the manager to take control of:

- Five computers on the neighborhood network.
- Five computers by direct access.
- Fifteen computers recorded in the database whose access is secured by the server.

For a remote-control session between two computers, you must configure the:

- The Manager

It enables its user to see the screen of a remote computer and to take control of it.

- The Agent

Once it is installed on a computer, the Agent enables the computer to be controlled by a Manager. It has two parts:

- The Listener: an executable installed as a service on the computer. This service, always running in the background, enables the computer to be controlled by the Managers.
- A graphical interface. Among its numerous functions, this interface enables the user of the controlled computer to chat with the Manager, send messages, and accept or refuse a remote-control session.

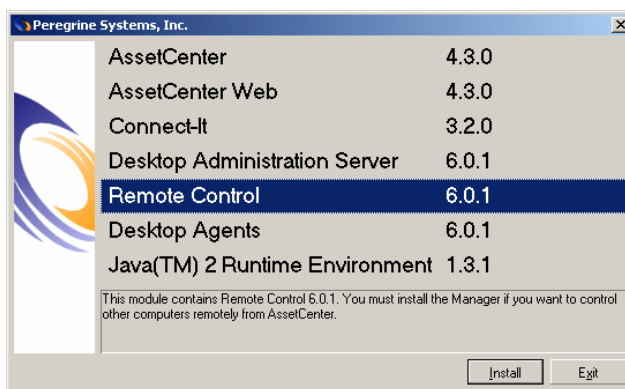
There are two different versions of the Agent module:

- The agents provided with version 4.x
This was provided with the Remote Management 4.x clients. These Agents are available for DOS, OS/2, Windows 95, 98, and NT.
- The agents provided with versions 5.5x and 6.x
These Agents are available for Windows 95, 98, NT, 2000 and XP.

Graphic installation of the Manager

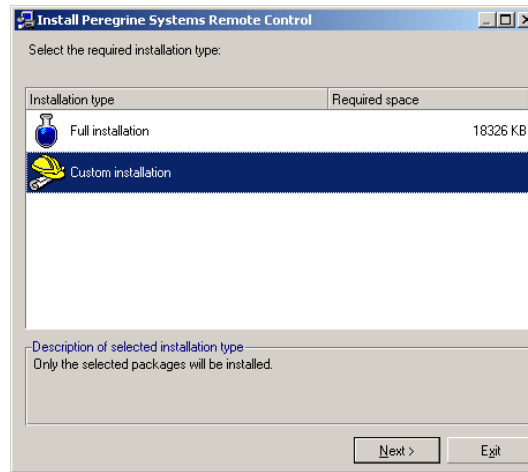
To install the Manager.

- 1 Insert the AssetCenter CD-ROM.



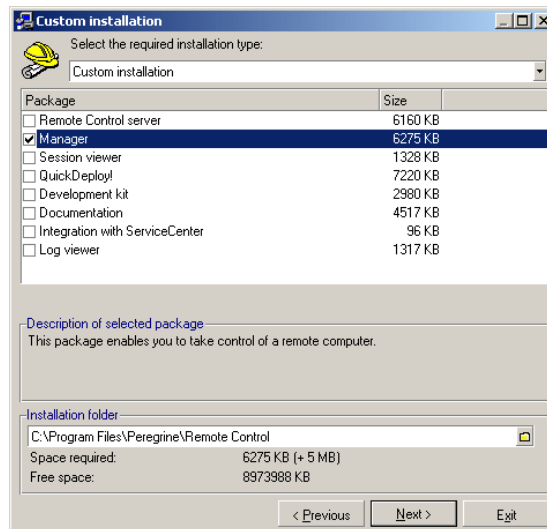
- 2 Click **Install** in the window that appears.

3 Select **Custom Installation**.

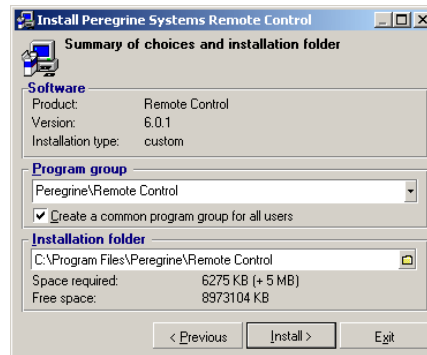


4 Click **Next**.

5 Select the **Manager** package.



6 Click **Next**.



7 Make sure that the installation folder is fine.

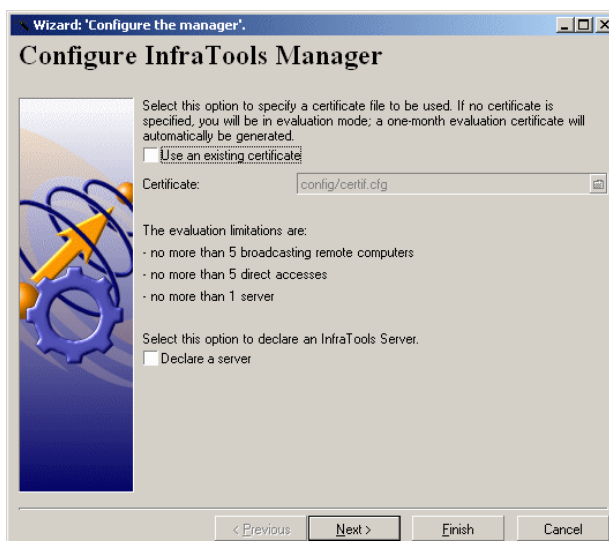
8 Click **Install**.

Launching the Manager

To use the Desktop Administration Manager:

- Select **Manager** from the Peregrine Remote Control program group.

The **Configure the Manager** page appears.



This wizard enables you to modify the Manager's default parameters. They are the following:

- TCP/IP communication protocol.
- No RSA security key is used.
- No server is defined.
- Remote control possible on version 4.x, 5.5x and 6.x agents.

If the default parameters suit you, click **Finish**.

If you do not like the default parameters, click **Next** to get to the pages where you can modify these parameters (communication protocol, for example). The second page of the wizard is the **Agent versions** page.

Agent versions

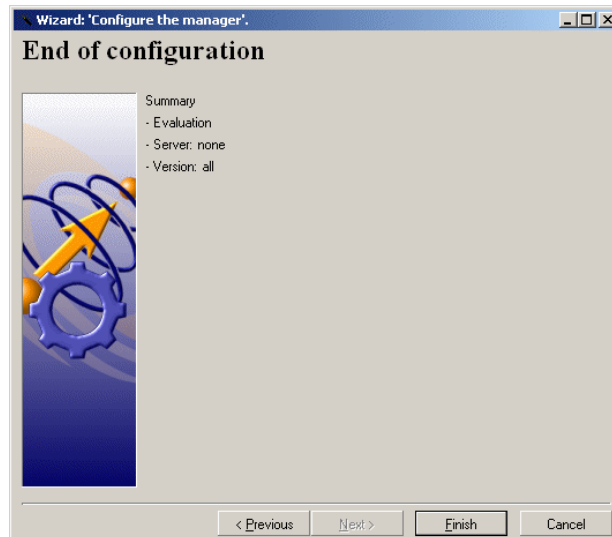


This page enables you to select the versions of the agents that the Manager will control. You can select from:

- **Version 4.x only**
- **Versions 5 or 6 only**
- **All versions**

Click **Next** to go to the **End of configuration** page.

End of configuration

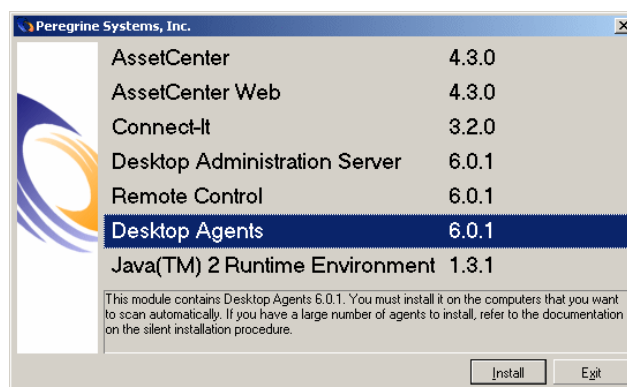


Click **Finish** on the page that summarizes your Manager's configuration.

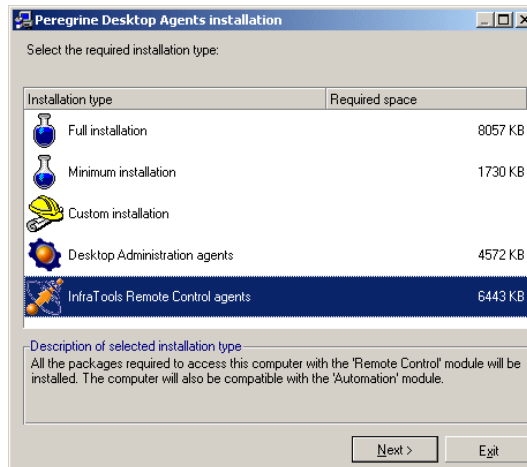
Graphic installation of the agent

To install the agent:

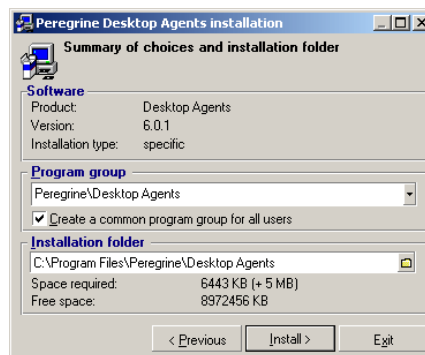
- 1 Insert the Desktop Administration installation CD-ROM



- 2 Click **Install** in the window that appears.
- 3 Select **Agents for Peregrine Remote Control**.



- 4 Click **Next**.



- 5 Make sure the installation folder for the agent is suitable.
- 6 Click **Install**.


Configuring the agent

Configuring the agent enables you to modify its default parameters. They are:


- TCP/IP communication protocol.
- Managers wanting to take control of a computer will not be asked their password.
- No RSA security key is used.
- No Remote Control server is declared.

If these default parameters suit you, go directly to the chapter **Using the graphical interface of the agent** of the User's guide.

If, on the other hand, these default parameters do not suit you, follow these directions to modify them:

1 Double-click , located on the Windows toolbar.

or

Right-click , located in the Windows toolbar. Then select **Restore** from the menu that appears.

2 Select the **Tools/ Configuration** menu in the window that appears.

3 Click **OK** in the window requesting your password.



If your agent was installed using an installation script, the password must be given to you by your administrator.

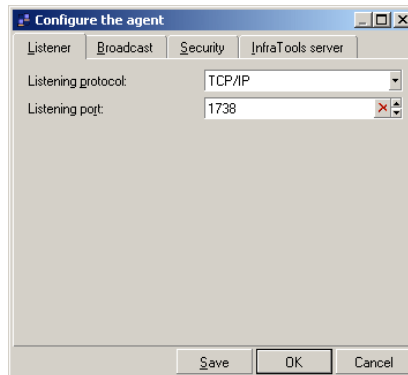
There are four tabs in the window that enable you to configure the following parameters:

- Listener parameters
- Broadcast parameters
- Security parameters
- The connection parameters to the **Remote Control** server.

At the bottom of each tab, the **OK** button enables you to finish the configuration at any time.

When you configure for a remote-control session between two computers, you only need to configure the listener and broadcast parameters.

Listener

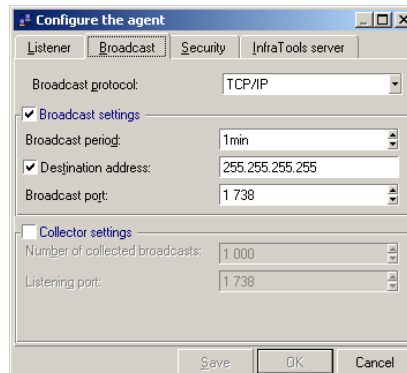


The Listener is the program that enables the agent to be controlled by the Managers picking up its broadcast signal. The Listener is a Windows service that runs permanently as a background service once the agent is installed on the computer.

The Listener's configuration consists of defining a communication protocol. The available communication protocols are as follows:

- **TCP/IP**
For this protocol, the listening port's default value is **1738**.
- **NetBIOS**
For this protocol, the name of the listening service corresponds to the name of the network computer.
- **Null Modem**
By default, the values of the serial port and its speed correspond to those of your computer.
- **Modem**
The list of modems corresponds to the modem drivers installed on your computer.
- **IPX/SPX**
The socket number's default value is **1244**.

Broadcast



The broadcast parameters correspond to the signals sent by the Agents on the network. To remotely control the Agent, the Agent must broadcast signals using the same protocol as the Manager.

The three available protocols are:

- **TCP/IP**
For this protocol, the listening port's default value is **1738**.
- **NetBIOS**
For this protocol, the listening name by default is **OLDRMBCST**.
- **IPX/SPX**
The socket number's default value is **1244**.

Unselect the **Collector settings** option.

Remote control by the Manager

You just installed the Manager on your computer and the agent on a remote computer. You can now take control over the remote computer and perform certain operations, which are described in this section.

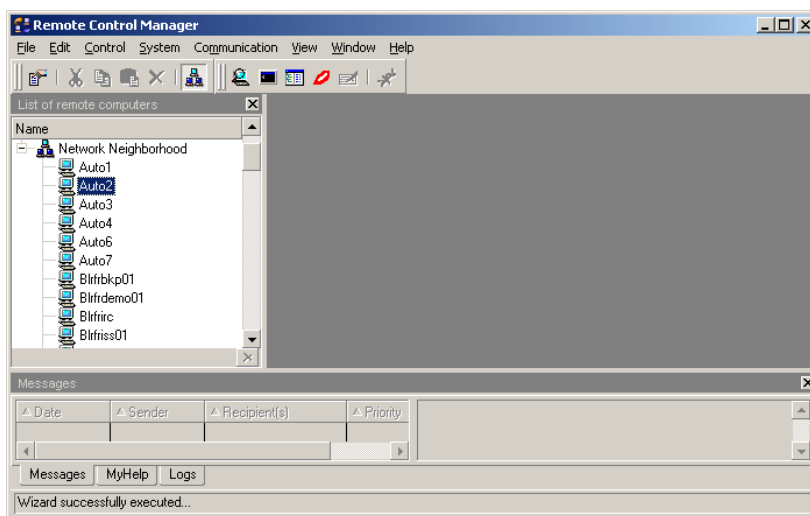
This section describes how you can use the Manager to:

- Take control graphically of a remote computer on your network neighborhood.
- Launch the Manager explorer.

- Start a terminal session.
- Chat with an Agent during a remote-control session.

To launch the Manager, select **Manager** from the Peregrine Remote Control startup menu.

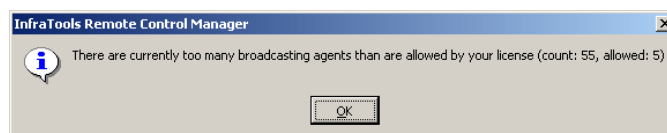
Figure 9.1. Manager window



 **Note:**

In evaluation mode, a dialog box appears every time that the certificate's limits have been exceeded. The limitations permit:

- Five computers on the network neighborhood.
 - Five computers by direct access.
 - Fifteen computers saved in the database whose access is secured by a server.
-

Figure 9.2. The evaluation-mode dialog box

Taking control graphically of a computer on your network neighborhood

The computers on which an agent is installed broadcast on the local network. The Manager detects the signal and can take control of them.

To take control graphically of a computer on your network neighborhood:

- 1 Launch the Manager.

The computer previously installed is visible in the Manager's list of remote computers under the **Network Neighborhood** node.

- 2 Double-click the computer.

or

Use the combination of keys **Ctrl + T** after having selected the desired computer.

Launching the Manager explorer

The Manager explorer resembles a Windows explorer, but instead of just displaying the hierarchy of the remote computer's drives, programs, folders and files, it allows the Manager to perform administrative tasks on it, too.

The explorer enables you to view:

- The drives of your computer and those of the remote computer.
- Certain system parameters of the two computers (system use, processing lists, services, etc.).

Depending on your control rights, you can copy, move or delete the files and folders on the remote computer.

To launch an explorer on a remote computer of your network neighborhood:

- 1 Launch the Manager.
- 2 Select the desired computer under the **Network Neighborhood** node.

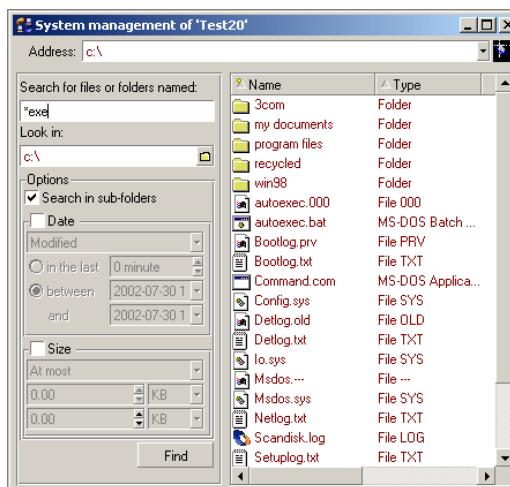
- 3 Right-click.
- 4 Select **Explorer** in the contextual menu that appears.

or

Use the key combination **Ctrl + S**.

To perform a search on the remote computer from the explorer:

- 1 Launch an explorer on a remote computer.
- 2 Select the explorer node corresponding to the remote computer.
- 3 Right-click.
- 4 Select **Search** from the contextual menu that appears.




Starting a terminal session

A terminal session is the equivalent to a DOS command prompt. If you need to enter commands on the remote computer and you are using a low-speed connection, it is more efficient to launch a terminal session rather than a command prompt in a graphical remote-control session.

To start a terminal session:


- 1 Launch the Manager.
- 2 Select the desired computer under the **Network Neighborhood** node.
- 3 Right-click.

- 4 Select **Terminal session** from the contextual menu that appears.
or
Click  on the toolbar.

Chatting with a remote computer

The Manager can chat with any remote computer using an instant messaging system.

