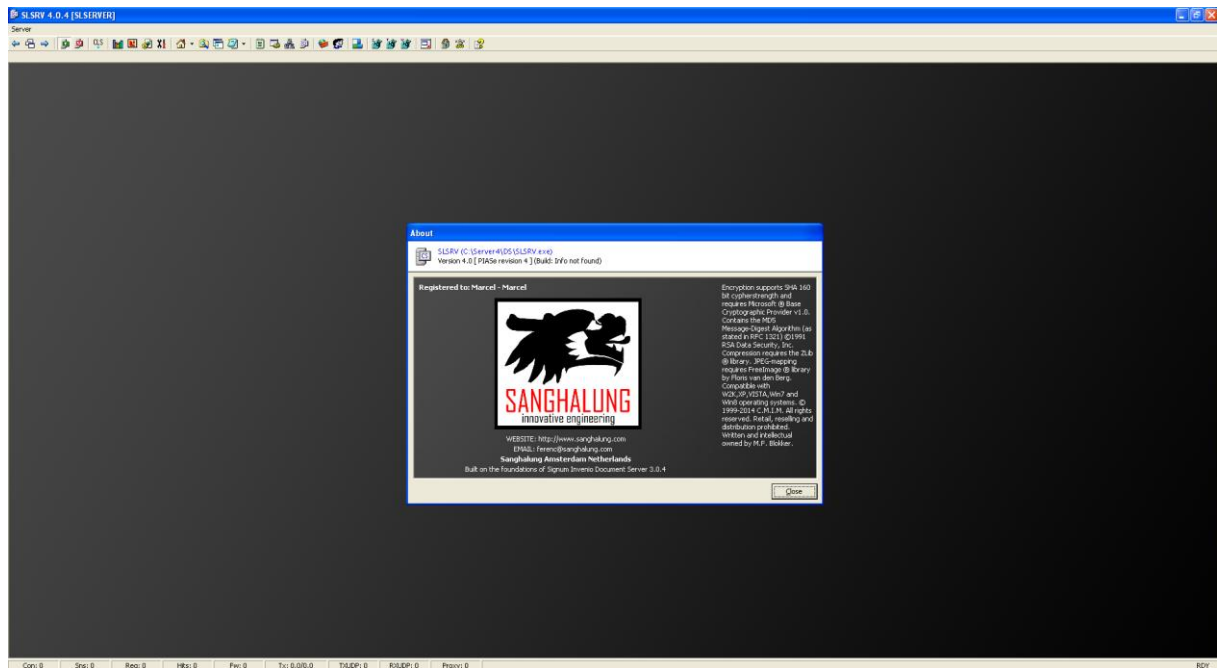


INTRODUCTION

SL SERVER 4



THANK YOU FOR DOWNLOADING SL SERVER 4

SL Server 4 is an intranet/Internet web server delivering its content using the HTTP 1.0 protocol. SL Server 4 can serve documents based on simple HTML-coding or advanced server side scripting technologies. SL Server 4 supports also a UDP server enabling messaging broadcasts and the receiving of broadcast messages over the network for P2P purposes.

SL Server 4 does not run as a service like most servers do, it runs as a normal desktop program. The application can be minimized either in the taskbar or system tray. The administrative functions are embedded in the application for easy maintenance but can be accessed through the IDE or its web interface (browser) by using PIASe scripting language.

The server supports a custom version of Visual Basic for Applications active scripting language enabling you to write advanced and dynamic applications. The standard library has many functions to manipulate incoming and outgoing HTTP streams.

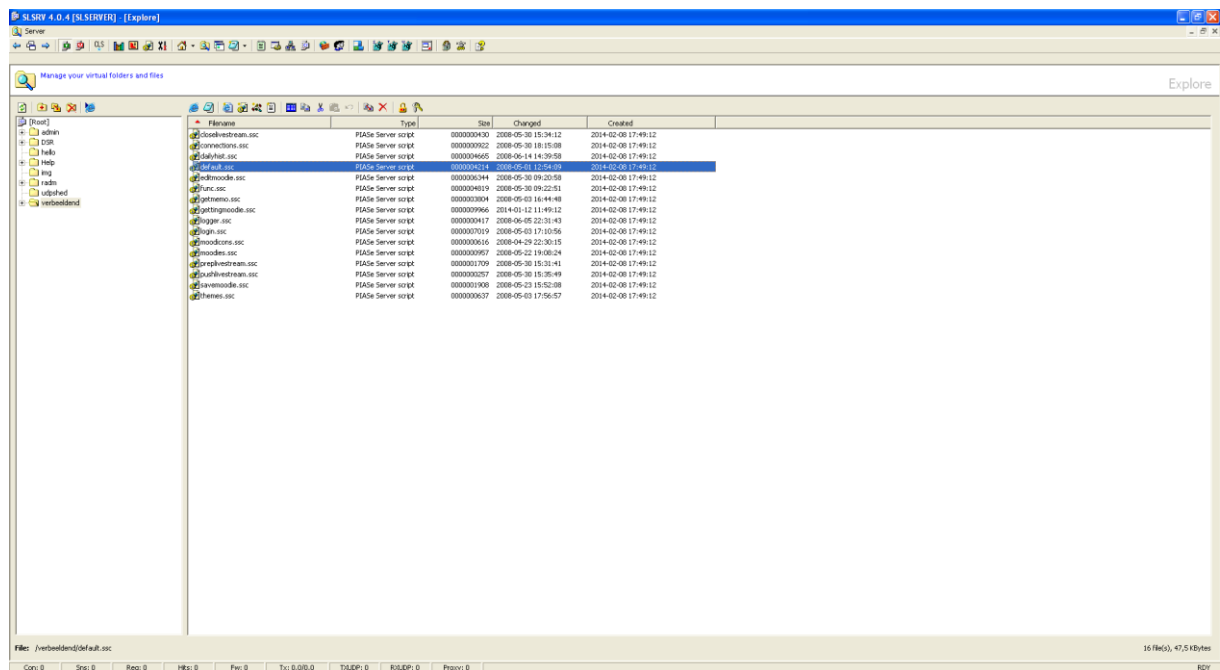
THE IDE MAIN WINDOW

The main window of SL Server 4 contains three items. A server menu, a toolbar and a status bar. The server menu allows you to access server windows, dialogs and functions.

Press the ALT+S key followed by shortcut keystrokes to open the menu and open/activate the desired item or left click the menu and navigate through the menu using the mouse. When working in the main window you'd best use the much quicker approach of the toolbar buttons.

The status bar informs you about current connections, traffic and internal status.

WINDOW: IDE MAN WINDOW



NAVIGATE THROUGH WINDOWS

Toolbar buttons:

Navigate through opened windows. Alternatively you can press Control+F6.


NORMALIZING WINDOWS

Double-click on the white title bar to normalize or click on the appropriate windows button at the right top of the window.

CLOSING WINDOWS



Double-click on the large window icon at the left of the white title bar to close a window or click on the appropriate windows button at the right top of the window.



ACTIVE WINDOWS

Toolbar button: 

View a list of active windows where you can select a window that is currently in the background.



TOGGLE TCP HTTP SERVER

Toolbar button:  / 


To turn on the TCP HTTP server click on the button until it is lit green (). Request are being served. To turn on the TCP HTTP server click on the button until it is lit red (). Request are being denied. Alternatively you can switch mode from the main menu under submenu services.

TOGGLE UDP SERVER

Toolbar button:  / 

To turn on the TCP HTTP server click on the button until it is lit green (). Broadcasts are being served. To turn on the TCP HTTP server click on the button until it is lit red (). Broadcasts are being denied. Alternatively you can switch mode from the main menu under submenu services.


BROWSE

Toolbar button: 

Opens the root of SL Server 4 using an external Browser. By default the root page or script will be served.


Optionally you can select to open your personal start page or a blank page.

EXPLORE

Toolbar button: 


Opens the Explore window, The file manager for the Virtual File System. From this window you can manage your documents, scripts, images and multimedia files.

DOCUMENTS

Toolbar button: 

Display a list of current or recently edited documents.

EDITOR

Toolbar button: 


Opens a new editor window containing a new HTML document.

When you open the dropdown menu from the toolbar button you can choose other file formats based on template files.

FILE TYPES


Menu item	Extension	Template
New HTML document	.htm	/admin/template.htm
New PIASe Server Script	.ssc	/admin/template.ssc
New Server OS Script	.os	/admin/template.os
New Text document	.txt	Not used

DEBUG CONSOLE

Toolbar button: 


The debug console is used to view debug information.

SESSIONS

Toolbar button: 


This window will inform you about currently running sessions.

HTTP SERVER INFORMATION

Toolbar button: 


This window will inform you about server properties and global memory variables.

FIREWALL

Toolbar button: 


In this window you can edit firewall rules to enable or restrict access to the server.

CONFIGURE USERS

Toolbar button: 


In this window you can add user-profiles.

TCP LOG FILE

Toolbar button: 


The TCP log file shows you the port connecting and port transferring process in detail. This information will be useful when determining problems on TCP level. The log can hold a maximum of 4096 log items and will rotate when exceeded.

SERVER LOG FILE

Toolbar button: 


This window will show you a log of all HTTP transactions (permitted by the firewall) of the current day.

FIREWALL LOG FILE

Toolbar button: 


This window will show you a log all transactions not permitted by the firewall of the current day.

CUSTOM MENU

Toolbar button: 


From the submenu of this button you can create custom menu items (listed under the same submenu) pointing to pages or external programs.

STARTUP / SHUTDOWN OPTIONS

Toolbar button: 


Shows you the configuration startup and shutdown configuration options.

TCP OPTIONS

Toolbar button: 


Shows you the configuration TCP (webserver) configuration options.

UDP OPTIONS

Toolbar button: 

Shows you the configuration UDP (broadcast server/client) configuration options.

HIDE CONSOLE

Toolbar button: 


Closes all open windows and minimizes the server to the system tray.

OPEN CONSOLE

(System tray menu).


Click when the application is minimized to the system tray on the SL Server 4 icon in the system tray to open the menu and select "Open console" to restore the IDE main window.

LOCK APPLICATION

Toolbar button: 


Clicking on the lock application button while close all windows (except the main window) and locks all toolbar buttons and menu items. To access the toolbar buttons and menu items you must provide the administrator password. The default administrator password is admin.

CHANGE PASSWORD

Toolbar button: 

This will open a dialog window that allows you to change the administrator password.

HELP

Toolbar button: 

Opens this manual.

THE VIRTUAL FILE-SYSTEM

The virtual file-system is part of the Windows file system and resides on your hard-disk. You can specify its location by editing the *ServerRoot* configuration key. Normally the root is starting in the *www* folder located in the application folder but can be located in any folder and on any windows hard-disk inside your system or network.

The VFS is normally the only part of your file system that is exposed to the HTTP port. By setting permissions for users you decide who may access certain folders within the VFS. Other parts of your hard disk can be exposed too but can only be exposed programmatically using PIASe file system and file mapping functions.

If you are planning to make changes the OS part of the server it is recommended to specify another root location on your drive than the default *www* location. Windows setup may restore any changes made to the OS part of the server when the standard locations is used for root.

ACCESSING THE VFS

The VFS initially contains a root and at least 1 subfolder (*/admin/*). Its not the personal folder of the administrator but is used for the Server Operating System.

The root itself is the main entry of the VFS and can be access through the HTTP protocol by typing the following URL in the address bar of your browser: *http://YourServerName/*.

If a file with the name *default.htm* or *default.ssc* exists inside the root or any subfolder it will be read / executed when a browser is requesting the root (*/*) or a folder name without a filename specified.

If the requested file is not found, the VFS will look for a file with the name *404.ssc* to notify the user or to redirect the request to another page. The VFS will generate a standard error page (status code 404) when a default file and the *404.ssc* file were not found.

When requesting the default file or script by only specifying a folder-name, the folder name must contain a slash (*/*) at the end. Omitting the slash causes the VFS to look for a file having no extension and most likely it will generate a 404 error page.

http: //YourServerName/Test

The URL above causes the server to look for a file named *Test* in the root.

http: //YourServerName/Test/

This URL causes the server to look IN folder *Test* for a default file.

THE VFS SUBFOLDERS

THE */ADMIN/* FOLDER.

The admin folder is an area only to be accessed by the administrative user *admin*. Common and anonymous users are not allowed to access this folder or any of its subfolders.

THE */ADMIN/SERVER/* FOLDER.

This folder contains the Server Operating System (SOS) of the HTTP, UDP -server and Proxy extensions. The SOS contains 5 files having a .os extension. These files should not be modified, moved or deleted in any way without solid knowledge about the SOS because it may halt all services or compromise security.

The VFS hand over control to the SOS after parsing and validating the request. The SOS is responsible for user validation and file-retrieval. Because the SOS is written in PIASe native script an experienced programmer could create additional functionality without the modification of the SL Server 4 executable and new functionality does not depend entirely on new releases of SL Server 4

THE */ADMIN/SERVER/MSG/* FOLDER


This folder contains the various messages the server may generate towards the client. You may change the textual properties of the HTML formatted files but keep in mind that any control characters like @ must stay in place because the VFS will replace control characters with detailed status information (see the message file */admin/server/msg/servererror.htm* for example).

FILE CACHE SYSTEM

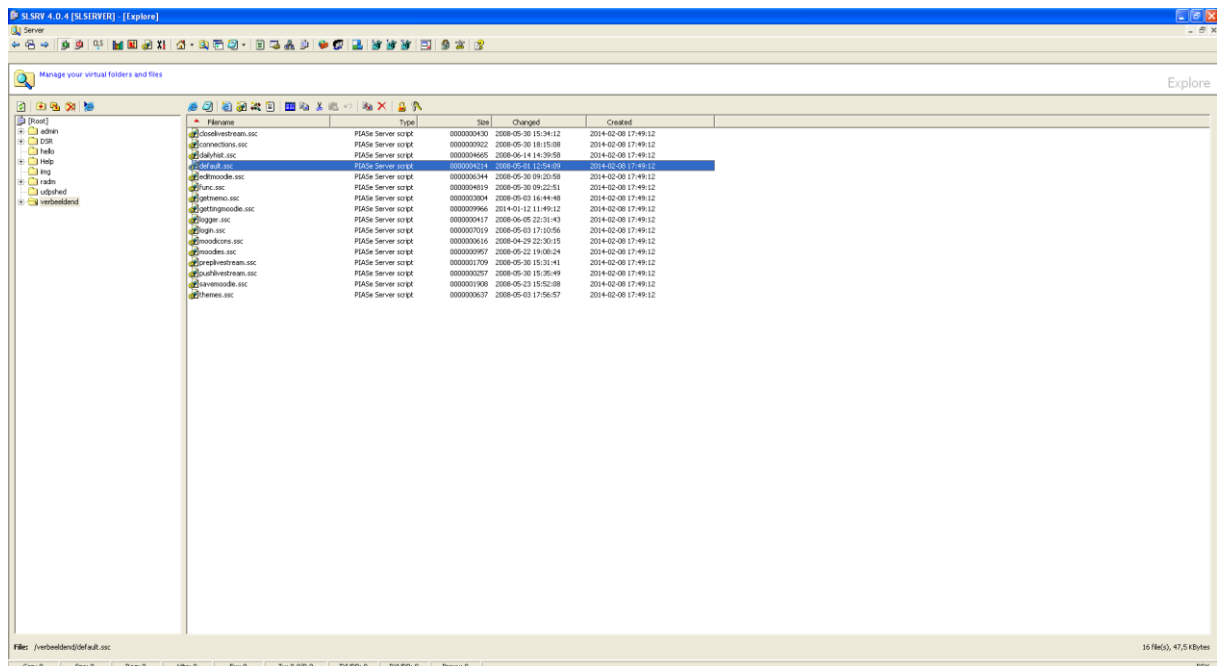
The VFS uses a file cache system (FCS) to store cached files. Cached files cause the VFS to serve faster because the file is already in memory and disk access is not needed. Files that are not read frequently are removed from the cache when it runs out of cache slots.

The PIASe preprocessor uses the cache to store it's compiled results. Whenever a script changes it will be recompiled again replacing older compiled results in the FCS. Preprocessing and compilation are performed on a compile on demand basis.

