

# OutsideView Users Guide

© 2023 Crystal Point, Inc.



The future. We'll be there.™

# Table of Contents

Foreword	0
<b>Part I OutsideView Users Guide</b>	<b>6</b>
<b>Part II What's new in OutsideView 9.1?</b>	<b>6</b>
<b>Part III Version Compatibility</b>	<b>6</b>
<b>Part IV Asian Usage Notes</b>	<b>7</b>
<b>Part V Configuring OutsideView</b>	<b>7</b>
1 Converting Evaluation licenses.....	7
2 Individual OutsideView Installation.....	8
3 Quick Start.....	8
4 Application Look.....	9
5 Default Application Settings.....	9
Directories tab .....	10
Settings tab .....	10
Context Recognition .....	11
File Transfer tab .....	11
Session Bar tab .....	13
Dynamic Input Assistance .....	16
Auto Login tab .....	17
Auto Connect tab .....	18
New Session tab .....	18
Miscellaneous tab .....	19
Session Bar .....	21
Workspaces .....	24
Individual Workspace Settings.....	25
Session Bar Filter .....	26
Session Activation Control.....	31
Session Bar Color Coding for Status.....	32
Status Bar .....	33
Toolbars .....	33
6 Session and Workspace Overview.....	34
7 Creating New Sessions.....	35
8 Session Settings.....	36
Session Category .....	36
Identity Caching .....	38
Emulation Category .....	40
I/O Category .....	42
Protocol Category .....	42
Display Category .....	43
Colors Category .....	45
Keyboard Map Category .....	46

Capture Category .....	47
Macro Toolbar Category .....	48
<b>9 Keyboard Mapping.....</b>	<b>49</b>
About Keyboard Mapping .....	49
Mapping Terminal Functions .....	50
Mapping Key Sequences.....	50
Mapping Macros .....	51
<b>10 Toolbars.....</b>	<b>51</b>
Toolbar Overview .....	51
Default Toolbar Icons .....	53
Customizing Toolbars .....	53
Reset Toolbars .....	55
Changing Icon images .....	55
Macro Toolbar .....	58
<b>11 Dynamic Input Assistance.....</b>	<b>60</b>
Overview .....	60
Quickly Changing your Dynamic Input Assistance Mode .....	61
Configuring Dynamic Input Assistance Defaults .....	62
Dynamic Input Assistance - Main Settings.....	62
Dynamic Input Assistance - Cmd History.....	64
Dynamic Input Assistance - Spell Checking.....	67
Dynamic Input Assistance- Command Auto-completion Assistance.....	70
<b>12 Context Recognition.....</b>	<b>70</b>
Creating New Contexts .....	71
Editing Contexts .....	72
Editing Context List .....	73
Context-Sensitive Toolbars .....	75
<b>13 Identity Management.....</b>	<b>77</b>
Simple Logons .....	78
Multiple Logon Screens .....	79
Complex Multiple Formatted Logon Screens .....	81
Example; Multiple Formatted Logon Screens .....	84
RE-activating Identity Manager .....	92
<b>14 Security.....</b>	<b>93</b>
Security Overview .....	93
SSH Security .....	93
ID Management and SSH.....	93
SSH I/O .....	95
SSH Certificates .....	101
Adding user-generated key file to NonStop hosts.....	103
SSH access for Cloud Computing.....	106
Converting SSH keys to SSH2.....	107
SSH Encryption Algorithms.....	109
SSL Encryption .....	109
SSL Server Authentication.....	109
Advanced Certificate/Encryption Options.....	111
Importing Root CA Certificates.....	113
<b>Part VI Using OutsideView .....</b>	<b>118</b>
<b>1 OutsideView UI Overview.....</b>	<b>118</b>
<b>2 Session Settings Password.....</b>	<b>119</b>

<b>3</b>	<b>Working with Tabbed Group Windows.....</b>	<b>121</b>
<b>4</b>	<b>IPV6.....</b>	<b>125</b>
<b>5</b>	<b>Dynamic Windows Area.....</b>	<b>125</b>
<b>6</b>	<b>Application Message Log.....</b>	<b>125</b>
<b>7</b>	<b>Right-Click Option.....</b>	<b>126</b>
<b>8</b>	<b>Printing.....</b>	<b>128</b>
<b>9</b>	<b>Copy/Paste.....</b>	<b>128</b>
<b>10</b>	<b>Searching Buffers.....</b>	<b>128</b>
<b>11</b>	<b>National Character Set Support.....</b>	<b>129</b>
<b>12</b>	<b>Logging Session Activity.....</b>	<b>130</b>
<b>13</b>	<b>Command Line Options.....</b>	<b>131</b>
<b>14</b>	<b>Guardian File System Graphical Navigation.....</b>	<b>132</b>
<b>15</b>	<b>Session Bar Color Coding for Status.....</b>	<b>134</b>
<b>16</b>	<b>Session Bar Filter.....</b>	<b>134</b>
<b>17</b>	<b>Session Activation Control.....</b>	<b>140</b>
<b>18</b>	<b>Smart Docking.....</b>	<b>141</b>
<b>19</b>	<b>File Transfer.....</b>	<b>142</b>
	<b>SFTP (&amp; FTP) file transfer .....</b>	<b>142</b>
	Guardian Operating System Notes.....	142
	Configuring File Transfer Defaults.....	147
	Creating an SFTP file transfer session.....	148
	Creating an SSL-secured file transfer session.....	154
	Creating a new FTP file transfer session.....	158
	Saving a File Transfer Connection.....	160
	Opening Previously-defined SFTP connection files.....	160
	Using a File Transfer connection.....	161
	Uploading Files .....	163
	Downloading Files .....	168
	File Transfer, Imbedded Editor.....	169
	Edit Monitor .....	170
	Host-to-Host file transfers.....	171
	Multiple Host file transfers.....	171
	Modifying a File Transfer Connection.....	172
	File Transfer Progress.....	172
	"Classic" FTP .....	173
	Invoking "Classic" FTP .....	173
	Classic FTP Settings .....	176
	Classic FTP Command Mode.....	178
	Classic FTP Dialog Interface.....	179
	Transferring Files in Classic FTP.....	181
	Classic FTP Trace .....	182
	<b>IXF .....</b>	<b>182</b>
	IXF Receive .....	183
	IXF Send .....	184
<b>20</b>	<b>HTML Tunnel.....</b>	<b>185</b>
	<b>ID Management and HTML Tunnel .....</b>	<b>185</b>
	<b>Configuring HTML Tunnel .....</b>	<b>186</b>



<b>21</b>	<b>Macros.....</b>	<b>188</b>
	Macro Editor .....	188
	Running Macros .....	188
	View Macro Status .....	189
<b>22</b>	<b>OV Automated Error Reporting.....</b>	<b>189</b>
	Bug Report Wizard .....	189
	Report submission Process .....	203
	Optional Directory Settings .....	208
	MFC Support .....	209
 <b>Part VII Troubleshooting</b>		 <b>209</b>
<b>1</b>	<b>OutsideView File Locations.....</b>	<b>209</b>
<b>2</b>	<b>UTF-8 Support.....</b>	<b>210</b>
<b>3</b>	<b>Recovering Unavailable Components.....</b>	<b>211</b>
<b>4</b>	<b>Pre-Compilation of .Net components .....</b>	<b>212</b>
<b>5</b>	<b>Diagnostic Traces.....</b>	<b>213</b>
<b>6</b>	<b>Extended Diagnostics for Auto Login.....</b>	<b>214</b>
<b>7</b>	<b>Additonal Tracing Capabilities.....</b>	<b>214</b>
<b>8</b>	<b>Contacting Support.....</b>	<b>214</b>
 <b>Index</b>		 <b>215</b>

# 1 OutsideView Users Guide

## OutsideView Users Guide

Welcome to the OutsideView Users Guide. This guide provides individual users with assistance in **configuring and using** OutsideView.

- A good starting point for learning to use OutsideView is the [OutsideView User Interface Overview](#).
- To create a new terminal emulation session to your host system, see the [Creating New Sessions](#) topic.
- For an overview of OutsideView terminal emulation sessions and workspaces, see the [Session and Workspace Overview](#) topic.

If you want information about installation, deployment and administration of OutsideView for multiple users, please see the **System Administrators Guide**.

For assistance creating or editing macros, please refer to the **Visual CommBASIC Reference**.

NonStop is a trademark of Hewlett-Packard Development Co.

# 2 What's new in OutsideView 9.1?

For the most complete comparison between OutsideView releases, go to our website <https://www.crystalpoint.com/products/outsideview-documentation> and select the link "Compare OutsideView Versions"

Here is a summary description of the new features in OutsideView 9.1:

Updated SSH Libraries - Enhanced security and latest ciphers

Updated Support Libraries - Support newest Windows versions

Support for Windows 11 - Support newest Windows versions

Support for Microsoft Server 2022 - Support newest Windows Server versions

Support for SQL Server 2022 - Support newest SQL Server Versions

Support for FTP/STP for Single User Passwords - Enhanced security

# 3 Version Compatibility

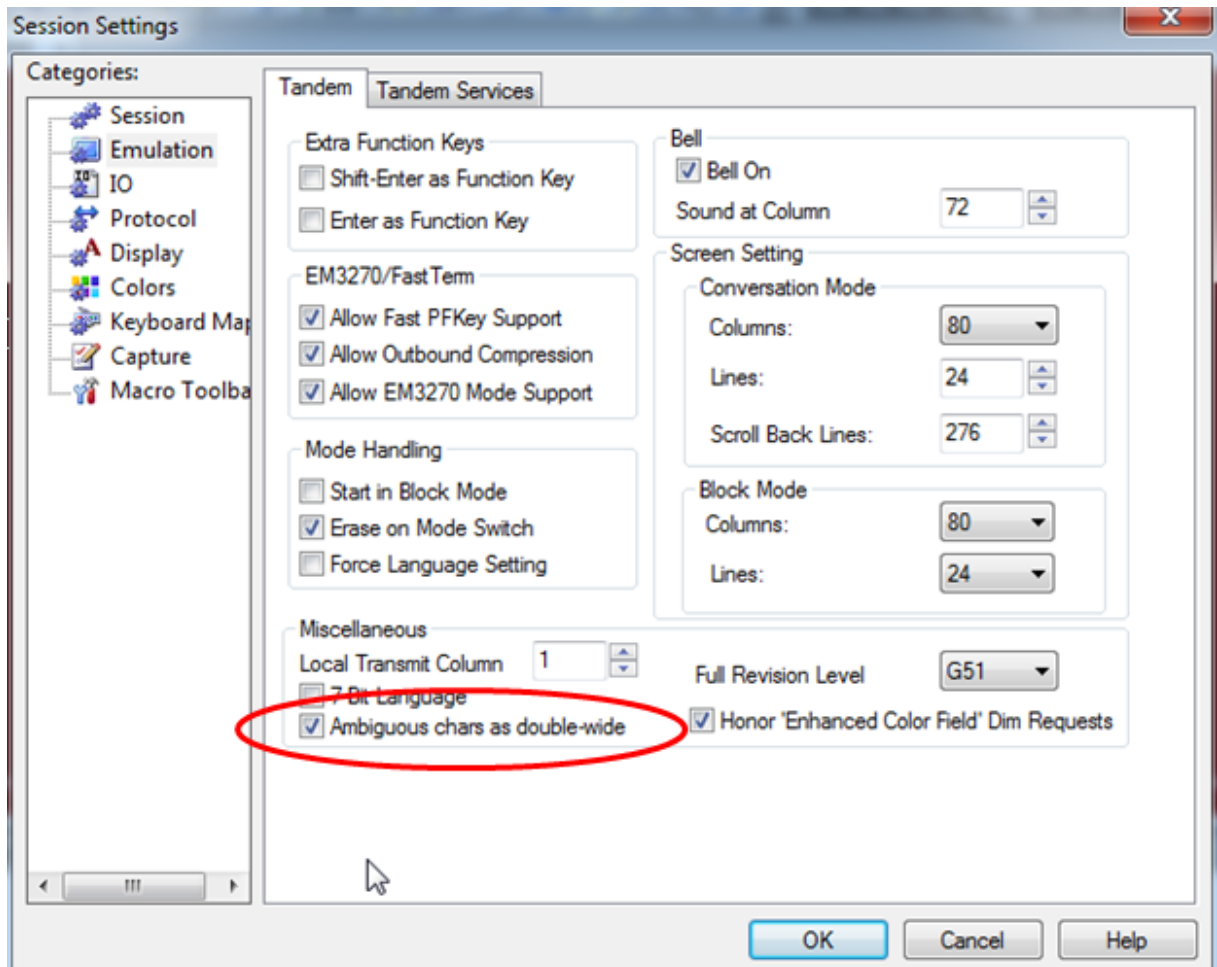
OutsideView will properly display workspaces, sessions, and other components such as color files, from OutsideView 8.2. However if you want the new "Fast Load" feature then user should re-save the sessions in OutsideView 9.1.

If you are coming from 8.1 or earlier, it is recommended that users recreate their session and workspace files to acquire new capabilities that are not present in these earlier versions.

## 4 Asian Usage Notes

When OutsideView is used with Japanese fonts it is recommended that the settings switch "Ambiguous characters as Double-wide" be set to ON. For Chinese or Korean fonts, this setting should not usually be enabled.

This setting is accessed by opening or creating a session, selecting Session, Session Settings, and choosing the category "Emulation"



## 5 Configuring OutsideView

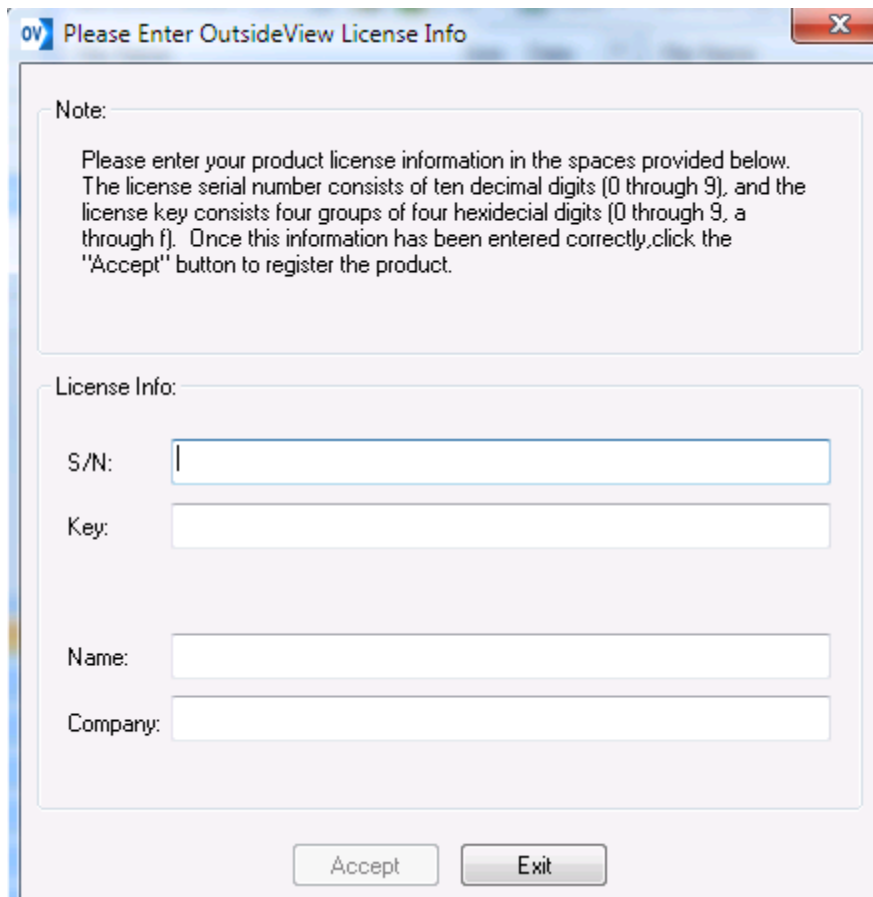
### 5.1 Converting Evaluation licenses

If you have been testing OutsideView in desktop or corporate mode using temporary (evaluation) licenses, we have made it easier to switch over to permanent (production) licenses.

1. Start OutsideView,
2. Select Help, About OutsideView

### 3. Select "Change Product License"

Enter your production license information to replace/update evaluation license information without having to reinstall.



ov Please Enter OutsideView License Info

Note:

Please enter your product license information in the spaces provided below. The license serial number consists of ten decimal digits (0 through 9), and the license key consists four groups of four hexadecimal digits (0 through 9, a through f). Once this information has been entered correctly, click the "Accept" button to register the product.

License Info:

S/N:

Key:

Name:

Company:

Accept Exit

## 5.2 Individual OutsideView Installation

### Desktop installation of OutsideView

To install a single copy of OutsideView requires a serial number (such as 91010 00043 30) and key (such as 6335-nab7-06da-061e-18), and administrative rights (or capability to "Run as Admin") on the PC.

With these requirements met, simply locate the installation media, navigate to the folder "OutsideView", and click on the executable file OutsideViewSetup, and follow the prompts.

For information about installation, deployment and administration of OutsideView for multiple users, please see the **System Administrators Guide**.

## 5.3 Quick Start

To create a basic NonStop 6530 telnet session, simply start OutsideView, select File, New Session, provide the host IP address or DNS name and select OK. That's all it takes! Once you confirm you

are communicating correctly, then select File, Save Session As, to create a session (.cps) file of whatever name you prefer.

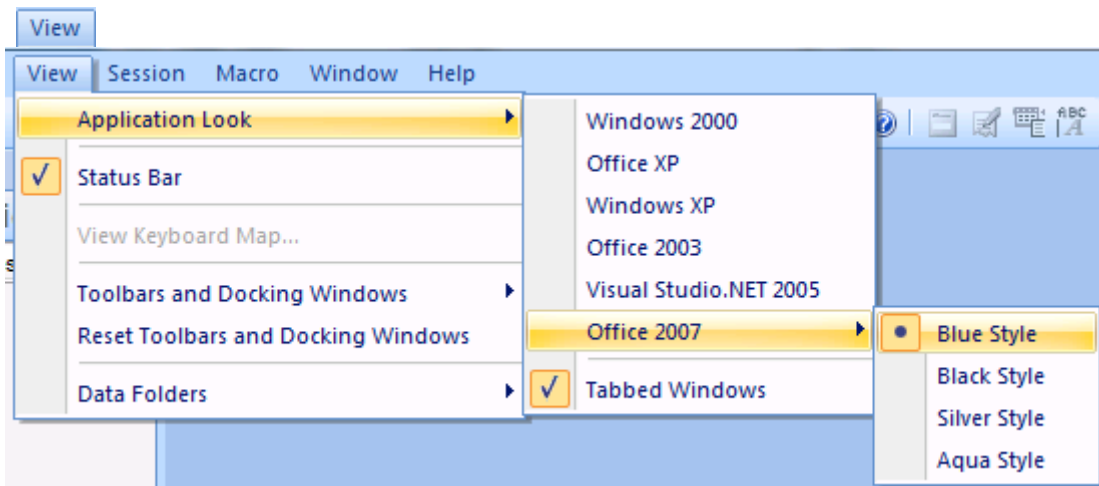
For further information on configuring individual sessions , see [Session Settings](#)

For information about groups of sessions, see [Workspaces](#)

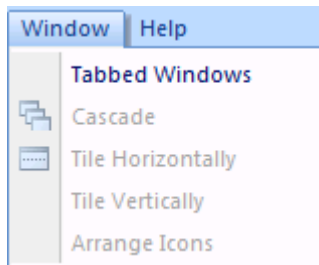
For information on configuring the overall behavior of OutsideView, see [Application Settings](#)

## 5.4 Application Look

Select View | Application Look to choose the overall appearance or 'look' of OutsideView, and to choose whether to have a Tabbed, Cascaded, or Tiled view of your sessions. The default value is "Tabbed Windows"



The Tiled and Cascade options are configurable from the Window menu option when the Tabbed Windows option is unchecked:



## 5.5 Default Application Settings

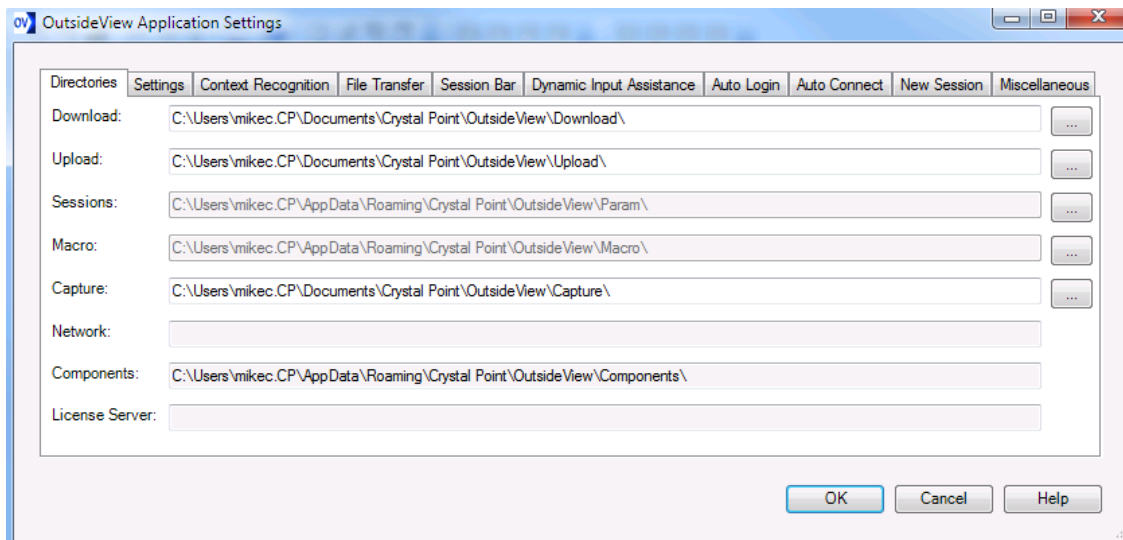
OutsideView is an application for communicating with NonStop and other host systems.

Before considering how individual connectivity sessions should behave, it's helpful to know how to tune OutsideView's overall operation to your preferences. To do that, Start OutsideView, and then select **Edit | Default Application Settings** from the menu bar. Changes made here affect **default**

behaviors of the application, and its workspaces. Click here to see how to [configure individual workspaces](#).

### 5.5.1 Directories tab

The **Directories** tab lets you see and modify the location of various files and components of OutsideView. For instance, you will notice the location for Upload, Download and Capture files are located in your Documents area, while the various configuration files are located in your personal application data area. You can also click on the ellipses button on the side of the text box and that will bring up a folder browser so that you can easily change the location of these settings.

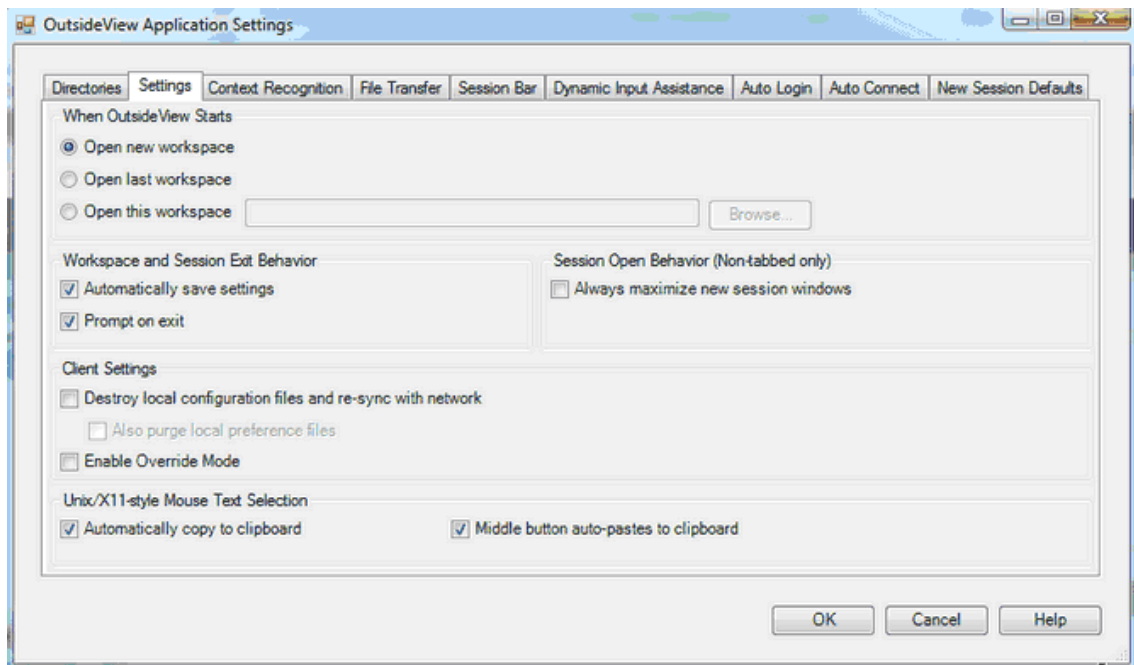


### 5.5.2 Settings tab

#### Settings tab

[Top](#) [Previous](#) [Next](#)

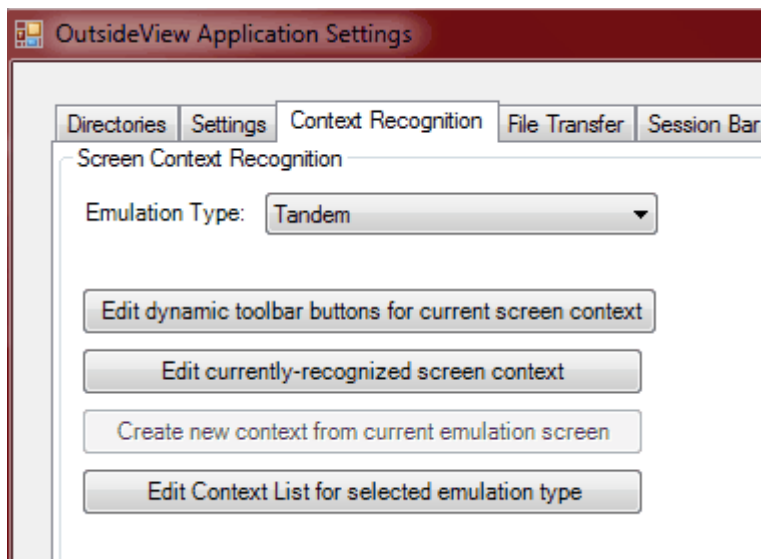
The **Settings** tab lets you choose the startup and exit behaviors of OutsideView. For instance, you may choose to turn off the prompt to save changes, or the Prompt on Exit of OutsideView. Unix/X11-style Mouse Text selection, when on, means that highlighting any text 'loads' it for pasting.



The Unix/X11 mouse text selection is fairly new. If checked, then any text highlighted is automatically copied to the clipboard. Another option is to have clipboard content pasted to the cursor location simply by clicking the mouse roller wheel.

### 5.5.3 Context Recognition

This dialog permits editing the context recognition settings, and invocation of the Screen Visualizer. For detailed information, refer to [Context Recognition](#)



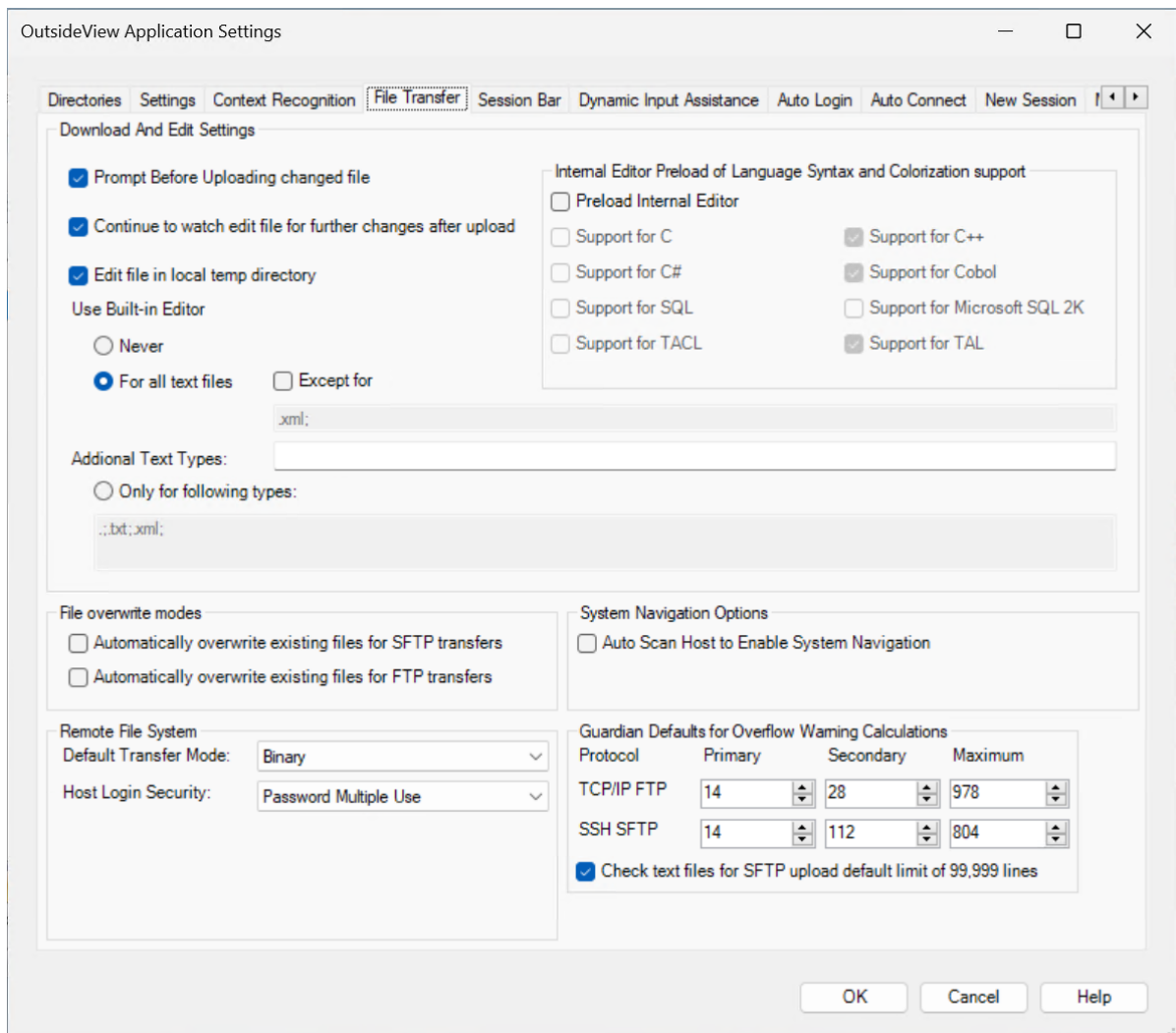
### 5.5.4 File Transfer tab

The **File Transfer** tab lets you fine tune the behavior when editing files you have transferred.

The Code Editor built into OutsideView consumes approximately 15 MB memory. The various code language syntaxes each require additional memory. SQL syntax requires the largest single amount, at about 40 MB. If the Code Editor and all syntaxes are loaded, the memory usage is 100+ MB.

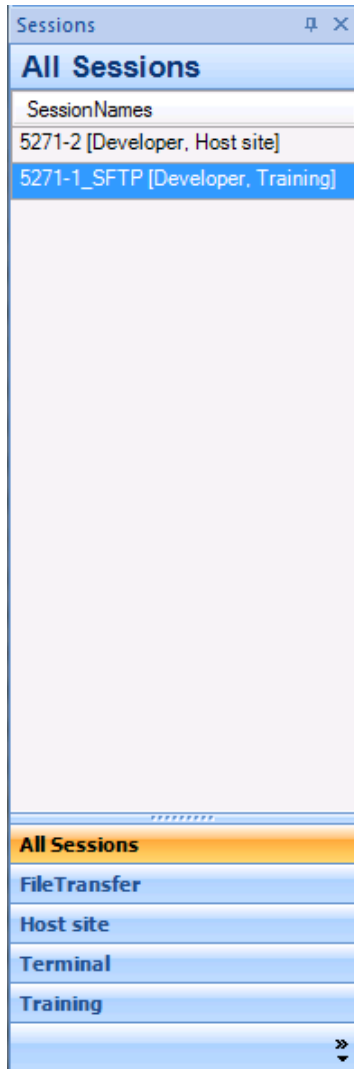
- Internal Editor Preload of Language Syntax -- by default, the Code Editor is pre-loaded into memory, along with selected syntaxes. If you are a developer, and use the builtin editor frequently, you may use this screen to have the editor pre-load only your preferred syntaxes/languages.
- System Navigations -- by default, OutsideView will scan your host file tree to enable host file navigation. If desired, you may disable this Auto-scan option.
- Guardian Systems Defaults for File Allocation Extents -- by default the FTP and SSH\SFTP protocols have a default allocation file size to prevent small files from consuming large amounts of disk space under the Guardian file system. Most companies simply go with the defaults; however, if the system administrator for your company has changed the defaults you would enter the new defaults in this dialog. These values are used when testing local file size to give you a visual indicator when files are too large to upload without changing the allocation extents when the file is created. It is also used by the right mouse click option in the local directory window to upload with attributes. This dialog give a graphic representation of the file allocation by the host, red indicating that it will error out during transfer. Note: To conserve space on the host, first adjust the secondary extent allocation value. If the file is expected to grow after uploading; adjust other extent values to enable the growth as needed. Check with your system administrator to see if these values have been adjusted for your site. Generally, these values are adjusted upwards to make it simpler for the users if lots of large file uploads are envisioned.





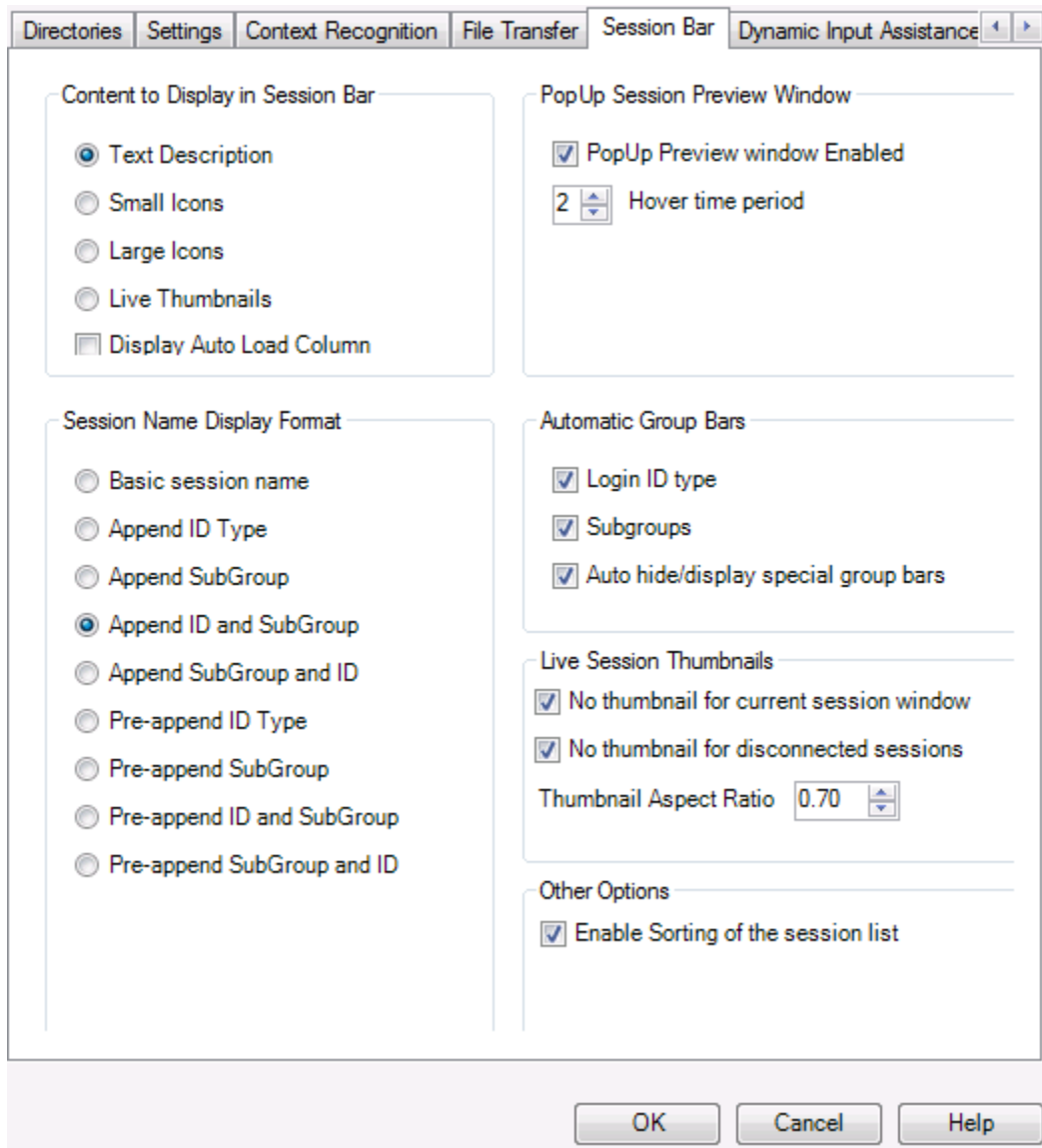
## 5.5.5 Session Bar tab

The **Session Bar** is the area on the left of the OutsideView screen:

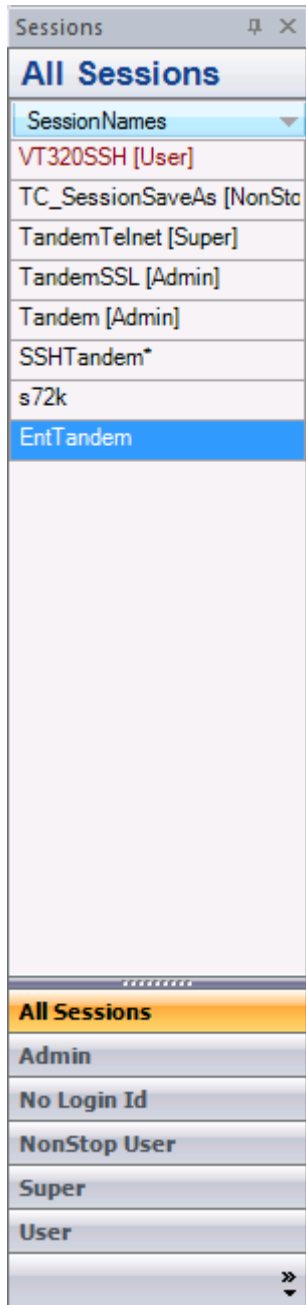


It lists your active sessions, including Host sessions, file transfer sessions, or editor sessions. This **Session Bar** tab lets you define how the Session Bar operates, by **default**. For instance, you may want live thumbnail views representing your active sessions rather than icons. Or, you might want to list icons, but have a live thumbnail preview popup if you hover your mouse over the session icon. When your sessions are listed in the session Bar, you may want them to be labeled with just the session name, with the session name and the ID Type for that session, or with session Name, ID Type and Subgroup.

**Hover Time Period** is a delay counter; when hovering your mouse anywhere within the session bar, before live thumbnail views will pop up. This delay is reset each time your mouse leaves the entire session bar area. So, to peruse multiple sequential thumbnail views, without waiting for the delay each time, keep your mouse within the Session bar frame.



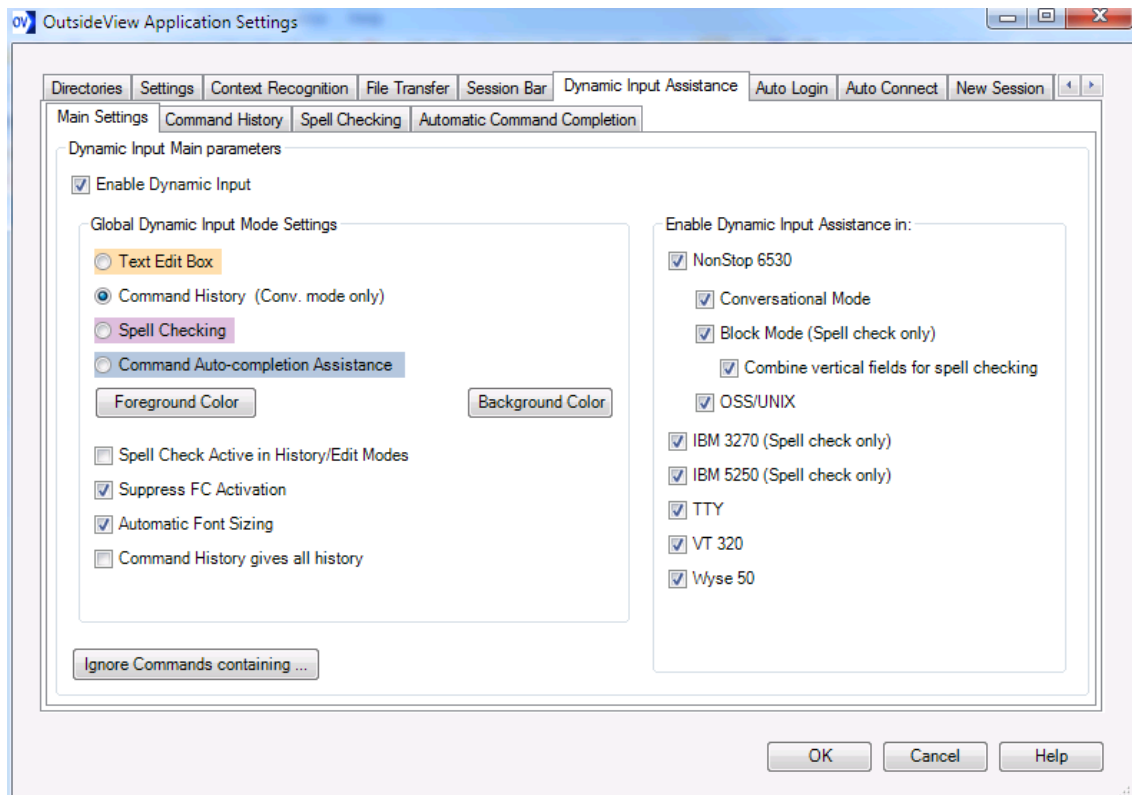
**Enable Sorting of the session list** allows the user to apply the alphabetical / reverse alphabetical sort onto the SessionBar list of sessions. You click on the SessionNames sort button to apply the sorting behavior to the sessions. You can still move the sessions around via drag and drop to change the order around (Note moving the sessions around will only work if the Session Filter is set to All Sessions).



### 5.5.6 Dynamic Input Assistance

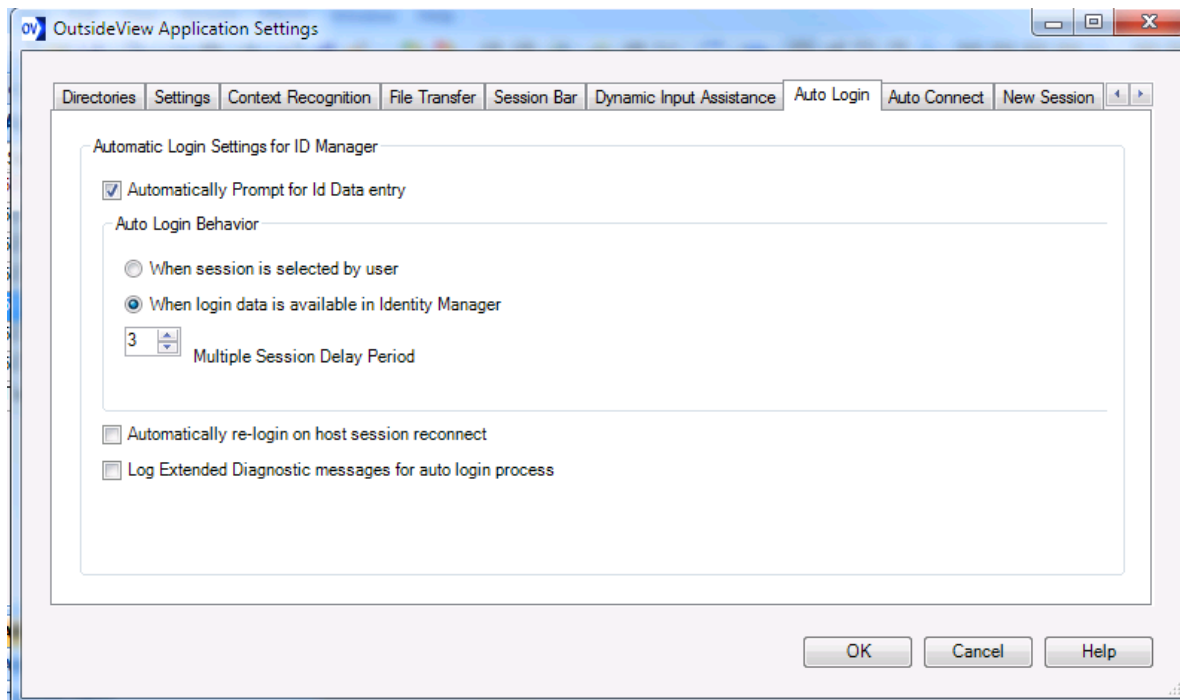
This is an area to access your settings for Dynamic Input Assistance. For more detailed information see

[Dynamic Input Assistance - Main Settings](#)



### 5.5.7 Auto Login tab

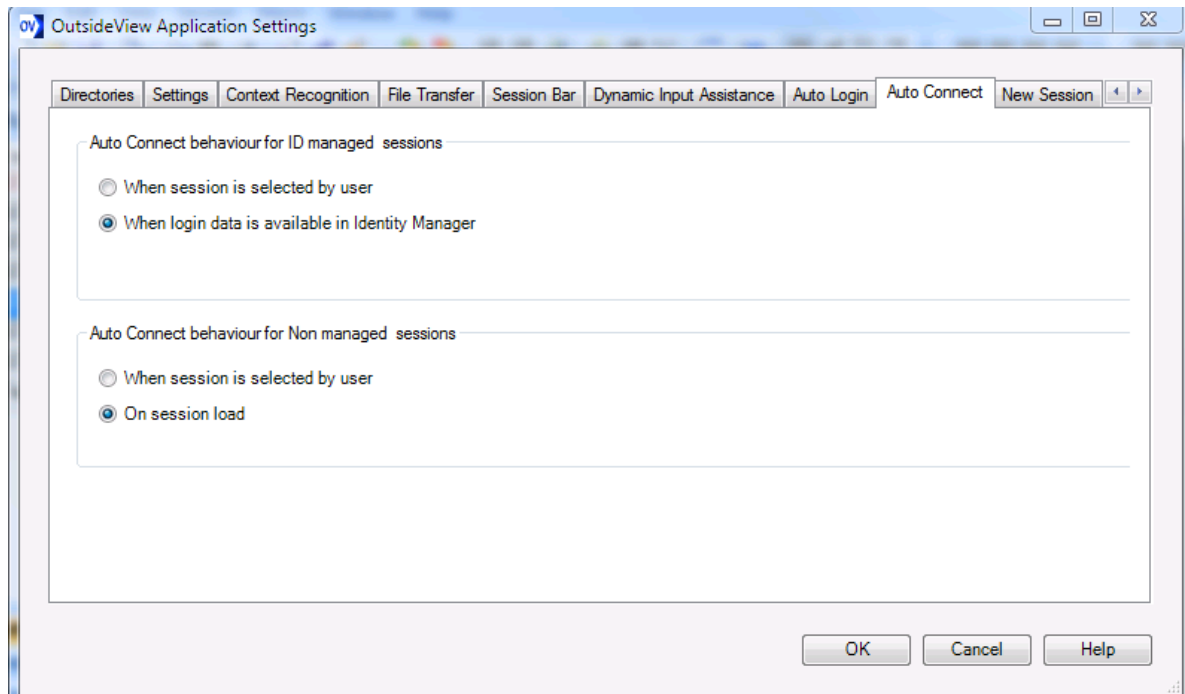
The **Auto Login** tab lets you define whether to prompt for User credentials, and when.



### 5.5.8 Auto Connect tab

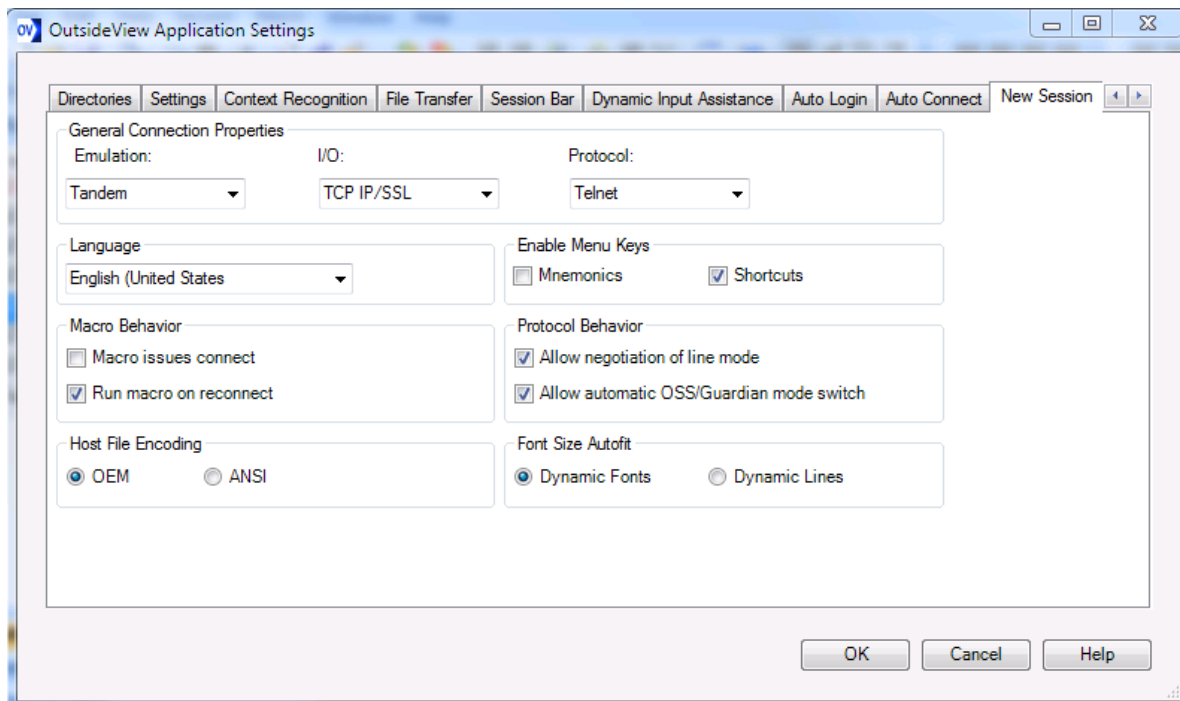
The **Auto Connect** tab lets you specify when sessions (with and without a defined ID Type) actually initiate communications with the host. A session could be open within OutsideView but not immediately communicate to the host.

For instance, you might want communications to the host to be initiated on session load, When session is selected (given focus) by the user, or when login data is available for the session.



### 5.5.9 New Session tab

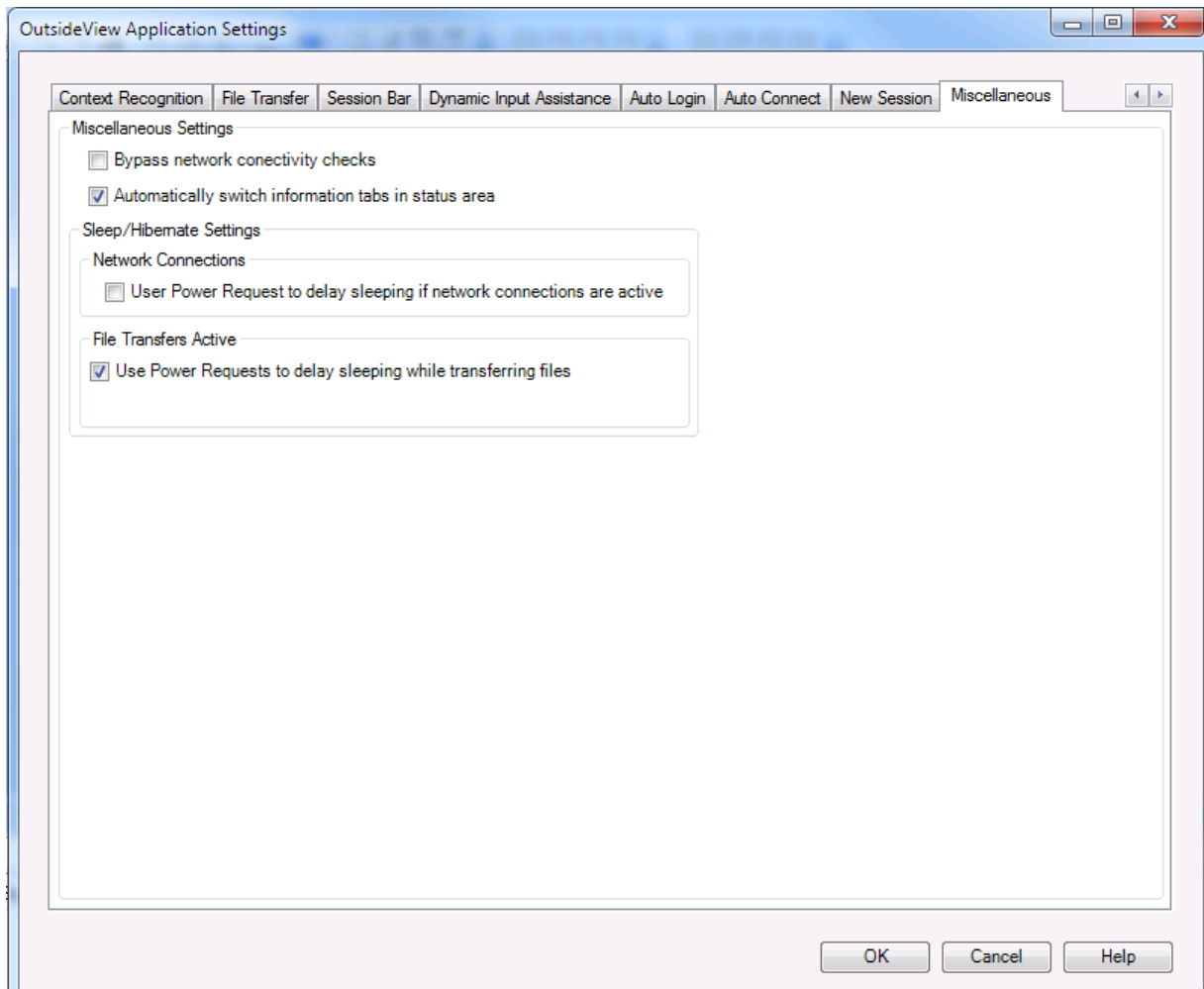
The **New Session** tab lets you modify default settings of sessions to be created in the future. This will not change the settings within any existing sessions.



## 5.5.10 Miscellaneous tab

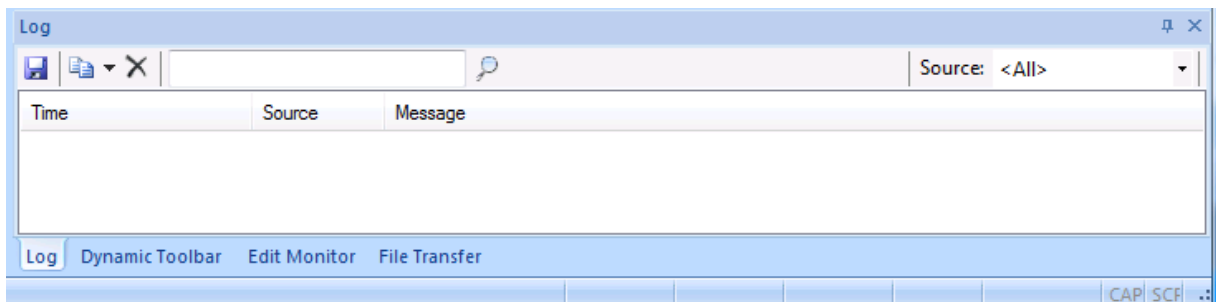
### Miscellaneous Settings

All settings within the Miscellaneous settings group box are saved in the workspace.



**Bypass network connectivity checks** - is a setting that enables OV to automatically monitor the network state of your PC. When working remotely it is a common mistake to not plug in the network cable, join a wireless network or start a VPN for work access. With this option enabled; OV will automatically attempt to connect unconnected sessions when there is a change in local network state.

**Automatically switch information tabs in status area** - enables or disables the status pane switching. When users are switching sessions, the status panes at the bottom of the window should reflect the current state of the active session. When the terminal session is not logged in, the the OV Log status pane is active. When the session is connected, the pane will switch to the dynamic toolbar. For a file transfer session, the active pane will switch to the transfer monitor status pane.





**Sleep Hibernate Settings** with OutsideView's ID Management functionality and network interface monitoring, it isn't much of an issue for the user if the PC is configured to go asleep as the sessions can be reconnected and automatically logged back into. However, ongoing file transfers are an exception to this criterion as they are not recoverable from a sleep event. The 2 check boxes for User Power Requests will open a system power request when network sessions are active. As for file transfer, each file transfer will issue power requests. Users can open a dos command window in Administrative mode and issue the command "PowerCfg /Requests" to see the requests for delaying sleep.

**Network Connections - User Power Request to delay sleeping if network connections are active** this option enables the user to prevent their PC from going to sleep if there are active network connections.

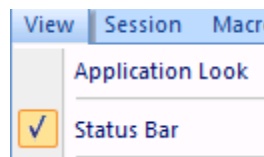
**File Transfer Active - User Power Requests to delay sleeping while transferring data** this option enables the user to prevent their PC from going to sleep if there is an active FTP session transferring data. By default this option is enabled for file transfer.