To chat with a remote computer:

- 1 Launch the Manager.
- 2 Select the desired computer under the **Network Neighborhood** node.
- 3 Right-click.
- 4 Select **Chat** from the contextual menu that appears.
or
Click  on the toolbar.
- 5 Enter your message in the zone at the bottom of the chat window that appears.
- 6 Press **Enter** to send your message.
- 7 Wait for the remote user's response.

10 | Control rights

CHAPTER

In order to secure control sessions between the Manager and the remote computer Remote Control enables you, from AssetCenter, to:

- Define control rights.
- Assign control rights to these Manager groups over computers or computer groups.

Defining control rights

To access the remote-control rights, select **Elementary Remote Control rights** from the **Functions and favorites** menu in AssetCenter.

There is already a set of default rights in the Rights table, but you can also select specific remote control rights depending on the rights you want to grant to a Manager group later on.

This section presents:

- An explanation of each right.
- How they are used in AssetCenter.

Description of the control rights

Control rights are organized into the following categories:

Generic rights

There are three generic rights:

Do not ask for confirmation before connecting

If this option is cleared, the Manager must wait for the user of the remote computer to accept the remote control session.

Starting a terminal session

This option enables the Manager to start a terminal session on the remote computer.

Start a chat session

This option enables the Manager to chat with the user of the remote computer.

Graphical control rights

The graphical control rights are shown as a list of options to be selected.

Start a remote control session

This option enables the Manager to take graphical control of the remote computer.

Start full screen/windowed session

This option enables the Manager to start a full screen/windowed session on the remote computer. If this option is cleared, the Manager controls the active window at the start of the session.

Workstation

This sub-category relates to the different rights of the Manager concerning the remote computer.

Log off workstation

This option enables the Manager to log off from the workstation (a Windows session, for example) being controlled.

Allow connection even when a session is already open on the remote computer

Selecting this option enables the Manager to control the remote computer when the user is logged on (Windows, for example). This option must be used with the **Do not ask for confirmation before connecting** option. When the remote control session is started, the user of the remote computer must:

- 1 Close the current session.
- 2 Open a new session.
- 3 Let the Manager start the remote control session

Ctrl+Alt+Del

Selecting this option enables the Manager to use **Ctrl+Alt+Del** during the remote control session.

Shut down/Restart workstation

This option enables the Manger to shut down and restart the remote computer.

Blank screen

This option enables the Manager to blank the remote computer screen. This is useful when the Manager wants to hide a procedure or a password from the user of the remote computer.

Remote printing

This option enables the Manager to print documents on the remote computer on the local network.

Send/Receive contents of Clipboard

This option enables the Manager to send and receive the contents of the Clipboard of the remote computer.

Rights concerning the explorer

The rights concerning the explorer are those exercised by the Manager when launching the explorer on a remote computer.

Launching an explorer or a scan on a remote computer

This option enables the Manager to start a scan or an explorer on the remote computer.

Network neighborhood

This line relates to a Manager's rights on the remote computer's network neighborhood.

View network neighborhood properties

This option enables the Manager to see the Network Neighborhood properties of the remote computer.

Modify/Delete network neighborhood files or directories

This option enables the Manager to modify or delete files or folders on the Network Neighborhood of the remote computer.

Executing the network neighborhood file

This option enables the Manager to execute the network neighborhood files of the remote computer.

System

This sub-category relates to the management of the remote computer's operating system.

Services

The services options enable the Manager to:

- View the remote computer's services.
- Start or stop the remote computer's services.
- Install and uninstall the remote computer's services.

Devices

The device options enable the Manager to:

- View the remote computer's devices.
- Start or stop the remote computer's devices.
- Install and uninstall the remote computer's devices.

Event log

This sub-category relates to the remote computer's current event logs.

- Application

The options in this section enable you to:

- View the application log.
- Clear the application log.

- System

The options in this section enable you to:

- View the system log.
- Clear the system log.

- Security

The options in this section enable you to:

- View the security log.
- Clear the security log.

Netwatch

This sub-category relates to Netwatch on the remote computer.

Opening files

This option in this section enables managers to view files from Netwatch.

Sessions

The options in this section enable the Manager to:

- View the remote computer's current sessions.
- Kill the remote computer's current sessions.

Task manager

This category concerns the Task Manager of the remote computer.

Processes

This section enables the Manager to:

- View the remote computer's system or user processes.
- Kill the remote computer's user or system processes.

Application

This section enables the Manager to:

- View the remote computer's current applications.
- Kill the remote computer's current applications.
- Start the remote computer's applications.

Performance metering

This section enables the Manager to view the remote computer's performances.

System information

This section enables the Manager to view the remote computer's system information.

File

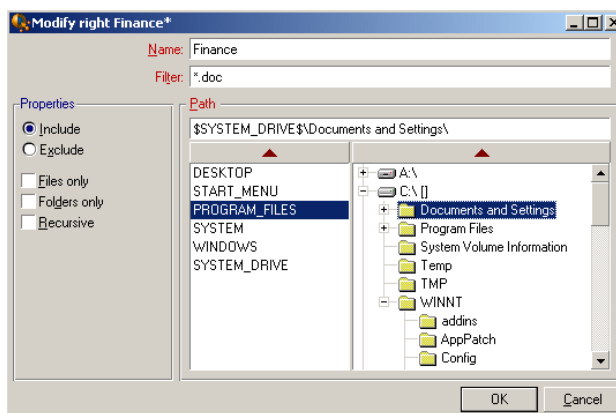
This section concerns the rights over the remote computer's files and folders.

To access the window to create rights over files and folders:

- 1 Double-click **File** in the rights window.
A window appears showing your computer's hierarchy.
- 2 Select the files or folders for which you want to create specific rights.

 **Note:**

We use the general assumption that files and folders are organized in the same way on all the remote computers. This tends to be the case in a company using a network operating system such as Windows NT.

Figure 10.1. Window to create rights over files and folders

To create a right over files:

- 1 Populate the **Name** field.
- 2 Populate the **Filter** field.
- 3 Populate the **Path** field.
- 4 Click **OK**. (The created right is displayed in the rights window.)
- 5 In the rights window, select the options of your choice. The options available for each created right are:
 - View files or folders
 - Modify or delete files or folders
 - Execute files

The "Name" field

This field enables you to indicate the name of a file or folder you want to exclude from the path.



Note:

You can use the asterisk * as a wildcard to replace any number of letters in a name or extension of a file or folder.

For example: To indicate all **.doc** files, enter "***.doc**".

You can use the question mark ? to replace an individual letter in the name of a file or folder.

For example: To indicate all four-letter file names beginning with "g", enter "g???.*".

If the **Include** option is selected, the right applies to the file or folder in the path indicated in the **Filter** field only.

If the **Exclude** option is selected, the right applies to all files or folder except the file or folder indicated in the **Filter** field.

For the selected path, you can also indicate whether the inclusion or exclusion concerns **Files only** or **Folders only**.

The **Recursive** option enables you to apply the filter to all files in all sub-nodes of the selected path.

The "Filter" field

To populate this field:

- 1 Select an element in the tree-structure of your computer.
- 2 Click the arrow above the pane showing the tree-structure.

The environment variables pane shows those variables most frequently found in a Windows environment. They make it possible to locate a path more quickly. For example: The PROGRAM_FILES environment variable enables you to quickly find the installation folder of an application.

To use an environment variable:

- 1 Select an environment variable.
- 2 Click the arrow above the pane showing the environment variables.

To create a new environment variable (which you can on all computers in your company if you want to):

- 1 Double-click the last variable in the list.
- 2 Enter the value of the variable in the text zone that is displayed.

Right options

For each right, the following options are available:

Edit rights

When you right-click on a right, a shortcut menu enables you to:

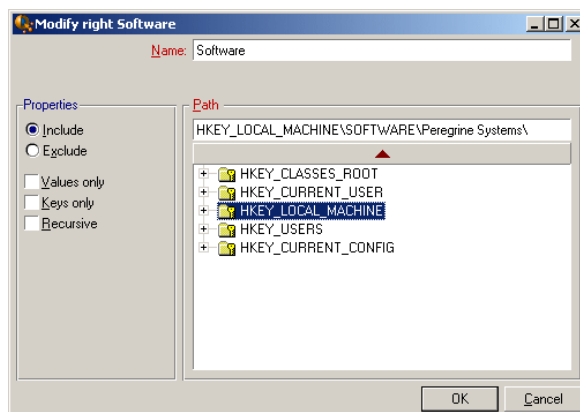
- Create a new right.
- Modify the selected right.
- Delete the selected right.
- Cut the selected right.
- Copy the selected right.
- Paste the selected right.

Registry

To access the window for the creation of rights for keys and for the values of a remote computer's Registry:

- 1 Double-click **Registry** in the rights window. A window will appear showing your Registry's organization.
- 2 Select the Registry's keys or values for which you want to create specific rights.

Figure 10.2. Window for the creation of rights for keys and for the values of a remote computer's Registry



To create a right over the Registry:

- 1 Populate the **Name** field.
- 2 Populate the **Path** field.
- 3 Click **OK**. (The created right is displayed in the rights window.)
- 4 Select the options of your choice for this right in the rights window.

The Path field

To populate this field:

- 1 Select one of the sub-branches of your Registry.
- 2 Click the arrow above the Registry pane.

The options in the **Properties** zone enable you to include or exclude values or keys in the selected Registry sub-branch.

The **Recursive** option enables you to include or exclude keys or values to sub-branches of a selected branch in the Registry.

Right options

For each right in the Registry, the following options are available:

- View values/keys
- Modify or delete values/keys

When you right-click on a right, a shortcut menu enables you to:

- Create a new right.
- Modify the selected right.
- Delete the selected right.
- Cut the selected right.
- Copy the selected right.
- Paste the selected right.

Editing control rights in AssetCenter

Control rights can be edited in AssetCenter and in the Manager.

Editing control rights in AssetCenter

You can edit control rights in AssetCenter by:

- Defining the database's default rights.
- Defining the control rights that you attribute to a Manager group.

- Defining the control rights that you attribute to a single Manager while creating that manager's certificate.

Editing control rights in the Manager

You can edit control rights in the Manager by:

- Editing the control rights on the remote computers of your network neighborhood.
- Editing the control rights of your direct accesses.



Note:

The ability to edit control rights in the Manager must be allowed for in the certificate used.

Assigning control rights

Once you have defined the control rights in the Rights table, you can then assign them to employee groups for computers or computer groups from within AssetCenter.

To do this, you must:

- Define employee groups.
- Assign control rights to these groups of employees, as well as to certain computers or groups of computers.

Definition of an employee group

These employee groups represent Manager groups who can take control of remote computers.

To define an employee group:

- 1 Select the **Portfolio/Groups** menu.
- 2 Click **New** to create a new group.
- 3 Indicate the name of your employee group.
- 4 Indicate a manager.
- 5 In the **Composition** tab, add the number of employees you want to include in your Manager group.

Assigning control rights to Manager groups

To assign control rights to a Manager group over certain computers or computer groups:

- 1 Select **Manager-group rights** from the **Functions and Favorites** menu.
- 2 Specify a name for your set of rights.
- 3 Select the Manager group to whom you want to assign these specific control rights.
- 4 Using the drop-down list, select the computer or computer group that the Managers can control according to their rights.
- 5 Select the rights that you want to assign to your Manager group.

11 | Using the Manager

CHAPTER

The Manager is the program that enables you to control remote computers on which the Desktop Administration or Remote Management agent is installed. The Manager is launched when the remote-control function is invoked from AssetCenter.

 Note:

You can launch the Manager by itself. In this case, you will only be able to control the computers in your own computer population.

This chapter covers the following points:

- How to start the Manager module for the first time.
- The interface of the Manager module.
- How to access remote computers.
- How to manage the list of remote computers.
- How to control a remote computer.
- How to communicate with the user of a remote computer.
- How to edit the properties of remote computers.

Starting the Manager module for the first time

To start the Manager module:

- Select **Manager** from the **AssetCenter** program group in the Windows Start menu.
- or
- Start **Iftman.exe** in the **Bin** sub-folder of the AssetCenter installation folder.

The configuration wizard starts automatically the first time you start the Manager module.

Configuring the Manager

This wizard enables you to:

- Declare a server if you are using the evaluation mode.
- or
- Select the certificate that the Manager uses to control remote computers.
- Indicate the version of the Agent installed on the computers over which the managers take control.

When you declare a server, the following pages will appear in the wizard:

- Configuration
- Declare a server
- Connection parameters
- Summary of the connection
- Agents versions
- End of configuration

Configuring the Manager



You declare a sever if using the evaluation mode. If you are using a certificate:

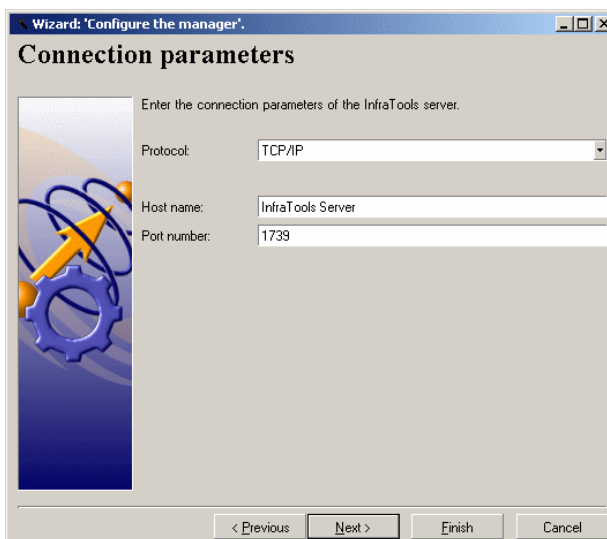
- Either the server is already declared in the certificate.
- Or you declare it by selecting **New/Remote Control server** from the **File** menu in the Manager.

Declare an Remote Control server



Indicate the name of your server on this page.

Connection parameter



This page enables you to indicate how the Manager connects to the computer hosting the server.

To specify the computer hosting the server, you can choose between the TCP/IP, NetBIOS and IPX/SPX protocols.

To declare a TCP/IP connection:

- 1 Indicate the name of the server host, which can be:
 - The IP address of the computer
 - The name of this computer on the network.
- 2 Indicate a port number.

To declare a NetBIOS connection you need to indicate the NetBIOS identifier.

This identifier is usually made up of the name of the server host and a suffix of up to 3 letters.

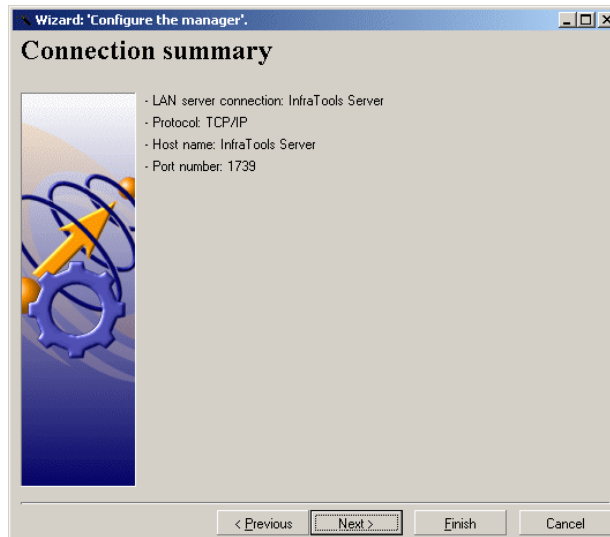
To establish an IPX/SPX connection:

- 1 Indicate the network number.
- 2 Indicate the node number.
- 3 Indicate the socket number.

The connection to the server is then tested:

- If the connection succeeds, the **Summary of the connection** page is displayed.
- If the connection fails, an error message is displayed.

Summary of the connection



This page summarizes your server connection.

Agents versions

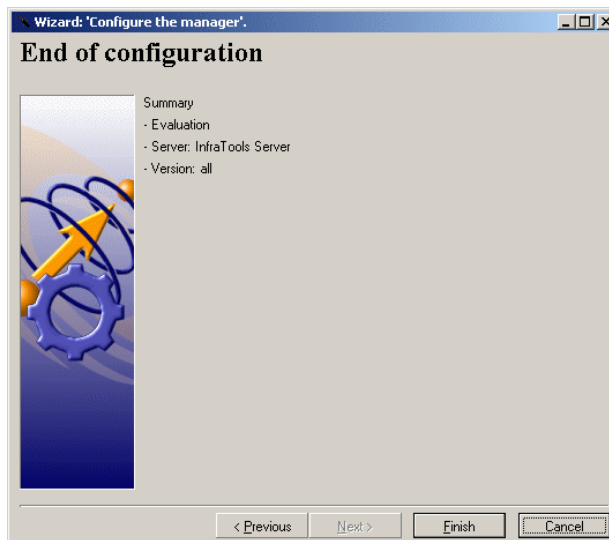


This page enables you to indicate the version of the Agents of which the Manager will take control.

You have the choice between three options:

- **Version 4 only**
- **Versions 5 or 6 only**
- **All versions**

Click Finish to obtain the **End of configuration** page.



If Peregrine Systems, Inc. provided a certificate, the following pages will appear in the wizard:

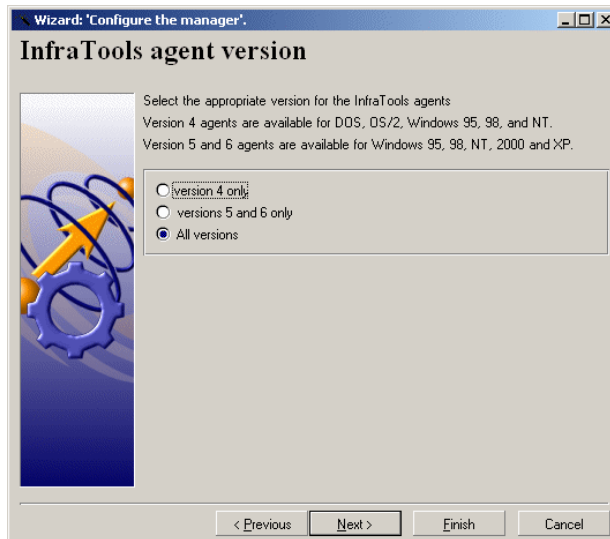
- Configuring the Manager
- AssetCenter agent versions

- End of configuration



- Select the **Use an existing certificate** option.
- Enter the name of the certificate you want to use in the **Certificate** field.
- Click **Next** to go to the **InfraTools agent version** page.