EXPLORING FILES

The Explore window is a file/folder browser specially for the VFS. It does not explore your common hard-disk, its reserved for the VFS only. From this window you will manage your virtual files. Click on the explore toolbar button  from the main toolbar to open the explore window.

WINDOW: THE EXPLORE WINDOW



The explore window has two panels: The left panel contains the folder structure of the VFS and the right panel contains the files stored in the selected folder. Folders are not listed in the files panel.


SIZING THE PANELS

Move the mouse over the bar that separates both panels from each other, left-click the mouse and start dragging. Size the panels to a more suitable width and release the mouse button.

THE FOLDERS PANEL

Functions in the folders panel can be accessed by clicking its corresponding toolbar button or by selecting a folder and right-click the mouse to open the context-menu.

REFRESHING THE FOLDERS PANEL

Click on the refresh toolbar button  to reload the folders and files panel. You may need to refresh when you have copied files and folders to the VFS outside the IDE.

ADDING A NEW SUBFOLDER

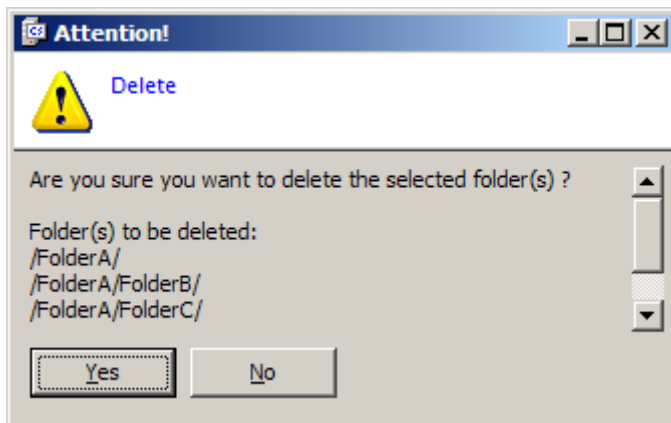
Click on the new folder toolbar button (📁+) to add a new subfolder to the selected folder. Type the new folder name and press enter to complete the process. Press escape to cancel the addition of the new subfolder.

RENAME A SUBFOLDER

Select a folder, click on the rename folder toolbar button (📁✎) to edit the name and change it. Press enter to complete the renaming process. A subfolder cannot be renamed when the editor has open documents in the subfolder you wish to rename.

DELETE A SUBFOLDER

DIALOG: DELETING FOLDERS



Select a subfolder, click on the delete folder toolbar button (📁✖) or press the delete key to delete. Confirm your deletion by clicking on the Yes button in the confirmation window. Any subfolder(s) including any existing files inside the subfolder(s) will be deleted too (All affected subfolders are shown in the confirmation window).

Caution:

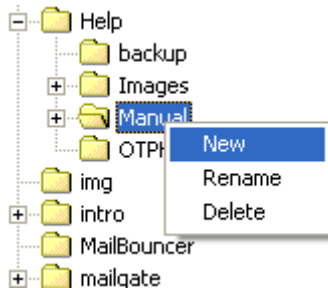
The deletion of folders, subfolders and files is permanent and they are not moved to the bin.

RUN DEFAULT

Mostly, a default script is present in the root or the subfolders. If you want to browse a default script quickly without searching for its presence, click on the run default toolbar button (🔍) from the left panel. This function will look for files named default.ssc, default.htm or 404.ssc.

CONTEXT-MENU

MENU: CONTEXT MENU



Click the right mouse button once while pointing to a subfolder in the left panel to open the context-menu.

MOVE A SUBFOLDER

Select a subfolder, press and hold the left mouse-button while dragging the folder to its new destination. The mouse-pointer will show an additional rectangle. The subfolder, including any subfolders will be moved when you release the mouse-button. During the move a status window is shown indicating the progress.

You may cancel the move procedure by clicking on the cancel button in the progress dialog.

Folders and files will not be moved by the more or less traditional *rename* method but by a *copy first and then delete* method. When you cancel the move you may find the source folder fully intact but you may need to delete files already copied to the selected destination.

If you once started the dragging process you may move the mouse pointer to a location not applicable for moving (the mouse pointer will change to a no-entrance sign) to abort the move.

COPY A SUBFOLDER

Select a subfolder, press and hold the control key, click and hold the left mouse-button while dragging the folder to the destination folder. The mouse-pointer will show an additional plus symbol (+). The subfolder, including any subfolders will be copied to the pointed location when you release mouse-button.

During the copy a status window is shown indicating the copy progress. You may cancel the procedure by clicking on the cancel button in the progress window.

CANCEL DRAGGING

Move the mouse to a location where the mouse pointer changes to a no entrance sign and release the left mouse-button and eventually any pressed key or press the escape key and release the left mouse-button. In both cancel methods the mouse pointer will turn to the default pointer state.

AUTO-EXPANDING SUBFOLDERS

Note that subfolders expand automatically when dragging over a subfolder for a short period of time.

THE FILES PANEL

Functions in the files panel can be accessed by clicking its corresponding toolbar button or by selecting a file and right-click the mouse to open the context-menu.

SIZING THE COLUMNS

Move the mouse over the edges that separates two columns and start dragging. Size the columns to a more suitable width and release the mouse button. Double-clicking a column to size-to-fit.

PREVIEW IN BROWSER





Click on the open location toolbar button () to preview a document using a browser.

EDIT A FILE

Click on the edit file toolbar button () to start editing an existing document.


CREATE A NEW FILE

FILE TYPES

Click on...	To create a...
	new HTML document
	new PIASe script
	new Operating System script
	new Text document

For each file type a different editor mode is used to colorize HTML tags and script code.

SELECTING FILES


Click on the select all toolbar button () to select all files or select a group of files by drawing a selection rectangle over the desired files.

Hold down the control key while you left-click a file to add/remove individual files to your selection.

COPY / PASTING FILES

Select a file or a range of files and click the copy selection toolbar button () to copy the selected file(s).

The selection will change to bold marked files.


Select the destination folder in the folders panel and click the paste toolbar button () to paste the selection into place.


COPY FILES (DRAGGING)

You may also drag and copy files to a folder in the folder pane. Select the file(s) you wish to copy, press and hold the Control key, press and hold the left mouse-button and drag the selection to the destination folder.

Release the mouse-button and control key when you pointing to the desired folder and start the copy. Note that folders expand automatically when hovering in drag-mode over a folder for a short period of time.

CUT FILES

Select a file or a range of files and click the cut selection toolbar button () to cut the selected file(s).

The selection will change to ghost marked files. Select the destination folder in the folders panel and click the paste toolbar button () to paste the selection into place.


MOVE FILES (DRAGGING)

You may also drag and move files to a folder in the folder panel.


Select the file(s) you wish to move, press and hold the left mouse-button and drag the selection to the destination folder.

Release the mouse-button when you selected the desired folder to start the move. Note that folders expand automatically when hovering in drag-mode over a folder for a short period of time.

PASTE FILES

To start copying or moving a selection you must select files first and then paste the selection into place by clicking the paste toolbar button (.

UNDO CUT/COPY

Click the undo cut/copy toolbar button () to undo a selection. Once a copy or move is pasted you can't undo the action.


BACKUP A FILE

To quickly create a backup file before editing click the right mouse-button when pointing to a file and select backup from the context menu.

The selected file will be copied to a file having the same filename plus an additional .bak extension.

A confirmation window will appear if a backup already exists.

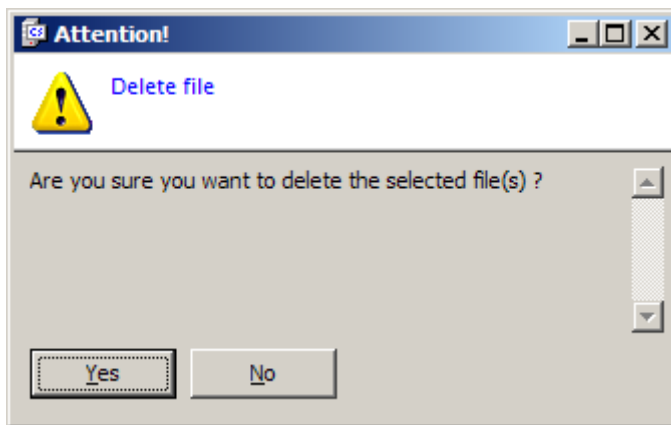
RENAME A FILE

Select a file to rename and click on the rename toolbar button () to start editing the filename.

The filename will keep its extension if you do not type an extension. If you do not wish an extension at all just enter a period at the end of the filename.

DELETE A FILE

DIALOG: DELETE FILES



Select a file or a range of files and click the delete selection toolbar button (✖) to delete the selection.

A confirmation dialog will appear before this action is performed.

ENCRYPT A SELECTION

DIALOG: ENCRYPT SELECTION



Select a file or range of files and click the encrypt selection toolbar button (🔒) to encrypt the selection.

PASSWORD

You have to supply a password to start the encryption of the selection.

USE PUBLIC ENCRYPTION


Check this box if you want to exchange the encrypted file(s) with another SL Server 4.

Note that script-files cannot be interpreted by the script-engine when encrypted.

DECRYPT A SELECTION

DIALOG: DECRYPT SELECTION



Select a file or range of files and click the decrypt selection toolbar button () to Decrypt the selection.

PASSWORD

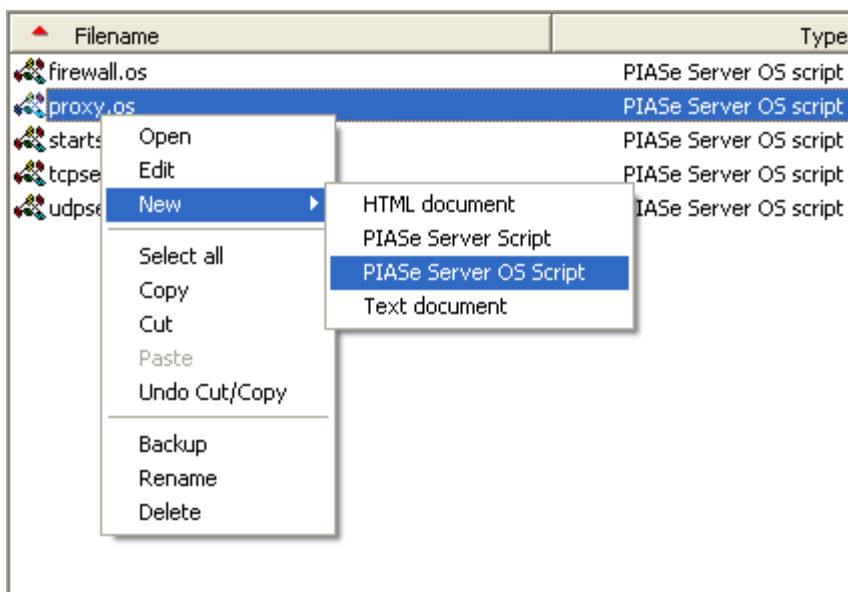
You have to supply a password to start the decryption of the selection.

USE PUBLIC ENCRYPTION

Check this box if you want to decrypt files derived from another SL Server 4 that were encrypted using the public encryption method.

CONTEXT-MENU

MENU: FILE CONTEXT MENU



Click the right mouse button once while pointing to a file in the files panel to open the context menu.


COPY THE CURRENT FILENAME TO THE CLIPBOARD

Click on the filename at the lower-left corner of the explore window, select the entire filename and press control + C. The filename and its path are formatted according the HTTP protocol (forward slashes) and can be pasted easily into the address-bar of a browser or a script-editor.

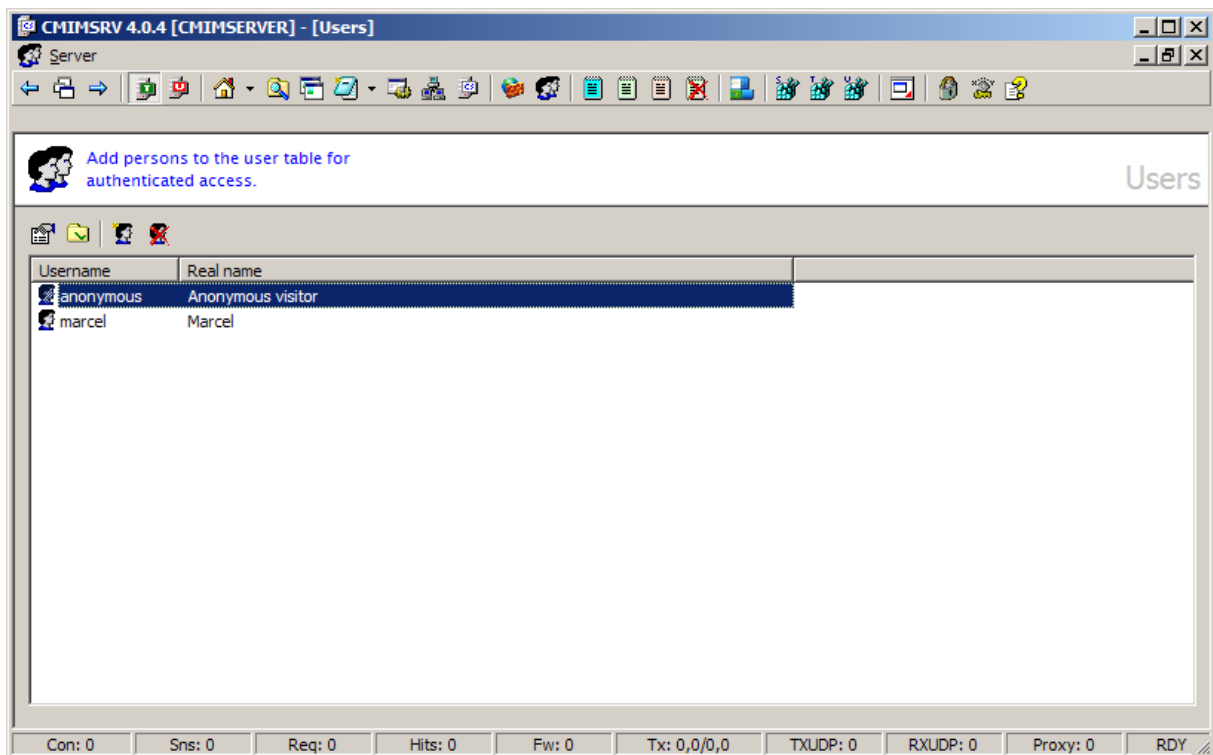
CONFIGURE USERS

The virtual file system of the HTTP service is using an authentication system providing access to folders for individual users. Whenever a page is requested limited by permissions, a login window will appear in the user's browser window. When logged on correctly, the page will be served. If the user fails to logon correctly, an error page is served.

Per user you can specify a set of folders they are allowed to visit. Per folder you can specify a set of flag's allowing the user to do some particular action in the specified folder. The flag's assigned to a folder can be inherited to its child subfolders.


Click on the users toolbar button () from the main window to open the users window.


SCREEN: USERS




You may notice that user anonymous is already listed. The administrative user admin does not appear in this list. User admin has all rights because of its administrative role and editing permissions for user admin is not possible.

Any user that did not logon is by default an anonymous user. By default, the user anonymous may read documents and execute active script listed in the root (/) of the virtual file system.

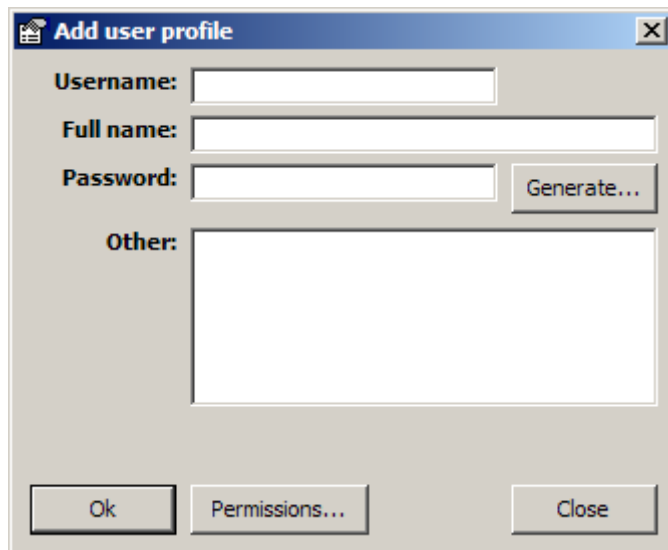
Add a user by clicking the add new user toolbar button ()

Edit a user by double-clicking it's username or by selecting the name of the user from the list and click the user properties toolbar button ()

ADD A NEW USER PROFILE

Click on the add new user toolbar button () to add a new user.

