COCKPIT5i

For Secure Browsing
Administrator Guide

JETRO PLATFORMS
Team Company

Statement and Terms of Use

Chapter 1: Important Notice

Publication date: January 2016

Part No. Jet-01-16A

Chapter 2: Support and Contact Information

For information about Jetro Platforms and our products, visit our website at http://www.jetroplatforms.com

Or contact us by e-mail or phone at:

- **E-mail**: jetroplatforms@jetroplatforms.com or
- **Phone**: +972-3-9267063

Chapter 3: Introduction

This chapter introduces the COCKPIT5i Version 5.1 Secure Browsing platform and presents the workflow for installing and configuring the Secure Browsing Platform Servers and Clients.

This chapter contains the following topics:

What is Jetro COCKPIT?

Jetro COCKPIT5i Secure Web Browsing provides corporate users with a secure way to remotely browse the Internet using virtualization servers residing in a DMZ (Demilitarized Zone), outside your corporate network.

COCKPIT5i is a server-side virtual browser that browses the web from the DMZ. Instead of the regular HTML-based web browsing, COCKPIT5i streams web pages as video bitmaps so that the content that end users view does not contain any HTML, JavaScript, JPEG, Flash, or any other kind of Internet content. Therefore, this solution makes web browsing resilient against both known and unknown security threats.

Designed for enterprises that must keep their corporate networks disconnected from the Internet, COCKPIT5i keeps all TCP/IP ports closed at the firewall, including HTTP, HTTPS and all other ports. No active code travels through the network. Only the outbound, secure COCKPIT5i port is left open so that no content can penetrate the network. This means that nothing is open to being exploited!

While Secure Browsing is built for the most demanding level of security, it provides an unparalleled level of end user transparency. It is at the same time easy to use while still guaranteeing that organizational productivity is not compromised at the expense of security. It solves the security-related issues of file upload, download, printing, and emailing, while preserving the ability of end users to point-and-click Internet links in desktop applications. Additionally, it enables users to switch seamlessly between internal and external web pages, and much more.

This topic has three subtopics:

Enterprise-grade Solution

Secure Browsing is designed to meet the needs of a variety of enterprise infrastructures. It is scalable and easy to manage. Its enterprise-grade architecture ensures that all of the products' components can be deployed with full redundancy and that all production servers can be pooled under load balancing schemes. Secure Browsing can handle multiple network zones and enables administrators to optimize end users' web browsing routes.

Benefits

The following is a list of the benefits of COCKPIT5i Secure Browsing:

- **Eliminates security risks** - Jetro's Secure Browser guarantees 100% safe web access. Secure Browsing streams web pages as video bitmaps so that the content that end-users view does not contain any HTML, JavaScript, JPEG, Flash, or any other kind of Internet content. In this way, Secure Browsing-enabled web browsing is resilient against both known and unknown security threats.
- Enhances control
- Secure printing
- Reduces costs
- Enhances browser performance and improves user experience

Features and Capabilities

The following is a partial list of COCKPIT features and capabilities:

- **Seamless Web Access for Enterprise Users**
  - Seamless and transparent browsing experience using the standard Internet Explorer
  - Same launch methods for both internal (inside the enterprise's LAN) and external (outside the enterprise's LAN) browsing
  - Synchronization of personalization between internal and external browsing
- **Seamless and transparent browsing experience using the standard Internet Explorer**

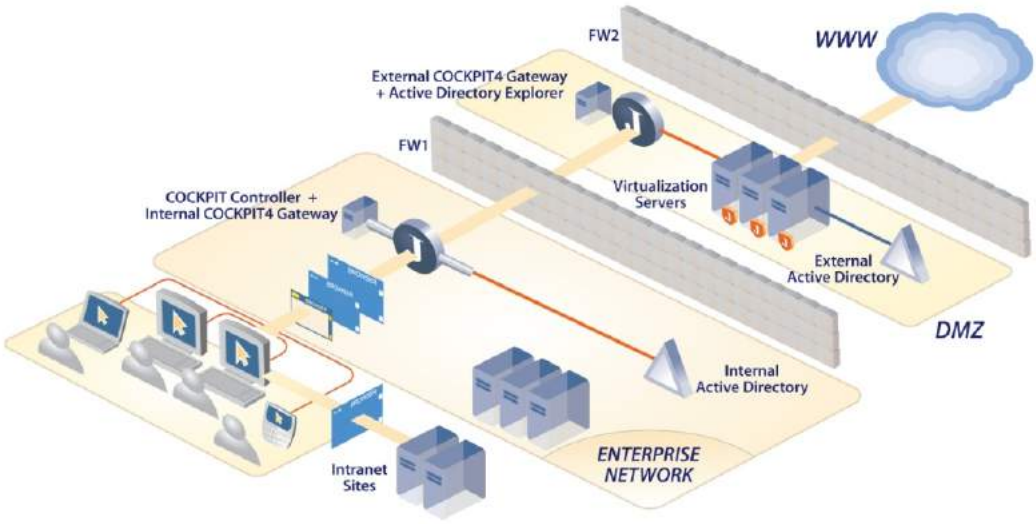
- Same launch methods for both internal (inside the enterprise's LAN-Local Area Network) and external (outside the enterprise's LAN) browsing
- Synchronization of personalization between internal and external browsing

- **Smart Links URL Switching and Launch**
  - Automatic and seamless switching between internal browsing and remote virtual browsing
  - Virtual web browser launches directly from non-web applications including email, MSOffice document, or any other source on the user's client desktop
- **Smart Links Firewall**
  - Built-in whitelisting and blacklisting
  - Rule-based access control to web sites according to multiple properties, such as: user name, client machine, as well as schedule based access control
- **Secure File Download**
  - Built-in secure download management
  - FTP/HTTP ports remain strictly closed throughout the entire download process
  - Integrates with file cleansing/laundering solutions
  - Integrates with the organization's malware protection solutions
- **Secure File Upload**
  - Built-in secure upload management
  - FTP/HTTP ports remain strictly closed throughout the entire upload process
  - Integrates with data leakage prevention and content inspection solutions
- **Secure Send2Me**
  - Simple and intuitive alternative method for downloading content
  - Point-and-click on a target to send the target via email
  - Content passes through the corporate regular security screening for incoming emails
- **Favorites Synchronization**
  - Synchronizes between the user's favorites on the desktop and the user's favorites in the virtual browser

- **Complete Anonymity**
  - Virtual browsing is performed under randomly-generated user names and passwords that meet Microsoft complex requirements.
  - Translation of real user names is only kept inside the network
  - Only administrators can access the translation tables
  - Prevents exposure of employees' identity to the target web sites
  - Complete anonymity without losing the ability to integrate with proxy servers
- **Robust Foundation**
  - Highly scalable architecture that supports multi-server farms of virtual browsers
  - Full redundancy and hot failover for all system components
  - Supports complex network deployments including multiple sites, zone preferences and more
  - Central administration and reporting
  - Tight Active Directory integration
  - Automatic centralized distribution of software upgrades
- **Stand-By session**

Secure Browsing Architecture

The following diagram shows a typical Secure Browsing implementation and the components that enable the secure flow of data:



Secure Browsing Architecture: Basic System

Three zones are managed in a Secure Browsing system architecture: the enterprise LAN (Local Area Network), the DMZ (Demilitarized Zone) and the external world of the Internet. The zones are separated by an internal and external firewall.

This topic has three subtopics:

Enterprise LAN Zone

DMZ

WWW (External Zone)

Enterprise LAN Zone

The LAN (Local Area Network) zone is inside the organization and consists of:

- Desktop Users
- Clients
- Intranet Sites
- Controller and Internal Gateway
- Internal Active Directory
- Administration Console

Clients

COCKPIT5i Clients run on each user's computer and enable approved COCKPIT5i Client users to browse the Internet without being directly connected to the Internet. These users and their computers are completely disconnected from the Internet. COCKPIT5i opens an RDP session via the Secure Tunnel and the entire browsing experience is delivered over the RDP stream without any Internet content whatsoever entering the corporate network.
The primary purpose the COCKPIT5i Client is to trap browsing events, such as when a URL link in an email is clicked by a user. The COCKPIT5i traps these events and automatically determines whether each link is inside the corporate network, in which case it is displayed in a local browser, or whether the link points to an external address, in which case an external browser is opened on a Terminal Server. This mechanism is called SmartLinksTM, which is the ability to switch seamlessly between internal and external browsers just by linking to a URL in the usual manner, such as by clicking on it in a web page or in an email.

Intranet Sites

Intranet sites are located inside the corporate network. These are the sites to which COCKPIT5i Clients are allowed to browse inside the organization. Secure Browsing Clients browse to these sites using the local internal browser on their computer.

Controller+Internal Gateway

The Controller manages and monitors application and content delivery on the COCKPIT5i site, as well as the relationships between all the elements in the COCKPIT5i site Server-Based Computing network.

The Primary Controller also acts as the Internal Gateway. The COCKPIT5i Primary Controller Server is therefore known as the COCKPIT5i Primary Controller Server+Internal Gateway.The COCKPIT5i Internal Gateway is located in the enterprise LAN (Local Area Network) zone. It connects the Primary Controller to the External Gateway in the

DMZ, which connects to the Terminal Servers.

The connection between the COCKPIT5i Primary Controller Server+Internal Gateway (located inside the enterprise LAN zone) with the COCKPIT5i External Gateway (located in the DMZ) provides a Secure Tunnel between the enterprise network and the DMZ which contains the COCKPIT5i External Gateway and the Terminal Servers.

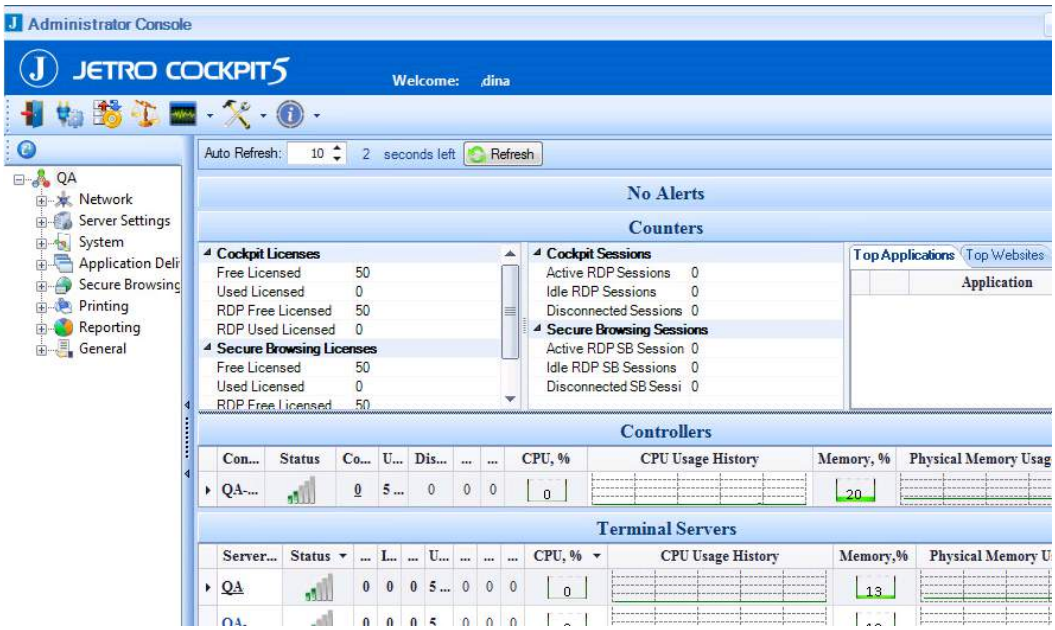
Internal Active Directory

The internal (corporate) Active Directory Server is a non-dedicated Active Directory that sits inside the enterprise LAN Zone. It is typically an enterprise's existing Active Directory Server that serves various internal corporate needs, such as for email.

Administration Console

The COCKPIT5i Administration Console provides the site administration functionality and user interface described throughout this guide. The COCKPIT5i Administration Console is typically run on the Primary Controller, but can also easily be installed on the system administrator's machine. The Administration Console communicates with all the other COCKPIT5i site components, such as the Terminal Server COCKPIT5i Agents.

The main window of the COCKPIT5i Administration Console is shown below:



DMZ

The DMZ (Demilitarized Zone) is outside the corporate LAN and consists of:

- External Gateway+Active Directory Explorer
- External Active Directory
- Terminal Servers
- DMZ Communicator

The DMZ is used for the anonymization of the identity of corporate users, in order to prevent their disclosure to the outside world.
The dedicated External Active Directory creates fake profiles for each corporate user and a map to the internal users in order to enable the persistence of each user's browsing experience from session to session in regard to favorites, cookies, preferences, saved passwords, and so on.

External Gateway+Active Directory Explorer

COCKPIT5i External Gateway: The COCKPIT5i External Gateway is located in the DMZ and communicates with the Internal Gateway in the Enterprise Network zone through the firewall. Secure Browsing Clients are able to browse to sites outside the organization through the external browser situated on the External Gateway Server.

Active Directory Explorer is a viewer and editor for Active Directory databases. It can be used to navigate around and modify Active Directory entries. The External Active Directory Explorer communicates with the External Active Directory. The External Active Directory creates fake user profiles for users in the DMZ.
See the COCKPIT's Secure Tunnel section for a description of how the COCKPIT5i Primary Controller Server + Internal Gateway located inside the Enterprise Network Zone communicates with the COCKPIT5i External Gateway, located in the DMZ.

External Active Directory

The External Active Directory Server is a dedicated Microsoft Active Directory Server that sits in the DMZ, meaning outside the organization. It contains fake user names, passwords and user profiles that are shown to the outside world (meaning outside the enterprise) in order to protect the identity of corporate users. These fake users are created and managed by the Controller.
The dedicated External Active Directory creates fake profiles for each corporate user and a map to these internal users in order to enable a consistent browsing experience for each user from session to session, regarding favorites, cookies, preferences, saved passwords and so on.

Terminal Servers

The Terminal Servers run browsers for COCKPIT5i Clients. The Terminal Servers are able to communicate with the Internet, through the external firewall, via standard Internet protocols, such as an HTTP, HTTPS or FTP protocol. The COCKPIT5i architecture ensures that the Internet protocol is terminated at the Terminal Server, which is in the DMZ. This means that no Internet protocol ever enters the corporate network through the Terminal Server. This means that the Internet remains completely outside the corporate network, which also provides the enterprise with the ability to block outbound connections from a client in the corporate network.

WWW (External Zone)

The External zone is the external world of the Internet, meaning outside the enterprise's LAN and outside the DMZ. This is the zone that corporate users want to access and from where they need protection.

COCKPIT's Secure Tunnel

The COCKPIT's Secure Tunnel provides complete security for COCKPIT5i Clients. For example, it enables multiple corporate COCKPIT5i Clients to access the DMZ through a single port in the firewall.

This topic includes two subtopics:

- Secure Communication
- Communication Through the Tunnel

Secure Communication

COCKPIT5i enables enterprises to keep their corporate networks disconnected from the Internet because only the outbound, secure COCKPIT5i port is left open. Therefore, no active code or content can penetrate the network.

The connection between the COCKPIT5 Primary Controller Server + Internal Gateway (located inside the Enterprise Network zone) with the COCKPIT5 External Gateway (located in the DMZ) provides a S**ecure Tunnel** between the Enterprise Network and the DMZ that contains the COCKPIT5 External Gateway and the Terminal Servers.

The tunnel provides security in the following ways:

- **Single Opening through the Firewall**: The tunnel enables multiple corporate COCKPIT5i Clients to access the DMZ through a single port in the firewall, instead of creating an opening through the firewall for each corporate client.
- **Single-directional Opening though the Firewall**: The tunnel serves as a one-way exit for information from the corporate to the DMZ. Tight security and control is provided for communications back into the corporation.

Communication Through the Tunnel

This Secure Tunnel feature is achieved by the COCKPIT5i components collaborating to control all communication between the COCKPIT5i Client and the Terminal Server, including the RDP stream, all XML messages, and so on.

The tunnel is encrypted and multiplexed so that, for example, 1000 COCKPIT5i Client user streams can securely connect to 10 Terminal Servers.

The COCKPIT5i Controller controls the establishment of the tunnel, to enable the following secure communication flow:

- From the COCKPIT5i client to the COCKPIT5 Internal Gateway.
- From the to the COCKPIT5 Internal Gateway to the COCKPIT5 External Gateway.
- From the COCKPIT5 External Gateway to the Terminal Server.

The Controller directs the connection of the various components according to connection and load balancing policies. For each COCKPIT5i Client it defines which route to take when connecting from the COCKPIT5 External Gateway to a Terminal Server.

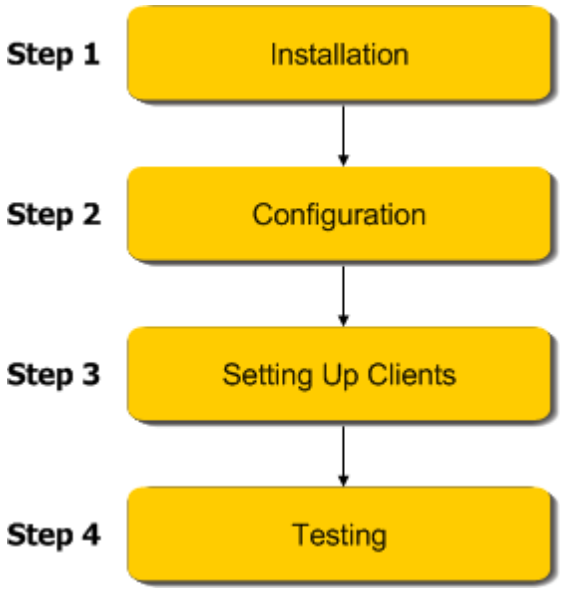
When a COCKPIT5i user tries to open a browser, the Controller determines which Terminal Server it will access.

Security is retained because the translation of the internal (real) user name and the external (fake) user name is performed entirely inside the corporate network so that the real identities of the users are never sent outside the corporate network.

Installation and Configuration Workflow

The following presents the workflow for installing and configuring the various components of a Jetro COCKPIT5i Secure Browsing system. This procedure can be performed quite quickly and may vary between organizations.

We highly recommend that you closely follow the instructions provided in this guide. This guide is organized so that you can read it from cover to cover in order to set up your first Secure Browsing experience.



- **Step 1, Installing Secure Browsing Servers** describes how to install the Servers that enable Secure Browsing. Secure Browsing is enabled by installing a Primary Controller (and optionally a Secondary Controller) and Terminal Servers that serve the applications.
- **Step 2, Configuring Secure Browsing Servers** describes how to configure Secure Browsing Servers.
- **Step 3, Setting Up Secure Browsing Clients** describes how to install the Jetro Secure Browsing Client on a user's computer.
- **Step 5, Testing Secure Browsing Usage** verify that the Secure Browsing is operating properly.

Chapter 4: Installing COCKPIT

This chapter describes how to install COCKPIT5i Version 5.1 Secure Browsing. This includes:

Installation System Requirements

This topic describes the prerequisites that must be installed before installing the COCKPIT5i for Secure Browsing components.

1. The COCKPIT5i External Gateway + Active Directory Explorer Server needs to communicate with the Anonymous Directory Server. Therefore, the COCKPIT5i External Gateway + Active Directory Explorer Server must have read/write administrative user name and password permissions to the Anonymous Directory Server. The user name and password is stored encrypted inside the LAN.
2. The COCKPIT5i Internal Gateway + Primary Controller Server must have read-only permission to the internal organization's Active Directory Server.
3. All the Secure Browsing Servers in the organization's DMZ must be members of the External Active Directory Server's domain.
4. A one-way port connection between the COCKPIT5i Internal Gateway and the COCKPIT5i External Gateway must be created. Its port number through the firewall must be 13000.
5. The COCKPIT5i system can be installed on any machine that is suitable for Microsoft Window Server 2003 SP2, Window Server 2008 (X86 and X65) and Windows Server 2012 r2 architecture.

License Server Installation

The License Server defines the maximum number of concurrent users that are able to use COCKPIT desktops simultaneously. The same License Server can serve all Jetro COCKPIT products.

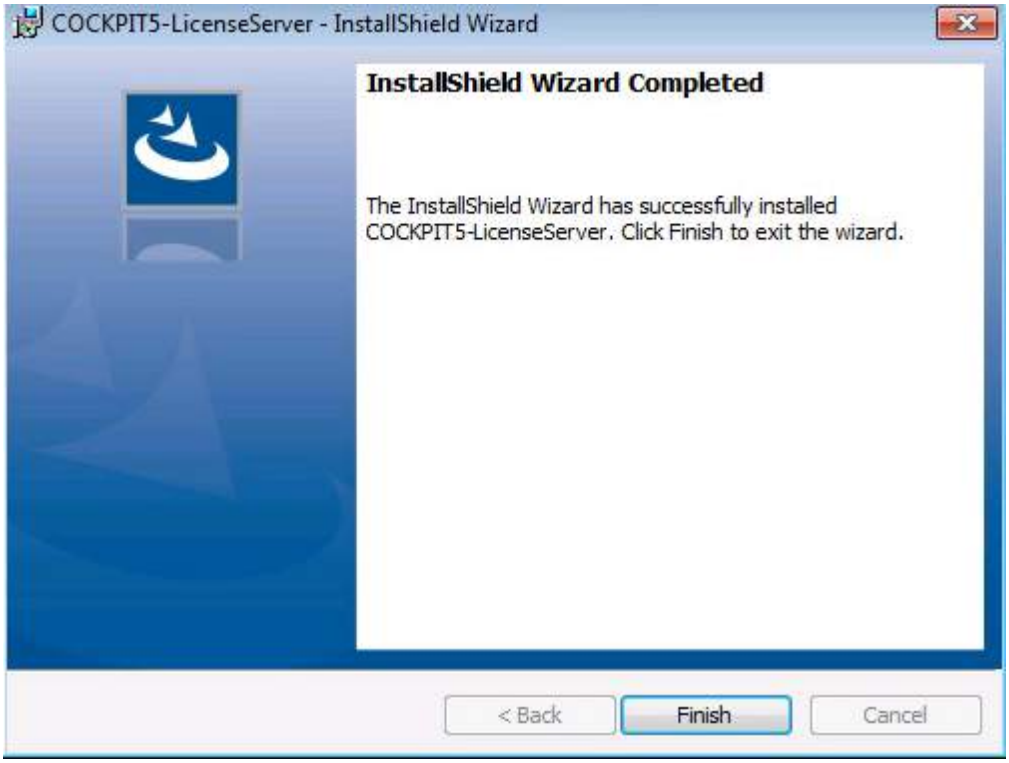
Installation Considerations:

1. COCKPIT5i Secure Browsing requires a License Server. The out-of-the-box License Server provides the system with 50 concurrent users for 30 days. After 30 days, the system requires a valid activation file.
2. It is recommended to install the License Server on the machine you intend to be the Primary Controller. However, it can be installed on any computer that has continuous communication with the Primary Controller.

To install the COCKPIT License Server:

1. Run **COCKPIT5-LicenseServer.exe** from the files that you received from the Jetro package.

2. Follow the wizard's instructions until the InstallSheild Wizard is completed.



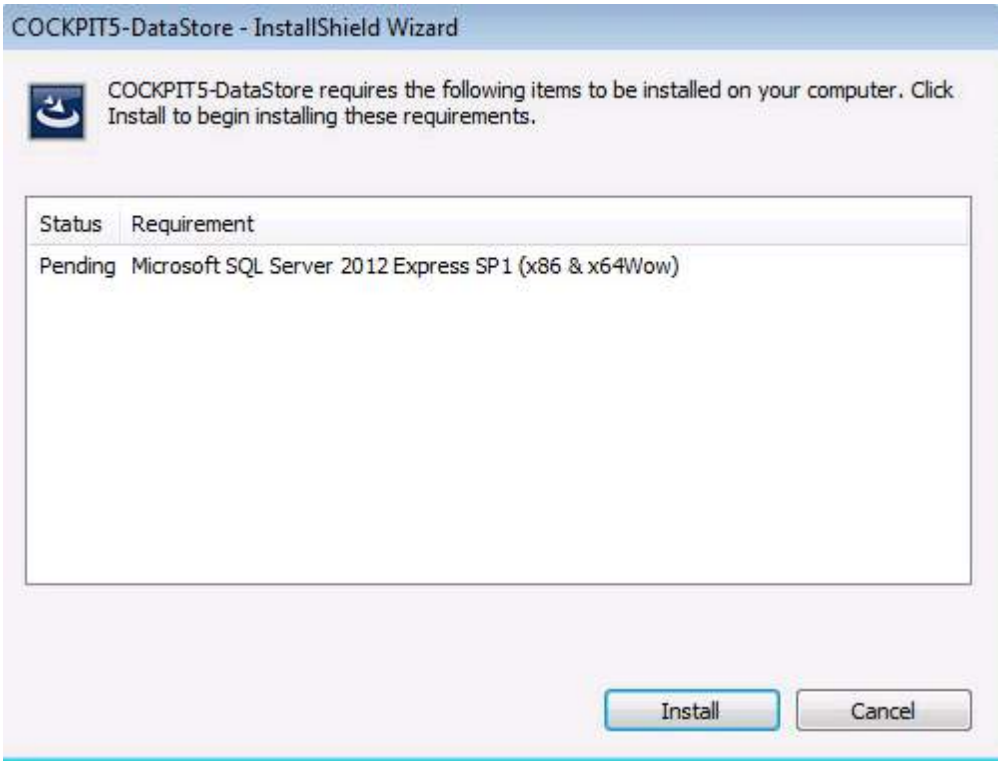
Congratulations! The installation procedure has successfully installed the COCKPIT License Server.

Data Store Installation

Data Store is the database for the COCKPIT5i Secure Browsing system. This setup also installs MS .Net framework 3.5 and 4, SQL Server Express 2008 Express SP1, and MSXML 6.x, if they are not already installed on the machine.

To install COCKPIT Data Store:

- Run **COCKPIT5-DataStore.exe** from the files that you received from the Jetro package, and follow the wizard's instructions. COCKPIT Data Store will take a few minutes to install.



COCKPIT Server Installation

This topic explains how to install the COCKPIT Server. The Server can be installed as a:

- Primary Controller Server
- Terminal Server
- Other COCKPIT Services - Gateway.

Before installing the COCKPIT Server, ensure you have installed the License Server and Data Store as described in the previous topics.

The installer must be logged onto the Server as Domain Admin.