Agent versions

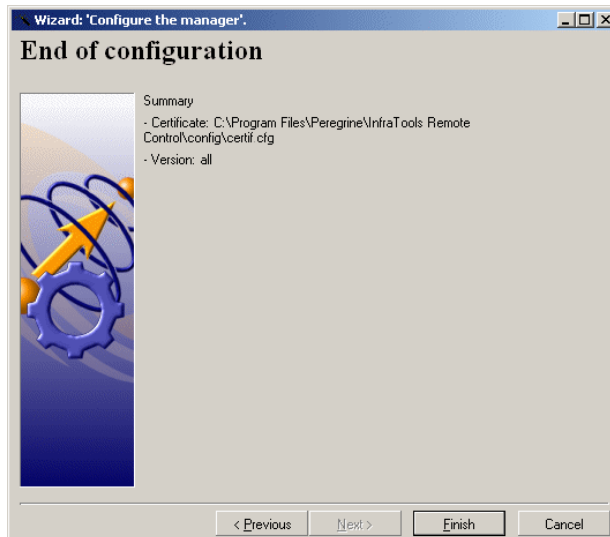


This page enables you to select the versions of the agents that the Manager will control. You can select from:

- **Version 4.x only**
- **Versions 5 or 6 only**
- **All versions**

Click **Next** to go to the **End of configuration** page.

End of configuration



Click **Finish** on the page that summarizes your Manager's configuration. The Manager is launched automatically.

The interface of the Manager

The main window of the Manager is made up of three panes:

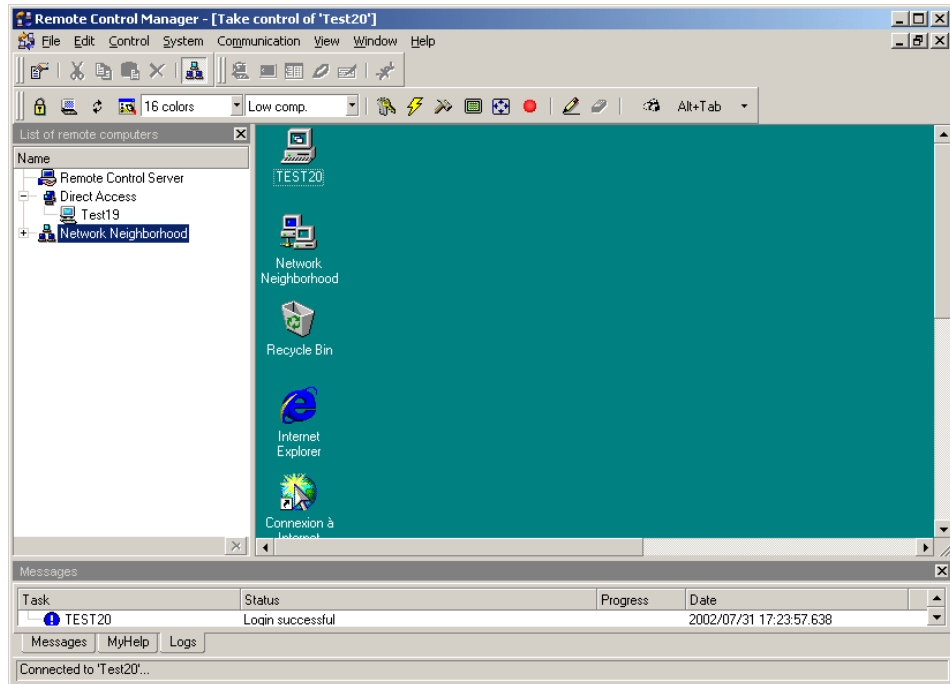
- A pane showing the list of remote computers.
- A pane where the Manager can control the remote computer.

In graphical control mode, this pane enables the Manager to see the screen of the remote computer being controlled.

- A pane composed of several tabs:
 - A **Messages** tab
This tab displays the messages that the employees connected to your Remote Control server exchange.
 - A **MyHelp** tab
This tab displays the agents of the remote computers that send a MyHelp message to the Manager.

- The **Logs** tab
This tab displays in detail the tasks performed by the Manager as well as the status bars that enable the completion of these tasks.

Figure 11.1. Main window of the Manager



The panes showing the list or remote computers and messages can be hidden using the **View** menu.

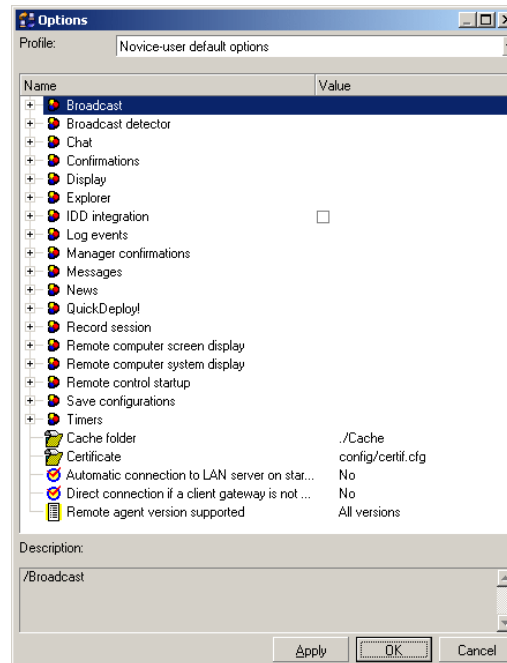
 **Note:**

Note on the organization of groups: It is possible to manage several thousand computers within a same given group. In order to obtain acceptable response times when accessing these groups, we recommend limiting the number of computers in each group to under 1000. If necessary, you can use AssetCenter to reorganize the groups of computers.

Manager options

To access the Manager's options, choose **Options** from the **Edit** menu.

Figure 11.2. Manager options window



Accessing remote computers

The Manager can identify a computer in three different ways:

- Via the neighborhood network

The agents transmit a signal on the local network thereby enabling managers to see them. The Manager connects directly to the remote computer using TCP/IP, NetBIOS, IPX/SPX communications protocols or a modem link or null modem.

- Via a broadcast detector

The broadcast detector is an agent that transmits an activity signals on a given network. It also collects broadcast signals from other agents on the

same network but which are not visible to the Manager. The Manager connects to this broadcast detector and can then access remote computers.

There are broadcast detectors for versions 4.x, 5.5x and 6.x:

- The broadcast detectors versions 4.x correspond to the client gateways of Remote Management versions 4.x.
- The broadcast detectors versions 5 and 6 are computers on which the Agent is installed and configured to collect the activity signals sent out by the Agents on their network. ► [Configuring the agent](#) [page 184]
- Via a server

The server provides the information from the database relating to the computers and the control rights assigned to the Managers and Manager groups. It verifies the control rights of the Manager and authorizes or refuses the connection to the remote computer.

The following diagrams summarize the different possible connection modes.

Access by broadcast detector

The role of broadcast detectors is to:

- Identify computers issuing broadcast signals.
- Relay this information to the Manager.

To view the list of computers identified by a broadcast detector, the manager must declare this broadcast detector (► [To declare a broadcast detector](#) [page 159]). Each Manager module can also visualize the computers emitting activity signals on its network: These computers appear under the **Network neighborhood** node in the list of remote computers.



Remote Management 4.x client gateways can be used as broadcast detectors. In this case, a greater number of communication protocols is supported. The Manager can also pass by a version 4.x Remote Management Manager gateway.

When using the broadcast detectors, the two following architectures are possible:

- Manager - Client gateway (4.x broadcast detector) - Agent
- Manager - Manager gateway (4.x broadcast detector) - Client gateway (5.5x or 6.x broadcast detector) - Agent

The two following diagrams show how to:

- Use a client gateway when a Manager uses a TCP/IP protocol and wants to access an agent using a modem connection, for example.
- Use a Manager gateway and a client gateway when a Manager using a TCP/IP protocol wants to access an agent, and neither gateway uses the same communication protocol.

Figure 11.3. Using a client gateway

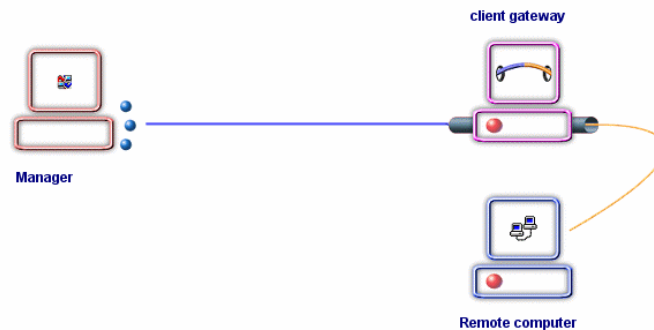
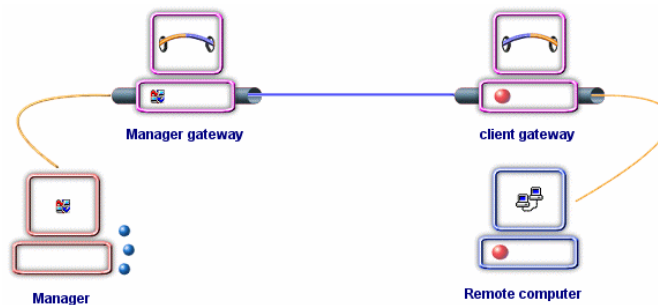


Figure 11.4. Using a Manager gateway and a client gateway



Which computers are identified by a broadcast detector?

The computers identified by a broadcast detector are those:

- On which the AssetCenter agent or the Remote Management client is installed (version 4.x agents).
- That are on the broadcast detector's network.
- That issue broadcast signals.

To configure the activity signals of the agents, refer to the chapter 'Using the graphical interface of the agent'.

Secure access

Which computers have secure access?

Those computers registered in a database, which the Manager accesses by connecting to the server, have secure access provided.

In a secure environment, Manager groups have specific rights over computers or computer groups.

The role of the server is to use information contained in its database or information from the user's NT login to:

- Identify the Manager and authorize access to the computers registered in the database.
- Assign specific rights over this computer.



Direct access

The direct-access method enables a Manager to control a computer without verification from a server. The information relating to these computers is contained locally in a certificate.

The certificate used by the Manager may or may not authorize the creation of direct accesses.



What is the utility of the direct-access method?

The direct-access method makes it possible to create a description of a remote computer on the workstation where the Manager is installed. It enables an off-site employee to take control of one of your computers from a laptop without having to go through the server or having access to the information in the database.

The number of direct accesses and the capability to edit them is limited by the Manager's certificate and your company's AssetCenter license.

Communication protocol settings

The Manager can take control of a 5.5x or 6.x agent using the following communication protocols:

- **IPX/SPX**
- **TCP/IP**
- **NetBIOS**
- **Modem**
- **Null modem**

For the version 4.x agents, the list of available protocols is larger:

- **APPC/APPN**
- **CAPI**
- **IPX/SPX**
- **TCP/IP**
- **NetBIOS**
- **Modem**
- **Null modem**
- **X25**

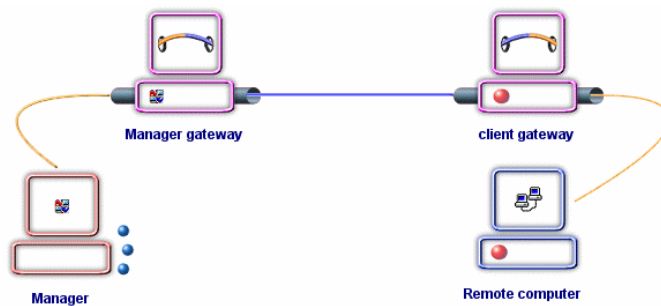
For each protocol other than the TCP/IP protocol, the Manager must configure their parameters. (Example: Indicate the modem used for the modem connections.)

If the Manager cannot connect directly to an agent (Example: the 4.x agents use the X25 protocol), the Manager must connect to:

- Either a client gateway by using a protocol that it supports.
- Or a Manager gateway when it cannot connect directly to an agent

The following diagram indicates the configuration type used in Remote Management versions 4.x.

Figure 11.5. Using gateways in Remote Management 4.x



Warning:

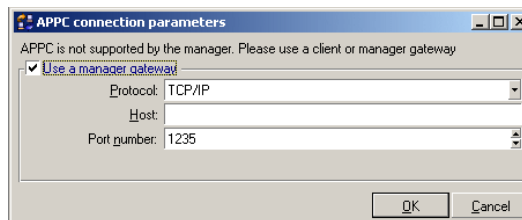
A Manager can only connect to one Manager per protocol.

To enter the communication-protocol parameters used by the Manager, select one of the protocols by selecting **Parameters** from the **Edit** menu.

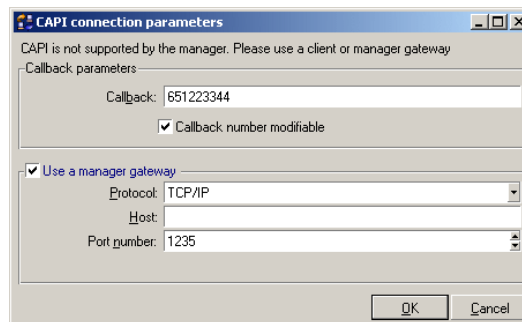
The protocols necessitating a configuration of the Manager are:

- **APPC/APPN**
- **CAPI**
- **IPX/SPX**
- **NetBIOS**
- **Modem (TAPI)**
- **Null modem**
- **X25**

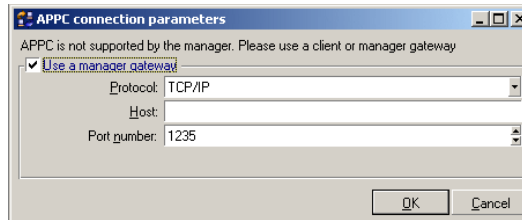
APPC/APPN protocol



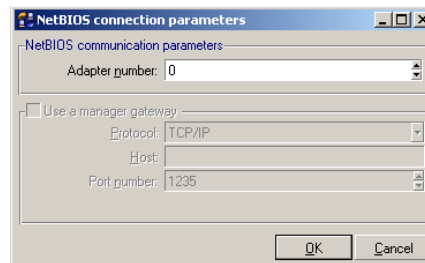
CAPI protocol



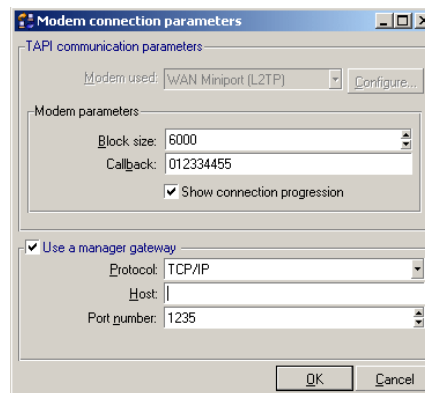
IPX/SPX protocol



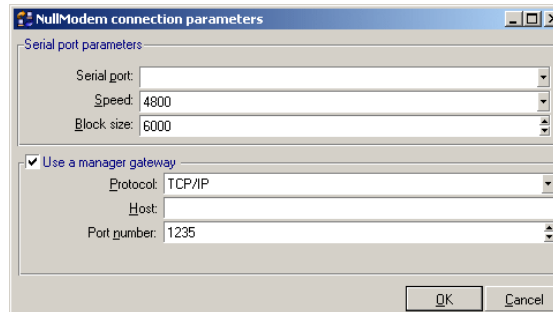
NetBIOS protocol



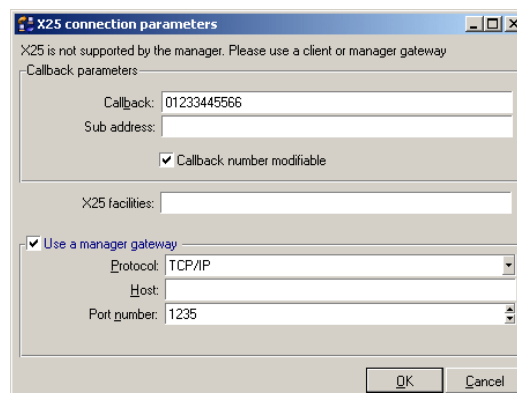
Modem



Null modem



X25



Managing the list of remote computers

According to the Manager's certificate, the Manager can manage the list of remote computers by:

- Creating and editing direct accesses if the certificate authorizes it.
- Declaring servers.

Each new Remote Control server gives access to new computers listed in a database.

- Declaring broadcast detectors.
Each new broadcast detector gives access to computers that can be controlled on LAN networks.
- Adding new connections to your direct accesses.
Several connections can be created for the same direct access. Depending on the performance of the connection, a manager can choose a given connection. Example: For the same direct access, a modem-type connection can be added to the TCP/IP-type connection declared during the creation of the direct access.

The Manager can also add a direct-access connection to a computer. In this way, it is possible to use different communication protocols to connect to a computer.

Creating a direct access

The certificate that you use may or may not enable you to create direct accesses. These direct accesses can be created in two different ways:

- From the computers on your network.
In this case, you can simultaneously create direct accesses on several computers.
- Manually naming one computer.
In this case, you can create one direct accesses.

These direct accesses can be created on the computers on which the Agent module is installed (either the version 4.x, 5 or 6).

Creating a direct access from computers on your network

Creating a direct access from the computers on your network enables you to use your network to dynamically retrieve the names of the remote computers to be controlled. If you do not have access to your network, this mode of creation is quicker since it enables you to create multiple direct accesses on one domain.