DIALOG: ADD USER PROFILE



- ⇒ Enter a username that starts with a non-numeric character.
- ⇒ The username may contain numeric characters.
- ⇒ Enter the full name of the user.
- ⇒ Enter a password for the new user or generate one.
- ⇒ If a user forgot it's password you must reset this field to a new password.
- ⇒ If some additional information is needed like a phone-number you may enter the additional information in the "Other" textbox.

Save a user-profile by clicking the Ok button and assign permissions by clicking the permissions button from the users window.

ABOUT USERNAME AND PASSWORD

Usernames and passwords are case sensitive. For example, QuickFox is not the same as quickfox. Lower and uppercase characters are different when comparing.

GENERATING A PASSWORD AUTOMATICALLY

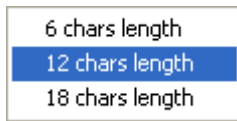
SL Server 4 can generate case sensitive passwords that are to some extent easy to remember. It does so by generating parts consisting 4 non numeric characters and 2 numeric characters. Possible characters are: "BCDFGHJKMNPSTVWZ" on position 1 and 3, "AEU" on position 2 and 4, "0123456789" on position 5 and 6. Characters "o", "i", "l", and "y" are omitted because they could be easily confused with "0", "1" and "j" when printing or writing down the credentials on paper (not advisable).

The passwords resemble the fundamental building of western words and are easy remembered this way.

Examples of passwords: "vehU91" (6 chars), "ZEGE95guBe90" (12 chars) or "FafU30zusE67DetE53" (18 chars).

Click on the generate button and select the length of the password from the popup menu. It's recommended to use 6 characters for nonpublic intranet services, 12 characters for public internet services and 18 characters for persons having special privileges.

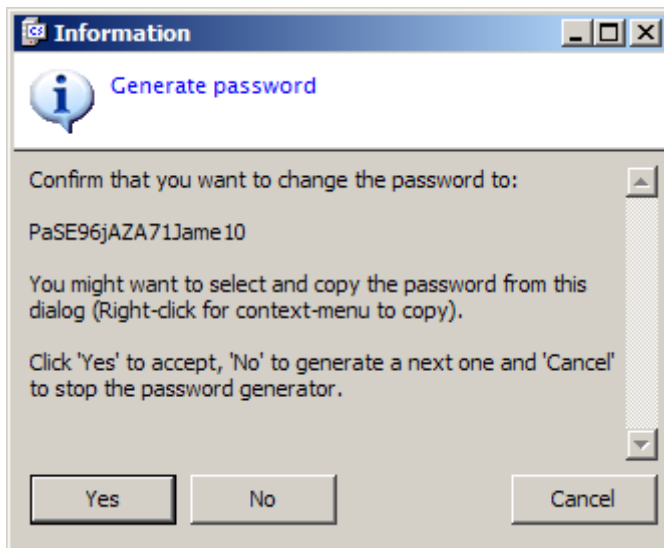
MENU: PASSWORD LENGTH



After the length selection the generator creates a unique password (does not exist as a password in the user table and will not be generated again in the same generator session). Click the yes button to copy the new password to the entry field or no to generate another one. Click cancel to abort the generator without copying the generated password.

If you want to keep record of the password or want to email the new password to the user, you may select the password in the password generator dialog, copy it to the clipboard and paste it into a document or message body. It is not possible to copy the password from the password field itself.

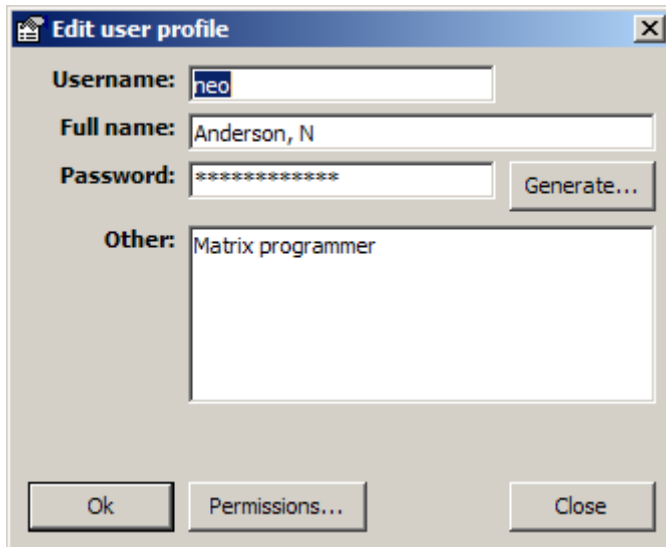
DIALOG: GENERATE PASSWORD



EDIT A USER PROFILE

Select a username from the list and click on the user properties toolbar button (👤) or double click the list-item to edit an existing user.

DIALOG: EDIT USER PROFILE



The screenshot shows a dialog box titled "Edit user profile" with a close button (X) in the top right corner. The dialog contains the following fields and controls:


- Username:** A text input field containing "neo".
- Full name:** A text input field containing "Anderson, N".
- Password:** A text input field containing "*****" and a "Generate..." button to its right.
- Other:** A text area containing "Matrix programmer".

At the bottom of the dialog, there are three buttons: "Ok", "Permissions...", and "Close".

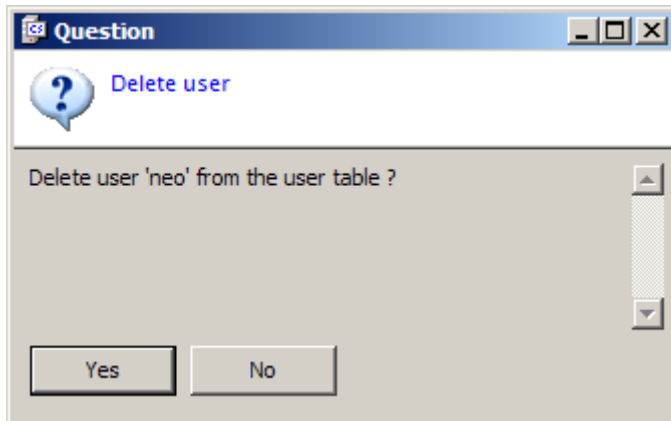
- ➔ Enter a username that starts with a non-numeric character.
- ➔ The username may contain numeric characters.
- ➔ Enter the full name of the user.
- ➔ Enter a password for the new user or generate one.
- ➔ If a user forgot it's password you must reset this field to a new password.
- ➔ If some additional information is needed like a phone-number you may enter the additional information in the "Other" field.

Save a user-profile by clicking the "Ok" button and assign permissions by clicking the permissions button from the users window.

DELETE A USER PROFILE


Select a user from the list and click on the delete user toolbar button () to delete the user from the user table.

DIALOG: DELETE USER



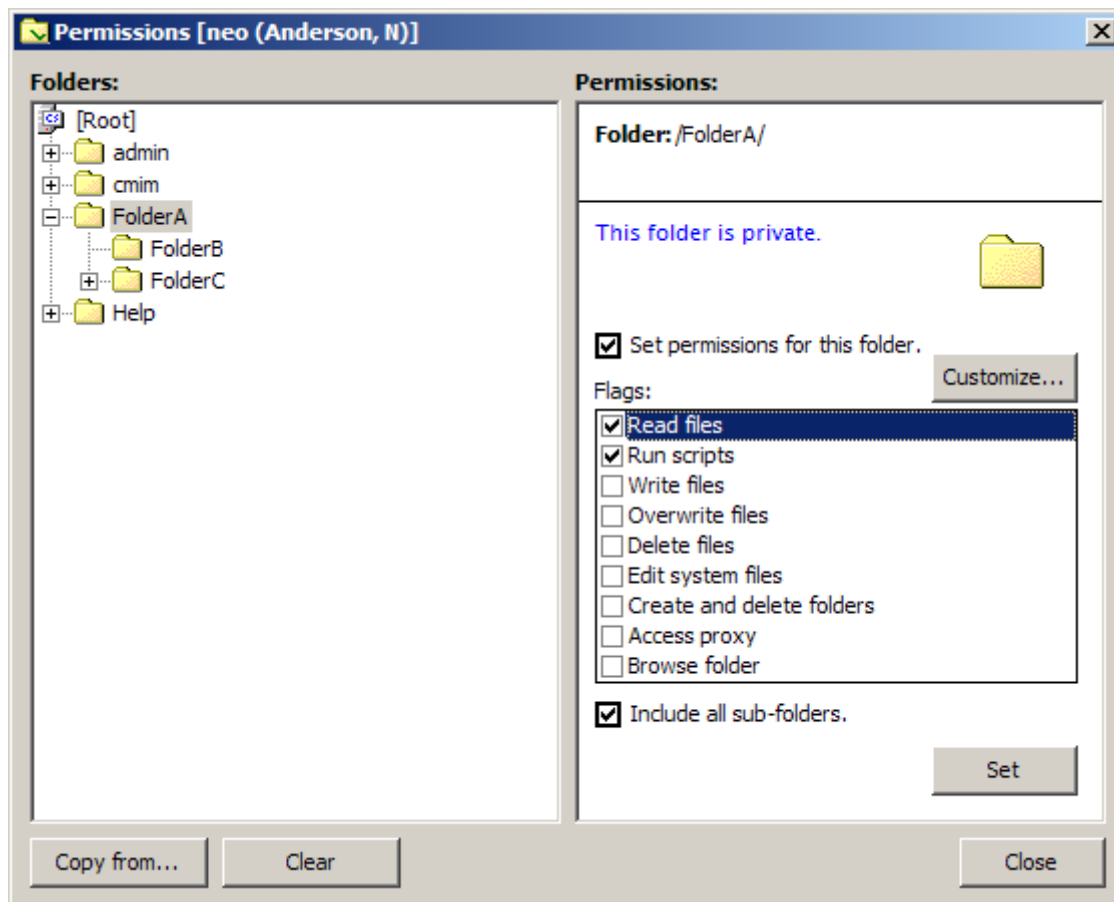
Confirm the deletion by clicking the yes button.

PERMISSIONS

Select a user from the list and click on the "User permissions" toolbar button () to open the permissions dialog.

From the permissions dialog you can assign permission-flags to folders representing certain actions a user is allowed to do. Permissions can only be set for folders and its subfolders (inheritance) and are applicable to all files contained in these folders. Permissions cannot be set for individual files and we recommend to store sensitive files in a separate subfolder.

DIALOG: PERMISSIONS



FOLDERS

The folders panel contains a copy of the full tree of the server's virtual file system. Un-checked folders are private folders. No access is granted to a private folder. Green checked folders are folders a user may visit. Red checked folders are folders explicitly forbidden for the user except for the administrative user.

When folders are marked with a dotted line under the green or red checkmark, the folder is inherited by a setting from a parent node earlier in the tree.

Right-click the panel and open the context menu for expanding or closing the branches.

PERMISSIONS

When you check the set permissions for this folder checkbox you declare an permission record to be added for the selected folder. When you check the include all sub-folders checkbox, You declare an permission record for all child folders of the selected folder (inheritance).

FLAGS

Flags are checked to allow certain privileges. Check a flag to allow and uncheck a flag to deny privileges. You can add new flags to define new privileges for applications you might want to develop in future. Some flags are implemented as a checkable options but may not be implemented in the server operating system. Flags and

permission functions are available to the PIASe script programming language and from script you may decide programmatically how to implement these flags.

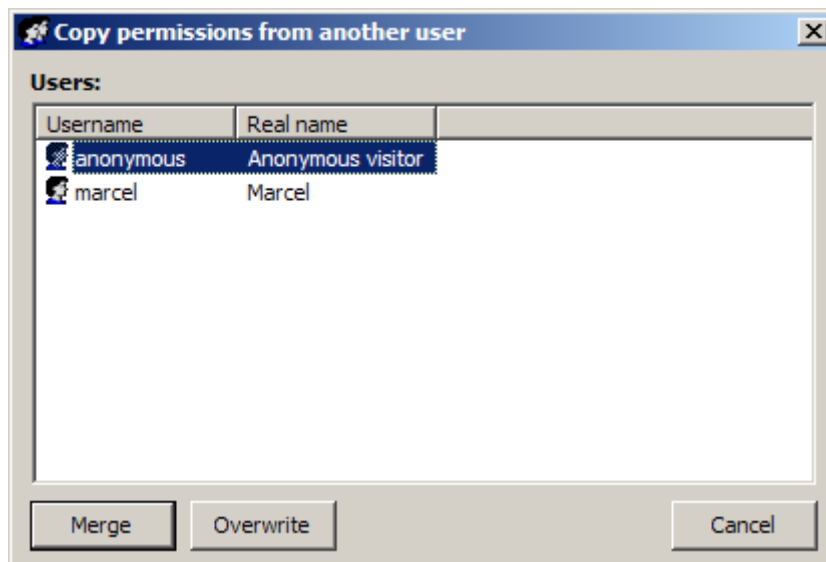
FLAGS IMPLEMENTATION TABLE

Flag	Function
Read files	(Implemented) Allows the download of non-script files.
Run scripts	(Implemented) Allows the execution of PIASe script files.
Write files	(Not implemented) Allows the upload of files.
Overwrite files	(Not implemented) Allows the overwriting of files.
Delete files	(Not implemented) Allows the deletion of files.
Edit system files	(Not implemented) Allows the editing of system files.
Create and Delete folders	(Not implemented) Allows the creation and deletion of folders.
Access proxy	(Implemented) Allows the usage of the proxy functions.

COPY PERMISSIONS FROM ANOTHER USER

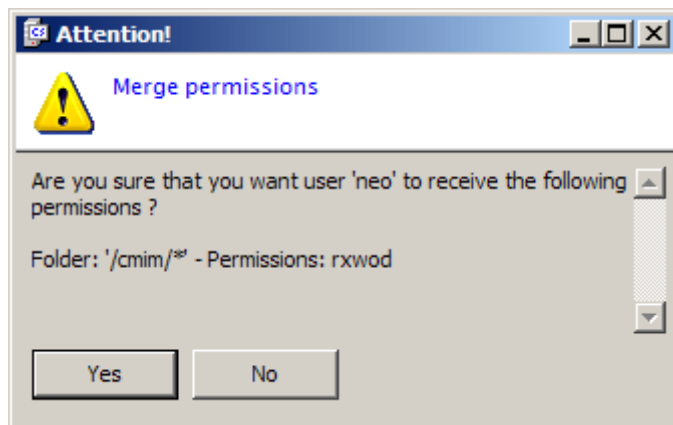
You can copy permissions from another user to the current user. Permissions can be merged with existing permissions or replaced by permissions from the other users. Click on copy permissions from another user to open a the copy dialog.

DIALOG: COPY PERMISSIONS FROM ANOTHER USER



Click on the merge button to add the new permissions to the already existing permissions without replacing the existing permissions. Click on overwrite to replace all permissions from the currently edited user.

DIALOG: MERGE PERMISSIONS



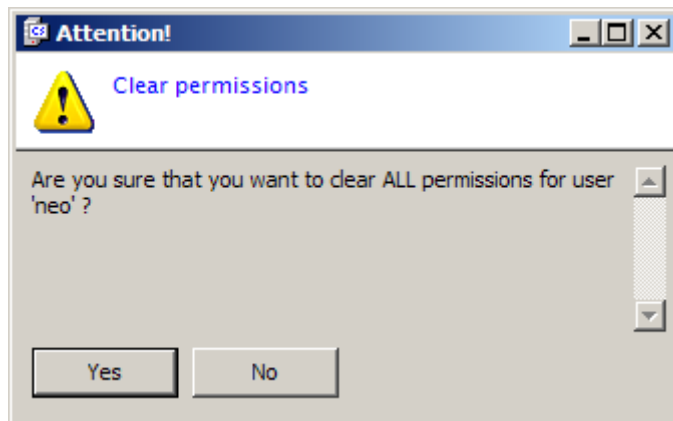
The merge or replace confirmation dialog (both are identical) will show you the modified permissions the user will receive. Click on the yes button to confirm the copy/merge. If the copy/merge is not acceptable, click no to abort.