**Battery Power Mode Note:**

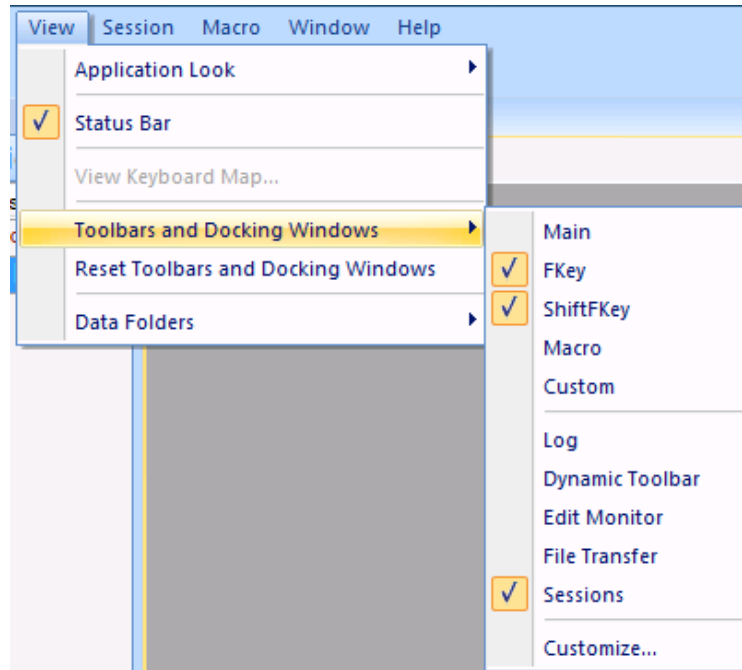
If the PC is running on battery power, the operating system enforces a five minute maximum delay by applications. OutsideView uses another technique to work around this limitation. Unfortunately there is an unavoidable side effect in that the screen on your laptop and tablet will not blank until the file transfers are finished.

### 5.5.11 Session Bar

To turn display of the Status bar on or off, select View, and then check the item on or off.

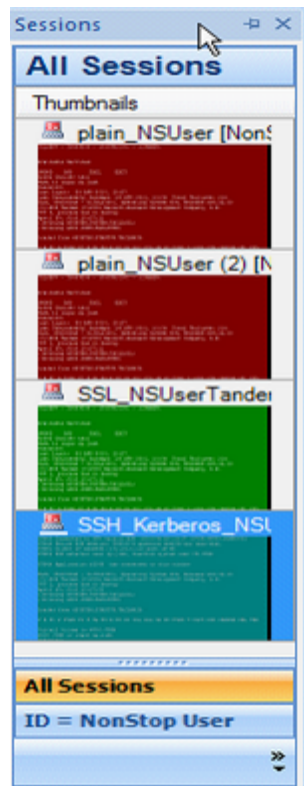


To turn the Session bar on or off, select View | Toolbars and Docking Windows | Sessions to check the item on or off.




These settings will be saved as part of your workspace settings.

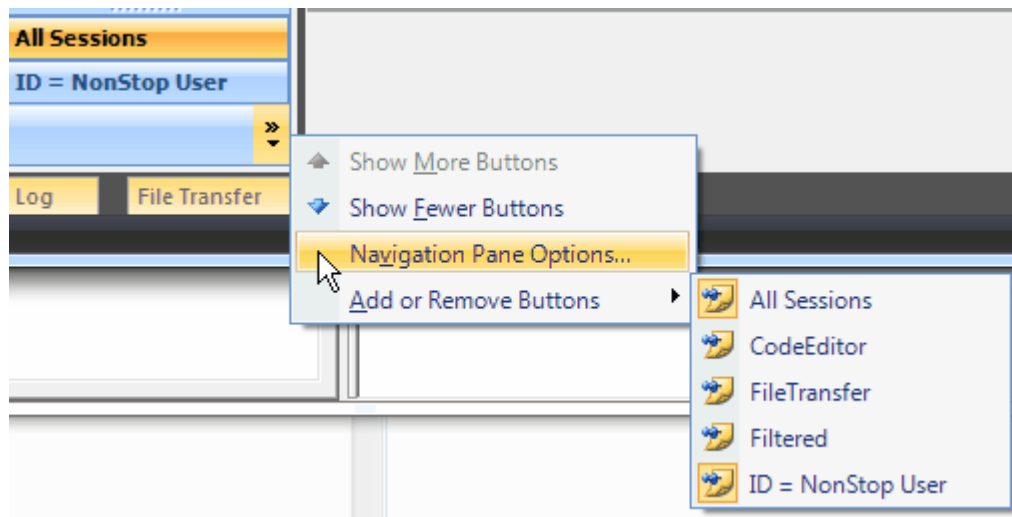
The Session Bar is the area to the left of the OutsideView window.



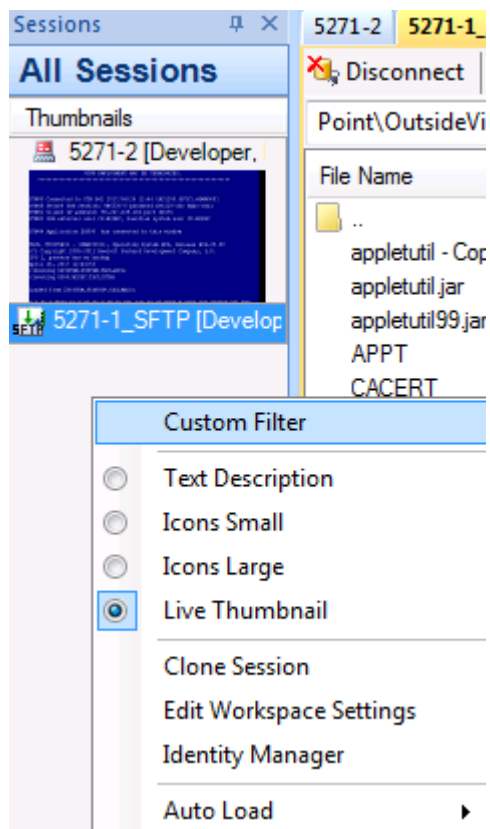
The Session Bar lists active emulation, file transfer, and edit sessions. It can be constantly displayed or in an auto-hide state. This is controlled by View | Toolbars and Docking Windows | Sessions, or by right-clicking on the session bar and toggling between the auto-hide or pinned state.

To select which Session groups display, users may click on the control at the bottom right of the

session bar.  This control lets you Add/Remove buttons or set Navigation pane options. The graphic below, for instance, shows the groups All Sessions and NonStop User to be visible. Clicking on others, such as File Transfer would activate those groups, too.




Another way to manipulate Session Bar behavior is by right-clicking on the Session Bar itself:



### 5.5.11.1 Workspaces

#### Workspaces

An OutsideView workspace defines a collection of sessions and how they are organized within the OutsideView application. You can organize your sessions to best suit your work requirements and save them as a workspace. To automatically re-open all those sessions at once, organized just the way you had them, simply open the workspace.

Under Edit | Workspace Settings, or the icon  users may define a startup macro to be executed when a workspace is opened.

Under Edit, Application Settings, user may define default workspace and application behavior

To modify behavior of an individual workspace, see the topic [Individual Workspace Settings](#)

To save a workspace:

1. Open all sessions you wish to be part of the workspace and organize them to best suit your needs.
2. Select File/Save Workspace As... to open the save dialog.
3. Enter a meaningful name for your workspace (e.g. MyHosts.cpw).
4. Click OK.

To open a saved workspace:

1. Select File | Open Workspace

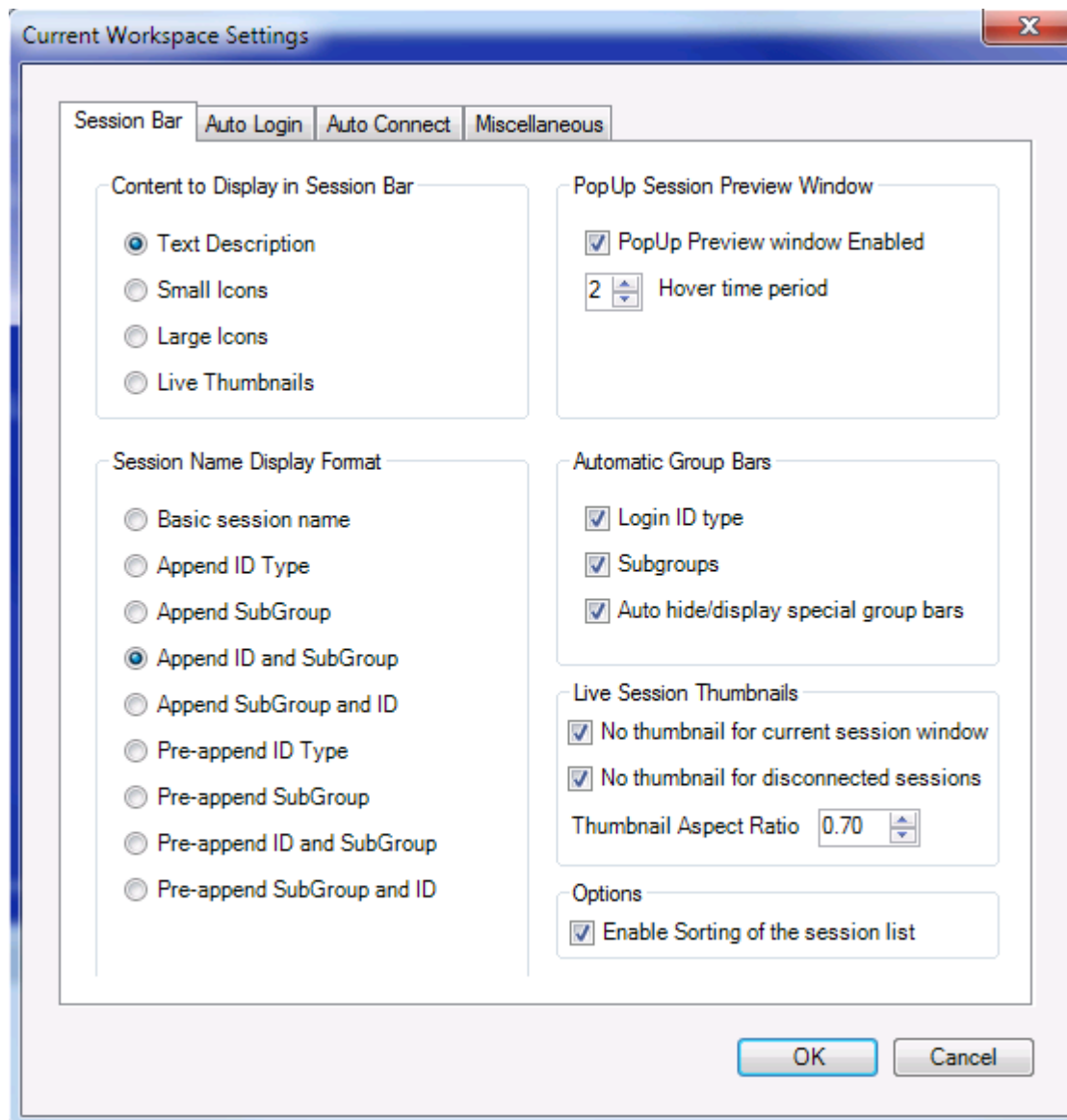
2. The Open Workspace dialog opens displaying all saved workspaces. Select the desired workspace and click Open.

### 5.5.11.2 Individual Workspace Settings

#### Configuring Individual Workspace behavior

Initial (default) workspace behaviors are set via Edit, Application settings.

To modify the behavior of the active workspace, right-click within that workspace's Session bar area, and select "Edit Workspace Settings" to see the following dialog:



More information about Session Bar can be found here: [Session Bar tab](#)

More information about Auto Login can be found here: [Auto Login tab](#)

More information about Auto Connect can be found here: [Auto Connect tab](#)

**Make changes as desired, but remember to save your workspace afterwards!**

### 5.5.11.3 Session Bar Filter

#### Session Bar Filter

**NOTE:** Users can only change session order via drag and drop sessions when the Session Bar Filter is set to All Sessions.

The Session Bar displays all sessions by default via the All Session filter button. The Session Bar filter buttons are created dynamically based on session type (terminal, File Transfer, Code Editor), ID type and Subgroup Type. You can even create a Custom Filter to filter both ID and Subgroup together.

The filter buttons on the Session Bar allows you to specify only the sessions you want to see displayed in the Session Bar based on the filter. For example the filters below show All Sessions filter, ID type = Developer and Subgroup = Training:

Sessions

**All Sessions**

SessionNames
5271-1_SFTP [Developer, Training]
5271-2 [Developer, Host site]
5271-3
5271-4* [Admin]
5271_5SFTPAdmin [Admin, Production]
5271-6 [Admin, intern]
5271-8 [Developer, Training]

---

**All Sessions**

- Admin
- Developer
- FileTransfer
- Host site
- No Login Id
- Production
- Terminal
- Training
- intern

Ready

Sessions

**List Locked**

4 Windows are Hidden

**Developer**

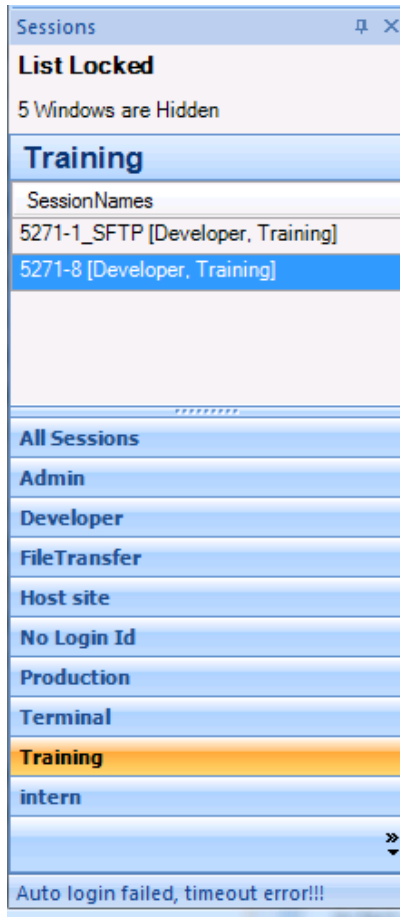
SessionNames
5271-1_SFTP [Developer, Training]
5271-2 [Developer, Host site]
5271-8 [Developer, Training]

---

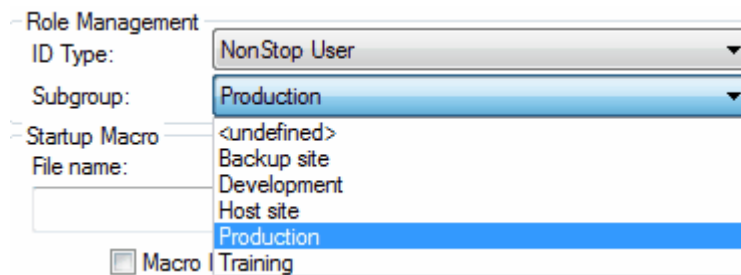
**All Sessions**

- Admin
- Developer
- FileTransfer
- Host site
- No Login Id
- Production
- Terminal
- Training
- intern

Auto login failed, timeout error!!!

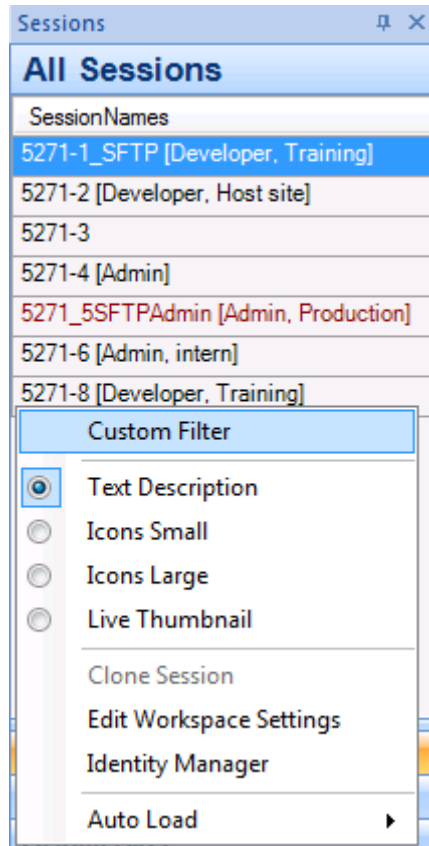


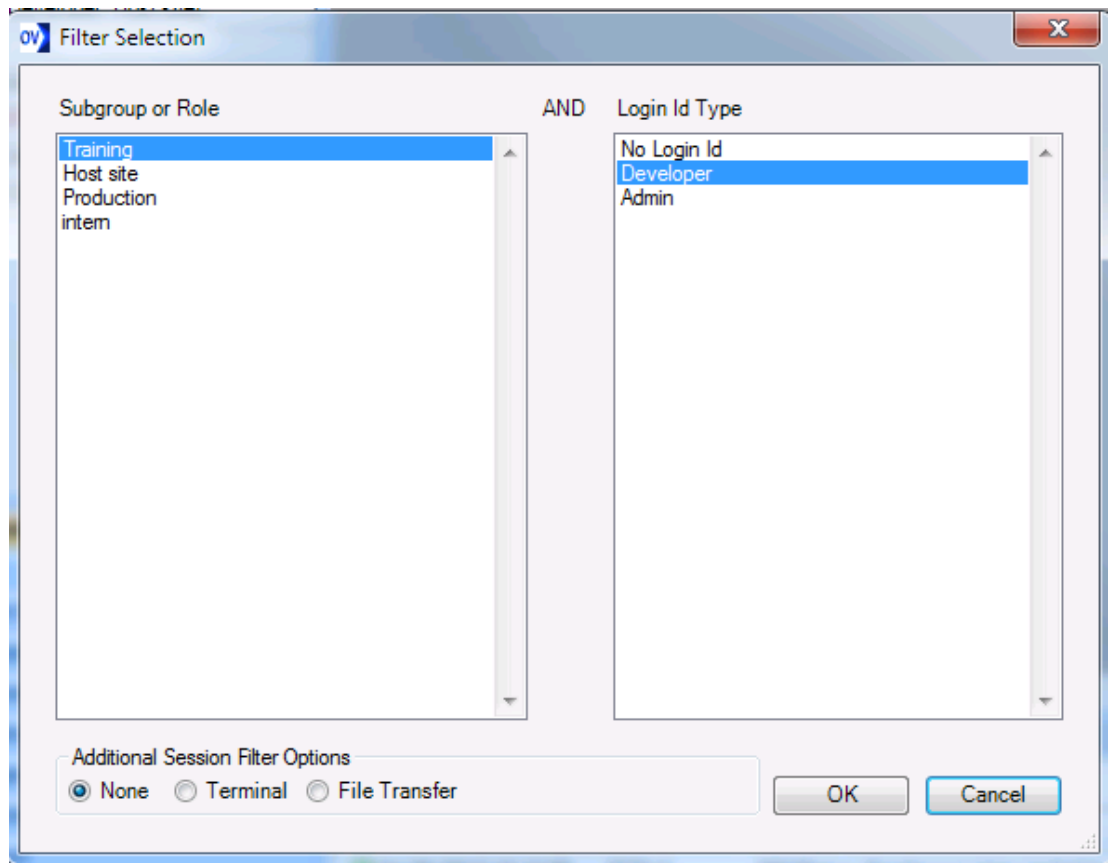
In order to filter by ID Type, Subgroup or both, you will need to specify these settings when creating a new session or modify existing session in the Session Settings dialog box's Role Management section:



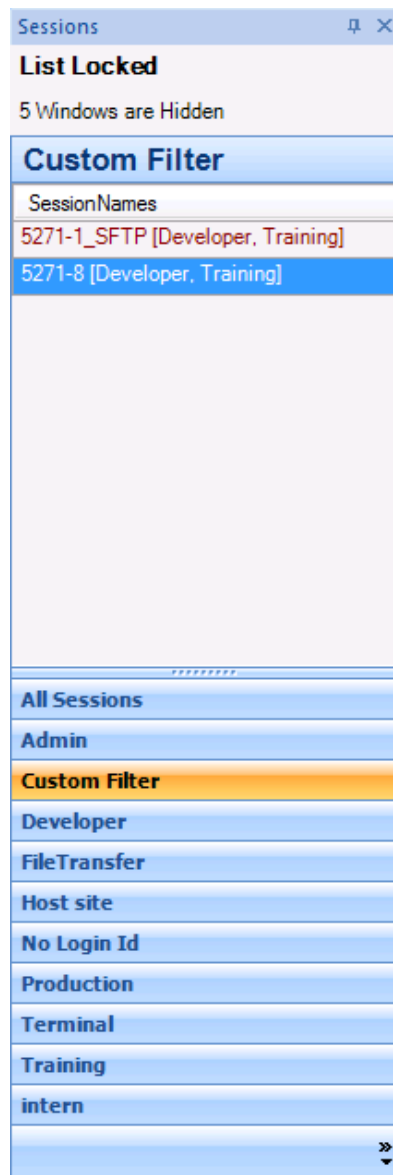
You can also configure a custom filter in which you can specify both ID Type and Subgroup:







The Additional Session Filter Options allow you to specify the custom filter to be applied to Terminal sessions only or File Transfer Sessions only.

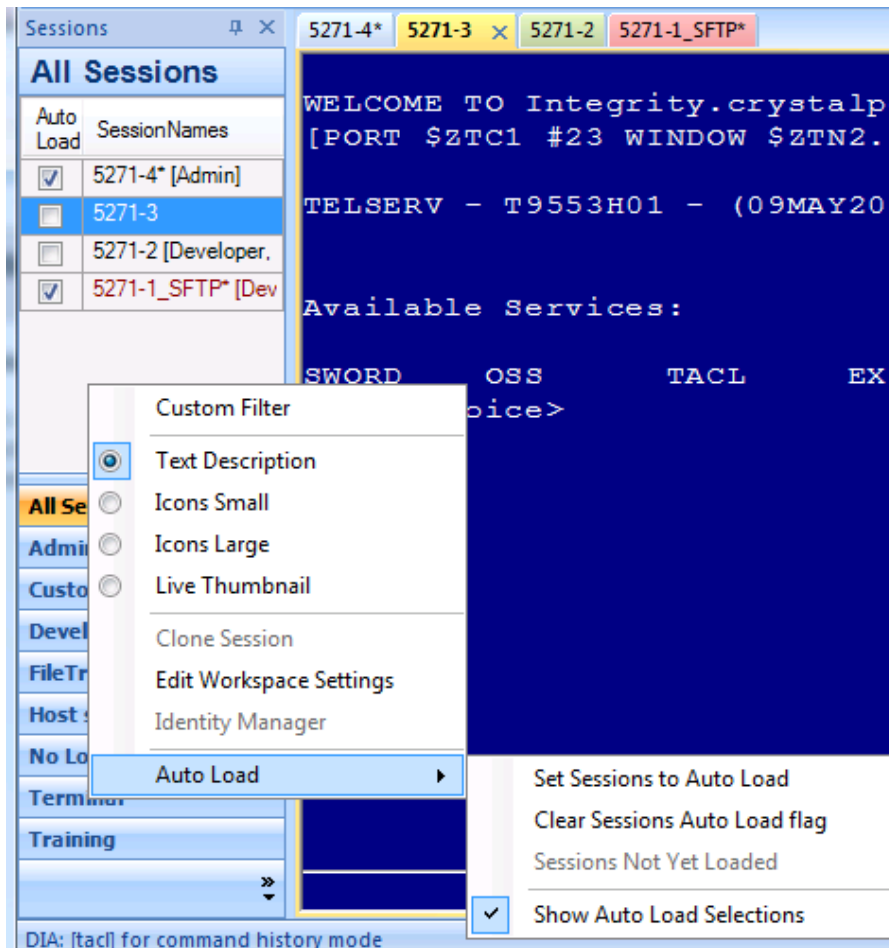


#### 5.5.11.4 Session Activation Control

##### Session Activation Control

Users can now choose, within a workspace, which sessions load and start automatically and which sessions are listed but not active until selected. This gives users the flexibility to focus on their primary sessions while having other sessions listed for immediate access, but held in reserve until needed.

To use session activation control you will need to right click mouse button when cursor is hovering over the Session Bar to bring up the pop up menu for Autoload:



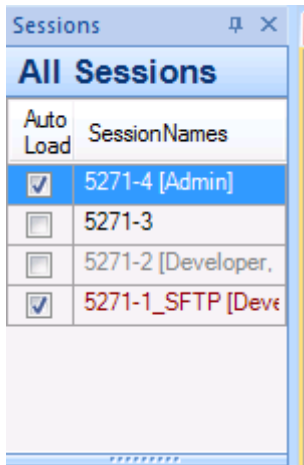
The Auto Load menu has 4 sub options that you can select:

1. Set Session to Auto Load - this menu option provides a quick select all option to make all sessions in the session bar to auto load when the Workspace is launched.
2. Clear Session Auto Load flag - this menu option provides a quick clear all sessions from loading when Workspace is launched.
3. Session Not yet Loaded
4. Show Auto Load Selections - This menu option if enabled displays a Auto Load check box next to the session depicting if the session is set to Auto Load or Not.

#### 5.5.11.5 Session Bar Color Coding for Status

##### Session Bar Color Coding for Status

Session Bar listings are now color-coded to complement the new Session Activation Control feature. Users can identify at a glance, by listing color, which sessions are preloaded but not yet active, which sessions are active, and which sessions are disconnected.



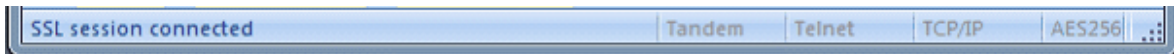
**Red** color -- Session is disconnected from host

**Black** color -- Session is connected to host

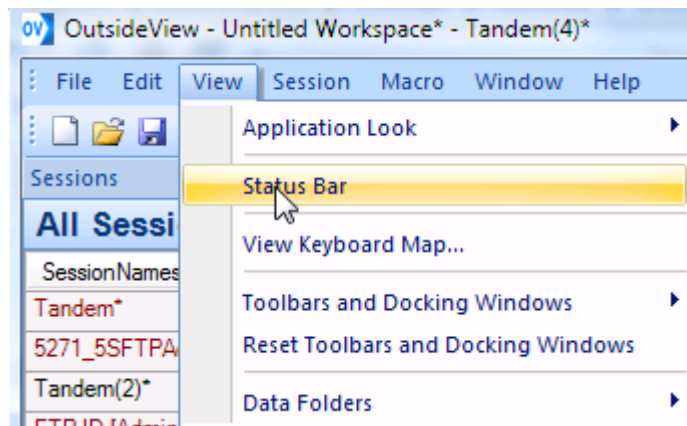
**Grey** color -- Session is not loaded

### 5.5.12 Status Bar

The status bar appears at the bottom of OutsideView and provides such useful information as what context you are in, what emulation type, cipher suite, etc.



To turn display of the Status bar on or off, select View, and then check the item on or off. This View setting will be saved as part of your workspace configuration.

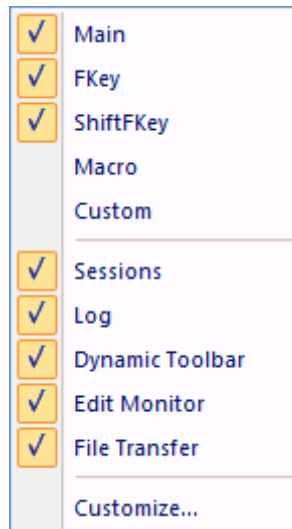


### 5.5.13 Toolbars

The toolbar content is defined at the individual workspace level, and toolbar position is defined at the application level. This is change from prior versions, where toolbar settings were stored per

individual session. Customers requested this change, to make toolbar control more efficient, and less labor-intensive.

To turn display of toolbars on or off, simply right-click within a toolbar to see the configuration menu.



Toolbars are movable, and modifiable. To move a toolbar, simply drag & drop it. Save your workspace in order to have the position remembered when the workspace is next opened.

To learn how to modify toolbars, see the topic [Customizing Toolbars](#)

## 5.6 Session and Workspace Overview

### Session and Workspace Overview

Once OutsideView is started, you create and use various **session** files to communicate with various host systems. A session might be a terminal emulation or a file transfer window to a host system. Through the session windows, you interact with the host and its applications. In addition, OutsideView delivers many of the features you would expect of standard Windows applications, such as copy/paste and graphical toolbars.

By default, OutsideView displays session windows as tabs within the OutsideView 'parent' window. You can also configure OutsideView to display multiple sessions in either tiled, or cascaded views.

Whichever view you select, you can open and connect several simultaneous sessions to various hosts within a single instance of the OutsideView application. You may, for example, open a session to your NonStop system in one tab, a session to the same host in another tab, an IBM session in another tab, perhaps one or more file transfer tabs, or have sessions to UNIX systems. There is virtually no limit to the number of concurrent sessions you may open; we test up to 256 simultaneous sessions.

An OutsideView **workspace** defines a collection of sessions and how they are organized within the OutsideView application. For instance, let's say you have several sessions open. Do a File | Save

Workspace. Thereafter, opening that single workspace will automatically open all the associated sessions, in the layout you saved, and automatically activate those sessions' connections with their defined hosts.

Click [here](#) for instructions on the creation and editing of OutsideView sessions.

Click [here](#) for instructions on saving and managing OutsideView workspaces.

OutsideView will store each users settings separately on a given PC (unless configured otherwise via Enterprise mode) in your OutsideView configuration data folder. Those settings will include various pre-populated OutsideView files, all configuration files you have created, along with any files you might receive automatically from an Enterprise installation. To see your configuration data folder, select View, Configuration Data Folder. (This view is disabled for Citrix and Windows Terminal Server clients).


## 5.7 Creating New Sessions

### Creating New Sessions

**Note:** *OutsideView Enterprise Supervisors may disable this capability to promote use of standardized session files.*

To create a new session to a host system, the minimum information to be provided are the emulation type and connectivity parameters. Even after a host session has been established, you may continue to customize the session to better suit your needs (with [custom toolbars](#), [colors](#), [keyboard mappings](#), etc.) through the [Session Settings](#) dialog.

To create a new session:

1. Select File \ New Session... or click on the New Session toolbar button .
2. The [Session Settings](#) dialog will open.
3. Define the emulation type.
  - Tandem for NonStop hosts
  - TN3270 or TN5250 for IBM hosts
  - TTY
  - VT320 or Wyse 50 for UNIX hosts

**Note:** *If you are uncertain about the required emulation type, contact your host system administrator.*

4. Define the I/O type. The most commonly used I/O methods are:
  - ASYNC: For modem or direct RS-232 connections to the host
  - [HTML Tunnel](#): For routing (tunneling) through one intermediate host using Crystal Point's tunneling servlet
  - [SSH](#): For SSH-encrypted connections to the host.
  - TCP IP/SSL: For hosts connected over a network
5. Click OK
6. The I/O tab for the selected I/O method will display. Enter the parameters required for that I/O method.
7. Click OK. A session should open and connect to the host.
8. Save the session by selecting File/Save Session As...
9. Define the session file name as something meaningful (e.g. NSKDev.cps) and click OK.

Once your new session has been successfully connected, you can include this session in a [Workspace](#).

### Clone Session

You may right-click on any ID-managed session in the Session Bar, and select Clone Session. This will open an identical instance of this session and log that session in automatically.

NOTE: A cloned session is not regarded as part of a workspace and will not be saved as part of the workspace.

## 5.8 Session Settings

### Session Settings

The Session Settings dialog box, by default, allows you to specify all configuration parameters for a host session, which consist of the nine categories listed below.

**NOTE:** *Within the Enterprise mode of OutsideView, administrators may choose which of the session setting categories users may modify. If you see less categories than normal, it may be because some categories have been protected from change (disabled), to prevent accidental or unwanted modifications that might impair operation or security.*

The Session Settings dialog may be accessed by:

- Selecting File: New Session... (to create a new session file)
- Selecting Session: Session Settings... (to edit the settings for the currently active session)
- Accessing the context menu (right click on the active session) then selecting Session Settings

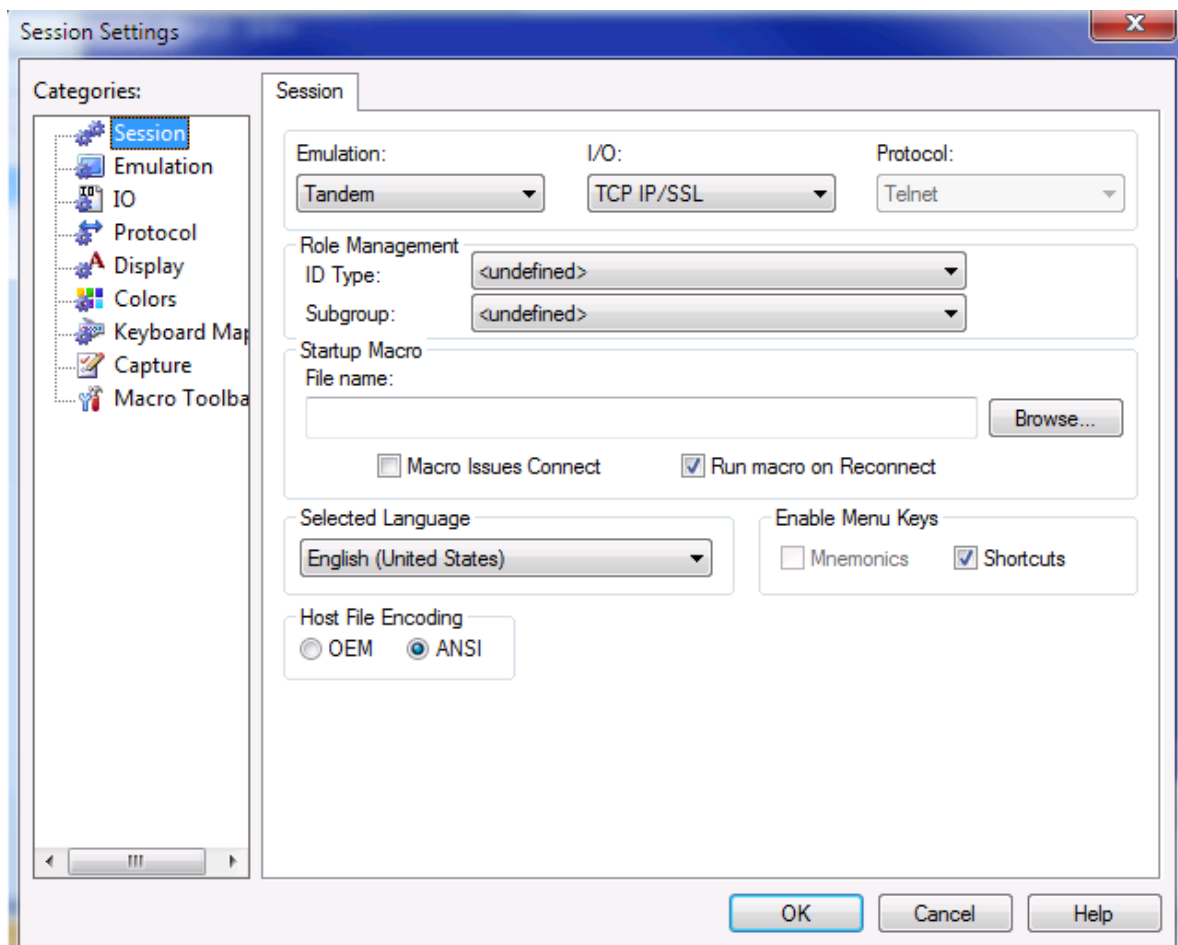


- Clicking on the Session Settings toolbar button
- The session configuration parameters are grouped into nine categories accessed via their icon in the Category column.
- [Session](#)
  - [Identity Caching](#)
- [Emulation](#)
- [I/O](#)
- [Protocol](#)
- [Display](#)
- [Colors](#)
- [Keyboard Map](#)
- [Capture](#)
- [Toolbars](#)

### 5.8.1 Session Category

#### Session Category





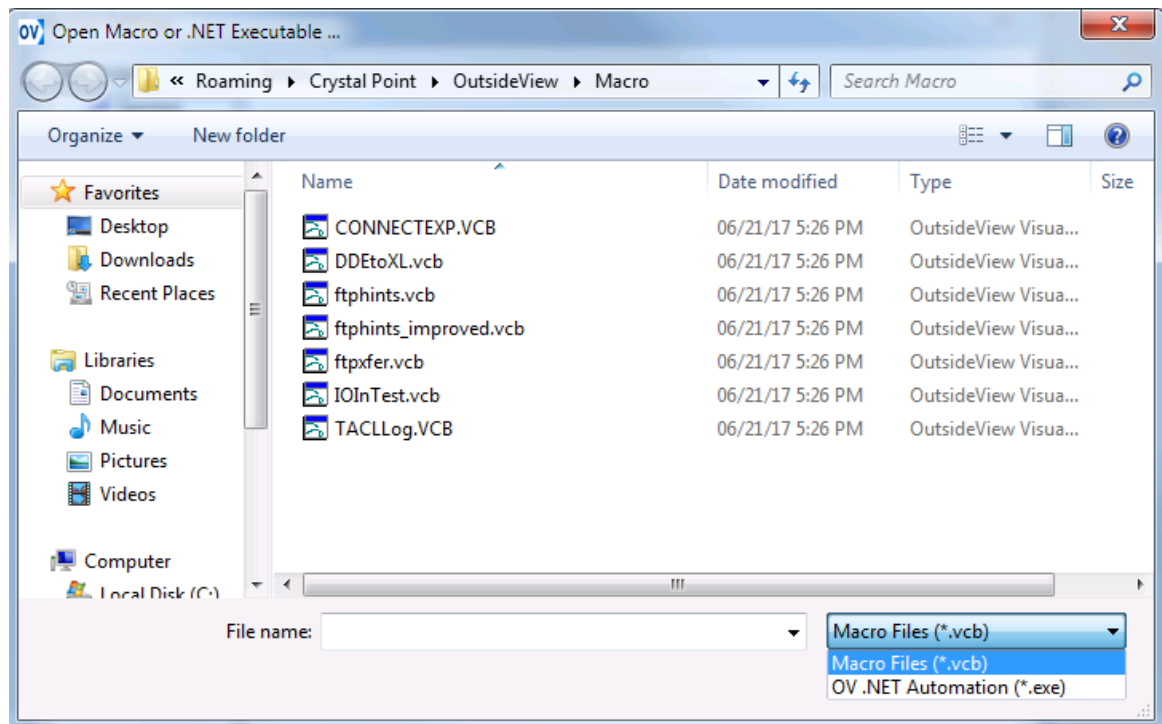
**Emulation:** The terminal type required

**I/O:** The connectivity method to the host

**Protocol:** The protocol applied (either Telnet or none)

Since **Role Management** is a newer capability, information is provided in detail. Please see [Identity Caching](#) or [Identity Management](#)

**Startup Macro:** This file can be either a Visual CommBasic macro, or a **.Net Executable**, to be executed when the session begins. The Browse button starts from the Macro sub-folder, and defaults to listing VCB macros. Use the dropdown arrows (as illustrated below) to list .Net executables.



**Macro Issues Connect:** The session remains unconnected until the macro issues a connect command.

**Run macro on Reconnect:** The macro will be re-executed on every reconnect

**Selected Language:** Determines keyboard mapping and the ANSI code page that will be used by default. For a detailed description of national character set support in OutsideView, click [here](#).

**Enable Menu Keys:**

**Mnemonics:**

Off: (default) alt+key combination is sent to the host (Alt+Shift+F1 sends SF11 to Alt+Shift+F6 sends SF16).

**Shortcuts:**

On: Any Ctrl+key combination is processed by Windows (e.g. Ctrl+c will cop selected text).

Off: Any Ctrl+key combination is sent to the host.

**Host File Encoding:**

**OEM:** Host files are in OEM code pages

**ANSI:** Host files are in ANSI code pages

For a detailed description of national character set support in OutsideView, click [here](#).

## 5.8.2 Identity Caching

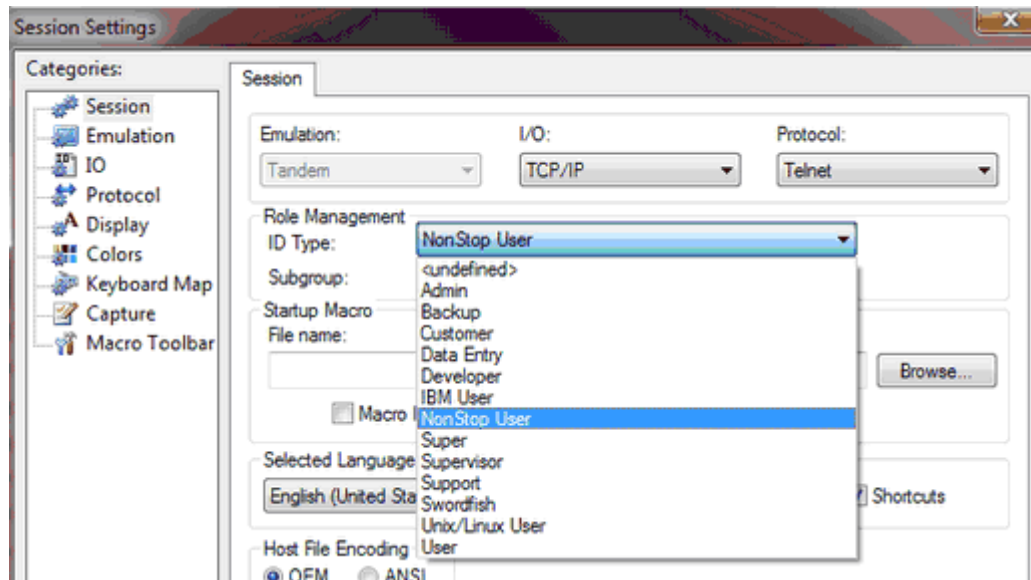
Identity Caching (Managed ID), or Role Management, is the **optional** capability of OutsideView to:

1. Store user credentials (encrypted) in RAM while the OutsideView program remains active.
2. Associate user credentials with an Identity Type
3. Automatically login in users for sessions with an Identity Type defined, and credentials stored in RAM.

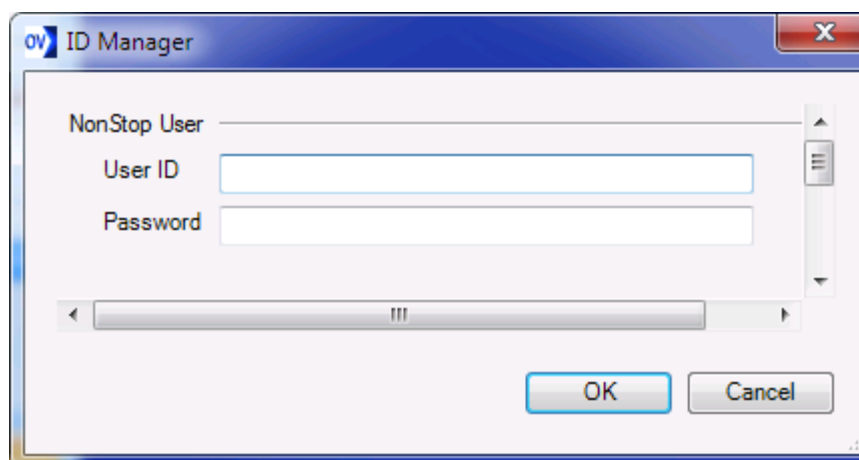
4. Purge all user credentials from (encrypted) RAM upon OutsideView termination

### Selecting ID Types

When setting session properties, select from the available ID Types. You should use the same ID Type for all sessions where you want the same credentials used. (For instance, assume you have three hosts but use the same logon for all. You would create three session files, each with a different host address, but all with the same ID Type.



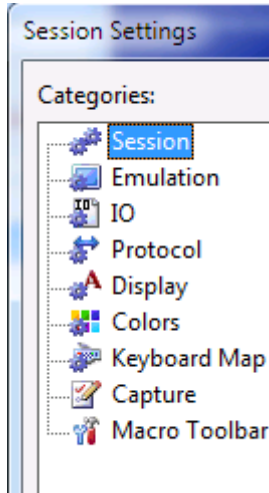
When the first session of a given ID Type starts, the user is prompted for their credentials:



These credentials are then stored (encrypted) in RAM. Whenever a session is opened or (optionally) re-connected, OutsideView will automatically login that session, using the stored credentials.

### 5.8.3 Emulation Category


#### Emulation Category



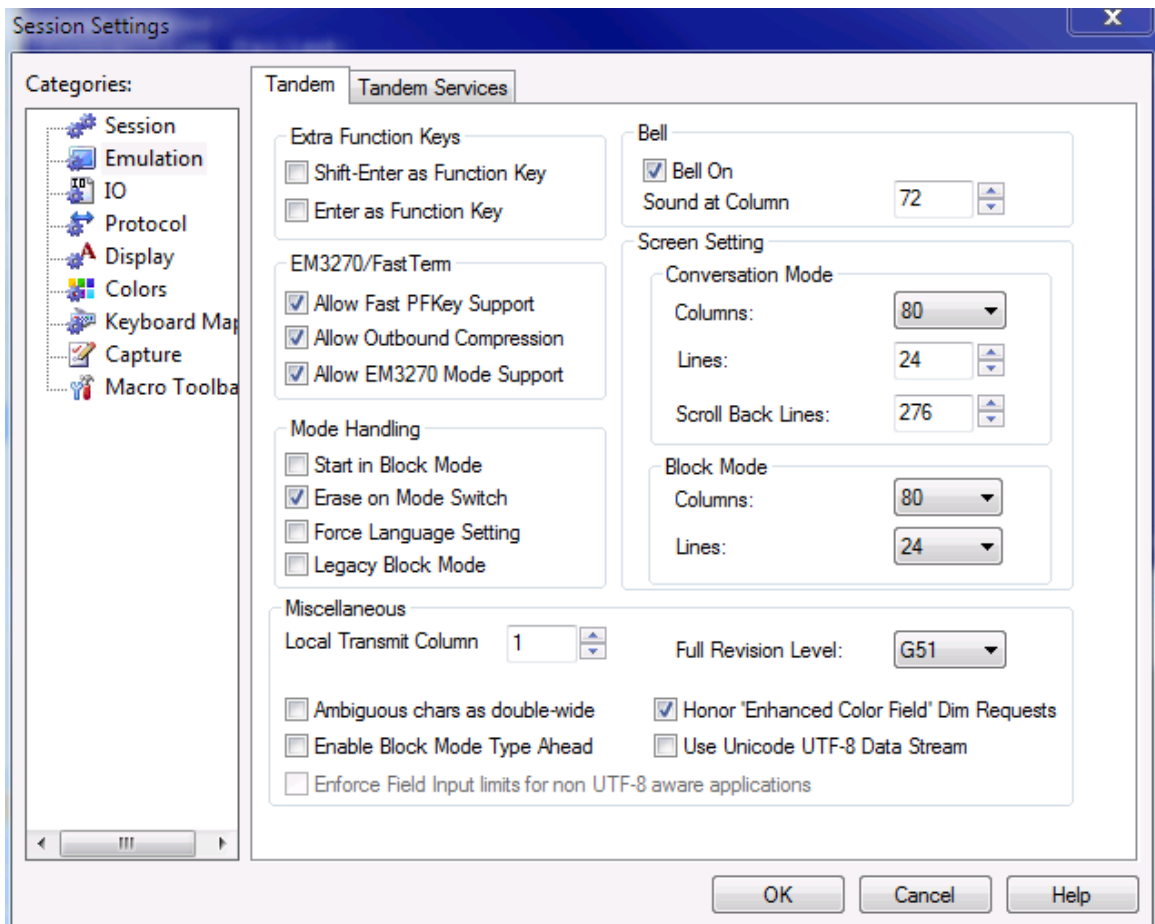
The Emulation tab allows definition of all parameters relating to the terminal type chosen in the Session tab. See your host system administrator if assistance is required for these settings.

If using a Tandem 6530 emulation, for instance, you will see this screen, where you can define such helpful settings as 80 or 132 column mode, how many lines are in the video scroll back buffer, etc.

**NOTE:** There is a toolbar icon, displayed by default, called the Toggle Screen Width icon:

 **Toggle Screen Width** which enables you to dynamically switch the OutsideView conversation mode screen between 80 and 132 columns.

**Legacy Block Mode** - This option preserves the original version of Block paste output formatting. Legacy Block Mode will allow users to use block text selection and be able to paste into multiple input fields at the same time.



**NOTE:** When using Japanese fonts, please set "Ambiguous chars as double-wide" (as shown above) to ON.

The 6530 emulator supports the UTF-8 data stream for character encoding. Two new check boxes have been added "Use Unicode UTF-8 Data Steam" and "Enforce Field Input limits for non UTF-8 aware applications.

The latter checkbox prevents the user from entering more glyph's into a input field than the host would expect to store in memory or to a fixed record length file.

For more information, see the UTF-8 [support notes](#) under troubleshooting.

The **Tandem Services** tab lets you define Tandem specific settings, such as whether to permit host-initiated IXF or raw printing..

**Tandem** Tandem Services

**Auxiliary I/O**

**Aux 1 Options**

**Form Feed**

None

Trailing

Leading

**Line End**

CR

LF

Form Feed Timeout

**Aux 1**

Printer  File

**Aux 2**

Printer  File

**IXF Support**

Allow Host Initiated IXF Transfers

Wait after Host Initiated IXF Transfers

**Raw Printing**

Send raw bytes directly to printer

## 5.8.4 I/O Category

### IO Category

After selecting an I/O method on the Session category screen, the I/O tab will display a screen appropriate for defining the parameters needed for that I/O method chosen.

Please select an IO method, below, to see the relevant screen and related information :

Async: For RS-232 connections from a PC COM port to the host or via modems

[HTML Tunnel](#) For routing (tunneling) through one intermediate host to reach the final destination.

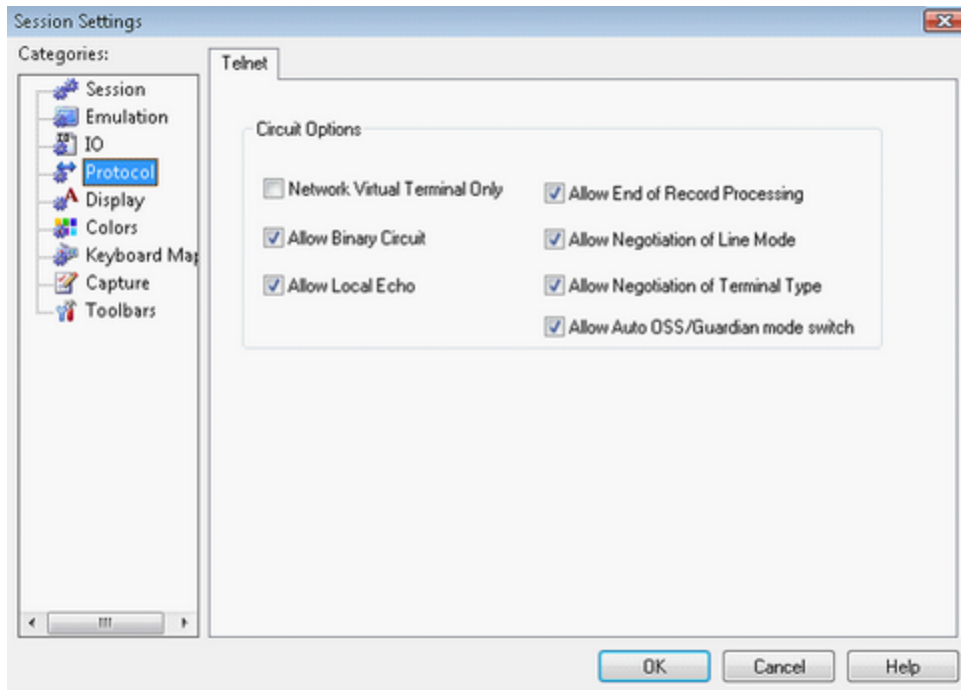
SSH: For ssh-encrypted telnet sessions

TCP IP/SSL: For connections using TCP networks.

See the Environment Variables topic for instructions on how Windows environment variables may be used to define I/O parameters.

## 5.8.5 Protocol Category

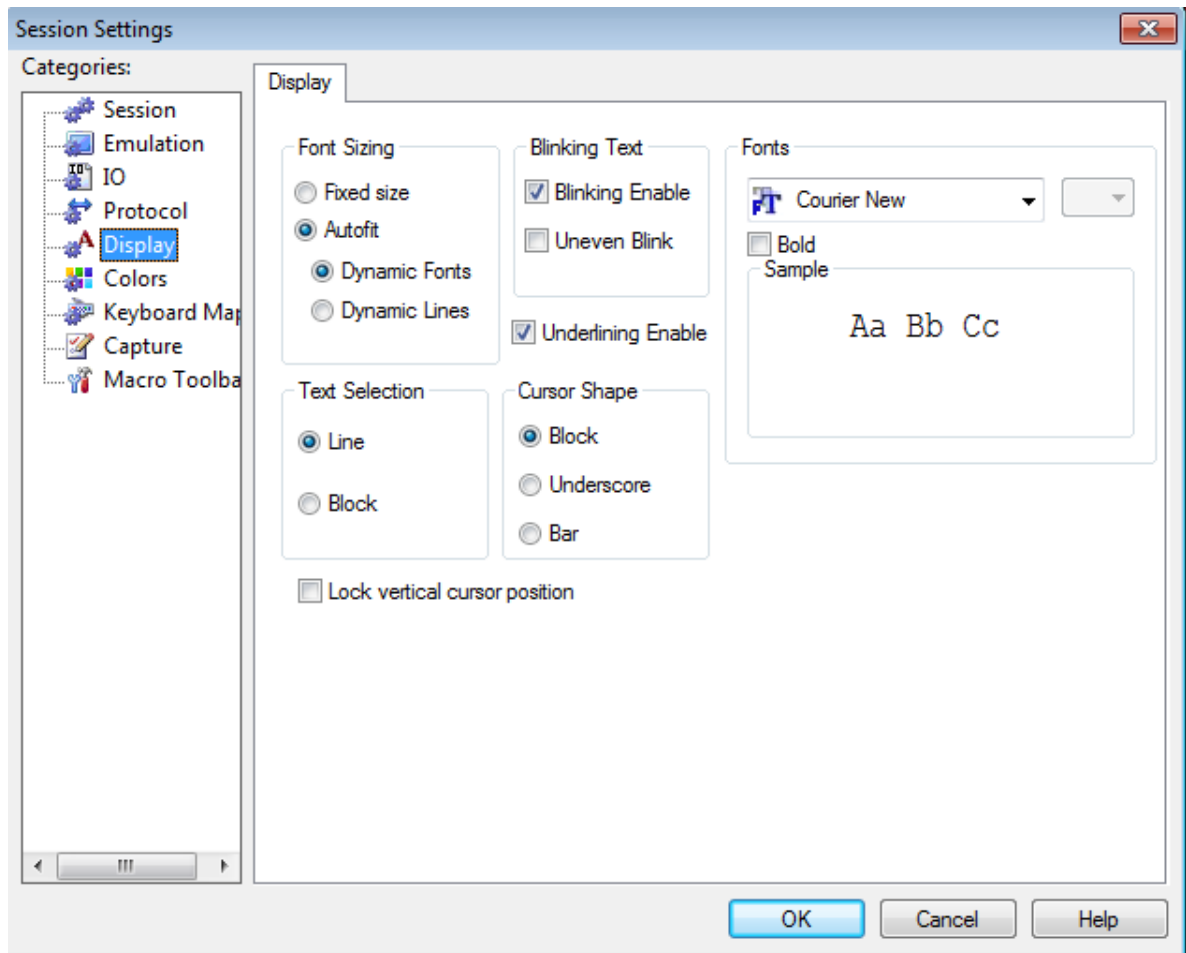
### Protocol Tab



The Protocol tab allows definition of all parameters relating to the telnet protocol. In most cases, these parameters should not be changed. Please consult your system administrator before changing these settings.

## 5.8.6 Display Category

### Display Category



The Display tab allows definition of all parameters affecting font and cursor types and display as well as text selection behavior.

### Font Sizing

There are several ways to set the font size used to display text within a session window:

#### Sizing Methods

**Fixed Size:** Uses the font size specified on the Session Properties Display tab, regardless of the size or shape of the session window. The entire session screen may not fit within the session window.

**Auto Fit:** Automatically sizes the font so the entire session screen fits within the session window, regardless of the size or shape of the session window.

**Dynamic Font:** An option within the Auto Fit mode, Dynamic Font will re-size the display font to match changes to the session display window dimensions. This may result in inserted pixels between characters to justify the display. This may affect graphics applications that require adjacent characters to touch for best effect. If you use applications that display graphics (such as boxes around menus, etc.), you may not want to use this option.

**Dynamic Lines:** A new option with the Auto Fit mode, Dynamic Lines will maintain a 16:7 font aspect ratio (the same one used for the Fixed Size option) regardless of the aspect ratio (dimensions) of the client window in which the font is being displayed. During a re-size of the client window, the character's width will increase as far as it can laterally, then fix itself at – or as close as it can to – the 16:7 ratio. To fill the remainder of the screen as needed, lines will



be added to the top of the display, from the video buffer, until there are no more remaining to be added. After that, blank lines will be added to the bottom. In all cases the cursor, regardless of its position on a screen, will be kept visible after the resizing completes. **This option facilitates moving OV windows from monitor to monitor, particularly between those landscape and portrait mode monitors.**

### Blinking Text

Allow or disallow blinking text (defined in character attributes from host).

### Fonts

All True Type fonts on the local system, whether fixed pitch or proportionally spaced, are available. An example of the selected font and bold option is shown in the Sample box.

Checking the Bold option will display all characters in bold.

**NOTE:** Most NonStop screens assume fixed pitch font. Screen text layout and columnar alignment may become erratic when/if selecting proportionally spaced fonts.

### Text Selection

Text may be selected on either a line-by-line basis (line) or as a rectangular selection (block).

Underlining Enabled

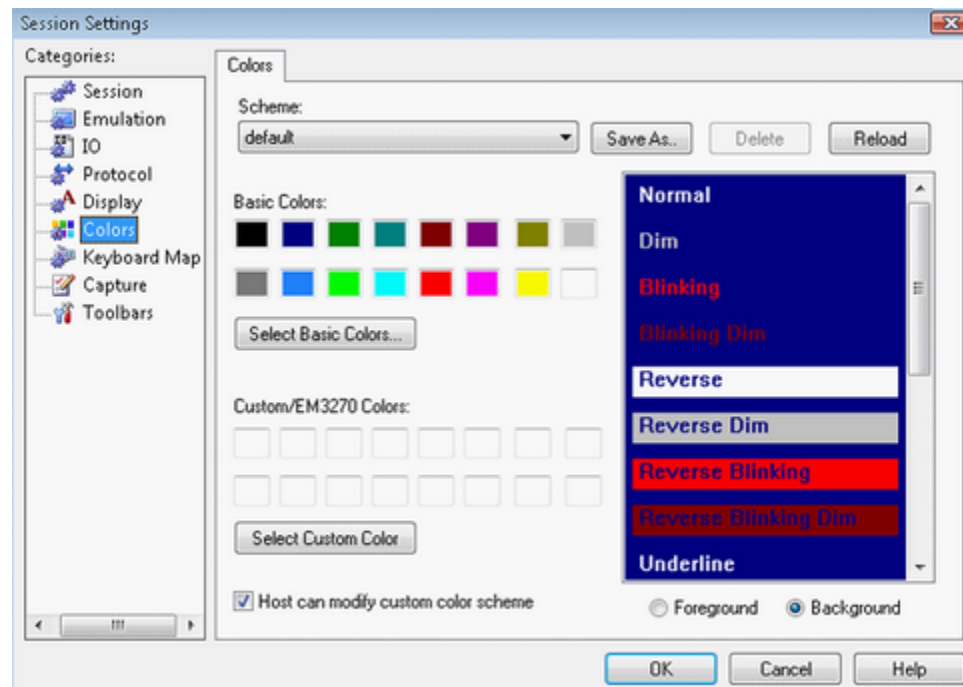
If selected, character streams from the host with the underline attribute will be displayed underlined.