> NOTE: The COCKPIT Server supports command line installation for automatic deployment. More details below:
>
> For example:
>
> - COCKPIT5-Server.msi [ROLE=TS|OTHER:PORT]

- For example to install Server as Terminal Server on port 13000:
  COCKPIT5-Server.msi ROLE=TS:13000
- To install as communicator show only progress bar (passive mode):
  COCKPIT5-Server.msi ROLE=OTHER:13000 /passive

This topic contains 3 subtopics:

- Primary Controller Installation
- Terminal Server Installation
- Secure Connector, Print Terminal and Gateway Installation

Primary Controller Installation

This topic explains how to install the COCKPIT Server and set it as the Primary Controller. The Primary Controller stores and manages the primary copy of the current COCKPIT administration data. This setup also installs MS .Net framework 3.5 SP1 if it is not already installed.

To install the Primary Controller:

1. Logon to the server that you want to assign as the Primary Controller and login as Domain Admin to the console (session0)
2. Run **COCKPIT5-Server.exe** from the files that you received from the Jetro package. .NET 2.0, and follow the wizard's instructions until you reach the **Server Configuration** screen.

3. Ensure the **Primary Controller** checkbox is selected, to assign this Server as the Primary Controller. The Controller checkbox will also be selected automatically.

4. Enter a server farm site name in the **Please enter a site name** box. A server farm is the environment that contains all servers. Every farm must have a Primary Controller and only one Primary Controller can be assigned to each farm.

5. In the **Database** section, select the **Local** checkbox, and click **OK**.

   NOTE If you wish to use a remote database, contact Jetro support before continuing with the installation.

6. Continue to follow the wizard's instructions.

Congratulations! The installation procedure has successfully installed the COCKPIT Primary Controller Server.

You are now in the Primary Controller environment.

Additional Options:

- To add a Secondary Controller, repeat this procedure and only select Controller in the Server Configuration screen.
- To configure the Secondary Controllers, see the Hosts topic in the Configuration section.

Terminal Server Installation

This topic explains how to install the COCKPIT Server and set it as a Terminal Server. Terminal Servers run browsers for COCKPIT5i Clients. The Terminal Servers are able to communicate with the Internet through the external firewall, via standard Internet protocols such as HTTP, HTTPS or FTP protocol. This setup also installs MS .Net framework

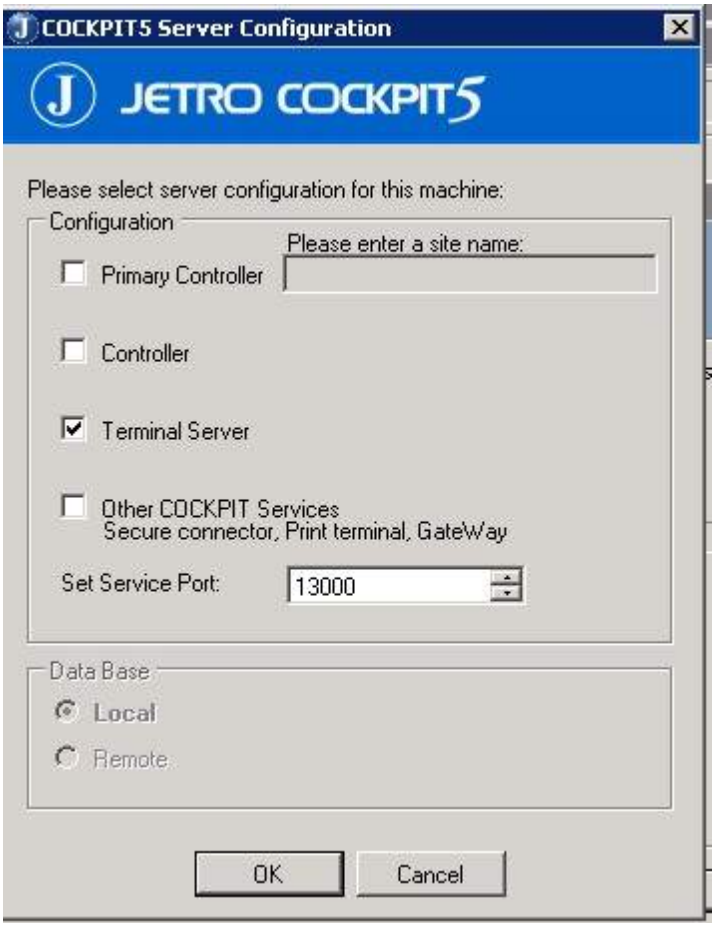
3.5 SP1 if it is not already installed.

Before installing the Terminal Server, ensure you have installed the Primary Controller.

To install the Terminal Server:

Logon to the Server that you want to assign as the Terminal Server, and login as Domain Admin to the console (session 0)

1. Run **COCKPIT5-Server.exe** from the files that you received from the Jetro package, and follow the wizard's instructions until you reach the **Server Configuration** screen.



2. Select the **Terminal Server** checkbox, to assign this Server as the Terminal Server.

3. Continue to follow the wizard's instructions.

Congratulations! The installation procedure has successfully installed the COCKPIT Terminal Server.

You are now in the Terminal Server environment.

Additional Options:

- To add additional Terminal Servers, repeat this procedure.

- To configure the Terminal Server, see the Hosts topic in the Configuration section.

This topic has one subtopic:

- Print Drivers Installation

Print Drivers Installation

This topic describes how to install the servers that enable the COCKPIT Printing Solution.

Installation Considerations:

- The COCKPIT system should be installed on every Terminal Server.
- If your organization uses a Print Terminal, then assign a Print Terminal role from the Administration Console.

To install a COCKPIT Printer Driver:

1. Logon to the Server that you want to assign as a Print Driver, and login as Domain Admin to the console (session 0).
2. Run **COCKPIT5-PrinterDrivers.exe** from the files that you received from the Jetro package, and follow the wizard's instructions.

NOTE During the installation, the **Hardware Installation** screen may appear. It appears if the printer drivers (PCL5, PCL6 and PostScript) have not passed a Window's Logo testing, which attempts to verify whether a driver is compatible with this version of Windows before installing it. The screen may appear 3 times, one for each printer driver. Click **Continue Anyway.**

Congratulations! The installation procedure has successfully installed the COCKPIT Printer Driver Server.

After completing the installation, COCKPIT-PrinterDrivers can be found in the Add or Remove Programs Window.

The following components are added to the Terminal Server:

- Printer Drivers
- JdsPort Port

Administration Console Installation

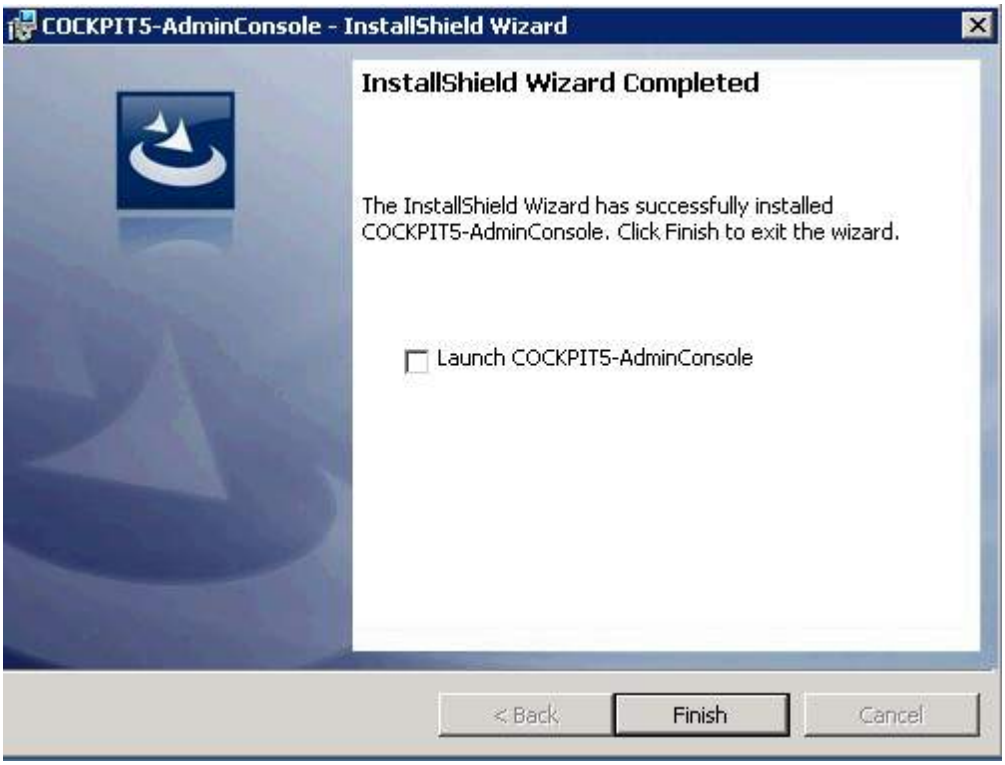
The System Administration Console provides the System Administrator with a centralized platform where he can configure, maintain, and troubleshoot the system.

Installation Considerations:

- It is recommended to install an Administration Console on the Primary Controller. This enables the administrator to configure the system and to verify that the system is functioning properly.
- System Administrators may find it convenient to install the Administration Console on their personal workstations, as shown in the system architecture diagram.

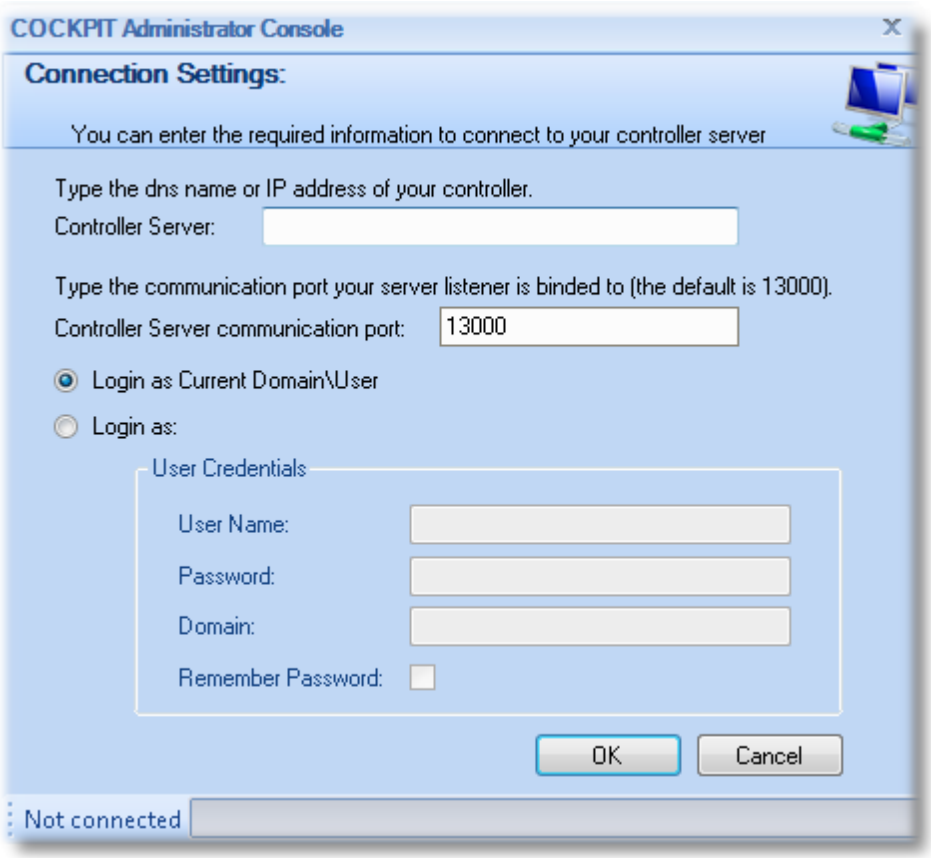
To Install the COCKPIT Administration Console:

1. Run **COCKPIT5-AdminConsole.exe** from the files that you received from the Jetro package. Follow the wizard's instructions until you reach the **InstallShield Wizard Completed** screen.



2. Launch the Administration Console by checking the **Launch COCKPIT5-AdminConsole** box at the end of the wizard, or click the Admin Console icon from the desktop after installation.

The **Connection Settings** screen appears. This screen only appears the first time you launch the Administration Console.



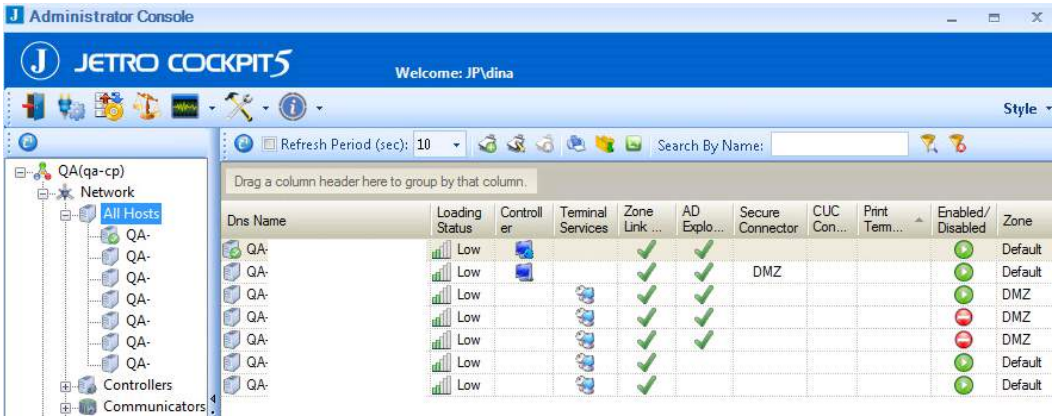
a) In the **Controller Server** field, enter the Server name or IP address of the Controller Server.

b) Leave the **Controller Server communication port** field value at 13000.

c) Select the **Login as** box, and enter your user name, password and the domain of the Controller.

3. Click **OK** to launch the Administration Console. The Primary Controller appears on the bottom left of the window.

4. Select the **Network > All Hosts** branch to display a list of all the defined hosts in this site.



5. Verify that the columns shown above have green checkmarks or icons.

Chapter 5: Configuring COCKPIT

This chapter contains basic configuration changes for the system to operate normally in your specific network architecture. Basic information only is provided. For more detailed information on all configuration options, refer to the COCKPIT User Guide.

This chapter contains the following topics:

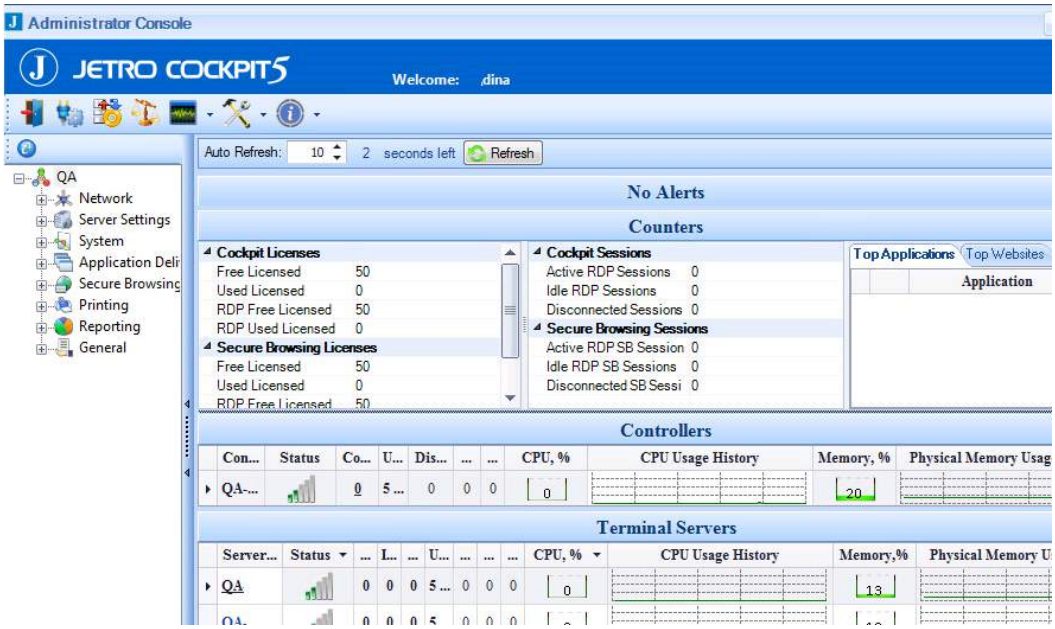
Logging on to the Administration Console

The Administration Console provides the ability to configure the COCKPIT site components. You need to be logged on to the Administration Console to configure the COCKPIT Servers. The COCKPIT Administration Console provides the site administration functionality. It is a graphical user interface (GUI) connected to the Primary Controller, which communicates with all the other COCKPIT site components, such as the Terminal Server COCKPIT Agents.

An administrator can use the Administration Console to configure the servers as well as to define which users can access which Applications and when.

To login to the Administration Console, click on the Administration Console icon.

The Administration Console screen appears:



The Administration Console window contains the following sections:

- **Menu Bar**

The Menu Bar contains buttons that enable you to carry out various functions including changing the connection settings.

- **Tree**

The administration tree provides access to all the configurable aspects of the COCKPIT site, such as managing items on the network and setting domains and zones. For detailed information on all the branches, see the COCKPIT User Guide.

- **Work Area**

The Work Area shows specific parameters and options for a selected branch in the tree.

Configuring the License Server

The License Server defines the maximum number of concurrent users that are able to use COCKPIT desktops simultaneously. This topic describes how to configure the Secure Browsing License Server Installation that you installed, as described in the Installation section.

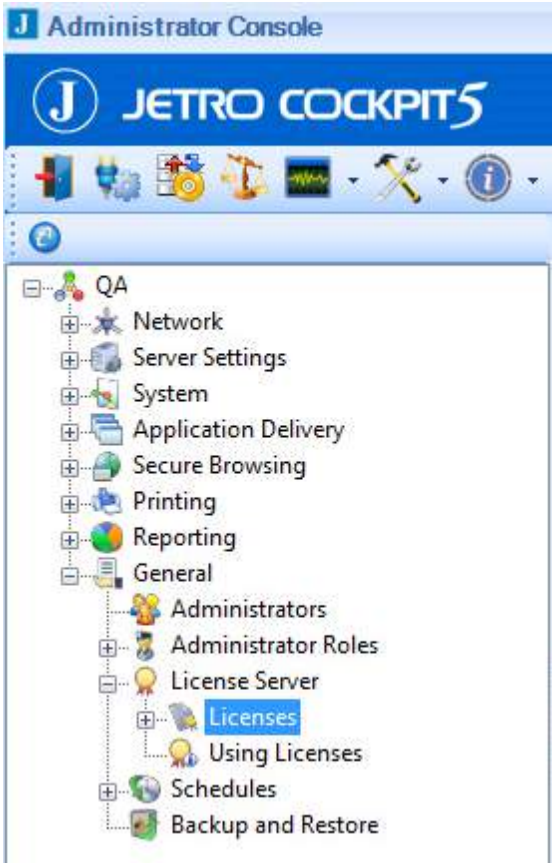
By default, COCKPIT software runs in evaluation mode. This automatically expires 30 days after installing the system. In order to be able to continue to use the COCKPIT software you MUST have a license activation key.

Configuration Prerequisites:

1. The Administrator Console that is used to register and activate the license should be installed on the COCKPIT Primary controller, and it should be launched from there.
2. The license activation file should be located on a local drive of the COCKPIT Primary Controller.

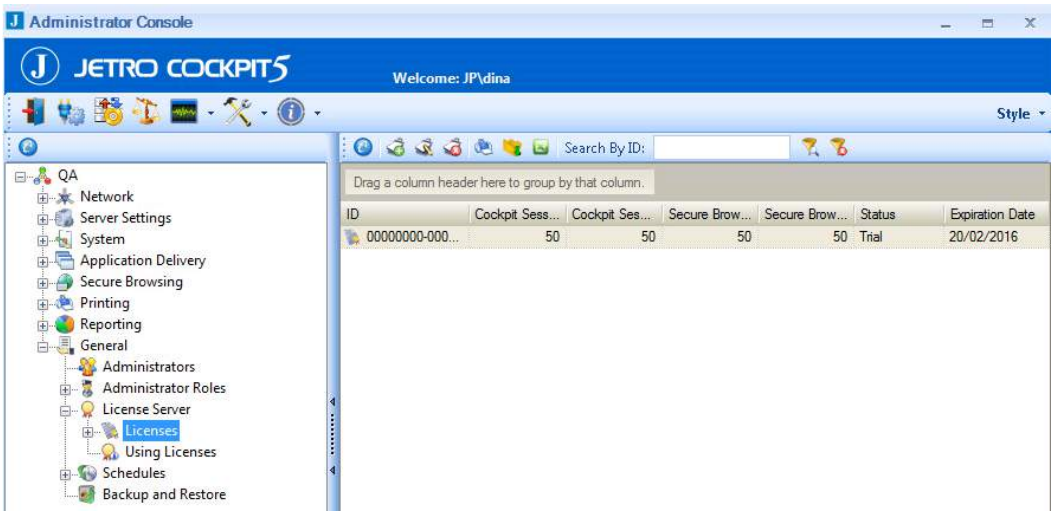
To attach and activate a license for the COCKPIT software on a server without internet access:

1. Connect to the COCKPIT Administrator Console.
2. From the COCKPIT Administrator Console tree, click “+” next to the **General** folder. A sub-tree appears.

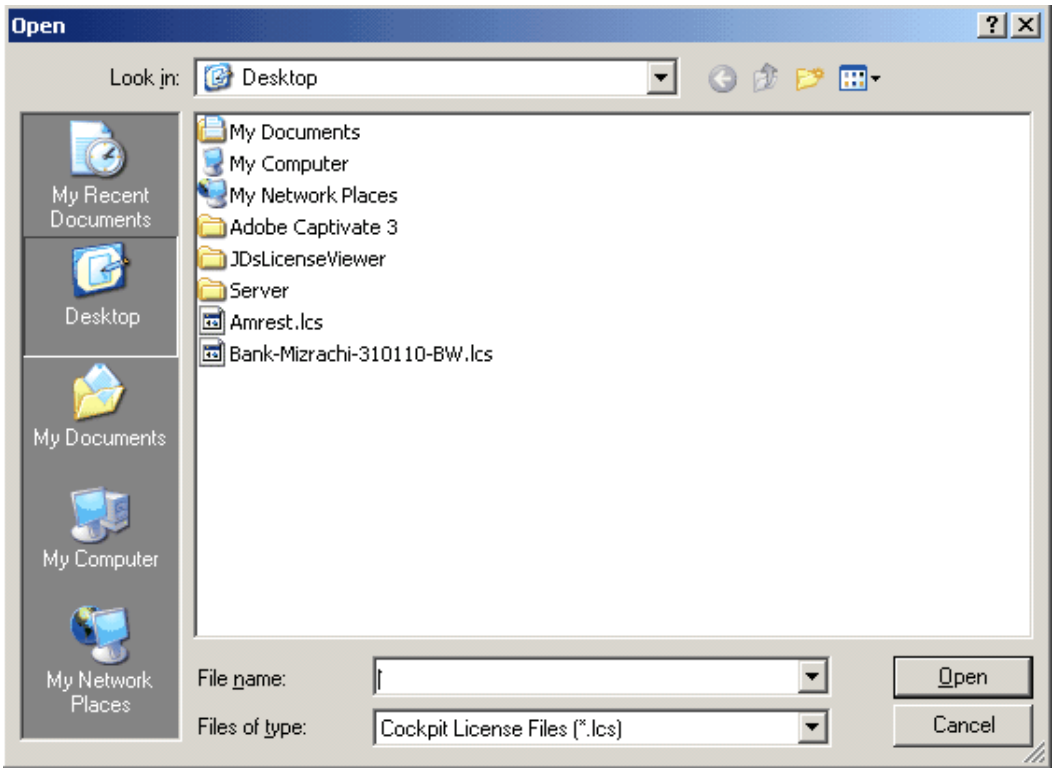


3. Click “+” next to the **License Server** folder. A sub-tree appears.

4. Click the **License** folder. The right-hand pane displays the licenses that are already attached and displayed for this License Server.

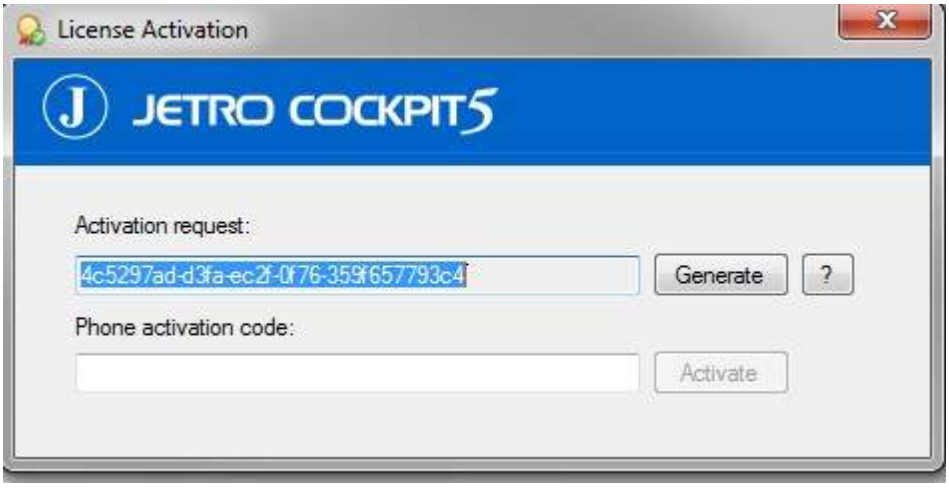


5. From the toolbar in right-hand pane, click on the **New License** icon  . A screen appears displaying COCKPIT license files.



6. Locate the license activation file that was saved on the COCKPIT Primary Controller, and click the **Open** button to initiate attaching and activating the license. The following message appears.

7. Click the **OK** button. The **License Activation** screen appears, displaying an **Activation Request** code:



8. Copy and paste the code into a text editor document.

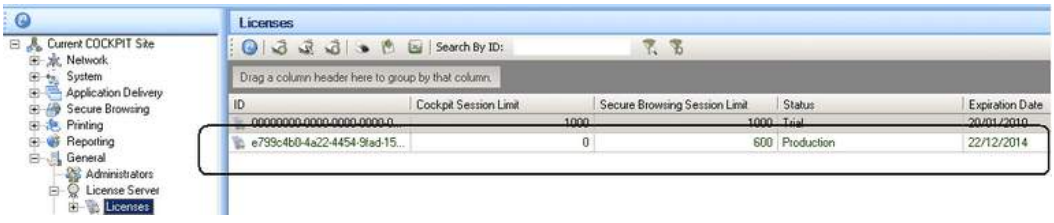
9. Transfer the document to a computer with internet access.