To create a direct access from the computers on your network:

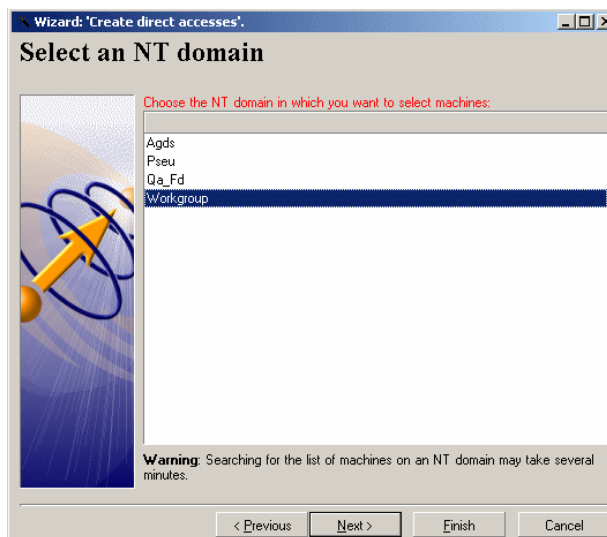
- 1 Select **New/Direct Access** in the **File** menu.
or
- 2 Right-click in the list of remote computers and choose **New/Direct access** from the shortcut menu that appears.

- 3 Wait for the **Create direct accesses** page to appear.

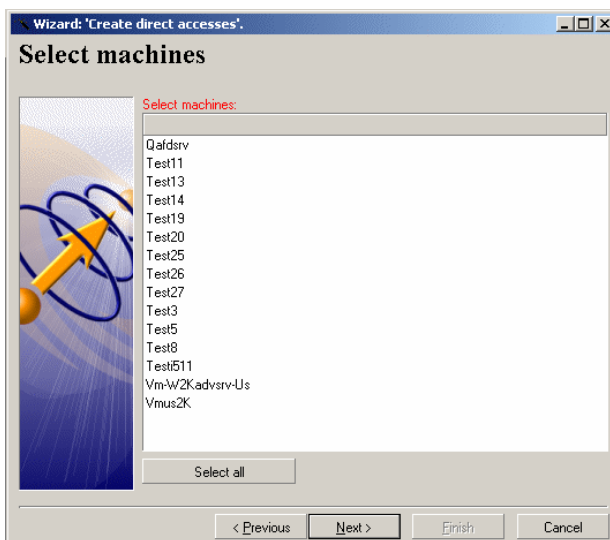


By selecting the **Advanced mode**, you can obtain additional pages.

- 4 Click **Next** to go to the **Select an NT domain** page.

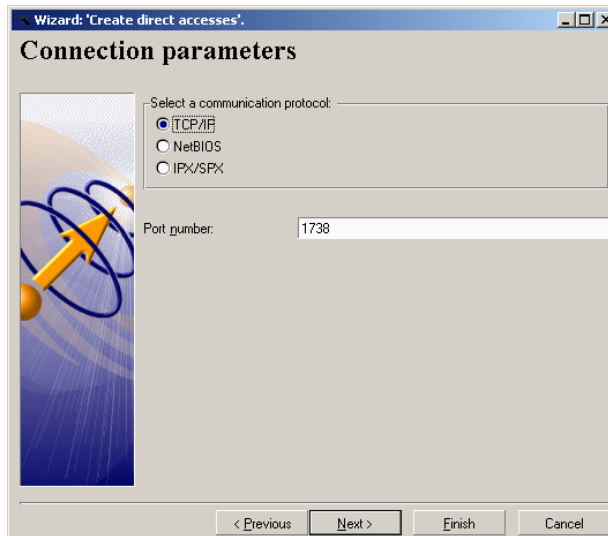


- 5 Select the domain which contains the remote computer for which you want to create a direct access.
- 6 Click **Next** to go to the **Select machines** page.



- 7 Select the remote computer for which you want to create a direct access.

- 8 Click **Next** to go to the **Connection parameters** (advanced mode) page.

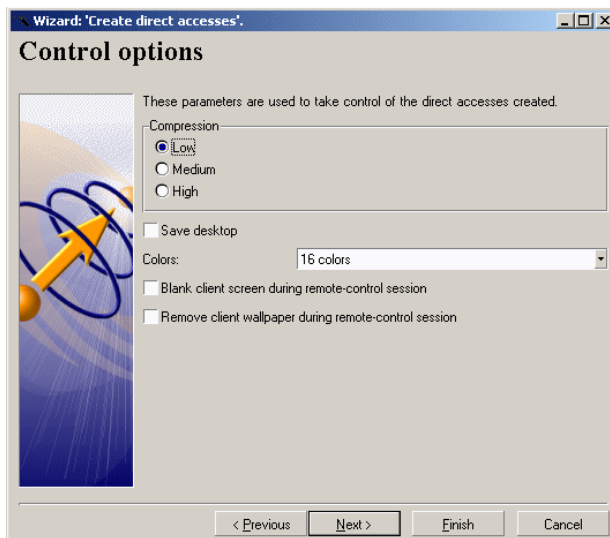


- 9 Enter the parameters that enable you to connect to one or more computers for which you want to create a direct access.

You have the choice between three connection protocols:

- **TCP/IP**
- **NetBIOS**
- **IPX/SPX**

- 10 Click **Next** to go to the **Control options** (advanced mode) page.



- 11 Select the control options of your choice.

 **Note:**

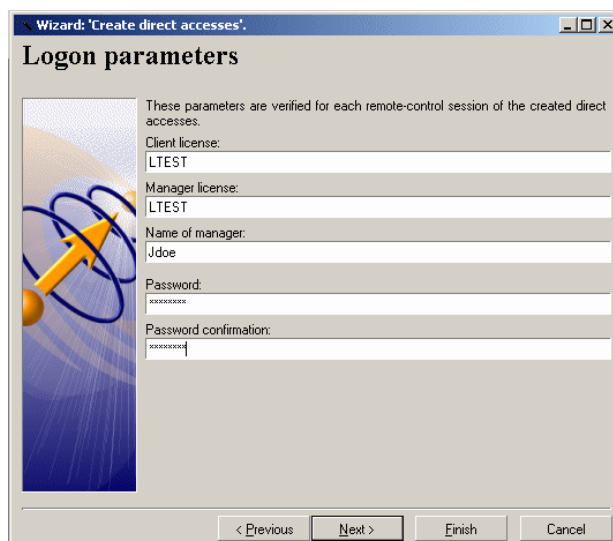
You must choose the control options according to your network's throughput.

If you use a modem connection, we recommend a 16-color resolution and a high compression.

If you connect to your LAN network, you can use a RGB resolution and a low compression.

- 12 Click **Next** to go to the **Logon parameters** (advanced mode) page.
This page is different depending on the agent version selected:

- Version 4.x



Wizard: 'Create direct accesses'

Logon parameters

These parameters are verified for each remote-control session of the created direct accesses.

Client license:
LTEST

Manager license:
LTEST

Name of manager:
Jdoe

Password:

Password confirmation:

< Previous Next > Finish Cancel

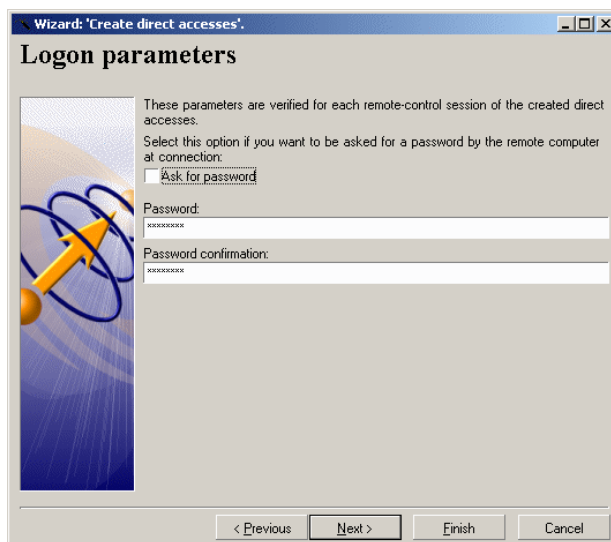
For this version, you must enter the following parameters:

- Client license
- Manager license
- Manager name
- Password (optional)
- Confirm password (optional)

 **Warning:**

If you use version 4.x agents, you must ask for a license from Peregrine Systems, Inc.

- Version 5.5x or 6.x



- In the case where the agent has a password, you have the choice between:
- Selecting the **Ask for password** option, which requires the Manager to enter the agent's password at the start of each remote-control session.
 - Entering a password in the **Password** and **Confirm password** fields. This option enables the memorization of the password and avoids having to enter it at each remote-control session.

- Click **Next** to go to the **Control Rights** (advanced mode) page.

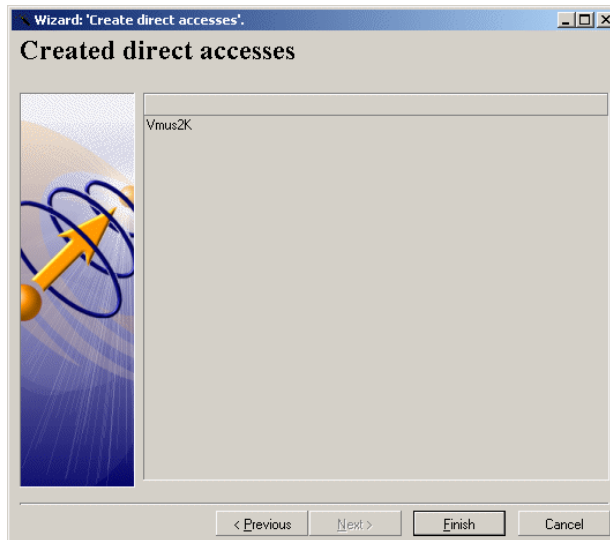


- Choose the rights that you want to exercise over the direct access(es) that you want to create.

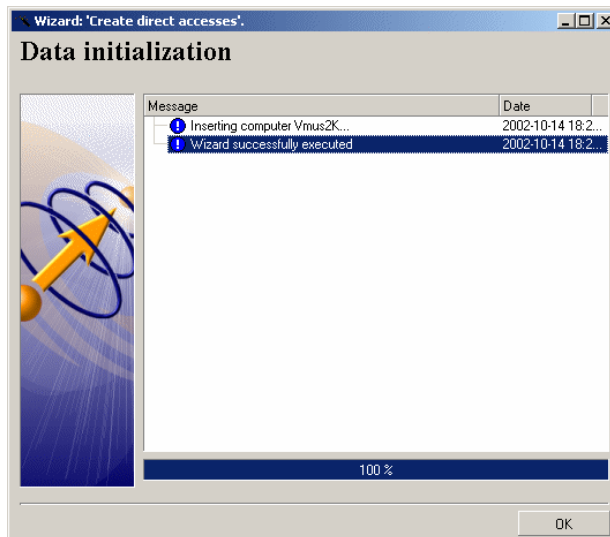
 **Note:**

By clicking **Default**, the Manager exercises the default rights defined in that manager's certificate.

- 15 Click **Next** to go to the **Create direct accesses** page.



- 16 Click **Finish** to launch the creation of the direct access.



Creating a direct access on only one computer

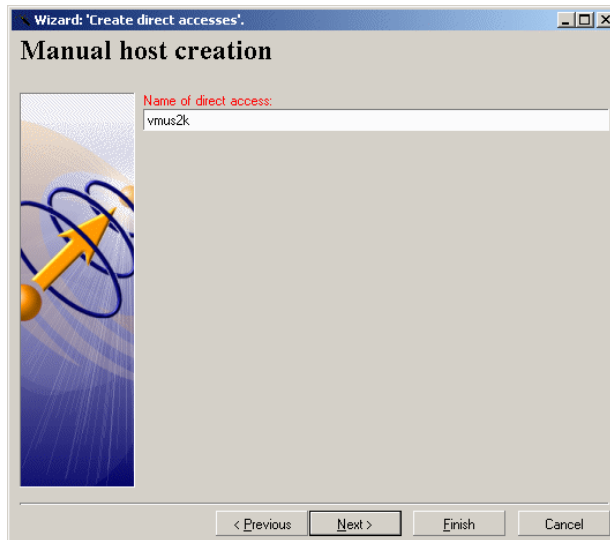
To create a direct access from the computers on your network:

- 1 Select **New/Direct access** in the **File** menu.
- 2 Wait for the **Create direct accesses** page to appear.



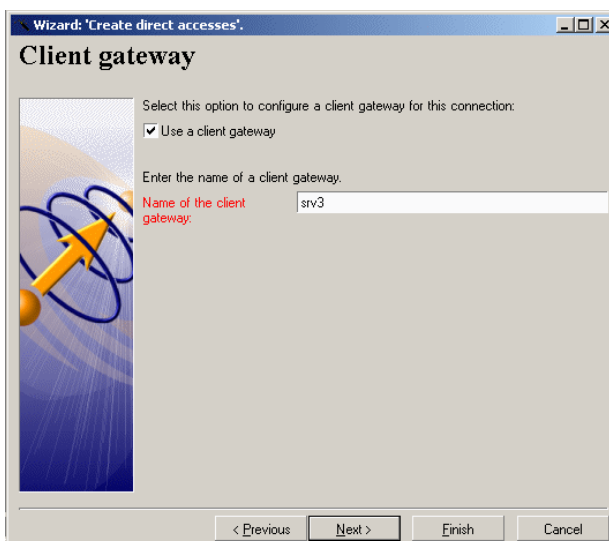
- 3 Unselect the **Machines on the network** option.
- 4 Select the **4** or **5 or 6** option depending on the version of the Agent installed on the computer for which you want to create a direct access.
- 5 You can select the **Advanced mode** option if you want. This option changes the data that you must enter in the wizard's pages if you want to create a direct access on a computer where a version 4.x Agent is installed.

- 6 Click **Next** to go to the **Manual host creation** page.



- 7 Enter the name of your direct access. This name appears in the manager's list of remote computers.

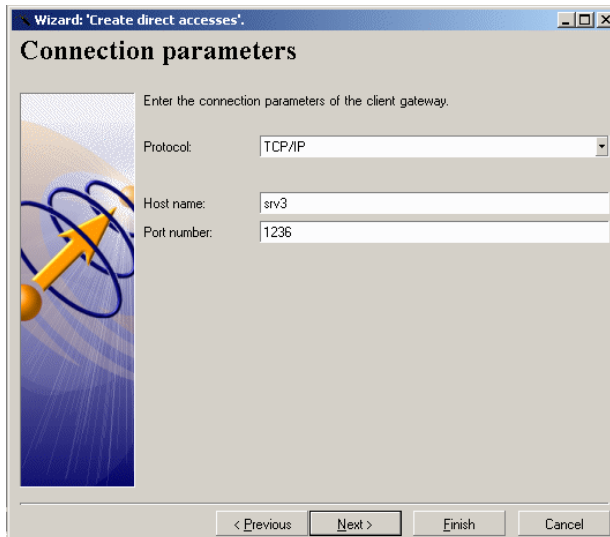
- Click **Next** to go to the **Client gateway** page (advanced mode for the 4.x agent only).



- Select the **Use client gateway** option if you want to access the remote computer by a client gateway.

You need a client gateway if you want the Manager to communicate with the agent used as a broadcast detector. This can be the case when a broadcast detector uses a modem connection.

- 10 Click **Next** to go to the **Connection parameters** page (advanced mode for the 4.x agent only).



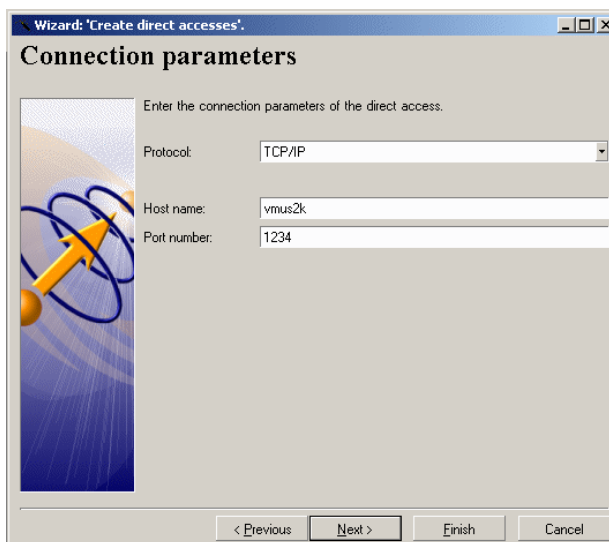
- 11 Enter the parameters that enable you to connect to a client gateway.
To connect to your client gateway version 4.x, you have the choice between six modes of connection:

- **TCP/IP**
- **Modem**
- **X25**
- **Null modem**
- **NetBIOS**
- **IPX/SPX**
- **APPC/APPN**
- **CAPI**

The connection parameters to a client gateway version 5.5x or 6.x are:

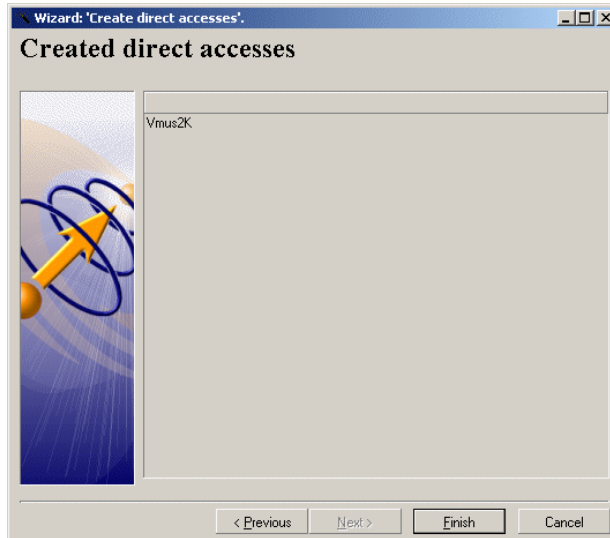
- **TCP/IP**
- **Modem**
- **Null modem**
- **NetBios**
- **IPX/SPX**

- Click **Next** to go to the **Connection parameters** page (advanced mode).