👉 Create fictional user accounts (starting the username with an underscore) to use it as a group template. Generate a password of 18 characters long and define the permissions for the group. Since the user table does not support groups you may use fictional user accounts to copy permissions from using the merge function.

CLEAR PERMISSIONS

Click on the clear button to delete all permissions for the current user.

DIALOG: CLEAR PERMISSIONS



Confirm your deletion of permissions (not the user) by clicking the yes button or cancel your operation by clicking the no button. Click on the set button in the permissions dialog to apply your new or changed settings.

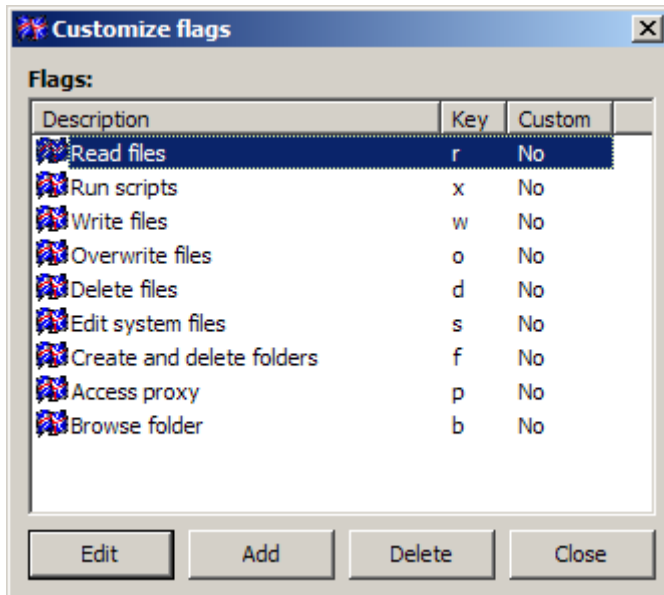
FIND A PARENT FOLDER

Click on the go to parent folder button to locate a parent folder of a child folder. This button is only visible when you have selected a child folder.

CUSTOMIZE FLAGS

Click on the customize button from the permissions dialog to open the customize flags dialog.

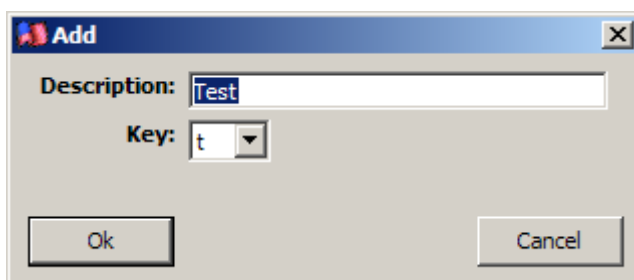
DIALOG: CUSTOMIZE FLAGS



There are two types of flags. Custom and non-custom flags. Non-custom flags cannot be changed because they are effectively in use or will be implemented in near future. Custom flags are tags you can assign to a particular user. You can interact with these flags programmatically.

ADDING A FLAG

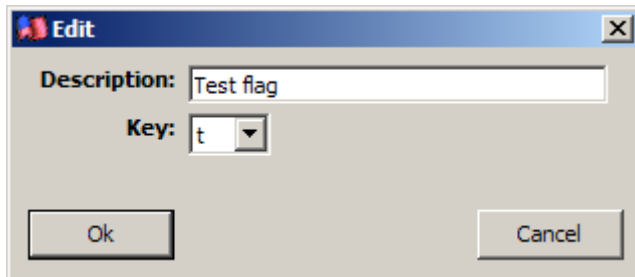
DIALOG: ADD CUSTOM FLAG



Type a description of the flag and select a key. Click on the ok button to complete the addition. Click on the cancel button to abort the action.

EDITING A FLAG

DIALOG: EDIT CUSTOM FLAG



Change the description and the key of the edited flag. Click on the ok button to apply the changes or click on the cancel button to abort the action.

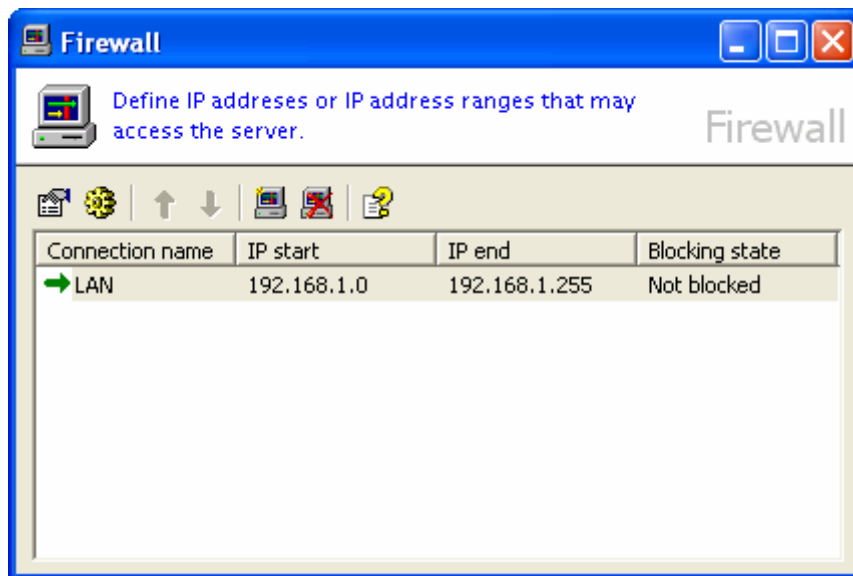
DELETING A FLAG

Click on the delete button in the customized flags dialog and confirm your deletion. Only custom flags can be deleted. Note that the system is not checking the usage of custom flags and you must implement flags into your script.

THE FIREWALL

Before a successful connection is made with the HTTP server, A connection validation mechanism called a "Firewall" checked the client's IP address and the content of the transmitted HTTP request data. The firewall is checking connections before they transmit data and after transmission but in both cases before the request is honored by the HTTP engine.

Click the "Firewall" toolbar button (🖥️) from the main toolbar to open the firewall window



The "Firewall window"

IP ADDRESSES

Every client has an IP address. Clients of a local area network (LAN) usually have IP addresses in the same range and Wide Area Networks (WAN) or the internet have great diversity of IP addresses.

IP addresses are made out of 4 numbers ranging each between 0 and 255 and represent a 32 bits number. IP addresses are used to route data from one network to another. An IP address has two parts, the network ID and the host ID of the computer. Both parts are not equal in bit-size but are sized by three classes: A,B and C.

Class	Values	Network ID	Host ID	Available networks	Hosts per network
A	1-126	w	x.y.z	126	16,777,214
B	128-191	w.x	y.z	16,384	65,534

C	192-223	w.x.y	z	2,097,151	254
---	---------	-------	---	-----------	-----

(w.x.y.z to designate the bytes of the IP address)

Address 127.x.y.z is reserved for loop back testing, Address 224.x.y.z and above are reserved for IGMP (Internet Group Management Protocol) and cannot be used as a host address.

To allow certain groups of IP addresses and IP address-ranges to access SL Server 4 whilst denying other groups of IP addresses or ranges you need to filter connections based on the IP addresses of those groups.

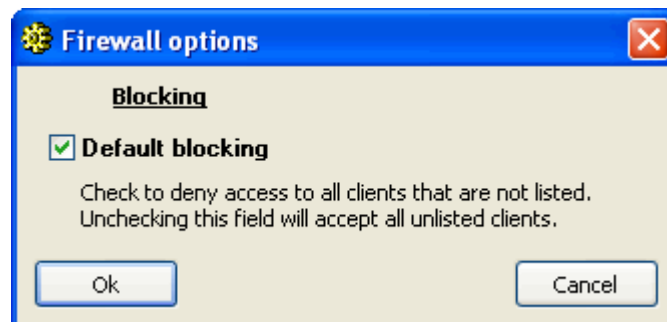
BLOCKING OR NON-BLOCKING

By default the firewall is blocking all connections except the one's that are listed in the firewall table. However, you could configure the firewall to accept all connections except the one's that are listed in the firewall table. The first option is called blocking behavior and is more suitable to intranet web-services. The second option is called non-blocking behavior and is more suitable to internet web-services.

Applying non-blocking / blocking behaviors in the logics of the firewall could save you a lot of IP address typing. Imagine a internet-server having a blocking only behavior. To grant the internet community access you need to enter all IP-address ranges known for the internet community into the firewall table. A non-blocking behavior would be a better solution.

FIREWALL OPTIONS


Click on the "Firewall options" toolbar button () to open the firewall options dialog.



The "Firewall options" window

Select the default blocking type and click on the "Ok" button to save the setting. Read also the "[Blocking or non-blocking](#)" section.

ADDING A FIREWALL ENTRY

Click on the "Add new rule" toolbar button () to add a new firewall entry.

Add rule

Client(s)

IP start-range: 1 . 0 . 0 . 0

IP end-range: 0 . 0 . 0 . 0

Description:

Blocking

Deny access to all services.

Ok Cancel

The "Add" window

If you want to add a range of IP addresses, Enter the starting IP address in the "IP start-range" field and enter the ending IP address in the "IP end-range" field. Type a description for this rule and check the "Deny access to all services" checkbox if you want to block this range of IP addresses.

If you want to add a single IP address, Enter the IP address in the first field ("IP start-range"). Leave or set the "IP end-range" field to "0.0.0.0". Type a description for this rule and check the "Deny..." checkbox if you want to block this IP address.

When adding single IP addresses you may use asterisks to mask IP sub-field values. The firewall will ignore a sub-field if a sub-field value is masked with a wildcard. An IP start-range having the value "192.168.1.*" will filter all IP addresses between "192.168.1.0" and "192.168.1.255".

👉 The use of an asterisk is not allowed when the "IP end-range" field is in use.

Click on the "Ok" button to save your entry or click on the "Cancel" button to abort the addition of a firewall rule.

EDIT A FIREWALL ENTRY

Edit rule

Client(s)

IP start-range: 192 . 168 . 1 . 0

IP end-range: 192 . 168 . 1 . 255

Description: LAN

Blocking

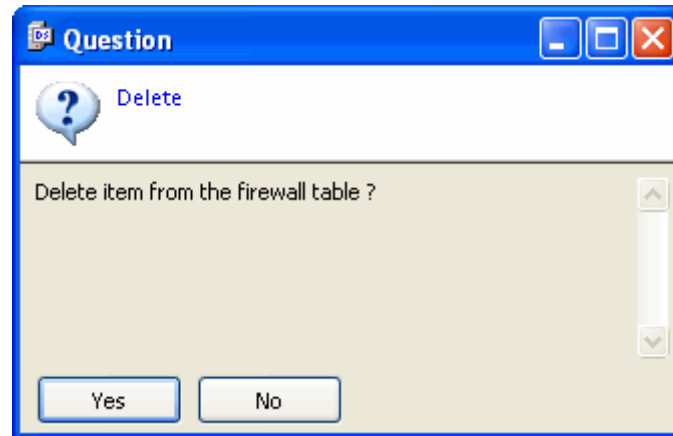
Deny access to all services.

Ok Cancel

The "Edit" window

Select a firewall entry from the "Firewall" window and click on the "Edit rule" toolbar button (📄) or double-click the firewall entry. Change the entry and click on the "Ok" button to save your changes.

DELETE A FIREWALL ENTRY



The "Delete confirmation" dialog

Select a firewall entry from the "Firewall" window and click on the "Delete rule" toolbar button (🗑️). Confirm your deletion by clicking on the "Yes" button in the confirmation window to complete the deletion.

MOVING FIREWALL PRIORITY

The firewall evaluates the rules-list from top till bottom. If an IP address is not filtered by a list rule, the default option is used. If an IP address is matched by more than one rules, the result of the last matching rule is the final result of the query. Moving the rules up and down the list will change the evaluation order of the list.

For example: If you add a non-blocking rule for domain 192.160.*.* but you wish to block station 192.160.1.5 you must move the second rule to a position that is **after** the non-blocking first rule. In that case all IP addresses of domain 192.160.*.* may pass with the exception of IP address 192.160.1.5.

If you would swap these rules the outcome would be initial a block on IP address 192.160.1.5 but by evaluating the second rule (192.160.*.*) it would allow the same IP address to connect since that is the result of the last evaluation.

Click the "Move rule up" toolbar button (⬆️) to move a rule up in the list and click the "Move rule down" toolbar button (⬇️) to move a rule down the list.

SESSIONS

SL Server 4 tries whenever a connection is made to match the connection to a session. Per successful transaction a session-cookie is successfully submitted to the client. If the client is returning the same session-cookie in the HTTP-header of the next request within a certain time-period (Time-to-live) the session will be maintained. If the next request doesn't return within a certain time period or the session-cookie isn't valid anymore the session will expire.

SESSION-COOKIE

A session cookie is basically a HTTP header-field containing a MD5 hashed value. This value is used by the server as a lookup value for information stored at server side and is used to keep previous stored results in relation to the connections and established sessions. The ID is unique during the run of the server and once a ID is issued it will never be issued again during a server run.

A sample of a HTTP response-header with the session-cookie marked in red:

```
HTTP/1.0 200 OK
Server: SLSRV/4.0.4;+MyServer
Date: Wed, 15 Oct 2003 23:47:53 GMT
Expires: Wed, 15 Oct 2003 23:47:53 GMT
Location: /Help/Manual/i010 Sessions/
Set-Cookie: uid=a7259ca65934ae6b0d38cf805a3daef6; path=/
Content-Type: text/html
Content-Length: 728
```

And in the request-header:

```
GET /Help/Manual/i010%20Sessions/ HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel,
application/msword, application/x-shockwave-flash, */*
Referer: http://127.0.0.1/Help/Manual/index.ssc
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: 127.0.0.1
Connection: Keep-Alive
Cookie: uid=a7259ca65934ae6b0d38cf805a3daef6
```

THE CREATION OF A SESSION

If a client is connecting for the first time it doesn't supply a session-cookie in the HTTP-header. The server will save the request and send a response (including a newly made and unique session-cookie) back to the client forcing the client to redirect to a special URL to verify if the client is returning the same unique session-cookie. If the client returned the same session-cookie the server will redirect the client to it's original request and allows the client to continue. At this stage, the session is created.

WHEN A CLIENT CANNOT HANDLE A SESSION


If a client is rejecting the session-cookie for a number of times the server will block the client and denies further service. The use of a session-cookie is required for normal operation. Using a two-stage mechanism to create a session prevents "scanners" (a tool used by hackers) to enter the server because most of such tools do

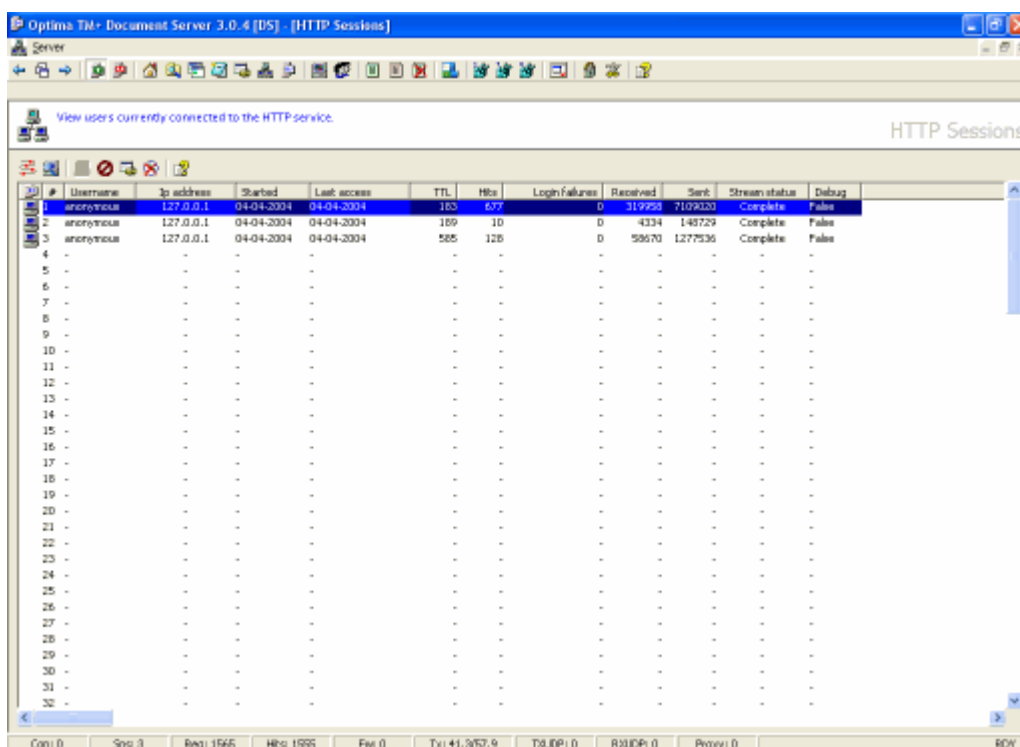
not redirect or support session-cookies. The number of bytes served to such malicious clients are limited to a minimum.