10. Send the Activation Request code to Jetro Support in an email to support@jetroplatforms.com. You will receive a reply with a Phone Activation code.

11. Enter the Phone Activation code into the **Phone Activation** Field in the **License Activation** screen shown above.

12. In the **License Activation** screen, click the **Activate** button.

An additional line appears in the right-hand pane of the **License** folder, indicating that the COCKPIT Controller has successfully imported and activated the license offline.



13. In the right-hand pane, delete outdated licenses, by right-clicking on the license and selecting Delete.

Congratulations! You have successfully completed the COCKPIT license activation process.

Configuring the Connection to the Hosts

This section describes how to add new hosts to your COCKPIT Server Farm. A host is any component of the COCKPIT Farm such as, Controllers, Communicators, Terminal Servers, and Active Directory Servers.

The Secure Browsing service must first be installed and running before adding a host in the administrator console.

This topic has two subtopics:

- Adding a Host - COCKPIT External Gateway and Active Directory Explorer Server
- Adding a Host - COCKPIT Terminal Server

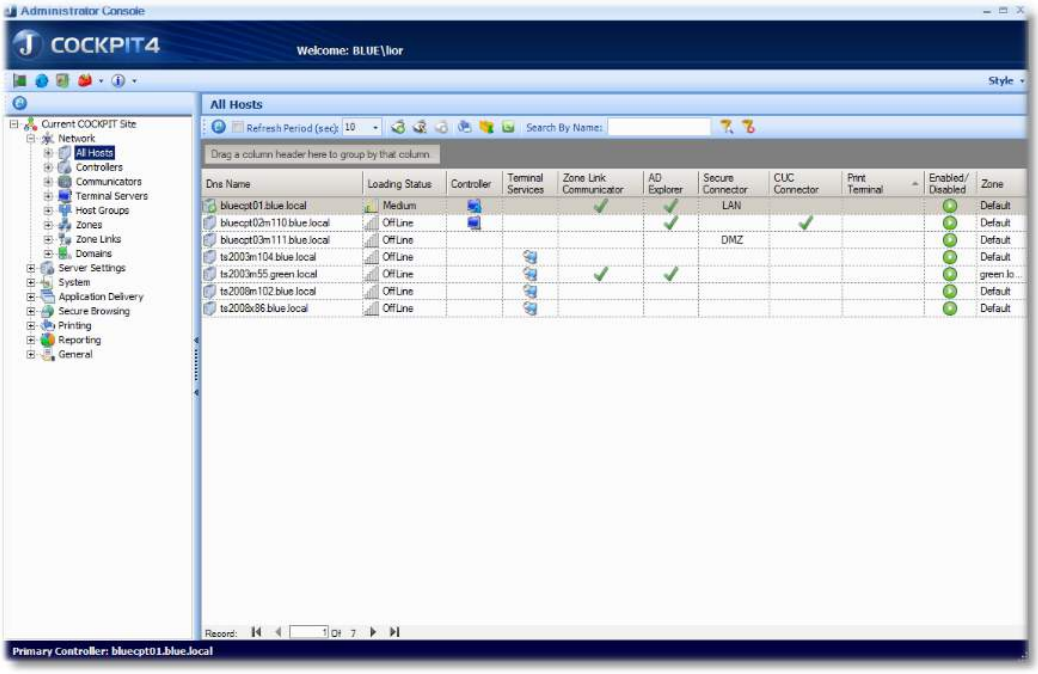
Adding a Host - COCKPIT External Gateway and Active Directory Explorer Server

This section describes how to add a COCKPIT5i External Gateway+Active Directory Explorer Server host to the Secure Browsing site.

The Secure Browsing service must first be installed and running before adding a host in the administrator console, as described below.

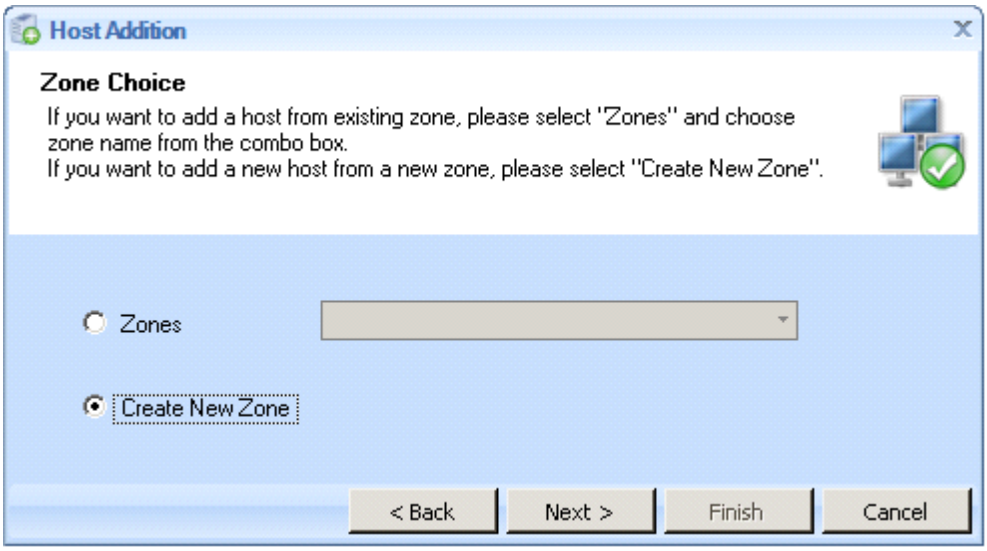
To add an External Gateway+Active Directory Explorer Server host:

1. Select the **Network > All Hosts** branch to display a list of all the hosts defined in the COCKPIT5i site, as shown below:



2. Right-click in the center of the page and select New or click the **New** tool. The first page of the **Host Addition Wizard** appears:

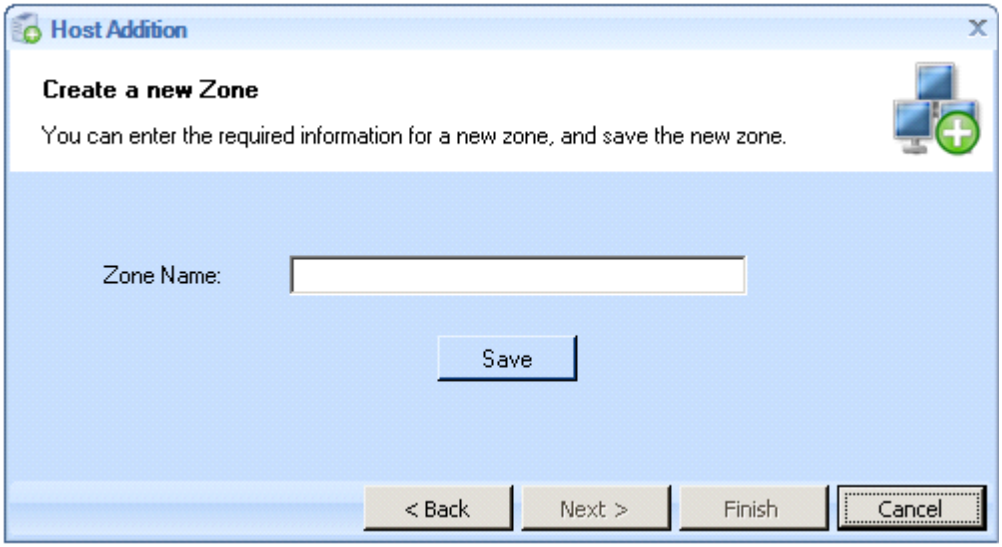
3. Click **Next** to display the **Zone Choice** screen:



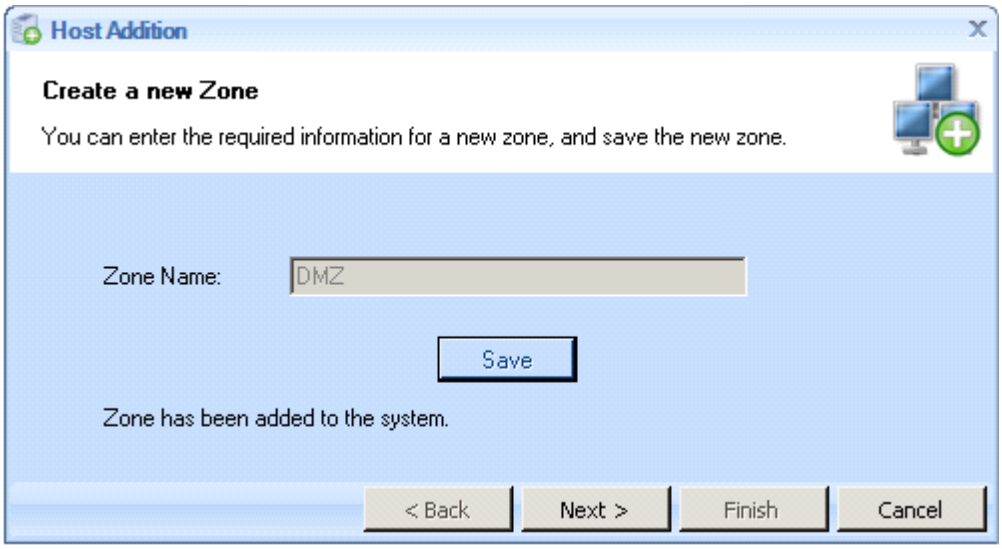
This screen enables you to define within which Zone the new host resides. A network is divided into segments by nature. A Zone can be either a remote or local network segment. In COCKPIT5i, a Zone defines the network segment in which each Secure Browsing component resides. The External Gateway+Active Directory Explorer Server is in the DMZ see External Gateway+Active Directory Explorer. You now create this zone.

4. To create a zone, select the **Create New Zone**.checkbox.

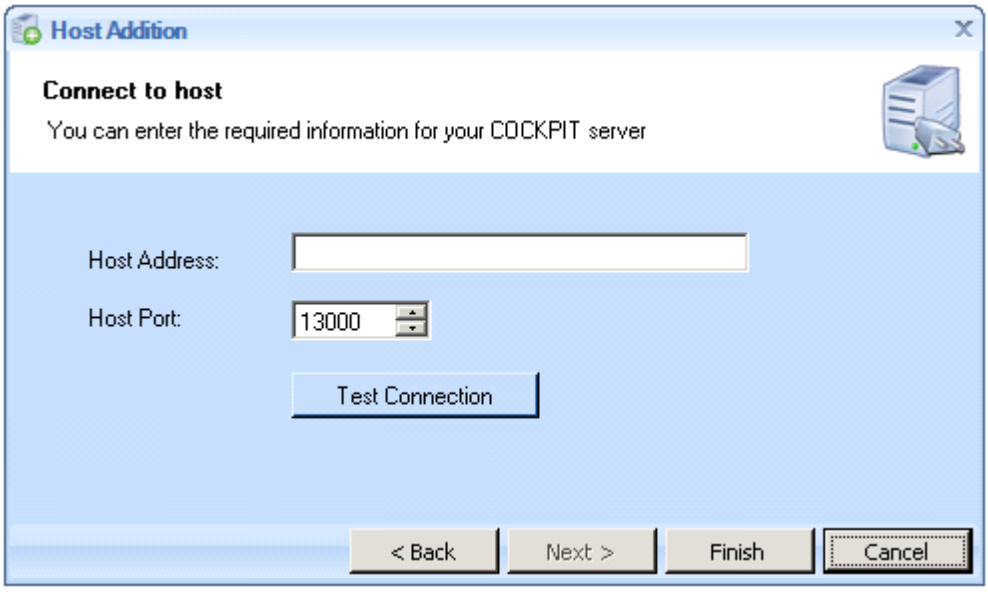
5. Click **Next** to display the **Create New Zone** screen:



6. In the **Zone Name** field, enter a name for this zone and click **Save**. A confirmation message appears:



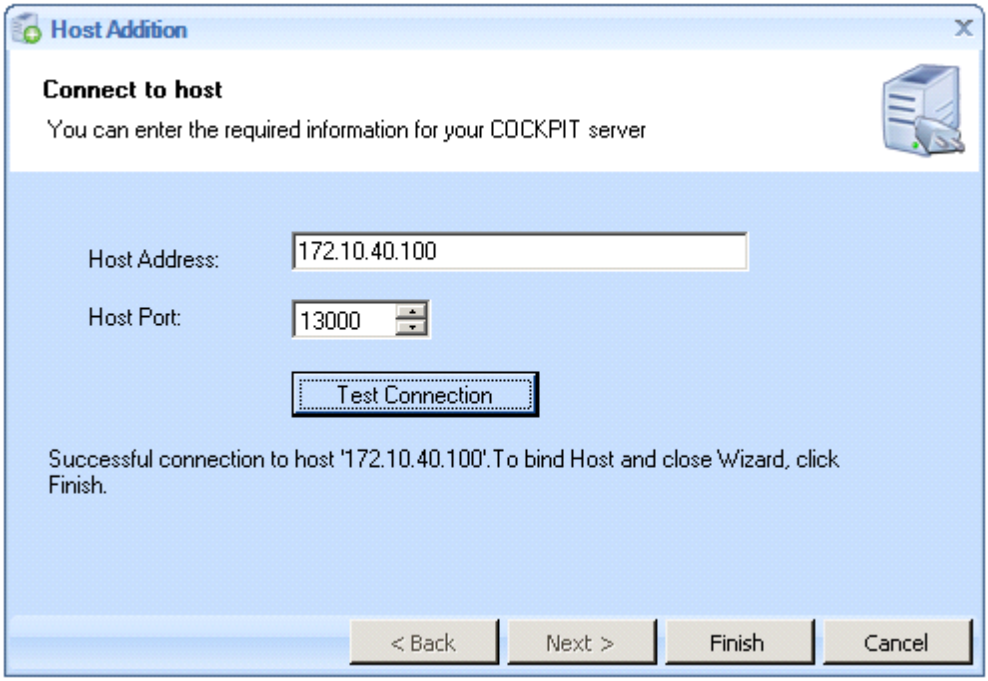
7. Click **Next** to display the **Connect to host** screen:



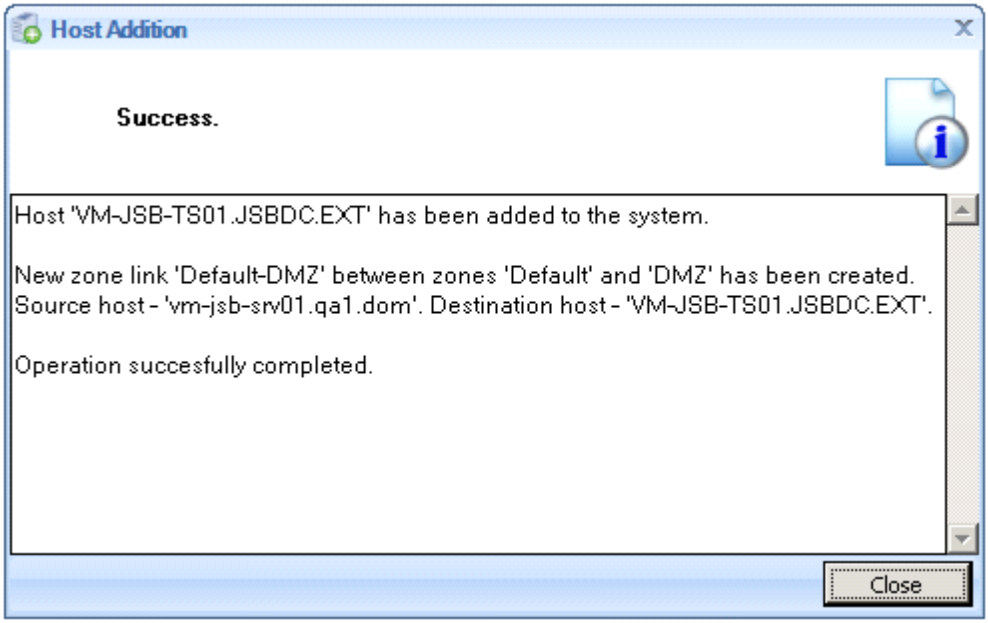
8. In this screen you define the connection between this host and the External Gateway, as follows:

   - In the **Host Address** field, specify the host's name or IP address.
   - Leave the **Host Port** field.

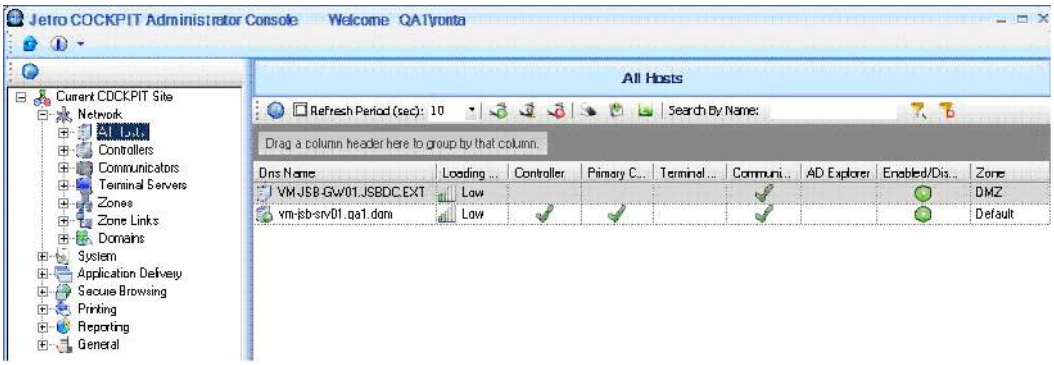
9. Click the **Test Connection** button to confirm that the External Gateway can communicate with this host through this port. A success message should be displayed at the bottom of the screen:



10. Click **Finish** to close the Host Connection Wizard. The following **Success** screen appears:



The administrator console now shows a new row representing the COCKPIT5i External Gateway+Active Directory Explorer Server that was added. As shown below, it is in the DMZ, it is a Communicator (as indicated by the green checkmark):



Adding a Host - COCKPIT Terminal Server

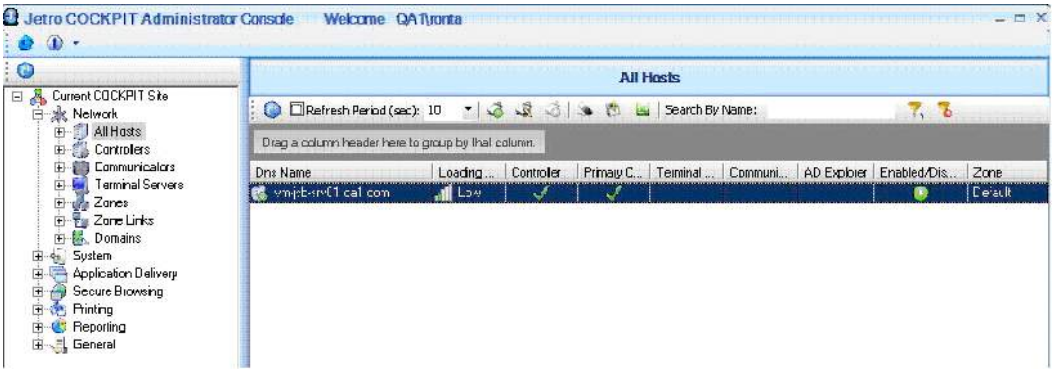
This section describes how to add one COCKPIT5i Terminal Server host to the Secure Browsing site. After you have completed all the processes in this guide and have tested that Secure Browsing is functioning properly, you can then add as many Terminal Servers as required.

The Secure Browsing service must first be installed and running before adding a Terminal Server in the administrator console, as described below.

Terminal Servers run browsers for COCKPIT5i Clients. The Terminal Servers are able to communicate with the Internet through the external firewall, via standard Internet protocols such as HTTP, HTTPS or FTP protocol.

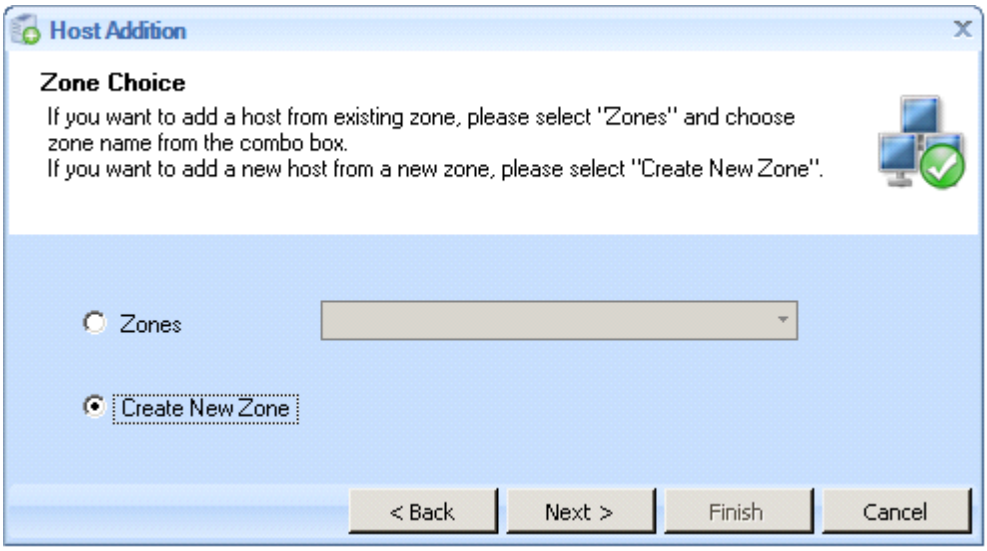
To add a Terminal Server:

1. Select the **Network > All Hosts** branch to display a list of all the hosts defined in the COCKPIT5i site:



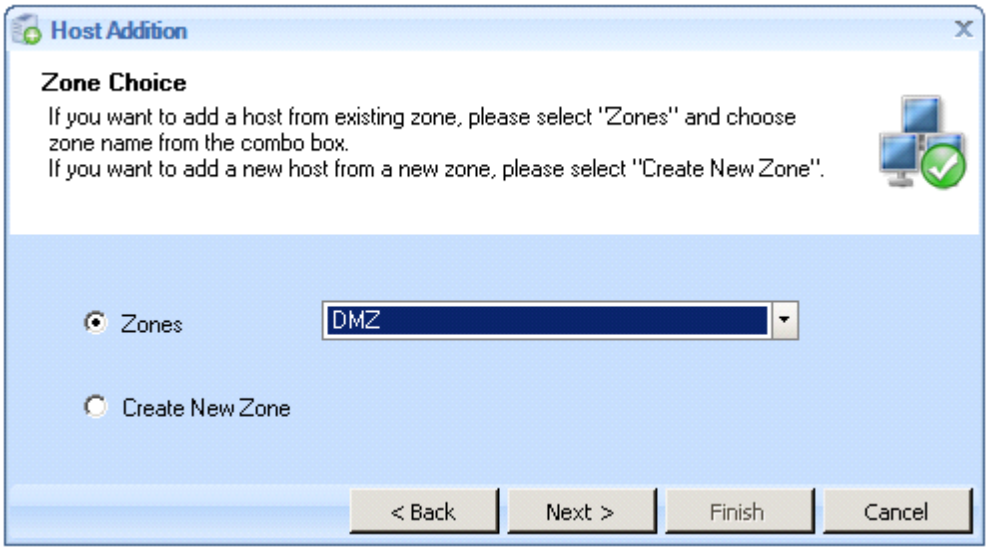
2. Right-click in the center of the page and select **New** or click the **New** tool. The first page of the **Host Addition Wizard** appears:

3. Click **Next** to display the **Zone Choice** screen:

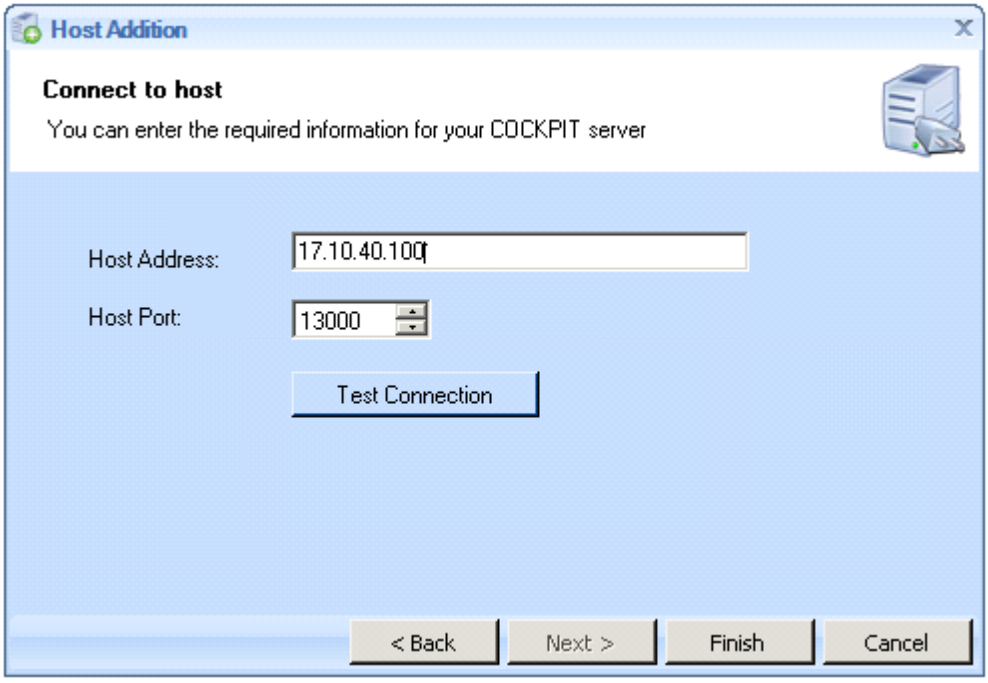


This screen enables you to define within which zone the new host resides. A network is divided into segments by nature. A zone can be either a remote or local network segment. In COCKPIT5i, a zone defines the network segment in which each Secure Browsing component resides. The Terminal Server is in the DMZ. You created this zone in the previous topic - Adding an External Gateway+Active Directory Explorer Server.