### Cursor Shape

The cursor may be displayed as a block, an underscore or as a vertical bar.

## 5.8.7 Colors Category

### Colors Category



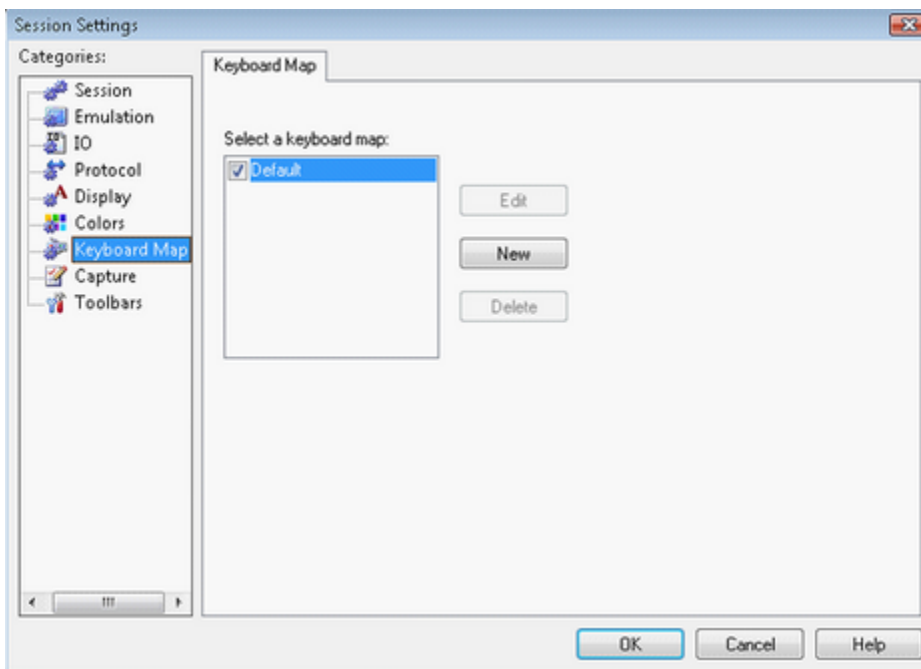
The Colors tab allows definition of the mapping of character attributes to display colors and saving of those mappings as color schemes (\*.cpc).

To change the mapping of character attributes to display colors:

1. Place the desired session in focus by clicking the session window, clicking that session's shortcut icon in the Shortcut Bar, or by selecting it from the Window menu.
2. Click the Session Color Settings button on the toolbar, or select Session: Session Settings from the menu.
3. Click the Colors category on the Session Settings dialog box.
4. Click the appropriate button to select either the Foreground or Background option. The foreground color is the text and the background color is the screen.
5. Click the desired color.
6. Click on the text attribute to apply your selected color. The possible text attribute combinations are shown in the list on the right. For example, if you change the color of Blinking Underlined Dim to pink, then all text sent to this session's screen as dimmed, underlined, and blinking will also be pink.
7. If the particular text attribute you want to change isn't immediately visible, use the scrollbar on the right to scroll down to additional combinations.
8. If you decide that you don't like your changes after all, you can click Reload to discard your changes and reload the last-saved setting of the current color scheme. You can also use the drop-down list to select another scheme to apply.
9. When you have set the colors as desired you may (optionally) save this new mapping as a color scheme file (\*.cpc) for application to other sessions. Click OK to close this window and apply your changes.

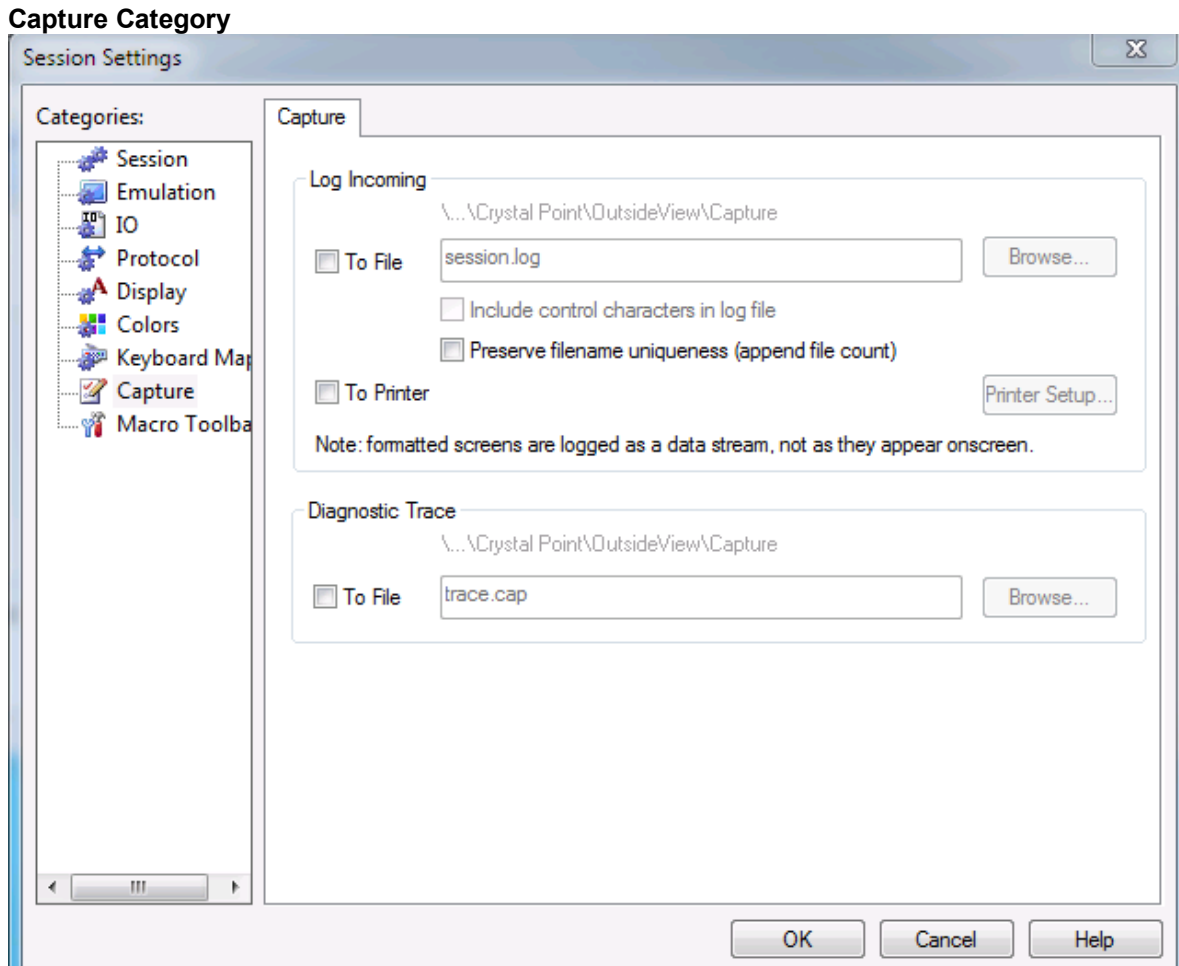
## 5.8.8 Keyboard Map Category

### Keyboard Map Category



The Keyboard Map tab allows creation of new keyboard map files, or assigning some other, custom keyboard map to the current session. Click [here](#) for instructions on creating or editing keyboard map files.

## 5.8.9 Capture Category



The Capture Tab allows configuration of session logging and creation of diagnostic traces.

### Log Incoming

The Log Incoming feature of OutsideView provides the capability to log the session data to either a file or a printer.

Note that data is logged as it is received: raw and unformatted. This means that formatted screens, such as Tandem block mode applications, will not appear in the log as they do on the session display.

If any errors occur opening a trace or log file, or opening and writing to a save file, then an error box is displayed describing the error and the trace file or log file setting is turned off automatically. Data logging automatically stops when you close the session that is being logged. It does not automatically restart if you reopen the session.

To Enable or Disable Data Logging

1. Place the session in focus by clicking the session window, clicking the icon in the Shortcut Bar, or by selecting it from the Window menu.
2. Use the File: Log Incoming menu command, and then select either To File or To Printer

or  
Access the Session Settings dialog (Session: Session Settings), click the Capture category  
or  
Right-click and select Log Incoming to File

Set the desired Log Incoming option: Log to File or Log to Printer.

If you select Log to File, specify a file name and whether you want control codes to be included in the log. Then click OK.

When you want to stop logging session data, simply repeat these steps and deselect the Log To option that you selected previously.

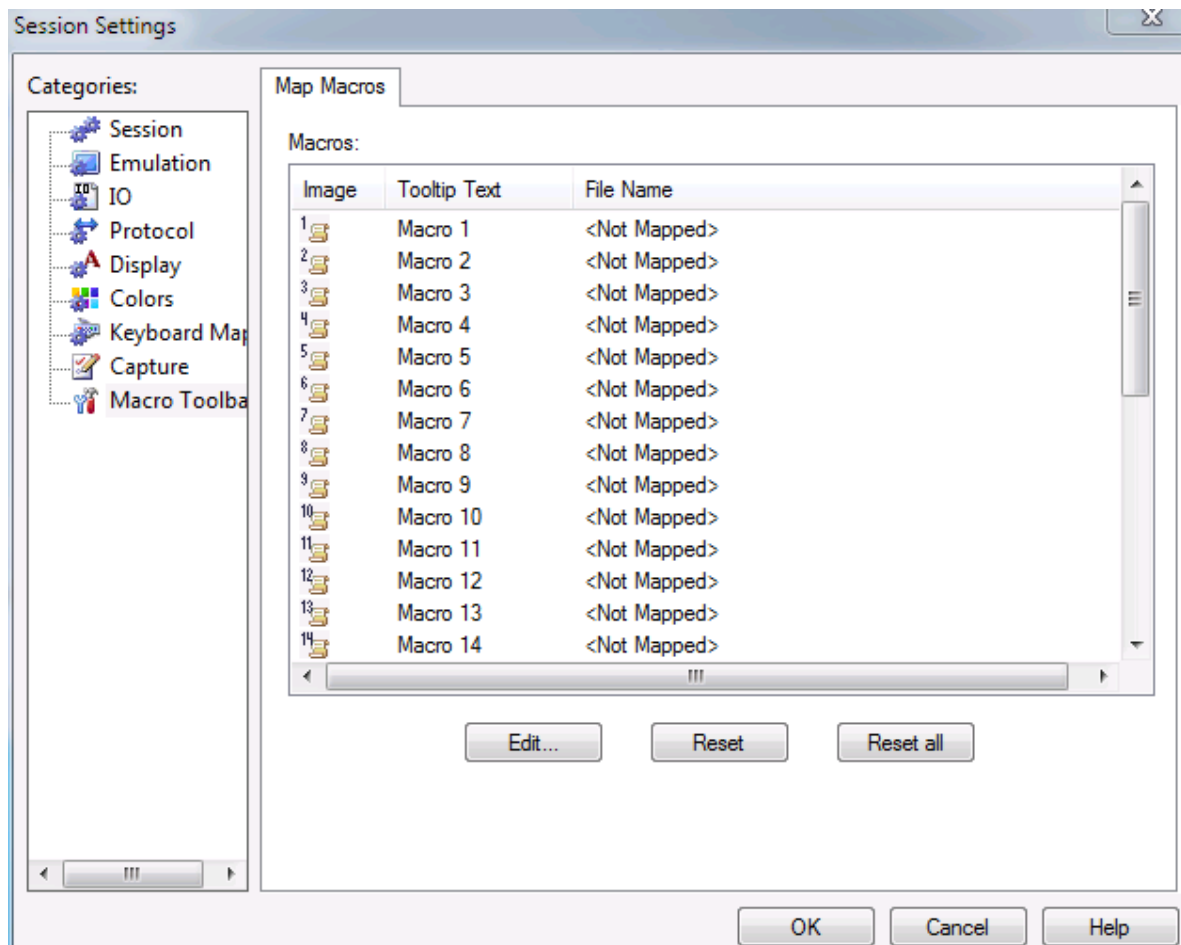
Logged session data saves to the Capture folder by default; you can specify an alternate location if you wish. That alternate location will become the default location until you close that session.

Diagnostic Trace

Please see the [Diagnostic Traces](#) topic for instructions on creating a trace file.

## 5.8.10 Macro Toolbar Category

### Macro Toolbar Category



The Macro Toolbar category allows assignment of macro files to macro toolbar buttons.

Please see the [Customizing Toolbars](#) topic for instructions on creating new toolbars.

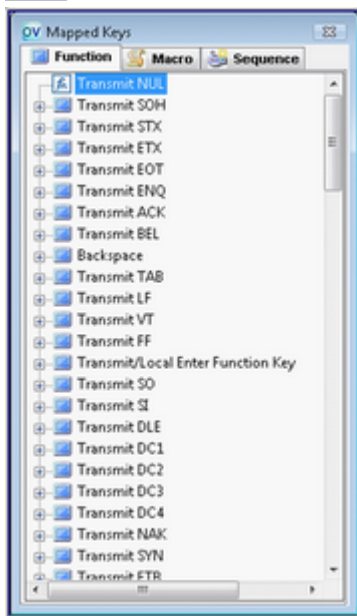
## 5.9 Keyboard Mapping

### 5.9.1 About Keyboard Mapping

#### About Keyboard Mapping

Keyboard mapping allows you to map keyboard character combinations (e.g. Ctrl+P) to terminal functions (e.g. Print), macros or key sequences. These mappings are saved in keyboard map files with the extension .cpm and may be assigned to any session. Keyboard maps are created and edited through the Key Mapper and Mapped Keys dialogs when accessed through the Keyboard Map tab of Session Settings or by pressing the Key Mapper tool bar button.

**NOTE:** Keyboard mapping is not effective within DIA input areas.



To create a new keyboard map:

1. Access the Keyboard Map tab in the Session Settings dialog.
2. Click New. The currently selected map will be used as a template. At this point, you can map key combinations to:
  - [Terminal Functions](#)
  - [Macros](#)
  - [Key Sequences](#)
3. After your edits are complete, select File/Save As... in the Key Mapper to create a new keyboard map file.

To edit an existing keyboard map:

1. Access the Keyboard Map tab in the Session Settings dialog.
2. Select an existing map and click Edit.
3. After your edits are complete, select File/Save in the Key Mapper.

**Note:** The **default** keyboard map cannot be changed (You can store changed keyboard maps under other names than default.)

### Deleting Mappings

- To delete a mapping, select the desired mapping in the Mapped Keys diagram and press the Delete key. The default key map itself cannot be deleted or overwritten.
- If you delete the customized key mapping that you are currently using, the session will automatically switch to the default key mapping.

### Keys That Cannot Be Mapped

- If you attempt to map a key or key combination that is already mapped, an error message displays. The Key Mapper changes its display to show you the current key/combination mapping. Delete the unwanted mapping, and then map the desired mapping
- The backslash (\) key and the forward slash key (/) on the main keyboard cannot be mapped, but the slash key on the numeric keypad can be used in mapping combinations. The numeric slash will not display in the Keys Pressed field while dragging, but will be correctly used in the mapping.

If you want to see which keyboard mappings are already in place for an active session, you can click View/Keyboard Map for a quick read-only view. The only options available on the menu will be Print and Exit, and you will not be able to map any keys.

- For instructions on mapping Terminal Functions click [here](#).
- For instructions on mapping macros, click [here](#).
- For instructions on mapping key sequences, click [here](#).

## 5.9.2 Mapping Terminal Functions

### Mapping Terminal Functions

To map a Terminal Function to a key combination:

1. Access the Keyboard Map tab in the Session Settings dialog.
2. Select a key map to edit and click Edit or click New to create a new map.
3. In the Mapped Keys dialog, select the Function tab to view available terminal functions.

**Note:** You may check existing key mappings by clicking on the + symbol for a function.

4. In the Key Mapper dialog, click and drag the key icon to be mapped to the target function within the Mapped Keys dialog. If a key modifier is to be applied, press the modifier keys (Ctrl, Alt or Shift) on the physical keyboard prior to clicking on the key in the Key Mapper.

**Note:** If the selected key is already mapped, the Mapped Keys dialog window will switch highlighting onto the function already mapped to that key. If you choose, you may [delete](#) that key mapping so that the selected key can be mapped to the purpose you prefer.

5. After your edits are complete, select File/Save in the Key Mapper to save an existing map file or File/Save As... to create a new map file.

### 5.9.2.1 Mapping Key Sequences

#### Mapping Key Sequences

Mapped key sequences can be a great time-saver. You can map frequently entered data, long commands, or escape sequences for special functions to a single key.

To Map a Key Sequence

1. Access the Keyboard Map tab in the Session Settings dialog.
2. Select a key map to edit and click Edit or click New to create a new map.
3. In the Mapped Keys dialog, select the Sequence tab to view available Sequences.
4. To create a new sequence, on the Key Mapper dialog, enter the desired text string in the Key Sequence edit field. To enter control or escape characters, use the format \nnn where nnn is the three digit decimal ASCII code for the desired character.

5. Drag the Seq# button to the left of the edit field to the Mapped Keys dialog box. It is added to the list of key sequences.
6. In the Key Mapper dialog, click and drag the key to be mapped to the target sequence within the Mapped Keys dialog. If a key modifier is to be applied, press the modifier keys (Ctrl, Alt or Shift) on the physical keyboard prior to clicking on the key in the Key Mapper.

**Note:** *If the selected key is already mapped, the Mapped Keys dialog window will switch highlighting onto the sequence already mapped to that key. If you choose, you may [delete](#) that key mapping so that the selected key can be mapped to the purpose you prefer.*

7. After your edits are complete, select File | Save in the Key Mapper to save an existing map file or File | Save As... to create a new map file.

### 5.9.2.2 Mapping Macros

#### Mapping Macros

To map a Visual CommBASIC macro to a key combination:

1. Access the Keyboard Map tab in the Session Settings dialog.
2. Select a key map to edit and click Edit or click New to create a new map.
3. In the Mapped Keys dialog, select the Macro tab to view available macros.
4. In the Key Mapper dialog, click and drag the key icon to be mapped to the target macro within the Mapped Keys dialog. If a key modifier is to be applied, press the modifier keys (Ctrl, Alt or Shift) on the physical keyboard prior to clicking on the key in the Key Mapper.

**Note:** *If the selected key is already mapped, the Mapped Keys dialog window will switch highlighting onto the macro already mapped to that key. If you choose, you may [delete](#) that key mapping so that the selected key can be mapped to the purpose you prefer.*

5. After your edits are complete, select File/Save in the Key Mapper to save an existing map file or File/Save As... to create a new map file.

## 5.10 Toolbars

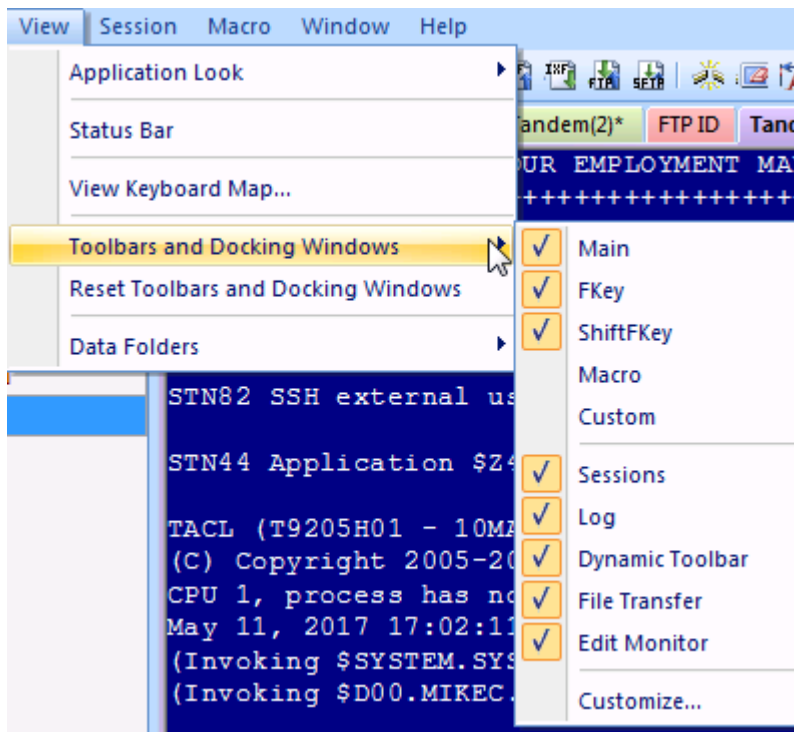
### 5.10.1 Toolbar Overview

#### Toolbar Overview

The toolbar content is defined at the individual workspace level, and toolbar position is defined at the application level. This is a change from prior versions, where toolbar settings were stored per individual session. Customers requested this change, to make toolbar control more efficient, and less labor-intensive.

Toolbars provide a quick way of performing common tasks (e.g. copying and pasting text), sending function keys to the host (e.g. Shift F16) or executing macros. OutsideView will, by default, display three toolbars; Main, FKey, and ShiftFKey. These are movable, and dockable. Merely drag the toolbar to the position you prefer.

To control which toolbars are displayed, select View | Toolbars and Docking Windows | and then check ON or OFF the toolbars you wish to see:



























All toolbar buttons (both pre-defined and custom) support ToolTips. To see what a toolbar's button does, hold the mouse pointer over the button without moving it. A very brief description will appear next to the button.

You can create additional toolbars as desired.

- See the [Customizing Toolbars](#) topic for instructions on creating custom toolbars
- See the [Macro Toolbar](#) topic for instructions on mapping macros to toolbar buttons.



## 5.10.2 Default Toolbar Icons

 <b>New Session (Ctrl+N)</b> Create a new Session Window	 <b>Send File</b> Send a file through the in-focus Session
 <b>Open Session (Ctrl+O)</b> Open an existing session from a session file	 <b>Receive File</b> Receive a file through the in-focus Session
 <b>Save Session (Ctrl+S)</b> Save the active session settings to a session file	 <b>FTP/SFTP Session</b> Launch FTP/SFTP
 <b>Open Workspace</b> Open an existing workspace from a workspace file	 <b>Send Break</b> Send a Break signal to the host
 <b>Copy (Ctrl+C)</b> Copy the selection and put it on the Clipboard	 <b>Clear Screen (Ctrl+L)</b> Clear the data fields for the active session
 <b>Paste (Ctrl+V)</b> Insert Clipboard contents	 <b>Toggle Screen Width</b> Switch between 80 and 132 columns
 <b>Print Screen (Ctrl+P)</b> Print the active Session Display	 <b>Session Messages</b> View Logged Session Messages
 <b>Workspace Settings</b> Changes various workspace settings	 <b>User's Guide (Ctrl+H)</b> User's Guide
 <b>Session Settings</b> Changes various session settings	 <b>Dynamic Input On/Off</b> Toggle Dynamic Input On/Off
 <b>Apply/Remove Session Password</b> Session Settings Password	 <b>Reissue Command</b> Reissue Command from History
 <b>Reconnect (Ctrl+R)</b> Cause in-focus session to reconnect to its host	 <b>Dynamic Input Settings</b> Invoke Dynamic Input Settings dialog
 <b>Disconnect (Ctrl+D)</b> Cause in-focus session to disconnect from its host	 <b>Spell Check Input Field(s)</b> Spell Check currently visible input field(s)

## 5.10.3 Customizing Toolbars

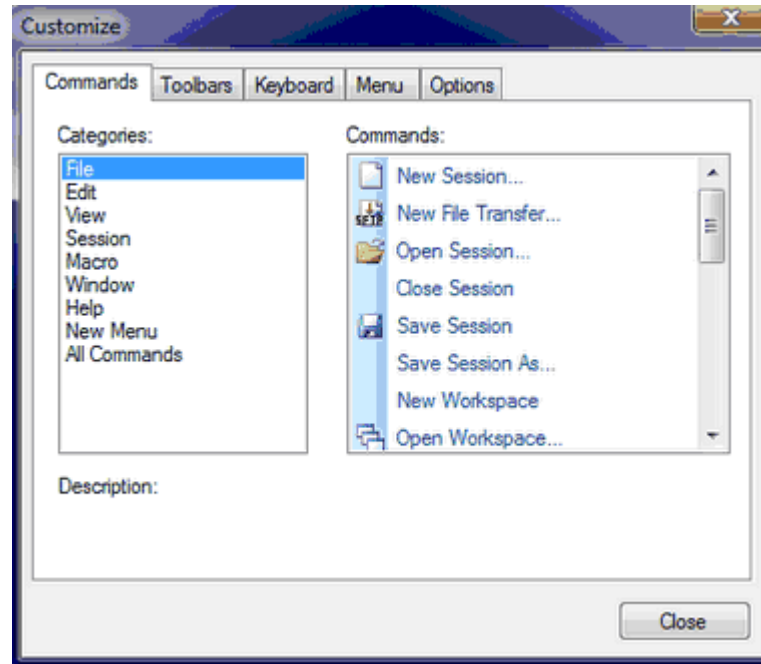
### Customizing Toolbars

OutsideView allows users to show or hide buttons on the various toolbars. Merely place your cursor on the right end of toolbar, to see the Add/Remove Buttons option. Check buttons On or OFF to have them display in the toolbar, or not.

OutsideView also ships with a non-displayed, nearly empty toolbar. All it starts with, is the Help icon. This toolbar is provided as the repository for those who wish to create a single, blended toolbar, rather than having multiple toolbars display.

To display the Custom toolbar, select View, Toolbar, and click on Custom. To populate the Custom toolbar with the icons of your choice, access the dialog for creating new, or modifying existing, toolbars by selecting View, Toolbars and Docking Windows, Customize when any session is active.

Another method for invoking Toolbar Customization mode is to right-click in any toolbar and select Customize.



#### Once in Customize mode, you may

- Remove icons by dragging them off the toolbar
- Move (drag+drop) icons from one toolbar to another
- Copy (control+drag) icons between toolbars.
- Select the Commands tab, and move or copy commands from there onto a toolbar. **The category All Commands includes commands not necessarily used in any default toolbars.**
- Use the Options tab to specify Tool tip and other 'hint' behaviors
- Use the Keyboard tab to edit accelerator keys, also known as speed keys or shortcut keys. For instance, set File, New to be Alt+G if you wish.

#### Toolbar tips:

- To insert a button between two other buttons, drag the button outline between them.
- To create button groups within a toolbar, drag any button already on the toolbar slightly away from an adjacent button. A separator bar will appear. Drag the button close to the button on the other side of the separator to remove the separator.
- To delete a button, drag it completely off the toolbar.
- If you drag the last button off a toolbar, the toolbar itself automatically becomes invisible. Close and re-open View: Toolbars, then check the toolbar's checkbox to make it visible again. Once it's visible again you can continue customizing it.
- Toolbars can be either "floating" or "docked," depending on your preferences. Floating toolbars are separate windows with title bars. Docked toolbars appear attached to the edges of the workspace.
- You may change the position of a toolbar by simply dragging it to the desired location. Floating toolbars can be dragged around by the title bar. Docked toolbars have a grooved handle at the

left or top side.

- If you need to, you may reset one or all toolbars by selecting "Customize", selecting the Toolbars tab, and then highlighting one toolbar and selecting "Reset" or select "Reset All" to restore all toolbars to their defaults.

## 5.10.4 Reset Toolbars

### Reset Toolbars

The new toolbar capability is very powerful. Users can do so much, they can possibly get too complex. If you ever want to just 'start over' with default toolbars, you may. Simply select View, Reset Toolbars.

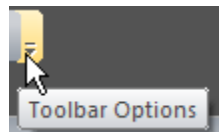
CAUTION: This deletes all toolbar customization and returns all toolbars to the default state.

## 5.10.5 Changing Icon images

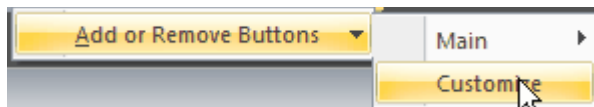
### Changing Icon images

To modify an icon of a toolbar, you must first set the toolbar into a customizable state.

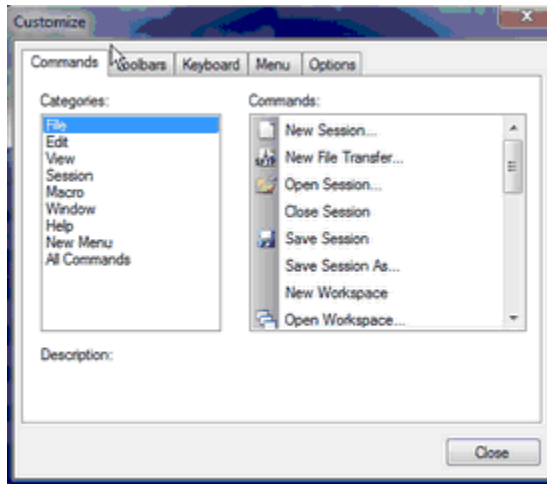
Set a toolbar into a customizable state by right-clicking on the toolbar options control at the end of the desired toolbar.



Then, select toolbar customization by clicking on the down triangle of "Add or Remove Buttons", then selecting customize.



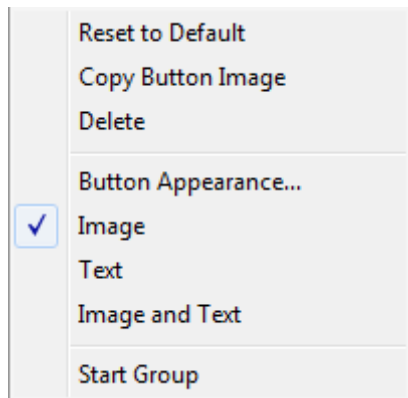
This will activate the Customize dialog:



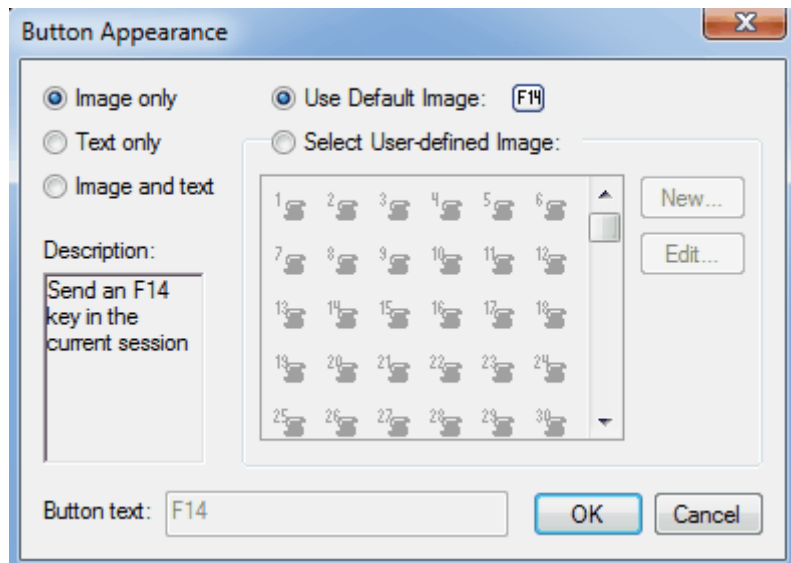
To modify an icon image, right-click on the particular icon you want to change:



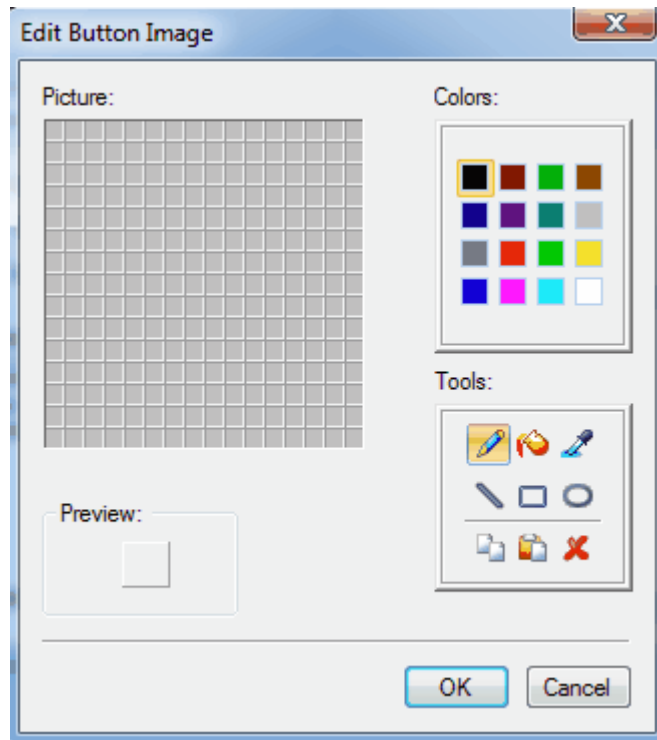
You will see the following menu:



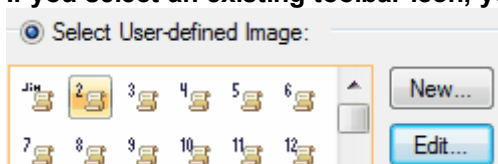
Select "Button Appearance" to see the button appearance frame:



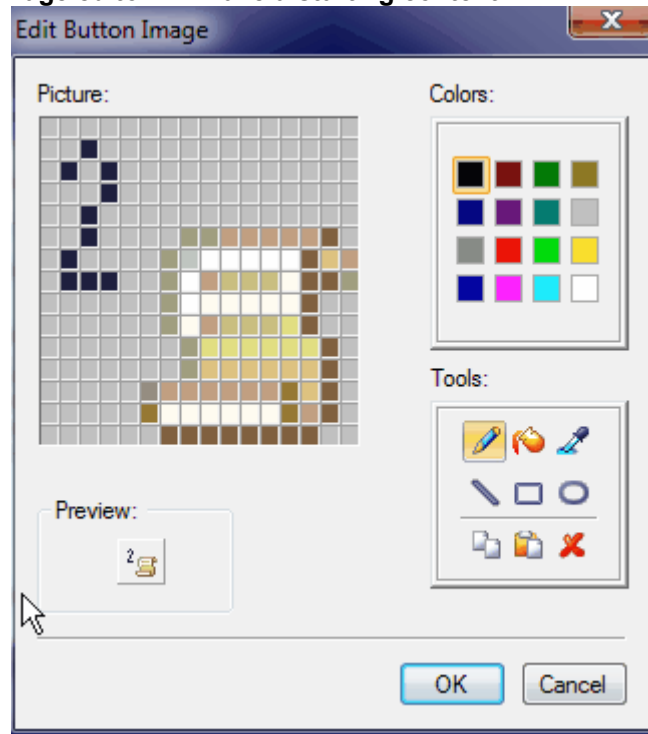
Select "Select User-defined Image" to enable the option "New".  
 If you select new, you will see the icon image editor:



**If you select an existing toolbar icon, you will have the option to edit the icon;**



and then the icon image editor will have a starting content:



## 5.10.6 Macro Toolbar

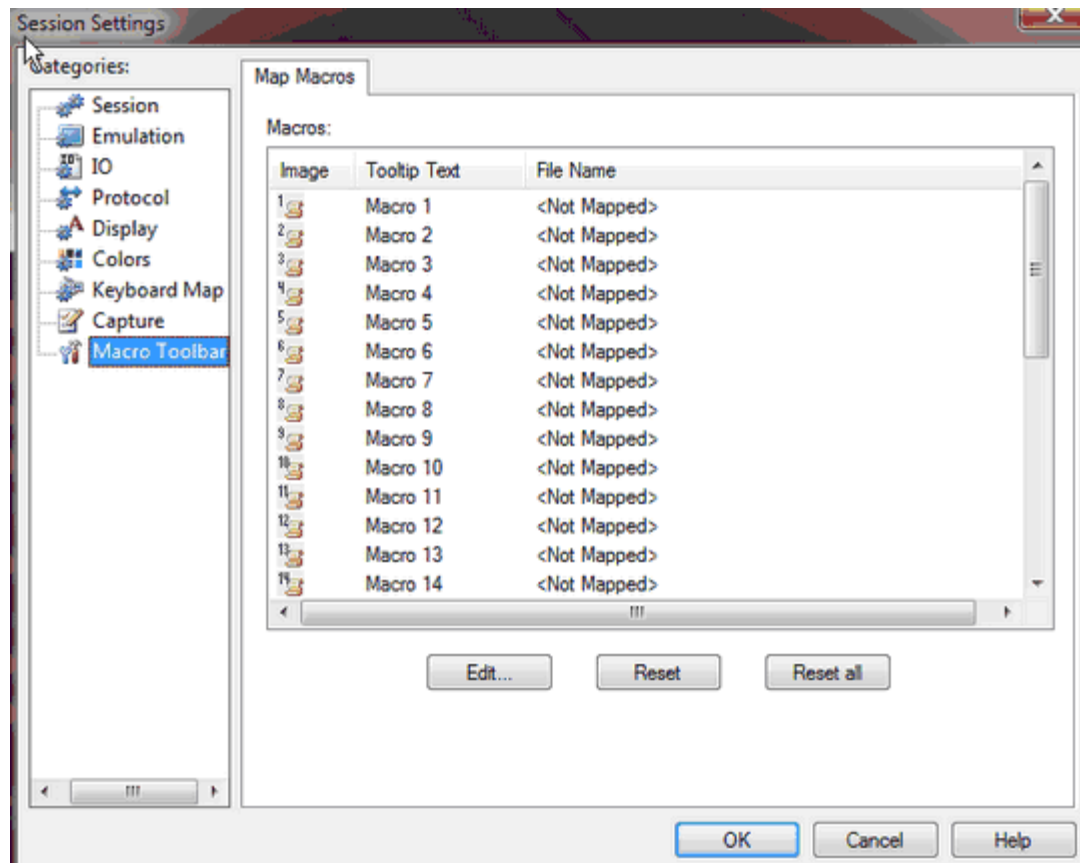
### Macro Toolbar

The Macro toolbar provides shortcuts to OutsideView Visual CommBASIC macros. (If you decide you'd rather map macros to keyboard shortcuts, see the [Mapping Macros](#) topic for instructions.)

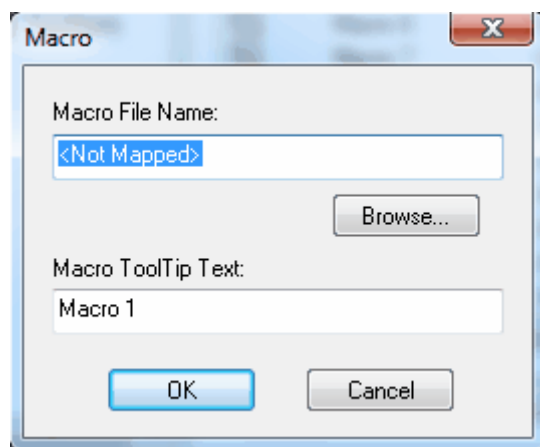
The Map Macros tab is accessed by accessing the Session Settings dialog and clicking on the Macro Toolbar category or selecting Macro/Map Macros/To Toolbar.... This tab displays the macro button assignments for the macro toolbar. The macro toolbar can have up to 20 macros mapped at one time. You can also use buttons from the macro toolbar on other custom toolbars. Once you've mapped a macro to a button, simply clicking the appropriate button will execute the macro.

To Map a Macro to a Macro Button:

1. Access the Map Macros tab by selecting Session/Session Settings..., selecting the Macro Toolbar category and clicking the Map Macros tab or by selecting Macro/Map Macros/To Toolbar...



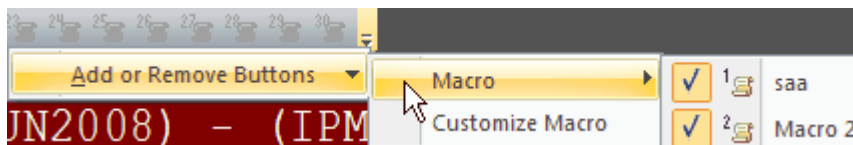
2. Select any unmapped buttons by clicking on the image in the leftmost column, and then click Edit (or double-click on the image)
3. A dialog will open that allows definition of the macro to be executed, and its ToolTip text. To modify the graphic used for the button, see the topic [Changing Icon Images](#).



4. Specify the macro to run when this button is clicked. You can use the Browse button to navigate to the desired macro file. Valid macro files will have a .vcb file extension.

5. Specify the ToolTip text. A ToolTip is a short reminder about what this button's macro does. In the main OutsideView window, holding your cursor over a button for a few seconds will display the button's ToolTip.

Once you've mapped the macro buttons, you can display just those macro icons which do have macros mapped to them. Click on the down glyph at the end of the macro toolbar and select add/remove buttons, Macro, and then check ON or OFF visibility for the various macro buttons:



## 5.11 Dynamic Input Assistance

### 5.11.1 Overview

#### Overview

Dynamic Input Assistance™ is a unique combination of capabilities that assist you in communicating more accurately, and more productively, with your NonStop host. You can quickly choose the Dynamic Input Assistance™ mode you wish to use, at a moment's notice. Dynamic Input Assistance capabilities, or modes, include:

#### In-line Editing

Entry of conversational mode input using a **text edit box**.

#### Command History

When typing conversational mode commands into your terminal emulation session, **Command History** mode will match what you are typing to what you have previously typed. OutsideView ships with (editable) default history files (per emulation type). These are copied into dynamic history files for each user. This provides each user with an immediate 'out-of-the-box' history list of common commands. As each user enters commands, they are added to each user's individual history file to create a personalized history. These history files are **persistent**; the information gathered in them will be available the next time you start OutsideView.

Our command history capability is **emulation sensitive** – so you see 6530 commands when in 6530 emulation, and VT type commands when in VT emulation. Our Command History mode is also **context sensitive**. That is, it recognizes command contexts. For instance, if you are in FUP you will only see commands entered within FUP. When at a TACL prompt, you will only be offered TACL commands. This focused delivery helps you receive precisely the information you need. OutsideView ships with (editable) default context files (per emulation type). These are copied into dynamic context files for each user. This provides each user with an immediate 'out-of-the-box' recognition of common contexts.

All Command History and command context files are **editable**. This means you can define new contexts unique to your organization, and otherwise tune these files' content to suit your needs and maximize their fit to your specific day-to-day work environment.

#### Spell Checking



Everyone is probably familiar with Spell checkers. OutsideView now contains a Spell checker that can use different language dictionaries, as well as editable custom dictionaries.

### **Command Auto-completion Assistance**

This sophisticated ability monitors conversational mode input and matches input against command utilities BATCHCOM, BIND, FTP, FUP, MEASCOM, PATHCOM, PERUSE, RJE CIR, SAFECOM, SCF, SPOOLCOM , and TMFCOM. You might think of it as being equivalent to having the reference manuals for these programs integrated into OutsideView. As you type commands, Command Completion will recognize the command being entered, and prompt you through entering proper parameters with proper syntax.

## **5.11.2 Quickly Changing your Dynamic Input Assistance Mode**

### **Changing your Dynamic Input Assistance Mode**

#### **Selecting your Dynamic Input Assistance Mode (Dynamic Input Configuration)**

Although OutsideView will have a default Dynamic Input Assistance mode, at times you may want to use other modes. To change which mode of Dynamic Assistance is active at a particular time (without changing your default settings):

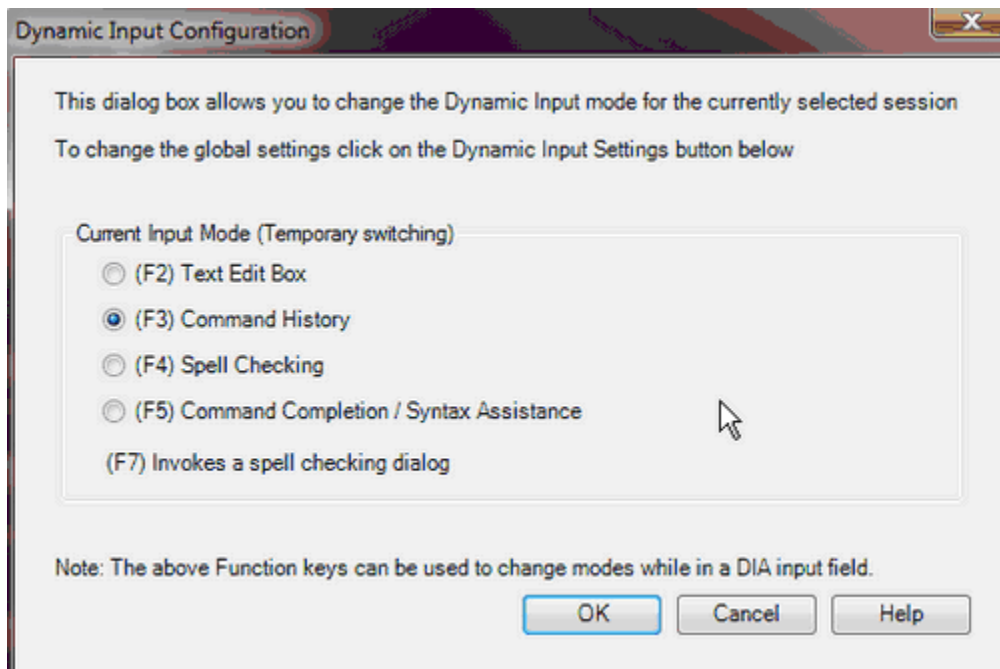
While your cursor is in the DIA area,

- press F1 to activate the Dynamic Input Configuration dialog
- press F2 to enter Text Edit mode
- press F3 to enter Command History mode
- press F4 to enter Spell Check mode
- press F5 to enter Command Completion mode
- press F7 to 'quick-call' the spell check function

#### **Dynamic Input Configuration**

There are 3 different ways to access the Dynamic Input Configuration screen:

-  Click on the toolbar icon
- Select Session, Dynamic Input Settings from the OutsideView menu
- From within any DIA area, press the F1 function key



### 5.11.3 Configuring Dynamic Input Assistance Defaults

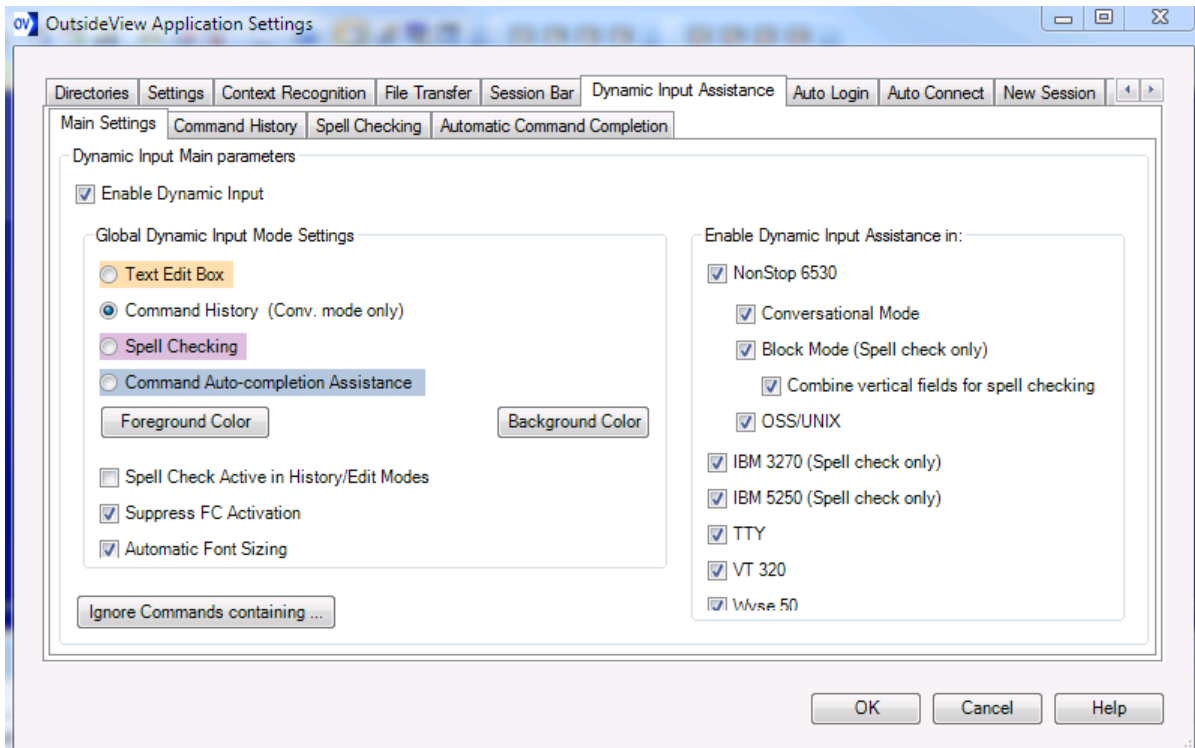
#### Dynamic Input Assistance™ Default Settings

To set your default Dynamic Input Assistance settings;

- Select Edit, Application Settings, and the Dynamic Input Assistance tab.

#### 5.11.3.1 Dynamic Input Assistance - Main Settings


##### Dynamic Input Assistance - Main Settings




**Enable Dynamic Input** turns Dynamic Input Assistance on and off (persistently).

**Temporary Suppression of Dynamic Input Assistance**

At times, you may find it temporarily convenient to suppress Dynamic Input Assistance. To momentarily disable/enable Dynamic Input Assistance;

- click on the tool bar icon .
- Select Session, Dynamic Input On/Off

When active, the Dynamic Input section of the toolbar will look like 

When suppressed, the Dynamic Input section of the toolbar will look like 

**Global Dynamic Input Mode** lets you set the **default** Dynamic Input Assistance mode. (You can also ‘toggle’ quickly between modes)

To assist users in quickly recognizing the active Dynamic Input Assistance mode, there are different default background hues for the various input modes. Users may also redefine these colors values, using the buttons



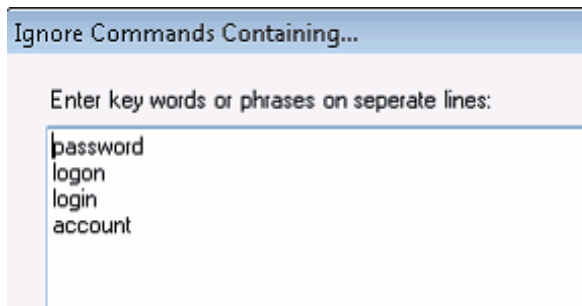
**Spell Check Active in History/Edit Modes** lets you enable spell checking in combination with other input modes.

**Suppress FC Activation** prevents the Dynamic Input text edit box from activating when the active command is FC.

**Automatic Font Sizing** causes OutsideView to set the font within the Dynamic Input Assistance frame to a close approximation of the screen font size.

**Command History gives all history** when checked ON removes context awareness of command history and provides a global history list.

**Ignore Commands containing...** lets you enter words or phrases which, if contained anywhere within a command, tell the history function to ignore the entire command. For instance, a default 'ignore string' is password – so any command containing 'password' will be entirely ignored.



Ignore Commands Containing...

Enter key words or phrases on separate lines:

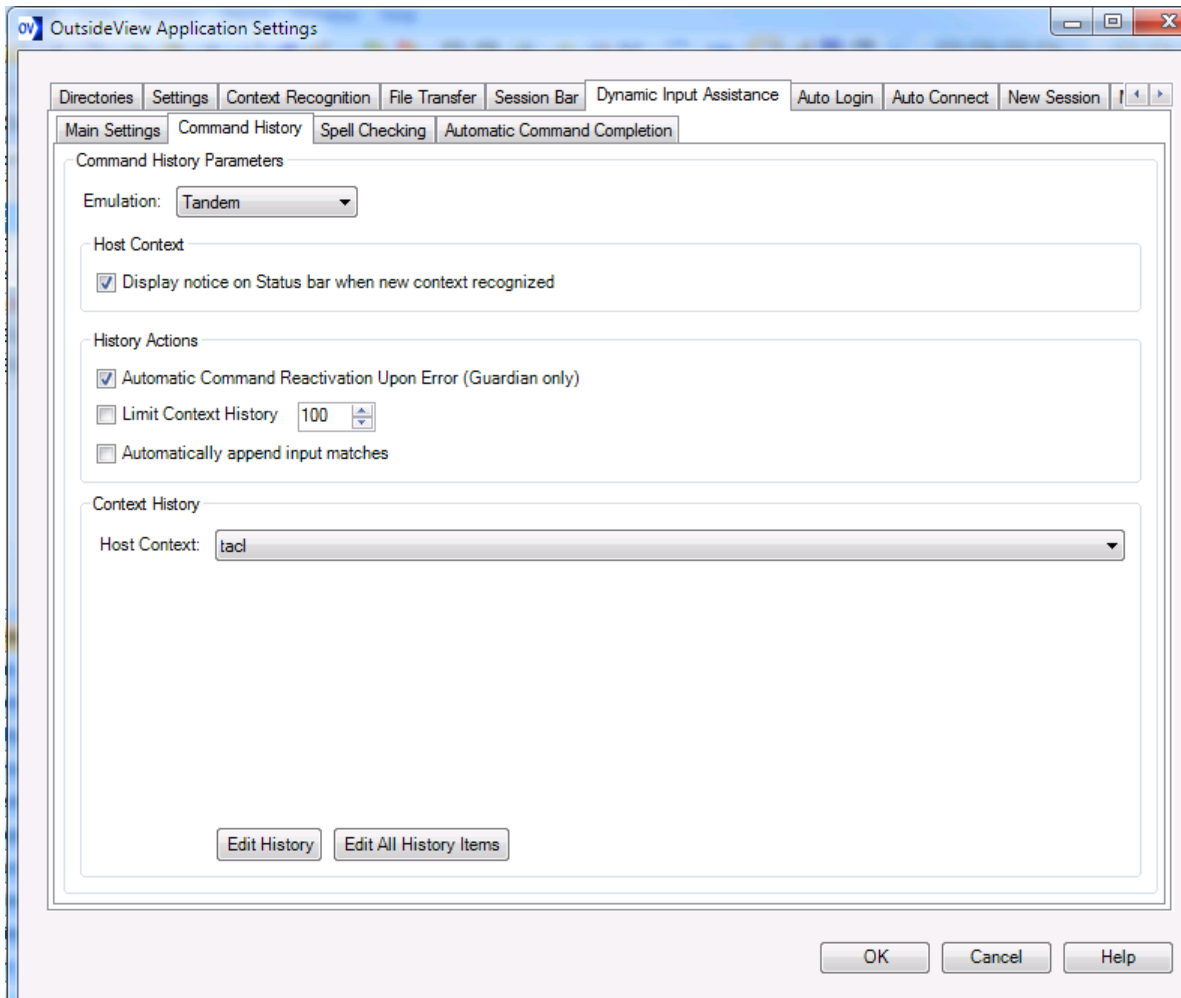
password  
logon  
login  
account

The '**Enable Dynamic Input Assistance in**' section lets you choose which emulations utilize Dynamic Input Assistance.

After making changes to any of these settings, you may press Cancel to abandon your changes, or OK to store your changes. Stored settings changes take effect immediately.

### 5.11.3.2 Dynamic Input Assistance - Cmd History

#### Dynamic Input Assistance - Cmd History



The Command History function is **emulation sensitive** and **context sensitive**. It can recognize various command utilities and environments, and store history in association with those environments. This means efficient and focused delivery of command history. Command history is stored, per user, and is persistent from session to session. History lists and context specific lists can be edited and maintained individually or automatically distributed using OutsideView's Enterprise mode.

For instance, the files `DefaultTandemContext.config` and `DefaultTandemHistory.config` are created automatically by OutsideView. These files can be directly edited using an XML editor. As a user works with OutsideView, context and command history data are accumulated into dynamic, individual files, such as `TandemContext.config` and `TandemHistory.config`. These files, too, can be directly edited with an XML editor.

Notes on Command History files;

- OutsideView comes with pre-populated 'starter files' for History and Context (i.e. `DefaultTandemContext.config` and `DefaultTandemHistory.config`). These files can be edited to reflect individual organization's needs.
- When a user first starts OutsideView, the 'starter files' are copied to individual user files (i.e. `TandemContext.config` and `TandemHistory.config`). The individual user files are dynamic, and store individual user's activities to provide personalization for each user. These files can also be edited, via our GUI, or using an XML editor.

### Command History Parameters

**Emulation** choice box defines which History and Context files are active (for editing) in the dialog.

**Display notice on Status bar when new context recognized** causes OutsideView to post a message to the status bar as it recognizes a context. For instance: `DIA: osh for command history mode`

### History Actions

**Automatic Command Reactivation upon error** When this option is active, a command that has resulted in an error response from the host will be automatically re-input, ready for editing

**Limit Context History** lets a user set a limit on the depth of the command history list, so that it contains only the specified number of most recently used commands.

### Automatically append input matches

If this option is **on**, then the first match is mirrored into the command line as you type. For instance, the input here is `va` and the first match is echoed to the input line. A down-cursor can override this selection.



If this option is **off** (the default setting), then historical matches are only sent to the input line when selected (by a down-cursor). For instance, the input here is `va` and only `va` shows on the input line.



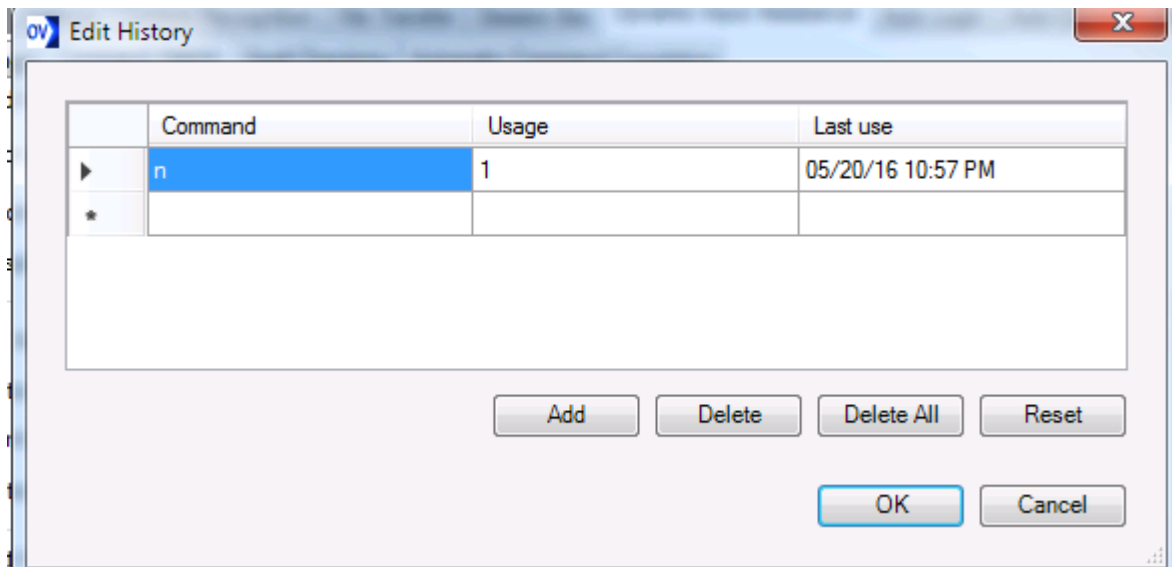
In both cases, commands remain editable when echoed to the command line until selected by clicking or pressing Enter.