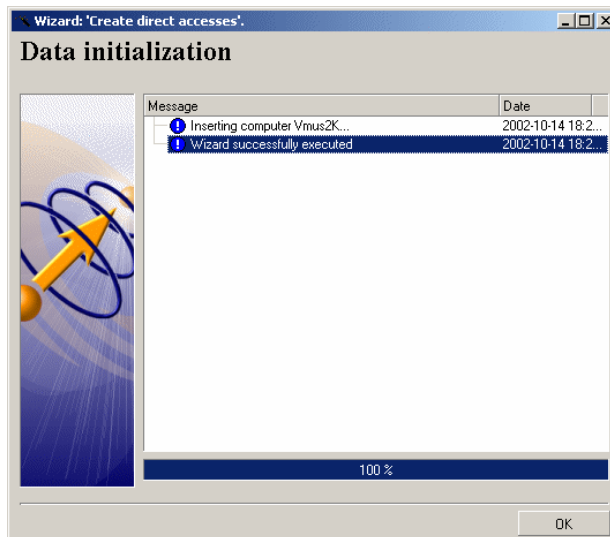


- Enter the parameters that:
 - Enable you to connect to the client gateway.or
 - Enable the client gateway to connect to the remote computer.You have the choice between three connection protocols:
 - **TCP/IP**
 - **NetBIOS**
 - **IPX/SPX**

- Click **Next** to go to the **Created direct accesses** page.



- Click **Finish** to launch the creation of the direct access.




Declare an Remote Control server

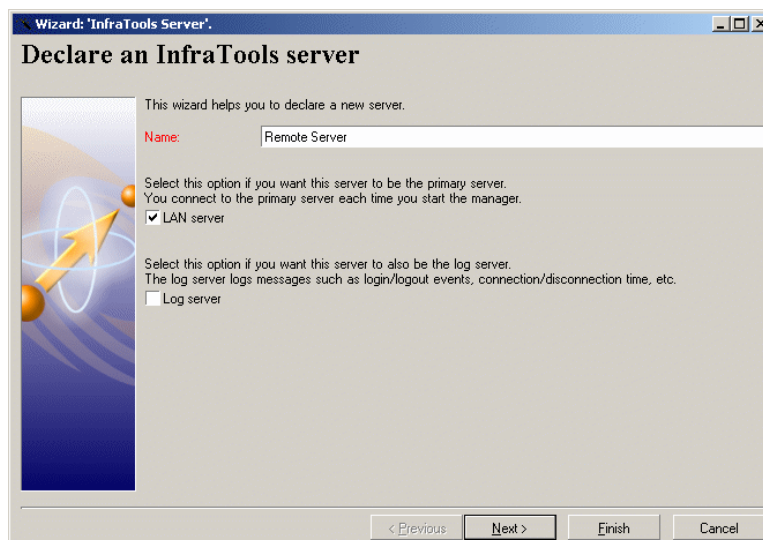
The server enables you to provide the Manager the information contained in the database relating to computers, Manager groups and control rights.

Once created, an additional node is visible in the Manager window. To declare a server:

- 1 Select **New/Remote Control server** from the **File** menu.

or

Click  on the toolbar



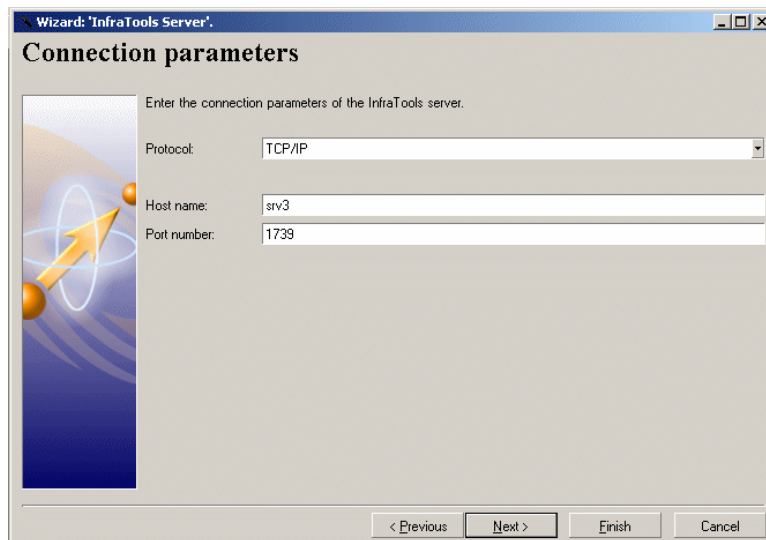
- 2 Enter the name of your AssetCenter server. This name will identify your server in the list of remote computers.

- 3 You can select the **LAN server** and **Log server** if you want.

If you select the **LAN server** option, one of the Manager options will enable you to connect automatically to this server every time the Manager is launched.

If you select the **Log server** option, all the Manager's remote-control sessions will be saved in the Events table managed by this server. This option is important when the manager works for an outside company, which needs to know the number and the durations of the remote-control sessions of your company.

- 4 Click **Next** to go to the **Connection parameters** page.

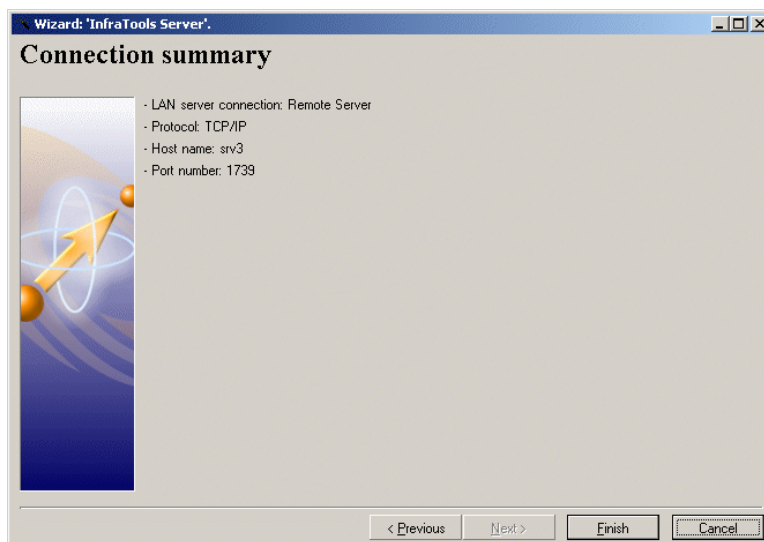


- 5 Enter the parameters that enable you to connect to your server.

The three available protocols are:

- **TCP/IP**
- **NetBIOS**
- **IPX/SPX**

- 6 Click **Next** to go to the **Summary of the connection** page.



- 7 Click **Finish**.


To declare a broadcast detector

In the Manager, you can declare a broadcast detector version 4.x, 5.5x or higher. Having the appropriate version of the broadcast connector makes it possible to detect the signals sent out by these versions. A version 4.x broadcast detector corresponds to a client gateway used in versions 4.x of Remote Management. A version 5.5x broadcast detector corresponds to an agent configured to be used as a broadcast detector on its own network. ► [Collector settings option \[page 186\]](#) of this manual.

To declare a broadcast detector:

- 1 Select **New/Broadcast detector** from the **File** menu.

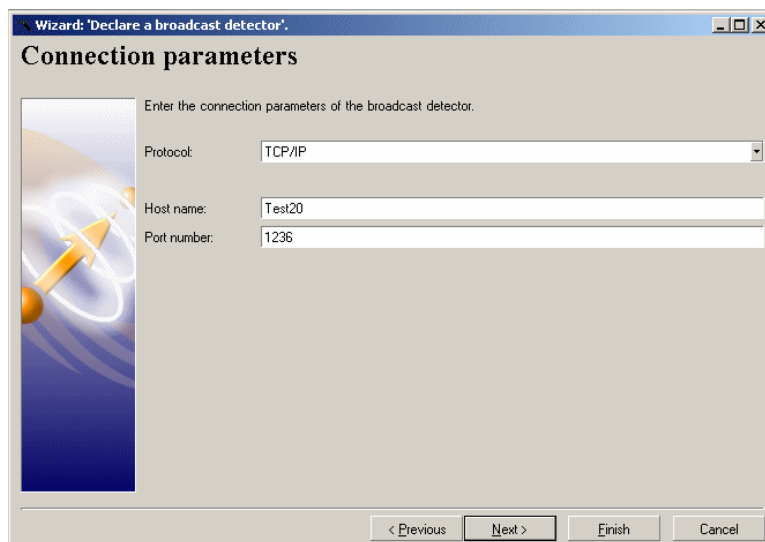
or

Click  on the toolbar



- 2 Enter the name of the broadcast detector as it appears in the list of remote computers.
- 3 Enter the version of your broadcast detector (version 4.x, 5.5x or higher).
- 4 If you declare a version 4.x broadcast detector (client gateway), you need to choose the communication protocol used by this detector in order to connect to the computers on its network. You can choose from three protocols:
 - **TCP/IP**
 - **NetBIOS**
 - **IPX/SPX**

- 5 Click **Next** to go to the **Connection parameters** page.



- 6 Enter the parameters that enable you to connect to your broadcast detector.

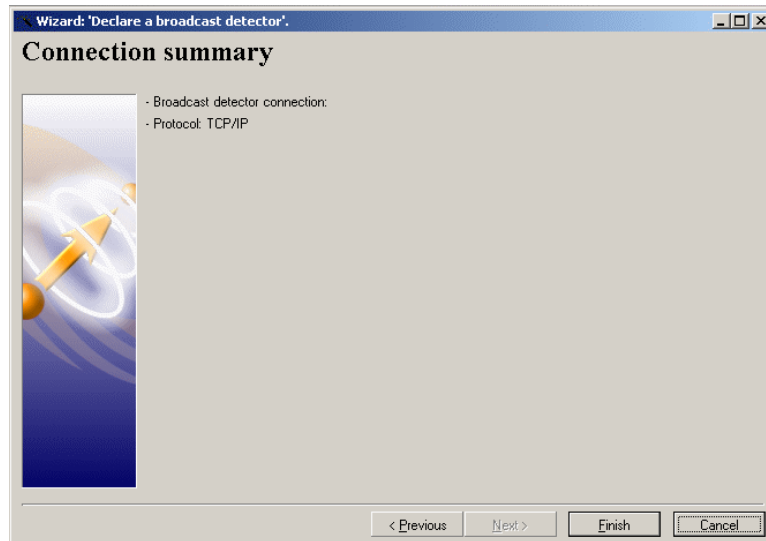
For a version 4.x broadcast detector, the available communication protocols are the following:

- **APPC/APPN**
- **CAPI**
- **IPX/SPX**
- **TCP/IP**
- **NetBIOS**
- **Modem**
- **Null modem**
- **X25**

For a broadcast detector version 5.5x or higher, the available communication protocols are the following:

- **IPX/SPX**
- **TCP/IP**
- **NetBIOS**
- **Modem**
- **Null modem**

- 7 Click **Next** to go to the next page.




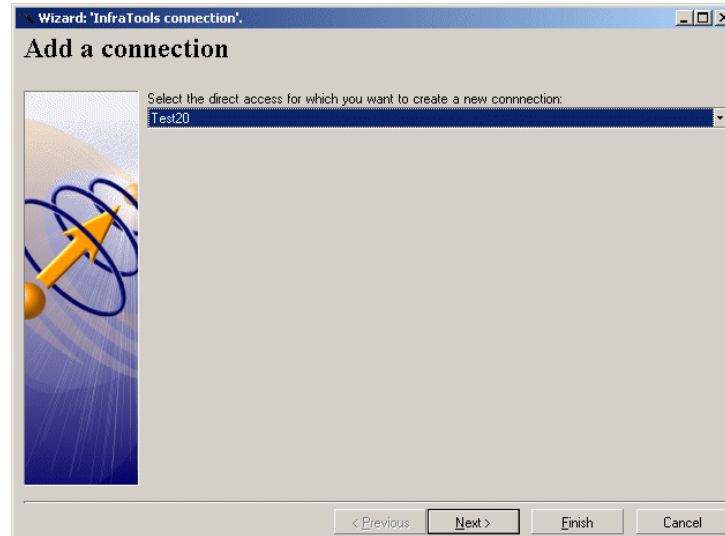
- 8 Click **Finish**.

Adding a new direct-access connection

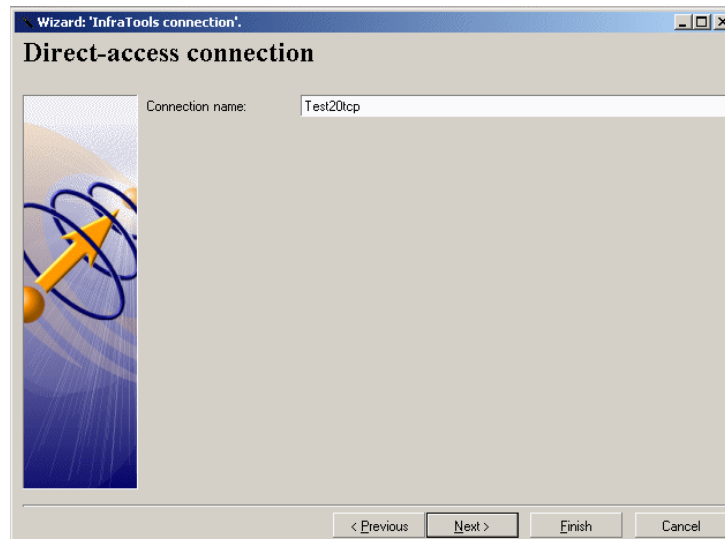
To add a direct-access connection to a computer:

- 1 Select **New/Connection** from the **File** menu.
or

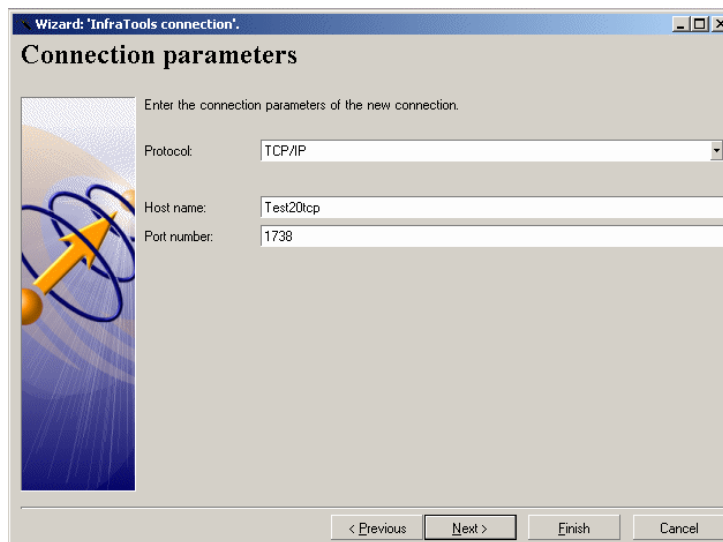
Click  on the toolbar



- 2 Select from the drop-down list the direct access for which you want to create a new connection.
- 3 Click **Next** to go to the **Direct-access connection** page.



- 4 Enter the name of the new connection.
- 5 Click **Next** to go to the **Connection parameters** page.

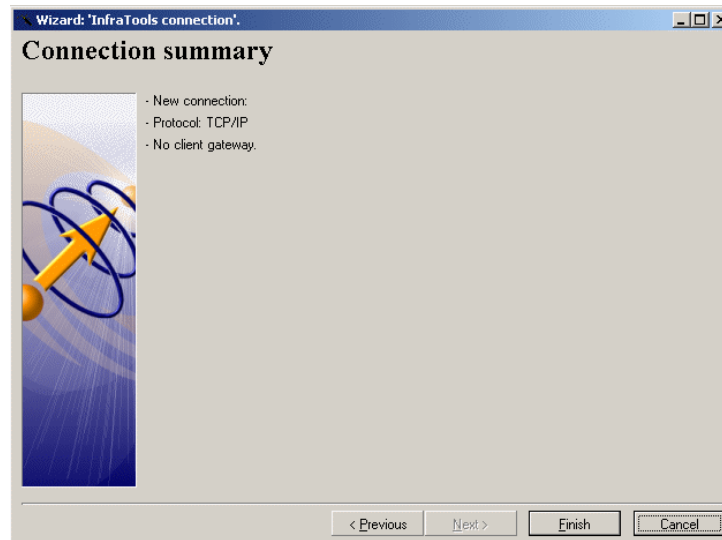


- 6 Select the communication protocol you want to use to connect to your direct access.

The available communication protocols are:

- **IPX/SPX**
- **TCP/IP**
- **NetBIOS**
- **Modem**
- **Null modem**

- 7 Click **Next** to go to the **Summary of the connection** page.



- 8 Click **Finish**.

Controlling a computer

To take control of a computer:

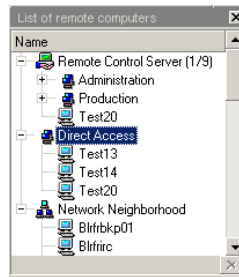
- 1 Select it in the list of remote computers.
- 2 Choose the control mode from the **Control** menu.

or

Click the icon on the toolbar corresponding to the required control mode.

or

Double-click the computer in the list to take graphical control.

Figure 11.6. List of remote computers

Graphical control

The graphical control method enables you to view the screen of the remote computer in the control pane.

The available control rights and options depend on the manager's certificate.

The manager's certificate also governs whether the manager can edit the options and control rights.

What is the utility of the graphical-control method?

When you control a computer graphically, it is equivalent to being in front of the remote computer: You can see the screen, control the mouse and the keyboard. This enables you to:

- Show the user how to use an application.
- Use the applications on the computer being controlled.

Control options

The graphical control options enable you to optimize the data-transmission speed between your computer and the remote computer.

You can only edit the default control options for the network neighborhood, broadcast detectors, or direct accesses if allowed to do so by your certificate.