4. To specify the zone in which this Terminal Server is located, select the Zone option and then select the same zone as the External Gateway. In this example it is DMZ:



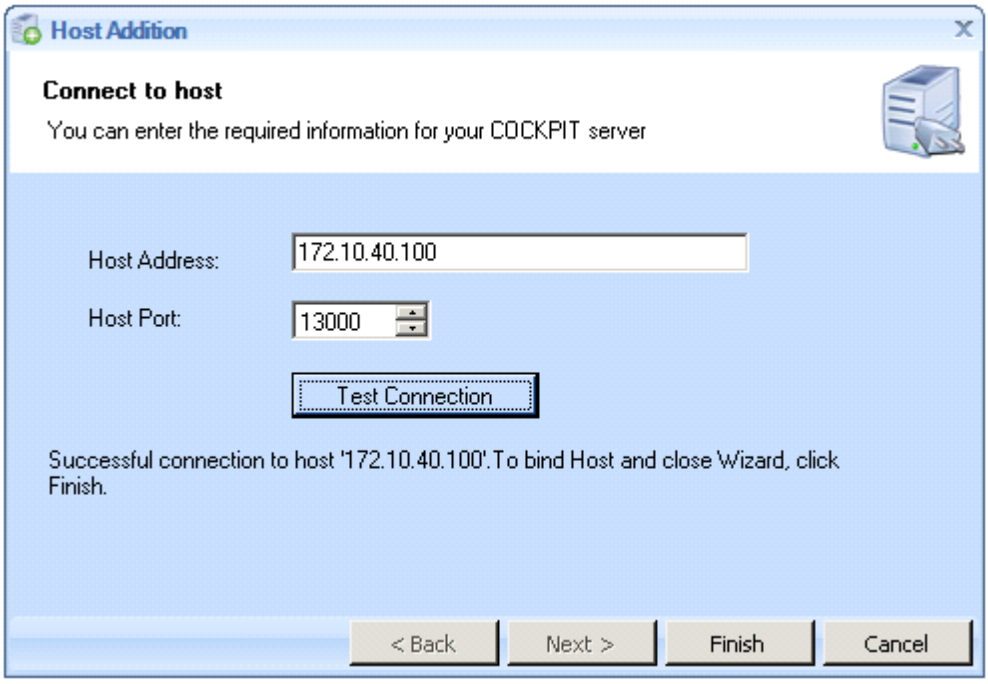
5. Click **Next** to display the **Connect to Host** screen:



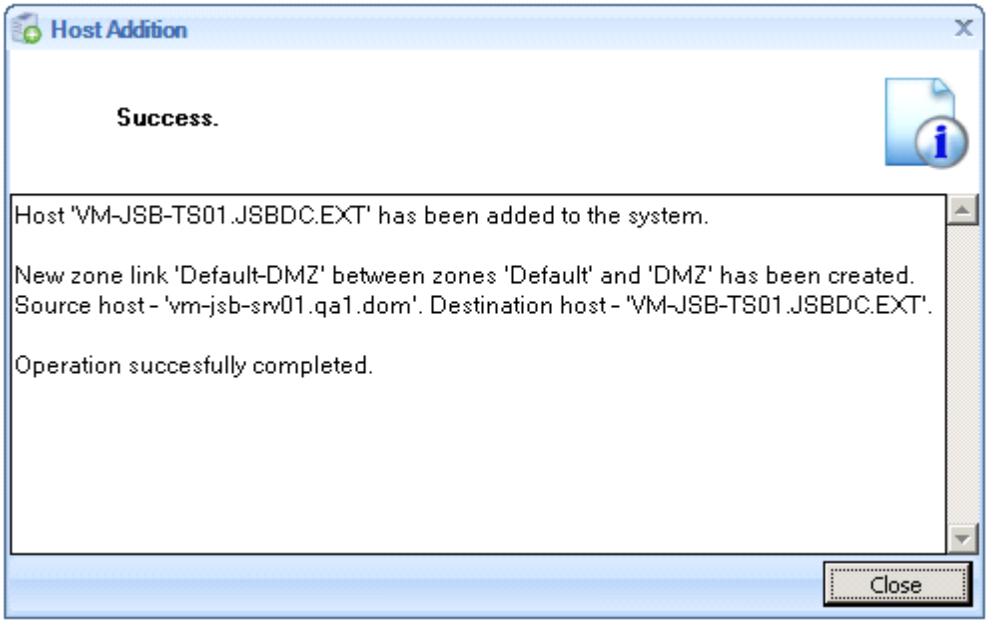
In this screen you define the connection between this host and the Terminal Server, as follows:

- In the **Host Address** field, specify the host's name or IP address.
- Leave the **Host Port** field.

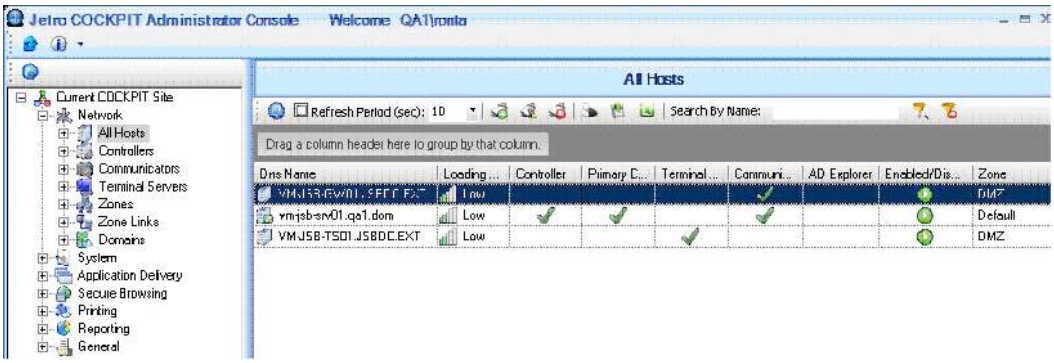
6. Click the **Test Connection** button to confirm that the Terminal Server can communicate with this host through this port. A success message should be displayed at the bottom of the screen:



7. Click **Finish** to close the Host Connection Wizard. The following **Success** screen appears:



This screen also now shows a new row representing the COCKPIT5i Terminal Server that was added. As shown below, it is in the DMZ, it is a Communicator (as indicated by the green checkmark)



Configuring Domains

A domain is the environment where a user is granted access to a number of computer resources.

The domain controllers are the servers that run Active Directory. Active Directory provides a central location for the network administration and security. It authenticates and authorizes all users and computers in the domain—assigning and enforcing security policies for all computers and installing or updating software. In order for a user to log on, that user must have an account in the Active Directory. That user can then log on from any computer.

A Client's membership in a Domain in the Active Directory, is used as the security object when configuring security settings and application permissions.

Secure Browsing uses Active Directory objects to manage users or user groups. In a Secure Browsing environment, at least two Active Directory domains are required: one in the internal domain and one in the external domain.

NOTE: If both COCKPIT Application Delivery and Secure Browsing are installed in the same environment, then the Active Directory domain used by COCKPIT Application Delivery will serve as the internal Active Directory domain for Secure Browsing and you must also register the external Active Directory domain for Secure Browsing.

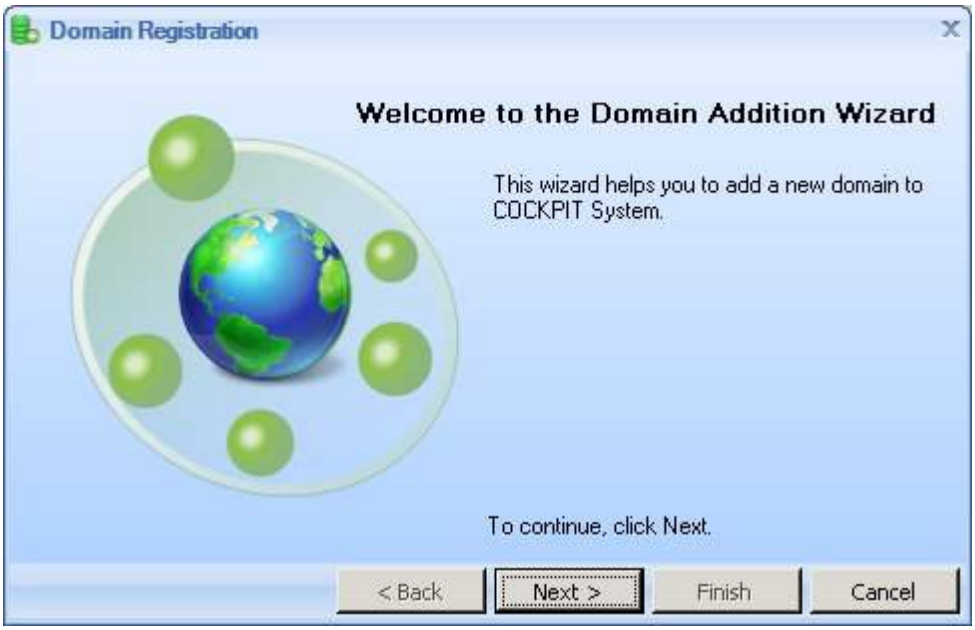
NOTE: In Secure Browsing, in order to log on, the computer must be a member in the Active Directory and the user must also have an Active Directory account.

The following describes how to register the two Active Directory domains required for Secure Browsing: the internal one and the external one:

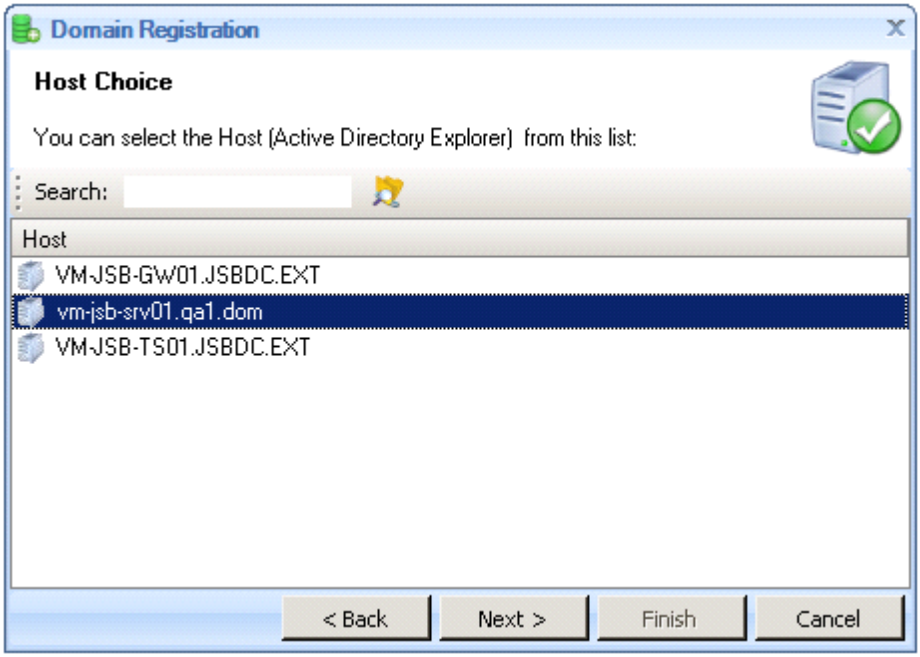
To add an internal domain for determining user access:

1. Open the Administration Console, and select the **Network > Domains** branch.

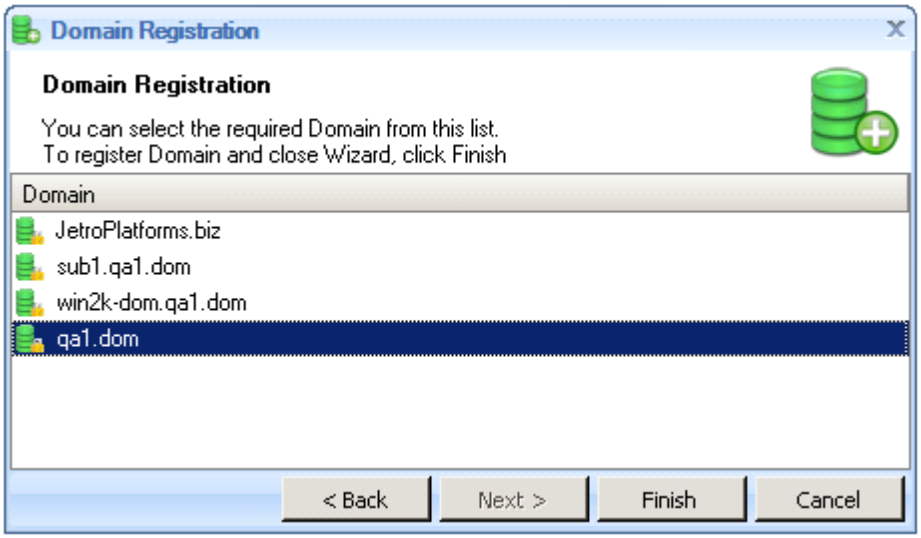
2. Right-click in the center of the page and select **New**, or click the **New** tool. The first page of the **Domain Addition Wizard** appears:



3. Click **Next** to continue. A list of the defined hosts is displayed in the Host Choice screen:



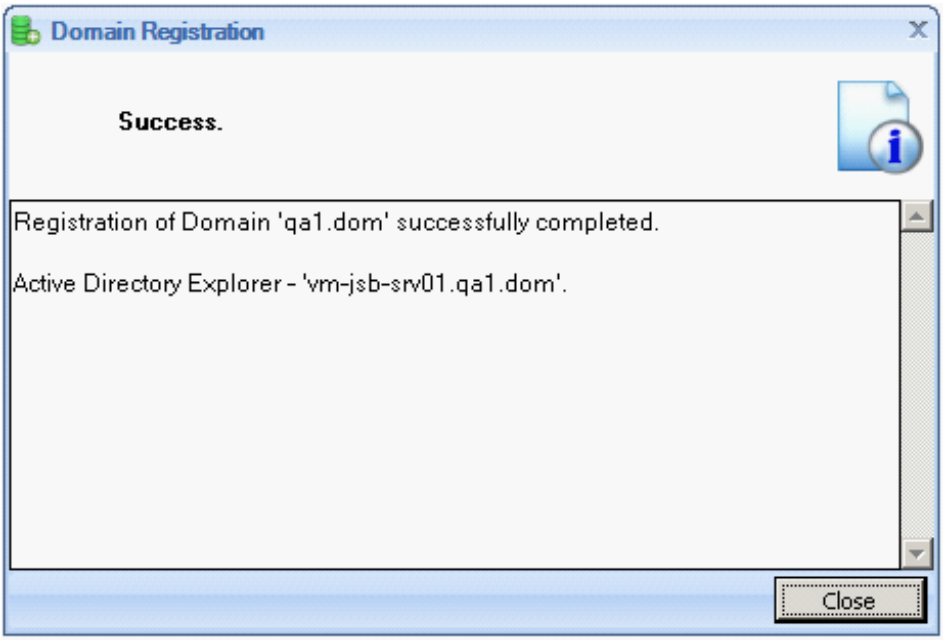
4. Select the Primary Controller host and click **Next** to display a list of all the domains that this Controller can see:



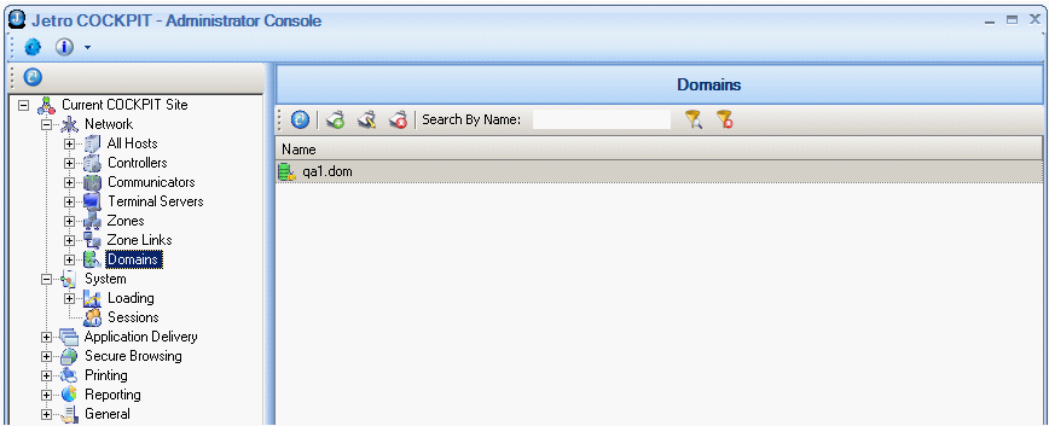
5. Select the domain that the Controller is registered in.

NOTE - This domain is only for deciding which users in your organization may surf.

6. Click **Finish**. The **Domain Registration** screen announces that the selected domain was registered successfully, and tells you the name of domain's Active Directory Explorer.



7. Click **Close**. The System Administrator Console is displayed showing the newly registered domain.



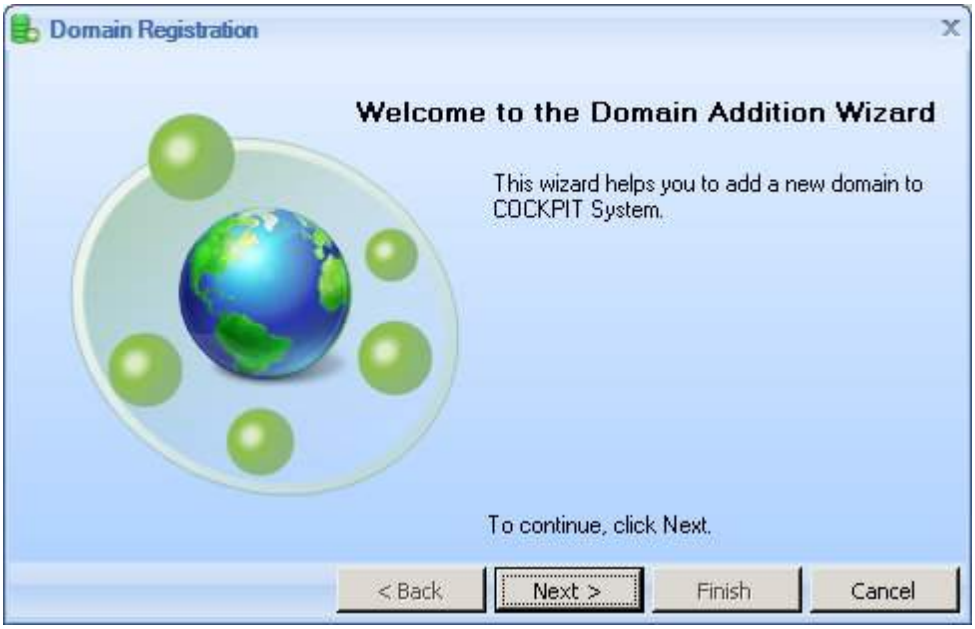
Note the following changes to the Console:

- The name of the registered domain appears in the list to the left of the display area.
- The name of the registered domain appears in the DNS Name field.
- The NetBIOS Name for the domain appears as well.

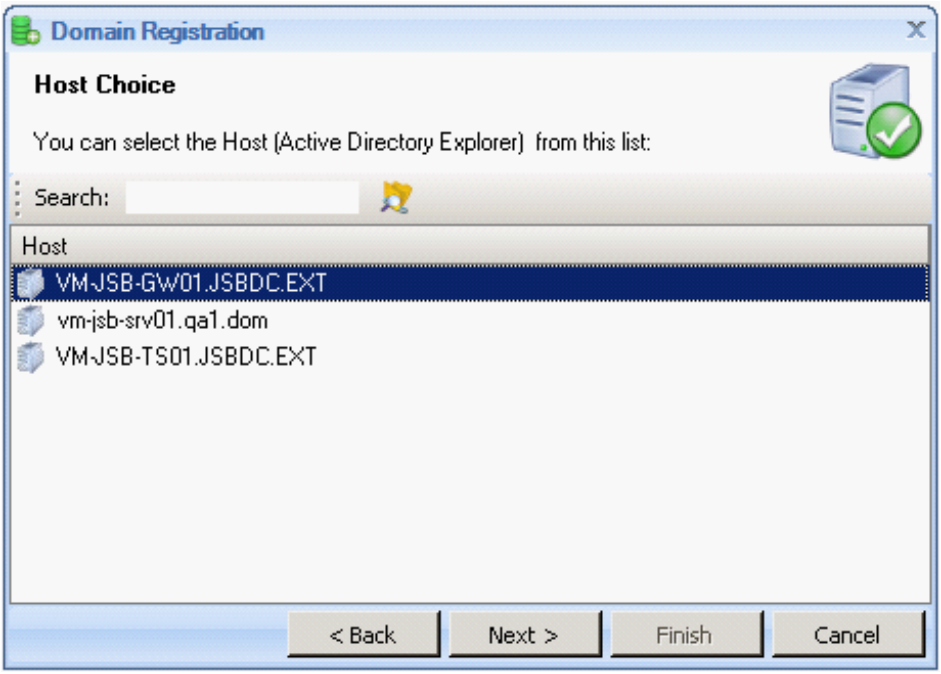
Summary: In a Secure Browsing environment, at least two Active Directory domains are required: one in the internal domain, as described above, and one in the external domain, as described below. See the Secure Browsing Architecture for more details.

To add an external domain:

1. Right-click in the center of the page and select **New** or click the **New** tool. The **Domain Addition Wizard Welcome** screen appears.

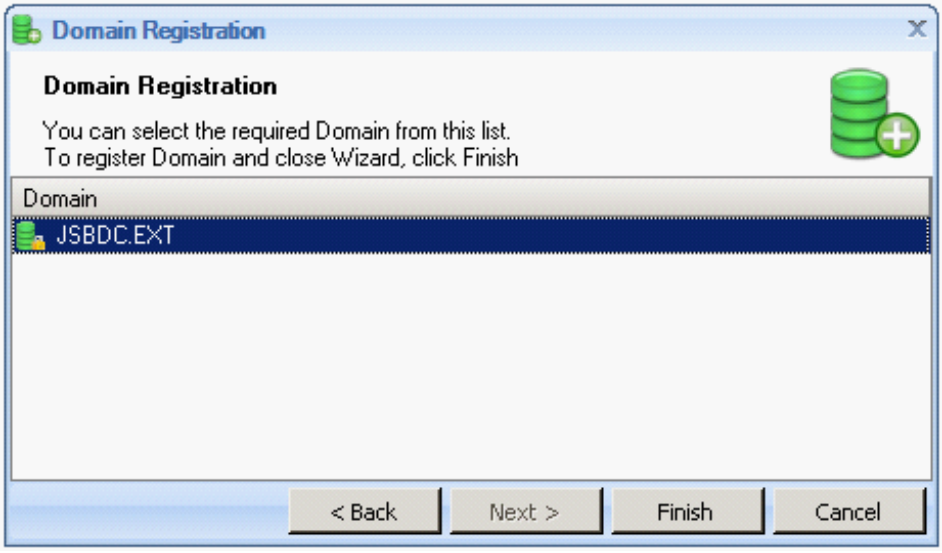


2. Click **Next**. A list of the defined hosts appears in the **Host Choice** screen:



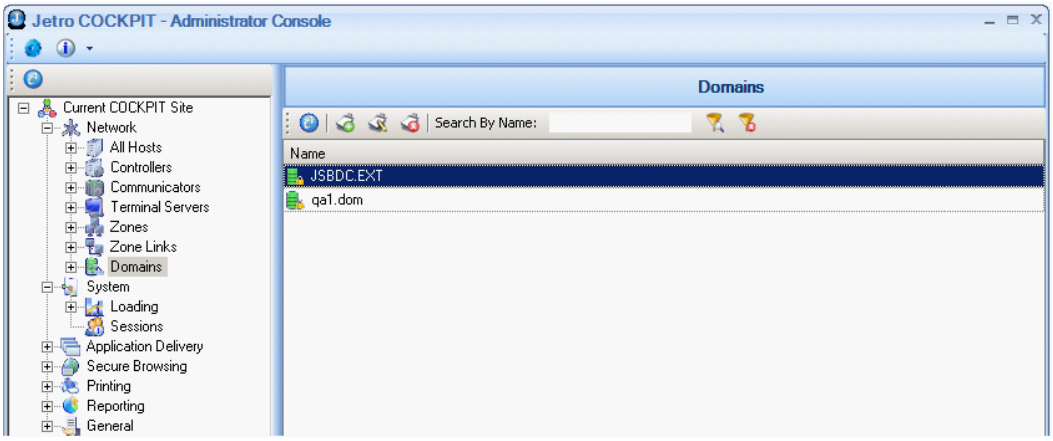
3. Select the External Gateway Server from the list of available hosts.

4. Click **Next**. The **Domain Registration** screen appears, highlighting the name of the External Gateway domain that you have selected.



5. Click **Finish**. The system registers the External Domain. The **Domain Registration Success** screen appears:

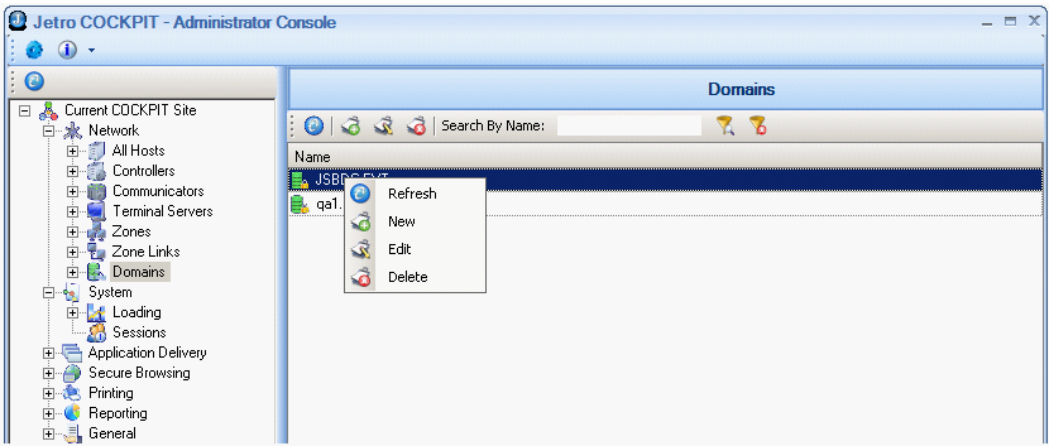
6. Click **Close**. The System **Administrator Console** appears displaying the newly registered domain.