### Context History

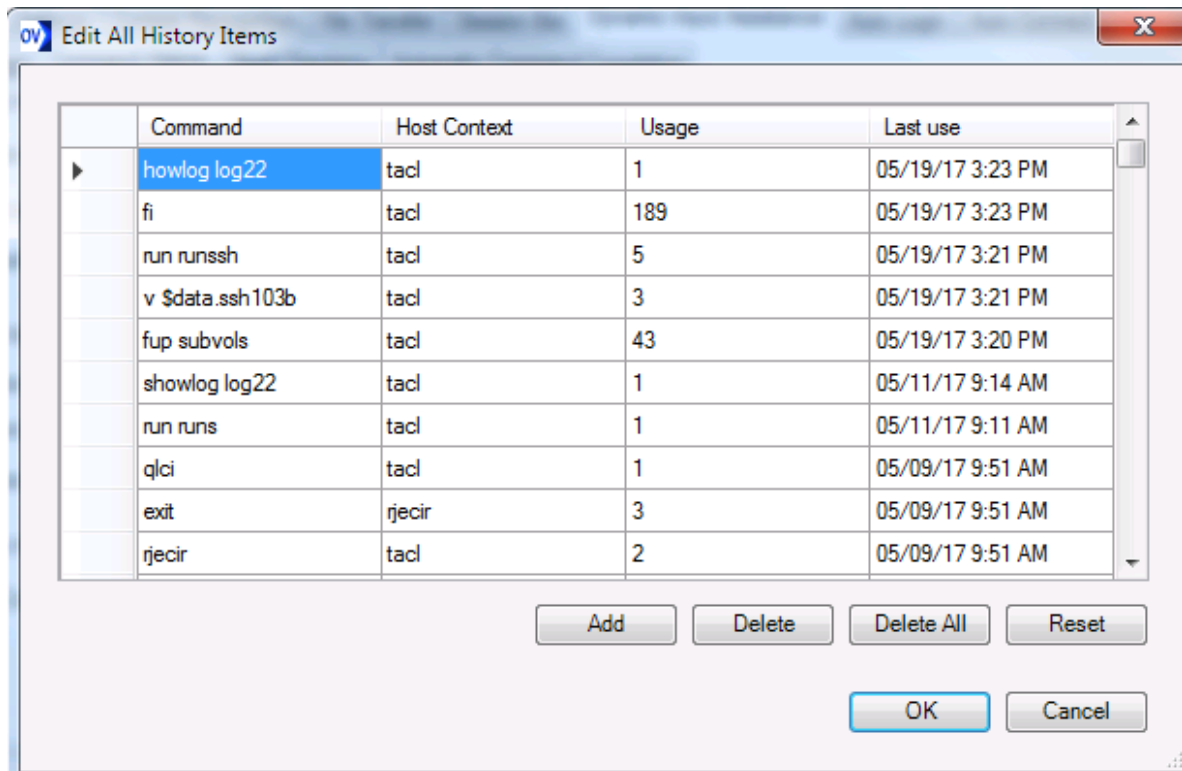
**Host Context** choice box lets you select a particular context of interest

**Edit Context List** opens the context file (for selected Emulation type) so you can define contexts and utilities in the dynamic XML file. OutsideView comes with many Tandem contexts pre-defined in a default file; this permits per-user modification to match your specific environment and usage. Additional contexts can be defined using regular expressions.

**Edit History** will give you an edit window into the command history of the **active Host Context**

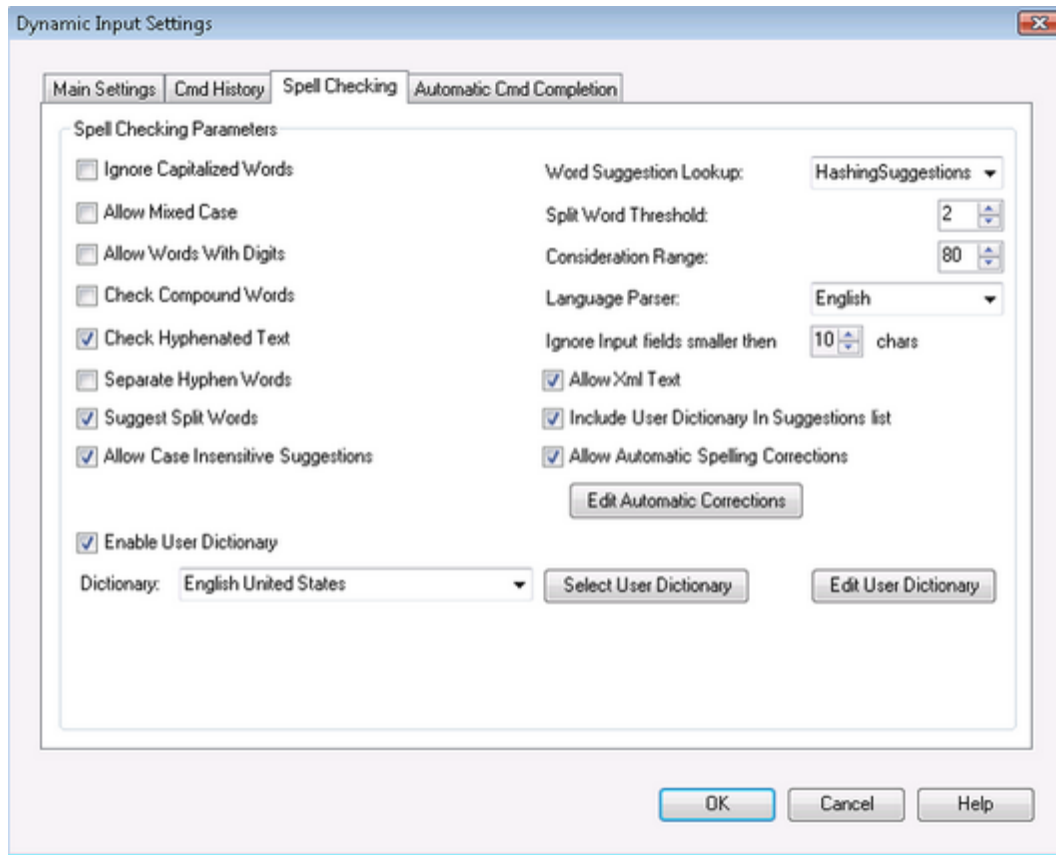


**Edit All History Items** lets you edit the entire history list (**for all contexts**) of the selected emulation type.




### 5.11.3.3 Dynamic Input Assistance - Spell Checking

#### Dynamic Input Assistance - Spell Checking

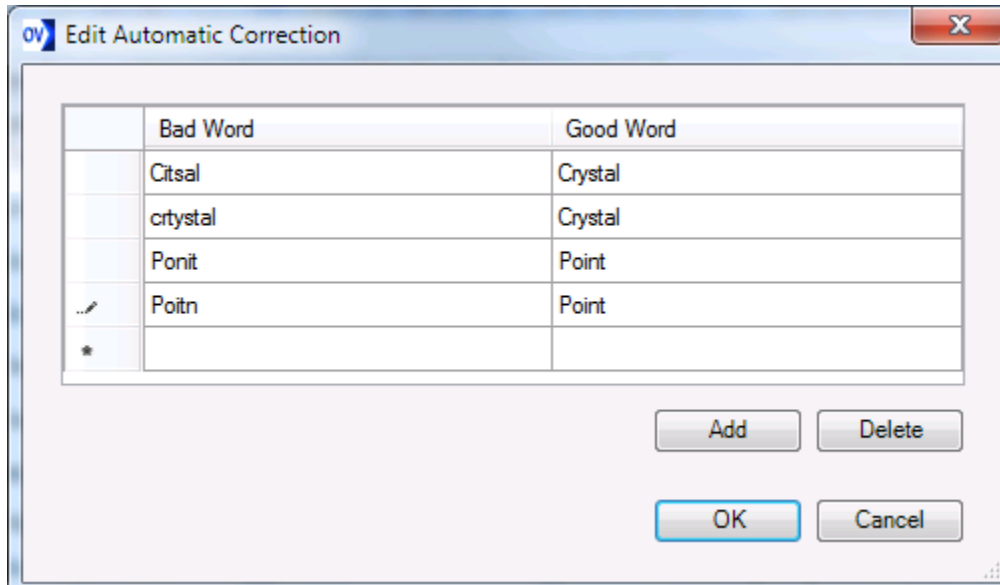


**Spell Checking Parameters** on the Spell Check tab of the Dynamic input Settings dialog let you tune performance of your Spell Checker, as desired, including choosing appropriate dictionaries, and editing custom dictionaries.


'Hover' your mouse over various input fields and switches of this dialog to receive field-by-field information.

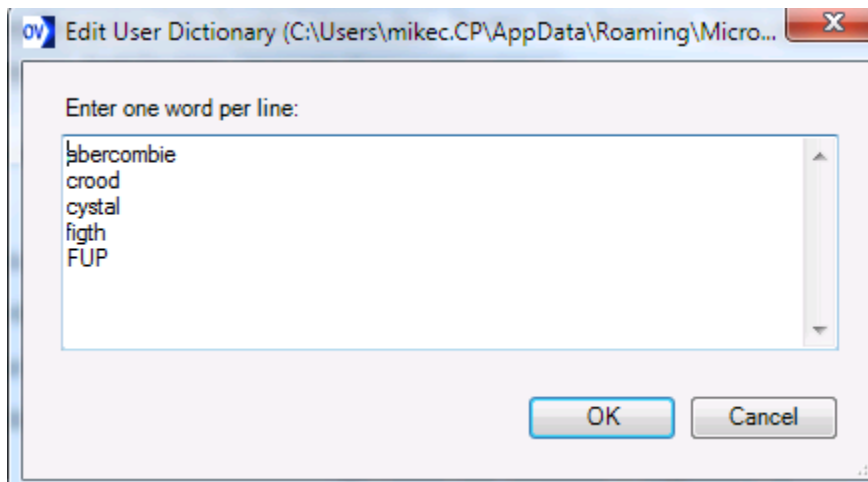
Select  to create or edit your list of corrections:






**Enable User Dictionary**, when checked, activates the specified user dictionary. By default, the Spell Checker uses a Microsoft Custom dictionary. To specify a different user dictionary, click on 

To edit the selected user dictionary, click on 

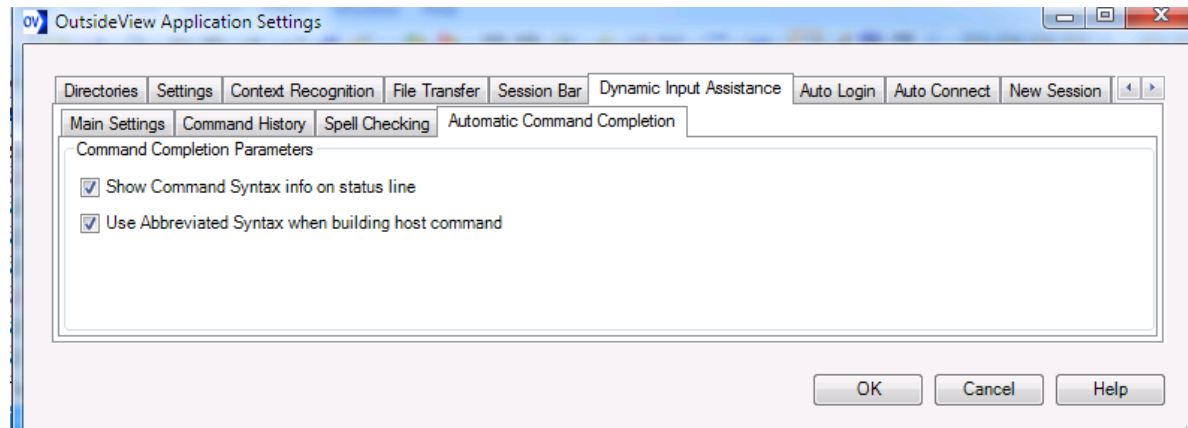


### Spell-checking in Block Mode

In block mode operation, you may click on the  spell-check icon, or select Session, Spell Check Input Field(s) to perform a spelling check on all contiguous, identically sized and vertically aligned block mode fields (such as comment block or a single Tedit screen). While active, you may correct individually-highlighted words. When your review and corrections are complete, press the **TAB** key to accept the spell-check results and redraw the fields with their corrected content. Press the **Esc** key, if you wish to abandon the spell checking process.

### 5.11.3.4 Dynamic Input Assistance- Command Auto-completion Assistance

#### Dynamic Input Assistance - Automatic Command Completion



**Show Command Syntax info on status line** when checked, will display syntax prompt information in the session status line. `Syntax: FUP ALTER filename , alter-option { , alter-option}...`

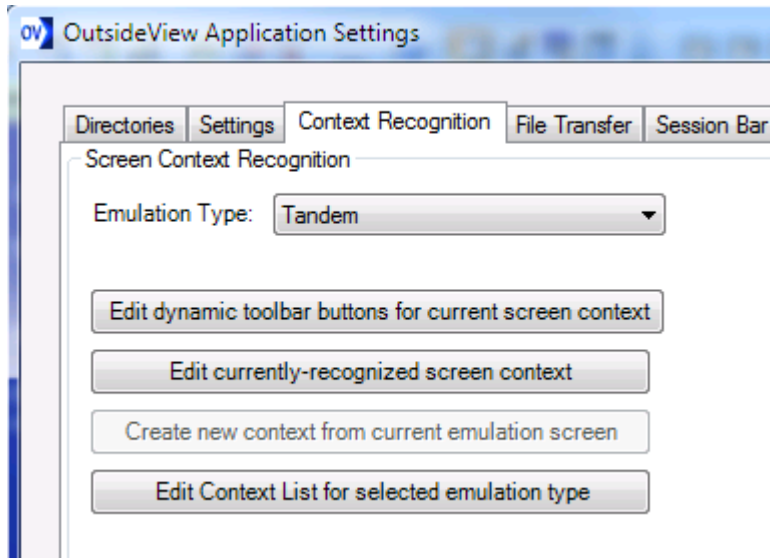
**Use Abbreviated Syntax** when checked, enables abbreviated input:

**Show Small Syntax Tool Tip** when checked, will display a syntax hint box when you 'hover' your mouse over the input area.

Notes on Command Completion files

Command completion XML/XSD files are located in the CLIPS directory (C:\Program Files\Crystal Point\OutsideView\CLIPS) and may be edited by advanced users. Additional command-completion files will be developed by Crystal Point over time, and made available for download to extend the Command completion scope. OutsideView contains assistance files for BATCHCOM, BIND, FTP, FUP, MEASCOM, PATHCOM, PERUSE, RJEICIR, SAFECOM, SCF, SPOOLCOM and TMFCOM.

## 5.12 Context Recognition



Context Recognition gives OutsideView the capability to track [command history](#), or to display [dynamically labeled function key toolbars](#)

### 5.12.1 Creating New Contexts

An easy way to create new contexts is to navigate into an unknown context. Upon entering an unknown context, OutsideView will display the following message on the status line;

`DIA: [Unknown] (Dynamic Input Assistance disabled)`

From this unknown context, right-click in the dynamic toolbar area, and select "Create New Context" to see the Visualize Screen Layout dialog.

Another way to access the Visualize Screen Layout dialog is from Edit, Application Settings, Context

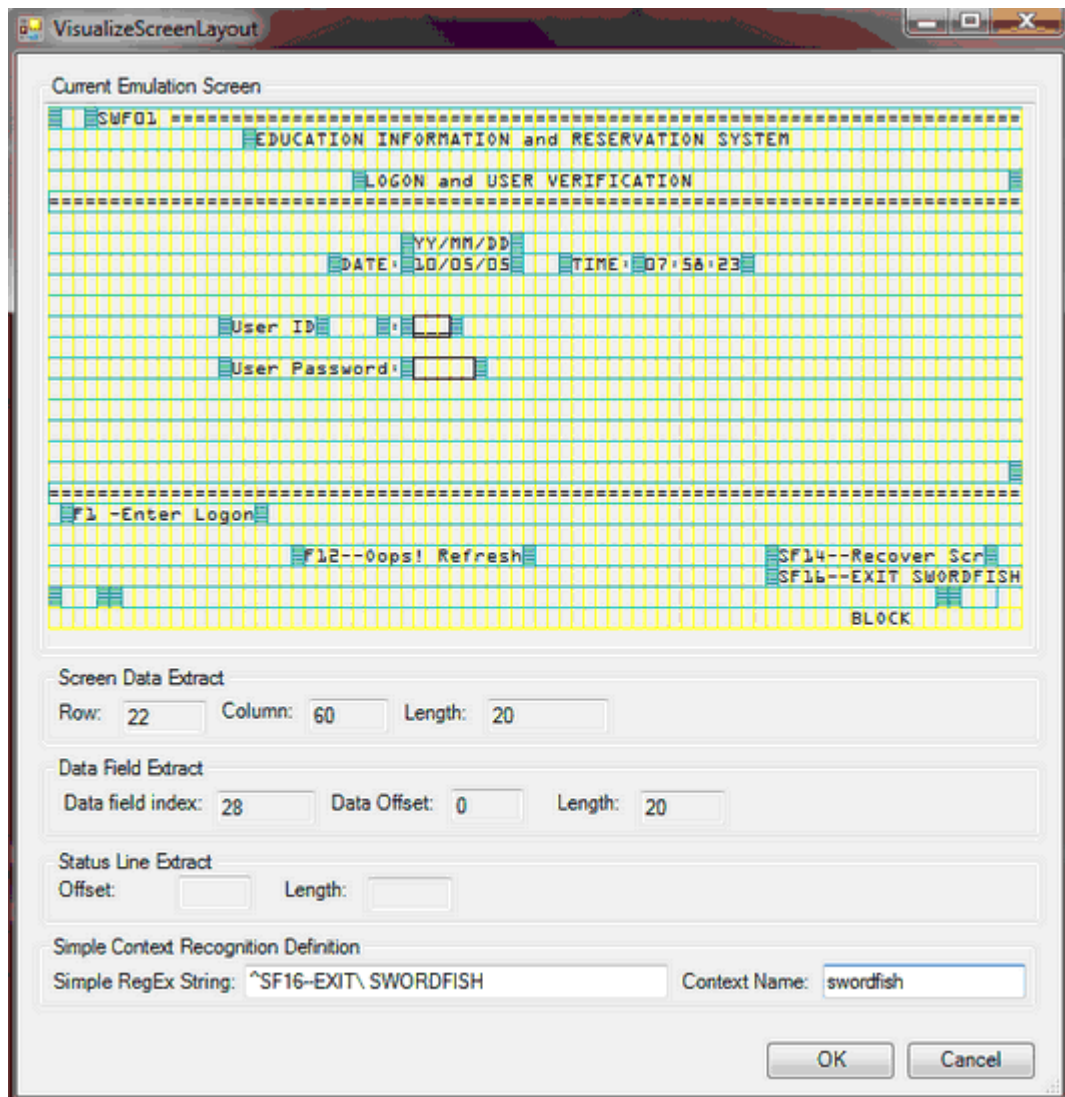
Recognition, and either

`Edit currently-recognized screen context`

or

`Create new context from current emulation screen`

The Visualize Screen Layout dialog permits defining a context through screen contents, data field contents, status line content, or a regular expression. Here, for instance, a portion of the screen that is static (identical on all screens of this application) is used to identify a context.



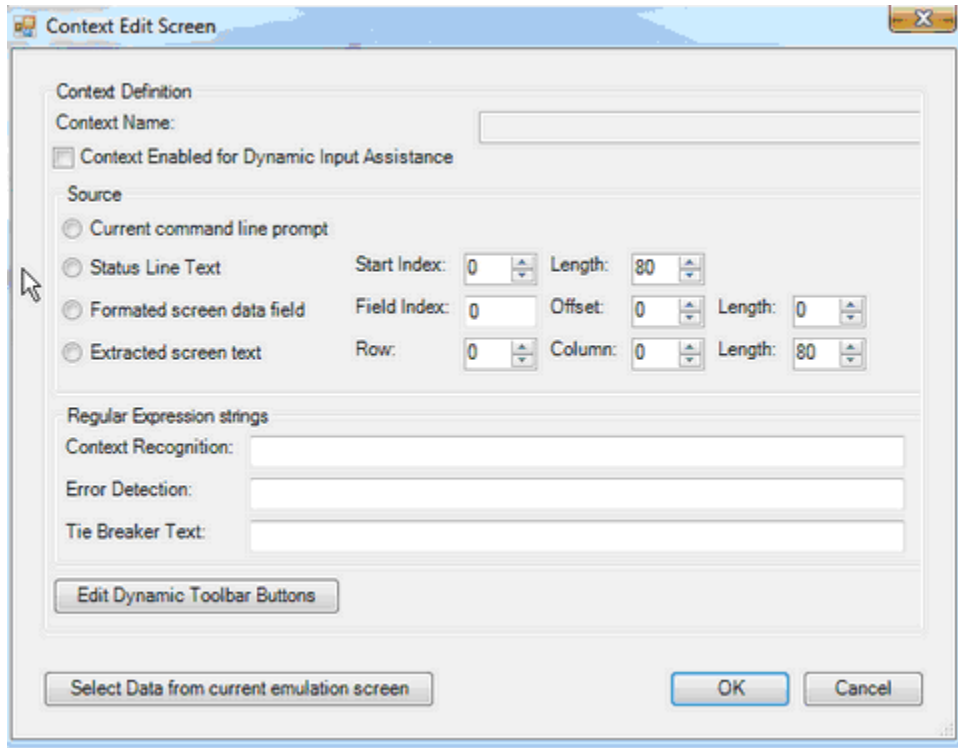
NOTE: The example above is from a block mode application. To define a block mode application as a context, you must either identify a specific area of the screen that is constant across all screens (and unique to the application), or define each screen(s) individually as contexts in their own right.

The choices made from the Visualize Screen Layout dialog feed into the Context Edit Screen.

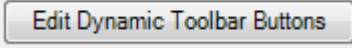
### 5.12.2 Editing Contexts


While in a recognized context, select Edit, Application Settings, Context Recognition,

to see the Context Edit screen.




Here you may change some settings directly,


or select  to edit [dynamic toolbar labels](#)

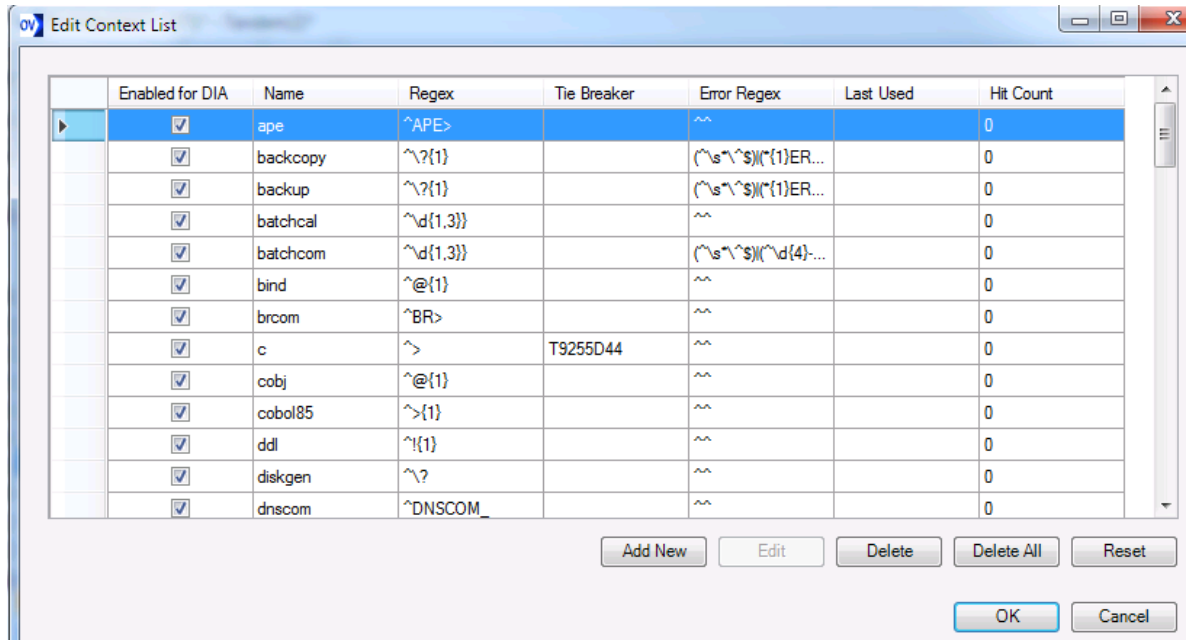
or select  to see the [VisualizeScreenLayout](#) dialog. Data from the Visualize Screen Layout dialog will feed back into the Edit context screen.

### 5.12.3 Editing Context List

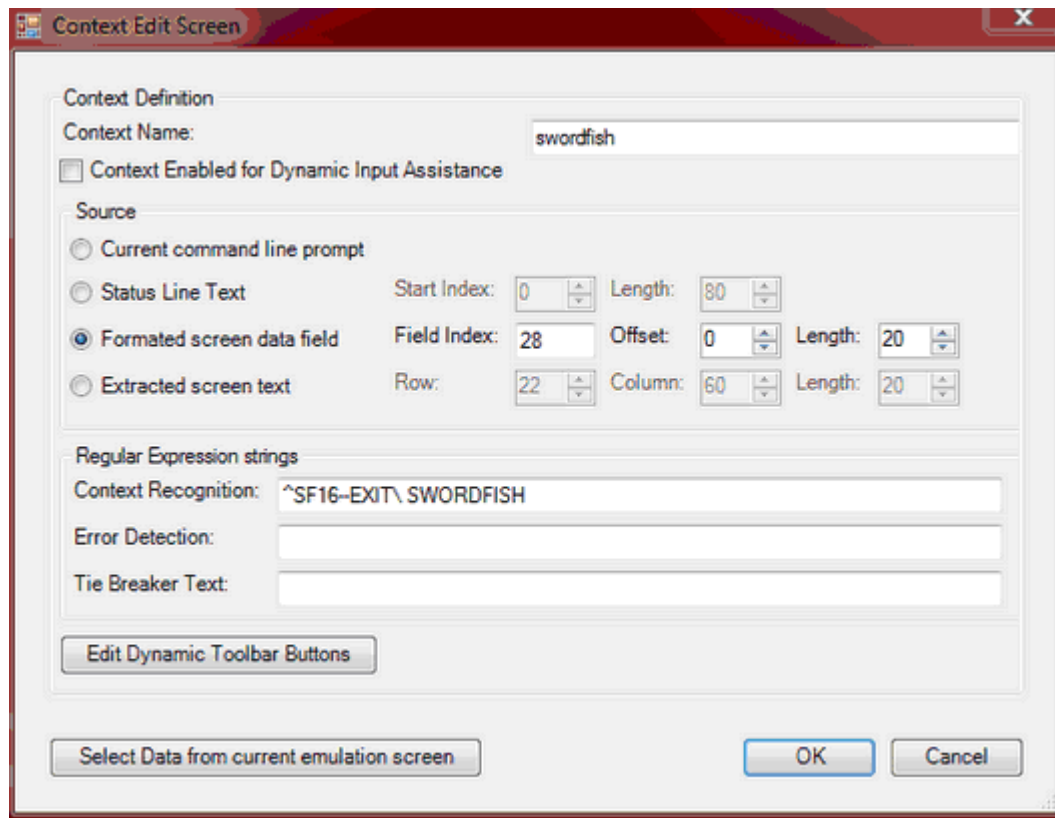
The Edit Context List dialog provides a general method for adding, deleting or editing the regular expressions of command prompts in order to identify various contexts. The overall context recognition list can be accessed by selecting Edit, Application Settings, Context Recognition tab.

There, select an **Emulation Type:** 

and then  to see the following dialog:



Select a given row (context) and select Edit to see the Context Edit dialog



NOTE: There is an option to have this context enable Dynamic Input Assistance (or not).

Once the context is known, the status line will indicate that when first entering the context:

DIA: [swordfish] for command history mode

#### 5.12.4 Context-Sensitive Toolbars

Users may define custom labels for their function keys, that will vary dynamically through context recognition.

For more information on defining contexts, see the topic [Context Recognition](#)

When an OutsideView session enters a new context, that information is displayed in the lower left corner of the status line. For example, here is the message when OutsideView first enters FUP:

DIA: [fup] for command history mode

Automatically responding to recognition of a context, OutsideView will display a dynamic toolbar. The content of that dynamic toolbar is, by default, blank.

To modify the function keys labels, either select Edit, Default Application Settings, Context

Recognition tab, [Edit dynamic toolbar buttons for current screen context](#) or right-click in the Dynamic Toolbar Area, and select Edit Button Values

Dynamic Toolbar Edit

Dynamic Toolbar Values

1-8 9-16 17-24 25-32

	Button label	Command Text	Action Key	Tool Tip Text
#1	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#2	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#3	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#4	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#5	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#6	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#7	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#8	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>

Reset to Default Erase Values OK Cancel

Edit the key labels as you wish:

Dynamic Toolbar Edit

Dynamic Toolbar Values

1-8 9-16 17-24 25-32

	Button label	Command Text	Action Key	Tool Tip Text
#9	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#10	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#11	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#12	Refresh	<input type="text"/>	F12 ▾	F12 to Refresh screen
#13	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#14	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#15	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>
#16	<input type="text"/>	<input type="text"/>	NONE ▾	<input type="text"/>

Reset to Default Erase Values OK Cancel



Accepting Keyboard Input with Function Keys.

The following is an example of a function key that accepts input. It reads "Logon (pipe symbol)". If you enter Command Text, there is an implied Enter. If you select a function, it will override the implied Enter. If you Enter Command Text ending in a pipe symbol, there is no implied Enter.

	Button label	Command Text	Tool Tip Text
#1	LOGON	LOGON	NONE

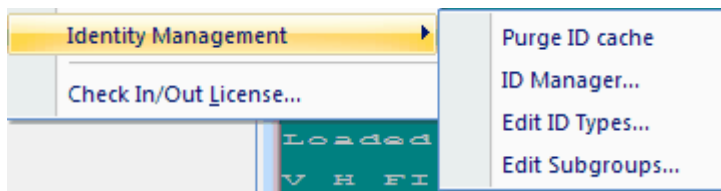
## 5.13 Identity Management

Identity Management is a labor-saving mechanism to reduce redundant or repetitive logging in throughout the day. By associating all session files using the same credentials with the same "ID Type" users will be prompted once for their credentials, and all subsequent sessions of the ID Type that are opened or reconnected will be logged in automatically. For instance, if you open a workspace containing 12 sessions, and all 12 sessions specify the same ID type, you would need to supply your credentials only once for all 12 sessions to be logged in. If you were to close and reopen that workspace, you would be automatically re-logged in to all 12 sessions without having to provide your credentials again.

For information on specifying an ID Type in a session, see the topic [Identity Caching](#)

The credentials for each ID Type must be supplied the first time by the user, and are then stored (encrypted) in RAM until OutsideView is terminated, or until the ID Cache is purged (Edit | Identity Management | Purge ID Cache).

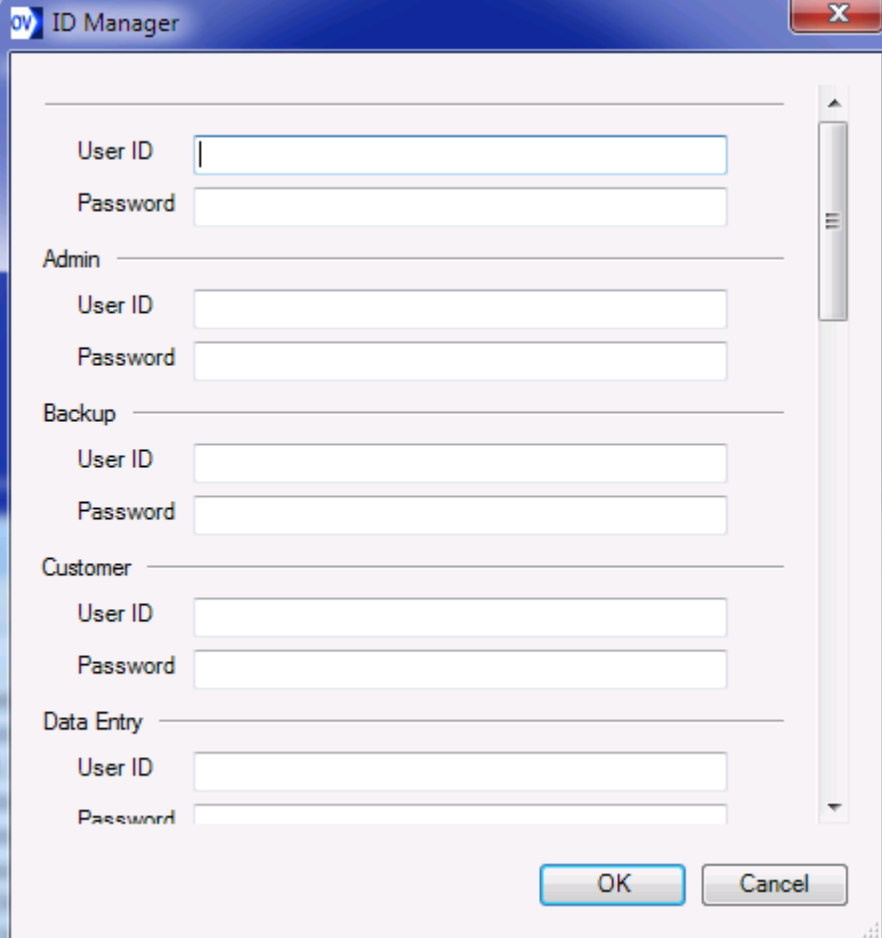
The cached user credentials, and various ID types may be controlled by selecting the menu choice Edit | Identity Management.



You may:

- Purge all user credentials in cache.
- Enter the ID Manager
- Add or Delete ID Types
- Add or Delete Subgroups

The ID Manager is also accessible from right-clicking in the Session Bar. It allows multiple ID Type credentials to be entered or changed.



The screenshot shows a dialog box titled "ID Manager" with a blue header bar. The dialog contains several sections, each with a "User ID" and "Password" field. The sections are: "Admin", "Backup", "Customer", and "Data Entry". Each section has a horizontal line above its fields. At the bottom right, there are "OK" and "Cancel" buttons. A vertical scrollbar is visible on the right side of the dialog.

### 5.13.1 Simple Logons

#### Simple Logons

In most scenarios, Identity Management is quite straightforward. For instance, to log in to a TACL service, you specify a User ID type, provide a user id and password when prompted by Identity Manager, and thereafter ID Manager will log you in automatically to all sessions with that ID Type.

**IdentityCacheID**

Name: NonStop User

Pre-Login required (NonStop Conv only)

Pre-Login Name: [Dropdown]

**Login Function Key**

Emulator Type: NA

Login Function Key String: [Dropdown]

Visible

**Field 1**

Field 1 Label: User ID

Visible  Sensitive Input Field  Required Entry

**Field 2**

Field 2 Label: Password

Visible  Sensitive Input Field  Required Entry

**Field 3**

Field 3 Label: [Text]

Visible  Sensitive Input Field  Required Entry

**Field 4**

Field 4 Label: [Text]

Visible  Sensitive Input Field  Required Entry

**Field 5**

Field 5 Label: [Text]

Visible  Sensitive Input Field  Required Entry

**Field 6**

Field 6 Label: [Text]

Visible  Sensitive Input Field  Required Entry

**Login Over-Rides**

Login split between formatted pages or panels

Match Formatted Input Field Prompts

**Application Startup**

Send Application Startup command on initial screen

Command: [Text]

Reset OK Cancel

## 5.13.2 Multiple Logon Screens

### Multiple Logon Screens

Some logon scenarios may be more complex. For instance, you may need to login to Safeguard prior to logging in to your application. In this situation, you can 'nest' logins by defining one ID type to follow a prior one.

Below, we illustrate creating an ID Type named Safeguard;

ov Add Identity Cache ID Item

IdentityCacheID

Name

Pre-Login required (NonStop Conv only)

Pre-Login Name

Login Function Key

Emulator Type

Login Function Key String

Visible

Field 1

Field 1 Label

Visible  Sensitive Input Field  Required Entry

Field 2

Field 2 Label

Visible  Sensitive Input Field  Required Entry

Field 3

Field 3 Label

Visible  Sensitive Input Field  Required Entry

Field 4

Field 4 Label

Visible  Sensitive Input Field  Required Entry

Field 5

Field 5 Label

Visible  Sensitive Input Field  Required Entry

Field 6

Field 6 Label

Visible  Sensitive Input Field  Required Entry

Login Over-Rides

Login split between formatted pages or panels

Match Formatted Input Field Prompts

Application Startup

Send Application Startup command on initial screen

Command:

Reset OK Cancel

Then, we create another ID Type, named Application.

**Note** that this ID Type says it requires pre-login by the ID Type Safeguard.

The screenshot shows the 'Add Identity Cache ID Item' dialog box. The 'IdentityCacheID' section is configured with Name: application, Pre-Login required (NonStop Conv only) checked, and Pre-Login Name: Safeguard. The Login Function Key section has Emulator Type: NA, Login Function Key String: (empty), and Visible: unchecked. Field 1 is labeled 'User ID' and is visible, sensitive, and required. Field 2 is labeled 'Password' and is visible, sensitive, and required. Fields 3, 4, 5, and 6 are empty and not visible, sensitive, or required. The Login Over-Rides section has both options unchecked. The Application Startup section has 'Send Application Startup command on initial screen' unchecked and a Command field. Buttons for Reset, OK, and Cancel are at the bottom.

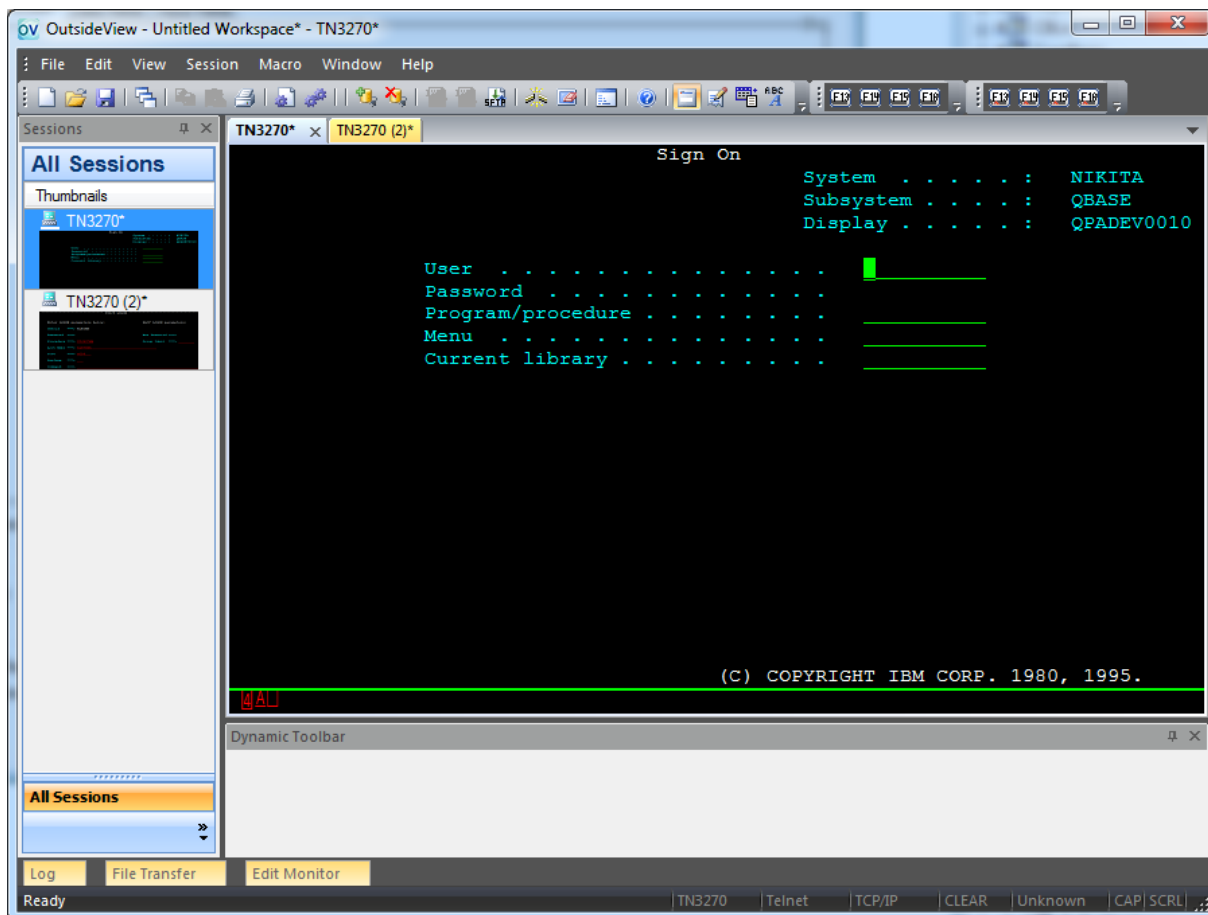
Configure the session file to connect to the host and port for Safeguard, specifying an ID Type 'Application'.

When opened, that session will prompt you for your Safeguard credentials and your Application credentials, connect to the Safeguard address and enter the Safeguard credentials, then automatically enter the application credentials at the next screen.

### 5.13.3 Complex Multiple Formatted Logon Screens

#### Multiple Formatted Block Mode Logon Screens

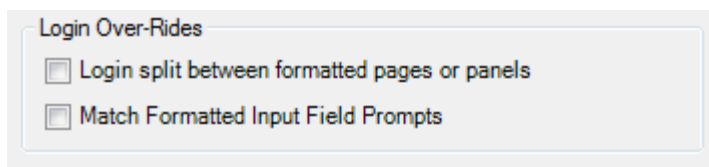
The default logic for formatted block mode screens is to look for a screen that has two input fields where the second field is a no echo input field for the password. The example screen below meets these criteria, and our standard pre-configured ID Types would work well here.



There are a wide variety of possible logon scenarios. Identity Management is engineered to support virtually all scenarios. If a host splits the login functionality between multiple screens, then ID Types must be created or configured to operate across multiple formatted screens.

To create or edit ID Types, select Edit | Identity Management | Edit ID Types, and then choose either Add or Edit.

Notice the Settings Category Login Over-Rides. These are the switches that enable more complex login behaviors.

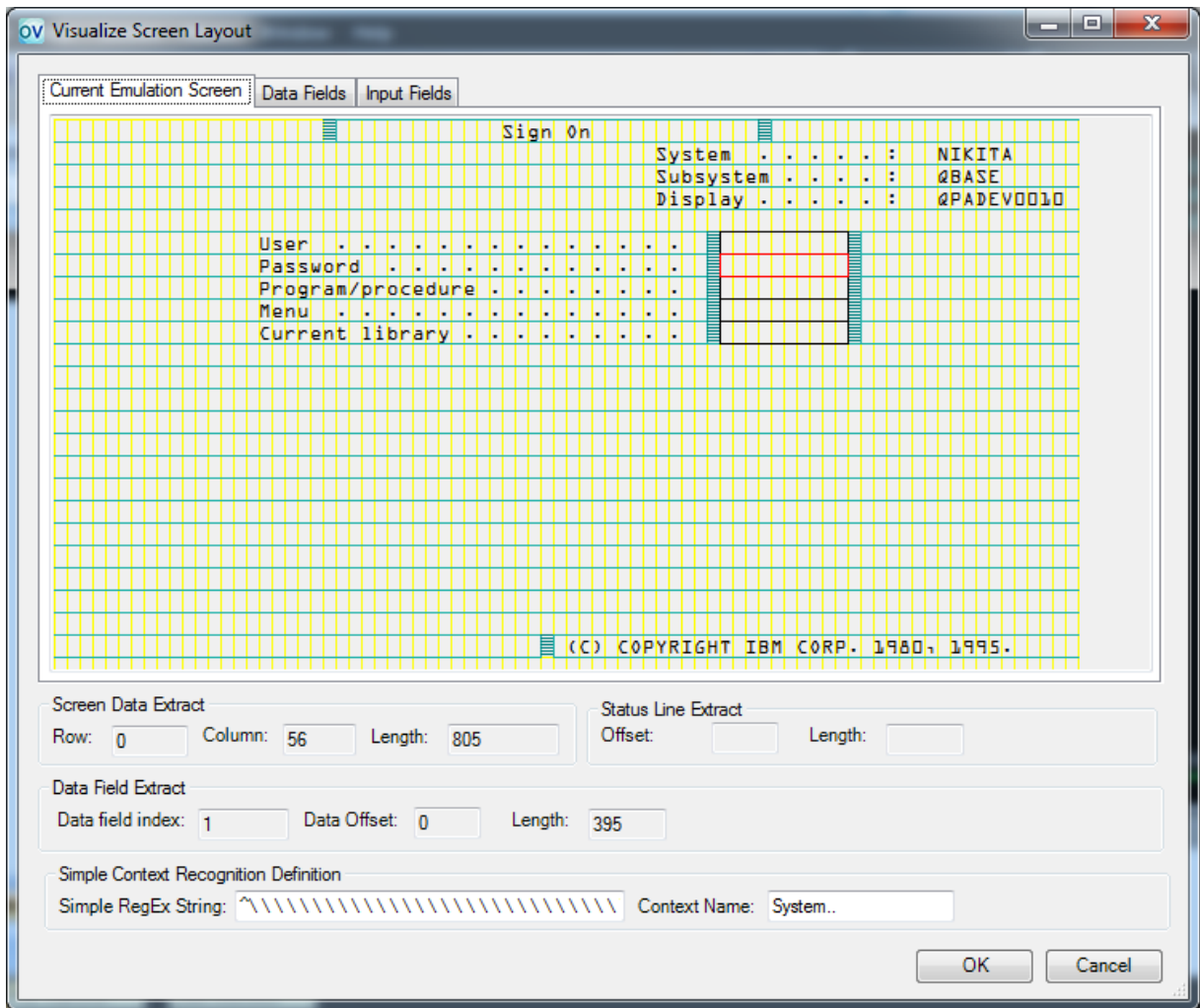
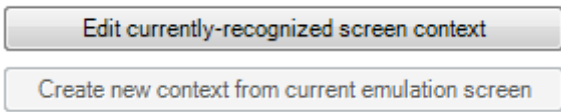


The switch for “Login split between formatted pages or panels” alerts the ID Manager to remain active across multiple block mode screens. (Since this is a frequent requirement in IBM environments, this switch is described in IBM terminology.)

The setting of “Match Formatted Input Field Prompts” will cause ID Manager to ignore the order in which input fields are listed within an ID Type and look instead for a match between the ID Type’s field label and the host prompt - in whichever order it occurs, and on whichever screen it occurs.

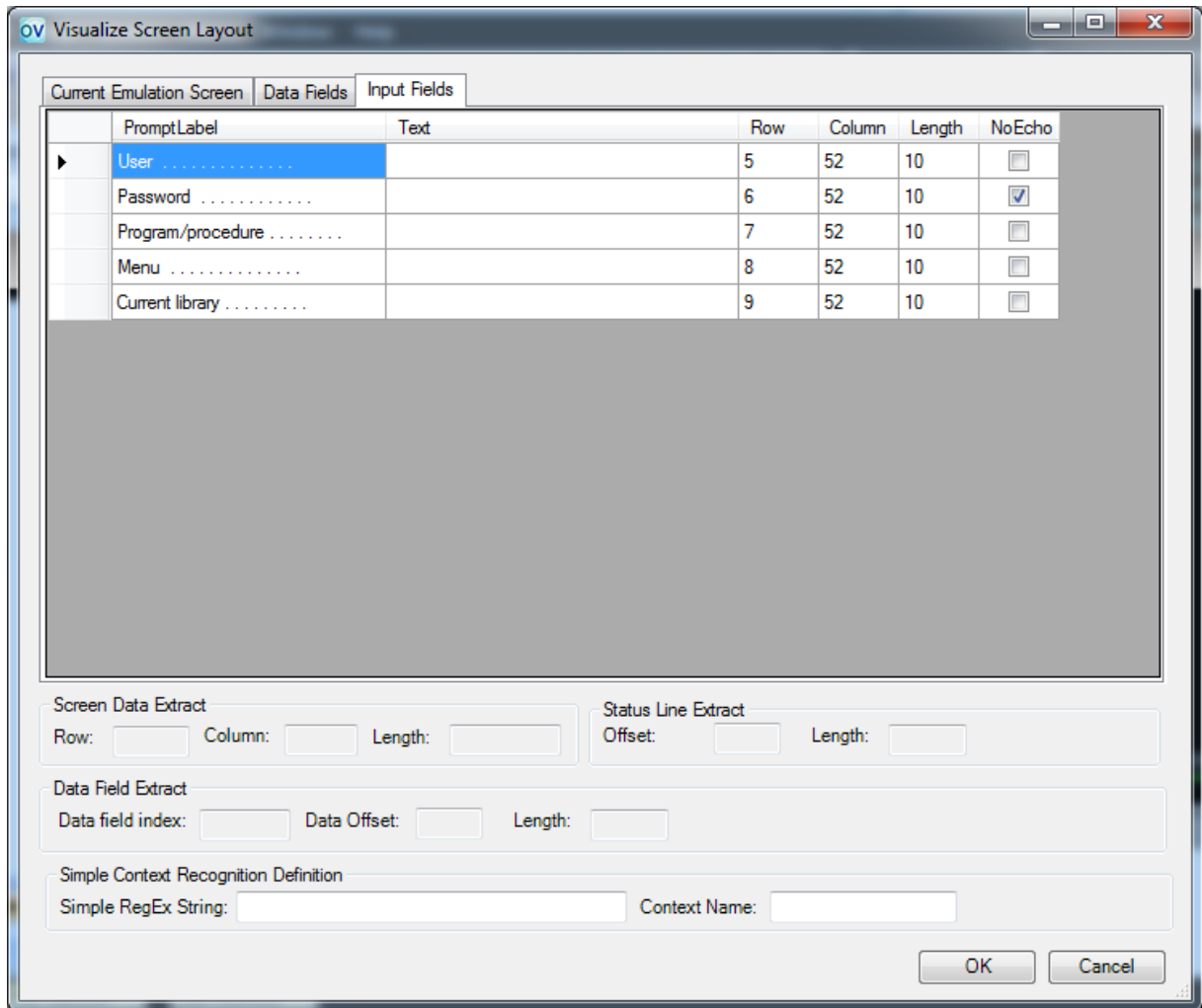
To define matching input field labels within an ID Type, you could simply type them in; but that can be a bit of a trial and error process. A more accurate process is to use of the ‘Visualize Screen layout’ control, as it shows the field marks and data that make up a screen.

To access the ‘Visualize Screen Layout’ navigate to the screen of interest, then select Edit, Application Settings, and the Context Recognition tab. There, select whichever of the following two buttons is enabled.



As you can see from the above example, the host formatted screen can contain a number of hidden field marks that define the beginning or end of input fields or protected areas.

The “Visualize Screen Layout” dialog also has an Input Fields tab that displays input fields after they are processed into logical objects).



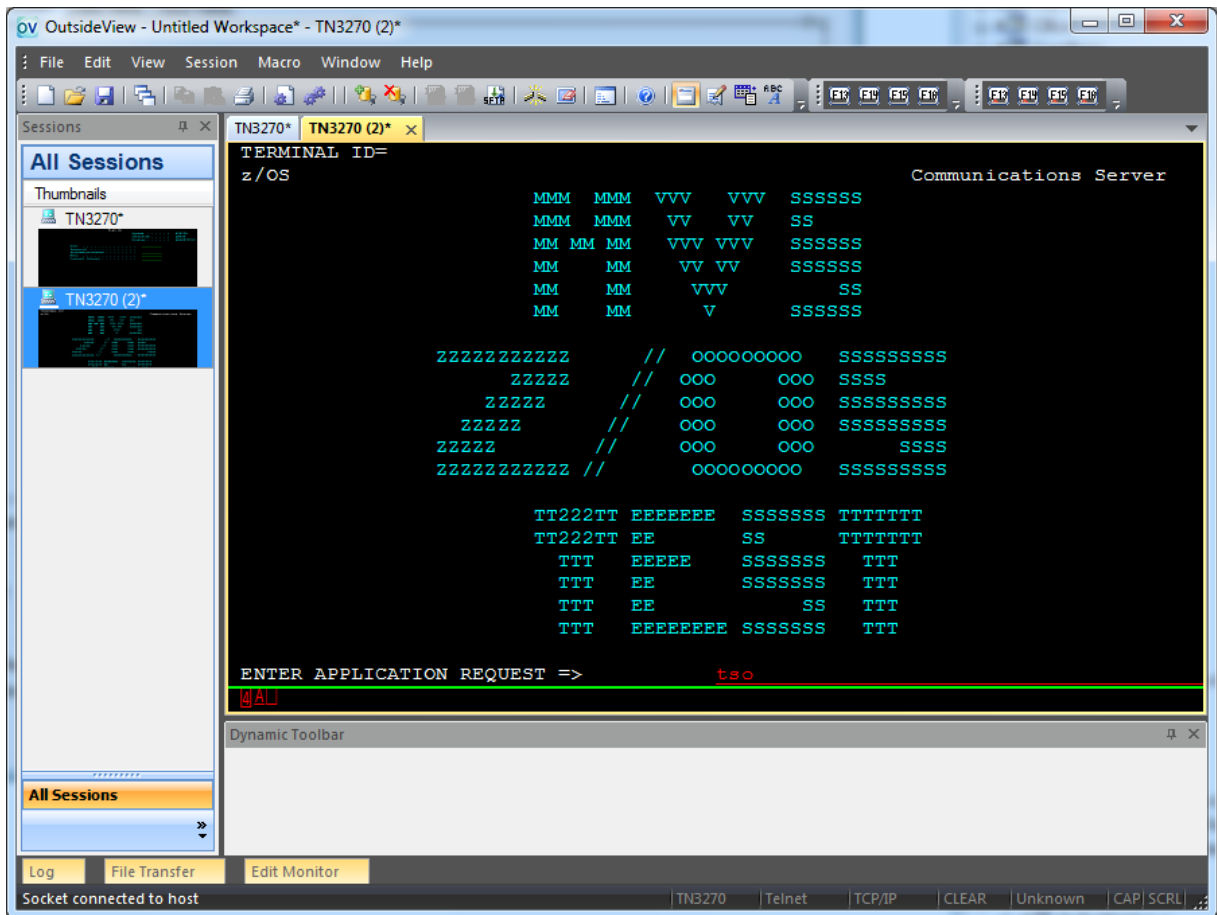
### 5.13.4 Example; Multiple Formatted Logon Screens

#### Example Multiple Formatted Screen Login

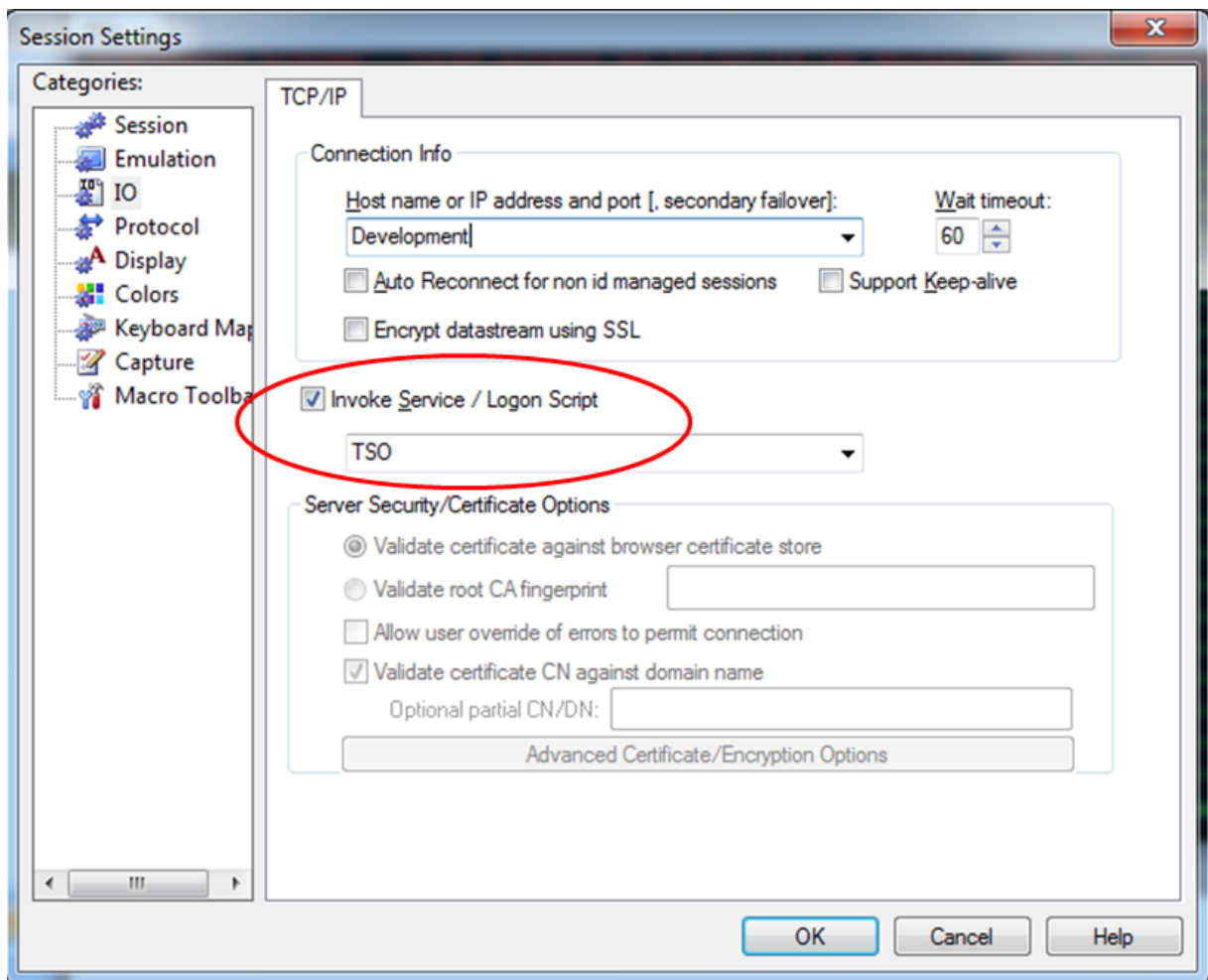
Let's use an example of automating login to an IBM TSO system. To create an appropriate ID Type, we will step through the logon process manually, capturing the host prompts and other information we need, and then configure an appropriate ID Type.