MAINTAINING A SESSION

When a client is sending its session-cookie to the server it will automatically increase the TTL for that session. The server will also compare the IP address of the client if it is the same IP address as the IP address that was registered during session creation. If both addresses do not match, A possible session hijack may have been performed and depending the server's configuration the server blocks further service.

THE HTTP SESSIONS WINDOW

Click the "HTTP Sessions" toolbar button () from the main toolbar to open the "HTTP sessions" window




#	Username	Ip address	Started	Last access	TTL	Hits	Login failures	Received	Sent	Stream status	Debug
1	anonymous	127.0.0.1	04-04-2004	04-04-2004	162	677	0	31995	710920	Complete	False
2	anonymous	127.0.0.1	04-04-2004	04-04-2004	169	10	0	4334	148729	Complete	False
3	anonymous	127.0.0.1	04-04-2004	04-04-2004	585	128	0	58670	1277536	Complete	False
4	-	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-	-	-
27	-	-	-	-	-	-	-	-	-	-	-
28	-	-	-	-	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-	-	-
30	-	-	-	-	-	-	-	-	-	-	-
31	-	-	-	-	-	-	-	-	-	-	-
32	-	-	-	-	-	-	-	-	-	-	-

The "HTTP Sessions" window


The "HTTP Sessions" window displays a list of active sessions. The list shows you the username, The IP address, session start time, last access time, TTL, Hits, Login failures, Received bytes, Sent bytes, Stream status and the debug status.

The list is dynamically updated when events appear to keep track on the real-time session status. This window also contains functions to control the behavior of live sessions.


ACTIVITY TRACKER

Will display a red cursor to indicate activity caused by a session. Toggle the "Activity tracker" toolbar button () to turn tracking on (pressed state) or off (depressed state).


HTTP SESSION INFO

This will display additional information and session variable use of the selected session. Click the "HTTP Session info" toolbar button () to open the "[HTTP Session info](#)" window.


ADD TO FIREWALL

Add a blocking rule for the IP address of the selected session to the [firewall](#). Click on the "Add to firewall" toolbar button () to create the firewall rule. Note that the local loop back address (127.0.0.1) cannot be added to the firewall because it will disable administrative access.


LOCK SESSION

Toggle the "Lock session" toolbar () button to deny or allow any resource to be sent to the client. If locked, the client will receive a message from the server that the session is locked by the administrator. Use this function if you need to make script modifications that requires 'radio silence'.

SEND TO DEBUG WINDOW

Toggle the "Send to debug window" toolbar button () to enable (pressed state) or disable (depressed state) the debug mode for the selected session. When you set the debug mode for a session all url's from requests made by the client owning the session are printed to the debug console. This enables you to trace link, post and redirection behavior from server side script.

RESET TTL TO ZERO

Click the "Reset TTL to zero" toolbar button () to end the selected session and to destroy all it's related session variables.

COLUMNS

Username

If a user is logged on (authenticated), it's username will be displayed otherwise the username "anonymous" is displayed.

IP Address

The IP address of the client computer (may be the IP of a proxy server).

Session start time

Date and time when the session was created by the server.

Last access time

Date and time when the client requested for a resource.

TTL

Time-to-live, Time left before a session expires. When you viewing session data using the "Session Info" window the session will be kept alive and will be set to 10 seconds until you close the info window.

Hits

Number of page/resource hits.

Login failures

Number of login failures.

When the username is not anonymous: A value between 1 and 3 indicates a "normal" logon, A value between 4 and 20 indicates a user that possibly typed it's password wrong and higher counts may indicate a successful brute-force logon.

When the username is anonymous: Any value may indicate that a user forgot it's password. High values (20+) may indicate a password hack attempt. Brute-force attempts (automated hack applications) may cause values between 1,000 and 100,000 depending the duration of the attack. The server will stop authenticating after 50 failed attempts. Any attempt after #50 still causes the login dialog to appear at client-side and the server still allows the "hacker" to send it's credentials but the server will not lookup the user database. As a result of that, the login attempt fails and a "access denied" response message is submitted by the server. The "hacker" will not know that the server is on to him and will most likely continue the brute-force attack enabling the administrator to detect the attack and find possible clues about the attacker.

Received

Number of bytes received by the server from the client.

Sent

Number of bytes sent by the server to the client.

Stream status

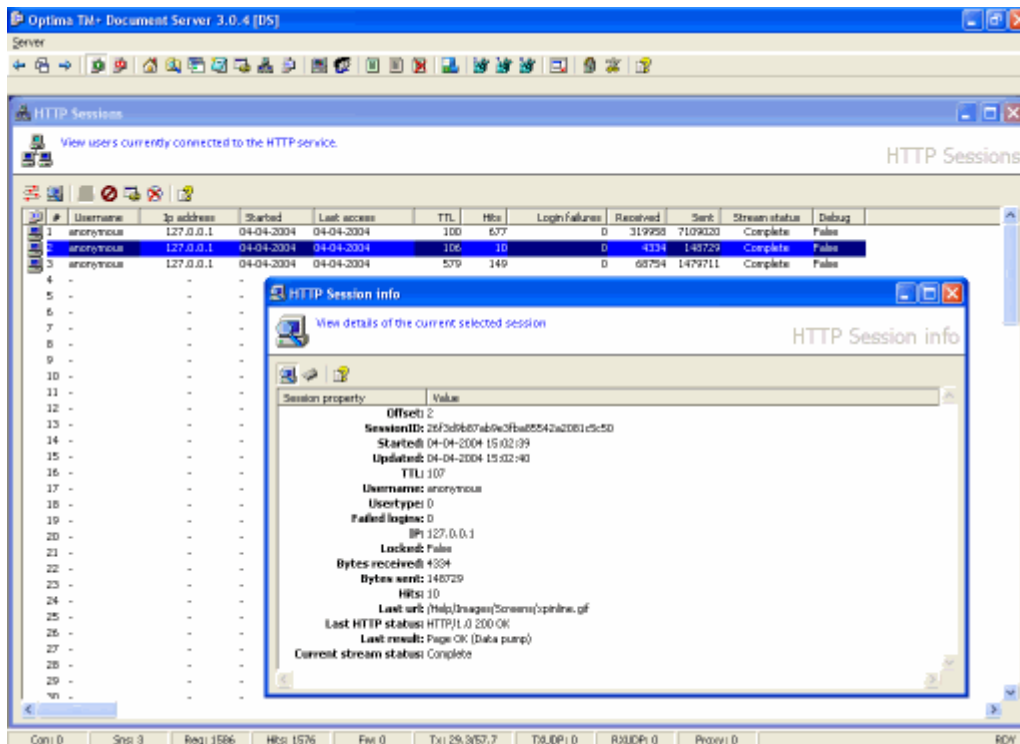
Indicates a running resource transfer ("Streaming"), Completed resource transfer ("Completed") or Resource transfer canceled by client ("Dropped").

Debug

Indicates whether the server should write all request url's of the session to the debug window and enables you to track a session by monitoring request behavior. This will help you to debug your server-side application or to find out what somebody is doing.

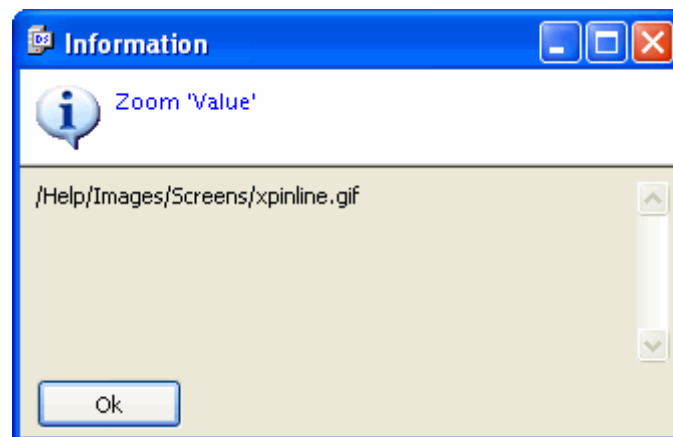
HTTP SESSION INFO

Select a session from the list in the "[HTTP Sessions window](#)" and click on the "HTTP Session info" toolbar button (🔍) or double-click a session in the list to open the "HTTP Session info" window to view session details. The "HTTP Session info" window may be sized to a larger format by dragging the borders of the "Information" window.



The "HTTP Session info" dialog

The info window will show additional (fixed) session variables not shown in the "HTTP Sessions" window. Only variables NOT shown in the "HTTP Sessions" window are described in the list below. From this window you can view the number and content of (user defined) session variables by clicking the "View HTTP Session memory" toolbar button (🔍). Click when you hovering the cursor over a name or value field to "Zoom" it's content. From the "Zoom" dialog you will be able to copy the zoomed value to the clipboard.



Zoom name or value dialog

FIELDS

Additional session variables listed by the "HTTP Session info" window. See for a description of the omitted fields: "[HTTP Session](#)" window.

Offset

The logical record number of a session.

SessionID

The assigned session ID cookie.

User type

0: Anonymous, 1:User and 2: Administrator.

Locked

The server will deny any resource requested by the client if the session Locked variable is set to True.

Last URL

The last Url retrieved by the client.


Last HTTP status

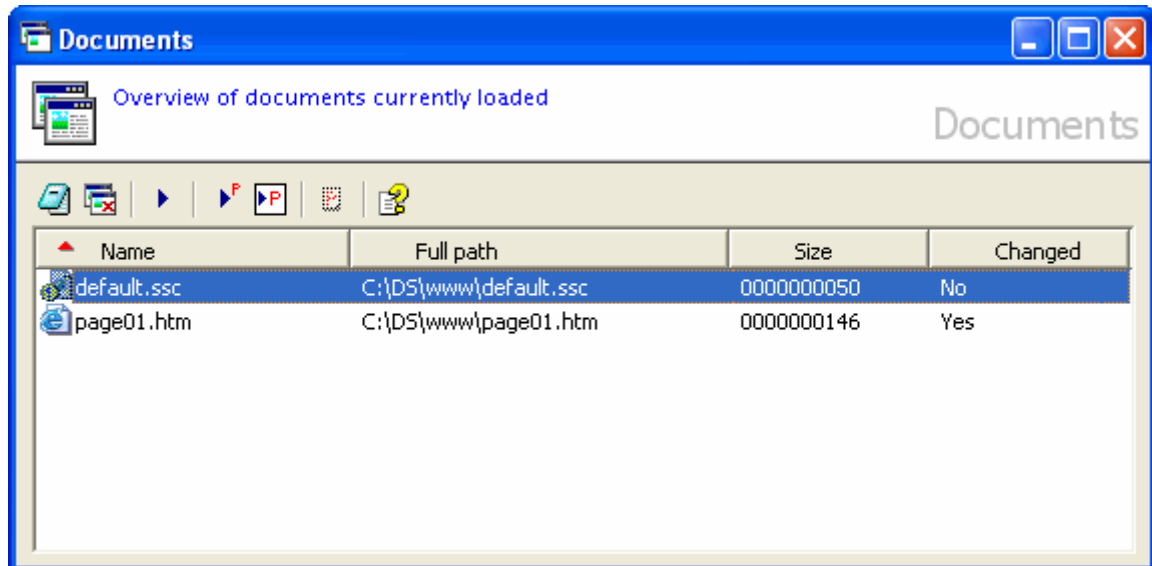
The HTTP status code as stated in the response header of the last request made by the client.

Last result



The server result code of the last request made by the client.

DOCUMENTS WINDOW


The "Documents" window contains a list of currently opened documents and documents that were opened before (grayed items). Click on the "Documents" toolbar button () from any toolbar to open the "Documents" window.



The "Documents" window



By double-clicking a file or by clicking on the "Edit" toolbar button () causes it's window to be the topmost one when it is already loaded or load the selected file in a new editor window. Click on "Close document" toolbar button () to close a file if it's still open or to remove a file from the list when it's already closed.

RUNNING SCRIPT


From the "Editor" or "Documents" window you can run a script file. In basics, it is the same as opening a location from the "Explore" window. Click on the "Save and run source" toolbar button () to run a script.

If you run a script from the editor window the script will be saved before it's location is opened by the "Browser" window. You may also press **Shift + F5** to run the current edited script.

RUNNING MAIN PROJECT SCRIPT

You can choose a script file to be the main file to start. First define a main file by selecting it from the "documents" window or by opening the main file in an editor window. Click on the "Set this page as default project start-page..." toolbar button () to mark the main script-file. Whenever you click on the "Run project default start-page" toolbar button () or press the **F5** key, the script marked as the main script-file will be opened as a location by the "Browse" window.

HIDE / SHOW HISTORY

Click on the "Maintain documents history" toolbar button () so that it is in a pressed state to memorize edited, but already closed documents. Depressing the button causes the list to display only documents currently in memory.

LOGGING EVENTS

Because you can't control visually the usage of the server, a logging system is reporting it for you. Logfiles keep track on every request and the response the server has generated. Logfiles grow very fast when the server has many visitors and need to be maintained on a regular basis to prevent a full disk.

SL Server 4 has three types of logging mechanisms; the firewall logger, the webserver logger and the UDP logger. The firewall logger reports connections that were bounced by the firewall, the webserver logger reports request of the served pages including the results of the request and the UDP logger log's all incoming and outgoing UDP traffic on the UDP port specified by the `UDPListenerPort` configuration variable.

The IDE supports two logging windows, The [webserver](#) log and the [firewall](#) log window.


EXTENDED LOGGING

The webserver logger can, if specified by configuration, log all content data (request and response) in a file per request. This type of extended logging is only of good use to track problems on content level and consumes diskdata in large quantities. See the configuration field [LogWSExtended](#) how to log extended information.

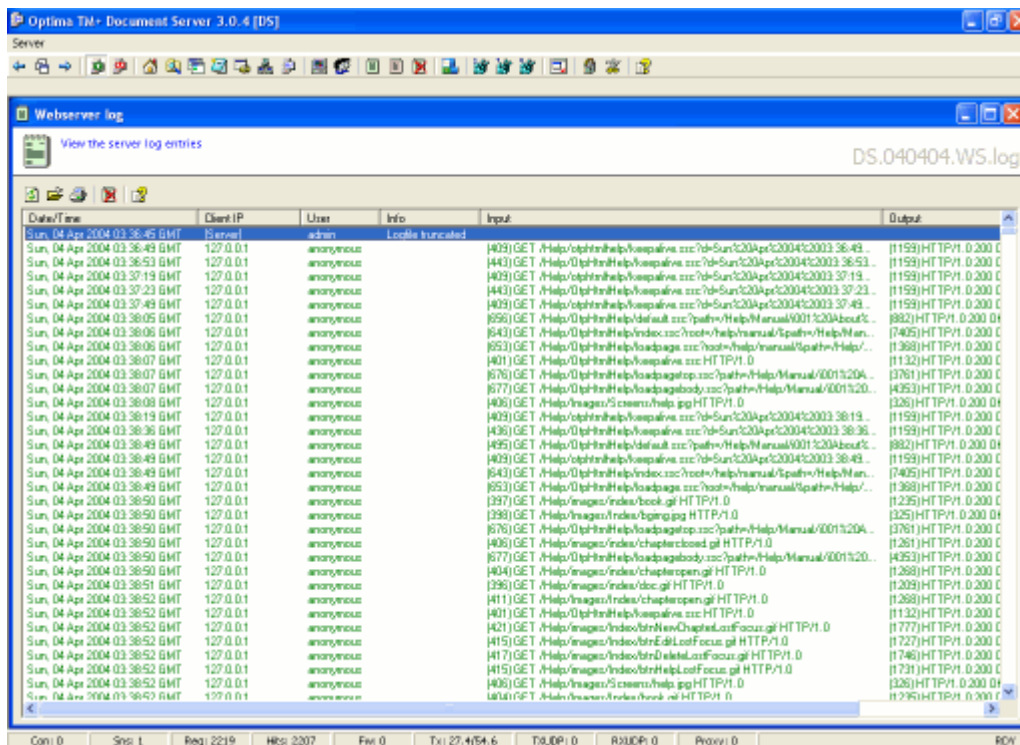
UDP LOGGING

The UDP logger (if the [LogUDP](#) configuration field has been set) log's it's data into the webserver log.