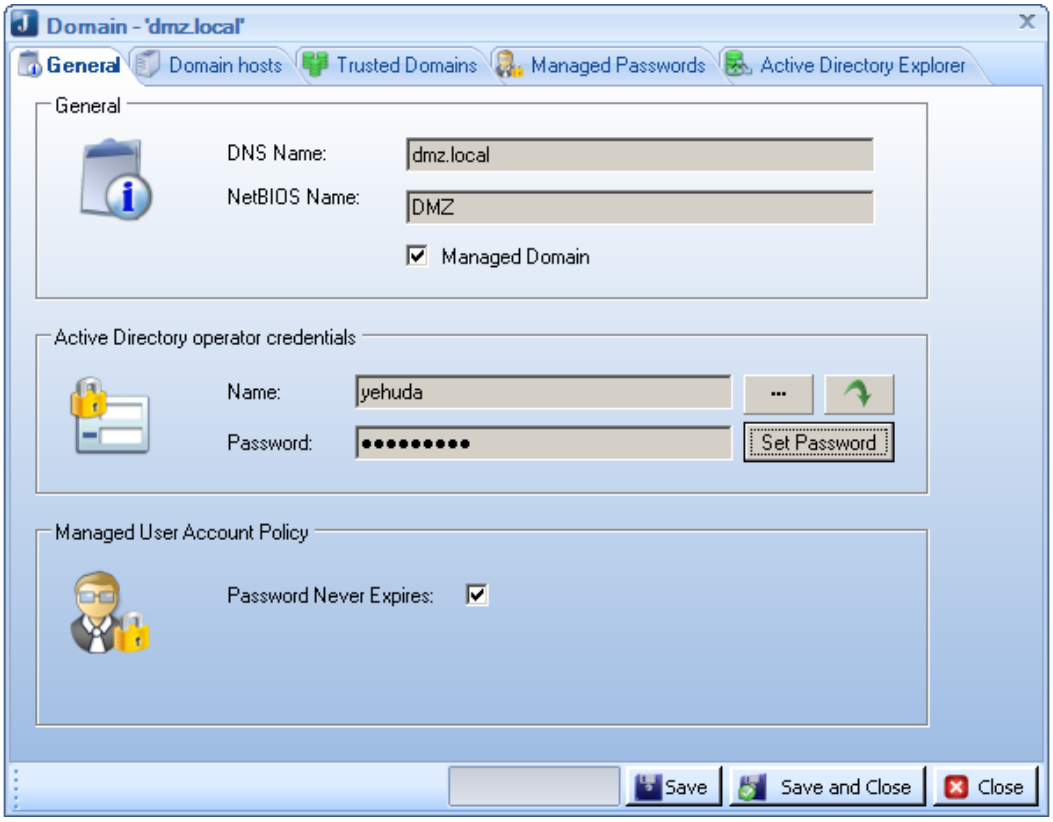
Note the following changes to the Console:

- Notice two domains - internal and external - in the **Domains** list.
- The name of the registered external domain appears in the **DNS Name** field.
- The NetBIOS Name for the domain appears.

7. To designate the external domain as managed, right-click on the External Gateway's row and select the **Edit** option:



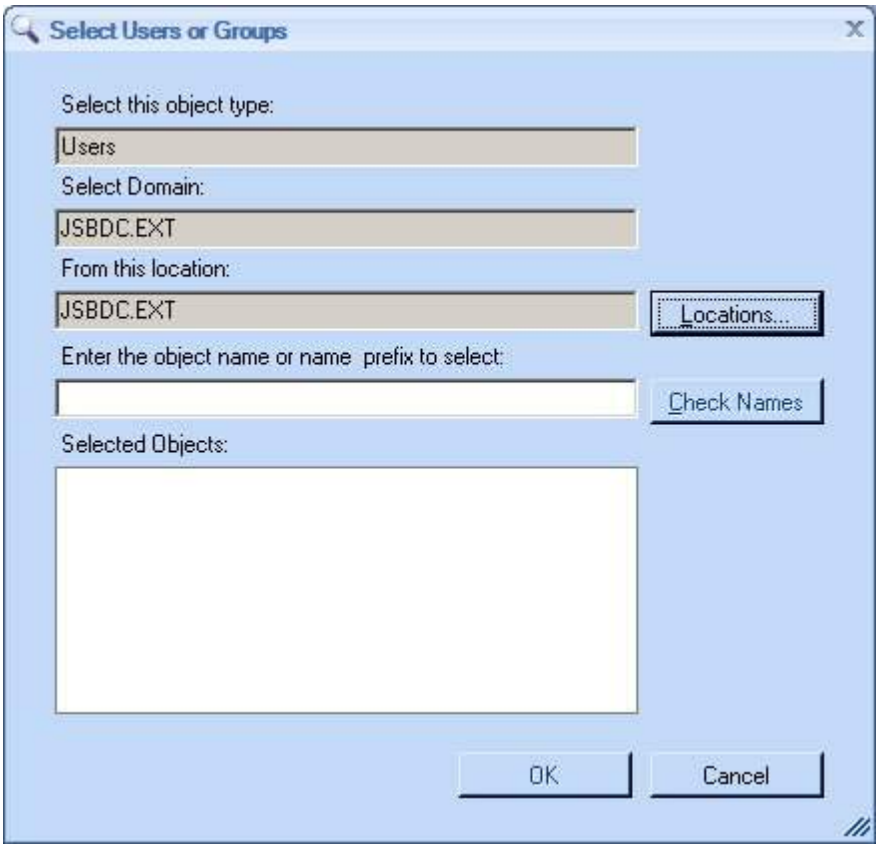
The following screen appears:



8. Select the **Managed Domain** checkbox for the external domain.

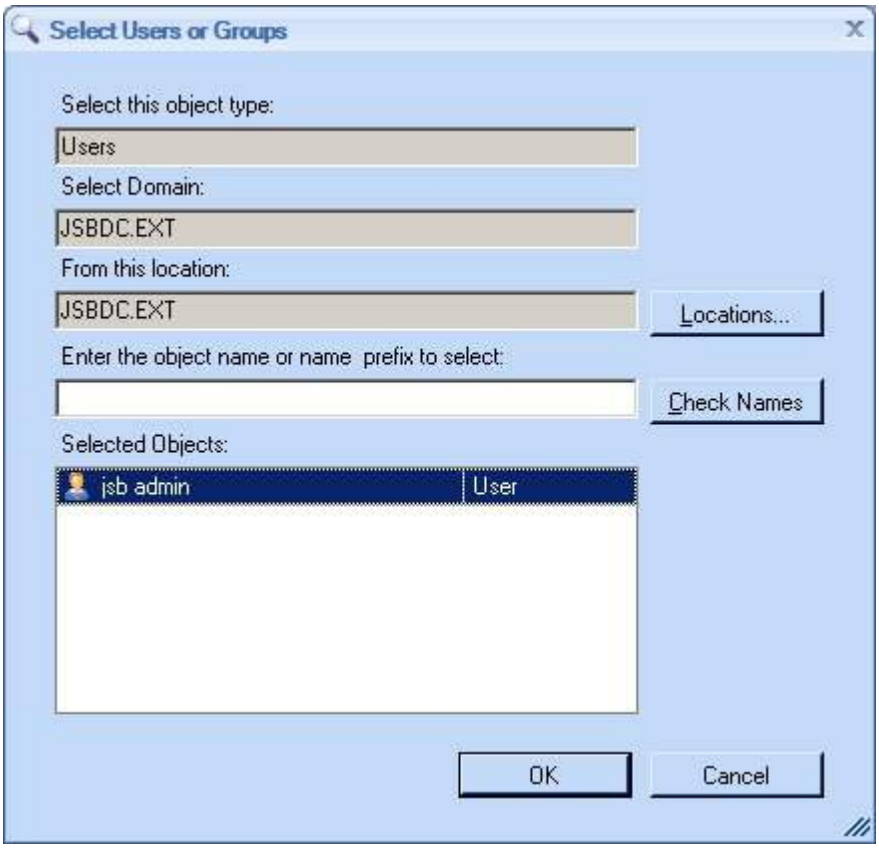
9. Specify the Active Directory used by the External Gateway in the **Active Directory Operator Credentials** area of the **General** tab, by clicking .

   The **Select Users or Groups** screen appears:



NOTE: The name of the registered external domain appears in the **Select Domain** and **From this Location** fields in the screen. This is the domain where you define user permissions. Later, if you define multiple external domains, you can select a different location.

10. Specify a domain administrator (this user must be an administrator) in the **Enter the object name or name prefix to select** field and click **Check Names**. The **Selected Objects** list shows the name of the User (group).



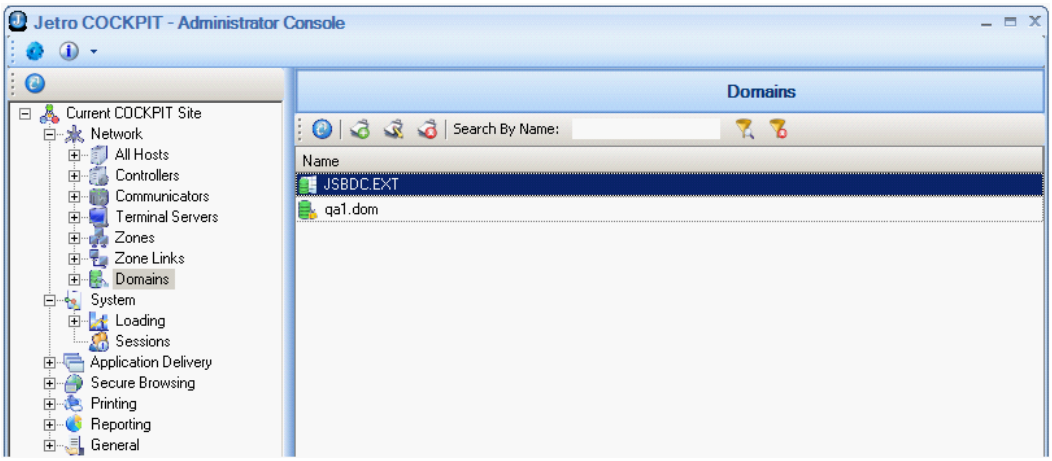
11. Click **OK**.

12. Click the **Set Password** button. The **Enter Administrator Password** screen appears:

13. Enter a password in the **Password** field, and confirm the password in the **Confirm Password** field.

NOTE: If you change the password in the Active Directory, you must change the password here to match it. Ensure that this password is only stored encrypted in the database of the Primary Controller and that it is never transmitted outside.

14. Click the **Save and Close** button. The external domain now appears with a different icon, to indicate that it is managed, as shown below:

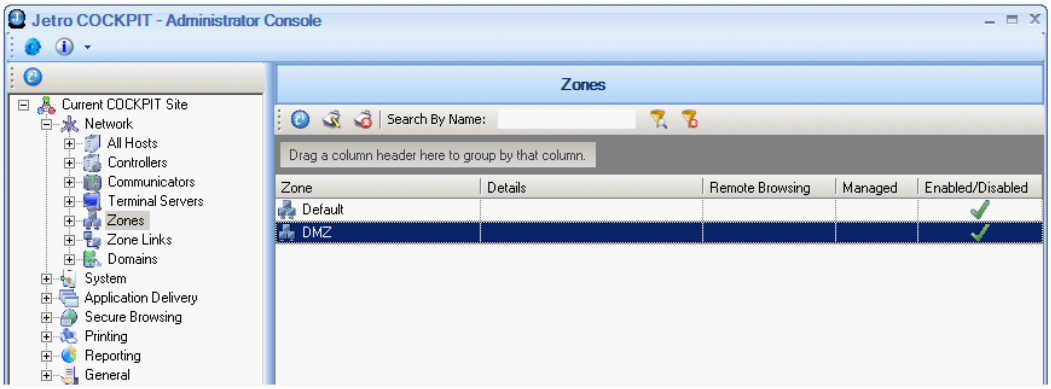


Configuring Zones

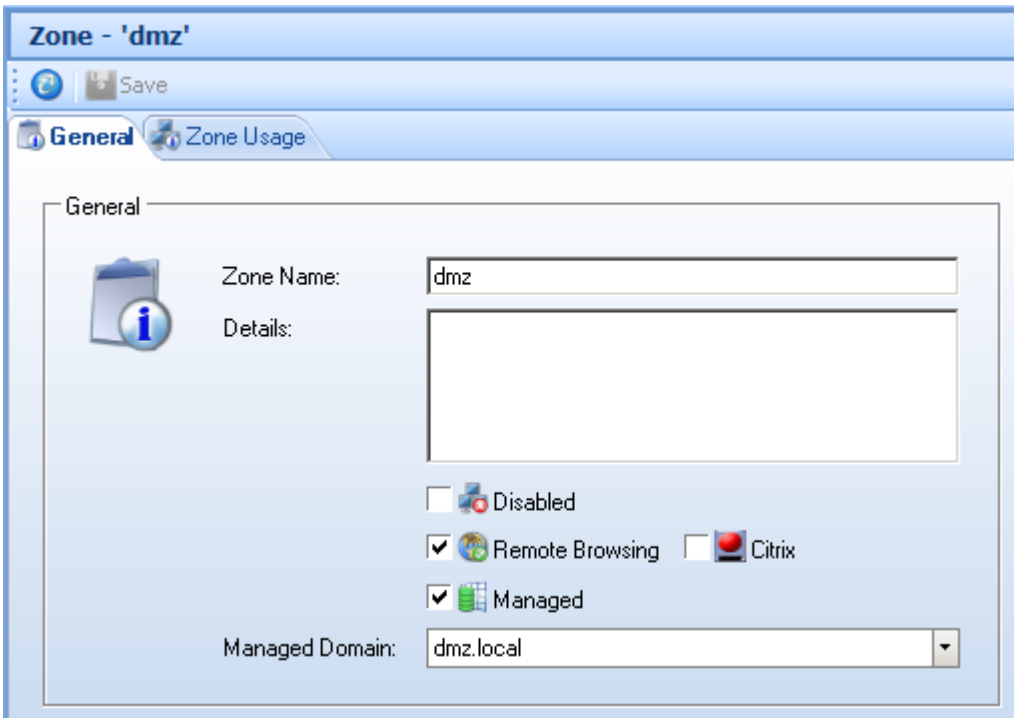
Now that you have defined both the internal and the external domains, you must configure the Zones of each. Zones are the logical entities in the Secure Browsing system used to represent domains and to enable their links.

To configure a zone:

1. Select the **Networks > Zones** branch to display a list of all the defined Zones:

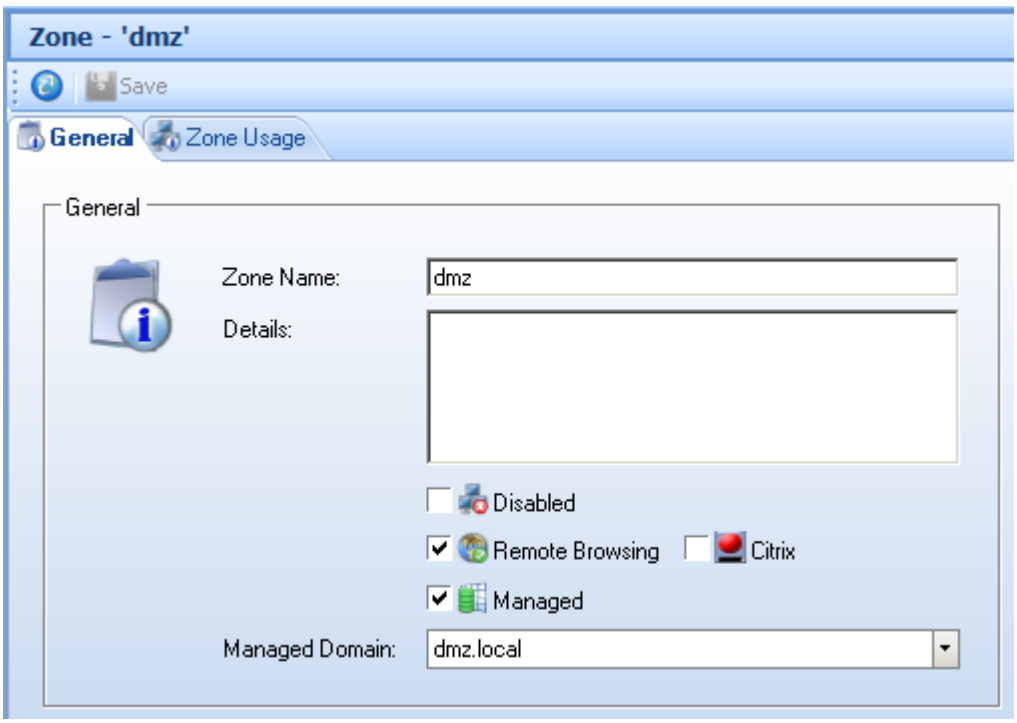


2. Right-click on the External Zone (in the example above, it is called **DMZ**) and select the **Edit** option to display the following screen:



The selected External Zone name appears in the **Zone Name** field.

3. In the **General** tab, select the **Remote Browsing** and **Managed** checkboxes, to designate this zone as a remote browsing and managed zone, as shown below:



4. In the **Managed Domain** field, select the managed domain of the External Gateway.

5. Click **Save**. This zone is then displayed with green checkmarks indicating that it is enabled for **Remote Browsing** and is **Managed**, as shown below:

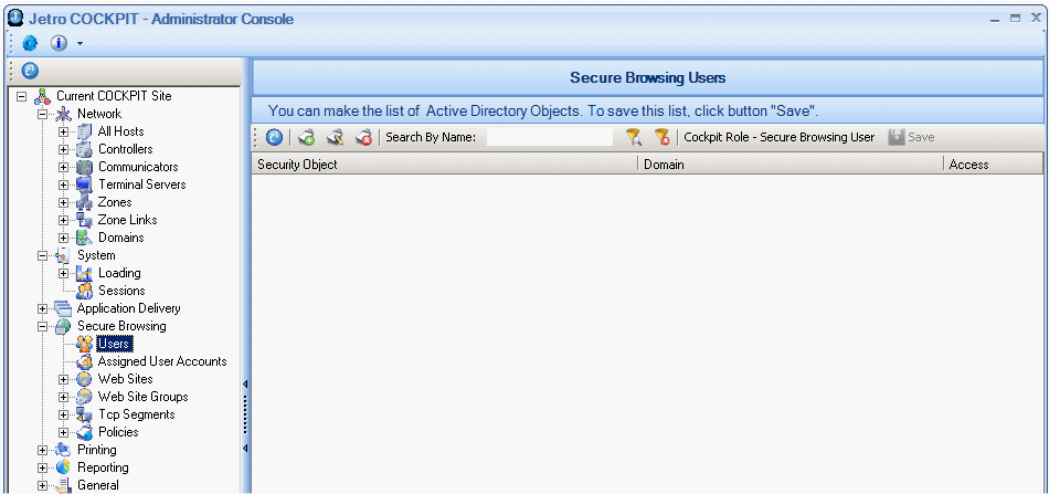
Summary: At this stage in the configuration of the Secure Browsing environment, you have defined two zones.

Configuring Secure Browsing Users

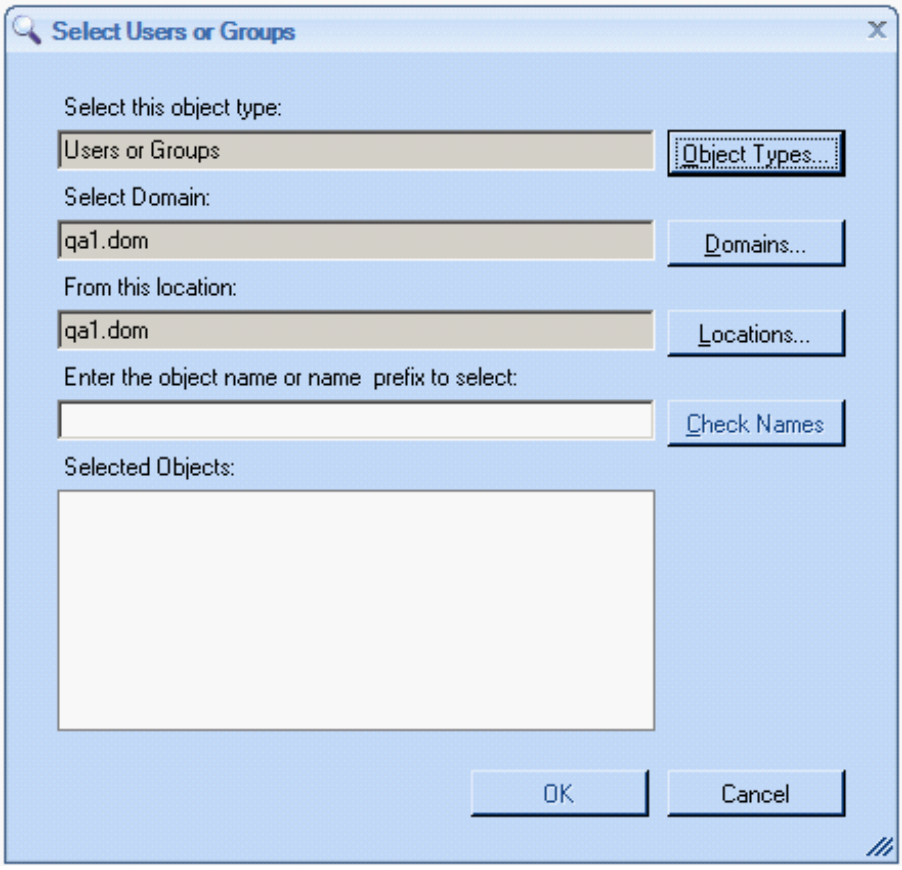
This section describes how to define which users are permitted to browse using Secure Browsing.

To configure Secure Browsing users:

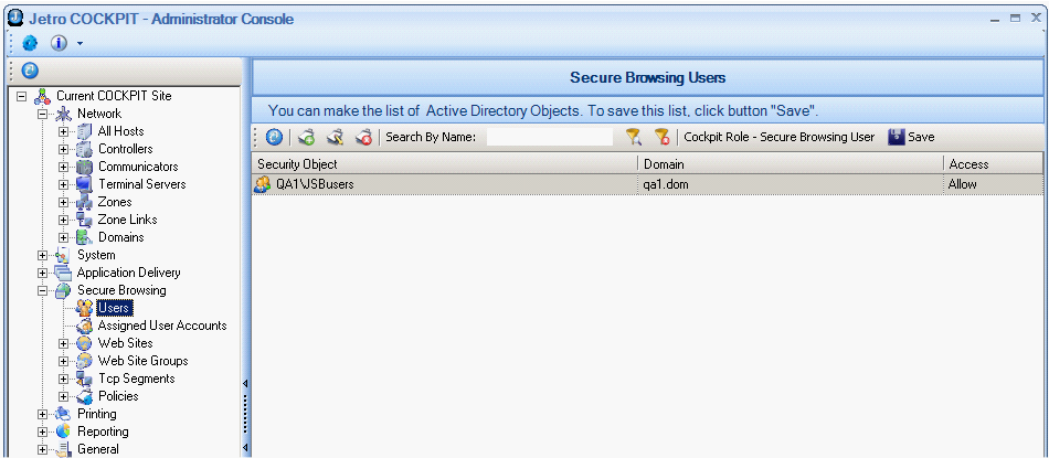
1. Select the **Secure Browsing > Users** branch, as shown below:



2. Right-click in the center of the page and select **New** or click the **New** tool. The following screen appears:



3. Select the relevant users or user groups and click **OK**. The selected users are then displayed, as follows:



Add only one user for testing or add as many users and/or user groups as required.

Configuring TCP Segments

TCP (Transmission Control Protocol) is a protocol developed for the internet to get data from one network device to another. TCP Segments specify the IPs that define an organization's local network. This definition differentiates between the inside of an organization and the outside. Typically, the barrier between them is the firewall. This topic

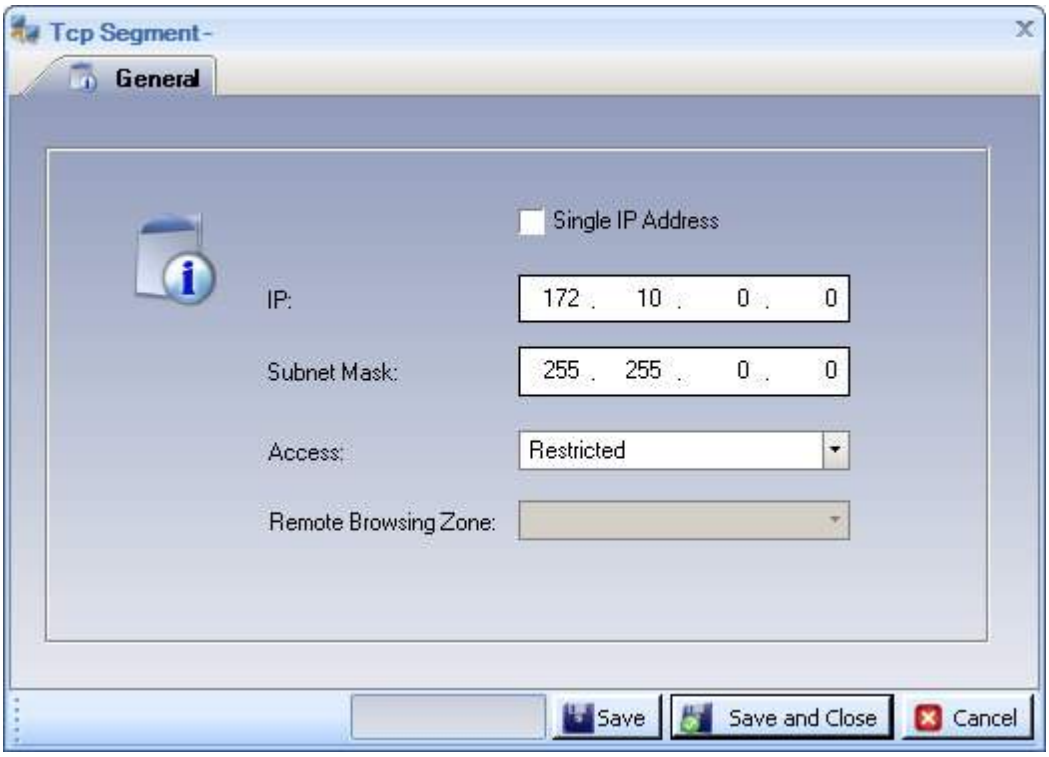
describes how to configure TCP segments. This will tell the system which elements constitute the LAN, and which elements constitute the DMZ, and how to distinguish between them.

Secure Browsing Clients are allowed to either browse to sites inside the organization using the browser on the Secure Browsing Client user's computer; this is called the **internal browser**. Or they are able to browse to sites outside the organization through the **external browser** situated on the External Gateway Server.