To edit the graphical-control options for a direct access:

- 1 Select this computer in the list of remote computers.
- 2 Choose **Properties** from the **File** menu.

or

Right-click the computer, then choose **Properties** from the shortcut menu.
Select the **Control options** tab (in the creation wizard) or **Configuration** (when editing properties).

To edit the graphical-control options for the network neighborhood:

- 1 Select the network neighborhood icon in the list of remote computers.
- 2 Choose **Properties** from the **File** menu.
or
Right-click, then choose **Properties** from the shortcut menu.
- 3 Select the **Default options** tab.


Graphical control rights

Your graphical control rights are defined either in your certificate or by Manager group to which you belong in the database.

Mouse and keyboard rights

When controlling a computer, you have the right to control its keyboard and mouse.

To lock the remote computer's keyboard and mouse:


- Select the **Control/Lock mouse and keyboard** menu.
or
- Click  on the toolbar

Display options for the remote computer screen

Once the remote computer's screen is displayed in your control pane, you can resize it and change the number of colors displayed.

Fitting the screen to the control pane

To fit the remote computer's screen to the control pane:

- Select **Stretched display**.
or
- Click  on the toolbar

Changing the number of colors displayed

To change the number of colors displayed in the Manager's remote-control pane:


- 1 Select the **Control/Colors** menu.
- 2 Then select one of the available values in the **Colors** option.

or

- 1 Select the option of your choice from the drop-down list corresponding to the color depth on the toolbar.


Refreshing the screen

To refresh the screen:

- Select the **Control/Refresh** menu.
- or
- Click  on the toolbar

Displaying the remote screen in full-screen mode

To display the remote screen in full-screen mode:

- Select the **Control/Full-screen display** menu.
- or
- Click  on the toolbar

To switch the remote screen back to the control pane:

- Press: Alt+Tab.
- or
- Double right-click.

Full-screen detection

When a remote computer switches to text mode, the control pane takes this change into account.

By default, full-screen detection for the remote computer is done in Read/Write mode.

To change the default mode, select **Full screen detection** from the **Control** menu. Four detection modes are available:


- By accessing the graphics driver.
- By analyzing graphics memory.

- Without using the graphics driver.
- Windows 95/98

Terminal session

Launching a terminal session enables you to execute command lines on the controlled computer. This control mode is the equivalent to launching a command prompt on the remote computer.

To start a terminal session:


- Select the computer in the list of remote computers.
 - Select **Session terminal** from the **Control** menu.
- or
- Click  on the toolbar

Execute commands from the displayed window.

Explorer

Accessing a remote computer via the explorer enables you to manage the computer's system.

To start an explorer on a computer:

- Select the computer in the list of remote computers.
 - Select **Explorer** from the **System** menu.
- or
- Click  on the toolbar

Inside the control pane, both a local explorer (the Manager's) and a remote explorer are displayed (see below).

You can manipulate elements according to your control rights.

The interface of the Manager

In Explorer mode, the control pane is separated into two sections:

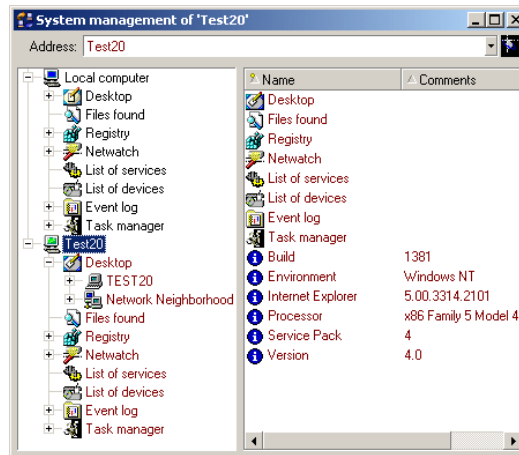
- A left pane that, by default, displays the list of both remote and local system objects.

The left pane can also display:

- Your list of favorites.
- A search window for local and remote files.

- A right pane showing the detail of the object selected on the left.

Figure 11.7. AssetCenter explorer window



Explorer menu

You can access the explorer's function via the **System** menu or via the shortcut menus displayed when you right-click the left or right pane of the explorer.

Explorer nodes

For each computer, the AssetCenter explorer has:

- A desktop
- The files found at the last search ► [To search for files or folders](#) [page 172]
- The Registry
- Netwatch
- A list of services
- A list of devices
- The event log
- The task Manager



Note:

For version 4.x agents, the explorer only shows the desktop and the files found.

Local explorer/Remote explorer

Each time you start an explorer session on the remote computer, a local explorer and a remote explorer are displayed.

To start a local explorer only, select **Local explorer** from the **System** menu.

Managing system objects on the remote computer

You can manage the remote computer's objects according to the rights given to you by your certificate for the remote computer.

To copy, paste, and delete folders and files, you can use the:

- Commands in the **Edit** menu.
- Commands in the shortcut menu that appear when you right-click in the detail pane.
- Icons on the toolbar.

You can also copy and paste files and folders by performing a drag-and-drop operation.

Managing the list of favorites

The list of favorites enables you to quickly find an object contained in one of the nodes of the local explorer.

To add a favorite to the list:

- 1 In the left pane, select a node in which you want to choose a favorite.
- 2 Right-click.
- 3 Select **Favorites** from the shortcut menu.
- 4 Select your favorite in the right pane.
- 5 Drag it to the favorites pane and to the folder of your choice.

Once you have your list of favorites, you can edit it and:

- Delete favorites.
- Change their icons.
- Organize favorites into sub-folders.

To edit the list of favorites:

- 1 Go to the left pane of the explorer.
- 2 Right-click.
- 3 Select **Favorites** from the shortcut menu.
- 4 Right-click.

- 5 Select **Edit favorites** from the shortcut menu.
- 6 Edit the favorites in the window displayed.

To create a sub-folder in the list of favorites:

- Click the **New** button.
- Enter a name in the **Name** field.
- Click **Modify**.

To search for files or folders

To search for a file or a folder in the explorer:

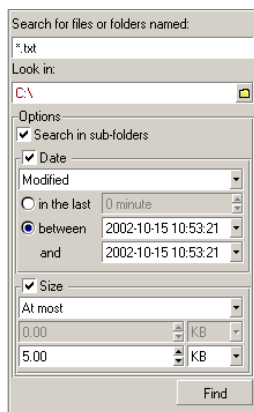
- 1 Go to the left pane of the explorer.
- 2 Right-click.
- 3 Select **Search** from the shortcut menu that appears.
- 4 Enter the search options in the window that is displayed.
- 5 Click **Find**.



Note:

The **Search** function in the **Edit** menu concerns computers in the Manager's list of remote computers.

Figure 11.8. Explorer search window



To configure the columns in the detail pane

You can add or remove columns appearing in the detail pane of the explorer.

To configure the detail pane:

- 1 Go to the detail pane.
- 2 Right-click.
- 3 Select **Configure** from the shortcut menu that appears.
- 4 In the window that is displayed, select the columns that you want to display in the detail pane.

Limitations of the AssetCenter explorer

You cannot copy-paste or cut-paste from the AssetCenter explorer to a Windows explorer or vice versa.

Editing the properties of remote computers

The properties of remote computers are:

- Connection parameters
- Control options
- Control rights

You can change the properties of the following types of remote computers:

- Computers accessible on the network neighborhood.
- Computers available by the broadcast method.
- Computers available by direct access.




Note:

Your certificate may forbid you from editing these properties.

Editing the properties of computers on the network neighborhood or via a broadcast detector


To edit the properties of computers on the network neighborhood or via a broadcast detector:

- 1 Select the **network neighborhood** or broadcast detector node.

- 2 Right-click, then choose **Properties** from the shortcut menu.
or
Click  on the toolbar
- 3 Edit the properties.

Editing the properties of a remote computer available via direct access

To edit the properties of a given direct access:

- 1 Select a direct access.
- 2 Right-click, then choose **Properties** from the shortcut menu.
or
Click  on the toolbar
- 3 Edit the properties.

To edit all direct accesses, select the node representing the direct accesses directly.

Editing the properties of the remote computers of an Remote Control server

The properties of computers entered in a database must be changed using Desktop Administration.

Other functions



When you control a computer graphically, the certificate you are using may allow you to:

- Save and replay a graphical remote-control session.
- Blank the remote screen.
- Lock the keyboard and mouse of the remote computer.
- Remove the wallpaper.
- Close a Windows session (log off).
- Restart the computer.
- Use a combination of keys on the remote computer.

Saving and replaying a remote-control session

Saving a graphical remote-control session lets the Manager replay it to verify the operations performed on the remote computer.

To save a session:


- Double-click the computer you want to control.
- Select the **Control/Save display** menu.
- or
- Click  on the toolbar
- Enter a title and description in the **Information about the logging of the session** window and click **OK**.
- To stop saving, unselect **Save display** in the **Control** menu.
- or
- Click  on the toolbar

The session is saved in an .rcr file in the InfraTools sessions folder, located by default in the user profile directory. You must use the Session viewer to read the .rcr file and replay the graphical remote-control session.

Blanking the remote screen

Blanking the screen of the remote computer enables the Manager to perform operations that they do not want to show the remote user (entering a password, changing a Registry key, etc.).

To blank the screen of the remote computer:


- Select the **Control/ Blank screen** menu.
- or
- Click  on the toolbar

Locking the keyboard and mouse

Locking the keyboard and mouse of the remote computer enables the Manager to perform operations without the risk of the remote user intervening.

To lock the keyboard and mouse:


- Select the **Control/Lock mouse and keyboard** menu.
- or

- Click  on the toolbar

To remove the wallpaper of the remote computer


Removing the wallpaper of the remote computer enables you remove the background of a screen that would otherwise slow down the speed of data transfer due to its size.

To remove the wallpaper of the remote computer:

- Select the **Control/ Remove wallpaper** menu.
- or
- Click  on the toolbar


To close a Windows session on this computer

To close a Windows session on the remote computer (log off):

- Select the **Control/ Close session** menu.
- or
- Click  on the toolbar

To restart the remote computer

To restart the remote computer:

- Select the **Control/ Restart remote computer** menu.
- or
- Click  on the toolbar

To use a combination of keys on the remote computer

To use a combination of keys on the remote computer, select one of the following options from the drop-down list on the toolbar. The different available combinations are:

- **Ctrl+Esc**
- **Ctrl+Alt+Del**
- **Alt+Esc**

- **Alt+Tab**
- **Alt+F6**

Communicating

The communication tools in AssetCenter enable the Manager to:


- Send messages to employees connected to the principle server.
- Converse with the users of remote computers being controlled.
- Receive and react to **MyHelp** messages.
- Draw on the remote screen of the computer being controlled.


To send a message

To send a message to the user of a remote computer connected to the principle server:

- 1 Select the **Communication/Message** menu.

or

Click  on the toolbar

Enter the alias of a recipient or a recipient group or click the magnifier  next to the **Recipient** field to select the alias.


- 2 Enter the message text
- 3 Click **Send**.

To chat with the user of a controlled computer

To chat with the user of a computer under graphical control:

- Select the **Communication/ Chat** menu.

or

- Click  on the toolbar

A chat window appears in which you can enter a message. To send this message, click **Send** and the message is sent directly to the user.

Any replies are displayed in the same window. You can reply by entering a new message in the same window.

If the user of the remote computer has not displayed the chat window in the foreground, you can sound a beep by clicking **Beep**.

Receiving and reacting to MyHelp messages

The user of a remote computer can send a **MyHelp** message to request help. To be able to respond to this message, the **MyHelp** option must be selected in the Manager's **Profile** tab in the database. If this is case, the message sent by the user is kept in the database's amTicket table. The manager can view this message in the MyHelp tab. The manager just needs to click the message to take control of the remote computer that sent the **MyHelp** message.

To respond to a MyHelp message:

- 1 Click the name of the agent or the message in the **MyHelp** tab.
- 2 Select the graphical control type you want to perform on this computer in the window that is displayed.



Note:

As soon as a Manager responds to a user's **MyHelp** message, the message disappears from the **MyHelp** tab of all Managers.


To draw on the screen of the remote computer

You can draw and write on the screen of the remote computer to highlight areas for the remote user.

To draw on the remote screen:

- Select the **Control/ Marker** menu.

or


- Click  on the toolbar

You can draw on the remote computer's screen using the mouse or directly type text that will appear on the screen.

To erase what you have drawn on the remote screen:

- Select **Eraser** from the **Control** menu.

or

- Click  on the toolbar

Managing news

The Manager can receive news items. These are organized by topic. Each topic corresponds to a tickertape displayed on the screen of employees connected to a server. News items are created and broadcast by the users of Desktop Administration.

To receive news

To receive news, the Manager or the user of the remote computer must subscribe to topics.

To subscribe to a news topic:

- Choose the **Communication/ Subscribe to news** menu.
- Select the topic of your choice in the window that is displayed.
- Click **OK**.

A tickertape corresponding to the topic to which you are subscribed is displayed on your screen.

Refreshing news

To refresh the news items being displayed, select **Refresh news** from the **Communication** menu.

Using the Manager from the command line



Note:

When you launch the Manager from the command line, AssetCenter is not launched, and therefore you do not have access to its functions.

To use the Manager from the command line:

- 1 Go to the folder where the **iftman.exe** program is located. Example:

```
C:\Program Files\Peregrine\AssetCenter\bin\
```

- 2 Run one of the command lines described in the following table.

Table 11.1. List of command lines that can be used with the Manager

Variable	Description	Possible values	Default value
General variables			
?, h, or H	Display help on using the Manager from the command line.		
close	Close the Manager when the control sessions are finished.		
connection	Remote computer connection name. By default, the first connection of the remote computer is selected.		
f	Text file containing a command to be executed later.		
host	Name of the remote computer to control.		
lftman	Start the Manager GUI.		
mode	Session mode started on the selected remote computer.	<ul style="list-style-type: none"> • gui Graphical control • Terminal Terminal session • Explorer Explorer • Scan IDD scanner • Viewlastscan See the last scanner launched on the remote computer. 	gui
verbose	Verbose mode for help and error messages.		
Variables concerning graphical control of the remote computer.			

Variable	Description	Possible values	Default value
blankscreen	Blanks the remote screen during control.		
colors	Number of colors used to display the remote screen.	16 256 RGB	256
compression	Data compression level	<ul style="list-style-type: none"> • low low • medium medium • high high 	low
fullscreen	Display the remote screen in full-screen mode.		
rmwallpaper	Remove wallpaper.		
savedesk	Save desktop for future sessions.		
speedopt	Enable speed optimization.		
stretch	Stretch the remote screen to the control pane.		
type	Access type	<ul style="list-style-type: none"> • da direct access • srv server 	
usedictionary	Save remote computer's images for future connections.		
Variables to use when the -srv mode is selected.			
srv	Name of the server you use to connect to the remote computer. If you do not specify this variable, your main server is selected by default.		

Variable	Description	Possible values	Default value
macaddr	Specify the MAC address of the specified remote computer.		
Variables to use when the -srv mode is selected.			
mode	Session mode started on the selected remote computer.	<ul style="list-style-type: none"> • gui Graphical control • Terminal Terminal session • Explorer Explorer • Scan IDD scanner • Viewlastscan See the last scanner launched on the remote computer. 	gui
viewscan	View the results file (.fsf) when the scan is finished.		

Remarks on certain variables in the installation script

-host:

- **da** mode (direct access)

The name of the computer must correspond to the name of the direct access as it appears in the Manager's list of computers.

- **srv** mode (server)

The name of the computer must be its full name as described in the database (SQL name: FullName).

-f:

This variable references an answer file edited with a text editor (Notepad, for example). This is useful for specifying a series of frequently used variables. For example: Entering a series of variables to control a given computer (-host: <computer name>), using a high compression level (-compression: high), blanking the remote computer's screen (-blankscreen), etc.

12 | Using the graphical interface of the agent

CHAPTER

The agent is made up of two component parts:

- The Listener server, which runs as a background task like a Windows service on your computer.
- The graphical interface that enables you to communicate with other AssetCenter users in your company.

You can start the graphical interface of the Agent in three different ways:


- 1 Select **Agent** from the **AssetCenter** program group in the Windows Start menu.
- 2 Right-click the # icon on the Windows toolbar and select **Restore** in the menu that appears.
- 3 Start **Iftagt.exe** located in the **Bin** sub-folder of the AssetCenter installation folder.

The graphical interface of the Agent enables you to:


- Protect, in read and in write, certain files and folders.
- Send messages to users connected to your server.
- Send **MyHelp** messages to Managers connected to your server.
- View news topics broadcasted by your server.

Configuring the agent

To configure the agent:

1 Double-click , located on the Windows toolbar.

or

Right-click , located in the Windows toolbar. Then select **Restore** from the menu that appears.

2 Select the **Tools/ Configuration** menu in the window that appears.

3 Click **OK** in the window requesting your password.

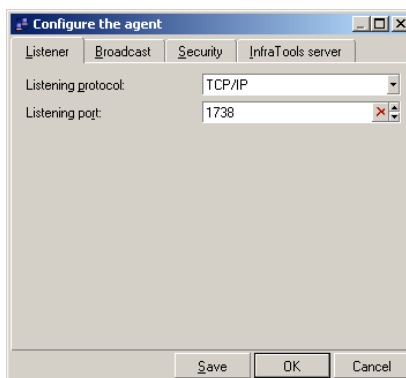
 **Note:**

If your agent was installed using an installation script, the password must be given to you by your administrator.

There are four tabs in the window that enable you to configure the following parameters:

- **Listener** parameters
- Broadcast parameters
- Security parameters
- Remote Control server and connection parameters

Listener

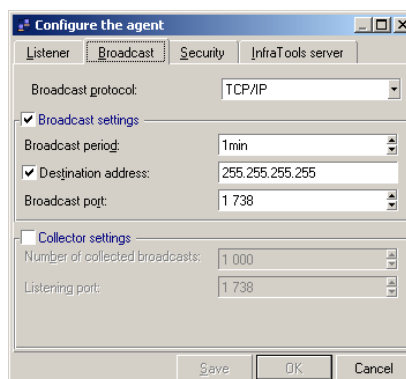


The Listener is the program that enables the agent to be controlled by the Managers picking up its broadcast signal. The Listener is a Windows service that runs permanently as a background service once the agent is installed on the computer.