Initial screen;

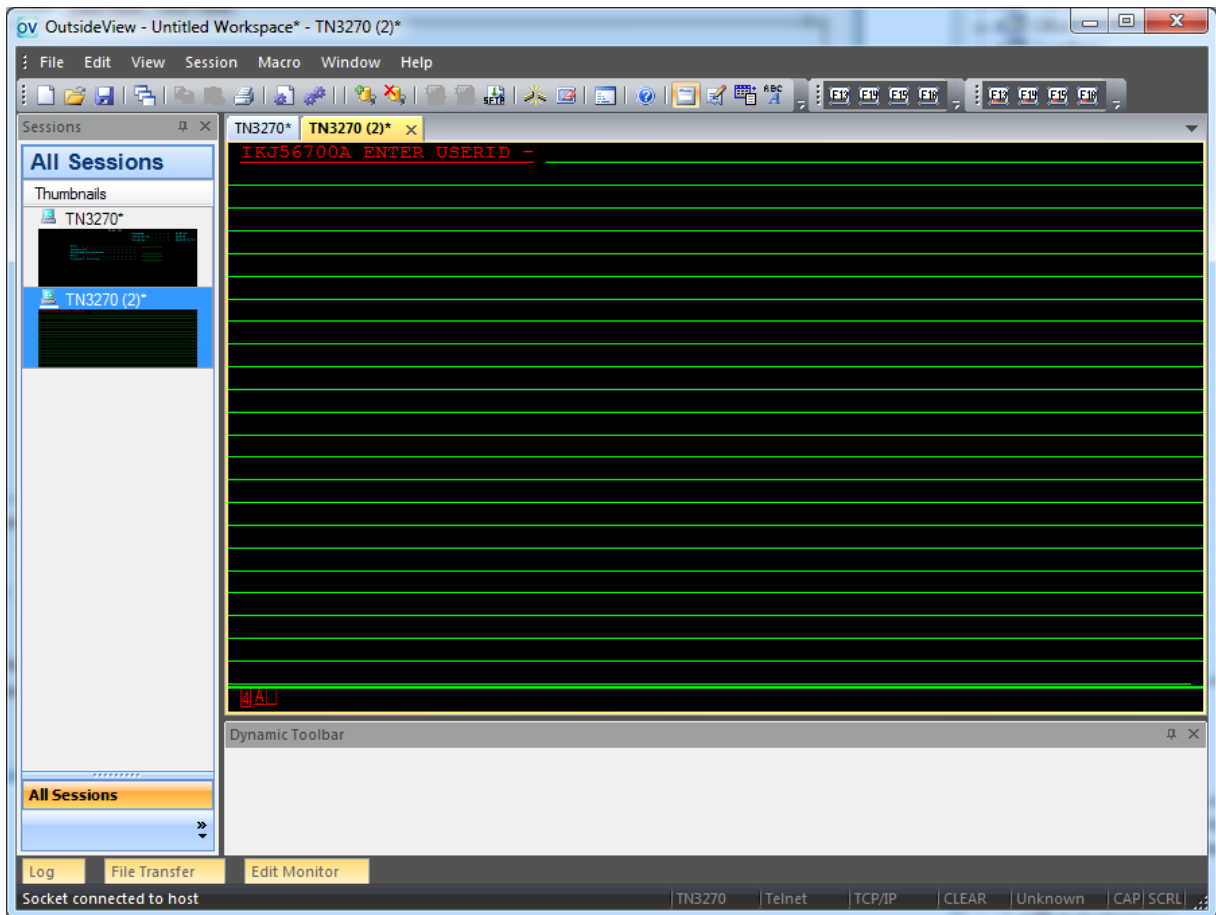




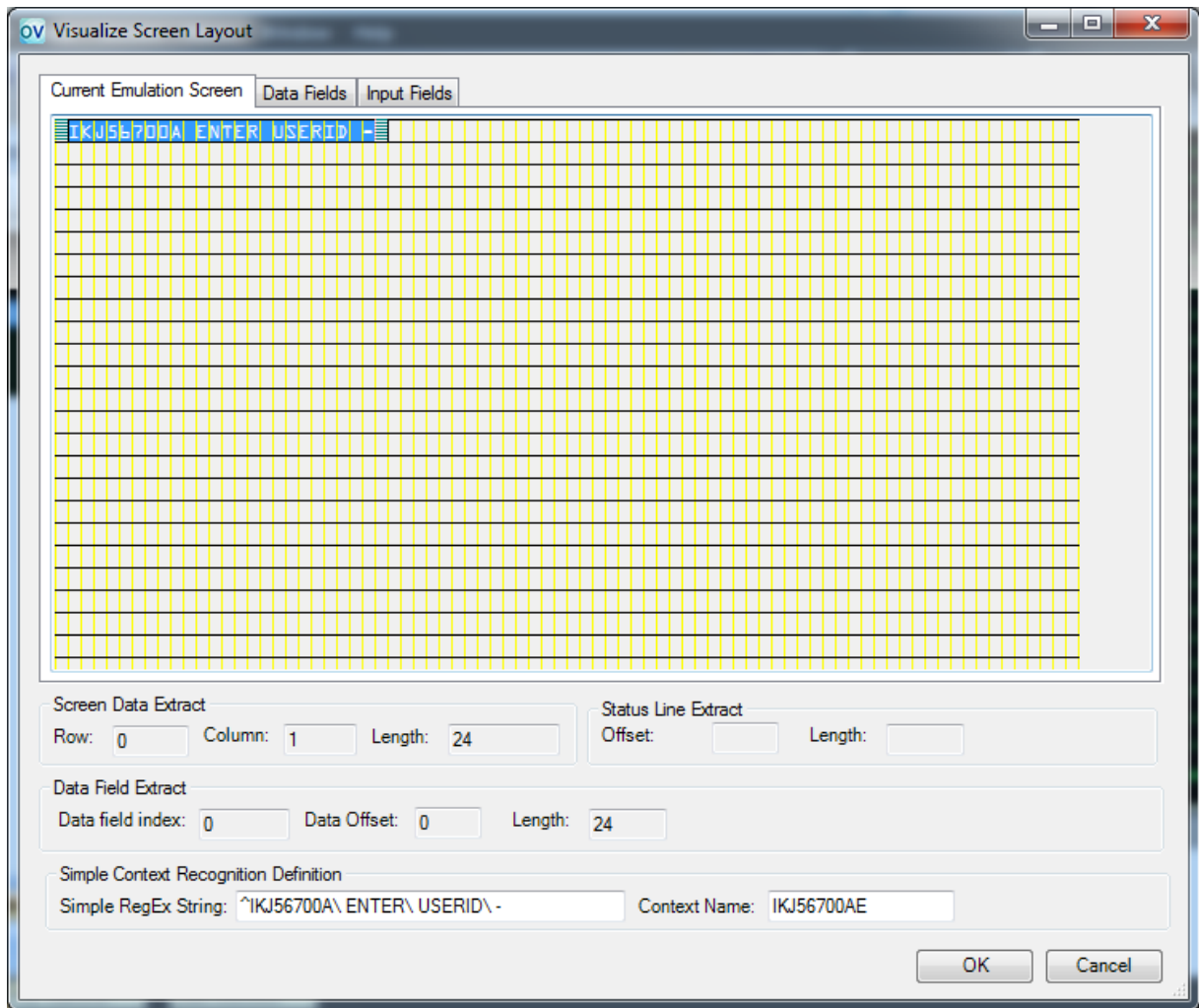
1. The host presents the user with an initial application request screen. At this point, the user selects the TSO sub system by entering TSO and depressing the enter key, or OutsideView can automate that selection by entering it as part of the session configuration as shown below.



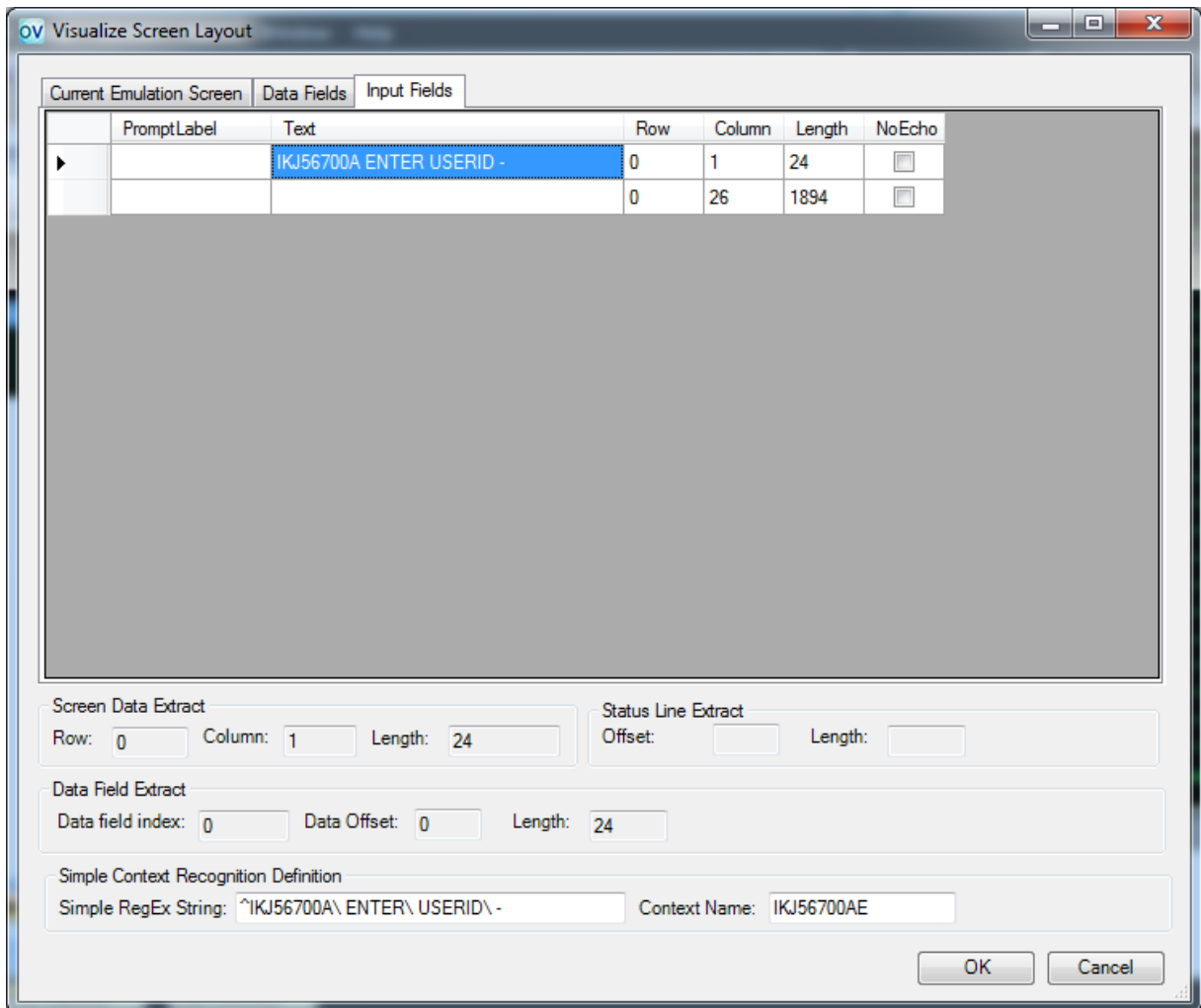
2. The host next asks for the user ID (below)



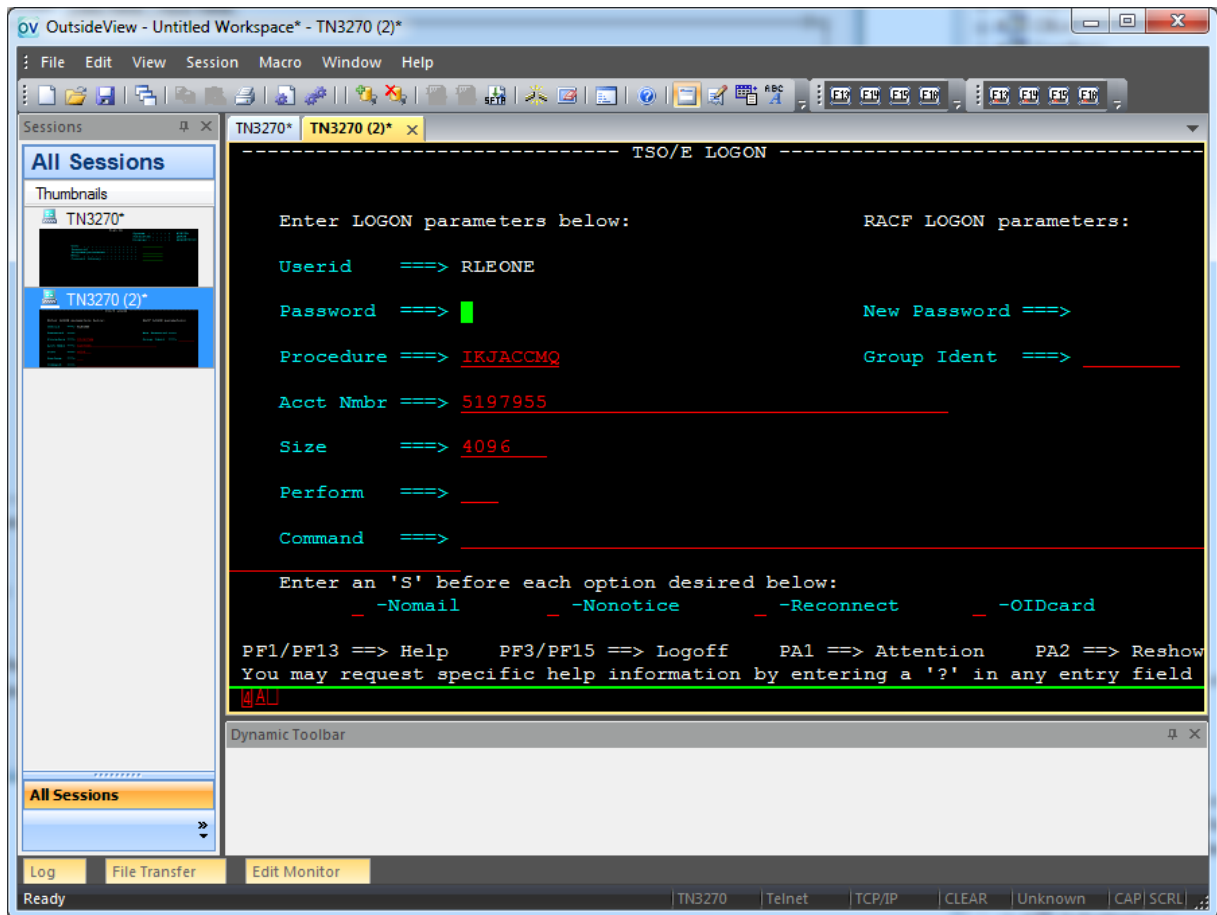
3. To accurately capture the text of this prompt for input field matching, bring up the Screen Visualizer. Do this by Edit, Application Settings, and the Context Recognition tab – or right-click within the Dynamic Toolbar area and select “Create new context”. (We are not going to create a context but make use of the Screen Visualizer that is displayed as the first step of the process.)



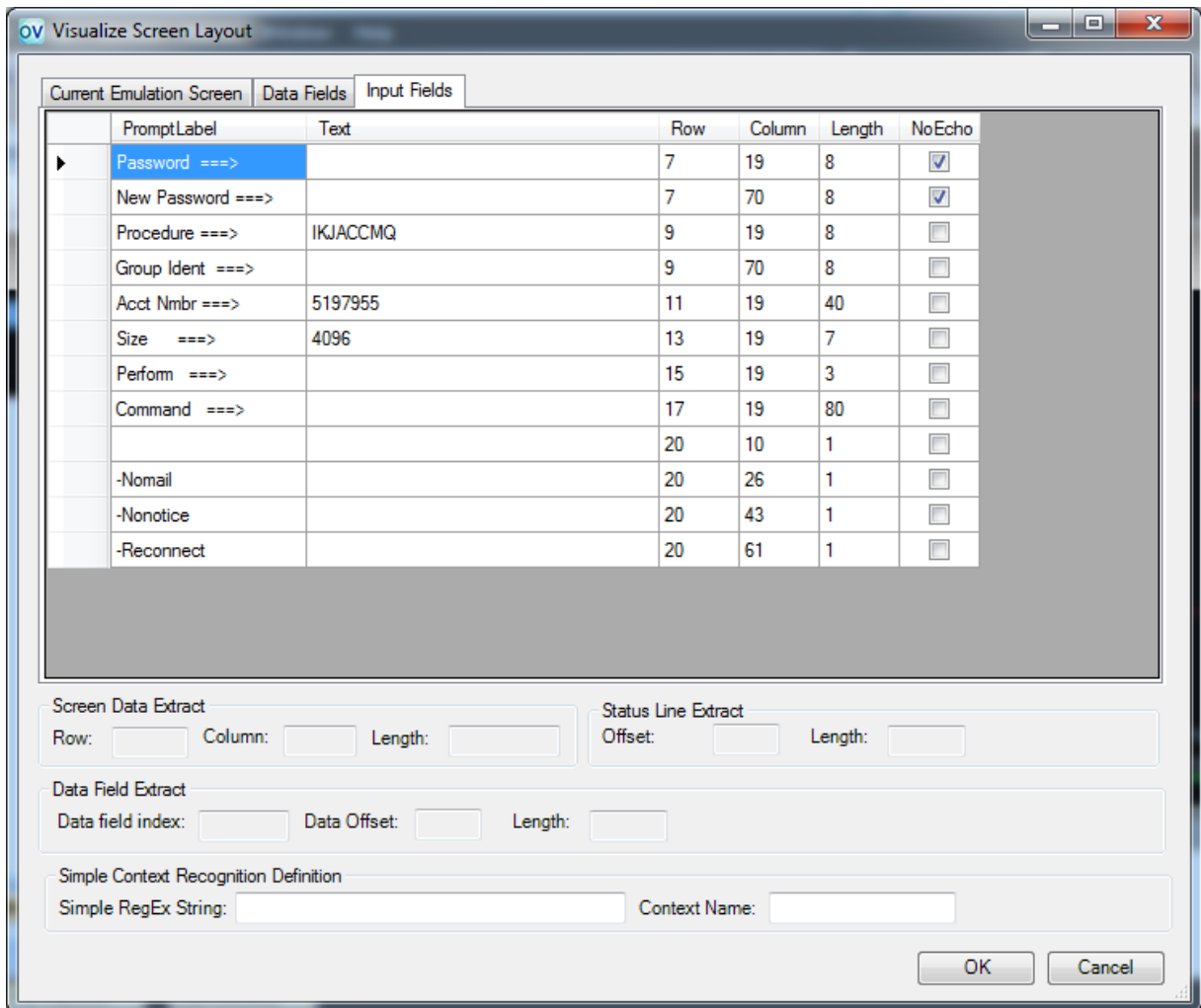
4. The Screen Visualizer gives us a visual representation of the screen layout. In the above image, we clicked on the field and the visualizer automatically selected all the text in that field. At this point, one could simply copy the information to a temporary Notepad document. However, we can get more informed detail by clicking on the Input Fields tab.



- From the Input Fields display, we can see that this screen is composed of two input fields; one that is 24 characters long and contains the prompt text and the other that is 1,894 characters long and into which the user inputs their user id. This screen breaks the general rule that user prompts are protected text and that the user inputs data in the unprotected area of the screen. In this case, the user can actually over type the prompt if they wish.
- Click on the prompt text and copy it to a temporary notepad document (for use later when we define our TSO ID Type).
- Click cancel to exit the Visualizer, and advance to the next screen of the login process to collect more prompt information.



8. This screen is much more complex and the host pre-fills in information for the user. The TSO login will need to prompt the user for three pieces of information.
  - i. User id (entered on the previous screen)
  - ii. Password
  - iii. Account number
  
9. Invoke the Screen Visualizer (Edit, Application Settings, Create/Edit Context OR right-click in Dynamic Toolbar area and Create/Edit Context)



10. To complete the login data collection phase, simply click on the password input label, copy it to the temporary notepad document, then click on the account number input label and copy it to the notepad document.
11. We are now ready to define our TSO login definition.
  - a. To do this, click “Edit” on the OutsideView menu bar, select “Identity Management”, followed by “Edit ID type”. Click the Add button and name the ID Type to be “TSO”.
  - b. Copy the captured prompt information from the notepad document into the field labels.
  - c. Enable the over-rides for “Login split between formatted pages or panels” and “Match Formatted Input Field Prompts”.
  - d. For the account number field, click the “Required Entry” checkbox (if required by your organization).

The screenshot shows the 'OV Add Identity Cache ID Item' dialog box. It is divided into several sections:

- IdentityCacheID:** Name: TSO; Pre-Login required (NonStop Conv only): ; Pre-Login Name: [dropdown].
- Login Function Key:** Emulator Type: NA; Login Function Key String: [dropdown]; Visible: .
- Field 1:** Field 1 Label: IKJ56700A ENTER USERID -; Visible: ; Sensitive Input Field: ; Required Entry: .
- Field 2:** Field 2 Label: Password ===>; Visible: ; Sensitive Input Field: ; Required Entry: .
- Field 3:** Field 3 Label: Acct Nmbr ===>; Visible: ; Sensitive Input Field: ; Required Entry: .
- Field 4:** Field 4 Label: [empty]; Visible: ; Sensitive Input Field: ; Required Entry: .
- Field 5:** Field 5 Label: [empty]; Visible: ; Sensitive Input Field: ; Required Entry: .
- Field 6:** Field 6 Label: [empty]; Visible: ; Sensitive Input Field: ; Required Entry: .
- Login Over-Rides:** Login split between formatted pages or panels: ; Match Formatted Input Field Prompts: .

Buttons at the bottom right: Reset, OK, Cancel.

12. When a user first connects to the host, using a session file with the ID Type of TSO, a credentials prompt is presented to the user to collect their information. And the entered information is properly processed across multiple screens to accomplish an automated login.

When opening additional sessions with an ID Type of TSO, or when reconnecting any such session, the users will be automatically logged in, using the credentials cached (encrypted) from the first login.

### 5.13.5 RE-activating Identity Manager

If you press the CANCEL button when Identity Manager is prompting you for user credentials, Identity Manager 'sets a flag' that you don't want to provide credentials. Identity Manager will then no longer prompt you when it otherwise would (such as when sessions or workspaces are opened or re-connected.)



If you decide you do want to use the Identity Manager again, choose Edit, Identity Management, Identity Manager, and enter the appropriate credentials. Thereafter, ID Manager will use them as needed.

## 5.14 Security

### 5.14.1 Security Overview

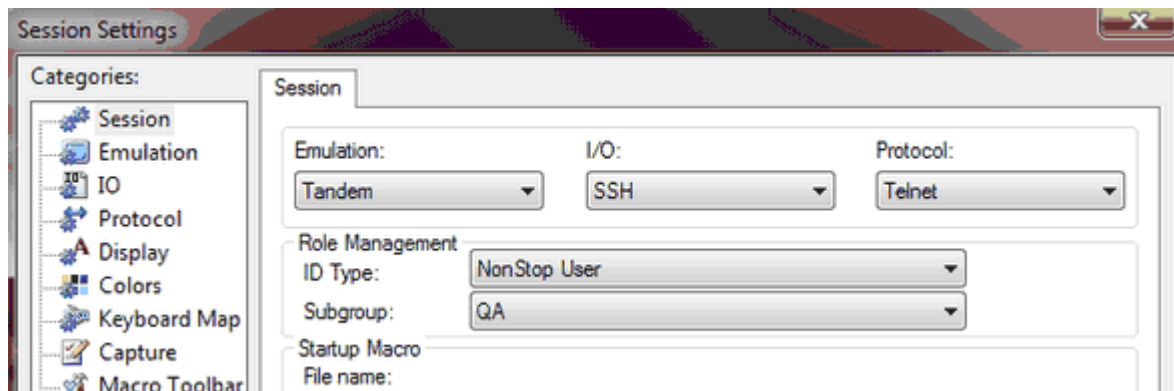
#### Security Overview

OutsideView version 9.1 supports **SSL/TLS** and **SSH** encryption to hosts or proxies supporting those protocols. SSL Encryption is enabled for a session by choosing TCP/IP as the I/O method and checking the "Encrypt Datastream using SSL" checkbox in the I/O category of Session Settings. SSH encryption is enabled for a session by choosing SSH as the I/O method.

### 5.14.2 SSH Security

#### SSH Security

When creating a new SSH session, use the Session tab to select SSH as the I/O method:



Thereafter, all SSH-specific settings are found within the I/O category. There are two tabs, SSH I/O and Certificate Tools.

#### 5.14.2.1 ID Management and SSH

##### Role Management and SSH

Role Management	
ID Type:	<undefined>
Subgroup:	<undefined>

Selection of an ID type is **Optional** in SSH.

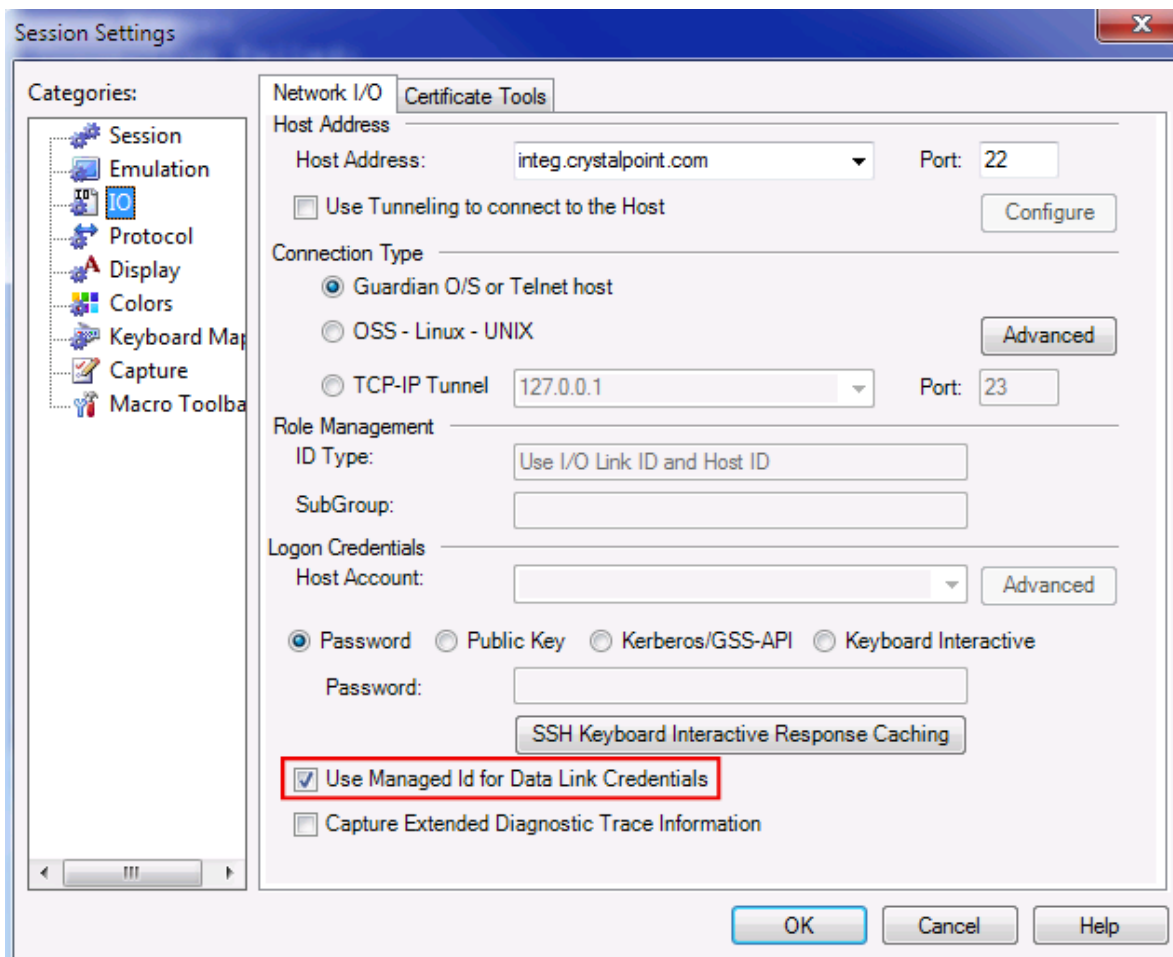
If an ID Type is specified, then the selected ID type and Subgroup will be displayed in the I/O tab, and the Host Account field will become a non-entry field (since that information is controlled via the Identity Manager).

### New ID Type introduced in OutsideView 9.0

- I/O Link ID
- Use I/O Link ID and Host ID

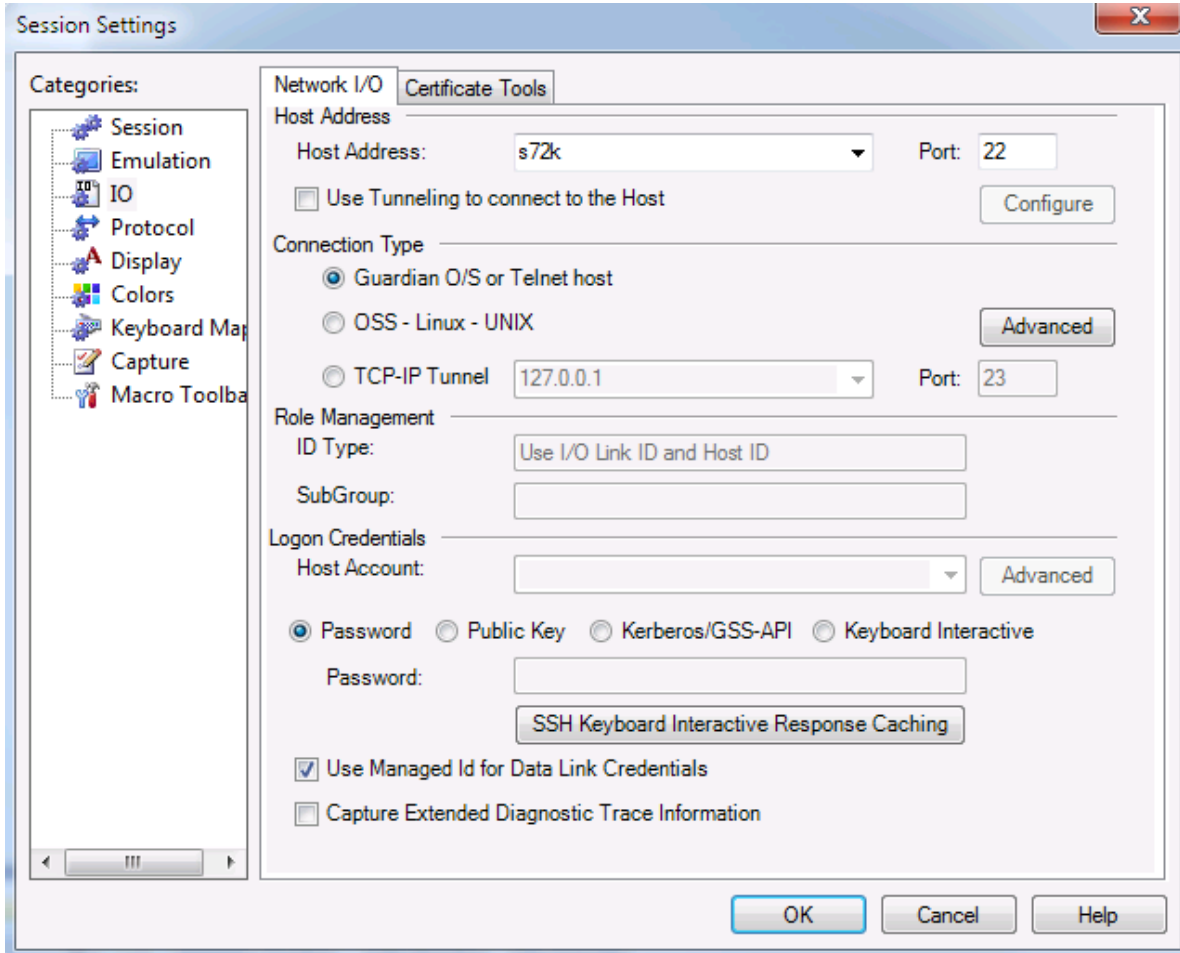
These two new ID types are used with the "Use Managed Id for Data Link Credentials" to provide login credentials for the data link and also for the host.

When using separate logins for the SSH data link level and host application interactions, it might be appropriate in your organization to use common credentials for securing the data link and save this information in the host configuration file that you distribute to the users. In this case you can still set a managed ID to prompt the user for their personal credential and enable the entering/retention of the link level credentials by **unchecking** "Use Manage Id for Data Link Credentials" checkbox.



5.14.2.2 SSH I/O

SSH I/O tab



**Host Address**

**Address** is the host IP address or domain name (Or the address of the SSH tunneling service)

**Port** defaults to 22, but may be modified

**IPV6:** IPV6 is now supported within OutsideView. The format for directly entering IPV6 addresses is the RFC standard format of surrounding the address with brackets. I.E. [2001:DEAD:BEEF:CAFE::8002]:23 with the :23 being the port number if being over-riden. You can also use IPV6 addresses in the Failover scenario for the Host field.

**Failover:** If you want your session to try to alternate host and port combinations such that if the first address/port does not work OutsideView will attempt the next address in the list. User will need to provide address information in the form: host port, host port, host port, ... For example: host1.crystalpoint.com 19, host2.crystalpoint.com 6, [2001:DEAD:BEEF:CAFE::8002]:23, host3.crystalpoint.com 22

## Multiple SSH Tunneling hops

Use Tunneling to connect to the Host

Define (add) intermediate SSH hosts, maximum of 5;

## Keep-Alive Settings

OutsideView SSH automatically sends a keepalive packet after an idle period of 5 minutes. .

## Connection Types

The OutsideView SSH protocol supports both pseudo-terminal and tunneling connection types.

## Login/Session Tab

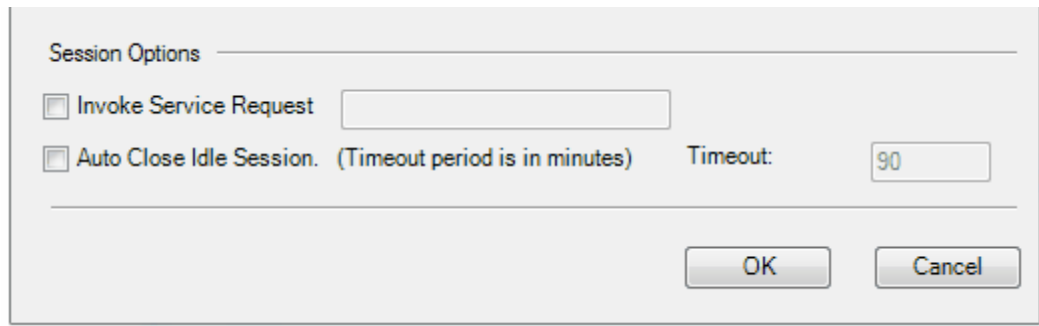
### Pseudo-terminal connections

**Guardian O/S or Telnet host** is a **pseudo-terminal connection**, and specifies terminal type TN6530-8 during session startup negotiations.

**OSS - Linux - UNIX** is also a **pseudo-terminal connection**, and specifies terminal type OSS6530 during session startup negotiations.

**Advanced**

**pseudo-terminal options include:**



Session Options

Invoke Service Request

Auto Close Idle Session. (Timeout period is in minutes) Timeout:

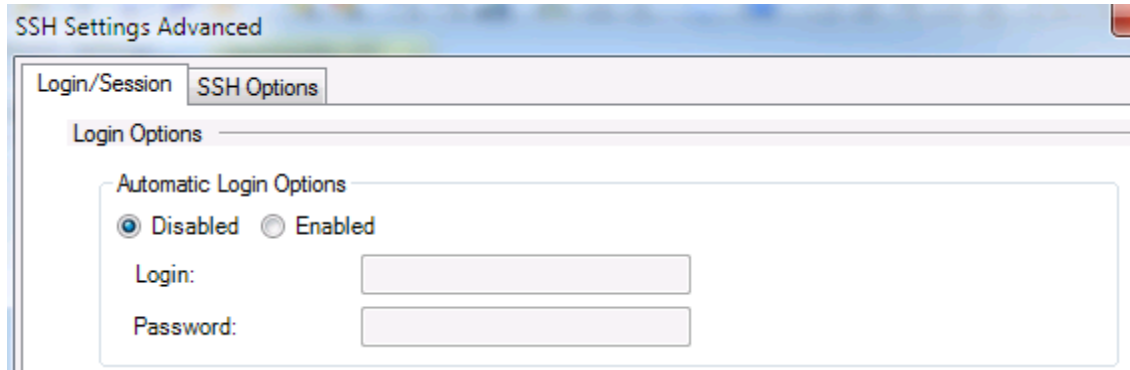
OK Cancel

## Tunneling Connections

TCP-IP Tunnel  Port:  is a tunneling SSH connection.

Tunneled connections require the address of the SSH listening service in the Host Address and port fields, and the final/forwarding destination (from the perspective of the listening service) for the decrypted information here.

**Advanced** SSH tunnel options include:



SSH Settings Advanced

Login/Session SSH Options

Login Options

Automatic Login Options

Disabled  Enabled

Login:

Password:

The advanced Login and Password fields allow a tunneled connection, after supplying credentials as defined on the primary I/O tab to the tunneling service, to also supply user name and password to the host system itself.

## Role Management

Within the SSH I/O tab, these fields are display only, and show the values defined in the Session category.



Role Management

ID Type:

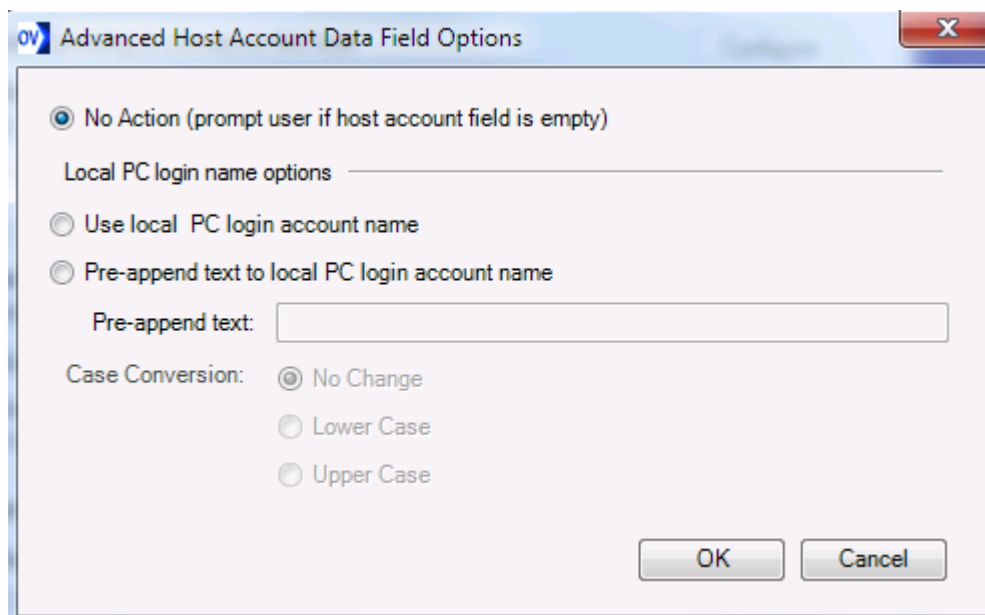
SubGroup:

## Logon Credentials

Users can authenticate their SSH pseudo-terminal session using a host account and host password (if the SSH configuration on the host permits), by using a passphrase to access and send a key file to the host, by keying in required information interactively, or by Kerberos/GSS-API authentication. This area is also used to pass credentials to the SSH tunneling server.

**Host Account** is the user's host account. (This field will be display-only if ID management is active.)

Advanced Host Account options are:



Advanced options can automatically derive/supply a user id. For instance, if your host account user name were identical with your PC login account user name, you could select

Use local PC login account name

If all host account user names are of the form cust.user, where 'cust' is fixed and 'user' matches your PC login user name, then you could select

Pre-append text to local PC login account name

Pre-append text:

For example, assume your PC login name is Bob, and your host account login is US.Bob. Enter the Pre-append text as US. Thereafter if Bob is logged in to the PC, the SSH session would attempt to login as US.Bob. If Sue logs in to the PC, the session would attempt to login as US.Sue.

**Case conversion is a convenience to allow login names to stay case-compliant with host account names.**

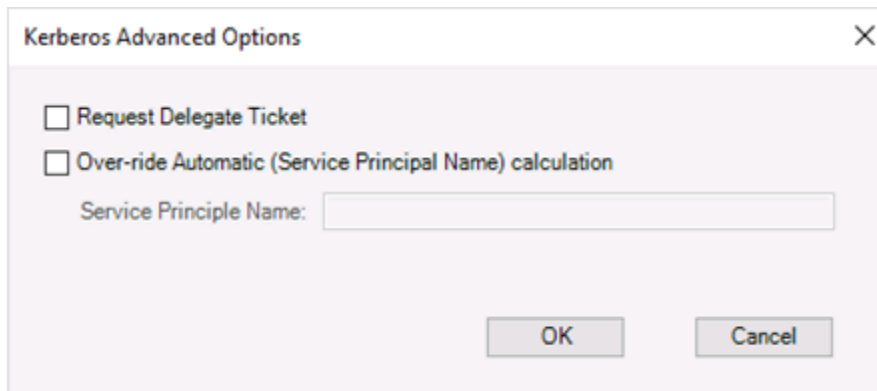
**Password** - This field will be display only if ID Management is active

**Public Key** - This option requires entry of a passphrase and selection of a public key file (see topic [SSH Certificates](#))

**NOTE:** When used in conjunction with ID Management, the passphrase should be provided, and the option to "Retain Login Info on session Save" should be enabled.

**Kerberos/GSS-API** - This option works in conjunction with the NonStop Secure Single Sign-on product to enable single sign-on wherein the active directory security token obtained at PC login is presented to the Single Sign-on component on the NonStop to authenticate the host session. See the NonStop Secure Single Sign-on documentation for information on configuring these options.

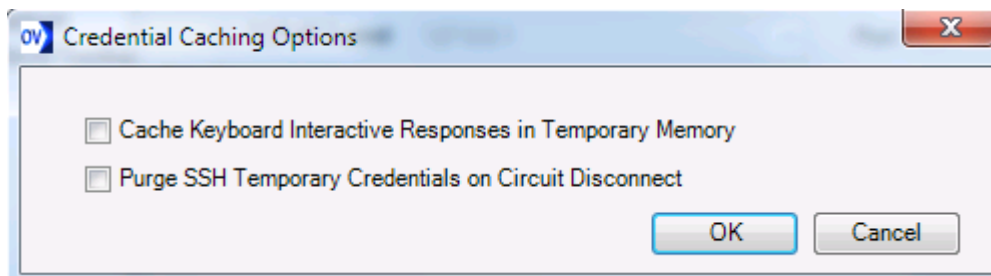
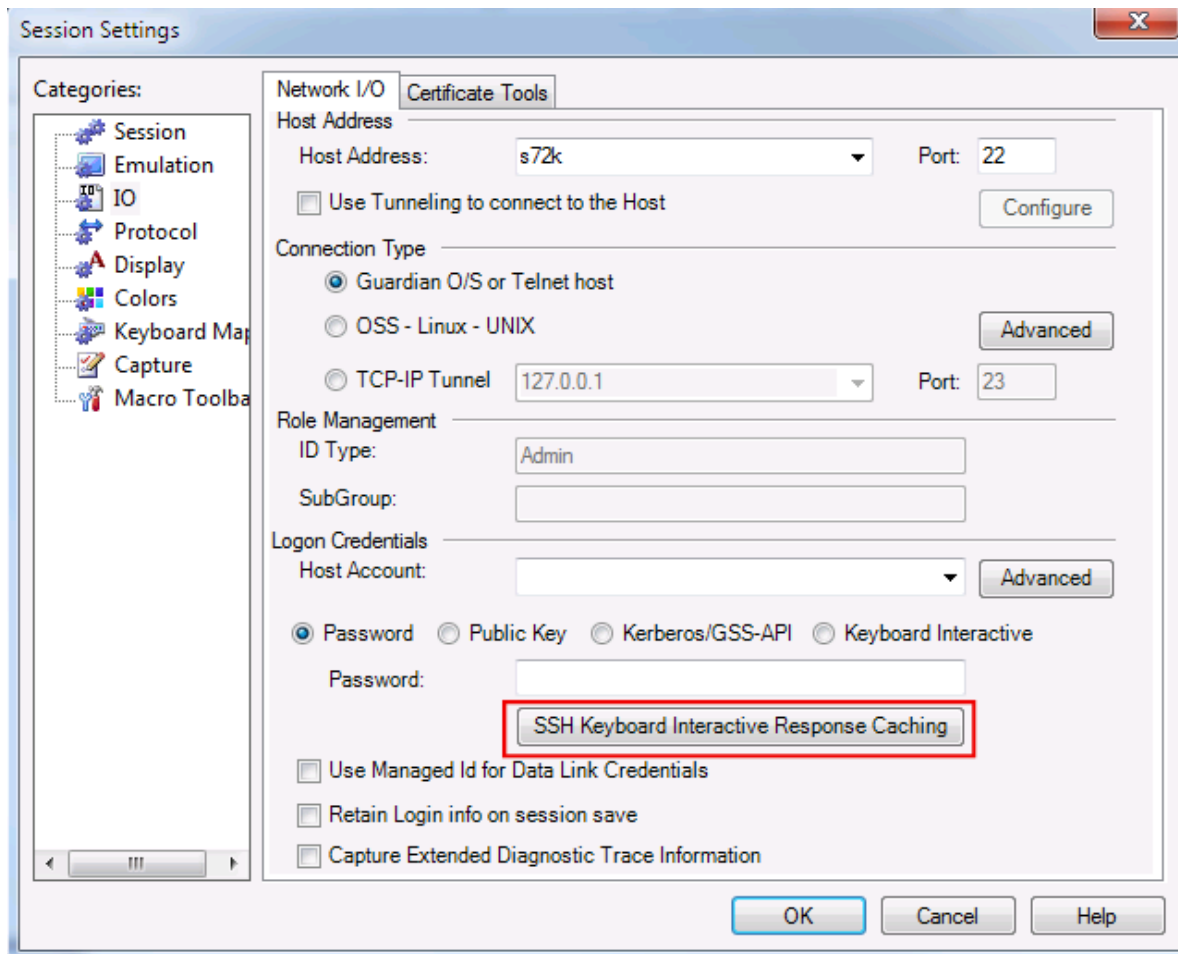
Configure Advanced Kerberos Options



The screenshot shows a dialog box titled "Kerberos Advanced Options" with a close button (X) in the top right corner. Inside the dialog, there are two unchecked checkboxes: "Request Delegate Ticket" and "Over-ride Automatic (Service Principal Name) calculation". Below the second checkbox is a text input field labeled "Service Principle Name:". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

**Keyboard Interactive** - Requires manual entry of user credentials to authenticate session.

**SSH Keyboard Interactive Response Caching**



**NOTE:** NonStop password expiration warnings will be displayed only in keyboard interactive mode.

**NOTE:** In keyboard interactive mode, an SSH session can be configured to save only the host account, and session startup will prompt for the user password.

**Use Managed Id for Data Link Credentials** - this option is default enabled when using Managed Id (ID Type). The credentials provided in the ID Type is used to connect to the host (Data Link). When using separate logins for the SSH data link level and host application interactions, it might be appropriate in your organization to use common credentials for securing the data link and save this information in the host configuration file that you distribute to the users. In this case you can still set a



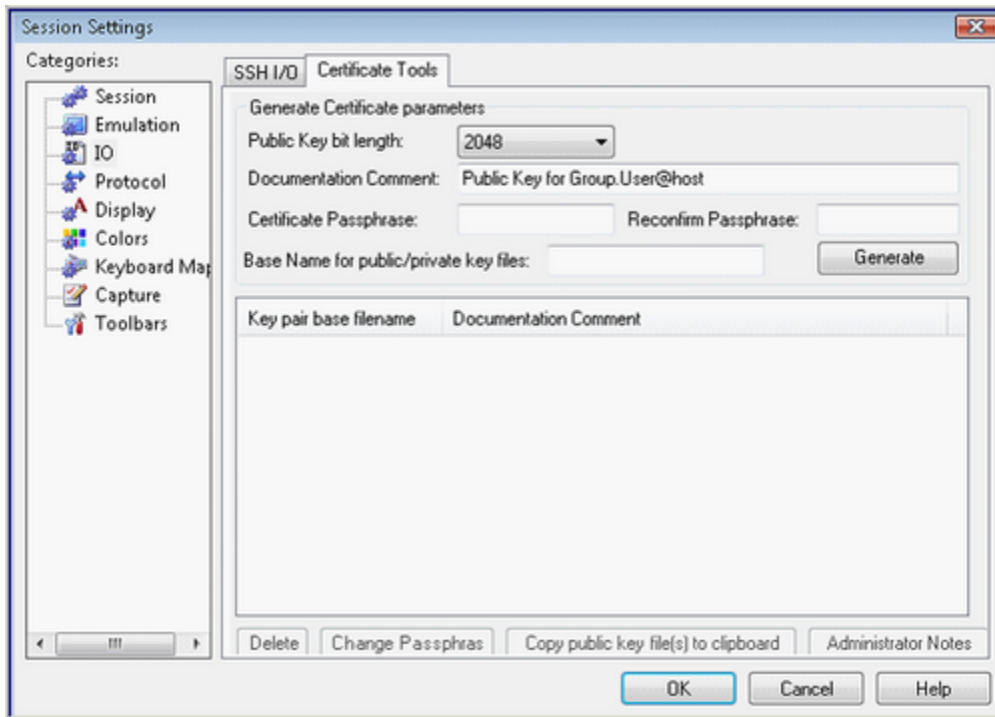
managed ID to prompt the user for their personal credential and enable the entering/retention of the link level credentials by **unchecking** "Use Manage Id for Data Link Credentials" checkbox.

**Retain Login Info on Session Save** - Note this option is Visible when the Use Managed ID for Data Link Credentials is **unchecked!** It allows you to save your credential into the session file if you do not use Managed ID.

**Captured Extended Diagnostic Trace Information** - this option is only for SSH session because normal trace will not work in getting trace data.

### 5.14.2.3 SSH Certificates

#### Certificate Tools tab



#### Example Usage:

Enter comments and passphrases of your choice, and select Generate

This creates three files that 'vouch' for your identity, and are stored as hidden files in your individual configuration data storage location, within the Crystal Point sub-folder SSH Store. .

In the above example, the public portion of your key is stored in the files james.OpenSSH and james.pub

The private portion of your key is stored as jameskey.pfx

Enterprise NOTES: To have individually generated certificates available to all members/workstations within a given profile, these files must be moved to the Enterprise Profile's SSH store location, (E.g., ...\\Profile\\Standard\\config\\SSH Store) for replication out to the SSH store of all profile members. (End-users will not be able to utilize these files without their passphrase.)

The public portion of these certificates must become known to the SSH layer on the host before you can use Public Key Authentication. That means you need to get those files to the host and update the host's SSH database. To accomplish that, you would typically go through your organization's security group. OutsideView has provided tools to help you send that information on to your security group:

You may highlight the created **public** key pair base file:

Key pair base fil...	Documentation Comment
james	Public Key for cp.jimh@s72k.crystalpoint.com

And then press

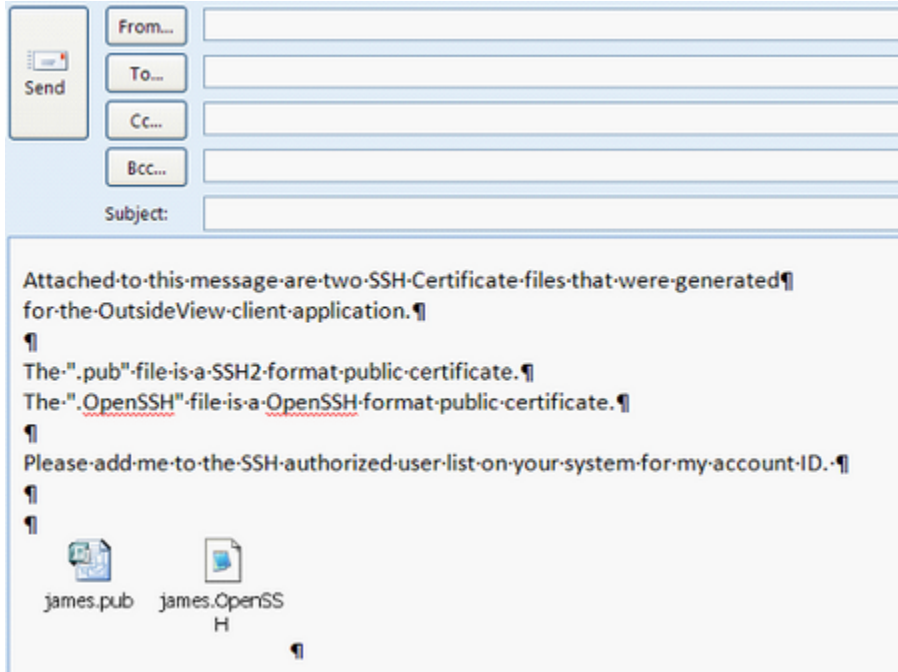
Administrator Notes

Now, start a new e-mail from within Outlook (or whatever) and select Edit, Paste to see the following:

Return to the SSH certificate tools and click on

Copy public key file(s) to clipboard

Go back to your e-mail and click Edit, Paste again to get to the following state:



The screenshot shows an email composition interface. On the left is a 'Send' button. The main area contains fields for 'From...', 'To...', 'Cc...', 'Bcc...', and 'Subject:'. The body of the email contains the following text:

Attached-to-this-message-are-two-SSH-Certificate-files-that-were-generated¶  
for-the-OutsideView-client-application.¶  
¶  
The-".pub"-file-is-a-SSH2-format-public-certificate.¶  
The-".OpenSSH"-file-is-a-OpenSSH-format-public-certificate.¶  
¶  
Please-add-me-to-the-SSH-authorized-user-list-on-your-system-for-my-account-ID.-¶  
¶  
¶

Below the text are two file attachments: 'james.pub' and 'james.OpenSSH'. The 'james.OpenSSH' attachment has a small 'H' icon below it.

Send this e-mail to your security group. They should take it from there, letting you know once they have made you known to the host.

#### 5.14.2.4 Adding user-generated key file to NonStop hosts

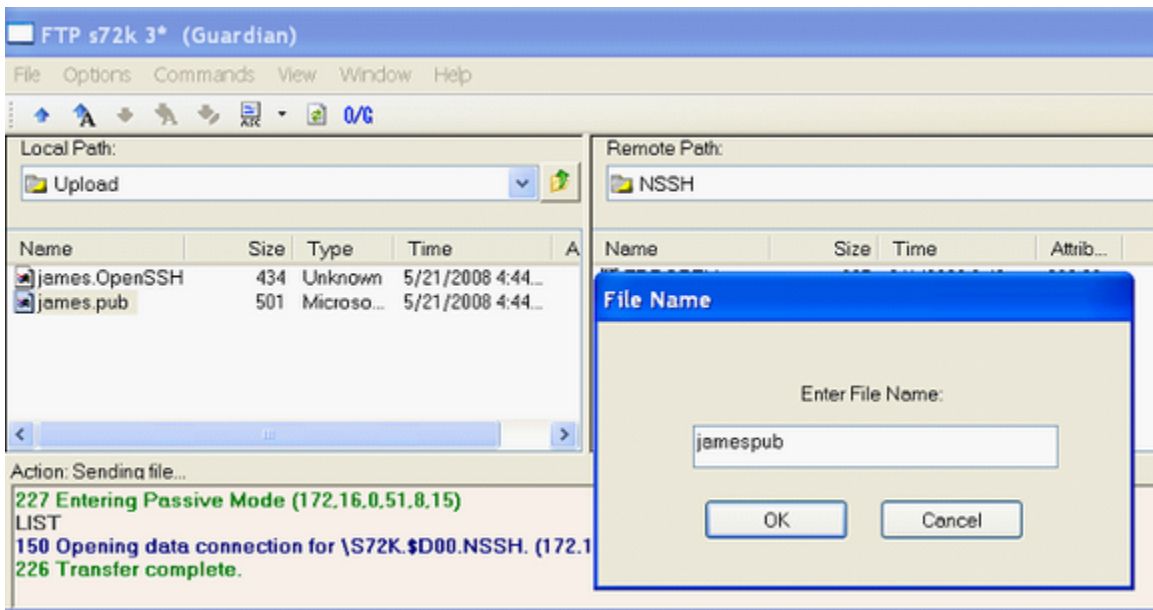
##### Notes For Security Group

Example of adding user-generated key file to NonStop host running Crystal Point's NonStop Secure Shell (NSSH)

##### Steps to add public keys to host

(Allowing OutsideView to communicate via SSH to the NSSH product on the NonStop)

Transfer the public key file to the NonStop directory in which NSSH is installed. (e.g. james.pub AS jamespub using ASCII mode, or OpenSSH certificates as binary.)