To add a TCP Segment:

1. Select the **Secure Browsing Services > TCP Segment** branch.
2. Click (**New TCP Segment**) to display the following screen. The values shown in the screen below represent a standard local area network TCP segment definition.

3. In the **IP** and **Subnet Mask** fields, enter the local area segments. You must adhere to standard IP and Subnet Mask syntax rules. The syntax is not validated.



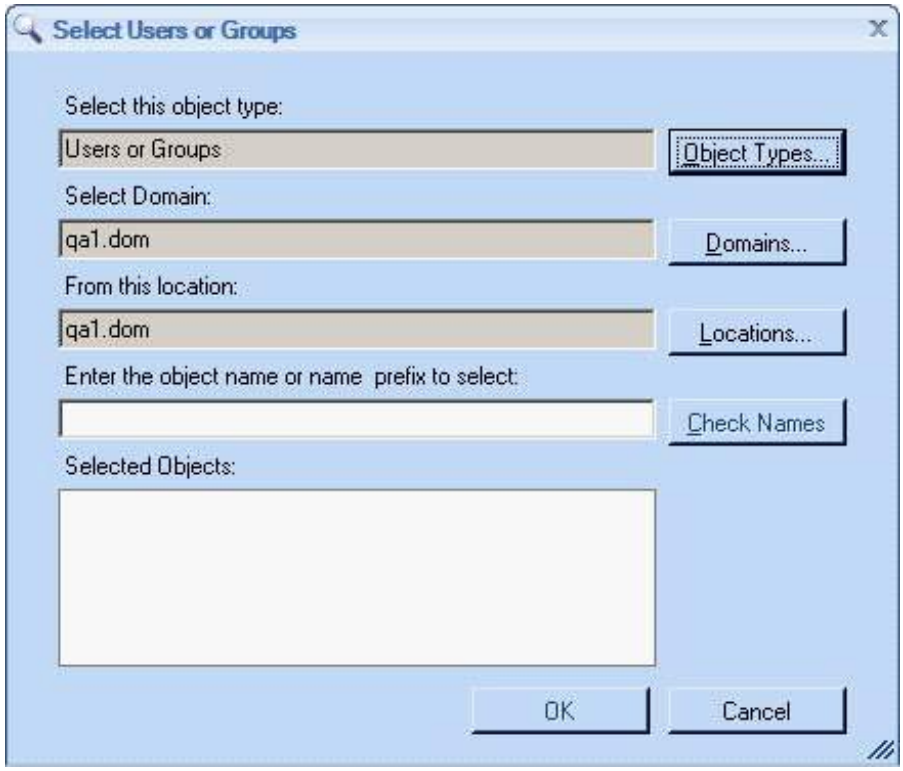
4. In the **Access** field, select **Local**, this defines the addresses in this TCP Segment as local, meaning inside the organization. For example, on the Intranet/LAN. When a Secure Browsing user browses to these addresses, the site opens in the user's standard browser, not in the external browser on the External Gateway.

5. Click **Save**. The following screen appears:

NOTE: When you save the segment settings, two tabs appear in the screen: General and Security. The Security Tab only appears when the **Local** or the **Remote** option is selected in the **Access** field.

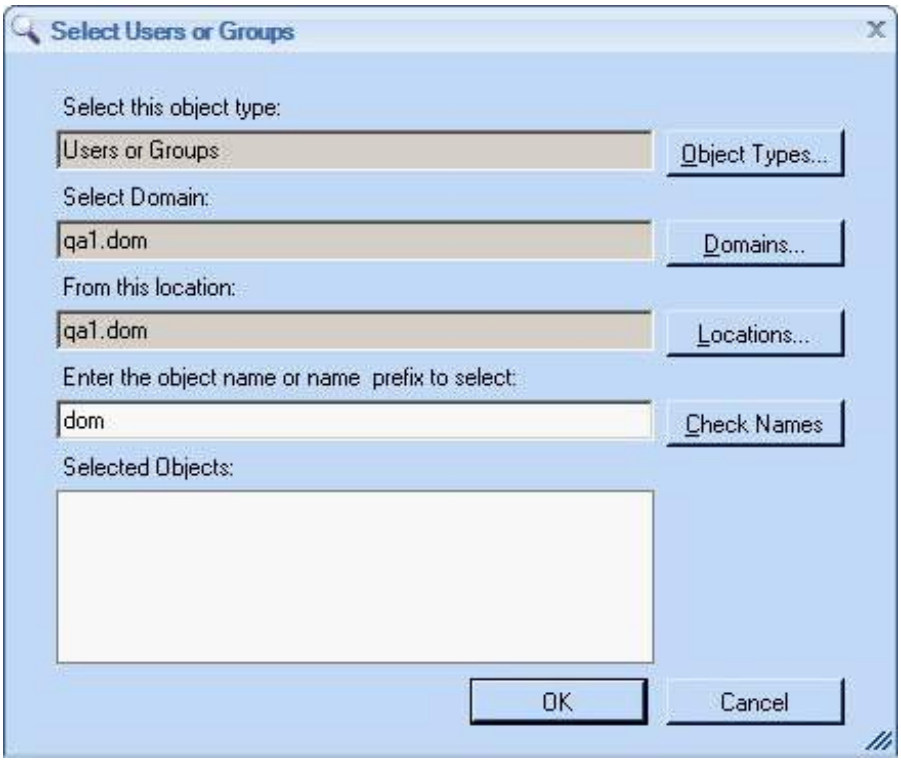
6. Open the **Security Tab**. The following screen appears:

7. Click (**New Security Object**). The **Select Users of Groups** screen appears:

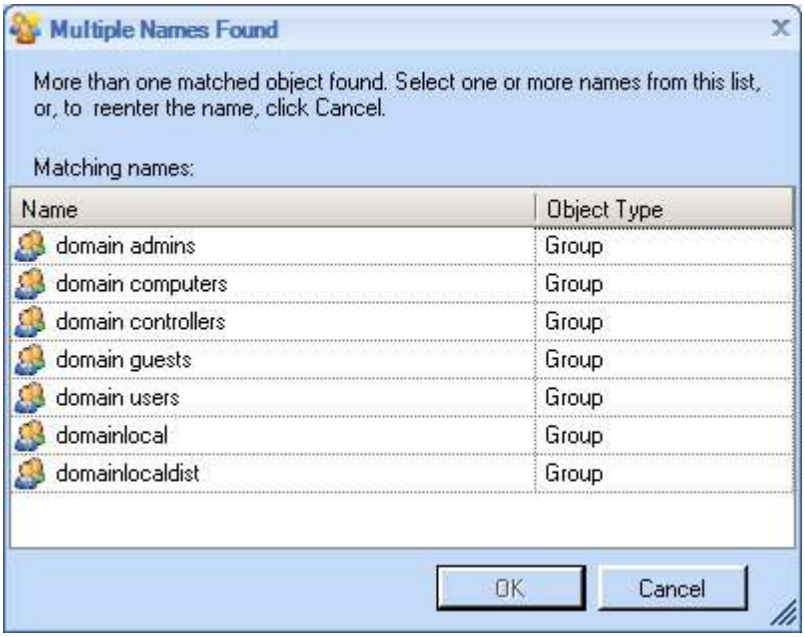


8. Enter the object name or name prefix and click **OK**.

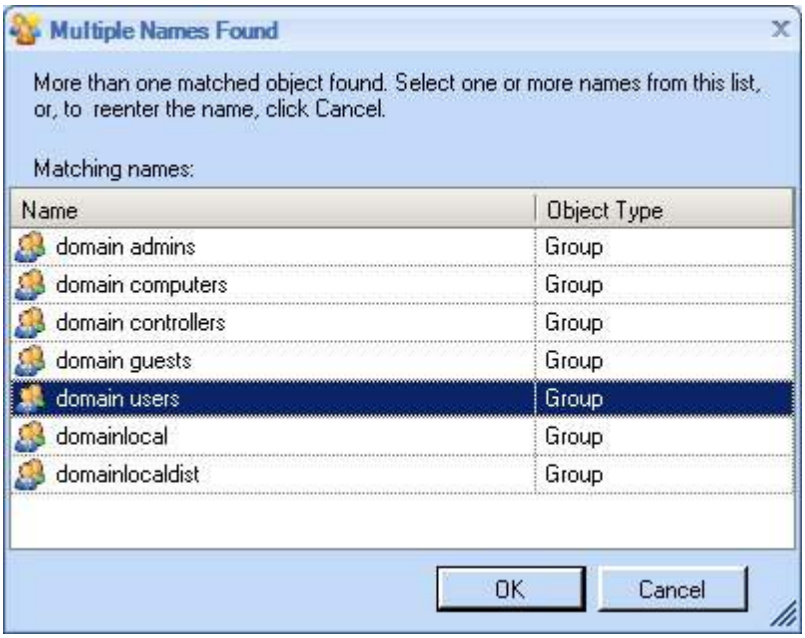
NOTE: You should select the same Security Object as the SBSecurity object defined previously. (Open the **Security** tab to check.)



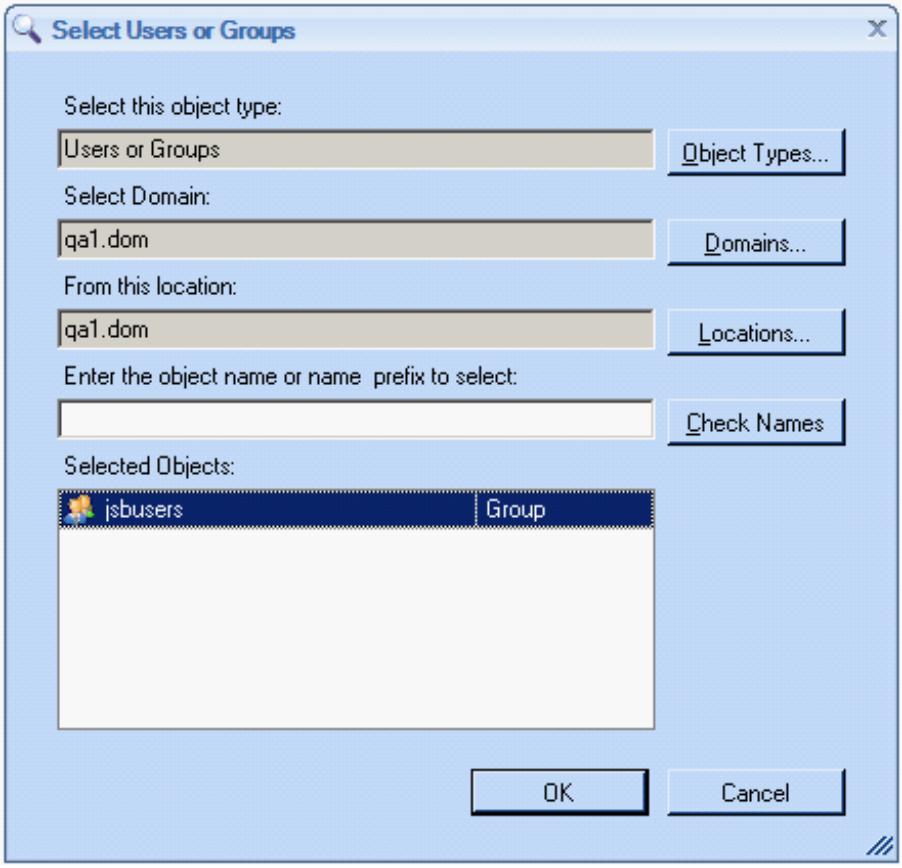
In the previous example, where you entered **dom** as the object name, the system returns a list of groups beginning with the prefix **dom**, as shown below:



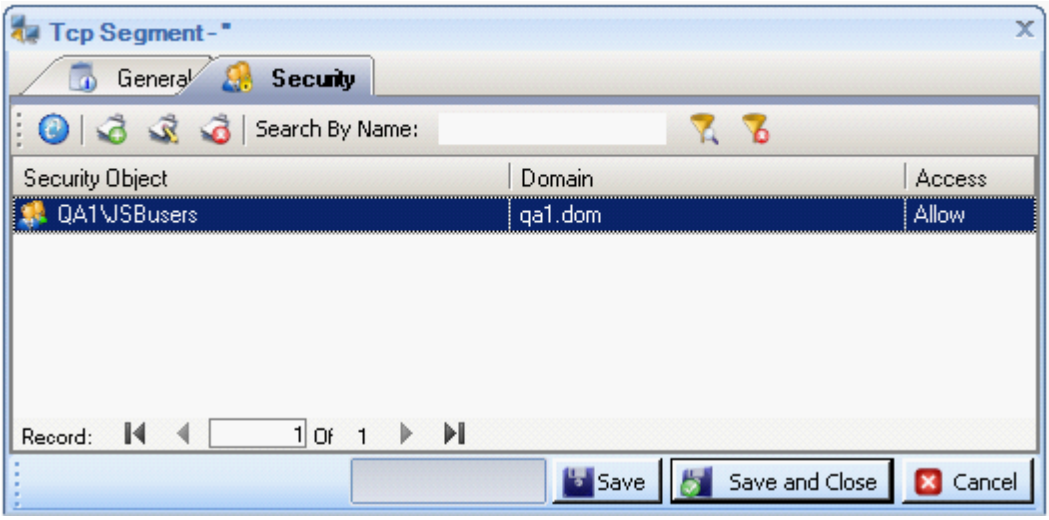
9. Select the Security Object you wish to associate with the TCP segment.



10. Click **OK**. The selected object appears in the list of **Selected Objects** in the **Select Users or Groups** window.

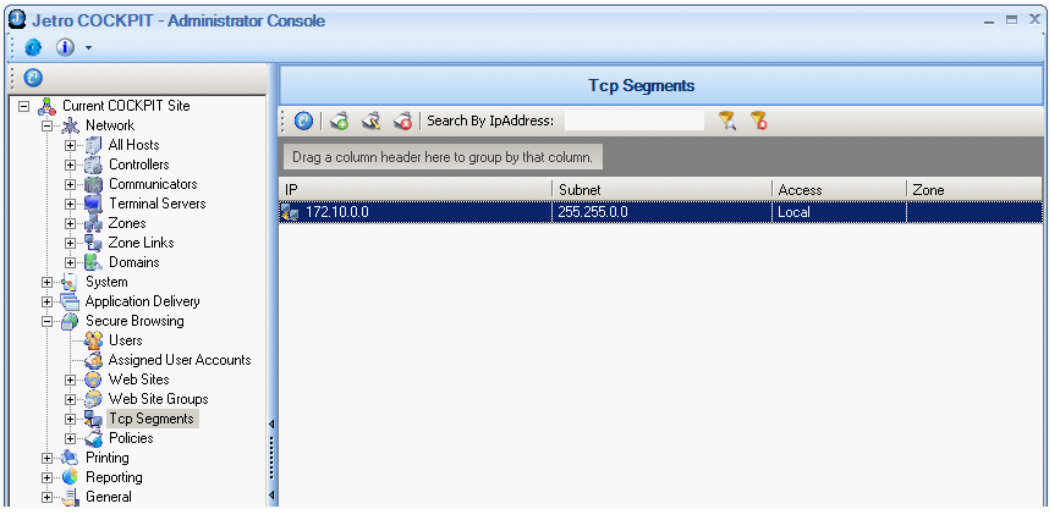


11. Click **OK**. The Security Tab is restored, showing the name of the **Security Object**, its **Domain** and level of **Access**.



12. Click **Save and Close**.

    The TCP Segments that you defined are added to the TCP list, as shown below. In the example below, there is only one segment currently defined. However, multiple TCP segments are common in sophisticated organizations.



NOTE: If you fail to configure the TCP segments correctly, the system will not perform properly. TCP Segments are the configuration settings that tell the system which elements constitute the LAN (meaning the internal network of the organization), which elements constitute the DMZ and how to distinguish between them.
Be aware that in a sophisticated organization you would expect to see multiple TCP segments, where each segment represents a different internal web site.

This default policy applies to all users by default unless another policy has been defined that applies to those users.

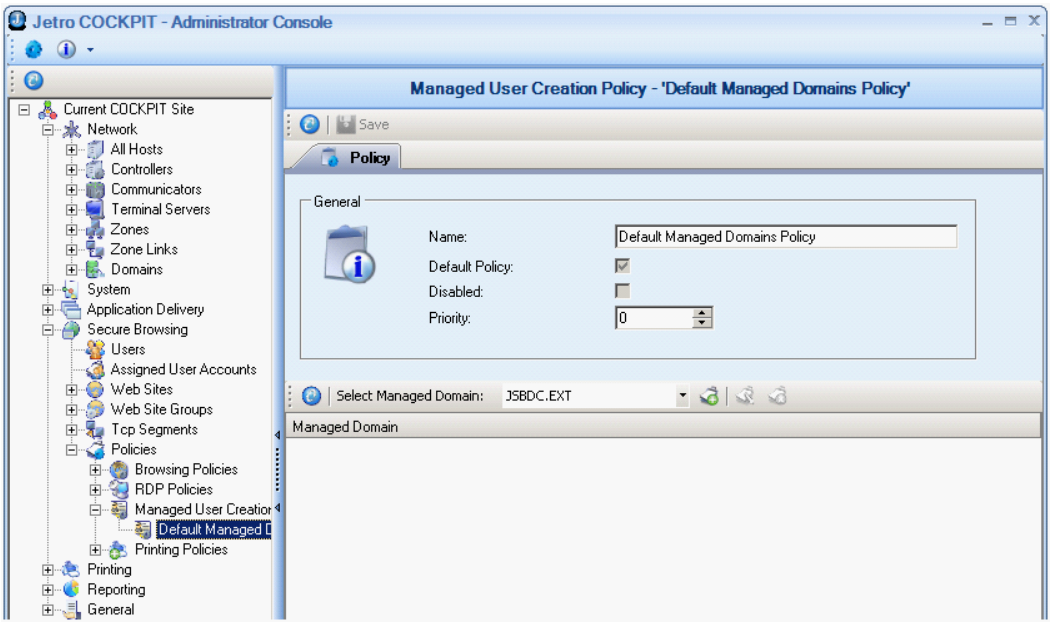
Configuring the Default Managed User Creation Policy

This section describes how to define the default policy for creating managed users. This is the policy that is applied by default to Secure Browsing users when a fake user profile is created while they browse to an external site from the External Gateway.

The default user policy applies to all users unless a Condition was defined in the **Conditions** tab, which is outside the scope of this manual. For the purposes of setting up and testing Secure Browsing, you only need to configure the default policy.

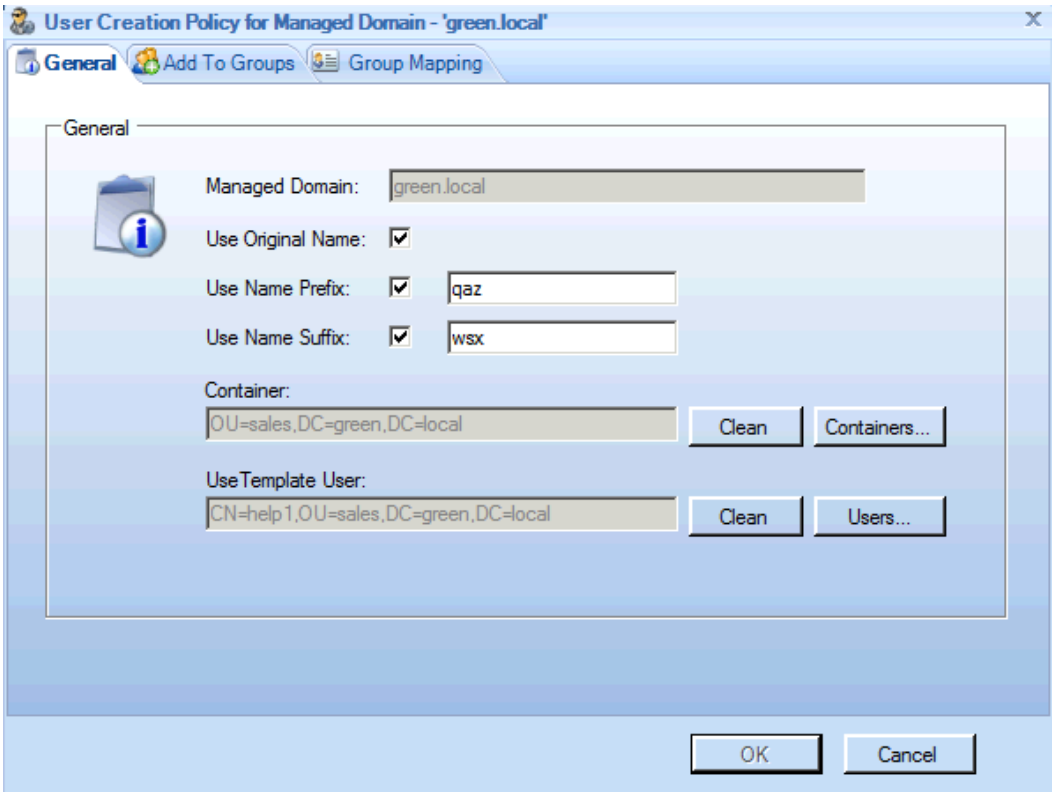
To define the default Managed User Creation policy:

1. Select the **Secure Browsing Services > Polices > Managed User Creation Policies** branch.
2. Select the **Default Managed Domain Policy** which is defined during installation, as shown below:



NOTE: In the sample window above, JSBDC.EXT is the name of the External Domain set up prior to installation.

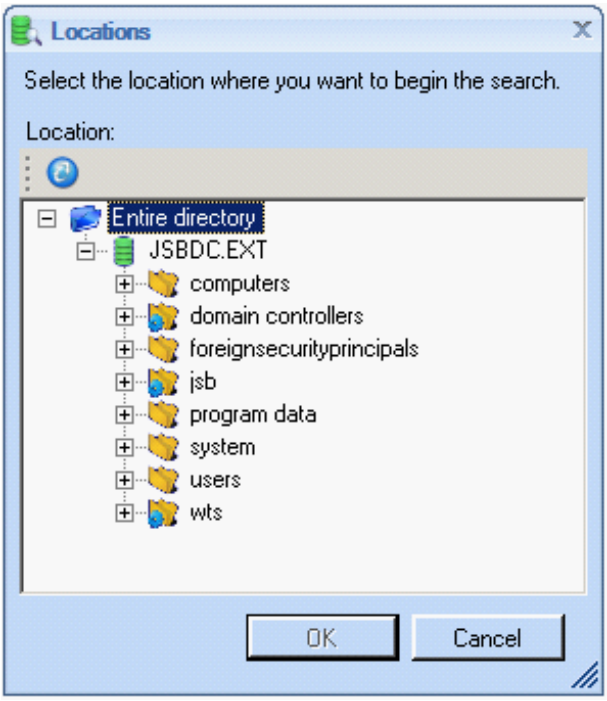
3. Click (**Add Managed Domain for User Creation**) to display the following screen:



4. Leave the following checkboxes empty: **Use Original Name**, **Use Name Prefix**, **Use Name Suffix**, and **Use Template User**.

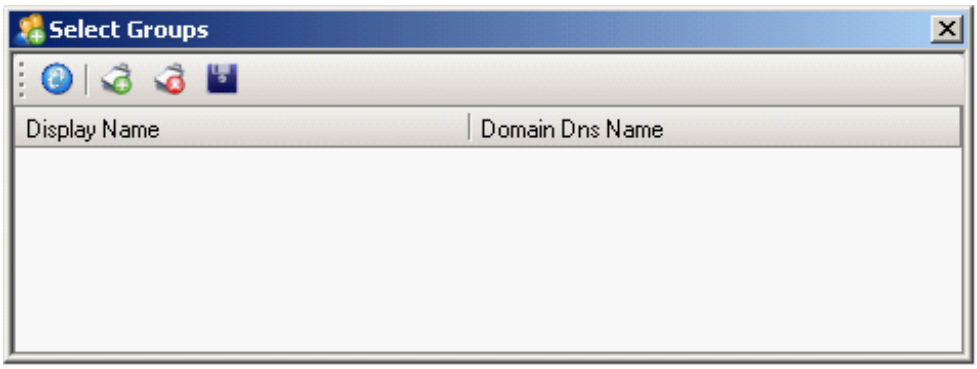
5. Active Directory managed users are typically stored in logical containers. For management efficient purposes, create a new container that will contain the fake external users that are created on-the-fly during Secure Browsing to external sites.
   If you do not have a dedicated container, all new users are added to the root of the directory, which becomes disorganized in an organization that has many users.

- Click the **Container** field's **Container...** browse button to select a Container.

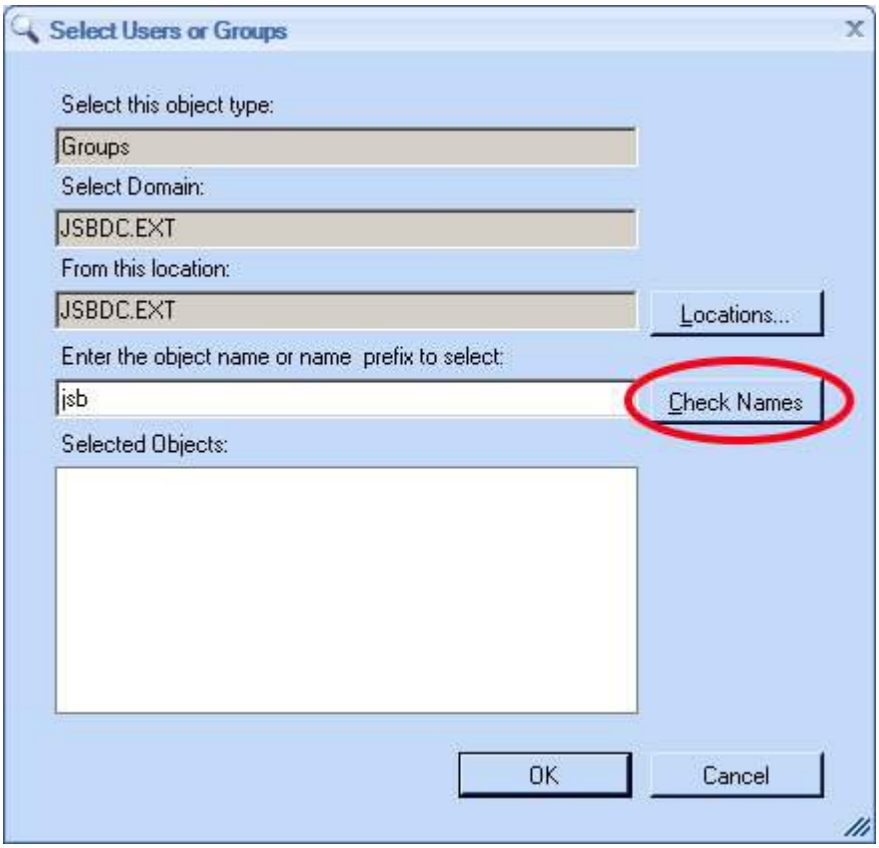


- From the **Locations** list, select the target Container.
- Click **OK**. The selected container appears in the **Container** field in the **Managed Domains** definition screen.