WEB SERVER LOG

All transactions permitted by the Firewall are logged to a web-server log-file. Log-files are created per day and are not created when no transactions were made during a particular day. Click on the "View server log-file" toolbar button () to open the log file.

Note that loading a log-file can consume time and will hold any requests made by a client. It is therefore recommended to inspect log-files on a quiet moment.




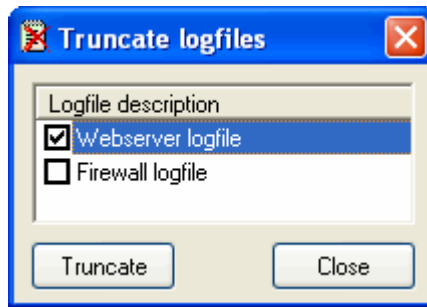
The "Web-server log" window.

The log-file contains date/time, IP, User, Status, Input and Output information. Red colored lines indicate a server error, Blue lines login attempts, Gray lines server status and green lines successful made transactions. Click on the "Refresh log" toolbar button () to refresh the content, Click on the "Open log-file" toolbar button () to load or delete another logged day, Click on the "Print" toolbar button () to print the loaded log-file and click on the "Truncate log-files" toolbar button () to truncate the active log-file.

Double-click an item to view it's details in a dialogue and to copy information from it. See also the "LogWSExtended" TCP configuration variable for more information about extended logging.

TRUNCATE CURRENT LOG-FILE

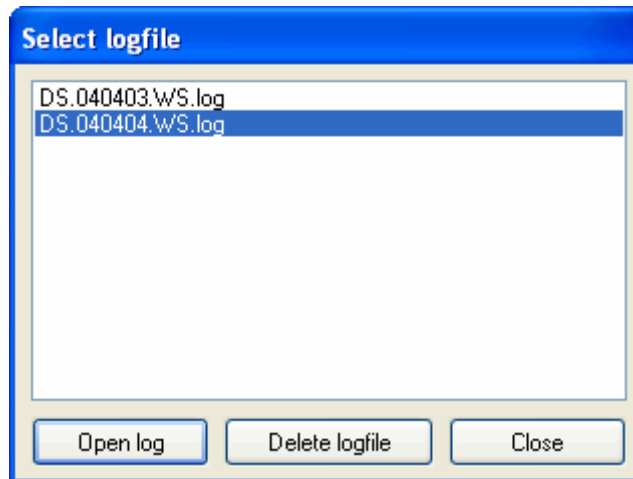
Only an active log-file can be truncated. Non-active log-file can only be deleted from the "Select log-file" dialog. Click on the "Truncate log-files" toolbar button () , Check the log-file checkboxes you wish to truncate and click on the "Truncate" button.



The "Truncate log-files" dialog

OPENING ANOTHER LOG-FILE

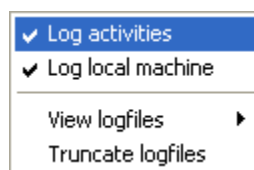
Click on the "Open log-file" toolbar button (📁) to load or delete another logged day. Select a particular day from the list and click on the "Open log" button. Filename's are formatted in a YYYYMMDD manner. Click the "Delete log-file" button to delete a particular log-file.



The "Select log-file" dialog

SET LOGGING BEHAVIOR

Logging information is depending on the settings you can apply in the logging menu. Select the menu "Server" → "Logging" to specify the logging behavior.



The "Logging" menu

In this sub-menu you can specify if SL Server 4 must log activities. Click on the "Log activities" to toggle logging. The current status is shown as "(on)" meaning that logging is currently on or "(off)" meaning that logging is currently off.

Local machine is the computer where SL Server 4 is running on. If you do not wish to log activities from this computer (mostly caused by the administrator) you can toggle local logging off.

EXTREME LARGE LOG-FILES

When log-files getting larger than 250 Kb a question will appear if you wish to read the complete file or only the last 250 Kb of log-data. Depending the information you're looking for you may choose to read the full file but consider longer list building-time. During long reads the server will continue to work normally but slower though and shows you a progress window giving you an idea when it completes the building of the list. The log-window will not be available during the building.

COLUMNS DESCRIPTION

Date time

The date and time of the request.

Client IP

The IP address of the requesting client.

User

The username of the client if logged on and "anonymous" when a client is not required to authenticate. If the field is empty no session could be established or the request was invalid or blocked by the firewall.

Info

Specific messages generated by the server.


Input

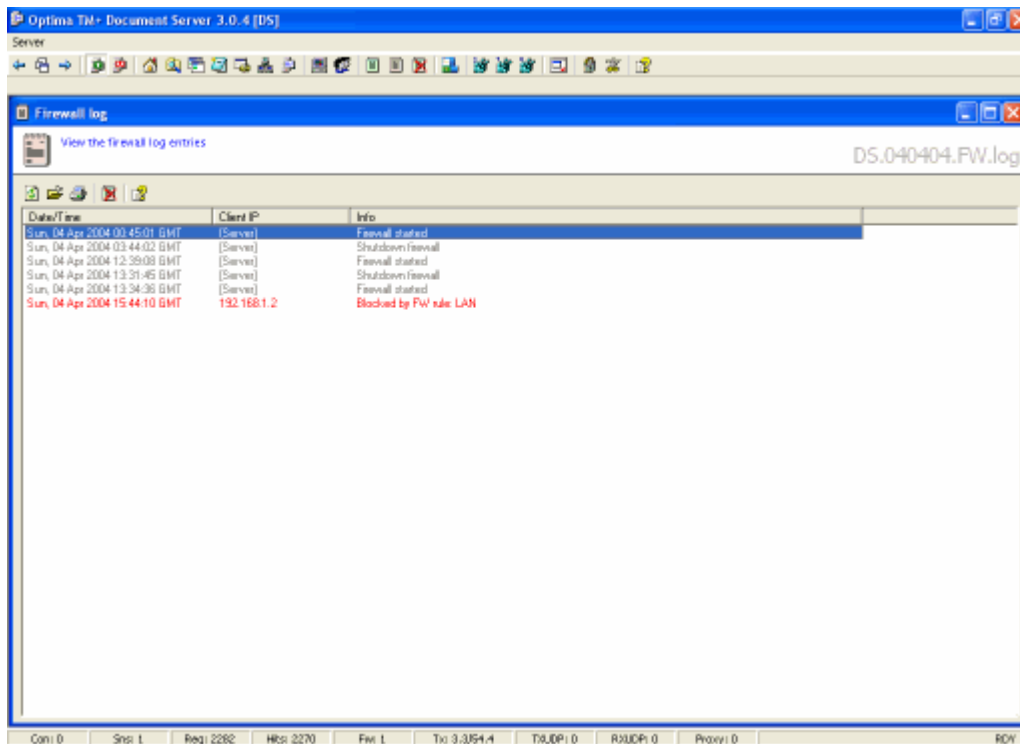
The request of the client.

Output





The response of the server.

FIREWALL LOG

All transactions not permitted by the Firewall are logged to a firewall log-file. Log-files are created per day and are not created when no denied-access attempts were made during a particular day. Click on the "View firewall log-file" toolbar button () to open the log file.




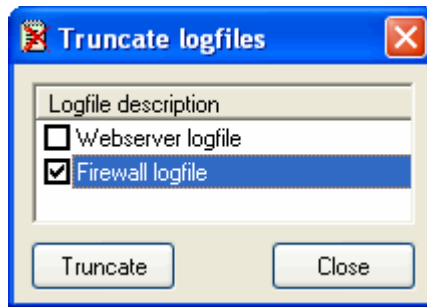
The "Firewall log" window

The log-file contains date/time, IP, and Status information. Red lines are specific denied requests and gray lines inform you about the firewall status. Click on the "Refresh log" toolbar button () to refresh the content, Click on the "Open log-file" toolbar button () to load or delete another logged day, Click on the "Print" toolbar button () to print the loaded log-file and click on the "Truncate log-files" toolbar button () to truncate the active log-file.

Double-click an item to view the row in a dialogue and to copy information from it.

TRUNCATE CURRENT LOG-FILE

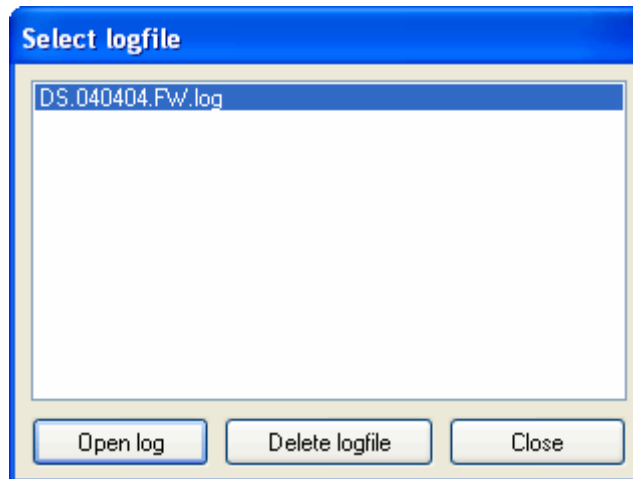
Only an active log-file can be truncated. Non-active log-file can only be deleted from the "Select log-file" dialog. Click on the "Truncate log-files" toolbar button () , Check the log-file checkboxes you wish to truncate and click on the "Truncate" button.



The "Truncate log-files" dialog

OPENING ANOTHER LOG-FILE

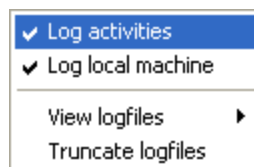
Click on the "Open log-file" toolbar button (📁) to load or delete another logged day. Select a particular day from the list and click on the "Open log" button. Filename's are formatted in a YYMMDD manner. Click the "Delete log-file" button to delete a particular log-file.



The "Select log-file" dialog

SET LOGGING BEHAVIOR

Logging information is depending on the settings you can apply in the logging menu. Select the menu "Server" → "Logging" to specify the logging behavior.



The "Logging" menu

In this sub-menu you can specify if SL Server 4 must log activities. Click on the "Log activities" to toggle logging. The current status is shown as "(on)" meaning that logging is currently on or "(off)" meaning that logging is currently off.

Local machine is the computer where SL Server 4 is running on. If you do not wish to log activities from this computer (mostly caused by the administrator) you can toggle local logging off.

EXTREME LARGE LOG-FILES

When log-files getting larger than 250 Kb a question will appear if you wish to read the complete file or only the last 250 Kb of log-data. Depending the information you're looking for you may choose to read the full file but consider longer list building-time. During long reads the server will continue to work normally but slower though and shows you a progress window giving you an idea when it completes the building of the list. The log-window will not be available during the building.

COLUMNS

Date/time

Date and time a connection attempt has been made.

Client IP

The IP address of the client.

Info

Information about the blocking.

TCP LOG

The TCP log is a rotating log file and can hold a maximum of 4096 items. The TCP Log displays the TCP connecting and transferring process in detail and is very helpful to analyze connection problems.

COLUMNS

Time

Date and time of the request.

Local IP

The IP address of the server. This may be local host (127.0.0.1), the IP address of the NIC or 0.0.0.0. When 0.0.0.0 is listed it indicates a connection problem and the server was not able to retrieve the IP address of the connecting party.

Local Port

The TCP port that the client used during the connection and servicing process.

Remote IP

The IP address of the client.

Remote Port

The TCP port of the client.

Module

WS – The module listening to port 80 and taking care of the transfer to a servicing port.

WSA(index) – The module that handles the receiving of the request and the sending of the response.

The index points to the connection object array that is used for the transferred connection.


State

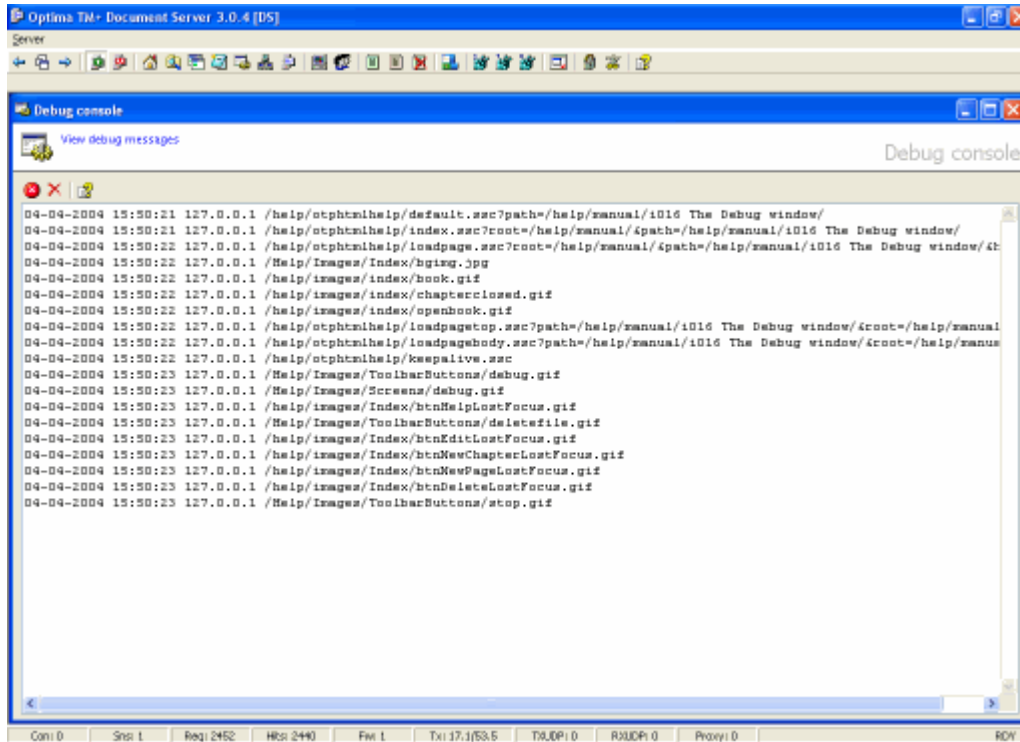
The state of the connection.

Info

Additional information about the connection state.

THE DEBUG CONSOLE

This window is used to print debug information on when a PIASe script is running or when you have set the "debug flag" for a session. Click on the "Debug console" toolbar button () to open the debug window.



The "Debug console"

PRINTING TO THE CONSOLE USING SCRIPT

The script command DPrint outputs expressions to the console and can be used to debug faulty script without the need to modify the HTML structure of a resulting page. When a faulty redirecting script does not output anything this window will come in handy to evaluate expressions to find out what's going on.


The syntax for printing to the console using script: **DPrint Expression**

Be sure when you done debugging to remove the DPrint commands because it will cause performance drop. The DPrint command has no effect in the UA edition of SL Server 4.


SESSION MANAGER DEBUG MODE

When you set the debug mode for a session (see also the "[Sessions](#)" window) all url's from requests made by the client owning the session are printed to the debug console. This enables you to trace link, post and redirection behavior from server side script.