1. Open a terminal session into the Host and enter SSHCOM

```

$D00 NSSH 2> status *, prog ssh2

System \S72K

Process                Pri PFR %WT Userid  E
$SSH01                1,371 168 P 005 255,255 $
$D00 NSSH 3> sshcom $ssh01
SSHCOM^H16^20DEC04
OPEN $ssh01
%

```

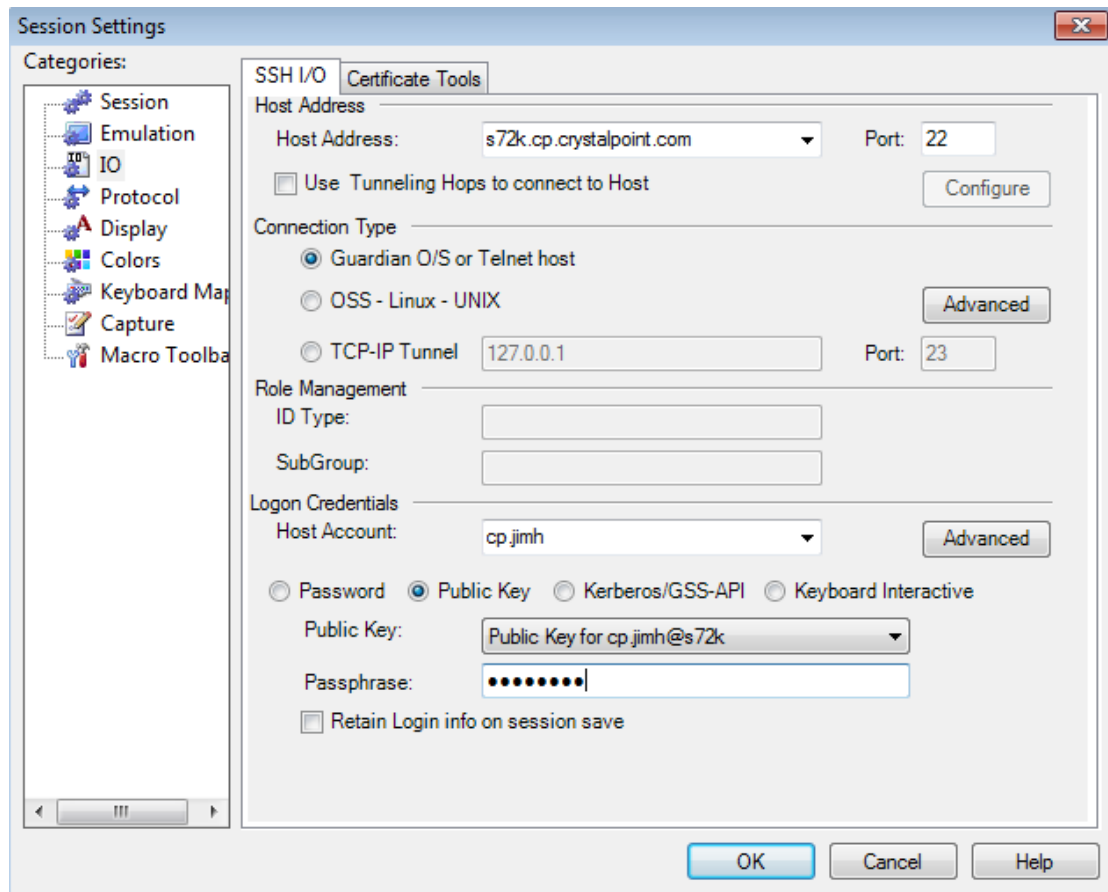
2. Add and Alter the user, as needed

```

% add user cp.jimh, allow-shell yes, allow-pty yes, allowed-subsystems (sftp, tacl)
add user cp.jimh, allow-shell yes, allow-pty yes, allowed-subsystems (sftp, tacl)
)
OK, user cp.jimh added
% alter user cp.jimh, publickey jamespub file jamespub
alter user cp.jimh, publickey jamespub file jamespub
OK, user cp.jimh altered
%

```

Once this has been accomplished, notify the user they may now connect (for Terminal emulation or SFTP file transfer) using Public Key Authentication;



```
STN00 Connected to STN version A78 2008/05/21 17:06 \S72K.$PTY.#ZWN0203
STN46 Secure SSH session: TN6530-8 publickey aes256-cbc hmac-sha1

TACL (T9205D46 - 27JUN2005), Operating System G06, Release G06.27.00
(C)1985 Tandem (C)2005 Hewlett-Packard Development Company, L.P.
CPU 1, process has no backup
May 21, 2008 17:06:59
(Invoking $SYSTEM.SYSTEM.TACLOCL)
(Invoking $D00.JIMH.TACLCSTM)

Loaded from $SYSTEM.STARTUP.TACLMACS:

V H F I P TYPE F I F FA FS W ST DS VOL DIR SP SU TYPE T COPY DUP CHKDSK DEL

Current volume is \S72K.$D00.JIMH
$D00 JIMH 1>
```

If you ever wish to delete the key, the SSHCOM syntax is:

Alter user [group.user], delete publickey [publickey value, e.g. jamespub]

### 5.14.2.5 SSH access for Cloud Computing

Many cloud computing infrastructures require SSH-secured access.

Typically, as part of the signup process, you receive an e-mail with an attached private key file to use with your SSH client.

If viewed, the key looks similar to;

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEA0BqU4eXQt4cCNU2ban2SEneyR0HbfCQUvt/rPkuV/kay2Llpm
6T4h7+n52dAbWv2ZgrsGmCepHoeJ5WEO9E29zU7k38wTEPILCPEXZon+4U6vMorZ
y/mHN7tnKnFHo2s+32V+wykQQagAgIVMumzYys5EHk/b8enNsH2TxfMjg0GqQTDu
OOXhAZYmWU6VM9G3u3IHpvufwG/b734amtiVjFoqaZL9YbnpA==
-----END RSA PRIVATE KEY-----
```

(Note we have shortened the above example.)

Let's assume you received a key file through an e-mail. There are two ways to import this key information into OutsideView's public key space. The first method is more technically correct, but requires access to a UNIX or LINUX system.

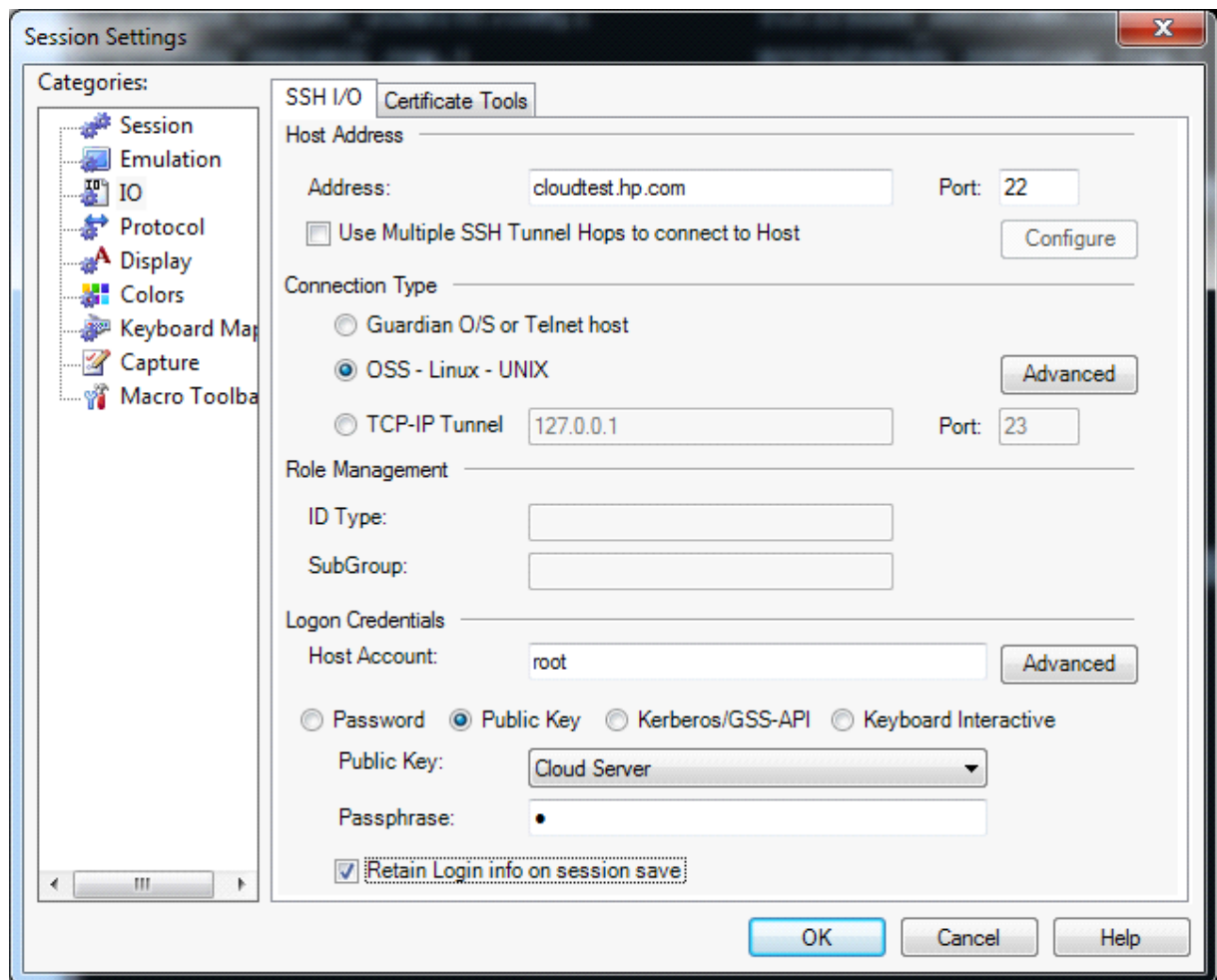
1. Using a UNIX system to import public key information into OutsideView
 

Do the following steps:

  - a. Upload the key file to the LINUX or UNIX machine as a file named cloudserver
  - b. At the UNIX command prompt, enter "ssh-keygen -e -f cloudserver >>cloudserver.pub"
  - c. Start OutsideView, select View, Configuration Data Folder from the menu.
  - d. Double click on the "SSH store" directory, then the "private" directory.
  - e. Copy this directory path to the clipboard; for instance, C:  
 \Users\John.domain\AppData\Roaming\Crystal Point\OutsideView\SSH Store\private
  - f. Open a file transfer session to the UNIX machine.
  - g. Set the local side of your file transfer window to the 'private' directory path (from the clipboard).
  - h. Download the file cloudserver from the LINUX/UNIX system into the 'private' directory.
  - i. Set the local side of your file transfer window to the 'public' subfolder.
  - j. Download the cloudserver.pub file into the 'public' directory.
  - k. Optionally; double click on the cloudserver.pub file to invoke OutsideView's internal editor and change the comment line to something more relevant then automatically inserted comment from the ssh-keygen program.
  
2. Importing public key information to OutsideView without LINUX or UNIX access:
  - a. Start OutsideView, select View, Configuration Data Folder.
  - b. Double click on the "SSH store" directory, then the "private" directory.
  - c. Copy this directory path to the clipboard; for instance, C:  
 \Users\John.domain\AppData\Roaming\Crystal Point\OutsideView\SSH Store\private
  - d. From your email client, save the private key file into the ... \SSH store\private directory AS "cloudserver" (Generally you can paste the path from the previous step to get to the correct directory.)
  - e. Navigate to the ... \SSH store\public directory and copy that path to the clipboard.
  - f. Now execute the following run command: Notepad <path>\cloudserver.pub
  - g. This brings up a blank text document into which you will type the following three lines of text.

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: Cloud Server
---- END SSH2 PUBLIC KEY ----
```

You can now configure your SSH session in OutsideView;



Notice that the Passphrase input box has a single space entered in it. Since passphrase is not used for this type of private key file, it simply keeps the SSH layer from thinking you haven't entered one yet and skip the prompting step.

#### 5.14.2.6 Converting SSH keys to SSH2

Some organizations generate SSH public/private keys on UNIX or LINUX systems (Usually in an RSA format) for remote access to selected systems. OutsideView requires SSH2 public/private keys.

To determine whether the keys in question are SSH or SSH2,

1. Login to your user ID on the UNIX or LINUX box
  1. Change to your SSH cache directory by issuing the command "cd .ssh"
  2. Locate your private/public keys. They are typically named something like user@host and user@host.pub



3. Do a cat of the public file using the command "cat [user@host.pub](#).
4. See the example below. An SSH2 key will identify itself as SSH2:

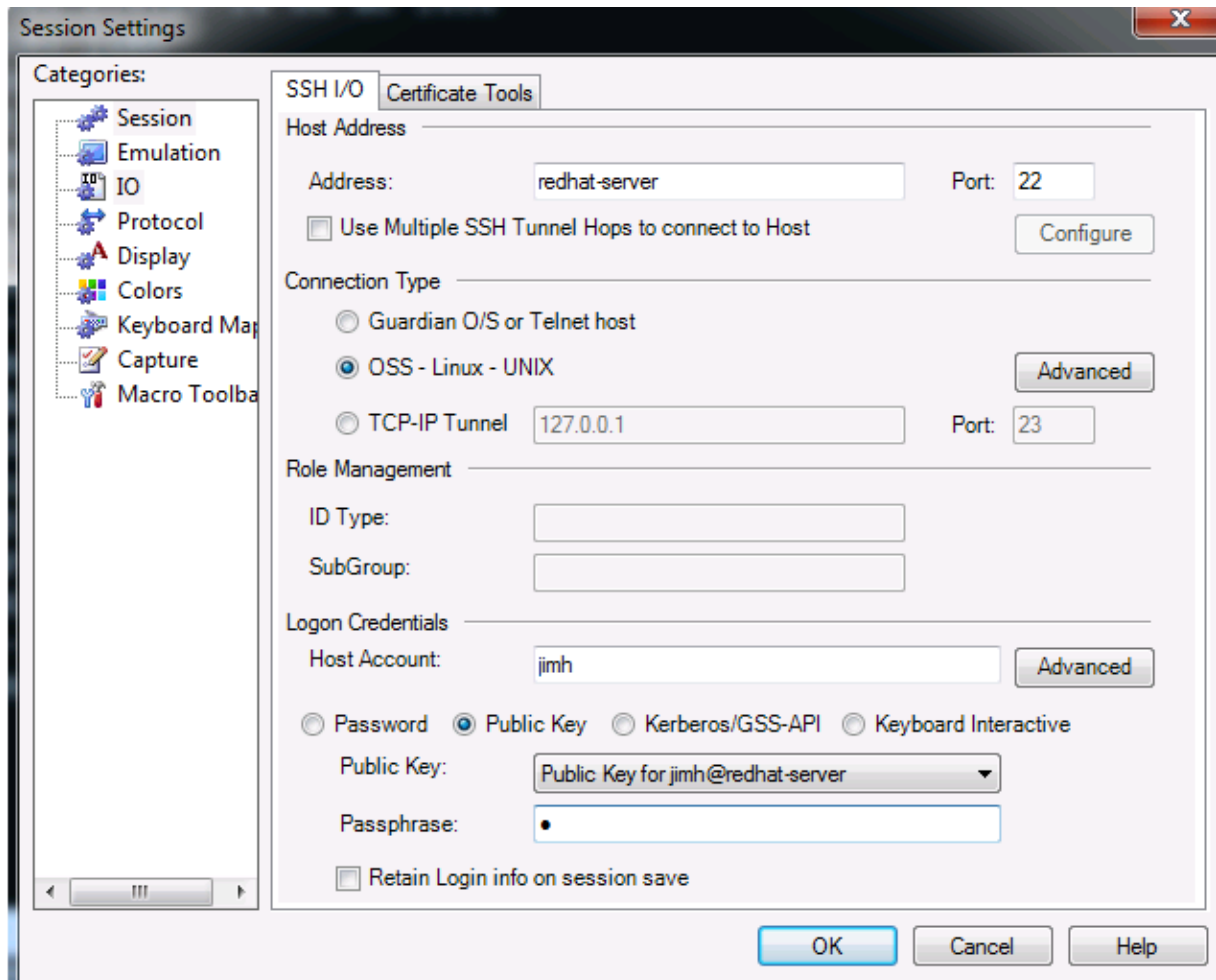
```
[jimh@redhat-server .ssh]$ cat jimh@redhat.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: Public Key for jimh@redhat-server
AAAAB3NzaC1yc2EAAAADAQABAAQADLn9WVYcxrZhdclRnuVTWW2mP3eWIuisLAXzsuIn/O
fI3dkRRz3FgS+wsXbk+64+l+6KAZHjKHHXQLU5Biwgg1DHi+EXi5/oNwkXp906vOuhxdq/Bz
MWBusc9CgI6gOvThcdETPCYGPLBF5RH4jsGXLzBtmyudEZt0I3iuF1t3kTXwxOExaP3vsXDz
spZ82R7DLjkVhWsluhkYvwDnZcaXL4m9lnh9UK1drAR1V+Yj6NlrCkmURAtw6enDCAKCV4Gk
X4EF4lGKuKHFb+aI1mj1QIvKHnk2kdFiQzRIEsCVFSEvtS+LRLTPTZgqTnhyASazX5UFe1qr
13z4LttE58tf
---- END SSH2 PUBLIC KEY ----
```

If the key is not an SSH2 key, you must convert an SSH key to SSH2 for use with the SSH I/O for OutsideView. Perform the following steps:

2. Login to your user ID on the UNIX or LINUX box
  1. Change to your SSH cache directory by issuing the command "cd .ssh"
  2. Locate your private key. It is typically named something like: [user@host](#)
  3. At the command prompt, type "ssh-keygen -e -f [user@host](#)>>[user@host.pub](#)"
  4. Copy the two key files to your PC workstations.
    - a. Start OutsideView, select View, Configuration Data Folder from the menu.
    - b. From the Configuration Data folder, navigate to the "SSH store" directory.
    - c. Copy the current directory path to the clipboard
  5. Open a file transfer session to your UNIX or LINUX box.
  6. In the local side of your file transfer window, enter the path from the clipboard
  7. Still in the local side, select the "private" directory and download the file [user@host](#) from the LINUX/UNIX system
  8. Next, still in the local side, navigate up a level and then back down to the "public" directory
  9. Download the [user@host.pub](#) file
  10. At this point, you may double click the [user@host.pub](#) file in the local window to invoke OutsideView's internal editor to change the comment line to something more relevant than the comment automatically inserted by the ssh-keygen program

You can now configure your SSH session in OutsideView;





Note the Passphrase input box has a single space entered in it. Since passphrase is not used for this type of private key file, it simply keeps the SSH layer from thinking you haven't entered one yet and skip the prompting step.

#### 5.14.2.7 SSH Encryption Algorithms

Please refer to the readme file for the most current list of supported SSH Encryption Algorithms.

NOTE: The host SSH layer determines which of these Encryption Algorithms is offered.

### 5.14.3 SSL Encryption

An essential component of any security implementation is positive identification of the communicating parties (authentication). OutsideView provides two methods for authenticating the SSL server, validation against the local certificate store and validation of the root CA fingerprint.

#### 5.14.3.1 SSL Server Authentication

##### Server Authentication

OutsideView provides two methods for authenticating the SSL server; validation against the **local certificate store** and validation of the **root CA fingerprint**.

Server Security/Certificate Options

Validate certificate against browser certificate store

Validate root CA fingerprint

Allow user override of errors to permit connection

Hide warning messages

Validate certificate CN against domain name

Optional partial CN/DN:

Advanced Certificate/Encryption Options

### Validate Certificate against local browser certificate store

This method of validation requires a server certificate on the host system that can be authenticated via the chain of authentication within your local browser certificate store. Such certificates are typically obtained from your organization's security group, or can be generated using the tools from OpenSSL.

For connection by remote users, the end user should be provided with some means of independent validation of the identity of the signing CA as well as the target host. Validation against the browser certificate store requires that the root CA certificate received from the server match a certificate already in the list of trusted certification authorities at the workstation. In addition, the common name included in the server certificate must match the fully qualified DNS name of the host being contacted\*. These steps assure that the communication is with a known host whose identity has been validated by a trusted authority virtually eliminating the possibility of "man-in-the-middle" spoofing.

If an organization maintains their own certificate authority, it is unlikely that the certificate from that CA will be in the certificate store of remote computers. The CA certificate may be distributed as a file and imported into the local computer's certificate store through the Microsoft Management Console (mmc) or it may be directly imported using OutsideView (if user override of server authentication errors is enabled).

To create an encrypted OutsideView session that validates against the browser certificate store: Within the Session Settings tab, I/O category:

1. Select "Encrypt datastream using SSL".
2. Select "Validate Certificate against browser certificate store" (default).
3. The "Advanced Certificate/Encryption Options" will allow selection of a cipher suite and definition of OCSP parameters. The Enable OpenSSL Default Cipher Suites radio button option is selected by default.

By default, authenticating against the local certificate store requires an exact match between the Common Name (CN) stored in the server certificate, and the returned DNS name of the server. This is to assure a one-to-one, unique identity match. OutsideView 8.0 and higher permits connections when the server certificate CN name field and server DNS name do not match exactly. This can be configured two ways: either entirely disable CN name validation within the certificate (not recommended), or leave validation on, but permit validation between a portion of the CN field and the server DNS name. This second method would permit, for instance, a single server certificate, generated for a particular domain, to be used successfully on multiple servers.

### Validate root CA fingerprint

This option permits session authentication by providing the public portion of the CA fingerprint. For intranet access where the users are likely to be employees of the organization, validation of the root CA fingerprint is probably sufficient. This method will insure that the server being accessed has

obtained a certificate signed by a CA trusted by the organization. The OutsideView administrator can create and distribute session configuration files (\*.cps) that contain the fingerprint of the root CA certificate.

If you wish to authenticate the server based on the fingerprint of the root CA certificate, you may obtain the fingerprint from your host administrator. To include the root CA certificate fingerprint in the session settings:

1. In the Session Settings I/O tab, select "Encrypt datastream using SSL".
2. In the "Server Security/Certificate Options" group, select "Validate root CA fingerprint".
3. Enter the value displayed in the Certificate Tools for the fingerprint value.

An option to **Allow User override of errors** is also provided to allow connection if the server authentication should fail. This facilitates testing or may be used where connectivity is paramount over security..

An option to **Hide warning messages** is provided to prevent non-fatal warnings from distracting end-users.

#### **Validate Certificate CN against domain name**

By default, authenticating against the local certificate store requires an exact match between the Common Name (CN) stored in the server certificate, and the returned DNS name of the server. This is to assure a one-to-one, unique identity match. OutsideView 8.0 and higher permits connections when the server certificate CN name field and server DNS name do not match exactly.

This can be implemented in two ways: either entirely disable CN name validation within the certificate (not recommended), or leave validation on, but validate a provided string against any portion of the CN field. This second method would permit, for instance, a single server certificate, generated for a particular domain, to be used successfully on multiple servers.

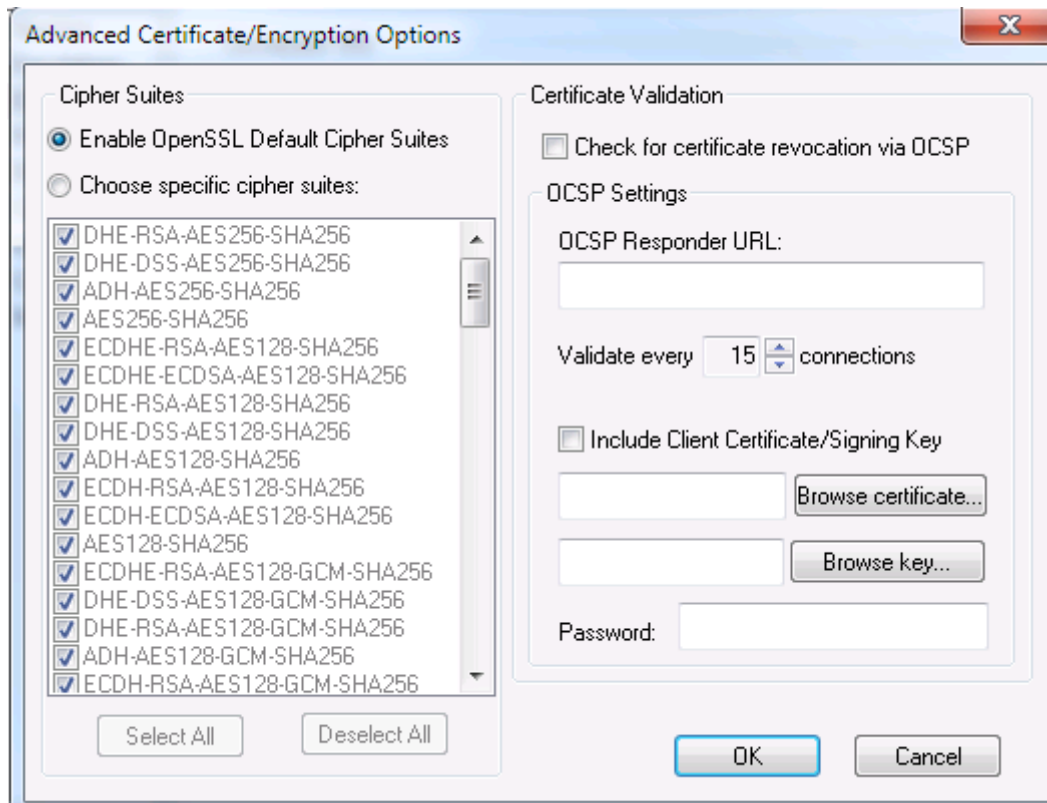
#### **5.14.3.2 Advanced Certificate/Encryption Options**

A **cipher suite** is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) network protocol.

The structure and use of the cipher suite concept is defined in the documents that define the protocol (RFC 5246 standard for TLS version 1.2). A reference for named cipher suites is provided in RFC 2434, the TLS Cipher Suite Registry.

In essence, the host system and the OutsideView client exchange a list of the cipher suites each supports, and negotiate to choose a common mechanism for encrypting the data packets transiting the connection.

By default, OutsideView supports the OpenSSL default cipher suites. This is a frequently changing list. The specific cipher suites OutsideView supports within that list are those checked ON in the drop-down lists of suites;



Alternatively, users may select a specific mix of cipher suites, by selecting the "Choose specific cipher suites" radio button option, and checking ON and OFF suites as they choose. When the "Choose specific cipher suites" option is enabled, buttons to Select All or Deselect All are also enabled.

The enabled cipher suites must include at least one suite supported by the target host. The strongest cipher supported by both parties will be determined during the SSL handshake and used for subsequent communication.

### TLS1.2 Cipher suites

DHE-RSA-AES256-SHA256  
 DHE-DSS-AES256-SHA256  
 ADH-AES256-SHA256  
 AES256-SHA256  
 ECDHE-RSA-AES128-SHA256  
 ECDHE-ECDSA-AES128-SHA256  
 DHE-RSA-AES128-SHA256  
 DHE-DSS-AES128-SHA256  
 ADH-AES128-SHA256  
 ECDH-RSA-AES128-SHA256  
 ECDH-ECDSA-AES128-SHA256  
 AES128-SHA256  
 ECDHE-RSA-AES128-GCM-SHA256  
 DHE-DSS-AES128-GCM-SHA256  
 DHE-RSA-AES128-GCM-SHA256  
 ADH-AES128-GCM-SHA256  
 ECDH-RSA-AES128-GCM-SHA256  
 ECDHE-ECDSA-AES128-GCM-SHA256

AES128-GCM-SHA256

### OCSP Certificate Validation

OCSP is a means for dynamically checking the revocation status of security certificates. To use this capability:

1. Check the "Check for certificate revocation via OCSP" check box.
2. Define the URL of the OCSP responder in the "OCSP Responder URL" field.
3. Define how often you wish to check the status of the server certificate in the "Validate certificate every [ ] connections" field. This check may be time-consuming and you may not want to incur this delay too often.

Some OCSP responders require authentication of the requesting clients. If a client certificate is required:

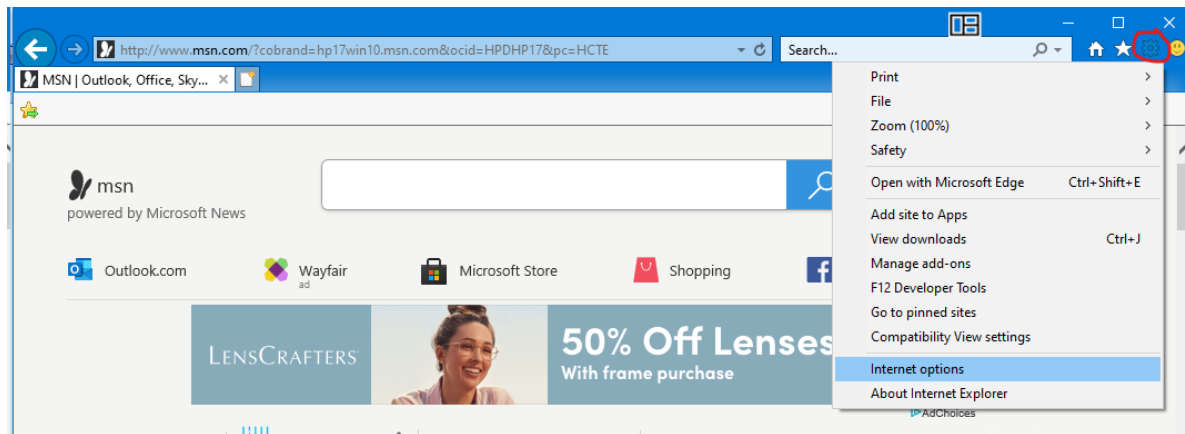
Check the "Include Client Certificate/Signing Key" check box.

1. Define the fully qualified path to the local client certificate (you may browse to its location).
2. Define the fully qualified path to the signing key (you may browse to its location).
3. Define the signing key password.

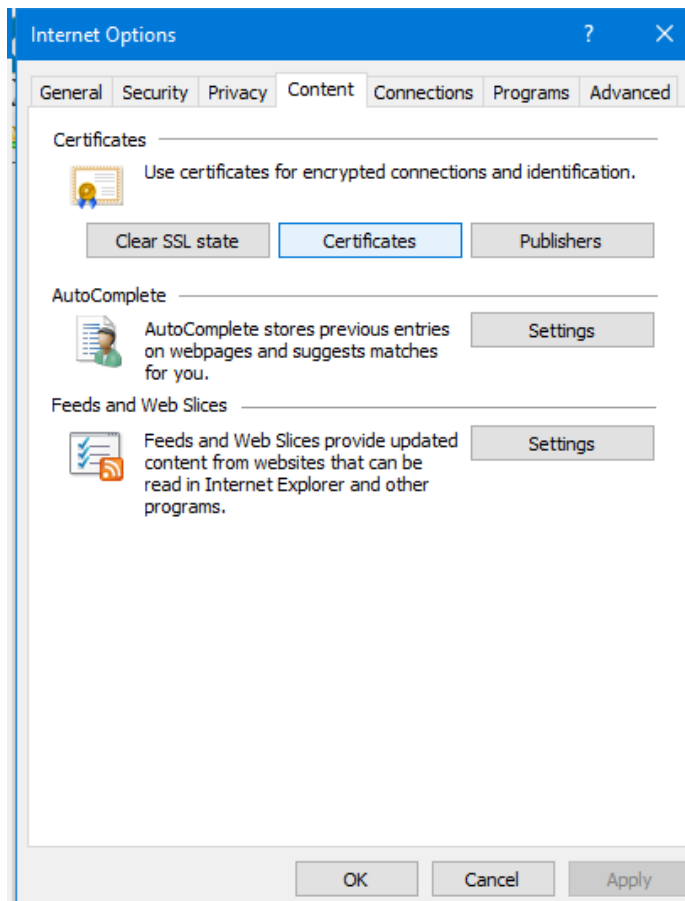
#### 5.14.3.3 Importing Root CA Certificates

##### Importing Root CA Certificates

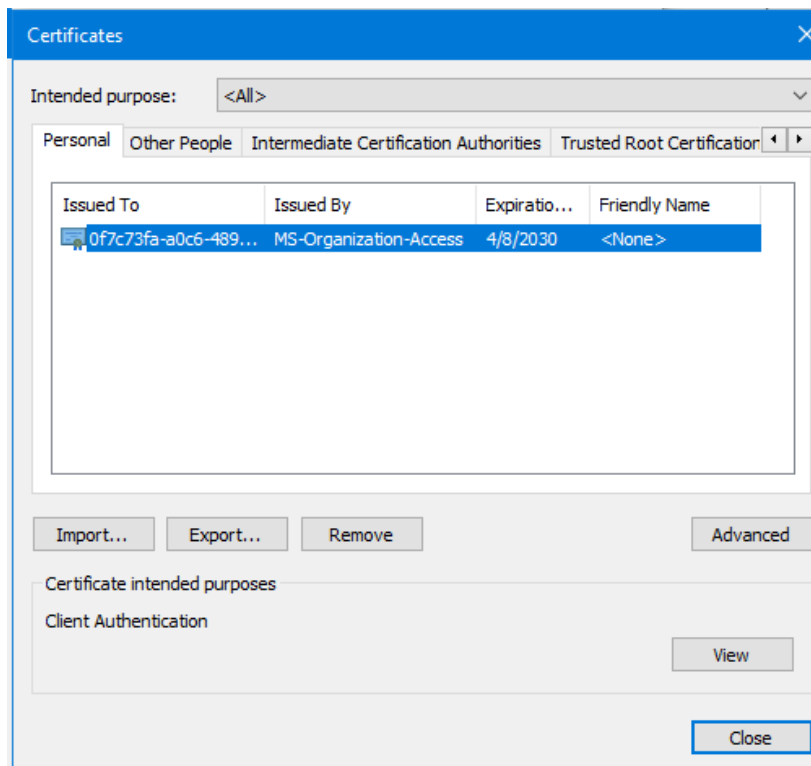
During the SSL handshake with the host, the OutsideView client will receive a certificate authenticating the server along with a self-signed Certificate Authority (CA) certificate. The CA certificate may be distributed as a file and imported into the local computer's certificate store through the Microsoft Management Console (mmc) or it may be directly imported using Internet Explorer 11 browser:



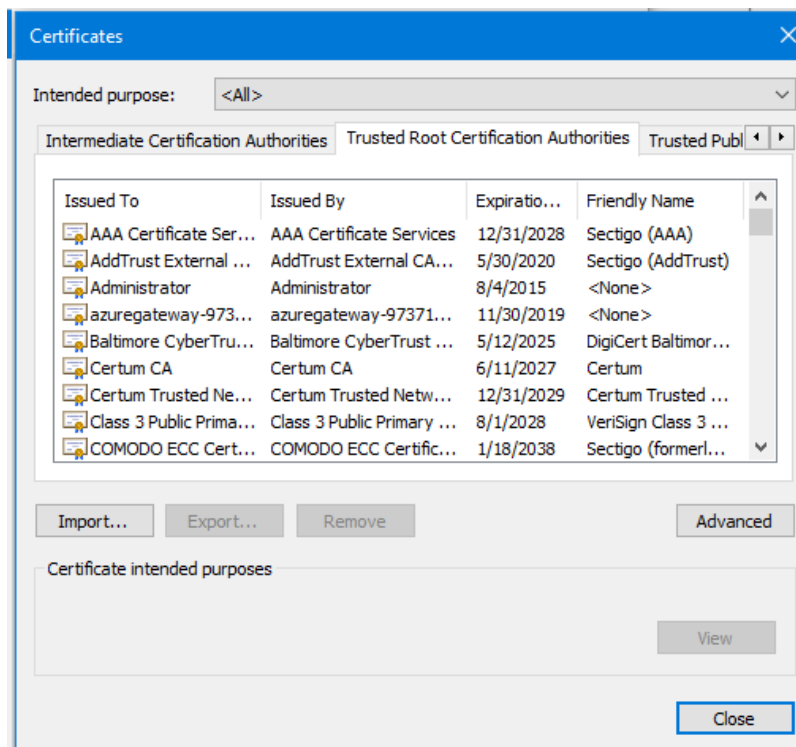
After clicking on the Internet options menu you should see Internet Options dialog box come up:



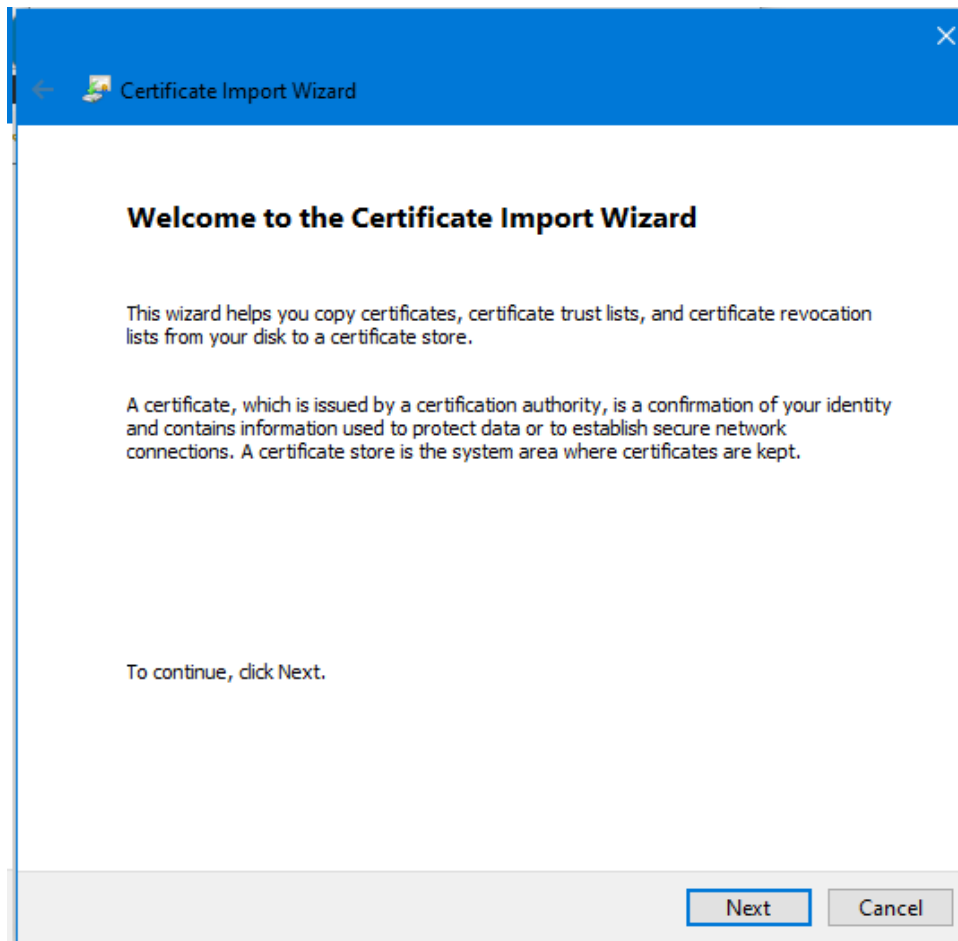
Click on the Content tab and then click on the Certificates button. The Certificate dialog box should come up:



In the Certificates dialog box, click on the Trusted Root Certification Authorities tab and check to see if the Root CA is present there. If not then you will need to import the certificate into here:

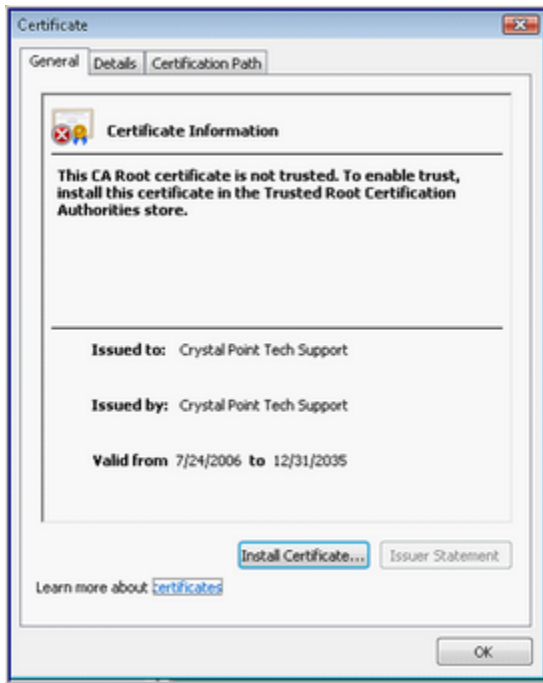


Finally click on the Import... button to launch the Certificate Import Wizard to import the Root CA Certificate into the IE Browser store:

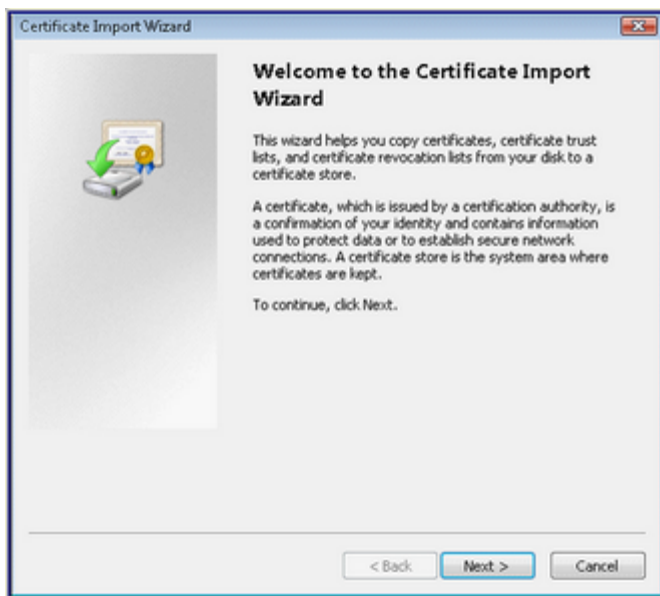


Alternatively, you can also click on the Certificate itself and that will bring up a Certificate dialog like below:





Click on "Install Certificate..." to launch the Certificate Import Wizard:



Accepting all the defaults presented by the import wizard will add the CA certificate to the individual user's local certificate store. Success is confirmed by the following message:




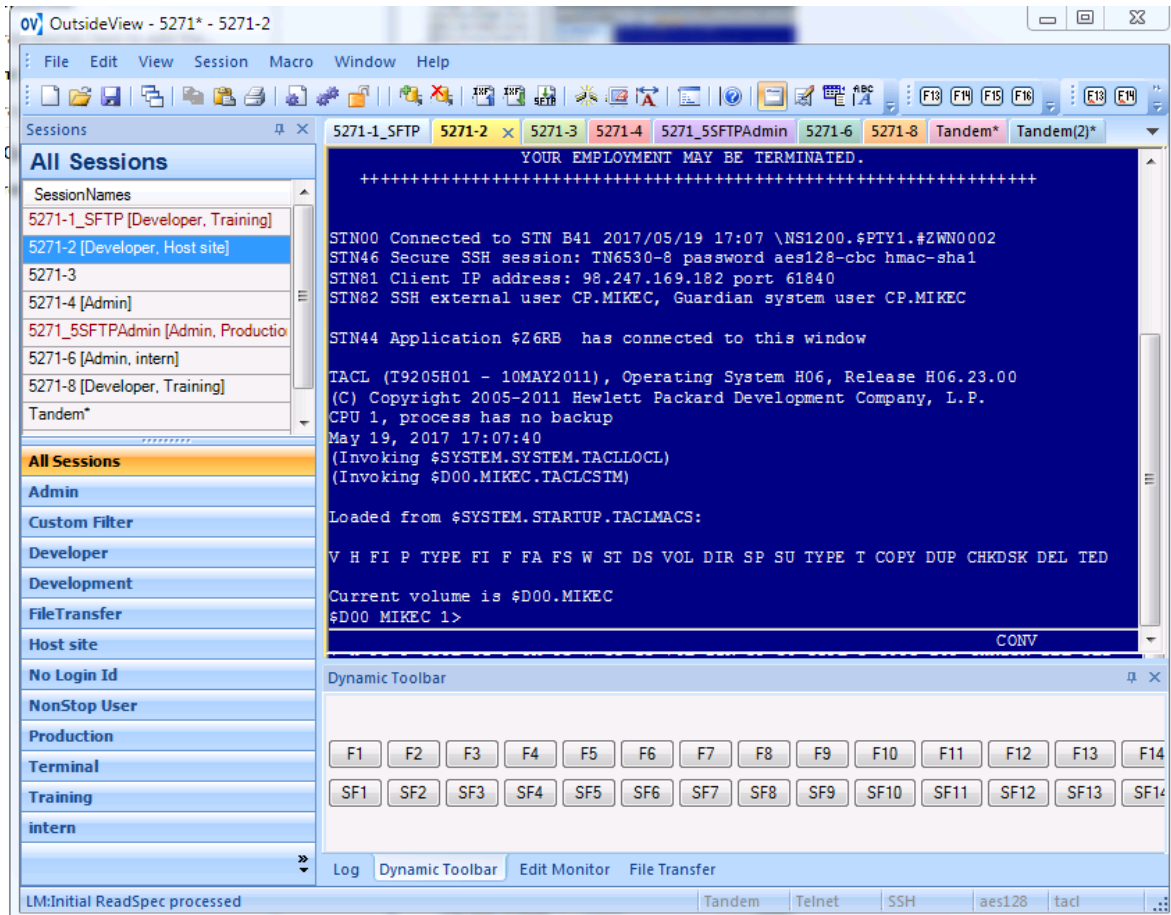
This operation needs to be done only once, per user. All subsequent connections to the host should proceed normally once the certificate has been imported. **Note** if you need to perform this per PC, then install the certificate into the Trusted Root Certification Authority instead.

## 6 Using OutsideView

### 6.1 OutsideView UI Overview

#### OutsideView User Interface Overview

Click on areas of the screen below to access more details on that topic. Click  [Back](#) to return here.



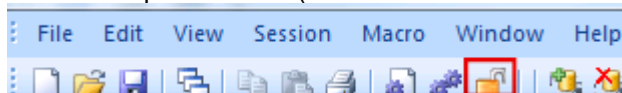
## 6.2 Session Settings Password

### Session Password

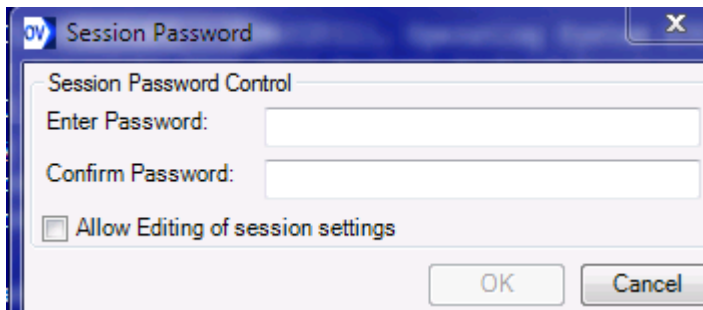
If your organization does not use the full capabilities of Enterprise OutsideView to create, distribute, update and protect your session files, you may find yourself in the position of distributing session files to users manually or programmatically. With OutsideView 9.1, those session files can themselves be individually password protected. Now you can (optionally) protect what you send out from user modification, thereby avoiding potential internal support issues.

There are two ways to set the session password:

1. Session | Session Settings Password menu
2. Tool bar padlock icon (unlocked means session is not protected):



To set the password on a session click on the toolbar unlocked padlock icon or Session | Session Settings Password menu. The Session Password dialog box will pop up:



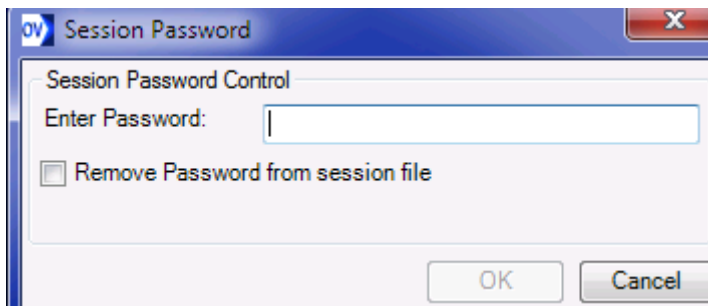
The **Allow Editing of session settings** checkbox permits the session owner to continue to modify session settings even after the session password has been set. Enter the password and then click on the OK button. User should notice that the unlock padlock icon becomes locked:



In order for users to modify the session settings they will need to unlock the session by providing the session setting password. To do this you can either way:

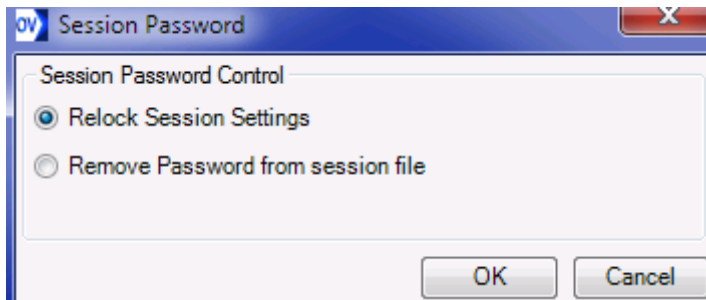
1. Click on the tool bar lock padlock icon or
2. From the menu Session | Session Settings Password.

User should see the following Session Password dialog box:



Users have the option of removing the password from this session file in addition to unlocking it via the password.

When the users go back and lock the session again via the menu or the tool bar icon, they will see the following dialog box pop up for Session Password:

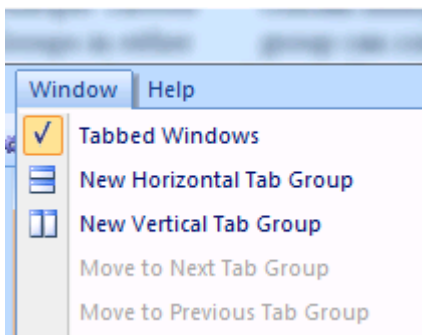


They can relock the session again or remove the password from the session file.

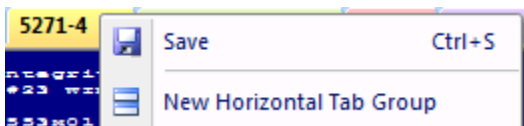
## 6.3 Working with Tabbed Group Windows

OutsideView 9.0 introduced the concept of multiple sub-groups of sessions in a single workspace. Each subgroup can contain multiple sessions, oriented vertically or horizontally.

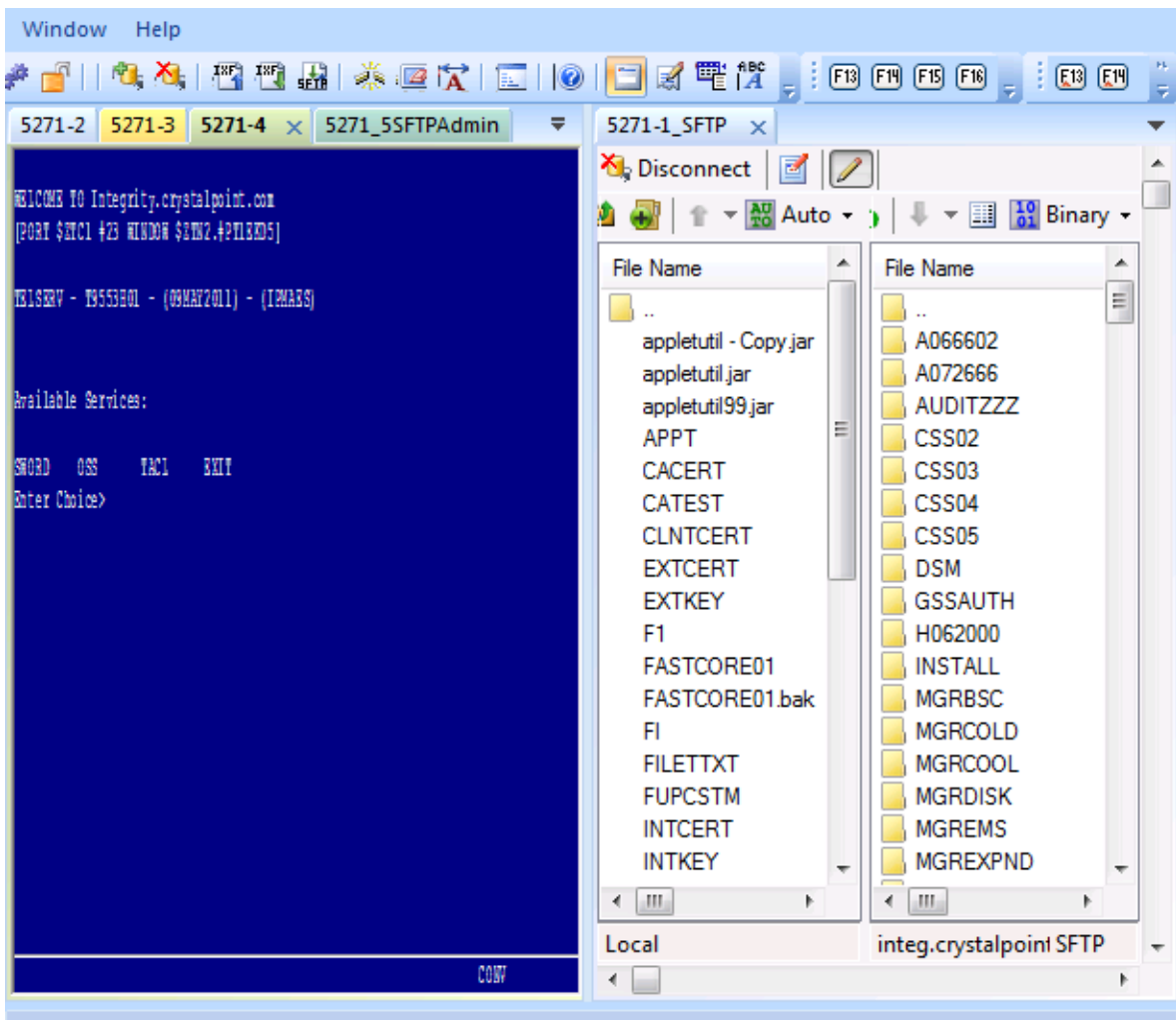
In order to use tab groups, you will need to make sure that OutsideView is in Tabbed Windows mode:



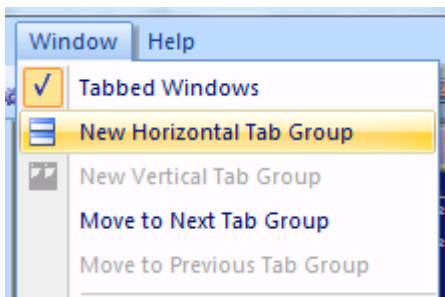
After confirming that OutsideView is in Tabbed Windows mode, the next step is to select New Horizontal Tab Group from the menu Window | New Horizontal Tag Group or right click mouse button on active session



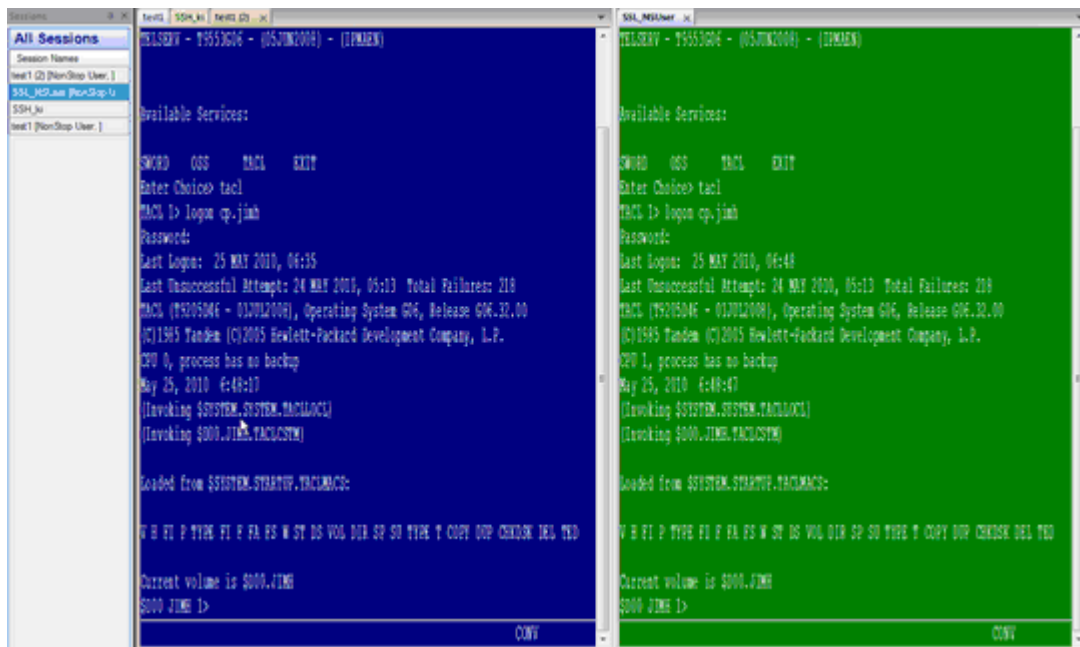




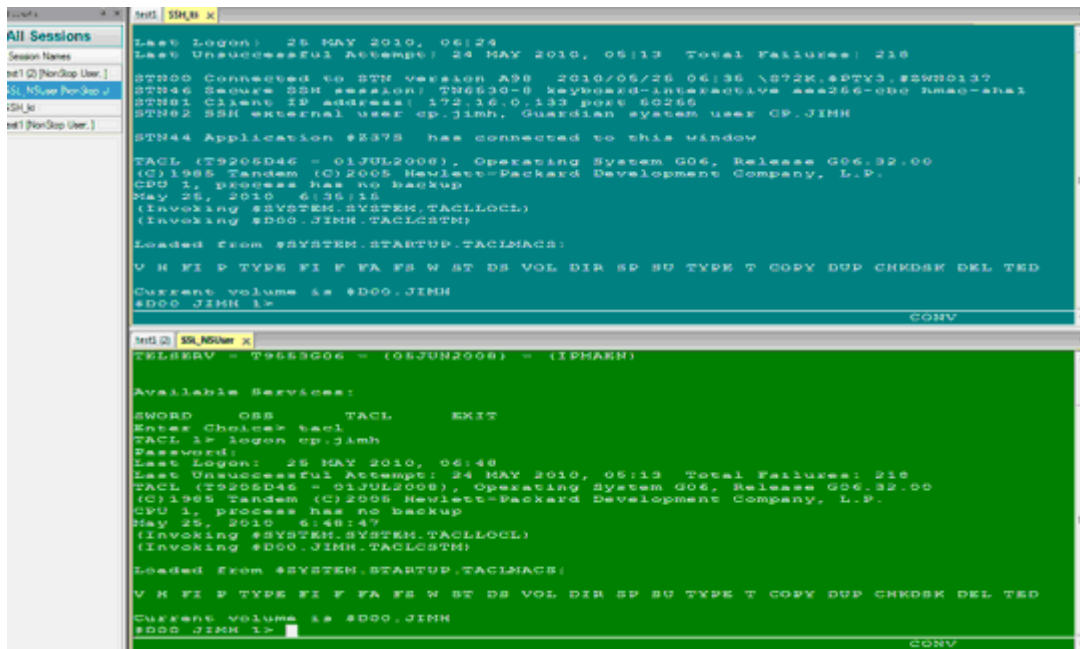
After selecting a tab group (horizontal or vertical), all new tab groups that can be created will be of the same group and the other tab group option will be greyed out:



Users may also drag and drop a given tab to the right to create one or more secondary tabbed view frames,



or drag a tab to the bottom of the frame to create horizontally stacked secondary frames:



When you have multiple tabbed view frames, you can move tabs from one frame to another simply by drag/drop the tab from one frame to another.