- The **Add To Groups** tab, refers to the static method of group assignment. The dynamic group assignment is not covered in the basic installation procedure.
  - Select the **Add to Groups** tab.
  - Click the **Browse** button to open the **Select Groups** window.

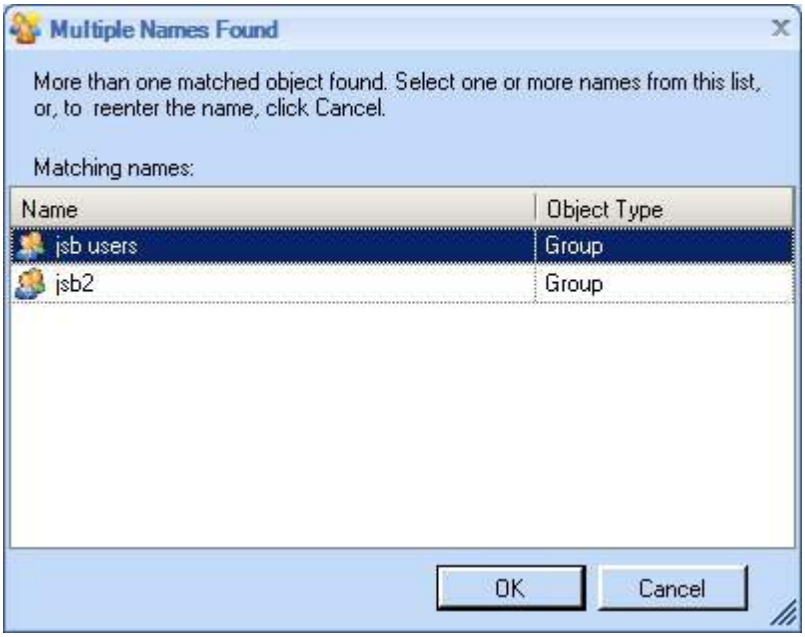


  - Click the  New button. The **Select Users or Groups** screen appears:



- Enter the object name or name prefix, and click the Check Names button to locate the User Group that you wish to select.

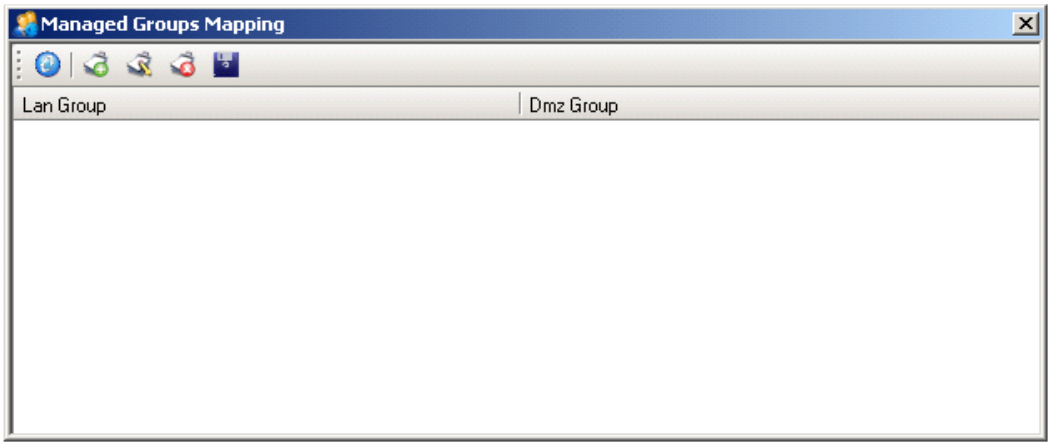
  The system displays a list of names that match the search criterion.



NOTE: In the example screen above, the system displays the names of two groups. There should always be at least one User Group defined in the system, namely, the User Group (OU) that the installer created prior to installation.

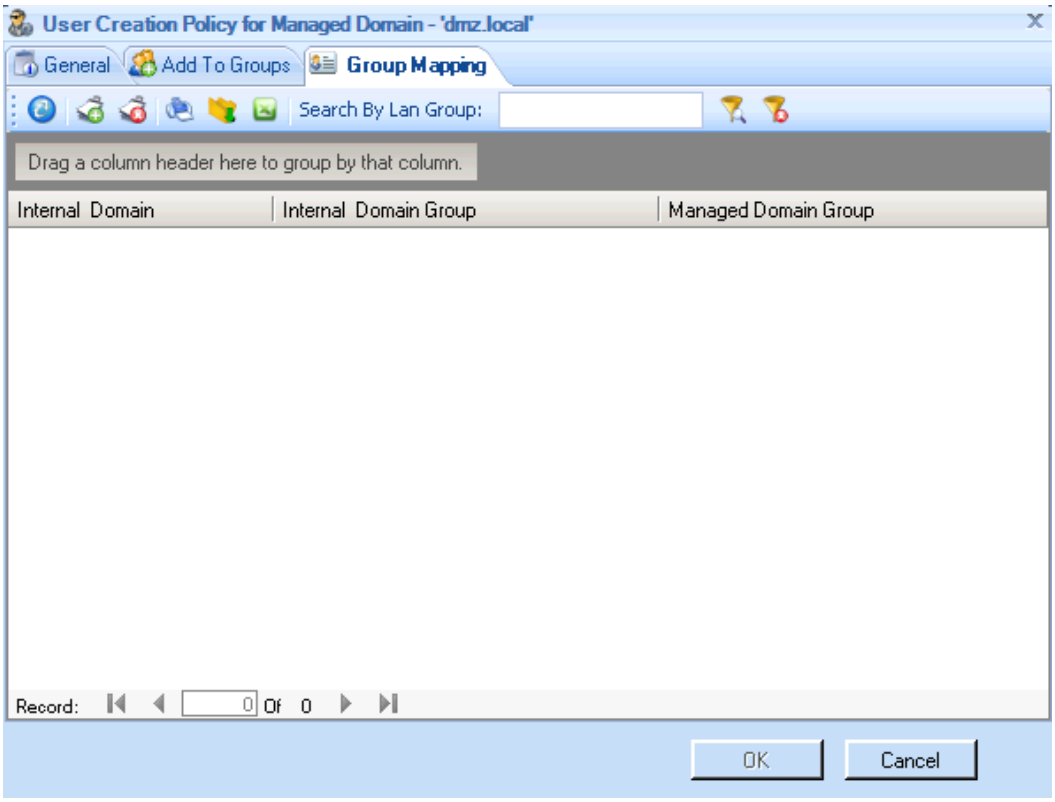
- Select the User Group that you wish to add.
- Click **OK**. The User Group appears in the **Selected Objects** list of the Select Users or Groups screen.

- Click **OK**. The **Select Groups** screen appears, displaying the selected User Group.



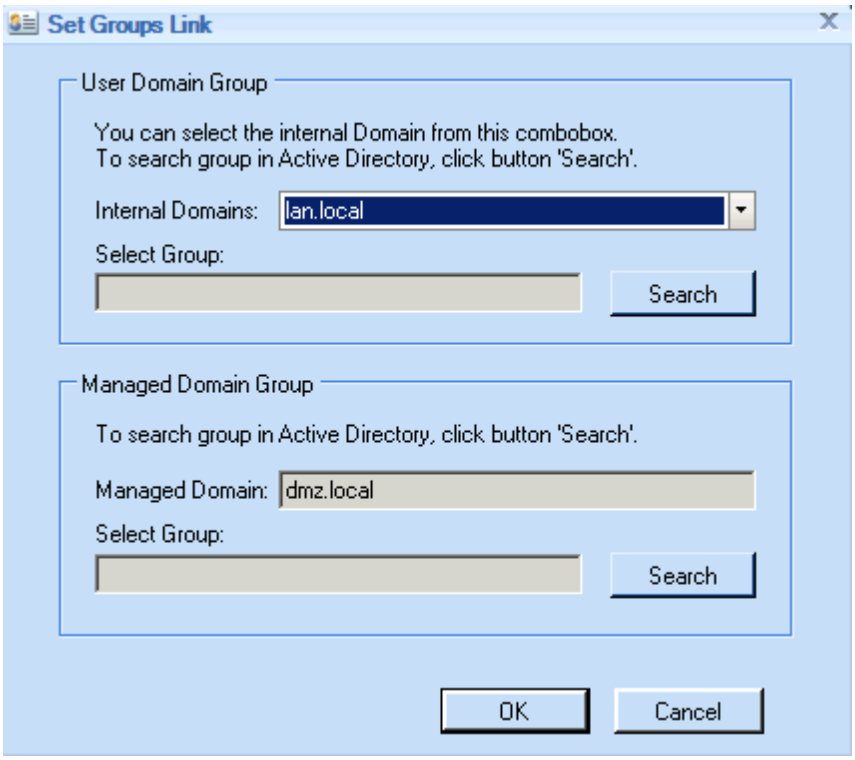
- Click **Save**.
- The User Group that the Client Rule will be added to is saved to the system and the **Policies** tab is restored.

- The **Group Mapping** tab creates a mapping between the user groups which a user belongs to in the internal domain (also called the LAN or the organization) and the user groups which the user belongs to in the external domain (also called the DMZ). This option statically adds the new fake user to the external Active Directory. External user groups enable administrators to assign polices to external user groups as required. Users may belong to more than one group.
  - Select the **Use Group Mapping** option.
  - Click the **Browse** button to display the following screen:

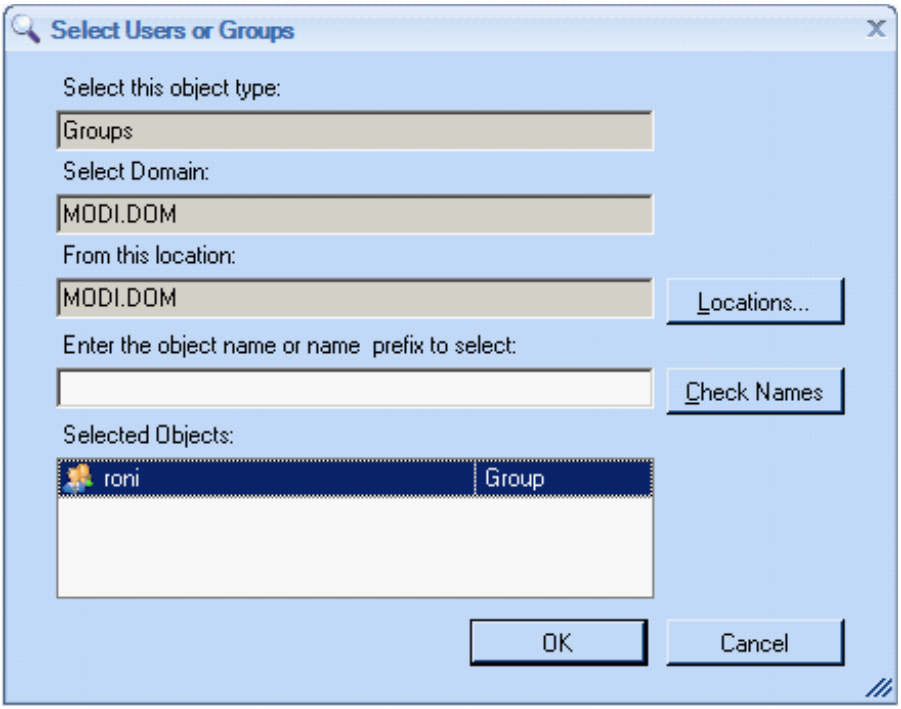


The left side of this screen lists the user group that this user belongs to in the internal domain. The right side of this screen lists the domains which this user belongs to in the external (DMZ) domain.

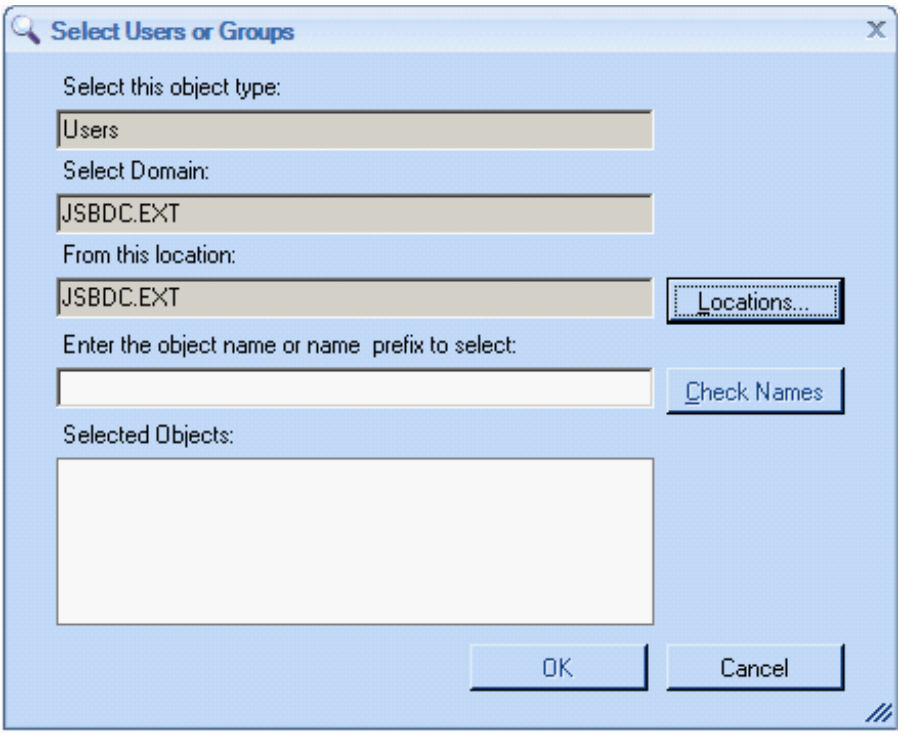
- Click the **New** button to display the following screen:



- In the **User Domain Group** area, in the **Domain** field, specify the user group in the Internal Domain by clicking the ... button to display the following screen:



- Select a User Group in Active Directory in the usual manner. In the **Managed Domain Group** area, in the **Domain** field, specify the user group in the External Domain by clicking the button to display the following screen:



Select a User Group in the Active Directory in the usual manner.

The external group begins after it is defined as empty. As each user browses to an external website, that user is added to the external user group.

6. Click **Save** to save this new default policy which is shown below:

Configuring RDP Policies

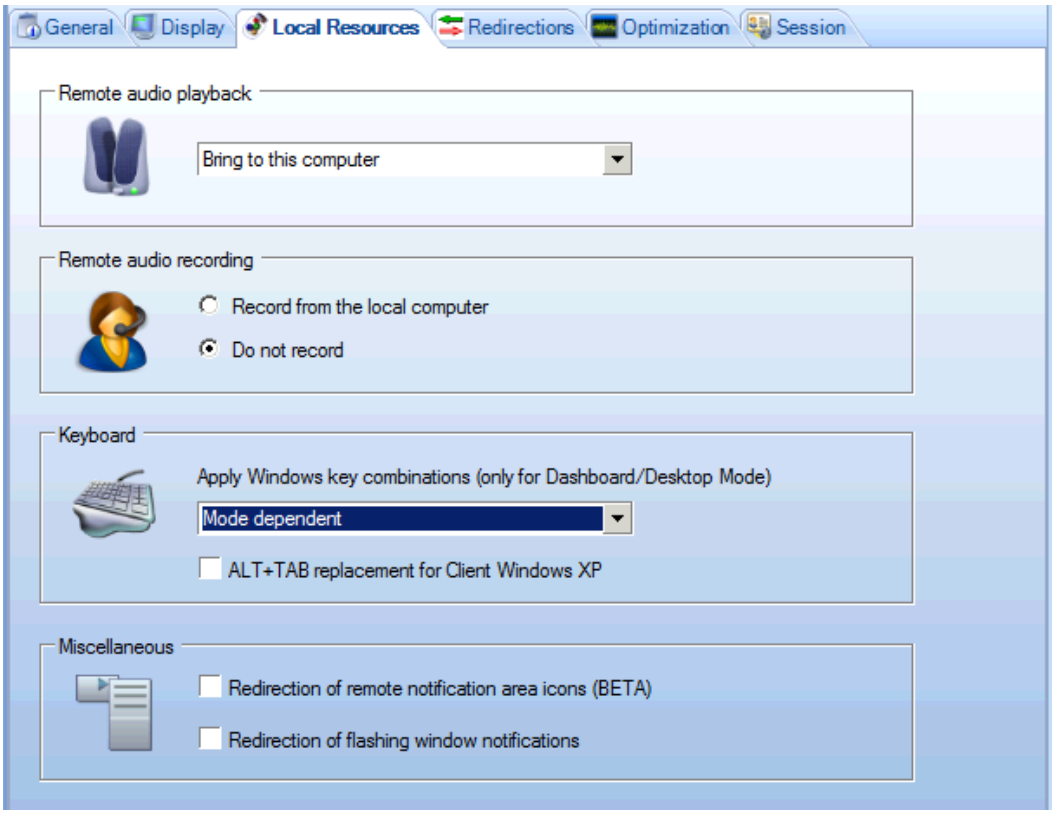
The Remote Desktop Protocol (RDP) determines various aspects of the look-and-feel and behavior of a user's Secure Browsing desktop. The different tabs on this branch allow you to set these definitions, such as the sound, colors, window size, local access options, and so on.

The default user policy applies to all users, unless a Condition was defined in the Conditions tab, which is outside the scope of this manual.

To configure RDP policies:

1. Select the **Secure Browsing > Policies > RDP Policies** branch.
2. Select the **Default SB RDP Policy** which is defined during installation, as shown below:

3. In the **Local Resources** tab in the **Remote Audio Playback** field, select the **Bring to this computer** option to specify that sounds are played on the user's computer, as shown below:



4. Click **Save**.

Configuring Browsing Policies

Browsing Policies define the Internet access that is provided to each user through the Secure Browser. The Default Browsing Policy is **Restricted**. This means that no one can surf outside of the organization unless he is included in a permissive Browsing Policy that is configured by the System Administrator. This is a useful policy for ongoing usage. However, for this initial setup stage you must create a new browsing policy, which you can either use or delete later.

Users can navigate to a URL inside their organization using a standard browser. When they try to navigate to a URL outside the organization, an external Secure Browsing browser opens on a Terminal Server. When a user tries to navigate to a URL inside the organization from this external Secure Browsing browser, the system behaves as defined in the Browsing policy.

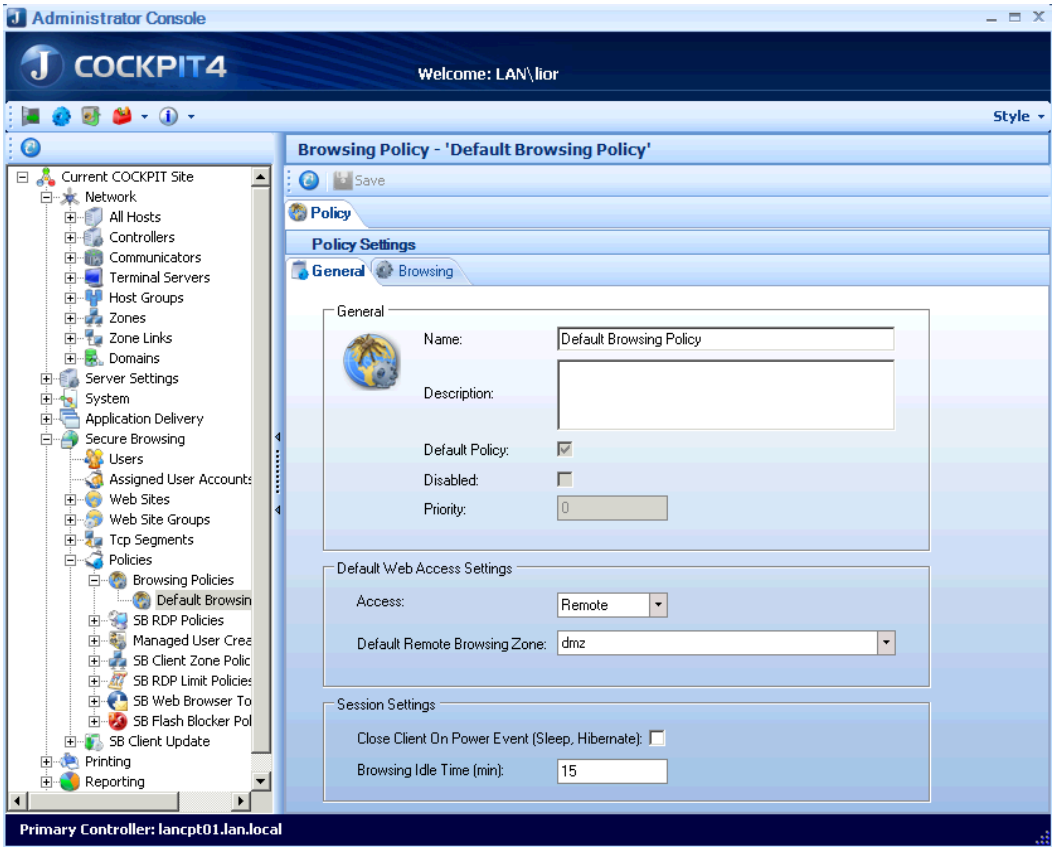
The default policy applies to all users. To define another policy you follow the same process as defining a default policy when filling out the General tab. However, you must also define which users the policy applies to in the Conditions tab. The default policy does not apply to any user that is included in an additional policy.

Only users who meet the conditions of the browsing policy will be able to browse.

To configure the Browsing Policy:

1. Select the **Secure Browsing > Policies > Browsing Policies** branch.

2. Click the **Add New** button or right-click on the **Browsing Policies** branch and select the **New Policy** option. The New Browsing screen appears:



3. In the **Name** and **Description** fields, enter a name and description of the browsing policy.

4. Select the **Disable Secure Browsing** checkbox to enable the Client to disable the browsing mechanism on his/her workstation.

We recommend selecting this option during the initial setup stages, and then, later, to disable it.

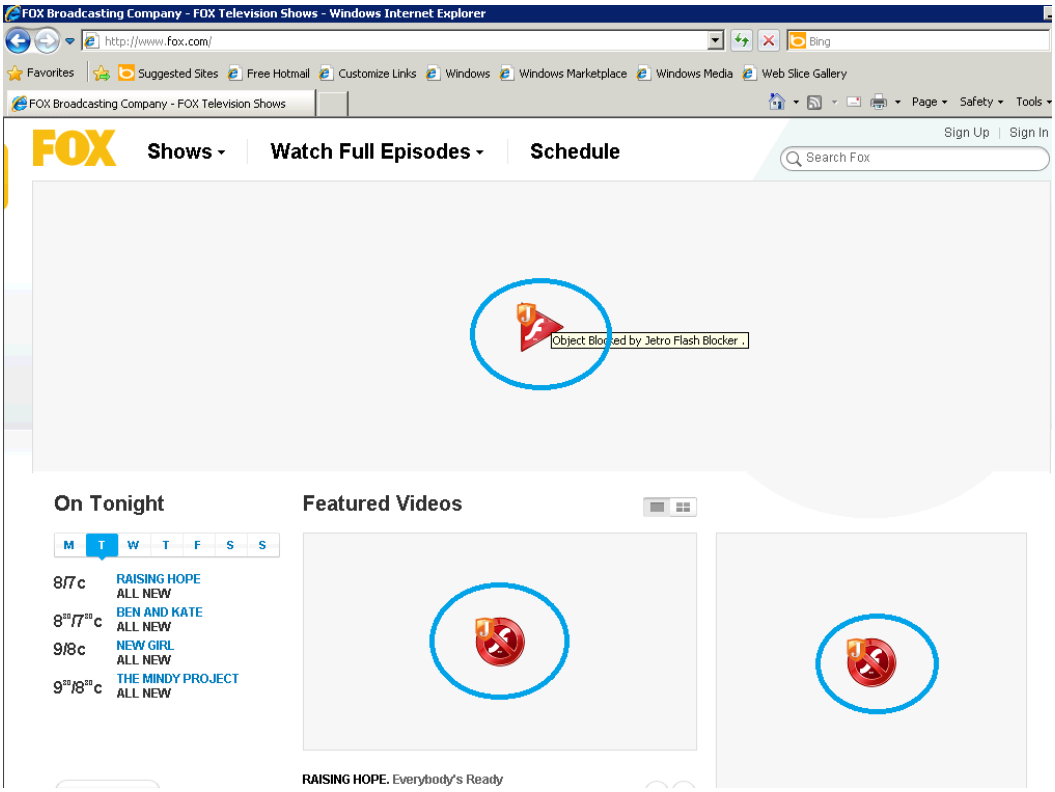
This setting gives an option to disable Secure Browsing in the Secure Browsing Client's tray icon. This is an option that must be stopped later to prevent users from having the ability to configure permission for themselves to browse without the protection of the Secure Browsing Client.

NOTE: This setting is active for the current session only, meaning that after a user Client closes his/her computer, then that user automatically becomes active again.

5. In the **Flash Blocking** area, select the **Block Flash** checkbox to block all Flash objects on the external browser. The flash blocking mechanism only starts after a page is fully loaded. The user receives a text message prompting him to override the block, as shown below:

6. By default, the user receives an icon prompting him to override the block.

The override is per Flash object in the web page, as shown below. Each command to run Flash affects the selected object only.