The configuration of the Listener consists of defining the listening protocol:

- **TCP/IP**
For this protocol, the listening port's default value is **1738**.
- **NetBIOS**
For this protocol, the listening name by default is **OLDRMBCST**.
- **Null Modem**
For this protocol, the default values of the series port and its speed are **COM1** et **1200**.
- **Modem**
The list of modems corresponds to the modem drivers installed on your computer.
- **IPX/SPX**
The socket number's default value is **1244**.

Broadcast



The broadcast parameters correspond to the signals sent by the Agents on the (broadcast) network. These signals are picked up by the Manager via the

Network neighborhood, via the list of remote computers or via a broadcast detector.

In order for a computer to send activity signals:

- 1 Select a broadcast protocol.

The three protocols that enable the Agent to broadcast an activity signal are the following:

- **TCP/IP**

For this protocol, the listening port's default value is **1738**.

- **NetBIOS**

For this protocol, the listening name by default is **OLDRMBCST**.

- **IPX/SPX**

The socket number's default value is **1244**.

- 2 Select the **Broadcast settings** option.
- 3 Choose the broadcast frequency by entering a duration in the **Broadcast period** field.

Unselect the **Collector settings** option.

Destination address option

The **Destination address** option enables you to restrict the broadcasting of activity signals to only one recipient or to a remote network. If this option is activated, the remote computer:

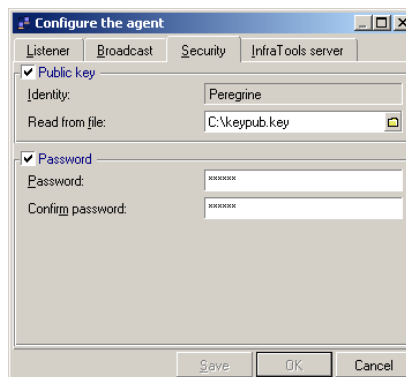
- Disappears from the **Network neighborhood** of the Manager, except for the Manager corresponding to the specific destination.
- Cannot be picked up by a broadcast detector other than the one that corresponds to the specific destination.

Collector settings option

The **Collector settings** settings option enables an Agent to be used as a broadcast detector. Depending on the protocol selected for the Agent module, you can enter a parameters enabling the Agent to detect the activity signals of other Agents on the network. Depending on the broadcast parameter selected, you can indicate:

- A port number for the **TCP/IP** protocol.

Security



The Agent's security is ensured with:

- An optional password

This password will be required by:

- All the Managers who want to take control of your computer. (In certain cases, the password is saved in the Manager's certificate.)
- The Agent user each time that the user selects a command from the **Tools** menu.
- A public key

This security key must be provided by your database administrator. The security key generated with AssetCenter must be included in the certificates of the Managers who take control of your computer. It enables you to:

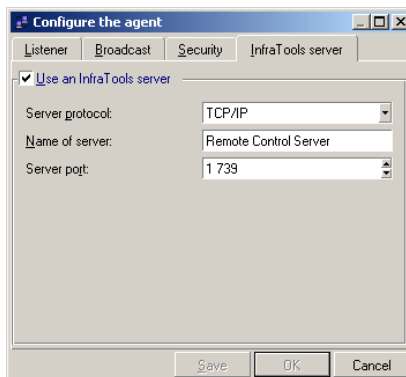
- Forbid a remote-control session on your computer by a Manager whose certificate contains a security key that differs from your own.
- Encrypt the data that you exchange with the Manager (Example: the transfer of files via the explorer).

To enter the security parameters:

- 1 Select the **Password** option.
- 2 Populate the **Password** and **Confirmation** fields. The Manager will be prompted for this password at the start of a remote-control session on your computer (graphical control, explorer or terminal session).
- 3 Select the **Public key** option.

- 4 Populate the **Read from a file** field by indicating the path of the file that contains the encryption key.
- 5 Click **OK**.

Remote Control server



This tab enables you to define the connection parameters of the Agent to the server.

Select an option from the drop-down list of the **Protocol** field. The three available options are:

- **TCP/IP**

If you select this option, you must populate two fields:

 - **Host name**

Indicate the number of computers on which you want to install your server.
 - **Port number**

Indicate the number of the port used by the server on the host. By default, the value of this port is **1739**.
- **NetBIOS**

If you select this option, you must indicate your NetBIOS identifier.
- **IPX/SPX**

If you select this option, you must populate three fields:

 - **Network**

Enter the value '0' or the value corresponding to the number of your network.

- **Node**

Enter the MAC address of the computer on which the AssetCenter server is installed.

- **Socket**

Enter the value '1234'.

Save the configuration of the Agent in an answer file.

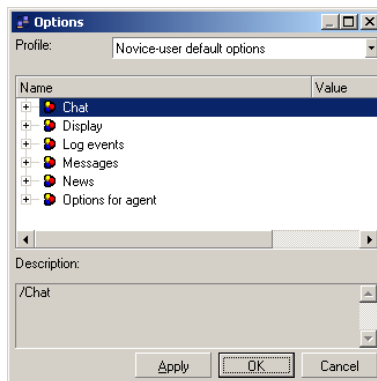
You can save the configuration of the Agent in an answer file (**.ans**). This answer file can be used to install from the command line the Agent module on other computers.

To save an answer file that contains the configuration of your Agent:

- 1 Enter your different configuration parameters.
- 2 Click one of the **Save** buttons at the bottom of all the agent configuration tabs
- 3 Enter the name of your answer file (the extension name of this file is **.ans**) in the **Answer file for unintended installation** window.
- 4 Click **Save**.

Agent options

To access the Agent module options, select **Options** in the **Tools** menu.

Figure 12.1. Agent options window

The options of the Agent are organized in categories:

- **Display**
- **Chat**
- **Log events**
- **Messages**
- **News**
- **Options for agent**

To change an option's value:

- 1 Go to the line corresponding to the option of your choice.
- 2 Double-click the default value.
- 3 Enter a new value.
- 4 Click **Apply**.

or

Click another area in the options window.


To change the color of an option:

- 1 Click the color box that represents the color selected by default.
- 2 Select one of the colors in the drop-down list.

or

Choose a color in the colors window that appears when you click **More** in the drop-down list.

To change the font options selected by default for the characters:

- 1 Double-click the value defined by default.
- 2 Click .
- 3 Choose a font, a font style and a size of character in the window that appears.
- 4 Click **OK**.

Display

The display options contain:

- A sub-category relating to the way in which tabs are displayed in the agent
- General options

Tab

The **Tab** sub-category enables you to:

- Choose whether or not to display an icon in the tab.
- Choose whether or not to display the ToolTip that appears every time your cursor rests on the tab.
- Choose whether or not to display the text of the tabs.
- Choose the way the tabs appear.

Calculator for numeric fields

This option enables you to display a calculator for numeric fields.

Display ToolTip

Using this option, you control whether or not to display the ToolTip obtained by pressing F1 while your cursor is inside a field.

Windows graphics

This option enables you to choose between a standard or a flat graphical Windows style.

Multi-document interface representation style

This option enables you to display the agent's panes in exploded view or in tab view.

Chat

This category enables you to choose the chat options. You can modify:

- **Color for your messages**
- **Color of others' messages**
- **Color of messages being typed**
- **Font to display messages**

Events to save in the database

This category enables you to select the elements to send to the server.

Send the connection events to the server

This option enables you to send all the connections performed by a Manager to the server.

Send all other events to the server

This option enables you to send all the operations performed during a remote-control session to the server.

Messages

This category enables you to choose the options for the messages that you exchange with others connected to your server. The available options are:

- **Font used to preview messages**
- **Number of recipients saved in the selection list**
- **Activate the window when restored**
- **Type-ahead for recipient names**

This option enables the automatic completion of message recipient's name after you have typed the first three letters of that person's pseudonym.

- **Check recipient names**

This option forbids you to enter a recipient name or alias.

- **Close the window when there are no more messages in the list**
- **Save messages when application is closed**
- **Use sound notification for new incoming messages**

- **Restore window when new messages arrive**

News

This category enables you to choose the options for the news to which a user can subscribe if they are connected to the server. You can modify:

- **Background color of news bar**
- **Color for topics**

Agent options

The agent options that you can modify are:

- How long to wait before trying to automatically reconnect to the AssetCenter server.
- The NetBIOS adapter number used by the Agent.
By default, the value of the interface number is **0**.
- Whether or not you want to receive a warning sound each time a remote-control session is started.

To choose the signal's sound that you want to hear at the start of each remote-control session:

- 1 Select this option.
- 2 Enter the name of the path of the file to use by clicking .

The file formats are those supported by your operating system.


To send a message

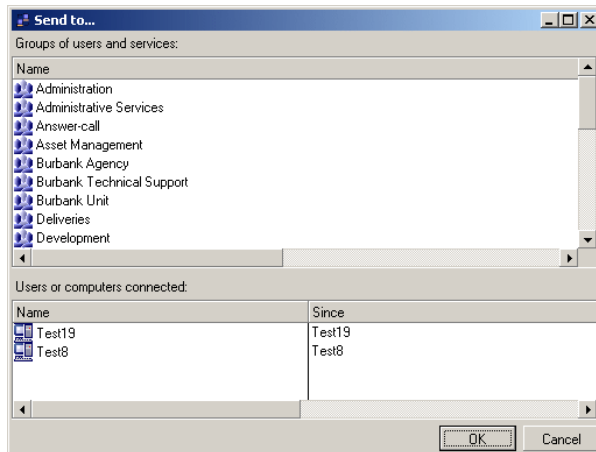
An agent can send messages to all users connected to its server (Managers and other agents).

To send a message:

- 1 Select **Communication/ New message**.
- 2 Enter the recipient's alias in the **Recipient** field.

In the **Recipient** field, you can select your recipient from the last ten recipients by clicking .

By clicking , the window of employees saved in the database generated by your server is displayed.



You can select your message's recipient directly in this window.

In this window, you can:

- Select a group of departments and employees to send the message to.
- Select the connected employees or connected computers.


MyHelp

You can initiate a remote-control session by sending a **MyHelp** message to the Managers connected to your server. Indicate in the message the reasons for the remote-control request: A problem with the computer; a request for advice; etc.


To send a **MyHelp** message:

- 1 Select **MyHelp** from the **Communication** menu.

or

Right-click the  icon in the Windows toolbar and select **MyHelp** from the menu that appears.

or

Click the  shortcut created on your desktop when the Agent Module is installed on your computer

- 2 Enter your message in the window that appears.
- 3 Click **Send** to send a message.

This message appears in the **MyHelp** tab of the Managers subscribed to this topic.

The Managers cannot subscribe to this topic if the **MyHelp** option has not been selected in the **General** tab corresponding to their entry in the database.

As soon as a Manager double-clicks a **MyHelp** message, a window appears asking whether or not they want to take control of your computer, either graphically, via the explorer, or to chat.

As soon as a Manager takes control of your computer, your **MyHelp** message will disappear from the **MyHelp** topic list.

Reading news

To receive news

To receive news, you must subscribe to news topics. For each topic, a news bar appears in your graphical interface.

To subscribe to a news topic:

- Choose the **Communication/ Subscribe to news** menu.
- Select the topics of your choice in the window that is displayed.
- Click **OK**.

Refreshing news

To refresh the news items being displayed, select **Refresh news** from the **Communication** menu.

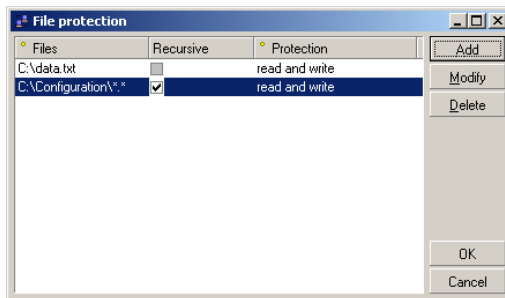
Protecting your files

The Agent module enables you to forbid Managers access to your file and folders.

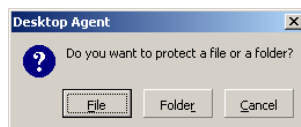
File protection

To protect a file:

- 1 Select the **Tools/ File protection** menu.



- 2 Click **Add** in the window that appears.



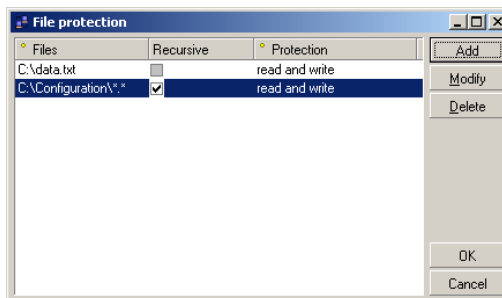
- 3 Click **File**.
- 4 Select a file using the explorer that appears.
The path and the name of the file will appear in the **File protection** window that appears.
- 5 Click the **Protection** column to modify the protection setting for your file.
By default, the file is read and write protected.
- 6 Choose a protection setting.
You can choose from two types of protection:
 - **Read and write** (default value)

- **Write**
- 7 Click **OK**.

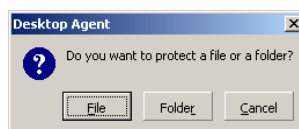
Folder protection

To protect a folder:

- 1 Select the **Tools/ File protection** menu.



- 2 Click **Add** in the window that appears.



- 3 Click **Folder**.
- 4 Select a folder using the explorer that appears.
The path and the name of the folder will appear in the **File protection** window that appears.
- 5 Click the **Protection** column to modify the protection setting for your folder.
By default, the folder is read and write protected.
- 6 Choose a protection setting.
You can choose from two types of protection:
 - **Read and write** (default value)
 - **Write**

7 Click **OK**.

13 | Using the Web surveillance agent

CHAPTER

Besides the graphical interface, Desktop Administration offers you a Web surveillance agent letting you consult a remote computer's key parameters using a simple Web browser.

Using the Web agent

During the default installation of the agent, the Web surveillance agent is also installed and listens on the TCP/IP 802 port. For security reasons, this agent is configured to be accessible only from the browser of a local computer.

This Web agent does not use online security (SSL) in its actual version. For this reason, we advise you against using it via uncontrolled networks.

The following section describes:

- The configuration specific to the browsers to use.
- The configuration of the agent enabling access from a remote computer.
- The different actions available on the Web surveillance agent.
- The security mechanisms.

Configuration

Browser

To access the Web surveillance agent from another computer, your browser must accept the use of nonencrypted passwords. If you use a Microsoft version 5.5 browser or higher, you must activate this function via the **Tools/ Internet Options/ Security/ Custom Level/ Submit nonencrypted form data** menu.

If your browser is not configured to submit nonencrypted passwords, you will not be able to access the Web agent.

Web agent

To activate access to the Web surveillance agent from a remote computer:

- 1 Select the **Peregrine/ Desktop Agents/ Web surveillance agent** menu to launch your browser.
or
- 2 Launch your browser and enter the following address: `http://127.0.0.1:802`
Your browser will start and the page with the connection to the Web surveillance agent appears.
- 3 Connect using the user name **WebAdmin** without any password.
If the connection fails, verify the parameters of your browser as described in the section [Browser](#) [page 200].
You then access the **General information** page. The system information for your computer is displayed.
- 4 Select **Administration**.
- 5 Enter a password, and confirm it.
A message informs you that your administrator account has been modified.
- 6 Select **Administration** again.
- 7 Delete the contents of the **Restrict Web access** field.
- 8 Click **Modify**.
If you only want to authorize Web access to certain computers, you can enter these computers in the **Restrict Web access** section. To indicate the computer(s) authorized to connect to the Web agent:
- 9 Enter the names of host(s) of the computer(s) authorized to access the Web agent.

If you do not want to restrict access to the Web agent, make sure the **Authorized computers** field is empty.

10 Click **Modify**.

11 Click **Exit** in the upper-left-hand part to close the session.

You can now access the Web surveillance agent from another computer.

Actions available on the Web surveillance agent

Connection and disconnection

To access the different pages of the Web agent, you must enter a user name and password. When the password is correct, the agent establishes a work context that lets you browse the different pages.

The Web agent can only handle one session at a time. Therefore, while you are connected, no other users may connect.

After 5 minutes of inactivity, the session will automatically close. The user must re-enter their user name and password to continue the session.

To close the session, click **Exit** on the upper-left-hand side of the main toolbar.

Homepage

When you are connected, the homepage displays information about the computer's features.

The menu bar enables you to access the other screens. This bar, as well as the **Refresh** section, is available from every page.

The highlighted menu indicates the currently selected page.

If you want the information displayed in the main part of the page to be automatically updated:

- 1 Select a refresh interval (10, 30 or 60 seconds) from the drop-down list.
- 2 Click **Apply**.



When the **Refresh** option is used, automatic timeouts for inactivity is not longer effective.

If you want to close the section, click **Exit** or close the browser.

Processes page

This page lists all the processes active on the computer.

The parameters indicated are the:

- ID number.
- Internal name.
- Generated CPU usage.
- Duration of the process since being launched.
- Memory consumed in kilobytes.

Services page

This page presents the:

- List of all known services.
- Name of the services.
- Status of the services (running or stopped).
- The startup conditions of the services.

Log page

This page enables you to view the last events saved in the system.

You can use the drop-down list to choose the type of event that you want to consult (Application, System or Security).

To obtain the detail of a particular event, click the **Source** field.

Statistics page

This page has a graphical representation of the system's activity:

- The CPU usage
- The memory used

Administration page

This page enables you to change the password for accessing the Web agent. It also lets you restrict access by indicating the names or IP addresses of the computers authorized to connect to the Web agent.

The list of computers authorized to connect to the Web agent must be composed of a host name and an IP address, separated by a space.

If you want to forbid external access and only allow local access to the Web agent, indicate the loop address **127.0.0.1**.

Web agent security rules

As previously described, the agent does not encrypt the data transmitted and does not implement the SSL norm, for example.

We thus recommend you only use this agent in a controlled environment protected by a firewall.