STOP FETCHING MESSAGES

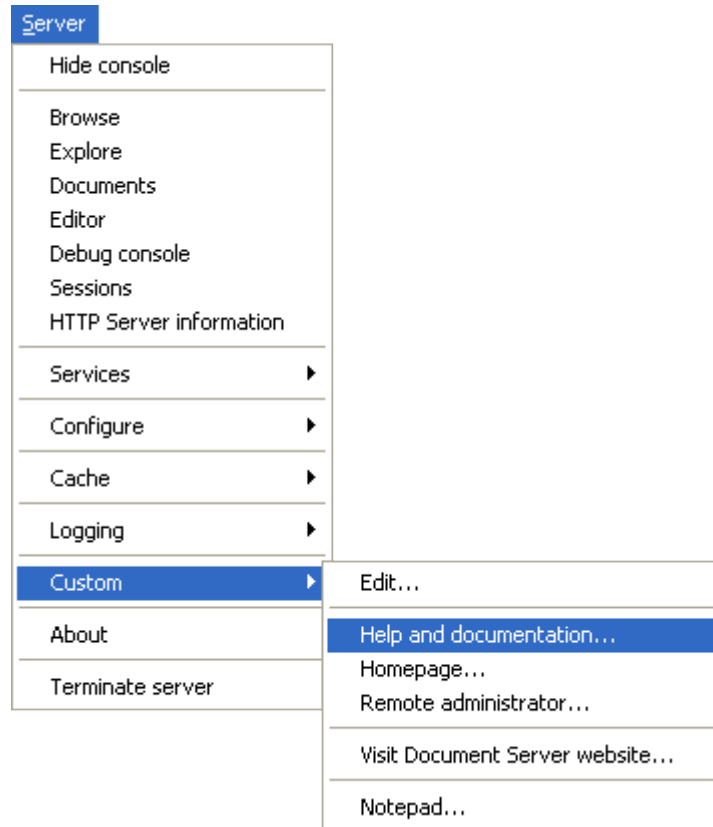
You can stop fetching messages by clicking the "Stop fetching messages" toolbar button () to read details without getting scrolled off-screen. Messages are still received and queued when in stop mode and when you continue to fetch messages all queued debug data is added to the window at once.

CLEAR CONSOLE

You can clear the console's buffer by clicking on the "Delete buffer" toolbar button (.

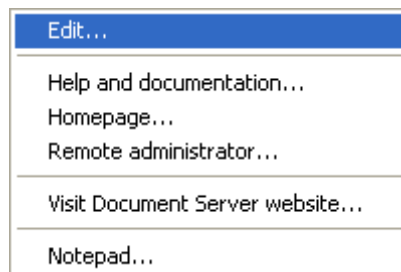
CUSTOM MENU ITEMS

When writing script or HTML pages there is always a nifty tool to use such as an image editor, a reference document, scripts or other needful things that may come in handy when working in the IDE. You can add shortcuts of locations and executables to the server menu by adding a custom menu-item.




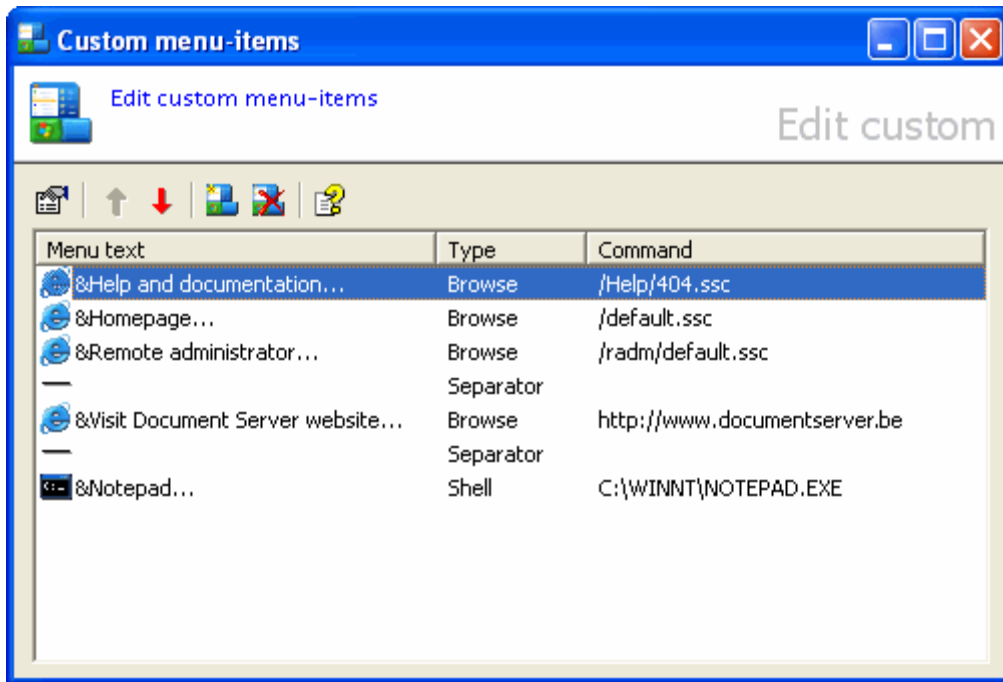
Custom menu-items in the "Server menu"

You can add a maximum of 20 custom menu-items and menu separators to the server menu, linking to locations or external programs (Separators excluded, they group menu-items). The custom menu-items are accessible from the server menu and the toolbar as a popup menu. The internal browser is used to open links to locations and external programs are directly executed using a shell.




Custom menu-items in the "Toolbar popup"

Click on the "Custom menu" toolbar  to open the "Toolbar popup" menu and click on the "Edit..." menu-item to add or change custom menu-items.

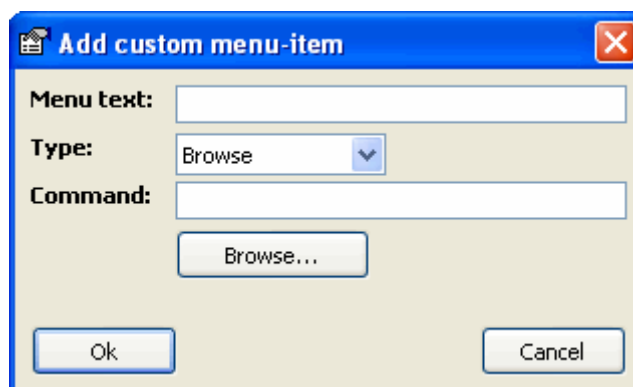


The "Custom menu-items" dialog

ADDING SHORTCUTS

Click on the "New shortcut" toolbar () button to add a new item or separator. Enter the menu-text and select the type of menu-item and the location of the file to open. If you select type "Browse" you must specify a file that resides inside the virtual file system. If you select type "Shell" you must type the name in the command textbox of an executable or a file that is associated with an executable on your hard disk(s). In both cases you can select a file or location by clicking the "Browse" button to open the associated "Select a ..." dialog.

You don't have to enter a menu-text or command value if you select a "Separator" type. All fields must contain a valid values if you selected a "Browse" or "Shell" type command before you can save the menu-item. Click on the "Ok" button to save the menu-item or click on "Cancel" to cancel the addition.



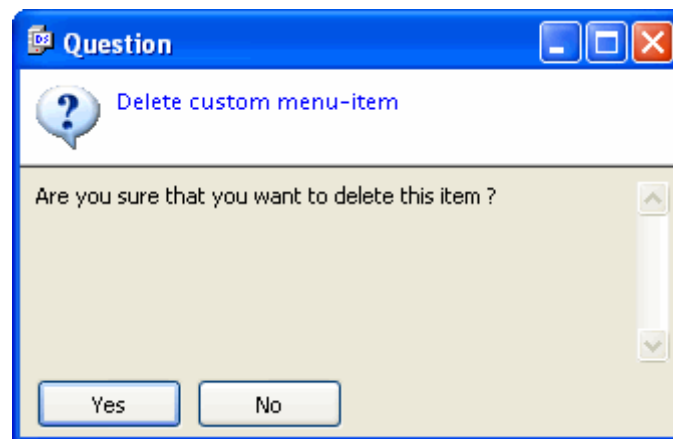
"Add custom menu-item" dialog

EDITING SHORTCUTS

Select a menu-item from the list in the "Custom menu-items" dialog and click the "Shortcut properties" toolbar button (📄) or double click the selected item to open it's properties. Change the settings of the menu-item and click the "Ok" button to save your changes or click "Cancel" to cancel your modification.

DELETING SHORTCUTS

Select a menu-item from the list in the "Custom menu-items" dialog and click the "Delete shortcut" toolbar button (🗑️) and confirm your action to delete the item from the menu.



"Confirmation dialog"

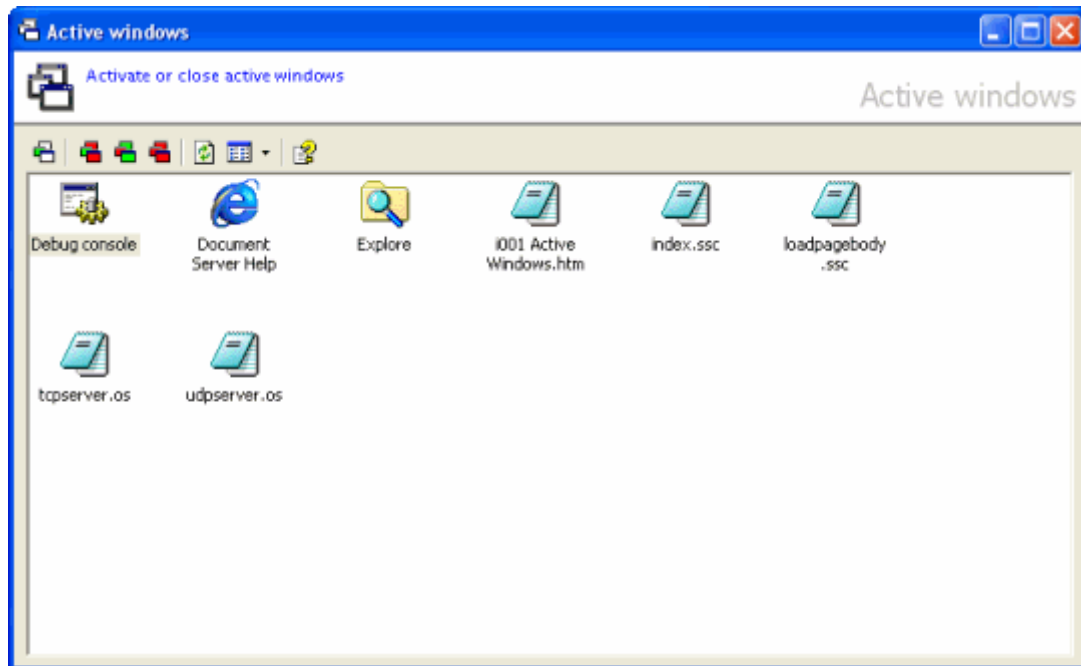
MOVING MENU-ITEMS

Click the "Move shortcut up" (↑) and "Move shortcut down" (↓) toolbar buttons to move items to another location in the list.

ACTIVE WINDOWS

While working in the IDE, a lot of windows may be opened (active windows). You may become 'lost' while searching for that particular script you were working on.

View a list of active windows where you can select a window based on its window icon. Click the "Active windows" toolbar button (📄) to open a list containing icons and descriptions of all active windows.



The "Active windows" window

SELECTING LIST MODE

The list has 2 views; "LARGE ICONS" and "DETAILS". Click on the "Display mode" toolbar button (📄) to select the mode you prefer.

SELECTING ACTIVE WINDOWS

To select a window to make it the topmost, double click the corresponding icon or select it by clicking on its corresponding icon (row in "Details" mode) and either press enter or click on the "Bring selected to front" toolbar button (📄). Click the "Close all but selected" toolbar button (📄) to close all active windows except the selected window. To close the selected window click the "Close selected" toolbar button (📄) and click the "Close all" toolbar button (📄) if you want to close all active windows at once.



REFRESHING THE LIST

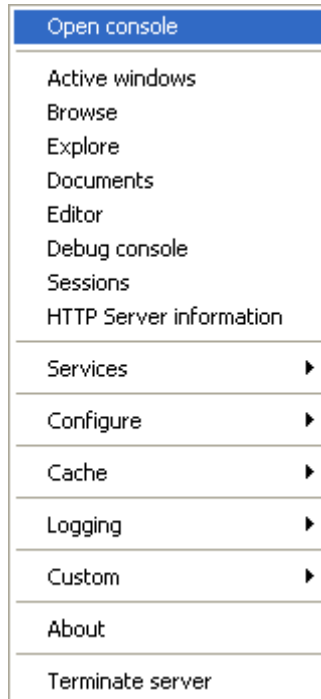
Because the "Active windows" window is not dynamically refreshing its list content when a application window is loaded into memory but refreshing the list content when the "Active windows" window receives the focus you may need to refresh the content of the list when you left the "Active windows" window open or when the "Active window" missed its queue. Click on the "Refresh" toolbar button (🔄) to refresh the content of the list.

SHORTCUT KEYS

Because you will most likely have many open windows when you're in **TYPING MODE** you may also press **Shift+Ctrl+F12** to open the "Active windows" window and **ESC** to close it again.

MINIMIZING TO THE SYSTEM-TRAY

Click on the "Minimize to system-tray" toolbar button () to minimize the server to the system-tray. SL Server 4 will close all windows preceding this action. When you click on SL Server 4's icon () in the system tray the "Server" menu will popup where you can select a server function. Clicking on the "Open console" menu item will restore the main-window of SL Server 4.



The "Server" menu

Sometimes it will happen that server menu will not close when clicking outside the menu area. If that happens click on a menu-item that has a submenu (Menu item "Services" for example) and click outside the menu area again to close the popup.

LOG ON / LOG OFF MODES

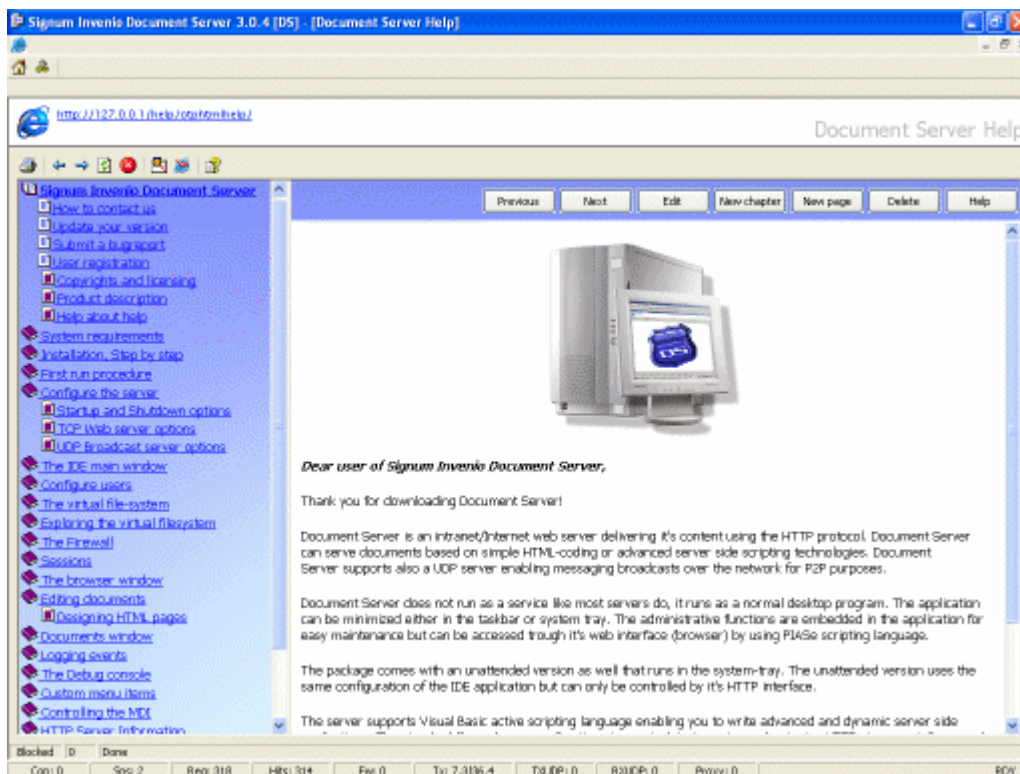
Depending the "[ConsoleLoginRequired](#)" and "[EndUserMode](#)" configuration setting, you need to logon when choosing a MDI function that requires a logon or when you click on the "Logon administrator" toolbar button (👤). To logoff the administrator click on the "Lock application" toolbar button (🔒).