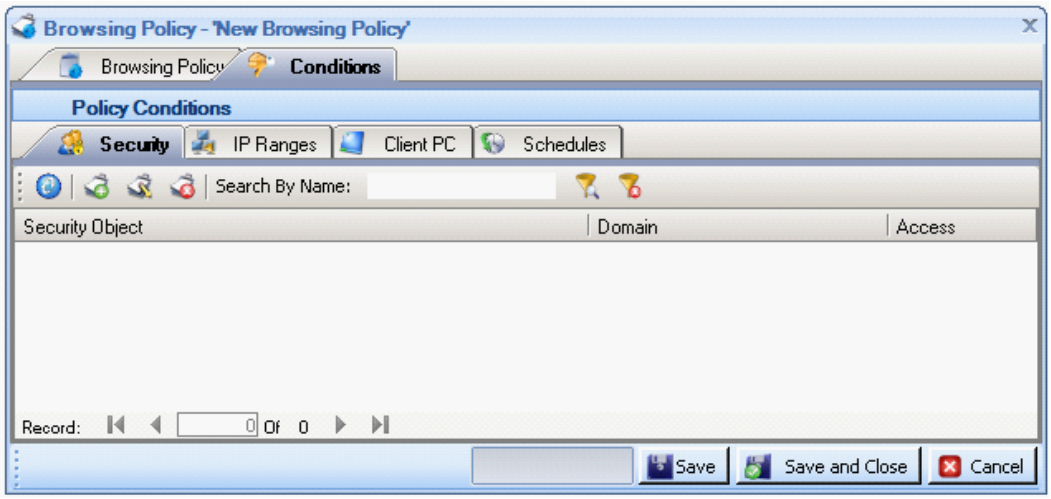
The Flash Blocker affects the external browser only.

NOTE: This critical feature helps organizations conserve resources. The Flash mechanism consumes resources at an astounding rate. In the Jetro test environment, two users with Flash enabled, consumed all the available CPU and network traffic resources that normally serve 52 flash-blocked users!

7. In the **Default Web Access Settings** area in the **Access** field select **Remote** to specify that external sites are open in the Secure Browsing browser.

8. In the **Default Remote Browsing Zone** field, specify which zone the Terminal Server is located.

9. Click the **Conditions** tab to display the following:

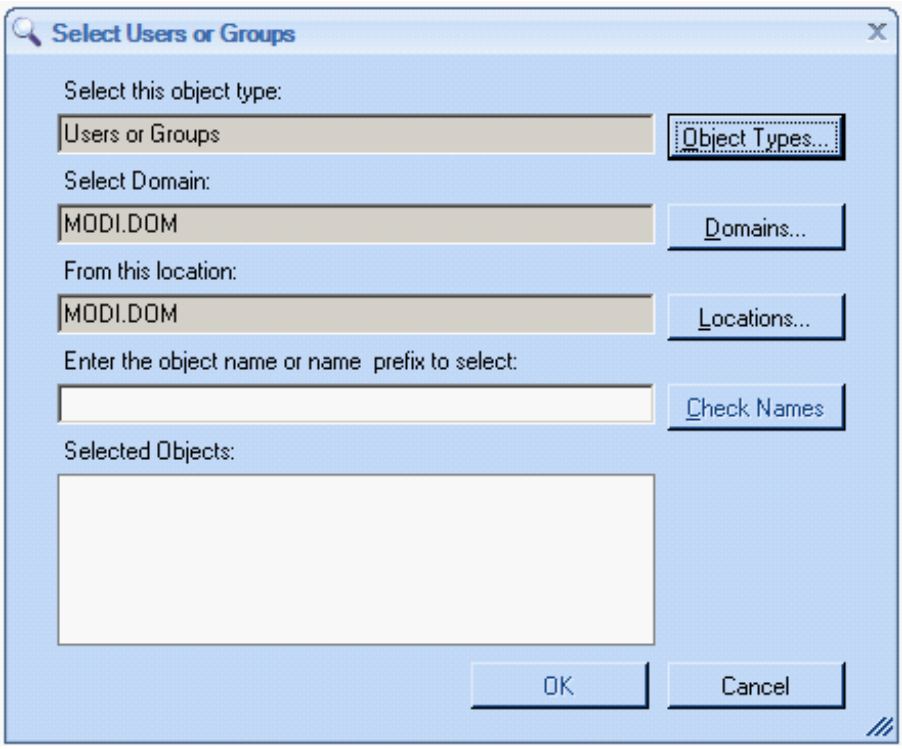


The **Conditions** tab contains sub-tabs where you can define which users this policy applies to. Define the users by

entering information in the tabs. Entering information in more than one tab, creates an AND relationship between these conditions. This means that all the defined conditions must be met for the policy to apply to a user.

10. In the **Security** tab, add users or user groups from the internal Active Directory by clicking the **Add New** button. The following screen appears, where you can select users. These are the users and groups that have permission to surf.

NOTE: For each user that surfs for the first time, a fake user is created on the external managed Active Directory.



11. Click **OK**.

12. Click **Save**.

Once you have successfully configured the default and user-specific Browsing Policies, Clients are able to surf the net securely from within the organization.

Chapter 6: Setting Up COCKPIT Clients

This chapter describes how to install and use the COCKPIT5i Secure Browsing Client on a user's computer and describes a user's surfing experience.

It also describes how to use various supplementary Add-ons.

This chapter contains the following topics:

Client Prerequisites

This section describes the prerequisites for installing a Secure Browsing Client:

- The Secure Browsing Client can be installed on any computer that runs any 32- and 65-bit version of XP OS, Vista, Seven, Server 2003 or Server 2008.
- The Secure Browsing Client must be installed on a computer that is a member of the same domain as the Secure Browsing Administration Console, which is described in section on configuring domains.
- The computer on which the Secure Browsing Client is installed must use Internet Explorer version 6 or higher.

- The Secure Browsing Client can be installed locally or remotely using MSI (Microsoft Installer). In both cases, the person who installs the Secure Browsing Client must have administrator rights to the computer on which it is being installed.
- The most recommended method for connecting the Secure Browsing Client to a Controller is to setup a designated description alias in your organization's DNS that points to the Controller. This alias should be called jsbserver1 for the Primary Controller (and jsbserver2 for the secondary Controller, if one exists). We recommend that you test the proper functioning of this alias by pinging the jsbserver1 alias from a Secure Browsing Client to see if the Controller responds. This must be performed before starting the Secure Browsing Client installation process. See the section Connection – Preferred Method

Installing the COCKPIT Client

To install the COCKPIT5i Client:

- Use a simple wizard

Run **JSB-ClientSetup.exe** from the files that you received from the Jetro package, and follow the wizard's instructions.

- MSI command line installation

The MSI installation is recommended for users who wish to customize their installation or manage automated installations for large numbers of users in the organization. When using the MSI installation package, the installer user must have Windows NT privileges that allow software installation.

The Secure Browsing Client can be installed using MSI with the following command line parameters:

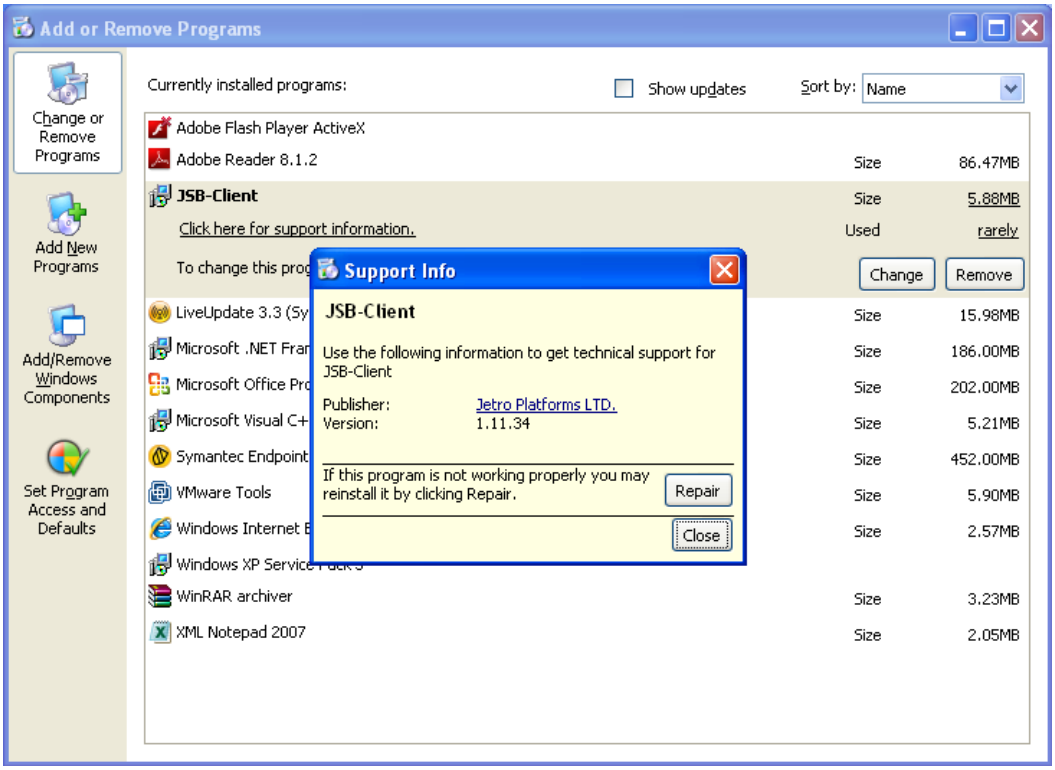
Parameter	Description	Default Value
JSBSERVER1	First Controller that the Client tries to connect to; in most cases, the Primary Controller.	JSBSERVER1
JSBSERVER1_PORT	Port for JSBServer1.	13000
JSBSERVER2	Second Controller that the Client tries to connect to.	JSBSERVER2
JSBSERVER2_PORT	Port for JSBServer2.	13000
ENABLEDA	For future reference.	1

Parameter	Description	Default Value
DASERVER		JDSDOWNLOADSERVER
DAPORT		13009
TSIDLETIME	Idle time in seconds before the current session logs off. 0=No Idle Time	900 (sec)
DNSTYPE		0
DNSTIMEOUT		500 (msec)
DNSRETRIES		2

Post Installation

When installation is complete, you will not see any differences on your desktop. No icon is added to the desktop, nor is a program added to the **Start > All Programs** menu. However, you can see the Secure Browsing Client in the Add or Remove Programs option in the Control Panel.

Select the **Click here for support information** link to see the Secure Browsing Client version information, as shown below:



Connecting the Secure Browsing Client to a Controller

This topic describes the ways that you connect the Secure Browsing Client to a Controller once you have completed installation of the Secure Browsing Client. If you pre-configured a DNS alias record that points to a Controller (the preferred method of connection), an orange icon appears in the system tray to indicate that the Client is connected to a Controller. Otherwise, a gray icon appears in the system tray to indicate that the Client is not yet connected to a Controller.

The reason the Client is not connected to the Controller can be because:

- The default of the Primary Controller's DNS is unmapped.
- The User does not have browsing permissions.
- The Primary Controller is down.

After the Secure Browsing Client is connected to a Controller, as described below, the icon becomes orange.

There are two options for setting up the initial connection between the Secure Browsing Controller and Secure Browsing Client:

- **Connection – Preferred Method:** the system has a pre-configured DNS alias that points to the Controller. This is the preferred mode of operation.
- **Connection – Manual Method:** the system has no pre-configured DNS record, which means that the Client cannot automatically connect to the Primary Controller without you performing a short manual configuration change.

Connection – Preferred Method

This topic describes the preferred method of connecting the Secure Browsing Client to the Controller. In this mode, the installer has pre-configured a DNS alias record that points to a Controller. This is the recommended method for connecting the Secure Browsing Client to a Controller. The alias should be called jsbserver1 for the Primary Controller (and jsbserver2 for the secondary Controller, if one exists. This option is outside the scope of this manual).

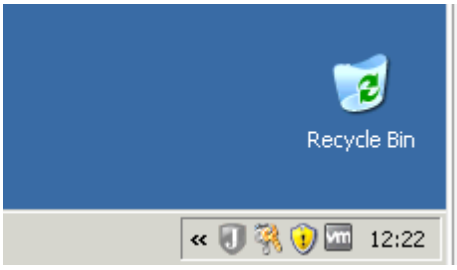
This must be prepared before starting the Secure Browsing Client installation process. We recommend that you test the proper functioning of this alias by pinging the jsbserver1 alias from a Secure Browsing Client to see if the Controller responds.

If the above has been setup before installing the COCKPIT5i Client, it automatically detects the Controller after you start the COCKPIT5i Client, as described below.

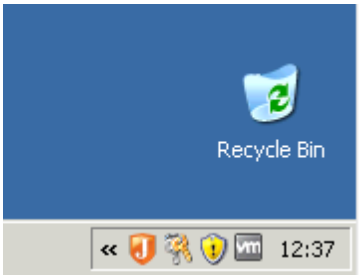
To connect when a DNS alias exists for the Controller:

- Click the browser icon (for example, Internet Explorer), as you would normally do.

- Note that the icon in the system tray is gray. It remains gray until the Client successfully connects to a Controller.



- When the icon becomes orange, it means that the system has found the DNS record and has successfully connected to the Primary Controller, which it automatically points to.



Connection – Manual Method

This topic describes how to connect to the Controller manually. This is necessary if you have not pre-configured a DNS alias record that points to a Controller. Until you connect manually the Client is unable to connect directly to the Primary Controller.

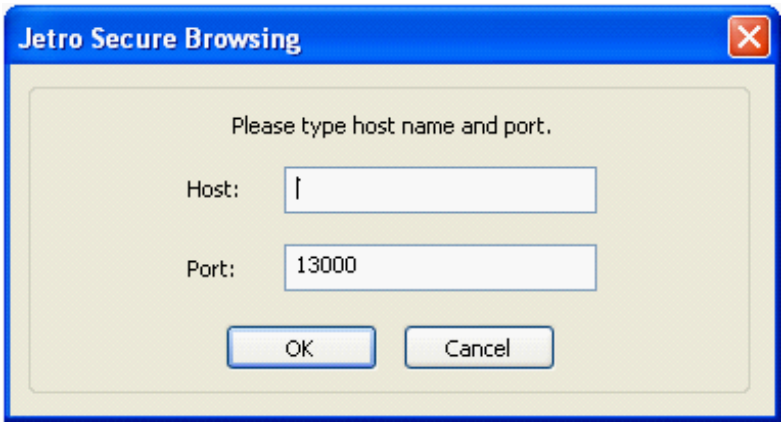
To manually connect the Secure Browsing Client to the Controller:

1. Click the browser icon (for example, Internet Explorer), as you would normally do.
   The Jetro intermediate screen is displayed briefly, followed by your home page. (At this point, the screens are the same as those in the procedure above.) However, you will not be able to surf via the Client.

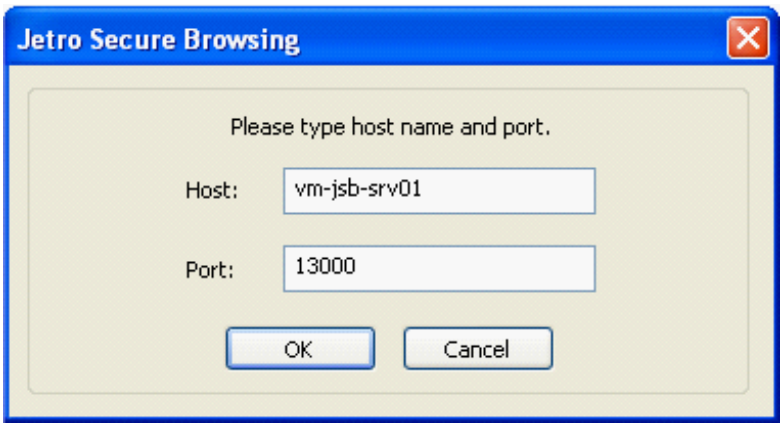
   NOTE: At this point, the Client is not connected to the Primary Controller. The system functions as if the Client is not there, as it was before you installed the Client. If you had permissions to surf the net previously, (i.e., not via the Client), you can continue to do so. If you were restricted previously, you will only be able to surf once the Client is properly connected to the Primary Controller.

2. Right-click the gray icon in the system tray to display the Secure Browsing Client drop-down menu, as shown below:

3. From the drop-down menu, select **Connect to Secure-Browsing Controller**. The **Jetro Secure Browsing** Agent screen appears:



4. Enter the name of the Primary Controller in the **Host** field. Use the actual name of the Primary Controller machine. An example is shown below. This is the name that was defined in the **Network > All Hosts** branch list.



5. In the **Port** field, specify the port of the Controller.

6. Click **OK**. The Secure Browsing Client tray icon changes to orange .
The Client connects to the Primary Controller entered in the Host field.

   - The icon in the system tray becomes orange.
   - The user can now surf securely via the Client.

NOTE: Once you have successfully connected to the Primary Controller, the system updates with the name of the host that you have entered manually.

Test Surfing

After the Secure Browsing system has been installed and configured, verify that everything is functioning properly by surfing to both an internal site and an external site. Refer to The Browsing Experience section for a description of what to expect when browsing using Secure Browsing.

The Secure Browsing installation is now complete and operating successfully. This means that you are consuming the licenses provided as part of the trial installation package. You must acquire a permanent Activation File to remove the limitations of the trial installation. Make sure you contact your authorized Jetro Reseller and make the necessary arrangements to activate the Secure Browsing product.

The Browsing Experience

This topic describes the browsing experience of using the Secure Browsing Client. You should continue to launch and use the same browser in exactly the same way as before. The Secure Browsing Client user does not need to know whether a site that you browse to is located internally or externally to the organization. The Secure Browsing Client handles all this automatically.

The Secure Browsing Client acts seamlessly. When surfing, it looks and feels like any other browser.

Secure Browsing has the following features which you should be aware of:

- In Secure Browsing, you surf from within the secure domain. There is no actual connection between the Client computer and the external domain. See the Secure Browsing Architecture section for more information.
- Secure Browsing enables you to switch seamlessly between the external and internal domains simply by browsing. Enter any internal URL in the address bar, and you are back in the internal domain.
- An internal site is displayed in the user's local browser and an external site is displayed through the browser on the External Gateway on the remote Terminal Server in the DMZ.

The following describes a few features that you may notice while browsing:

- **Splash screen**: When you invoke the Internet Explorer, the Jetro splash screen comes up first, very briefly.
- **Secure Browsing Client Tray Icon**: The tray shows a Secure Browsing Client icon. Right-click on the icon to display a drop-down menu, which is described in the Secure Browsing Client Tray Icon Menu section.
    - Immediately after installation, a gray icon appears in the system tray to indicate that the Client is not yet connected to any Controller.

- The Secure Browsing Client tray icon changes to orange to indicate that it is connected to the Controller.
- If there is a communication problem between the Secure Browsing Client and the Controller, the Secure Browsing icon turns gray. In this case, the Secure Browsing user can still navigate to internal sites, but not to external ones. See the Browsing Problems section for more information.

NOTE: There are various reasons why you can lose a connection to the Internet, most of them are not connected to Secure Browsing. For example, service provider problems, communication errors, browser bugs, viruses, and so on. We suggest that you restart your browser.

- **Terminal Server Browser Differences**: There may be slight differences in the appearance of the internal and external browsers. This depends on the settings the system administrator sets on the Terminal Server's browser. For example, the browser on the Terminal Server that is used to browse an external site may have a different browser version (such as version 6), whereas the Secure Browsing Client computer may have a different browser installed (such has version 7). In this case, the only differences between viewing an internal and an external site are are the inherent differences between these browser versions.
- **Browsing to an External Site**: When a Secure Browsing Client user browses to an external site for the first time after the Secure Browsing Client has been installed on that computer, the following screen may appear for a few moments:

This window might appear for a few moments after you close all browsers and then launch the Secure Browsing Client.

When a Secure Browsing Client user browses to an external site, the following screen appears for a few moments to indicate that the user is now browsing through Jetro Secure Browsing.

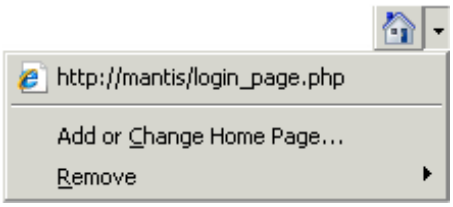
- **Favorites**: If no default settings regarding Favorites have been changed in the Administration Console, then the Favorites list is automatically copied from the internal browser to the external browser each time the Secure Browsing Client is restarted on the Client computer. This mechanism adds the Favorites in the internal browser to the Favorites in the external browser; it does not delete the Favorites in the external browser. For security reasons, the Favorites list is not copied from the external browser to the internal browser. However, changes made to the Favorites list in the external browser are saved.

  NOTE: The Secure Browsing Client usually restarts automatically every time the computer is restarted. You can use the Secure Browsing tray icon menu to exit and restart.

- **Home Page:** The Home Page is determined by the Home Page setting of the internal browser. The Home Page can be either an internal or an external website. If no default settings regarding the Home Page have been changed in the Administration Console, the Home Page setting is automatically copied from the internal browser to external browser each time the Secure Browsing Client is restarted on the Client computer. In this case there is no reason to change the Home Page in the external browser, since it automatically reverts to the internal browser's Home Page setting in the next session.

Typically, there are two ways to set a Home Page:

- Use the browser's option, as shown below:



- Click a link in a web page, as shown below:

These options only work if they are performed while you browse from the internal browser. To ensure that you are in

the internal browser, navigate to a website that is inside the organization's domain.

- When switching between the internal and external browsers, the previously displayed browser window closes when the new browser window appears. This is the default behavior.
- **Open RDP Tunnel**: When a user browses through an external browser on a Terminal Server, the connection goes through two gateways which form an RDP tunnel. While this RDP tunnel is open, it uses one of the Terminal Server Microsoft licenses. This license is freed after the RDP tunnel is closed. The RDP tunnel is closed by the Secure Browsing Client after all the external browsers used by this user are closed. Before closing the RDP tunnel, the Secure Browsing Client waits a considerable amount of time after all the external browsers used by this user are closed (15 minutes, by default).

Secure Browsing Client Tray Icon Menu

The Secure Browsing Client tray icon tells you about the status of the connection of the Client and the Controller. It appears immediately after installation as a gray icon to indicate that the Client is not yet connected to the Controller. It changes to orange when it is connected to the Controller.

If there is a communication problem between the Secure Browsing Client and the Controller, the Secure Browsing icon turns gray. If this happens, the Secure Browsing user is still able to navigate to internal sites, but not to external ones.

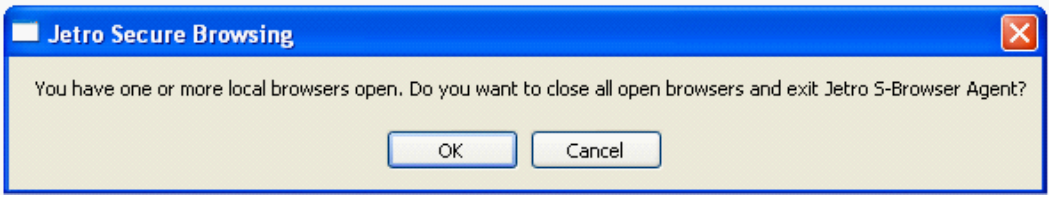
You can right-click on the Secure Browsing Client tray icon to display the following drop-down menu:

The options in the drop-down menu are as follows:

- **Disable Secure Browsing**: This option should not appear in your drop-down menu, because it enables a Secure Browsing Client user to disable the Secure Browsing Client, thus removing its protection. You can configure whether this option appears in users' menus in the Browsing Policy screen.
- **Enable Secure Browsing**: This option only appears when you select the **Disable Secure Browsing** option, as described above.This option enables the Secure Browsing Client.
- **Exit:** This option closes the Secure Browsing Client. Secure Browsing resets its settings each time you relaunch a browser, therefore there is no reason to use this option except for troubleshooting.

When you exit the Secure Browsing Client, the following happens:

- If only external browser windows are open, they all close without a warning.
- If an internal browser is open, the following window appears:



- **Settings:** Secure Browsing allows advanced administrative users to view and edit system settings from the tabs in the **Settings** screen. Although a full description of the advanced options in this screen is beyond the scope of this guide, the following must be noted:
  - By default, the **Settings** screen is Read Only.
  - To enable access to the **Settings** screen for advanced editing, you must change the Windows registry entry, as follows:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Jetro Platforms\Secure Browsing]
"SettingsReadOnly"=dword:00000000
```

This feature is described in full in the Jetro COCKPIT User Guide.

Browsing Problems

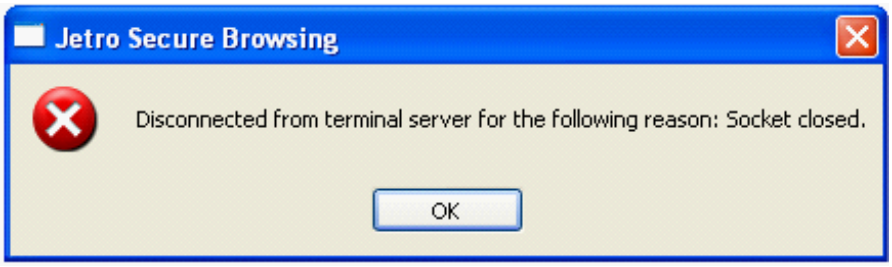
There are various reasons that you may lose connection to the Internet, and most of them are not connected to Secure Browsing. For example, service provider problems, communication errors, browser bugs, viruses, and so on. We suggest that you restart the browser. You should then check if others in your area are experiencing the same problem. If not, check the connection of your own computer.

If there is a communication problem between the Secure Browsing Client and the Controller, the Secure Browsing icon turns gray. In this case, the Secure Browsing user can still navigate to internal sites, but not to external ones.

If the Secure Browsing icon is orange, then the problem is the connection between the Controller and the Internet. The problem is either with the Internet or with the service provider.

Most Secure Browsing Client to Controller connection failures resolve automatically. You will see the icon change back to orange, and you can resume browsing. If it does not turn back to orange, search for the communication problem between the Secure Browsing Client and the Controller.

For example: The following error message appears, when the network cable of the computer on which the Secure Browsing Client is installed is disconnected:



This message is only displayed when there is a communication failure along the path consisting of the Secure Browsing Client computer, the Controller, and the Internet. The Secure Browsing Client tray icon only changes to gray if the problem is the connection between the Secure Browsing Client and the Controller.

When you click **OK** to close this window, the browser window closes.

Exiting the COCKPIT Client

This topic describes how to exit the COCKPIT5i Client.

To exit the COCKPIT4i Client:

1. Right-click the Secure Browsing Client tray icon. The following drop-down menu appears:

2. Select **Exit.**

When you exit the Secure Browsing Client, the following happens:

- If only external browser windows are open, they all close without a warning.
- If an internal browser is open, the following window appears:

Uninstalling the COCKPIT Client

To uninstall the COCKPIT Client, use the Add/Remove Programs utility in the Windows Control Panel.