You should also indicate the list of authorized computers on the Administration page for added security. If you want to deactivate the Web agent for security reasons, you can modify the startup status of the Peregrine monitoring Web Agent 6.x in the Services section of the Control Panel.

You must also modify the user name.

14 Integrating the Manager with other applications

CHAPTER

The Manager components of the Desktop Administration suite can be integrated with any application capable of launching it from the command line.

Next, the remote computer just has to be defined in the same way in the application and in the Manager (Example: the IP address of the computer).

The command must be formed as follows:

```
Iftman -host: <Name of the computer as displayed in the list of remote computers in AssetCenter>
```

For the list of command-line switches for the Remote Control manager, refer to chapter [Using the Manager from the command line](#) [page 179].

The Manager can be integrated with the following Peregrine Systems applications:

- ServiceCenter 5.5x and Service Center 4.x
- InfraTools Desktop Discovery

Integrating the Manager with ServiceCenter

Integrating the Manager with ServiceCenter enables you to control computers recorded in the **Device** file.

To do this if you are using the version 4.x, you must:

- Import the **irc.unl** file in ServiceCenter.
- Configure the control mode of your computers.
- Take control of computers from ServiceCenter.

If you use Service Center 5.5x, you do not have to perform operations because Manager integration is already configured.

Importing the Irc.unl file

If you selected **ServiceCenter Integration** when installing AssetCenter, the **irc.unl** file is located in the **sc** sub-folder of the installation folder.

To import the **irc.unl** file with ServiceCenter:

- Start ServiceCenter as SysAdmin (using the **falcon** login for example).
- Select the **Toolkit** tab.
- Click **Database Manager**.
- Wait for a new window to appear, and then select **Import/Load** from the **Options** menu.
- Enter the full name of the **.unl** file in the **File** field.
Example: c:\program files\Peregrine\AssetCenter\sc\irc.unl
- Click **Load fg**.

After this step, the Database Manager is displayed again. Click the green arrow to return to the main menu: The Manager icon is displayed.

Click this icon. A new window appears, which contains two icons that enable you to:

- Start the graphical interface of the manager.
- Configure the remote control type for the computers in ServiceCenter.

Configuring the Manager in ServiceCenter

To configure the Manager in ServiceCenter:

- Click the icon representing the Manager in the main window of ServiceCenter
- Click the icon marked **Configure InfraTools Remote Control**.

In the configuration window that is displayed, enter:

- The executable to use to start the Manager (**...launching the Manager** field).
If you enter **lftman.exe**, you don't have to enter the full path of the executable.
- The executable to start to control the remote computers from ServiceCenter (**... taking control** field.) If you use Remote Management 4.x, you must indicate the corresponding executable for this version: **rloader.exe**.
- The command to execute when controlling a computer from ServiceCenter.
The list of commands that can be used in the Manager is available in section [Using the Manager from the command line](#) [page 179] of this guide.

The notes contained in the configuration window help you create your command line.

Configuration window notes

In the command line, you can use any Manager command line option you want.

If you need a value from the ServiceCenter **device** file, you can access it using the field name.

There are a few predefined variables to help you out:

Pre-defined variables **\$L.name**: Asset name (For example: PC001)

\$L.full.name: Work group and asset name (For example: /group/pc001/)

\$L.ip.address: IP address of the asset (For example 100.200.123.456)

Any other field

network.name in \$Ldevice

serial.no in \$Ldevice

Examples:

```
"-host" + $L.name
```

```
"-type: srv -host" + $full.name
```

```
"-type: srv -hostIPAddress=" + $L.ip.address
```

```
"-type: srv -host" + network.name in $L.device
```

To control a remote computer

To control a remote computer, you must select the computer and then choose **Connect to device** from the **Options** menu.

Selecting this option is equivalent to executing the command line entered in the Manager configuration window.

This option only appears in certain contexts: Inventory Management, Problem Management, Incident Management, etc.

The **Remote Manager** option, which enables you to start the graphical interface of the Manager, appears in the same contexts.

To control a computer from the Inventory Management window

To control a computer from the Inventory Management window:

- Start ServiceCenter.
- Click **Inventory Management**.
- Click **GS Component**.
- Select the computer you want to control in the **Asset** field.
- Select **Connect to device** from the **Options** menu.

Integrating InfraTools Desktop Discovery with the Manager

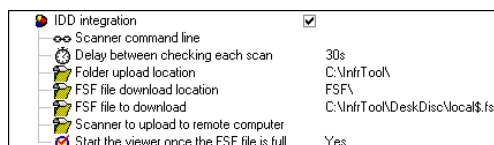
Integrating InfraTools Desktop Discovery with the Manager enables a Manager to start a Scanner on a remote computer. The results are stored in a results file (.fsf) that the manager can view using the InfraTools Desktop Discovery Viewer, for example.

Prerequisites

You must install InfraTools Desktop Discovery. It doesn't matter which version of this application you install since all versions can be used.

To enable InfraTools Desktop Discovery in the AssetCenter Manager:

- Choose **Options** from the **Edit** menu of the Manager.
- Select the **IDD integration** option.
- Populate the option fields by double-clicking the Value column.

Figure 14.1. InfraTools Desktop Discovery integration options

Remarks on the InfraTools Desktop Discovery integration options

Scanner command lines

For the list of commands to use with the Scanner, refer to "Command-line options and switches for DOS-based, Windows-based and OS/2" in chapter 4 "The Scanner Generator" of the InfraTools Desktop Discovery Version 6.00 User's Guide.

Starting the viewer once the FSF file is fully downloaded

If you select this option ('Yes' in the value column), the InfraTools Desktop Discovery Viewer is automatically displayed in the manager window.

FSF file to download

The results file (.fsf file) must match the file indicated when configuring the scanner you use.

To start a Scanner on the remote computer

Once you have enabled InfraTools Desktop Discovery integration:

- Select a computer in the list of remote computers in the manager.
- Choose **Scan** from the **System** menu.

or

- Right-click, and then choose **Scan** from the shortcut menu.

A progress window is displayed in which you can view the different steps of the scan.

To view the last scan

To view the last scan started on the remote computer:

- Select this computer in the list of remote computers.
- Choose **Explorer** from the **System** menu.
or
- Right-click one of the nodes of the remote computer.
- Choose **View the last scan** from the shortcut menu.

To start a scan from the command line

To start a scan on the remote computer from the command line, go to the sub-folder containing the manager on your computer and execute the following command:

```
iftman -host: <name of the remote computer> -type: <da/srv> -server: <name of the server used> -mode: scan -viewscan -close
```

Notes on the variables used

Type

This parameter is optional. By default, the value **da** (direct access) is selected. The direct-access name of the remote computer is not case sensitive. The **srv** variable is used for remote computers recorded in an InfraTools database managed by your LAN server. You must indicate its full name (FullName field, SQL name: iftHost_FullName).

To obtain the full name of computers in the database:

- Start InfraTools Administrator.
- Open the Computers table.
- Right-click the list of computers.
- Choose **Configure list** from the shortcut menu.
- Select the **Full name** field for the full names to be displayed in the list of computers.

To view the last scan from the command line

To view the last scan performed on the remote computer, execute the following command line:

```
iftman -host: <name of the remote computer> -mode:scan -viewlastscan
```

15 | Glossary (Remote control)

CHAPTER

Remote Control server

The server is a service that provides Managers with the list of employee groups and remote computers saved in the database. When you take control of a remote computer:

- It generates control rights assigned to each Manager.
- It validates access to the remote computers.
- It keeps the information pertaining to the remote-control session between the Manager and the remote computer.

Web surveillance agent

After the Web agent is installed and configured on a remote computer, it enables the manager to consult the computer's parameters from a browser:

- System information
- Activity
- Process

- Running services
- Application logs, system logs, security logs
- Processor load and memory consumption

Certificate

The certificate is a file provided to the manager from the database administration console. This file contains:

- The Manager's authentication parameters.

It can be a:

- Local password needed each time the Manager is started.
- Login saved in the database.
- Control rights on remote computers.
These control rights are defined for each access type (via network neighborhood, via server, via direct access).
- An encryption key that protects the data the manager exchanges with the users of the remote computers.
- A calendar defining authorized time periods for control.
- A period of validity.

To evaluate AssetCenter, a certificate that expires after one month is provided to Managers.



Note:

For version 4.x Agents, additional parameters are required: the license and name of the Manager and the license of the client. These parameters enable the manager to be identified by version 4.x Agents.

MyHelp

Users can ask for help using the MyHelp function from the agent installed on their computers. This function triggers the creation of a help ticket in the database.

When the Manager sees the MyHelp message, they can immediately take control of the employee's computer.

IV Transversal functions

PART

16 | Departments and employees

CHAPTER

This chapter explains how to describe and manage departments and employees with AssetCenter.

Use the **Portfolio/ Departments and employees** menu item to access the list of departments and employees.

Organization of departments and employees

AssetCenter organizes the list of departments and employees hierarchically.

Departments, which may be composed of sub-departments, and include employees (employees cannot have sub-records, however).

The best way to organize this table is to create a hierarchy of the departments in your company and to attach the employees to their respective departments. Employees are therefore at the end of the branches.

Departments and employees are created and managed from the same screen.

AssetCenter users

In order to protect access to the database, only an AssetCenter user who is declared in the database can open the AssetCenter database.

Several users may work simultaneously on the same database.

An AssetCenter user has a record in the list of departments and employees, and they have been assigned a **Login** and a **Password** (SQL names: UserLogin and LoginPassword) by the administrator.

AssetCenter administrators

An AssetCenter administrator is a user who has rights to all tables in the AssetCenter database.

Several users may be database administrators. To create a database administrator, another administrator simply assigns administrator rights to that user.

The Admin login

The Departments and Employees table includes an administrator by default whose **Login** is "Admin".

- When AssetCenter is first installed, this is the only login name that enables you to access the AssetCenter database for all administrative operations.
- This login name enables you to connect in case you cannot connect as an administrator under any other names. For reasons of security, its record cannot be destroyed.

Creating departments and employees

- 1 Select the **Portfolio/ Departments and Employees** menu item.
- 2 Click **New**.

A dialog box appears asking you if you want to create a department or an employee.



Note:

The database information and the tabs contained in the detail of a department and that of an employee are not the same.

Defining an employee's user profile

To assign a user profile to an employee and to specify a password, display the **Profile** tab in that employee's details.



Important:

Only administrators can see the **Profile** tab in an employee's detail.

Defining an administrator

To indicate an administrator for the database:

- 1 Populate the **Login** (SQL name: UserLogin) and **Password** fields (SQL name: LoginPassword).
- 2 Check the **Administration rights** field (SQL name: bAdminRight). This is equivalent to assigning that person all access rights to the database.

Defining a non-administrator user

To define a user who does not have database administration rights:

- 1 Populate the **Login** (SQL name: UserLogin) and **Password** fields (SQL name: LoginPassword).
- 2 Assign a user profile to the employee by populating the **Profile** field (SQL name: Profile).

The person can then access the AssetCenter database using their login name and view/modify the information according to their profile.

Employee groups

Use the **Portfolio/ Groups** menu item to create employee groups.

Employee groups are used in several areas of the software.

Employee groups are stored in the table of employee groups (SQL name: amEmplGroup). This table is hierarchical.

To create an employee group:

- 1 Select the **Portfolio/ Groups** menu item.
- 2 Click **New**.
- 3 Enter the name of the employee group.
- 4 Enter the group to which it belongs, if necessary.
- 5 Specify a group supervisor.
- 6 Specify the members of the group in the **Composition** tab.
- 7 Enter any locations dealt with by the group in the **Locations** tab.

17 | Locations

CHAPTER

This chapter explains how to describe locations with AssetCenter.
Use the **Portfolio/ Locations** menu item to display the list of locations.

Definition of a location

You company's locations are described in an independent hierarchical table.
A location is used to describe the physical situation of a computer, an employee, a group, etc.

18 | Features

CHAPTER

This section explains how to use features with AssetCenter.

Use the **Administration/ Features** menu item to display the screen for creating and editing features.

Definition of features

Features enable you to complete the description of objects (computers, departments and employees, etc.) in AssetCenter. They are associated with a value and are displayed directly in the **Features** tab of objects.

You can create as many features as you wish, and specify their entry mode (Numerical, Text, etc.). This makes AssetCenter very flexible and allows for extensive customization.

By using features, you can include additional information in areas of particular importance to you (technical or any other specific area).

Features provide additional "fields" for describing the records in your database.

Finally, features can be queried using the AssetCenter query language.

Description of the features

Creating a feature involves identifying it and determining how it behaves.

Identifying a feature

The upper part of the feature detail screen is used to identify and classify the feature (using feature classes). A feature is uniquely identified by its SQL name. The other fields in this part of the screen provide extra information on the feature and are described in detail in the extended help (press SHIFT+F1 to access the extended help on a field).

Behavior of a feature

The behavior of a feature depends on:

- Its input type, which determines the type of control used in the user-interface to populate the value of the feature for a record. The input type is associated with a unit.



The "Link" input type, which is complex, is the subject of a separate chapter in this manual.

Parameters of a feature

The parameters of a feature can be found in the **Parameters** tab of the detail of the feature.

Once you have created a feature, the parameters are used to specify:

- The names of the tables that can use this feature.
- The default value for the feature.
- Any data entry and display constraints concerning this feature.

Editing the parameters of a feature

If you click the  or  buttons, AssetCenter opens the screen for editing and creating parameters.

 **Note:**

The screen for editing parameters is not available until the feature has been created.

These parameters are linked to a table defined by the **Table** (SQL name: TableName). This field is filled in from a system itemized list (a list whose values cannot be modified) containing all the tables in AssetCenter.

 **Note:**

A given feature may have different parameters for different tables.

The parameters of a feature include data-entry constraints, a default value and the contents of the extended help for this feature.

Data-entry constraints

The possible values for each constraint are as follows:

- **Yes:** The constraint is valid for all records in the table with which the feature is associated.
 - **No:** The constraint is not valid for any record in the table with which the feature is associated.
 - **Script:** Application of the constraint is subject to a Basic script.
-

 **Note:**

It is not possible to edit or modify the Basic script used for a feature parameter.

The table below summarizes the different data-input constraints applicable to a feature:

Table 18.1. The different data-input constraints applicable to a feature

Constraint	Description
Available	Determines the availability of the feature.
Force display	Determines whether the feature is displayed by default.
Mandatory	Determines whether populating the feature is mandatory.
Historization	Determines whether history is kept for the values of the feature.

Default value

You can define a default value for a feature. This function is identical to that which is provided for other fields in the database.

Extended help

As for all other fields in the database, you can define three sections of extended help for a feature.

Feature classes

A feature class groups features with common properties. For example, features such as "Processor level 1 cache" and "Processor level 2 cache" may be grouped in a feature class called "CPU".



Use the **Administration/ Feature classes** menu item to access the screen for editing and creating feature classes.

Managing features


This section explains how to manage features.

Introduction

To add a feature to a record, simply move to the **Features** tab in the detail of a record in the table in question. This tab includes two parts:


- The right-hand side lists the features already associated with the record. Here you can add or remove features using the  and  buttons.
- The left-hand side displays a tree view of the feature classes; it is used to filter the features in the right-hand side.

You can only add a feature to a record if the feature applies to the table containing that record, and if the feature is available. In other words:

- The table must appear in the **Parameters** tab in the feature detail.
- The value of the **Available** field (SQL name: seAvailable) must be set to Yes or to Script if the Basic script updates the value of the field to Yes.
- The features for which input is mandatory cannot be removed and are not offered in add mode (by the  button).

Detail of the class tree structure

The left-hand side of the **Features** tab enables you to filter the features displayed in the right-hand side of the screen. It displays a tree view of the feature classes.

- When you select the node  (All) of the tree, AssetCenter displays on the right side of the tab all features associated with the record.
- When you select a branch in the tree (therefore a class or a sub-class), AssetCenter displays the features for that class or sub-class in the right-hand side of the tab.

When you check the **With sub-classes** box, AssetCenter also displays the features associated with the sub-classes of the selected classes, in the right-hand side of the tab.

Detail of features associated with a record

The right-hand side of the **Features** tab enables you to:


- View the features associated with the record
- Associate a feature with a record
- Remove a feature from a record



Note:

The **Features** tab in the record detail appears only if at least one available feature exists for this record's table (the feature is attached to the table and the **Available** field (SQL name: seAvailable) is set to Yes (either when specified directly, or defined with a script)).

Associating a feature with a record

When you add a feature by clicking the  button, AssetCenter opens the window for choosing the features available for the current record. This window displays the features in a tree structure, organized by class. This tree displays available features only, i.e. those whose **Available** field (SQL name: seAvailable) is set to Yes (either when specified directly, or defined with a script).


Now simply select the feature of your choice and click the **OK** button; AssetCenter will add it to your record.



Note:

This screen supports multiple selections using the CTRL and SHIFT keys. Thus you can add several features in a single operation.

Removing a feature from a record

When you remove a feature from a record by pressing the  button, AssetCenter opens a window for choosing the features already associated with the record. This window displays the features in a tree structure organized by class.

Simply select the feature you want to remove and then click the **OK** button; AssetCenter removes the feature from your record.



Note:

This screen supports multiple selections using the CTRL and SHIFT keys. Thus you can remove several features in a single operation.





Features that are mandatory or displayed by default (i.e. those whose **Mandatory** parameter (SQL name: seMandatory) is set to Yes and those whose **Force display** parameter (SQL name: seForceDisplay) is set to Yes) cannot be removed from a record.

Viewing features in a list

Features are displayed in the **Features** tab of a record, but you can also view them in the list of records in a table.

To do this, right-click the list to display the shortcut menu and select **Configure list**. AssetCenter opens the list configuration window.

The features associated with the table appear at the end of the list. First expand the tree to obtain a detailed list.

Then select a feature by clicking the  button. This adds a column to the list with the name of the feature in the header and the value of the feature for each record in the table. The  button removes a column from the list, and the  and  buttons change the order of the columns.