CONSOLELOGINREQUIRED

When this parameter is checked (see [Startup/Shutdown options](#) > [ConsoleLoginRequired](#)) a logon is required when you want to access initially the MDI. Note that the application is able to start with or without checking this setting.


ENDUSERMODE

When this parameter is checked (see [Startup/Shutdown options](#) > [EndUserMode](#)), all toolbar buttons except the "Open the homepage" (🏠) and "Logon administrator" (👤) toolbar buttons will be hidden including the server menu. The default homepage will be shown using the internal browser window. In this state a user can work with a script application without access to the maintenance of the IDE application unless a valid logon is established.



"End-user mode"

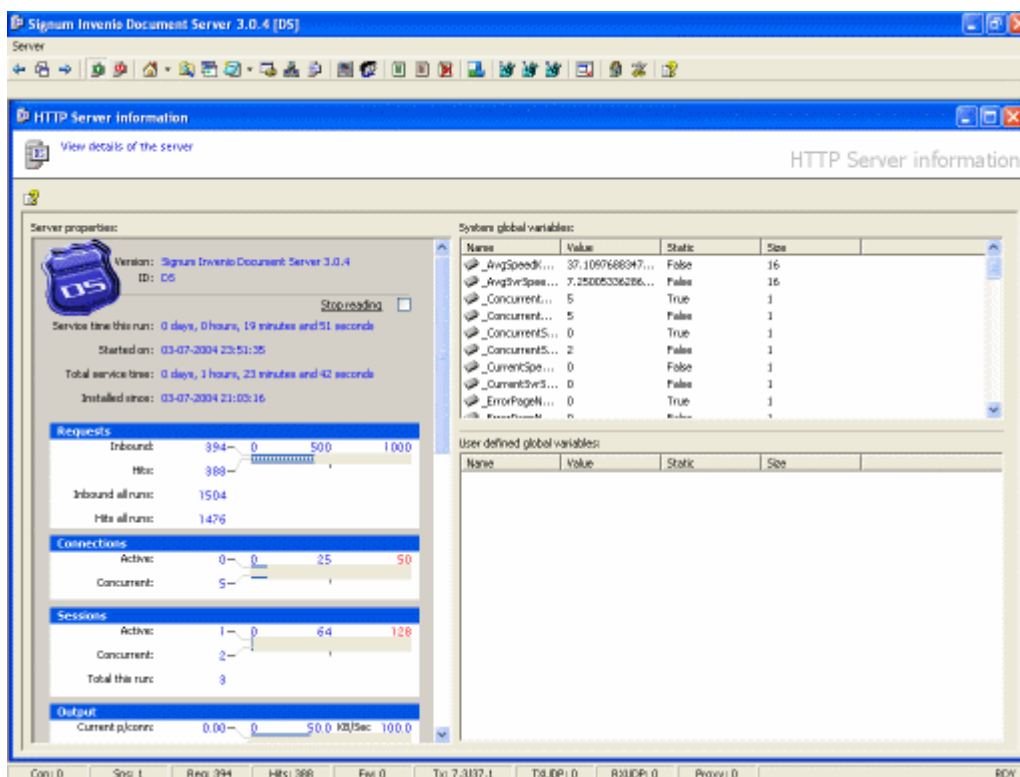
HTTP SERVER INFORMATION

Click on the "HTTP Server information" toolbar button () or select the "HTTP Server information" menu item from the server menu to open the "HTTP Server information" window.

The HTTP Server information window displays running properties of the server and its global memory usage. The window is divided in three panels. The left panel shows you the server properties and the right panels shows you the system global variables and user defined global variables currently in use. Global variables can be retrieved using PIASc script.

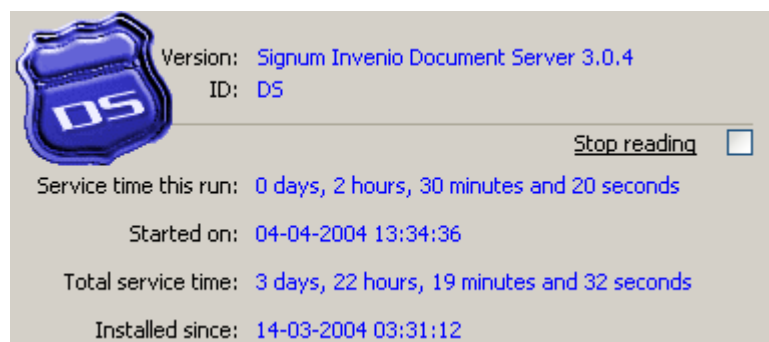
The system is updating the parameters every second and may cause a drop in server performance.

The panels can be sized by moving the mouse over the bars that separates the panels from each other and drag to size the panels to a more suitable width and height.



The "HTTP Server information window"

SERVER PROPERTIES

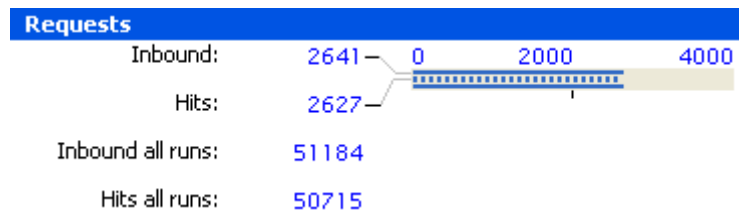


The header of the server properties report shows you the product name and version number, the server ID, the elapsed time since the run was started, the total elapsed (run) time and the date the service was installed on your system.

When you need to read the "now" situation you may need to stop the reading of status data by checking the "Stop reading" checkbox.

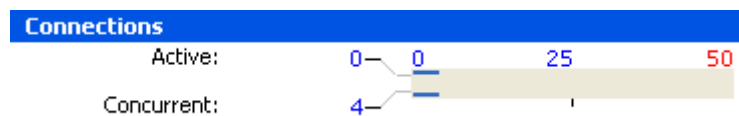
The loggers indicate a starting scale that changes when values exceed the maximum or getting below the minimum.

Requests



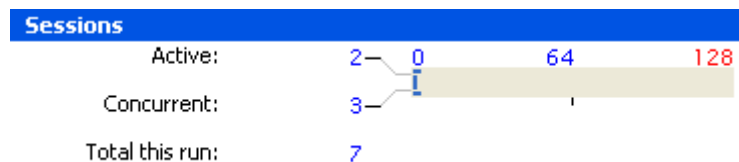
The requests section displays the number of incoming requests (outer bar - thick line) and the number of returned resources other than redirections (inner bar - dotted). The "all runs" values represent the cumulative inbounds and hit values since the installation date of the server.

Connections



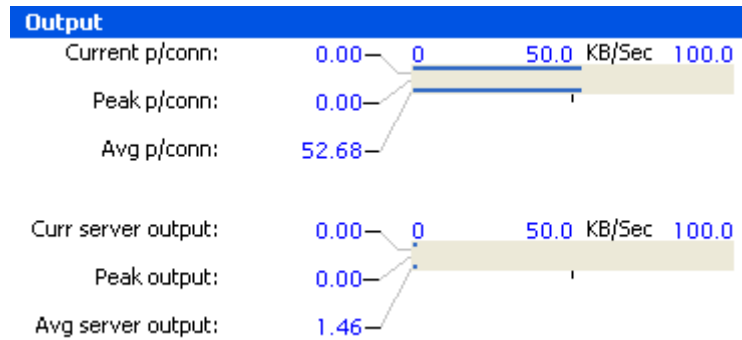
The connections section displays the active connections (inner bar - thick line) and the concurrent number of connections (outer bar - thin line) during the server run. A client may establish more than one connection at the same time. This will mostly happen when a page contains frames or images. Pages with much graphical detail can consume up to 40 connections and you may consider to increase the maximum connection count or remove some images from the such a page.

Sessions



The sessions section displays the number of active sessions (inner bar - thick line), the concurrent number of sessions (outer bar - thin line) during the server run and the total sessions this run. A session is a series of connections made by the same client within the TTL (time-to-live) timeframe. When the TTL time expires by means of a countdown, the session will be destroyed including all session variables and the server will create a new session when the client is connecting again.

Speed

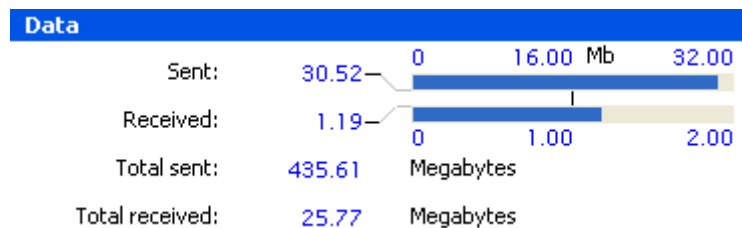


The upper part of output section displays the (est.) current speed per connection (middle bar - thin line), the fallback peak meter of the current speed per client (inner dotted bar) and the average current speed per client (outer bar - thick bar) in Kilobytes per second. The average speed per client is calculated over all current connections and indicates the bandwidth that is available to each connection currently downloading data.

The lower part shows you the current server output (middle bar - thin line), the fallback peak meter of the current server output (inner dotted bar) and the average server output (outer bar - thick line) in Kilobytes per second. The server output is calculated over periods of time between 1 and 30 seconds and may differ from the output of an average connection that is calculated during transferring time only.

Both meters may differ from speed reported by the Winsock's layer because of cache and packet balancing by the Windows operating system.

Data



The data section shows the number of megabytes sent (upper bar), received (lower bar) and total sent/received by the HTTP service. UDP packets are not recorded, only HTTP in and output is recorded. In future versions this window may contain UDP loggers as well.

Errors

Errors	This run	All runs
Server errors:	0	0
Bad requests:	0	8
Page not found:	0	134
Script errors:	0	27
Security errors:	0	0
Too many sessions CL:	0	0
Too many sessions SVR:	0	0
ID cookie rejected CL:	0	0
Proxy errors:	0	14

The error sections displays the various errors encountered this run and a cumulative count of errors encountered during the lifetime of the server.

Server error:

Errors that interrupted normal server operation inside the server engine (status code 500)

Bad requests:

Errors due to an invalid request header (non HTTP protocol)

Page not found:

Triggers when a resource could not be found (status code 404)

Script errors:

Runtime errors during a script execution

Security errors:

Triggered when sessions might be hijacked (Two or more IP addresses having the same session ID)

Too many sessions CL:

Triggers when a client is establishing too many sessions

Too many sessions SVR:

Triggers when the total number of sessions exceeds the maximum session count

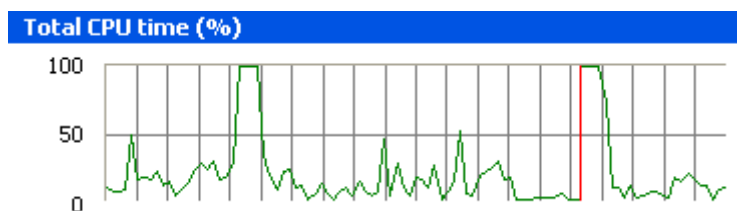
ID cookie rejected:

Triggers when a client does not accept cookies to maintain a session

Proxy error:

Errors triggered by the HTTP/Raw TCP proxy function

CPU MONITOR

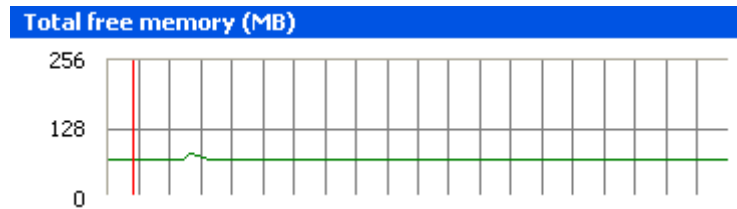


The CPU monitor indicates the current usage of the processor by all processes running on the system. When the pre-processor is compiling, CPU time will top the maximum level and is considered to be normal. When regular usage of SL Server 4 causes continues maximum levels you might need a faster processor or remove other processes (check your system tray) from memory.

Many system-tray programs use a lot of resource. For example, The Phillips Jack Rabbit CDROM burner comes with a tiny tool that is checking if you have pressed the so called "Blue button" of the burner and if so, all kinds of commercial Popup's and webpage's fly around over the desktop. This tool poll's constantly the USB port sucking up all processor time available and is an example of very, very, very bad multitasking programming. Mostly, these tools are written by inexperienced programmers getting in a state of 'celebration' when they

finally got the icon in the system tray but forgot all about their running wild polling-for-something loop causing the core to a near meltdown state...

MEMORY MONITOR




The memory monitor indicates the current number of megabytes still free to the system. If this line is reaching the zero line, Windows must release memory by paging it to the windows swap file. The writing to the windows swap file causes most definitely server performance flaw and high CPU peaks.

SYSTEM GLOBAL VARIABLES

Name	Value	Static	Size
_AvgSpeedKBperSecond	51.6833694000546	False	16
_AvgSvrSpeedKBperSecond	10.7699697071045	False	17
_ConcurrentConnectionsAllRuns	6	True	1
_ConcurrentConnectionsThisRun	4	False	1
_ConcurrentSessionsAllRuns	0	True	1
_ConcurrentSessionsThisRun	3	False	1
_CurrentSpeedKBperSecond	0	False	1
_CurrentSvrSpeedKBperSecond	0	False	1
_ErrorPageNotFoundAllRuns	134	True	3
_ErrorPageNotFoundThisRun	0	False	1
_ErrorProxyAllRuns	14	True	2
_ErrorProxyThisRun	0	False	1
_ErrorScriptExecAllRuns	27	True	2
_ErrorScriptExecThisRun	0	False	1
_ErrorServer500AllRuns	0	True	1
_ErrorServer500ThisRun	0	False	1
_ErrorTooManySessionsAllRuns	0	True	1
_ErrorTooManySessionsThisRun	0	False	1
_ErrorTotalBadHttpRequestsAllRuns	8	True	1
ErrorTotalBadHttpRequestsThisRun	0	False	1

This type of variable (variant) is in use by the server to record it's performance and other statistics. Global variables can be static meaning that the values of static variables are stored on disk when the server terminates and are reloaded when the server is started again. Global variables are available to the PIASE script engine and can be modified. Global variable names have an underscore prefix.

USER DEFINED GLOBAL VARIABLES

Name	Value	Static	Size	
 radm_costs	99	True	2	

This type of variable has the same properties as a system global variable and are maintained in the same memory space. Programmers can use a user defined global variable for PIASe applications that must exchange information across sessions or if static, even across server runs (configuration settings for example). When the status page of the RADM application has been opened once, a static global variable named "radm_costs" is created to remember the total cost value that is used to calculate average costs per session, megabyte, etc. It is not advised to use the global memory space as a database.

VIEW A SNAPSHOT OF A VARIABLE

A zoom window opens when you double click a system or user variable. The value(s) shown in the zoom window represents a snapshot of the selected variable and will not be updated.

SECURITY NOTES

IF YOU CHOSE BASIC AUTHENTICATION (BASE64)

User and password credentials are sent using the Base64 encoded format. Base64 is decoded easily using codec's widely available on the internet.

The Base64 authentication method is NOT RECOMMENDED !

It is not advised to transmit the user or administrator credentials over a non-private network using the Base64 authentication method. We advise you to use the RSA MD5 authentication method and use a secure tunnel connection (VPN) between two node's when clients need to connect and authenticate via the internet.

If you have chosen for RSA MD5 authentication a login is considered secure. MD5 does not transfer the password to the server like Basic authentication does and therefore preventing the 'snooping' of a password by the 'man in the middle'.

See also the "**MD5AuthLogin**" TCP configuration field to set the correct method of authentication.

NO SSL

SL Server 4 is not handling SSL certificates and therefore not encrypting pages. However, SL Server 4 has a collection of PIASe functions that can encrypt information based on RSA MD5 hashing to enable you to encrypt critical information based on your own methods whereas the client side must decrypt the information using JavaScript or other client side script languages.

AUTHENTICATION LOCKOUT

When a client is failing more than 50 times to logon correctly, SL Server 4 will stop authenticating the specific client. The browser logon window still appears to the 'failing' client but the result will be a no-go even if the client authenticates correctly. The server assumes a brute force logon when a client is exceeding 50 failed logon attempts and will stop authenticating without giving the client any clues about the server-side denial of service.