To close a frame, drag all tabs from it to another frame. An empty frame will close automatically. If you drag all tabs back into a single frame you can reselect the option of creating a vertical tab group or horizontal tab group.



## 6.4 IPV6

### IPV6

IPv6 is fully implemented in OutsideView 9.1. It provides more efficient data transport for long distance network communications. With named hosts, Domain Name Services will generally present IPV6 addresses before IPV4 addresses, allowing smaller connect delays.

Our implementation of IPv6 integrates seamlessly with standard IPv4; using internal logic to try any and all addresses returned by DNS. For instance, consider our feature of automatic failover, where a session file can contain a list of host addresses and ports, to which OutsideView will connect in order, as available. You can intermingle IPv6 and IPv4 addresses in that list - achieving maximum flexibility and fault tolerance in connectivity for your users.

IPv6 is supported in in the following I/O drop down options:

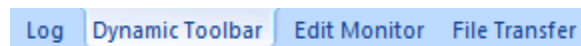
- SSH
- TCP IP / SSL

The format for directly entering IPv6 addresses is the RFC standard format of surrounding the address with brackets. I.E. **[2001:DEAD:BEEF:CAFE::100]:23** with the :23 being the port number if being overridden. You can also use IPV6 addresses in the Failover scenario for the Host field.

**Failover:** If you want your session to try to alternate host and port combinations such that if the first address/port does not work OutsideView will attempt the next address in the list. User will need to provide address information in the form: host port, host port, host port, ... For example:  
host1.crystalpoint.com 19, host2.crystalpoint.com 6, [2001:DEAD:BEEF:CAFE::100]:22,  
host3.crystalpoint.com 6020

## 6.5 Dynamic Windows Area

OutsideView offers a number of new, dynamic (auto-hide) windows to help you get the most out of our product. For instance, there are new file transfer progress monitors, dynamic toolbars, and edit monitors. Merely click on these items to bring up a window containing information. These windows can be pinned or unpinned (auto-hide).



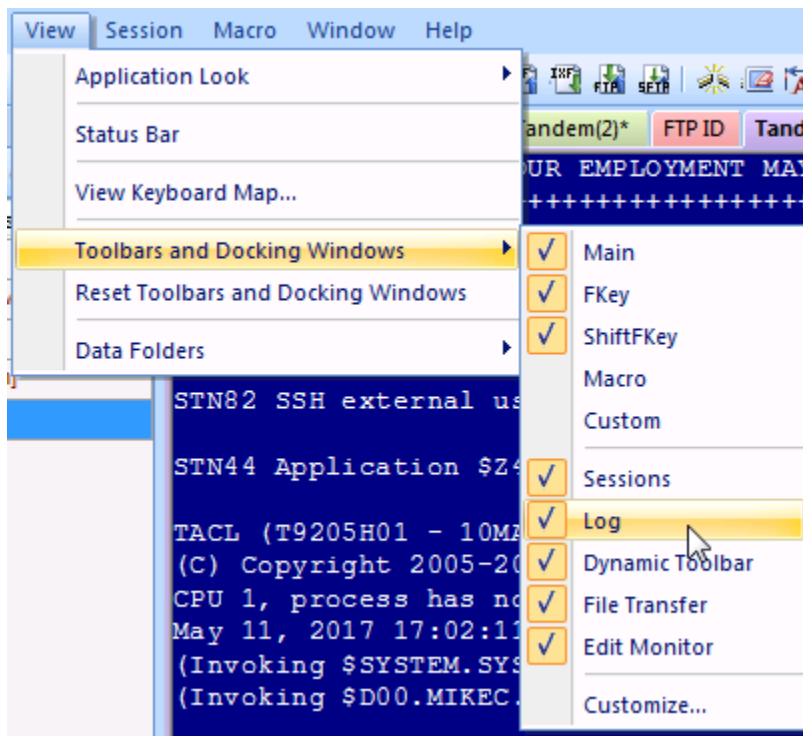
For more information, see the topics [Application Log](#), [File transfer Progress](#), [Edit Monitor](#), and [context-sensitive dynamic toolbars](#).

## 6.6 Application Message Log

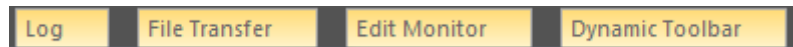
### Application Message Log

OutsideView maintains a log of messages for the entire application. This list of messages, including errors, is called the application log.

To Access the Application Message Log users will need to enable the Log option from the menu:



Once the Log menu item is enabled (checked), the user should see the Log panel area in the bottom area of the OutsideView screen. Just 'hover' the mouse over the log area of the dynamic window area.



This will display the Application Message Viewer window for this instance of OutsideView. You can now read the log, purge it, or save it to disk.

### Filtering Application Log

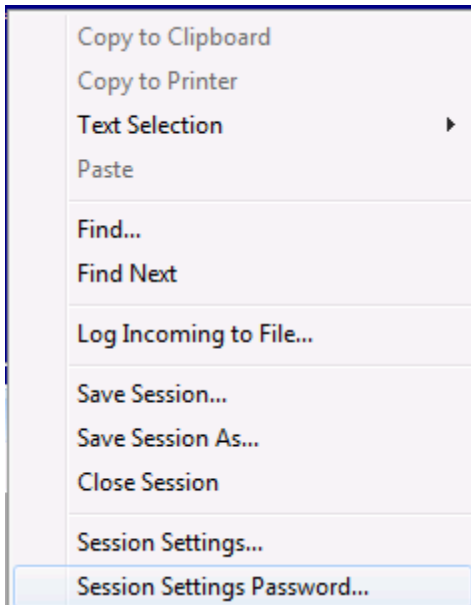
In the upper right corner of the application log is a control for source. The default source is All. You may select the down arrows and select from various individual sources (i.e., active sessions).

## 6.7 Right-Click Option

### Right-Click Options

By default, users may right-click their mouse while in a session to see the following options:

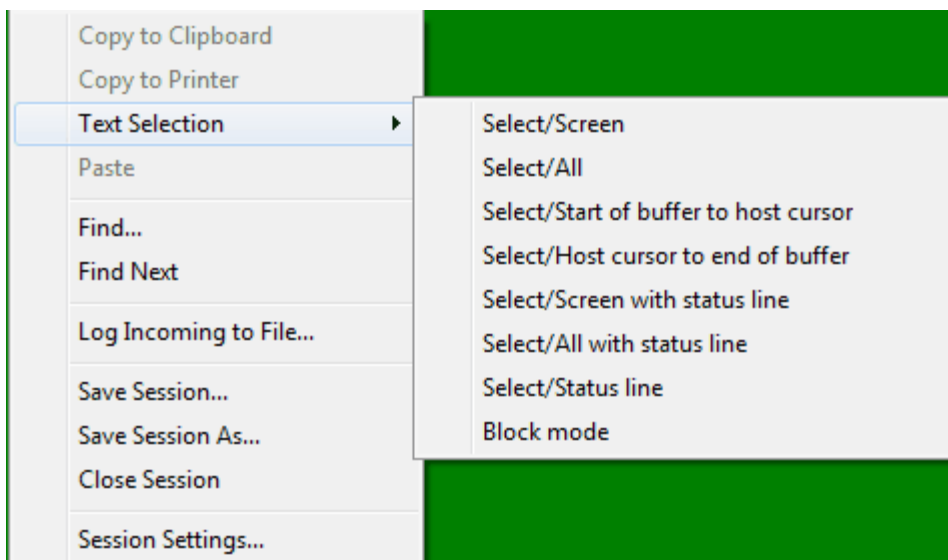
**NOTE:** OutsideView Supervisors have the option to disable this feature within Enterprise mode



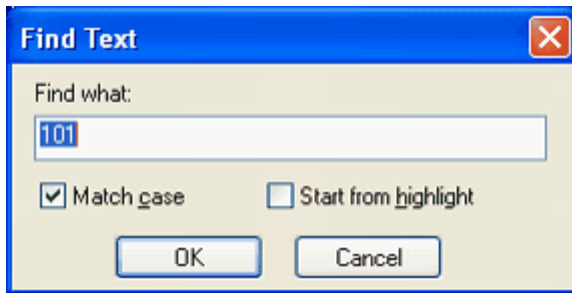
**Copy to Clipboard/Copy to Printer\*** will be enabled only when text is selected.

\*OutsideView Supervisors have the option to disable this feature within Enterprise mode

**Text Selection** offers sub-options that quickly and efficiently select the text you need:



**OutsideView Find/Find Next** OutsideView now offers a simple text search function for Tandem conversation mode session buffers. This can prove particularly useful, for example, in locating specific events in log files and should be of particular value to those involved with operations. This makes use of the existing text highlighting functionality.



**Save Session/Save Session As** let you quickly save new or modified session definitions (in Enterprise, this capability can be disabled).

**Close Session** closes the active or in-focus session,

**Session Settings** lets you access session settings from a right-click

**Session Settings Password** lets you password protect the session so users can't modify the settings

## 6.8 Printing

### Printing

OutsideView supports printing of the active session screen or a log of session activity.

To print the active session screen:

- Select File/Print Screen
- or
- Click the Print Screen toolbar button.

See the [Logging Session Activity](#) topic for instructions on printing a log file.

## 6.9 Copy/Paste

### Copy/Paste

OutsideView supports normal copy/paste operations within sessions. The text selection behavior may be either as rectangular blocks or line – by – line. See the [Display Tab](#) topic for instructions on setting this behavior.

**Note:** *OutsideView will insert a carriage return/line feed at the end of each line copied from the screen.*

Please also refer to the topic [Unix/x11 mouse text selection](#) for information on this quick and easy copy paste method.

## 6.10 Searching Buffers

### OutsideView Find/Find Next

OutsideView now offers a simple text search function for Tandem conversation mode session buffers. This can prove particularly useful, for example, in locating specific events in log files and should be of particular value to those involved with operations. This makes use of the existing text highlighting functionality.

### Usage

Two new menu options are offered under the Edit menu: “**Find...**” and “**Find next**”.

“Find...” will display a dialog which allows the user to specify the search string.

It includes two options: “Match case” and “Start from highlight”.

When match case is on, the string “TACL” will not match “tacl”.

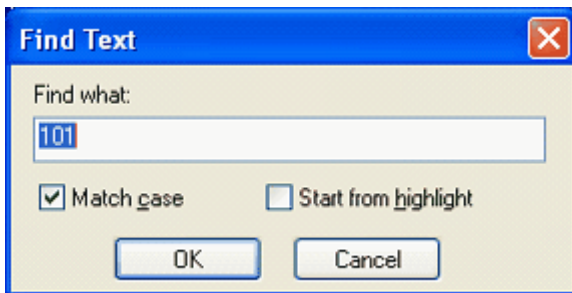
When “Start From Highlight” is on, the search will begin from the beginning of any actively highlighted text. Text can be highlighted by dragging the mouse over the desired area. If this option is off, or if no highlight is present, the search begins from the top of the buffer.

Once the user hits OK, OutsideView will immediately highlight any found match, and ensure it is displayed in the viewport.

“Find Next” searches from the current highlighted text plus one character.

If the current session is not searchable (is block mode or non-Tandem), the menu options will be grayed out accordingly.

### Example



## 6.11 National Character Set Support

### National Character Set Support

Proper handling in OutsideView of characters typed and returned from the host depends on proper settings for:

- Windows language
- OutsideView session language
- NonStop application mode (conversational or block)
- OutsideView session host file encoding (OEM or ANSI)
- OutsideView session 7-bit language
- OutsideView session font

The Windows language setting for an application determines keyboard mapping and the ANSI code page that will be used by default. Windows applications will receive (e.g. keyboard input) or send

(e.g. display) characters as their ANSI or Unicode values. OutsideView accepts only the ANSI character table (not Unicode) from Windows. For a complete listing of the code pages used for various language settings, see <http://www.microsoft.com/typography/unicode/cscp.htm>. For example, the ANSI code page used for Swedish, Norwegian and Danish is 1252 (Latin I). If your Windows workstation is set for Swedish, pressing the "Å" key sends a value of C4h (from the ANSI code page) to the in-focus application. If the application displays that character, it will display the glyph indexed by that value defined in the font currently selected in that application.

OutsideView also allows selection of the language for each session. This feature allows the user to view host files containing characters not included in their current Windows language setting. If the user wishes to edit the file, the keyboard mapping would have to be changed by selecting the desired language within Windows.

To support host files that were encoded using the OEM code pages, OutsideView allows a choice of OEM or ANSI for the code page used for each session. If ANSI is chosen for host file encoding, the value received from Windows is used directly to reference the correct character in the ANSI code page. If OEM is chosen, the ANSI value received from Windows is translated to the OEM value, and that value is used to index the correct character for the OEM code. With OutsideView settings of OEM host file encoding and a Windows language setting of Swedish, typing an "Å" on your Swedish keyboard will send a C4h value to OutsideView which translates that value to 8Eh and references the OEM codepage 850 to determine the correct character.

The Tandem 6530 terminal also provides support for the ISO 646 7-bit character set, also known as the NRC (National Replacement Character) set. To allow display of international characters, this character set uses a character substitution method in which certain characters from the ASCII character set (lower 127 code values) are replaced by characters from another language. With a Windows language set for English (United States), OutsideView language set to Swedish, host file encoding set to ANSI and using the 7-bit translation, pressing a "[" on the keyboard will send a 5Bh value to the emulator. If telnet line mode is active, the emulator will substitute the value C4h and send that value to the display. The value C4h corresponds to the "Å" glyph in the 1252 (Latin I) codepage (the active code page for an English US Windows language setting). The typed 5Bh value is stored in the buffer until a carriage return at which time the entire line is sent to the host. If telnet line mode is not active, the 7-bit value for the typed character is sent to the host. The host echoes that value back, and the emulator will substitute the correct international character.

Characters whose code value lies in the range of 80h to 9Fh are defined within Tandem 6530 terminal operations as upper control characters. Sending a character with a value that falls in that range to the host in conversational mode will be interpreted by the host as the beginning of a command. If the telnet protocol is not set for line mode, the host will echo back a caret (code value 5Eh) and another character. After a return, the typed character is returned by the host along with an error message. Typing a Euro character (€) at a tac! prompt (with host file encoding set for ANSI) will show this behavior since the code value for that character is 80h.

If your Windows workstation is set for a language other than English (United States) and you wish to send the characters corresponding to the keyboard map for that language, you should use ANSI host file encoding and not select the 7-bit Language setting. From your screen shot and session file, it appears that you were changing the Windows language and OutsideView language settings and typing three characters. The errors are due to selection of OEM host file encoding and 7-bit language.


## 6.12 Logging Session Activity

### Logging Session Activity

OutsideView provides the capability to log the data you receive from the host, with or without host control codes (escape codes). You can log incoming host data to either a file or a printer. Note that data is logged as it is received: raw and unformatted. This means that formatted screens, such as Tandem block mode applications, will not appear in the log as they do on the session display.

If any errors occur opening a trace or log file, or opening and writing to a save file, then an error box is displayed describing the error and the trace file or log file setting is turned off automatically. Data logging automatically stops when you close the session that is being logged and does not automatically restart if you reopen the session.

To Enable or Disable Data Logging:

1. Place the desired session in focus by clicking the session window, clicking the icon in the Shortcut Bar, or by selecting it from the Window menu.
2. Either:
  - Use the File: Log Incoming menu command, and then select either To File or To Printer.
  - or-
  - Click the Session Settings button  on the toolbar, or select Session: Session Settings.
3. Click the Capture category
4. Set the desired Log Incoming option: Log to File or Log to Printer.
5. If you select Log to File, specify a file name and whether you want control codes to be included in the log. Then click OK.

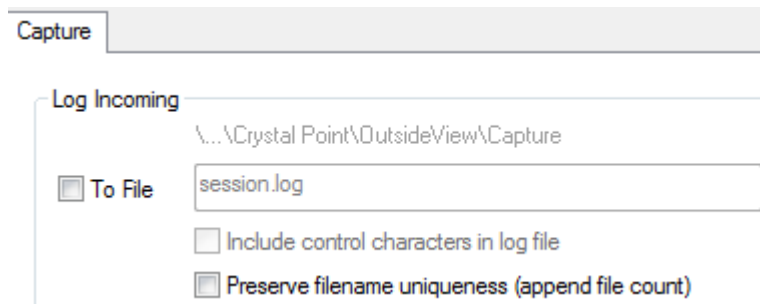
When you want to stop logging session data, simply repeat these steps and deselect the Log To option that you selected previously.

Logged session data saves to the Capture folder by default; you can specify an alternate location if you wish. That alternate location will become the default location until you close that session.

### Logging to Network Locations

If you specify a network location for your log files, it is recommend you use UNC pathing format (e.g. \\server\_name\folder\file) . If you user mapped drive format (e.g. w:\folder\file), the mapping may change and impact logging. This is particularly important when using the Enterprise form of OutsideView, as all end-users may not have the same drive mappings.

OutsideView will resolve **log file name conflicts**. In Session Settings,category Capture, the Log to File choice offers the option to **preserve filename uniqueness**.



Checking this option ON will cause OutsideView to append trailing numbers, log 1, log2, log3, etc. - if multiple sessions are open that specify the same log file name.

**NOTE: This will require periodic removal of old files, because they will accumulate.**

## 6.13 Command Line Options

### Command Line Options

The OutsideView command line provides you a method of loading a specific session file and/or macro during program startup. This is often an effective way to make sure the program launches in a standardized manner. Because you can specify full pathnames, you can use standard parameter and macro files located in shared network directories (instead of defaulting to user subdirectories).

❖ OutsideView accepts only one command line option.

**Command Line Syntax:**

[drive:]\Program Files\Crystal Point\OutsideView\outsplash.exe [option]

You can modify the command line either in Program Manager (click File, click Properties, edit Command Line field) or for the application shortcut (right click, click Properties, click Shortcut tab, edit Target field making all changes inside the quotes).

**drive:** The drive where the executable file outsplash.exe resides. If not specified, Windows uses the current drive.

**Options:**

Filename:

An optional parameter specifying the session file (.cps) to automatically load on startup. If not in the default PARAM directory, the full path (including drive, if necessary) must be specified. Long file names are supported by enclosing filename in double quotes.

/W filename:

An optional parameter specifying the workspace file (.cpw) to automatically load on startup. If not in the default PARAM directory, the full path (including drive, if necessary) must be specified. Long file names are supported by enclosing filename in double quotes.

/M filename:

An optional parameter specifying the Visual CommBASIC macro to automatically load on startup. If not in the default MACRO directory, the full path (including drive, if necessary) must be specified. The VCB extension is not required. Long file names are supported by enclosing filename in double quotes.

/Supervisor netpath:

An optional parameter specifying that OutsideView should launch in Supervisor mode. netpath is the network path to the user profile that will be administered on the Profile Server. Long file names are supported by enclosing netpath in double quotes.

/A guitype:

An optional parameter, provided for use in .Net controlled environments, to allow invocation of an OutsideView workspace or session, with a specific GUI level. Possible values are "minimalgui" which is no toolbars, or "simplegui" which is default toolbars only. Usage is similar to:

```
C:\Program Files\Crystal Point\OutsideView\outcore.exe C:  
\Users\jimh.CP\AppData\Roaming\Crystal Point\OutsideView\Param\telnet1.cps -A simplegui .
```

## 6.14 Guardian File System Graphical Navigation

### Guardian File System Graphical Navigation

This topic applies only to Hewlett Packard NonStop (Tandem) hosts and requires a NonStop Kernel environment of D20 or later.

OutsideView's IXF and FTP transfer facilities allow users graphical navigation of the NonStop Guardian file system. However it is necessary to provide this directory information to OutsideView. This can be done via **host hint files**, **FTP HINTS** or via the supplied **Host Scanning Utility**, **OVFSCAN**. If this directory information is not provided using one these two methods, users will need to specify exact system.volume.subvolume.file entries when transferring files. Depending on the



technical level of your users or security concerns, you may or may not need to offer host navigation services.

On NonStop systems without an OSS environment, host hint files are required for graphical FTP file transfer and for navigation. Host hint files can also be used for IXF transfer.

#### Host Hint Files

Hint files apply to FTP, and optionally to IXF. (For IXF, the preferred method is the Host Scanning Utility, detailed in the next section.) Hint files are static snapshots of the NonStop's directory and file structure. OutsideView uses the hint files for navigating host directories and displaying available files. To Use FTPHINTS and Create the Host Hint Files

1. Run OutsideView and establish a session to the desired host. You must be logged in and at the system or TACL prompt. Your logged-in user ID must also have super.xx or supervisor rights in order to create the necessary hint files.
2. Run FTPHINTS from the Utilities directory on the installation CD or from the menu choice Macro, Run Macro.

FTPHINTS uses the session to issue commands that create the necessary hint files. When users connect to the host and attempt IXF or FTP file transfers, those facilities in OutsideView access the hint files to allow graphical host navigation for both upload and download purposes. FTP transfers require hint files to offer this navigation; IXF transfers will use hint files if the host scanning utility (detailed below) is not detected.

**Note:** For NonStop systems without an OSS environment, *FTPHints* is required to permit graphical file navigation.

#### About the Hint Files

The hint files (SYSMAP, DRVMAP, DIRMAP) are a snapshot of the host file system. If your file system changes (new and deleted volumes, etc.), you need to run FTPHINTS again to update the hint files. As a general rule when using hint files, you should run FTPHINTS frequently to make sure you keep the hint files current with the host's actual file system.

If SYSMAP, DIRMAP, and/or DRVMAP are missing from host, the behavior of the FTP client will change. Even without these files, the dialog box-based FTP will still work, but the user will be warned that a file is missing. This warning will appear in the Status message box and indicates that FTPHINTS, located in the Util directory on the installation CD, should be run.

- If DRVMAP is missing, the Folders box in the FTP dialog box will be empty.
- If DIRMAP is missing, the FTP client issues a LIST command to the host, which may take longer to complete than expected (it is a slower procedure than parsing the DIRMAP).
- If SYSMAP is missing, the Volumes and Folders dialog boxes will become disabled. However, the list of files should appear. When these dialog boxes are disabled, the user cannot browse to the desired files and must manually enter the desired path. If the user wishes to change both volume and subvolume, they must be done in two separate steps: volume, then subvolume. Typing in a new volume and subvolume at the same time will result in the subvolume information being ignored.

For more technical information on and for mapping limitations of this macro, see the topic on FTPHINTS Macro Details.

#### Host Scanning Utility (OVFSCAN)

The host scanning utility OVFSCAN applies only to IXF transfers. This utility, because it runs each time the IXF transfer facility is invoked, provides a dynamic view of the Tandem's volume and file structure. OutsideView uses the information supplied by the host scanning utility for navigating host volumes and displaying available files. The host scanning utility OVFSCAN is provided for your convenience, and is found in the UTIL directory on the CD.

Once you have installed OutsideView and OVFSCAN, the procedure for uploading it to your Tandem host and enabling it for execution is:

1. Run OutsideView and establish a session to the desired host. You must be logged in and at the TACL prompt.
2. Select Session: Transmit File from the menu. In the Local Files list, click OVFSKAN. The file name automatically appears in the Host Filename field. Enable the Binary option. If you are not already in the system area, enter the host system in the Host Target Directory field. (For example, if your host uses the default system area, the Target Directory field should show "\$SYSTEM.SYSTEM.")
3. Set any other required options, then click OK. The utility is uploaded to the specified system area.
4. Once uploaded, you must enable OVFSKAN as an executable file. Make sure you are in the system area, and then type the command: FUP ALTER OVFSKAN, CODE 100

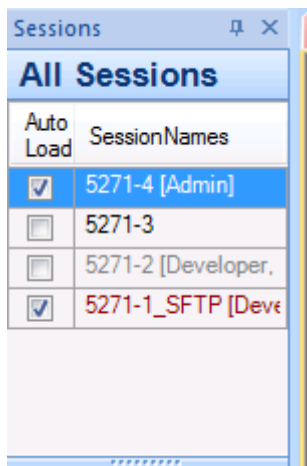
#### Notes

- When users connect to the host and attempt IXF file transfers, OutsideView uses OVFSKAN to allow graphical host navigation for both upload and download purposes.
- OVFSKAN requires a Tandem NonStop Kernel environment of D20 or later.

## 6.15 Session Bar Color Coding for Status

### Session Bar Color Coding for Status

Session Bar listings are now color-coded to complement the new Session Activation Control feature. Users can identify at a glance, by listing color, which sessions are preloaded but not yet active, which sessions are active, and which sessions are disconnected.



**Red** color -- Session is disconnected from host

**Black** color -- Session is connected to host

**Grey** color -- Session is not loaded

## 6.16 Session Bar Filter

### Session Bar Filter

The Session Bar displays all sessions by default via the All Session filter button. The Session Bar filter buttons are created dynamically based on session type (terminal, File Transfer, Code Editor),

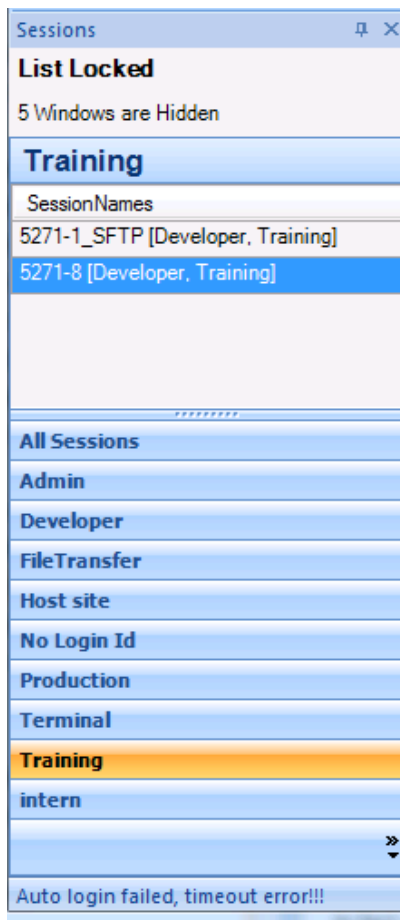
---

ID type and Subgroup Type. You can even create a Custom Filter to filter both ID and Subgroup together.

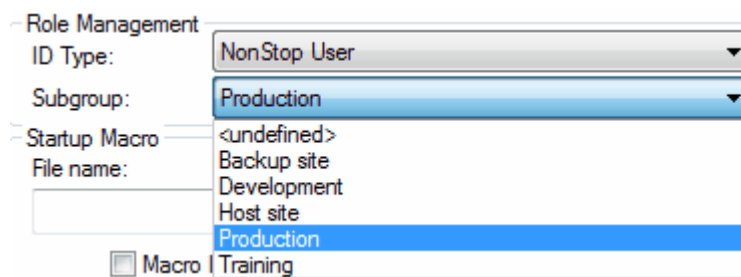
The filter buttons on the Session Bar allows you to specify only the sessions you want to see displayed in the Session Bar based on the filter. For example the filters below show All Sessions filter, ID type = Developer and Subgroup = Training:

Sessions	
<b>All Sessions</b>	
SessionNames	
5271-1_SFTP [Developer, Training]	
5271-2 [Developer, Host site]	
5271-3	
5271-4* [Admin]	
5271_5SFTPAdmin [Admin, Production]	
5271-6 [Admin, intern]	
5271-8 [Developer, Training]	
-----	
<b>All Sessions</b>	
Admin	
Developer	
FileTransfer	
Host site	
No Login Id	
Production	
Terminal	
Training	
intern	
	»
	▼
Ready	

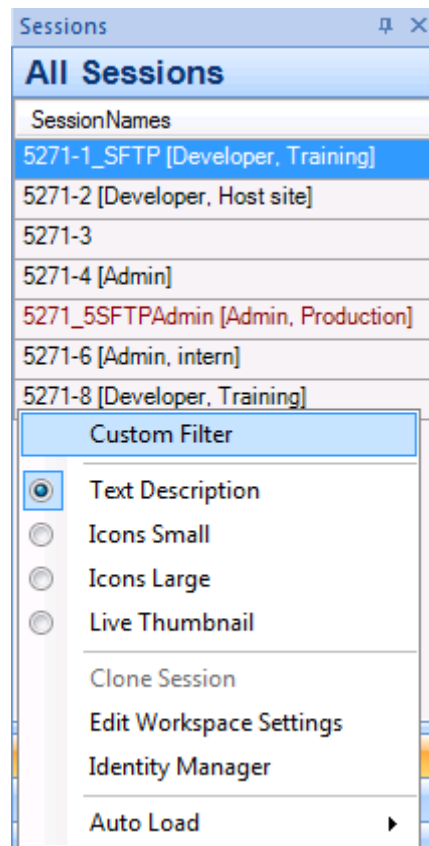
Sessions	
<b>List Locked</b>	
4 Windows are Hidden	
<b>Developer</b>	
SessionNames	
5271-1_SFTP [Developer, Training]	
5271-2 [Developer, Host site]	
5271-8 [Developer, Training]	
-----	
<b>All Sessions</b>	
Admin	
<b>Developer</b>	
FileTransfer	
Host site	
No Login Id	
Production	
Terminal	
Training	
intern	
	»
	▼
Auto login failed, timeout error!!!	

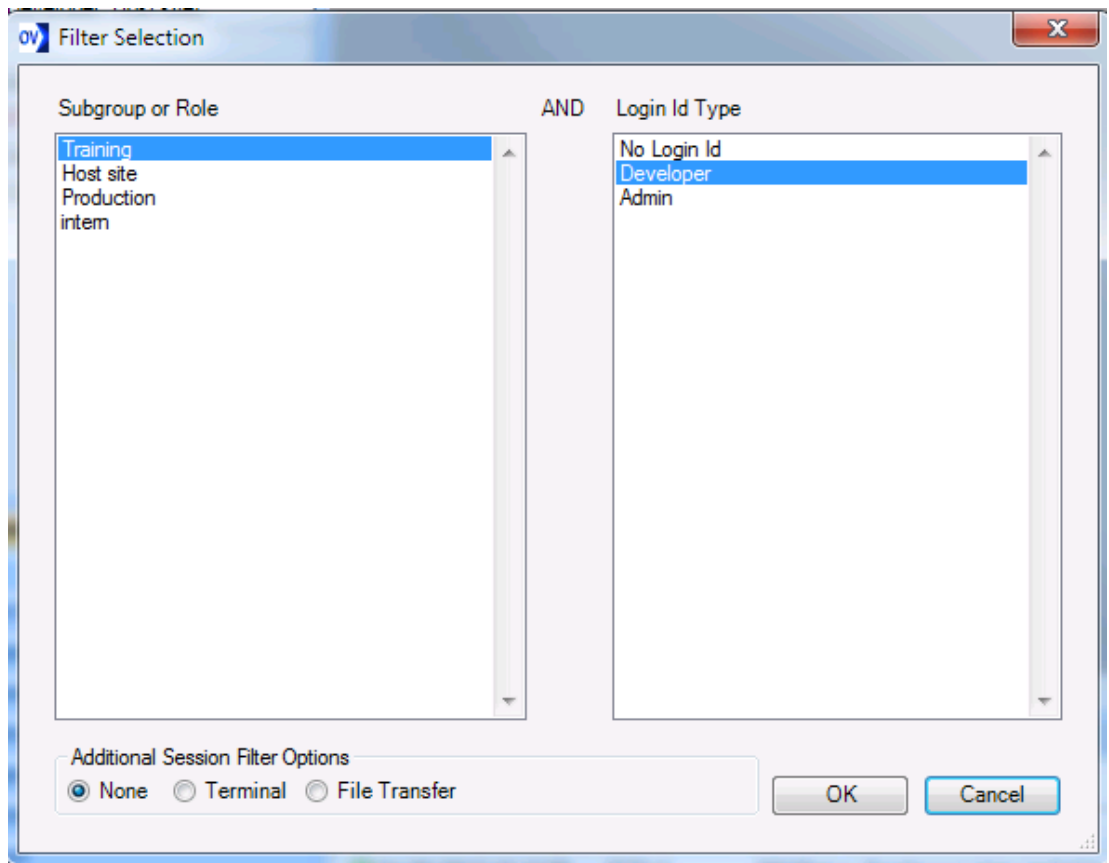


In order to filter by ID Type, Subgroup or both, you will need to specify these settings when creating a new session or modify existing session in the Session Settings dialog box's Role Management section:

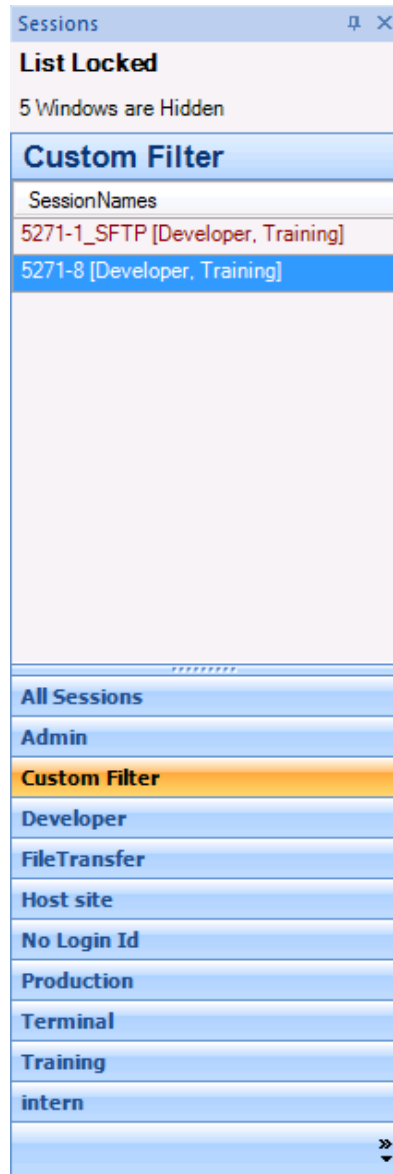


You can also configure a custom filter in which you can specify both ID Type and Subgroup:





The Additional Session Filter Options allow you to specify how the custom filter is applied Terminal sessions only or File Transfer Sessions only.



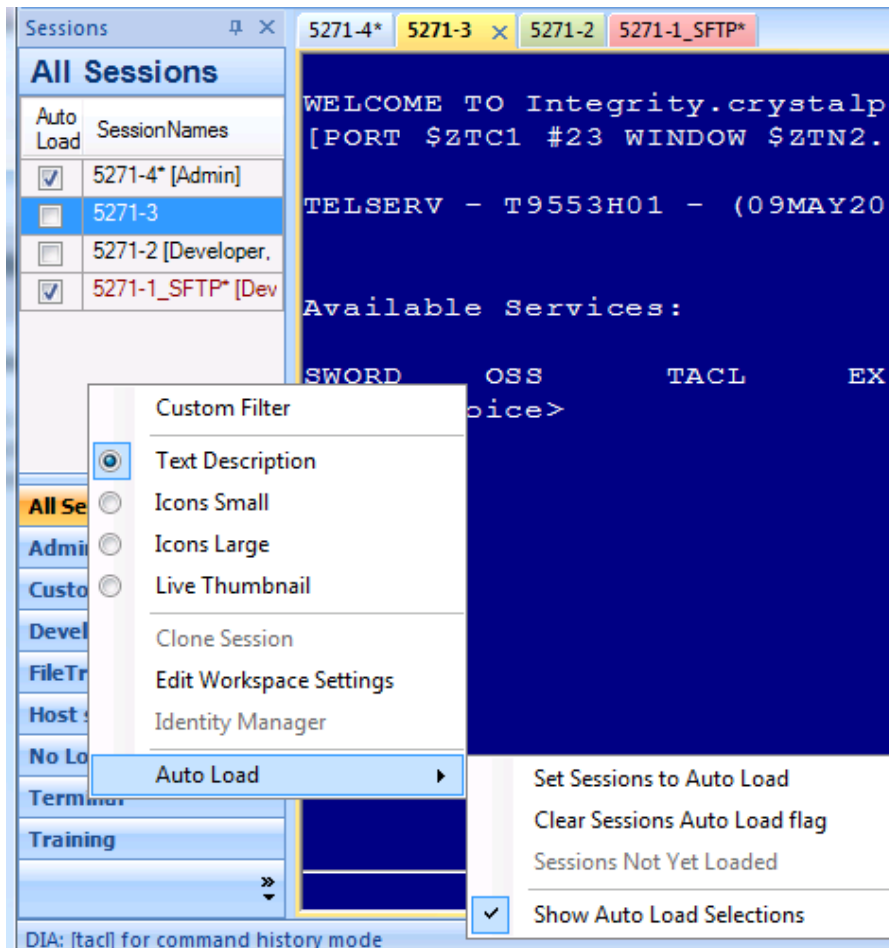
## 6.17 Session Activation Control

### Session Activation Control

Users can now choose, within a workspace, which sessions load and start automatically and which sessions are listed but not active until selected. This gives users the flexibility to focus on their primary sessions while having other sessions listed for immediate access, but held in reserve until needed.

To use session activation control you will need to right click mouse button when cursor is hovering over the Session Bar to bring up the pop up menu for Autoload:





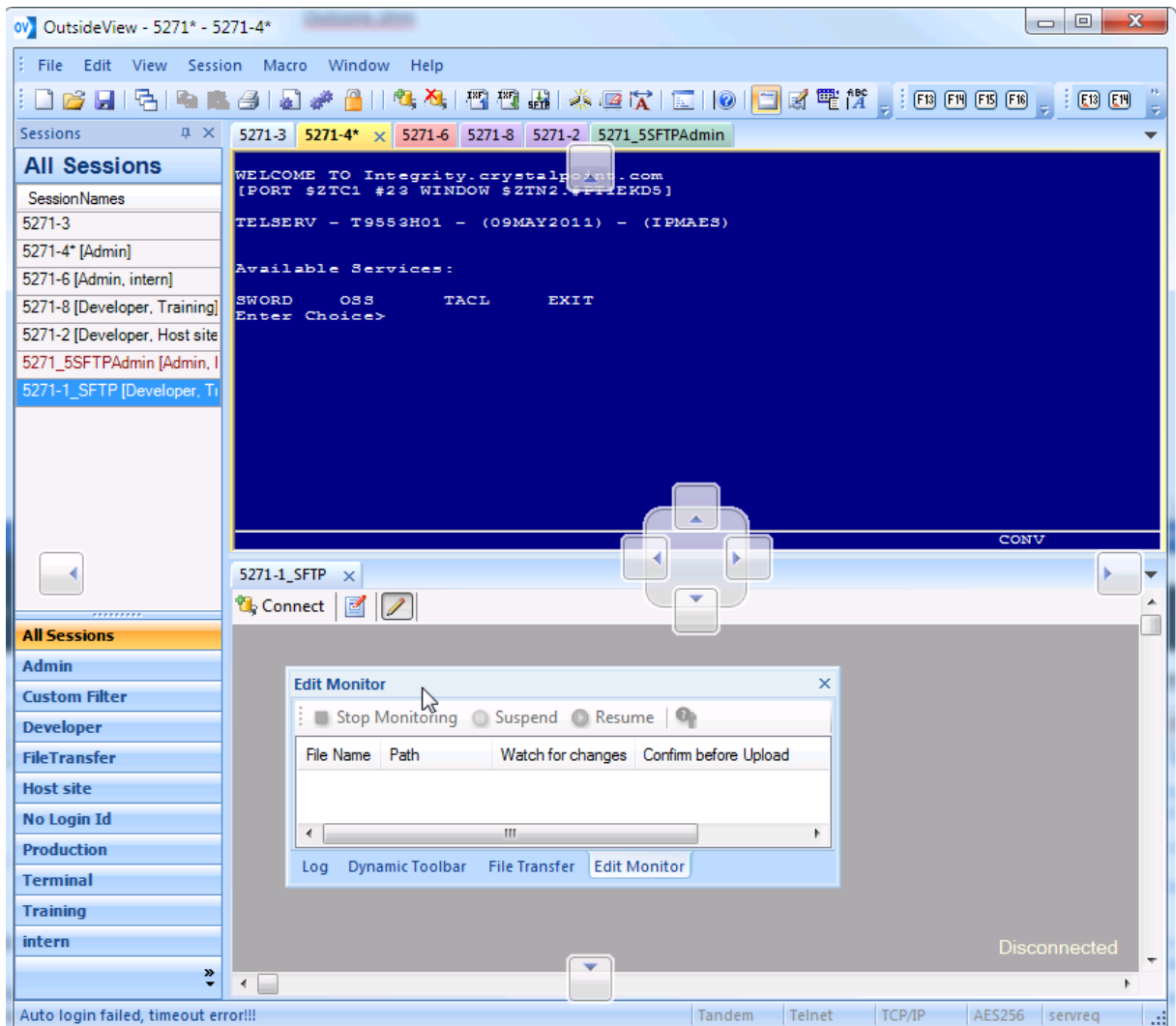
The Auto Load menu has 4 sub options that you can select:

1. Set Session to Auto Load - this menu option provides a quick select all option to make all sessions in the session bar to auto load when the Workspace is launched.
2. Clear Session Auto Load flag - this menu option provides a quick clear all sessions from loading when Workspace is launched.
3. Session Not yet Loaded
4. Show Auto Load Selections - This menu option if enabled displays a Auto Load check box next to the session depicting if the session is set to Auto Load or Not.

## 6.18 Smart Docking

### Smart Docking

OutsideView 9.0 introduced new visual indicators for tool bars and panels in the OutsideView application. To use smart docking, user will need to select the toolbar or panel they want to move and drag it. The user should see the visual indicators letting them know where they can place the panel/toolbar:



## 6.19 File Transfer

### 6.19.1 SFTP (& FTP) file transfer

#### 6.19.1.1 Guardian Operating System Notes

##### Guardian Operating System Notes

Modern NonStop systems are generally configured with two personalities: Guardian, which is the fault-tolerant operating system, and OSS, which is a derivative of Berkeley UNIX.

Given the fault-tolerant nature of the Guardian environment, it has several file types with a large number of parameters that can be used to create a data file. Some developers create template files with the parameters they desire, and then when they need to create a new file, they use a create-like option to reduce the operational overhead.

Only a subset of these file creation parameters is available when using FTP or SFTP file transfer methods to upload files to the host.

Some data files on the host have alternate key files that must be matched with the main data file. These file types require a large amount of manual effort to make usable after transferring them via FTP or SFTP.

Common file types under the Guardian operating system:

1. Text files
2. Binary files
3. Entry Sequenced files
4. Key Sequenced files
5. Entry Sequenced files with alternate key files
6. Key Sequenced files with alternate key files
7. Alternate key files
8. Relative Sequence files with or without alternate key files
9. SQL data base files

Only the first four types of files can be easily transferred via either FTP or SFTP.

Given this and it is highly recommended that the PAK/UNPAK utilities be used to move the other types of files between systems, and especially with Relative Sequence and SQL files.

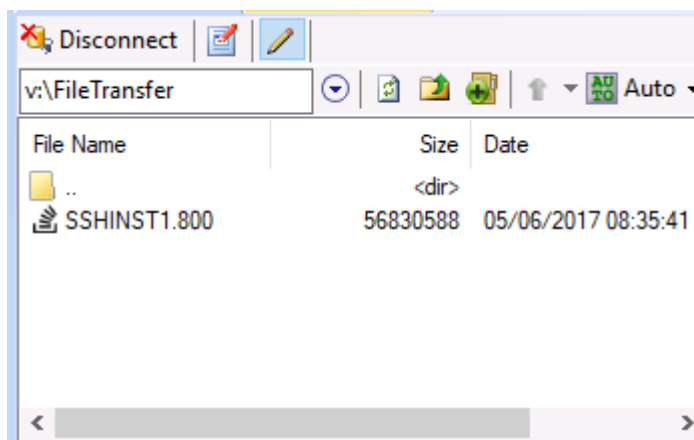
The host utilities PAK/UNPAK which frontends the official backup and restore utilities under the Guardian operating system PAK creates an archive that is similar in function to the popular ZIP file archive format. Hence you can use PAK to create a single binary file that contains all the host files that you desire.

### Default Guardian maximum file sizes for SFTP and FTP

Each transfer method (FTP or SFTP) has default parameters that are used when creating files before storing the uploaded data. The controlling parameters are primary allocation extents, secondary allocation extents and the maximum number of extents allocated that can be created as the file is uploaded. If these values are not large enough an upload operation will return an error 45 which indicates the destination file is full after the file transfer has completed (Many minutes or more later).

For FTP the default maximum file size is about 53 megabytes and for SFTP it is about 175 megabytes.

**Note:** These values can be configured differently on your host system by the system administrator.



For the NonStop Guardian operating system, any file that is displaying the overflow symbol should be uploaded with attributes, which presents the following dialog to assist in the process when you select it via right clicking on the file item and selecting “Upload with attributes”:

Upload with Attributes

Host FileName: SSHINST1 Size: 52.5Mb, Extents: 26887

Host File Allocation Values

Host File Size for current upload attributes 26.7Mb Unused Space: None

Guardian Attributes

File Attributes

File Code: 800

Primary Extents: 14

Secondary Extents: 14

Maximum Extents: 977

Adjust for File Size

Upload as

ASCII

Binary

Entry Sequenced file (Type E)

Key Sequenced file (Type K)

Reset to starting defaults OK Cancel

Clicking on the “Adjust for File Size” button calculates the extents needed for the file to successfully upload.

Upload with Attributes

Host FileName: SSHINST1 Size: 52.5Mb, Extents: 26887

Host File Allocation Values

Host File Size for current upload attributes 52.6Mb Unused Space: 43.7Kb

Guardian Attributes

File Attributes

File Code: 800

Primary Extents: 28 Adjust for File Size

Secondary Extents: 28

Maximum Extents: 961

Upload as

ASCII

Binary

Entry Sequenced file (Type E)

Key Sequenced file (Type K)

Reset to starting defaults OK Cancel

The above example assumes that the file will not grow once it is uploaded to the host; if you are uploading a text file that then will be expanded once it is on the host you would then adjust the Secondary Extents and Maximum Extent values to permit this expansion.

### Text File Notes

Text files are stored on the host as an unstructured file that contains internal pointers and have a maximum line length of 239 columns. From a file size standpoint expect uploaded text files to grow and downloaded text files to shrink when transferred.

In other environments text files are generally free format as to line length; with each line terminated by a new line indicator. In the PC environment, this new line indicator is generally a two-character pair of the carriage return and linefeed characters. In the UNIX environment, it is a single linefeed character.

OV attempts to estimate how large a text file will be once it is uploaded to the host to display an overflow symbol in the local directory to indicate files that more and likely error out on upload because they exceed the default file allocation size by the SFTP or FTP server on the host.

In SFTP if configuration override parameters have not been defined; there is limit to the number of lines of text that can be contained in a file. This is due to Guardian text files maintaining a line number id for each line of text that maxes out at 99,999 lines.

However, this internal line counter permits decimal notation that allows up to one thousand increments between the value one to another.

By default, the host SFTP server uses a line increment value of one which limits a text file upload to 99,999 lines unless it has been configured to permit decimal line increments.

The parameters that the host administrator would apply to ease this limitation are:

PARAM SFTPEditLineNumberDecimalIncr 4000000

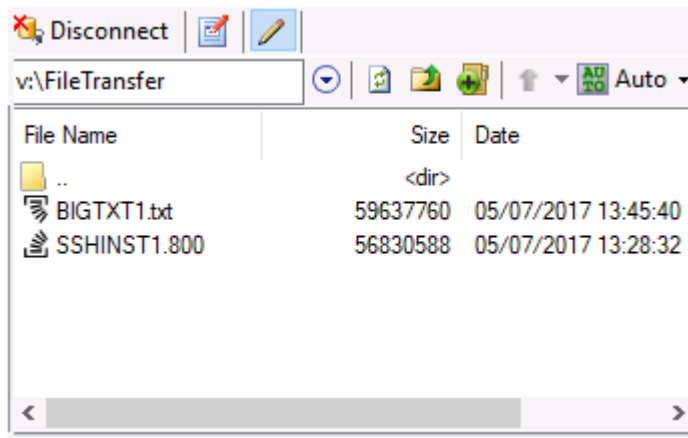
PARAM SFTPEditLineNumberDecimalIncr 3

For local text files that end in the file type of “.txt” or “.101” it will scan the file on dialog initialization to determine the approximate host file size from an extent allocation standpoint and the number of lines for SFTP upload limit checking. There is an application setting on the file transfer tab that turns off the 99,999 line monitoring.

Guardian Defaults for Overflow Warning Calculations			
Protocol	Primary	Secondary	Maximum
TCP/IP FTP	14	28	978
SSH SFTP	14	112	804

Check text files for SFTP upload default limit of 99,999 lines

If it is not turned off; it displays the overflow symbol upside down to indicate that the SFTP line limit has been exceeded.



#### Intermixing use of SFTP and FTP

As an operational note: You cannot download a structured file via FTP and then upload with SFTP as SFTP uses a record length size in front of each entry verses FTP's use of a CR/LF which indicate the end of a line or record.

Text and Binary files are the exception to this rule; however, you should only expect that the reported file sizes will match when you do binary file transfers, as the text file format for the NonStop Guardian personality has additional bookkeeping overhead for each line of text in the file.

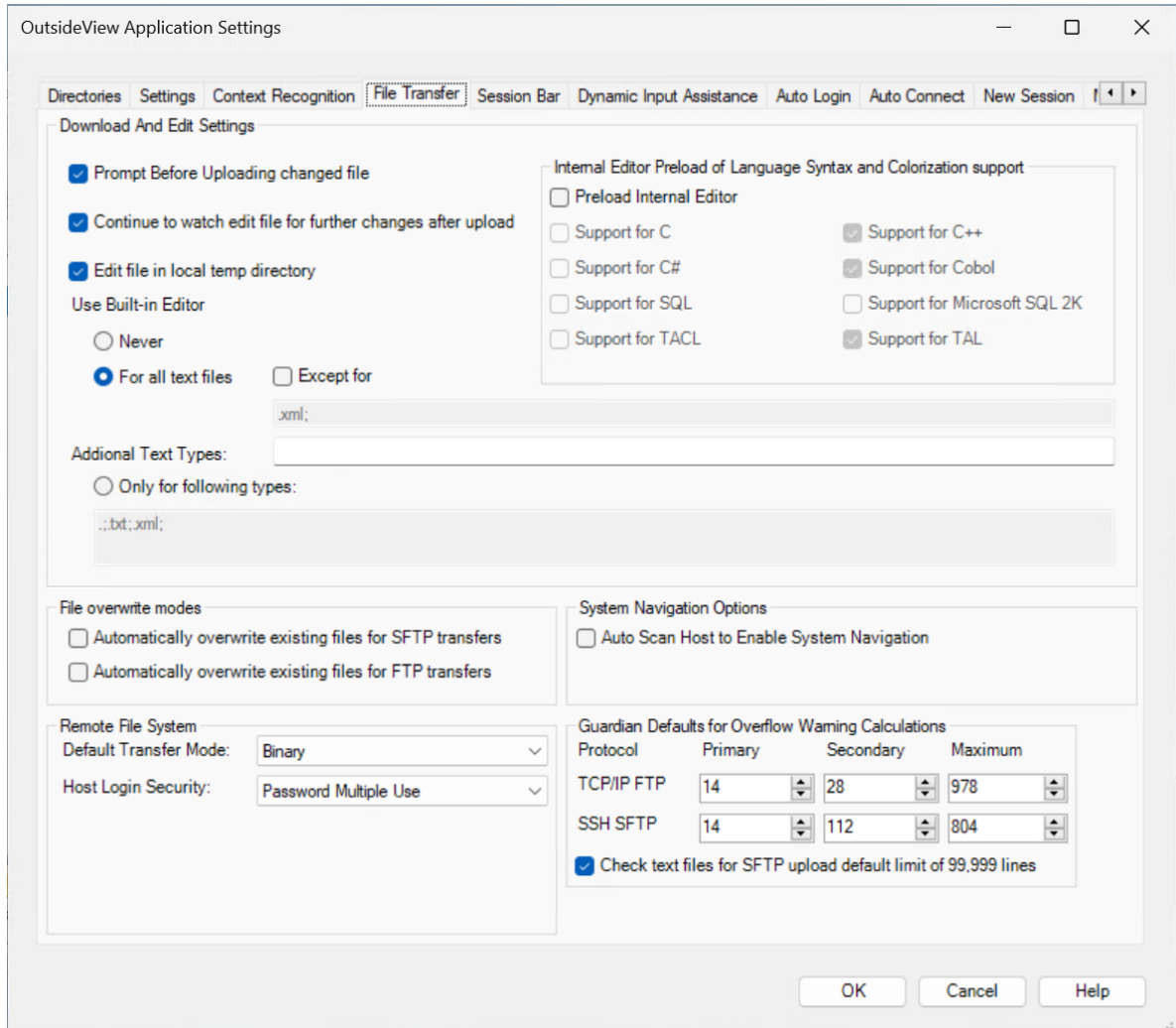
#### 6.19.1.2 Configuring File Transfer Defaults

The **File Transfer** tab lets you fine tune the behavior when editing files you have transferred.


The Code Editor built into OutsideView consumes approximately 15 MB memory. The various code language syntaxes each require additional memory. SQL syntax requires the largest single amount, at about 40 MB. If the Code Editor and all syntaxes are loaded, the memory usage is 100+ MB.

- Internal Editor Preload of Language Syntax -- by default, the Code Editor is pre-loaded into memory, along with selected syntaxes. If you are a developer, and use the builtin editor frequently, you may use this screen to have the editor pre-load only your preferred syntaxes/languages.
- System Navigations -- by default, OutsideView will scan your host file tree to enable host file navigation. If desired, you may disable this Auto-scan option.
- Guardian Systems Defaults for File Allocation Extents -- by default the FTP and SSH\SFTP protocols have a default allocation file size to prevent small files from consuming large amounts of disk space under the Guardian file system. Most companies simply go with the defaults; however, if the system administrator for your company has changed the defaults you would enter the new defaults in this dialog. These values are used when testing local file size to give you a visual indicator when files are too large to upload without changing the allocation extents when the file is created. It is also used by the right mouse click option in the local directory window to upload with attributes. This dialog give a graphic representation of the file allocation by the host, red indicating that it will error out during transfer. Note: To conserve space on the host, first adjust the secondary extent allocation value. If the file is expected to grow after uploading; adjust other extent values to

enable the growth as needed. Check with your system administrator to see if these values have been adjusted for your site. Generally, these values are adjusted upwards to make it simpler for the users if lots of large file uploads are envisioned.



### 6.19.1.3 Creating an SFTP file transfer session

Access the file transfer definition dialog by selecting File, New File Transfer or by clicking on the SFTP icon 

**For SFTP encrypted sessions, leave the mode radio button set to SFTP**

There are many variables for how this capability can be configured on your host systems. **Please contact your organization's NonStop systems personnel for guidance when defining SFTP sessions.** They can give you location-specific advice for connecting to hosts in your environment.



The screenshot shows the 'Connection Properties' dialog box with the following sections and controls:

- Protocol Selection:** Radio buttons for **SFTP** (selected) and **FTP**. A **File Transfer Settings** button is located to the right.
- Host Address:** A text field containing 'integ' and a **Port** field containing '22'. Below these is a checkbox for **Use Tunneling to connect to the Host** and a **Configure** button.
- Role Management:** Two dropdown menus for **ID Type** and **SubGroup**, both currently showing '<undefined>'. A horizontal separator line is below this section.
- Logon Credentials:** A dropdown menu for **Host Account** and an **Advanced** button. Below are radio buttons for **Password** (selected), **Public Key**, **Kerberos/GSS-API**, and **Keyboard Interactive**. A **Password** text field and an **SSH Keyboard Interactive Response Caching** button are also present.
- Session Options:** A checkbox for **Retain Login info on session save**.
- FTP/SFTP Default Directories:** Three text fields for **Local PC**, **OSS/UNIX**, and **Guardian**. The **Local PC** field has a browse button (...).
- File System Selection:** Radio buttons for **User Login default** (selected), **Guardian File System**, and **OSS/UNIX File System**.
- Advanced Options:** A checkbox for **Capture Extended Diagnostic Trace Information**.
- Buttons:** **OK** and **Cancel** buttons at the bottom right.

For additional information on creating SFTP sessions, including creating public key certificates, see the topic [SSH Security](#)

Set the **Protocol Type** as **SFTP** for encrypted connections, set the protocol type as **FTP** if your host system does not support SSH encryption.

**File Transfer Settings Options** - Allows users to modify the File transfer Settings on a per session basis:

OutsideView Application Settings

**File Transfer**

Download And Edit Settings

- Prompt Before Uploading changed file
- Continue to watch edit file for further changes after upload
- Edit file in local temp directory

Use Built-in Editor

Never

For all text files  Except for

.xml;

Additional Text Types:

Only for following types:

.;.txt;.xml;

File overwrite modes

- Automatically overwrite existing files for SFTP transfers
- Automatically overwrite existing files for FTP transfers

System Navigation Options

- Auto Scan Host to Enable System Navigation

Remote File System

Default Transfer Mode: Binary

Host Login Security: Password Multiple Use

Guardian Defaults for Overflow Warning Calculations

Protocol	Primary	Secondary	Maximum
TCP/IP FTP	14	28	978
SSH SFTP	14	112	804

Check text files for SFTP upload default limit of 99,999 lines

OK Cancel Help

When you initiate an FTP or SFTP session, OutsideView creates several user sessions behind the scenes. This is what enables it to perform several advanced functions, such as multiple simultaneous transfer threads and the ability to display file names in FUP INFO format. If the NonStop host system has been configured to use multifactor authentication, it may interfere with this feature.

Some forms of multifactor authentication allow a password to be used only one single time. This causes the subsequent helper threads to fail. If your host is configured this way, set the Host Login Security to be **Single Use Password or Token**. This disables the creation of the helper threads. To set it as the default for all future transfers, set this option in the File Transfer section of the **Default Application Settings** menu.

### Host Address

**Address** is the host IP address or domain name (Or the address of the SSH tunneling service)

**Port** defaults to 22, but may be modified

### SSH Tunneling

Use Tunneling to connect to the Host

Define (add) intermediate SSH hosts, maximum of 5;

Configure Multiple Nodes for SSH

Define Intermediate Hosts

Configure intermediate hops in order (maximum of 5).

Nodes

Node Connection Properties

Host Address

Address:  Port:

Logon Credentials

Host Account:

Password  Public Key

Public Key:

Password:

Retain Login info on session save

Edit Add Delete OK Cancel

### Role Management

Select your desired ID Type and/or Subgroup. For more information see the topic [Identity Caching](#)

Role Management

ID Type:

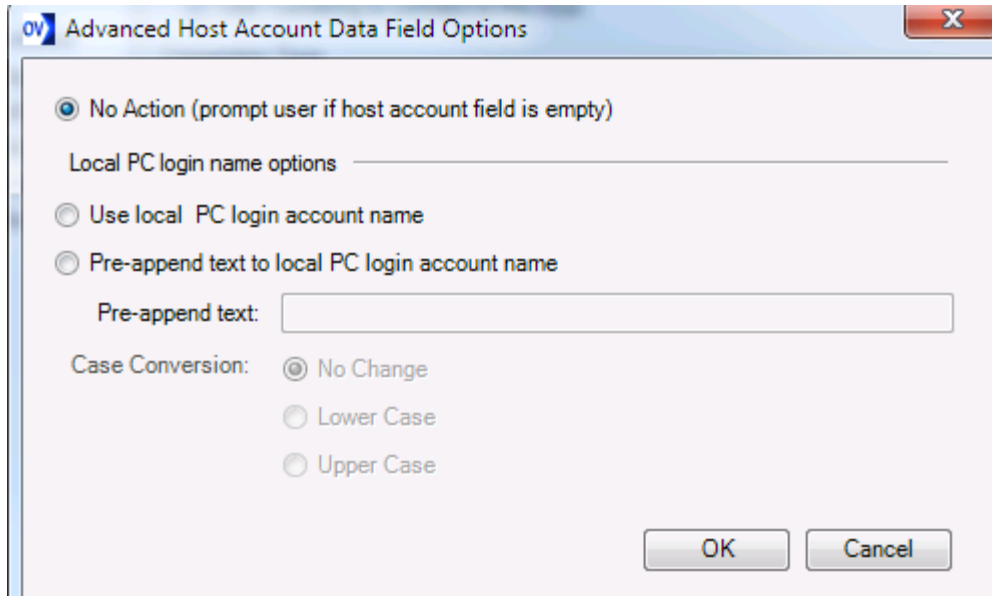
SubGroup:

### Logon Credentials

If Users do not take advantage of Identity Caching, they can authenticate their SSH pseudo-terminal session using a host account and host password (if the SSH configuration on the host permits), by using a passphrase to access and send a key file to the host, by keying in required information interactively, or by Kerberos/GSS-API authentication. This area is also used to pass credentials to the SSH tunneling server.

**Host Account** is the user's host account. (This field will be display-only if Use Managed Id for Data Link Credentials is unchecked.)

Advanced Host Account options are:



Advanced options can automatically derive/supply a user id. For instance, if your host account user name were identical with your PC login account user name, you could select

Use local PC login account name

If all host account user names are of the form cust.user, where 'cust' is fixed and 'user' matches your PC login user name, then you could select

Pre-append text to local PC login account name

Pre-append text:

For example, assume your PC login name is Bob, and your host account login is US.Bob. Enter the Pre-append text as US. Thereafter if Bob is logged in to the PC, the SSH session would attempt to login as US.Bob. If Sue logs in to the PC, the session would attempt to login as US.Sue.

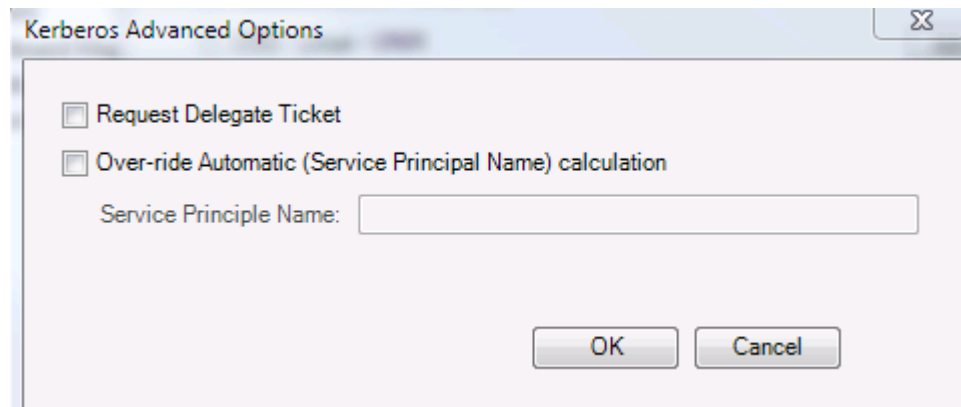
**Case conversion is a convenience to allow login names to stay case-compliant with host account names.**

**Password** - This field will be display only if ID Management is NOT active

**Public Key** - This option requires entry of a passphrase and selection of a public key file (see topic [SSH Certificates](#))

**Kerberos/GSS-API** - This option works in conjunction with the NonStop Secure Single Sign-on product to enable single sign-on wherein the active directory security token obtained at PC login is presented to the Single Sign-on component on the NonStop to authenticate the host session. See the NonStop Secure Single Sign-on documentation for information on configuring these options.

[Configure Advanced Kerberos Options](#)



**Keyboard Interactive** - Requires manual entry of user credentials to authenticate session.

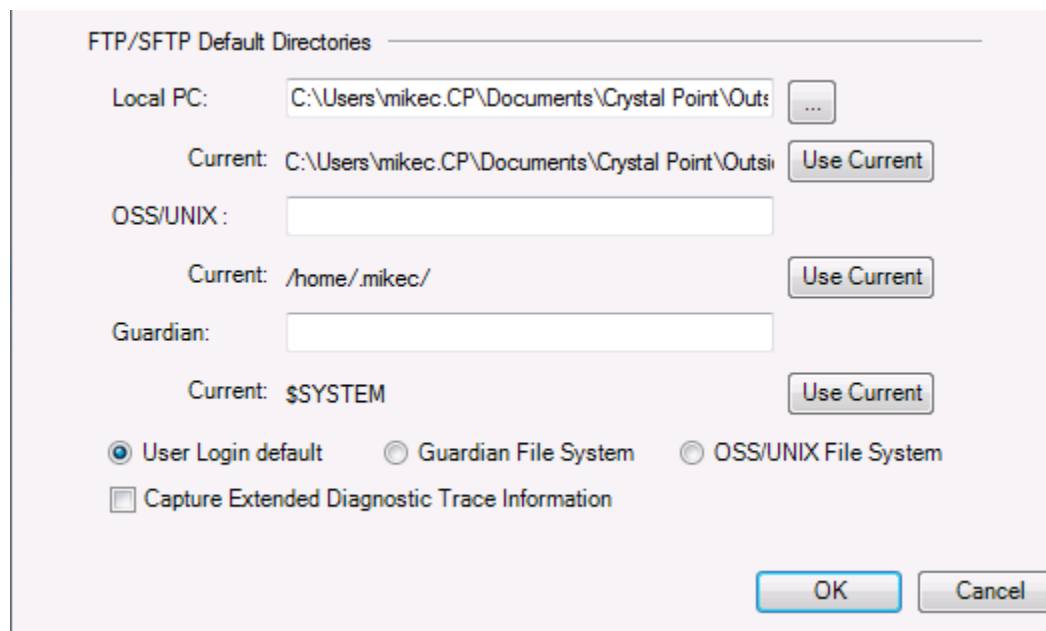
**Use Managed Id for Data Link Credentials** - this option is default enabled when using Managed Id (ID Type). The credentials provided in the ID Type is used to connect to the host (Data Link).

**Retain Login info on session save**

if activated, will store your login credentials for automatic reuse. Note this is only Visible when Use Managed Id for Data Link Credentials is **Unchecked** or ID Type is set to <undefined>!

**When a file transfer session is active (connected)**, the area below can be used to save/retain your local or remote default directories

If specific default locations are not specified, you can select whether to start in OSS or Guardian or login default modes.



#### 6.19.1.4 Creating an SSL-secured file transfer session

There are many variables for how this capability can be configured on your host systems. **Please contact your organization's NonStop systems personnel for guidance when connecting file transfer sessions.** They can give you location-specific advice for connecting to hosts in your environment.

Access the file transfer definition dialog by selecting File, New File Transfer or by clicking on the SFTP icon

For FTP file transfers (encrypted or not) set the radio button for transfer mode to be **FTP**

The screenshot shows the 'Connection Properties' dialog box with the 'File Transfer Settings' tab selected. The 'FTP' radio button is chosen. The 'Host Address' field is empty, and the 'Port' is set to 21. Under 'Role Management', 'ID Type' and 'SubGroup' are set to '<undefined>', and 'Host Account' is empty. The 'Advanced' button is visible. 'Passive Mode Ftp' is checked, and 'Use Anonymous Logon' is unchecked. The 'Password' field is empty. 'SSL Start Mode' is set to 'None'. The 'Advanced SSL Security Options' button is present. 'Retain Login info on session save' is unchecked. Under 'FTP/SFTP Default Directories', 'Local PC', 'OSS/UNIX', and 'Guardian' fields are empty. 'User Login default' is selected, and 'Guardian File System' and 'OSS/UNIX File System' are unselected. 'Capture Extended Diagnostic Trace Information' is unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

### Passive Mode FTP

By default, FTP will use passive mode, but you may uncheck this option to operate in non-passive, or Active mode.

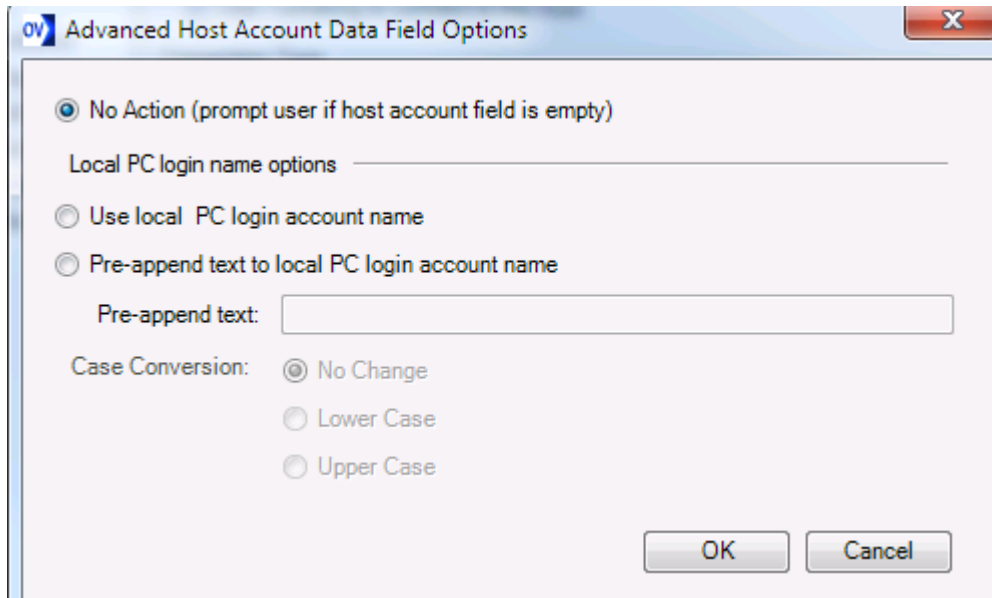
### Host Address

**Address** is the host IP address or domain name (Or the address of the SSH tunneling service)

**Port** defaults to 21, but may be modified

### Advanced Host Account Data Field Options

The Host Account and Advanced button are enabled when the Role Management for IDType is set to <undefined>.



Advanced options can automatically derive/supply a user id. For instance, if your host account user name were identical with your PC login account user name, you could select

Use local PC login account name

If all host account user names are of the form cust.user, where 'cust' is fixed and 'user' matches your PC login user name, then you could select

Pre-append text to local PC login account name

Pre-append text:

For example, assume your PC login name is Bob, and your host account login is US.Bob. Enter the Pre-append text as US. Thereafter if Bob is logged in to the PC, the SSH session would attempt to login as US.Bob. If Sue logs in to the PC, the session would attempt to login as US.Sue.

**Case conversion** is a convenience to allow login names to stay case-compliant with host account names.

### Role Management

Role management is optional, but can be very helpful here. If you specify an ID Type, then the Host Account credential fields become disabled, as this information will be controlled by the Identity Manager.

### Host Account

FTP sessions support only Host account and password credentials.



### Retain Login Info on Session Save

If activated, will store your login credentials for automatic reuse. Note this is only Visible when ID Type is set to <undefined>.

### Use Managed Id for Data Link Credentials

This option is default enabled when using Managed Id (ID Type). The credentials provided in the ID Type is used to connect to the host.

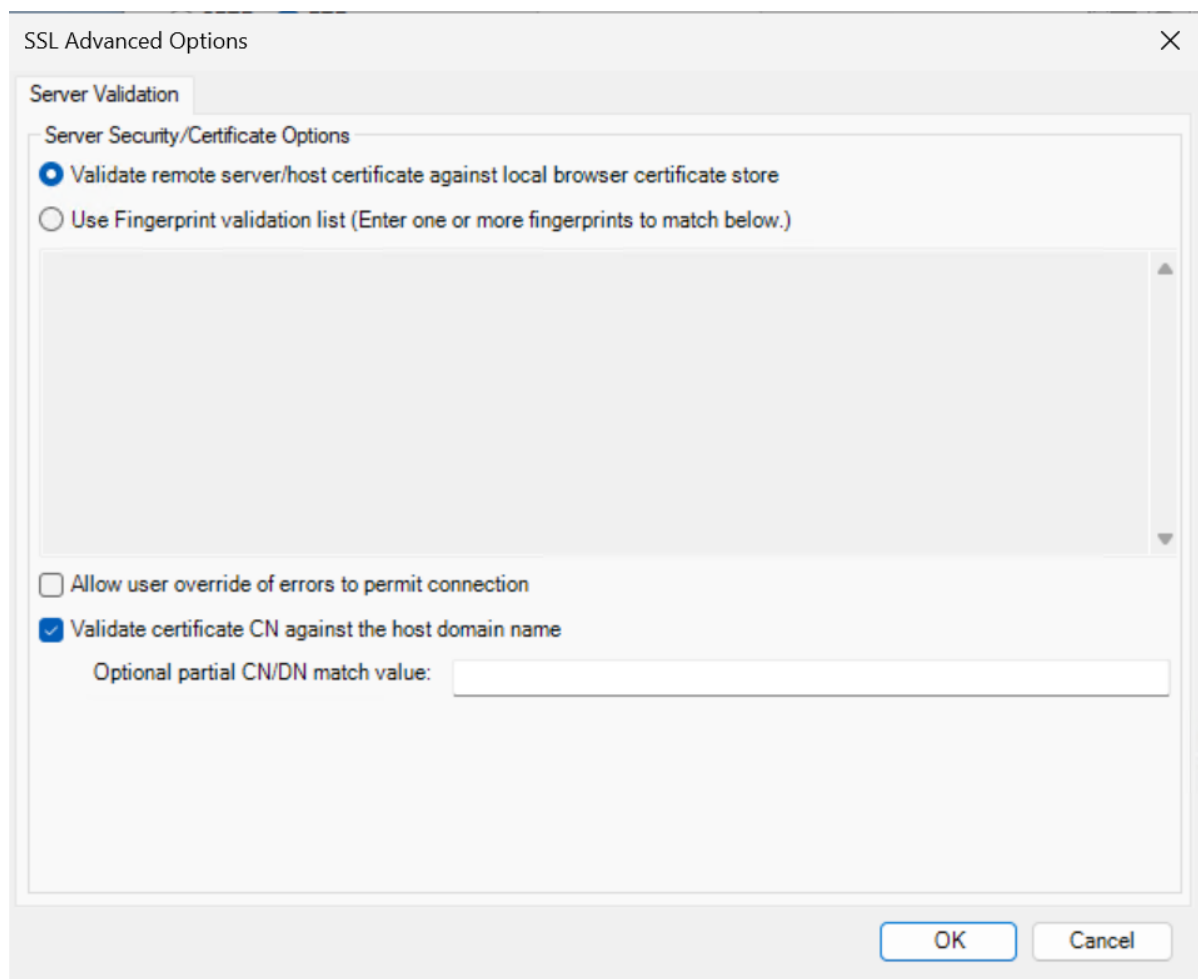
### SSL Start Mode

If you wish to have the file transfer session encrypted via Secure Socket Layer, you would select the method here. **AUTH TLS is the most common setting.** Some FTP servers require "implicit." Consult your systems administration personnel for additional information.

## SSL Advanced Options

### Server Validation

This screen allows definition of a detailed options, including server certificate options or fingerprint validation. For assistance with specific settings, consult your in-house NonStop or Security support group.



The screenshot shows a dialog box titled "SSL Advanced Options" with a close button (X) in the top right corner. The "Server Validation" tab is selected. Under the "Server Security/Certificate Options" section, there are two radio buttons: "Validate remote server/host certificate against local browser certificate store" (which is selected) and "Use Fingerprint validation list (Enter one or more fingerprints to match below.)". Below these is a large, empty text area. Further down, there are two checkboxes: "Allow user override of errors to permit connection" (unchecked) and "Validate certificate CN against the host domain name" (checked). Below the second checkbox is a text input field labeled "Optional partial CN/DN match value:". At the bottom right of the dialog are "OK" and "Cancel" buttons.

#### 6.19.1.5 Creating a new FTP file transfer session

There are many variables for how this capability can be configured on your host systems. **Please contact your organization's NonStop systems personnel for guidance when connecting file transfer sessions.** They can give you location-specific advice for connecting to hosts in your environment.

Access the file transfer definition dialog by selecting File, New File Transfer or by clicking on the SFTP icon

For FTP file transfers (encrypted or not) set the radio button for transfer mode to be **FTP**

The screenshot shows the 'Connection Properties' dialog box with the 'File Transfer Settings' tab selected. The 'SFTP' radio button is unselected, and the 'FTP' radio button is selected. The 'Host Address' field is empty, and the 'Port' is set to '21'. Under 'Role Management', 'ID Type' and 'SubGroup' are both set to '<undefined>'. The 'Host Account' field is empty, and there is an 'Advanced' button next to it. The 'Passive Mode Ftp' checkbox is checked, and the 'Use Anonymous Logon' checkbox is unchecked. The 'Password' field is empty. Under 'SSL Start Mode', the 'None' radio button is selected, and 'AUTH TLS' and 'Implicit' are unselected. There is an 'Advanced SSL Security Options' button. The 'Retain Login info on session save' checkbox is unchecked. Under 'FTP/SFTP Default Directories', 'Local PC', 'OSS/UNIX', and 'Guardian' fields are empty. The 'User Login default' radio button is selected, and 'Guardian File System' and 'OSS/UNIX File System' are unselected. The 'Capture Extended Diagnostic Trace Information' checkbox is unchecked. At the bottom right, there are 'OK' and 'Cancel' buttons.

### Passive Mode FTP

By default, FTP will use passive mode, but you may uncheck this option to operate in non-passive, or Active mode.

### Host Address

**Address** is the host IP address or domain name (Or the address of the SSH tunneling service)

**Port** defaults to 21, but may be modified

### Role Management

Role management is optional, but can be very helpful here. If you specify an ID Type, then the logon credential fields become disabled, as this information will be controlled by the Identity Manager.

### Logon Credentials

FTP sessions support only Host account and password credentials. Public Key and Kerberos options are disabled (grayed-out).


### SSL Start Mode

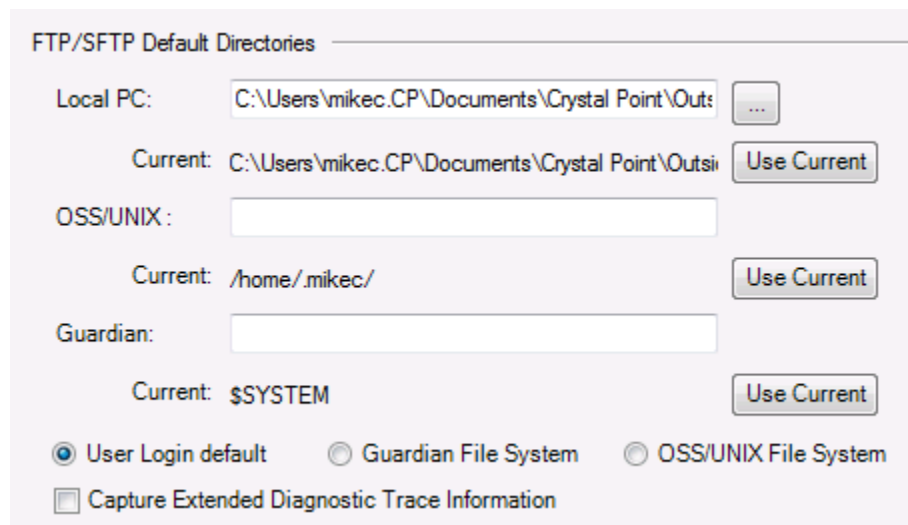
For plain, unencrypted FTP, select "None"

## 6.19.1.6 Saving a File Transfer Connection

### Saving a File Transfer Connection

Once the File Transfer session opens, select **File, Save**, or **File, Save As**, or click on the  icon.

You may also select the Connection Properties icon  to save your host and local directories, as your future starting locations:



FTP/SFTP Default Directories

Local PC:

Current:

OSS/UNIX:

Current:

Guardian:


Current:

User Login default     Guardian File System     OSS/UNIX File System


Capture Extended Diagnostic Trace Information

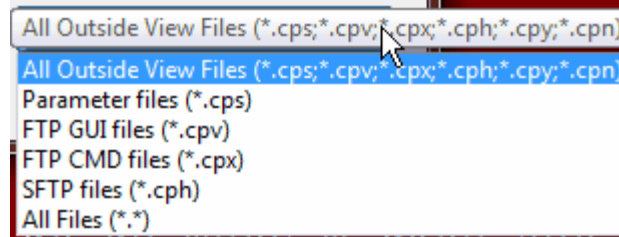
## 6.19.1.7 Opening Previously-defined SFTP connection files

### Opening Previously-defined File Transfer connection files

Select File, Open Session, (or ) and select your preferred file transfer session.

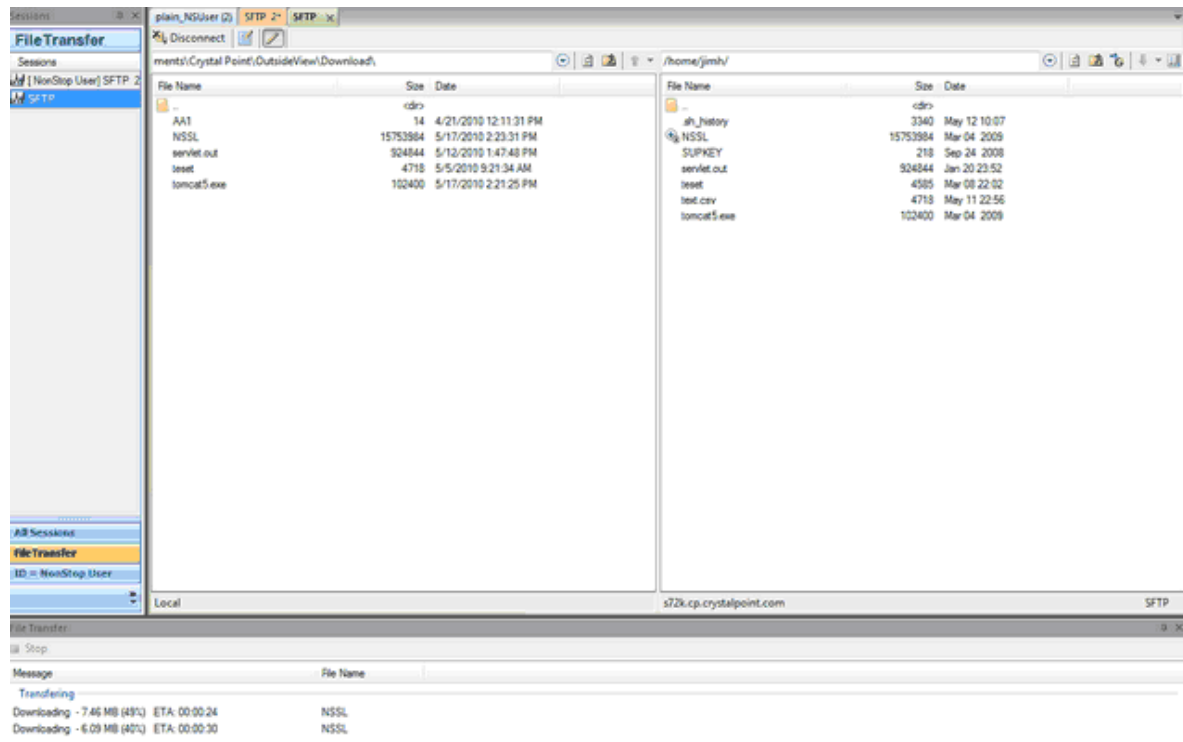
Note 1: OutsideView can display only session files of a specific type:

Note 2: All file transfer session defined via File, New File Transfer, or via the SFTP icon , will be listed as SFTP files and have the .cph suffix, whether using SFTP or FTP internally.



### 6.19.1.8 Using a File Transfer connection


#### Using a File Transfer connection





The left-hand side of the screen is the local PC file system. The right-hand side is the host file system.


A file transfer session will connect in OSS mode, if available – as shown above.


To change to Guardian mode, click on the  icon.



To change to OSS mode, click on the  icon.

To set Overwrite ON, click on the  icon

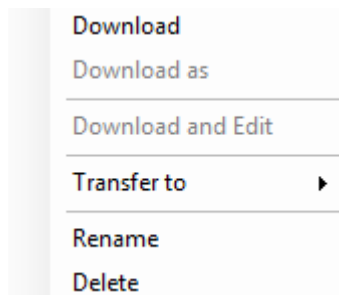
To see files in RAW view, click on  icon

To refresh the screen, click on the  icon

To move up one folder level, click on the  icon

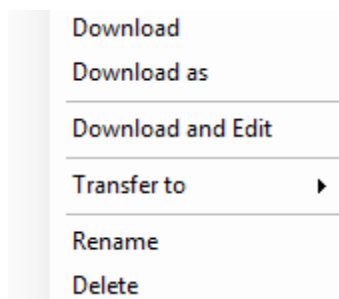
Hold down the mouse button or use Ctrl+click to select one or more files, then either drag the files to the receiving folder's frame. or click on the  icon to upload files to the host or the  icon when downloading.


You may also right-click after highlighting multiple files and have the following options (Download As and Download and Edit disabled for multiple files)

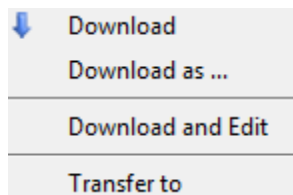


### Download-and-Edit

Whenever you want to quickly download, edit, and upload a **single** file, highlight that file and right-click to see the following options:

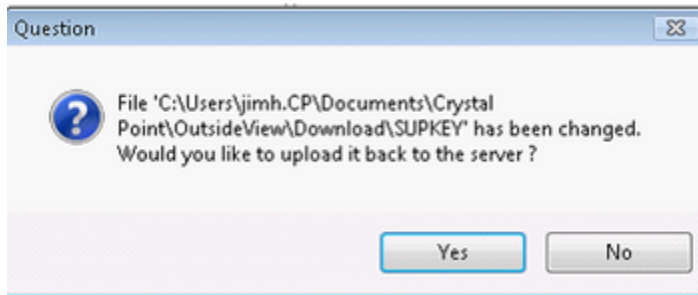


You may also select a single file and click the down mark next to the download icon  to see similar options




If you select **Download and Edit**, the file will be automatically downloaded, and automatically opened - either in a Windows associated application (i.e. Excel for a .xls file) or within OutsideView's new imbedded Code Editor for a text file. For more information concerning the imbedded code editor, see [Imbedded Editor](#).

If you make file changes, you should receive a prompt to automatically upload (overwriting) the file back to the host.



### 6.19.1.9 Uploading Files

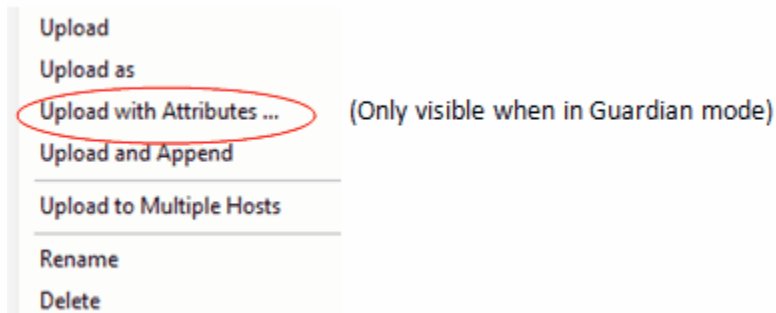
When transferring files from your local PC to a remote host, via SFTP or FTP, you may simply drag and drop a file or files from the left side (local file system) to the right side (host file system)

The Overwrite option is controlled by the  icon.

You may navigate to any local folder, using the controls at the top of the left-hand portion of the File transfer dialog.

You may navigate to any host folder, using the controls at the top of the right-hand portion of the File transfer dialog.

You may highlight a single file and right-click to see the following options



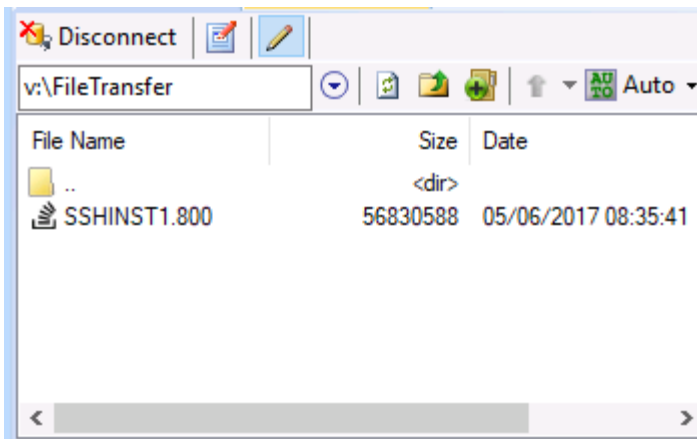
By default, both Upload and Upload As will transfer files to the host as code 0

### Default Guardian maximum file sizes for SFTP and FTP

Each transfer method (FTP or SFTP) has default parameters that are used when creating files before storing the uploaded data. The controlling parameters are primary allocation extents, secondary allocation extents and the maximum number of extents allocated that can be created as the file is uploaded. If these values are not large enough an upload operation will return an error 45 which indicates the destination file is full after the file transfer has completed (Many minutes or more later).

For FTP the default maximum file size is about 53 megabytes and for SFTP it is about 175 megabytes.

**Note:** These values can be configured differently on your host system by the system administrator.



For the NonStop Guardian operating system, any file that is displaying the overflow symbol should be uploaded with attributes, which presents the following dialog to assist in the process when you select it via right clicking on the file item and selecting “**Upload with attributes**”:



Upload with Attributes

Host FileName: SSHINST1 Size: 52.5Mb, Extents: 26887

Host File Allocation Values

Host File Size for current upload attributes 26.7Mb Unused Space: None

Guardian Attributes

File Attributes

File Code: 800

Primary Extents: 14 Adjust for File Size

Secondary Extents: 14

Maximum Extents: 977

Upload as

ASCII

Binary

Entry Sequenced file (Type E)

Key Sequenced file (Type K)

Reset to starting defaults OK Cancel

Clicking on the “Adjust for File Size” button calculates the extents needed for the file to successfully upload.

Upload with Attributes

Host FileName: SSHINST1 Size: 52.5Mb, Extents: 26887

Host File Allocation Values

Host File Size for current upload attributes 52.6Mb Unused Space: 43.7Kb

Guardian Attributes

File Attributes

File Code: 800

Primary Extents: 28 Adjust for File Size

Secondary Extents: 28

Maximum Extents: 961

Upload as

ASCII

Binary

Entry Sequenced file (Type E)

Key Sequenced file (Type K)

Reset to starting defaults OK Cancel

The above example assumes that the file will not grow once it is uploaded to the host; if you are uploading a text file that then will be expanded once it is on the host you would then adjust the Secondary Extents and Maximum Extent values to permit this expansion.

**Upload with Attributes** lets you specify how the file arrives;

Upload with Attributes

Host FileName: CACERT Size: 798B, Extents: 1

Host File Allocation Values

Host File Size for current upload attributes 53.5Mb Unused Space: 53.5Mb

Guardian Attributes

File Attributes

File Code: 101

Primary Extents: 14 Adjust for File Size

Secondary Extents: 28

Maximum Extents: 978

Upload as

ASCII

Binary

Entry Sequenced file (Type E)

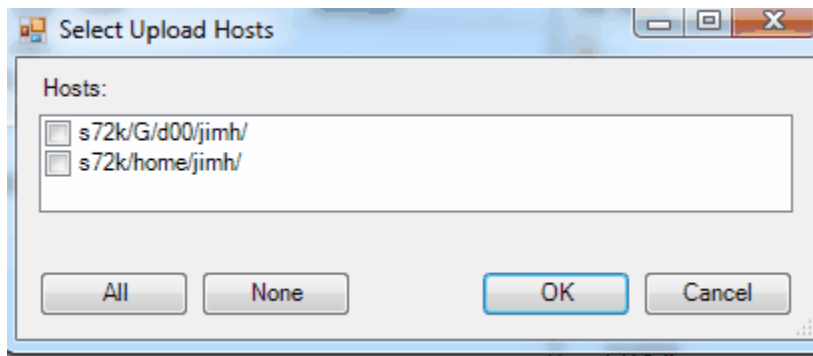
Key Sequenced file (Type K)

Reset to starting defaults OK Cancel

You may highlight multiple files , and right click to have these options active:

- Upload
- Upload as
- Upload with Attributes ...
- Upload and Append
- Upload to Multiple Hosts
- Rename
- Delete

If you select Upload to Multiple Hosts, you will be presented with a dialog showing all active File transfer sessions (and their current location on the host):



**NOTE:** This capability can be further extended if you create various workspaces that automatically open pre-defined sets of file transfer sessions. Each such workspace could act as, effectively, a distribution list....

#### 6.19.1.10 Downloading Files

##### Downloading Files

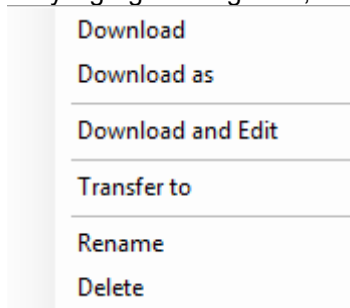
When transferring files from your remote host to your local PC, via SFTP or FTP, you may simply drag and drop a file or files from the right side (host file system) to the left side (Local file system)

The Overwrite option is controlled by the  icon.

You may navigate to any local folder, using the controls at the top of the left-hand portion of the File transfer dialog.

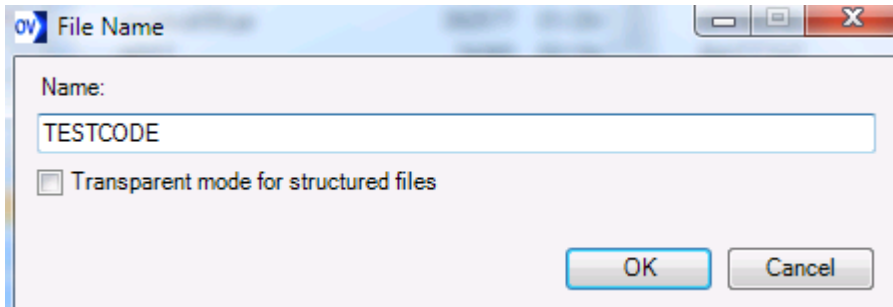
You may navigate to any host folder, using the controls at the top of the right-hand portion of the File transfer dialog.

You may highlight a single file, and right-click to see the following options



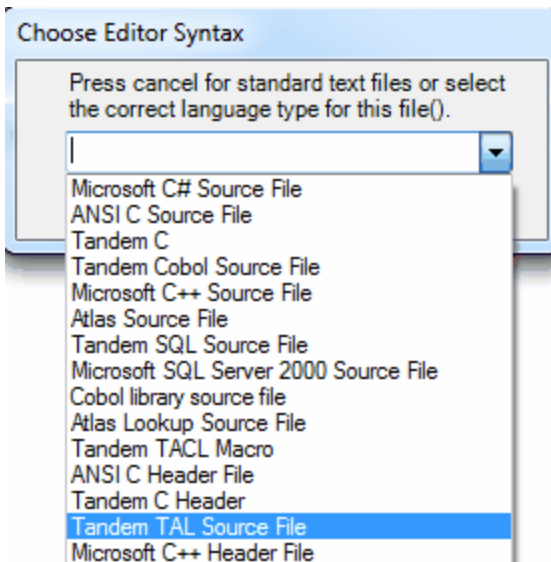
##### Download As

If you do a File, **Download As**, you will see the following dialog:



### Download-and-Edit

If you select **Download-and-Edit**, you *may* be prompted to identify which syntax to use in the Code Editor. To specify plain text, just press Cancel to leave the selection blank. If your PC has a file association mapped for a file with an extension, the mapped program will be used to open the file.



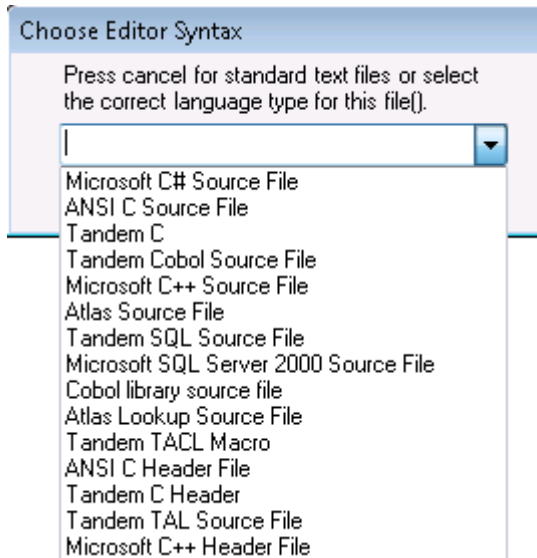
For information on configuring the download-and edit file transfer behavior, see [File Transfer tab](#)

#### 6.19.1.11 File Transfer, Imbedded Editor

##### File Transfer, Imbedded Editor

When selecting files for download, users may right-click and choose Download-and-Edit. OutsideView will download the file and open it with any Windows-associated program (i.e. Word for a .doc file). If the file has no suffix, and contains no binary characters, OutsideView will offer to open the file in the new OutsideView imbedded Editor. The edit window will show in your OutsideView session bar. The editor is syntax-aware and will allow the user to specify the language/syntax for the file. (Press cancel for standard text file).

You may also double-click on any file listed in the local PC side of your file transfer screen to open it in the OutsideView Editor



NOTE: To configure when the imbedded Editor is invoked, go to Edit, Application Settings, [File Transfer](#) tab.

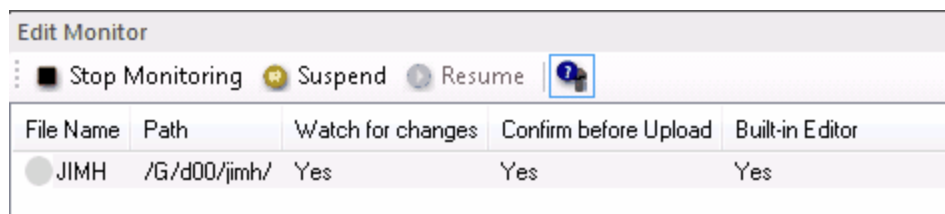
### Windows File Associations

Within a file transfer session, users may browse within their left hand (local PC) pane, and then double-click on any file to open it. The file will be opened in accordance with the file association of your PC.

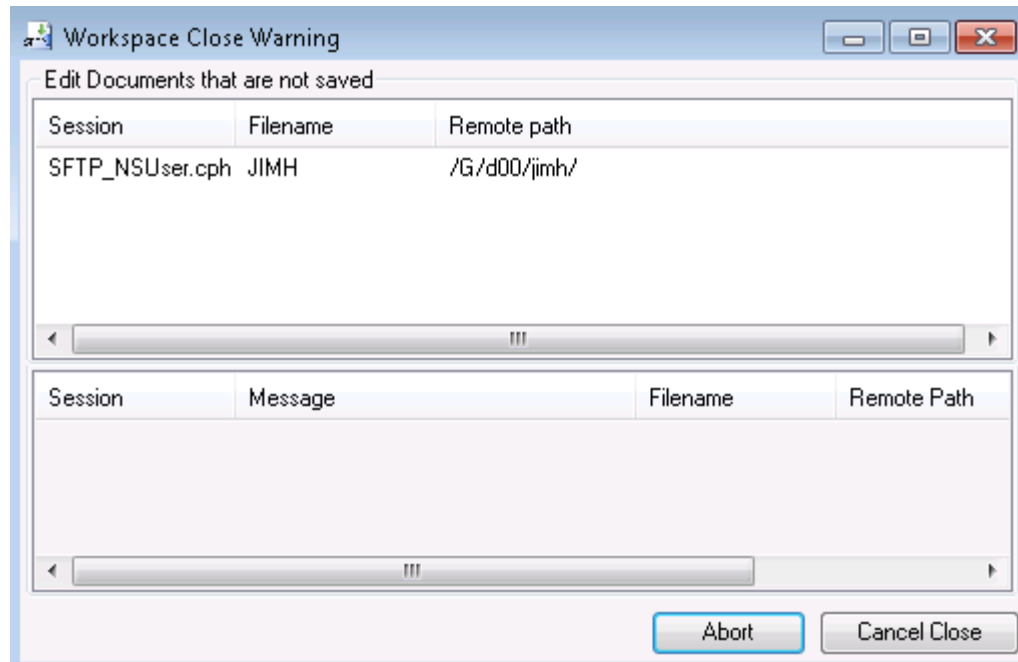
#### 6.19.1.12 Edit Monitor

##### Edit Monitor

Whenever you do a Download and Edit operation, OutsideView will monitor that file. Open the **Edit Monitor** to see the status of monitored files.



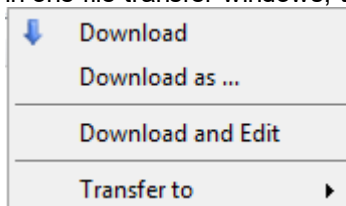
If you do change the local copy of the file, and then attempt to exit OutsideView before uploading the changed file, OutsideView will warn you before exiting.



Note; The lower portion of the screen would identify and warn of any in-progress file transfers.

### 6.19.1.13 Host-to-Host file transfers

When you have multiple File transfer connections active, you may select (highlight) one or more files in one file transfer windows, then click the download icon to get the following options:



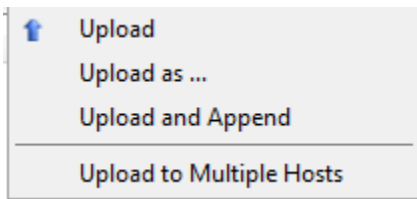
Selecting **Transfer to** will bring up a list of all other active file transfer sessions, showing their current active directory on the host.

You may select one destination to transfer a file laterally.

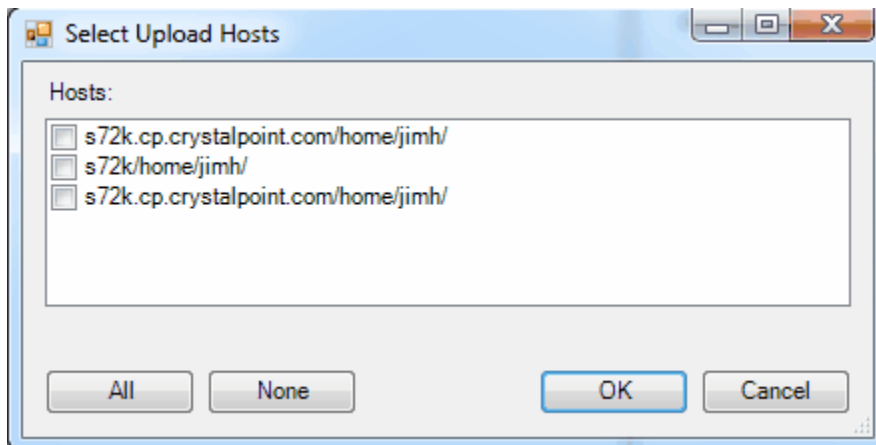
### 6.19.1.14 Multiple Host file transfers

If you have multiple active file transfer connections running within a copy of OutsideView, you may upload local files to multiple hosts.

In the local PC file window (left-half of file transfer dialog), browse to and select one or more files, then right-click or select the upload icon




Select **"Upload to Multiple Hosts"** to see a selection box listing all active file transfer sessions, showing their active host directory. :



Select specific destinations, or **All**, then click OK to send the local file to all selected host destinations.

### 6.19.1.15 Modifying a File Transfer Connection

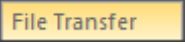
#### Modifying an File Transfer Connection

Click on the  icon to view/modify File Transfer session settings of your current session. You may have to Disconnect before modifying some properties.

Don't forget to SAVE afterwards if you wish the modification to be permanent.

### 6.19.1.16 File Transfer Progress

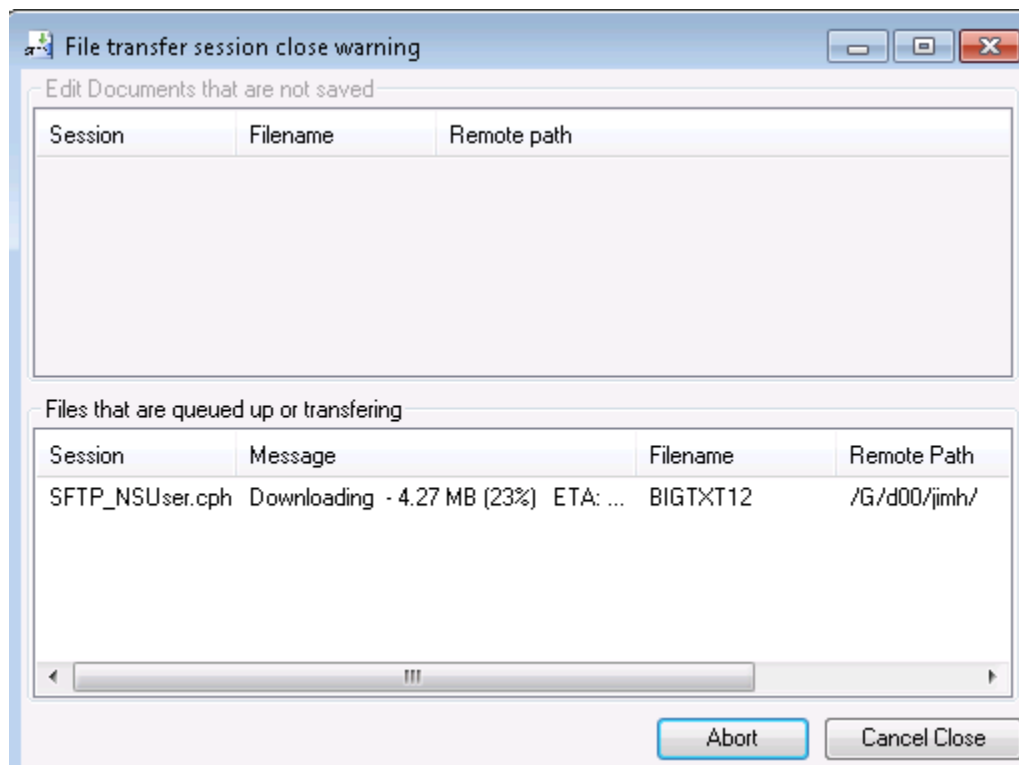
#### File Transfer Progress Monitor

Whether using FTP or SFTP, you may see the progress of your file transfer by selecting View, File Transfer Progress, or by clicking on the  within the dynamic host widow area.



File Transfer	
<input checked="" type="checkbox"/> Stop	
Message	File Name
<b>Transferring</b>	
Downloading - 5.89 MB (39%) ETA: 00:01:11	NSSL
<b>Complete</b>	
Download Completed in 1 second	tomcat5.exe

If you attempt to close OutsideView, or a workspace, or a session in which a file transfer is still in-progress, OutsideView will warn you:

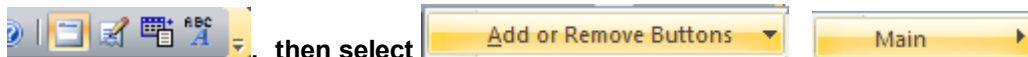


### 6.19.1.17 "Classic" FTP

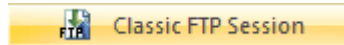
#### 6.19.1.17.1 Invoking "Classic" FTP

**NOTE:** 'Classic' FTP is being retained within OutsideView, in parallel with our new SFTP/FTP module, for a limited period of time. For most file transfer activities, the new SFTP/FTP mode is recommended. One current exception is use within MVS file systems.

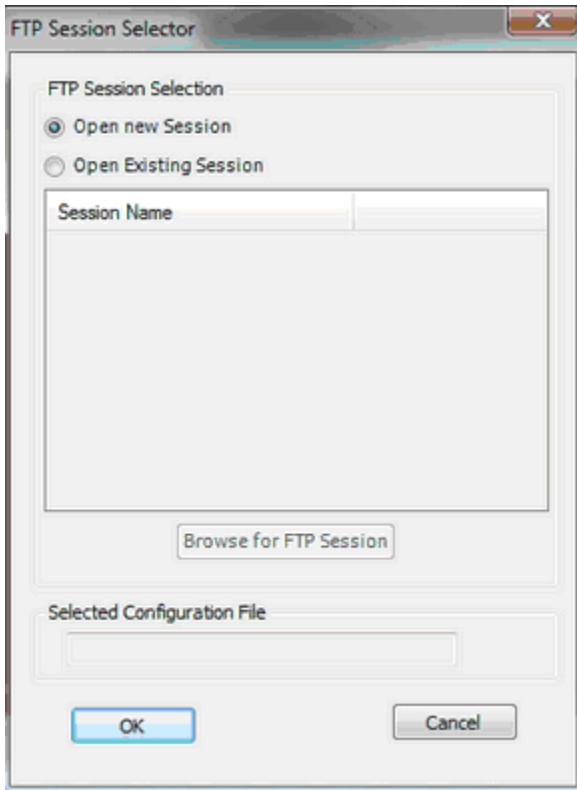
. To access classic FTP, invoke the main toolbar's options control, at the right end of the main toolbar::

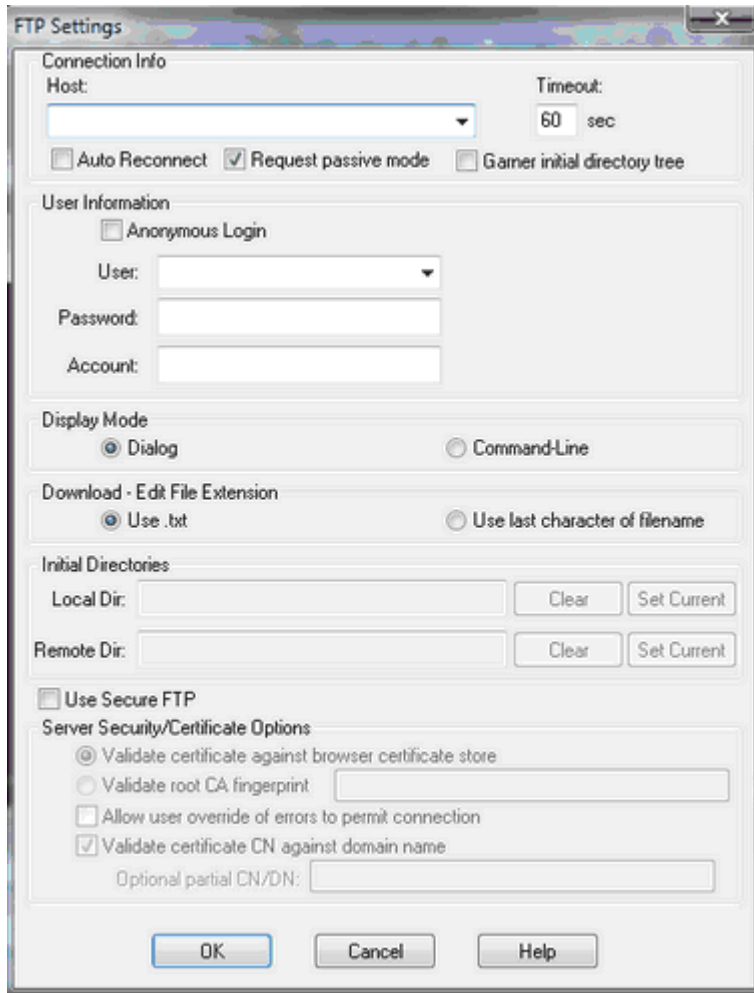


There, check on the option for the



This will display the icon  on the main toolbar and thereby give you access to the prior FTP code.





## 6.19.1.17.2 Classic FTP Settings

**"Classic" FTP Settings (Please refer to SFTP for current behaviors)**

**FTP Settings**

**Connection Info**

Host:  Timeout: 60 sec

Auto Reconnect  Request passive mode  Garner initial directory tree

**User Information**

Anonymous Login

User:

Password:

Account:

**Display Mode**

Dialog  Command-Line

**Download - Edit File Extension**

Use .txt  Use last character of filename

**Initial Directories**

Local Dir:  Clear Set Current

Remote Dir:  Clear Set Current

Use Secure FTP

**Server Security/Certificate Options**

Validate certificate against browser certificate store

Validate root CA fingerprint

Allow user override of errors to permit connection


Validate certificate CN against domain name

Optional partial CN/DN:

OK Cancel Help

### Creating a New Session:

To start an unsecured FTP session using the graphic interface:


1. Click the Classic FTP icon . The FTP Open dialog will open, defaulting to Open New Session.
2. Click OK. The FTP Settings will open.
3. Define the URL or IP address followed by a space and the port number (port number 21 is assumed).

4. Enter your user information to access the FTP server, or check "Anonymous Login" if anonymous access is allowed.
5. Select "Dialog" for the Display Mode.
6. Click "OK"

An FTP session will open to the target server using the graphic interface. This session may be saved (File/Save As... within the FTP window) for future use.

#### **Creating a New SSL-Secured FTP Session:**

To start a secured FTP session using the graphic interface:

1. Click the Classic FTP icon . The FTP Open dialog will open, defaulting to Open New Session.
2. Click OK. The FTP Settings will open.
3. Define the URL or IP address followed by a space and the port number (port number 21 is assumed).
4. Enter your user information to access the FTP server, or check "Anonymous Login" if anonymous access is allowed.
5. Select "Dialog" for the Display Mode.
6. Select "Use Secure FTP" to activate SSL-based encryption

[1. Select Either "Validate certificate " or "Validate root CA fingerprint" \(and provide it\)](#)

[2. If desired, check on "Allow user override of errors](#)

[3. If desired, check on Validate certificate CN against domain name and provide a partial CN/DN value.](#)

7. Click "OK"

An FTP session will open to the target server using the graphic interface. This session may be saved (File/Save As...) for future use.

When an FTP session is saved, the stored Remote Dir value sets the OSS/Guardian 'state and the O/G switch becomes unavailable.

For instance,

sets state to OSS

sets state to Guardian.

To reactivate the O/G switch, Clear the Remote Dir value (Options, FTP Settings)


#### 6.19.1.17.3 Classic FTP Command Mode

#### **"Classic" FTP Command Mode (Please refer to SFTP for current behaviors)**

**Note:** The Dialog option provides a much more intuitive interface for FTP sessions. Command mode should be used only if you wish to make extensive use of FTP commands.

Creating a New Session:

To start an FTP command line session:

1. Select the FTP toolbar icon . The FTP Open dialog will open displaying all defined FTP sessions and a "New" icon.
2. Double-click on the "New" icon. The [FTP Settings](#) dialog will open.
3. Define the URL or IP address followed by a space and the port number (port number 21 is assumed).
4. Enter your user information to access the FTP server, or check "Anonymous Login" if anonymous access is allowed.
5. Select "Command-Line" for the Display Mode.
6. Click "OK"

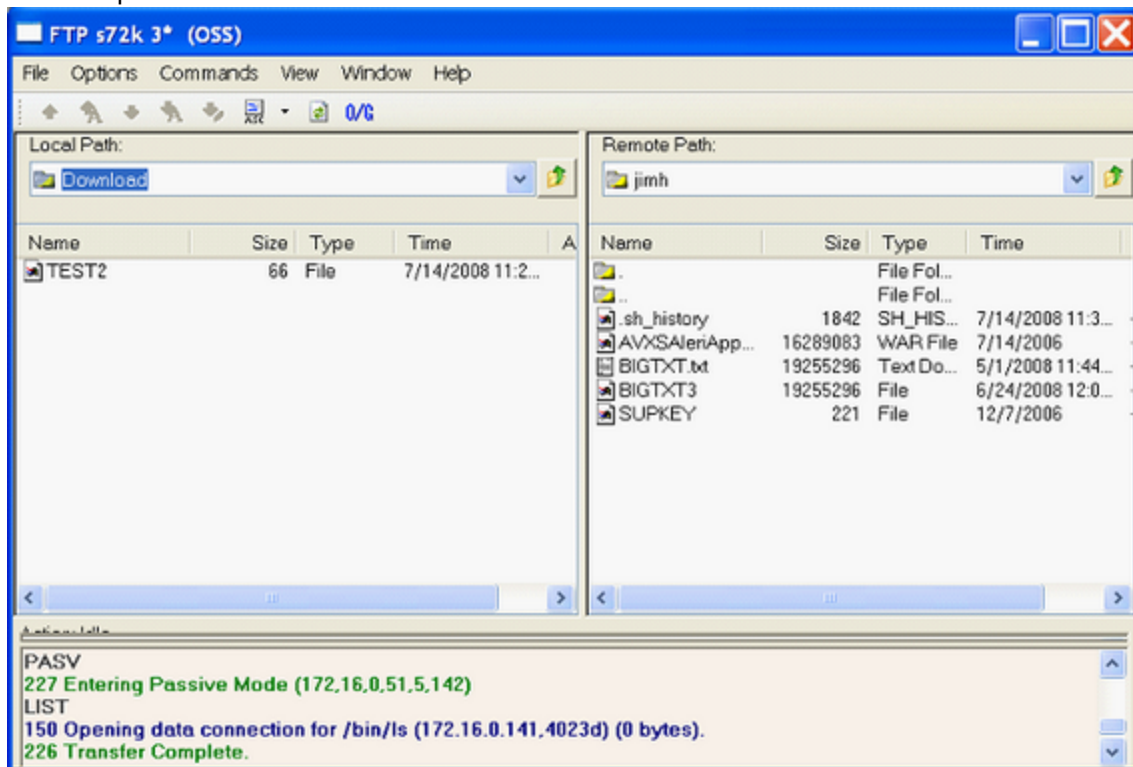
A command line FTP session will open to the target server. This session may be saved (File/Save As...) for future use.

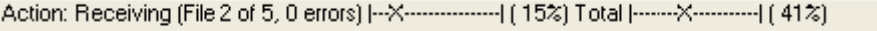
See the FTP Commands topic for descriptions of the commands supported in FTP command mode.

#### 6.19.1.17.4 Classic FTP Dialog Interface

##### "Classic" FTP Dialog Interface (Please refer to SFTP for current behaviors)

When an OutsideView FTP session is opened in Dialog mode, a graphical FTP client window opens. This window provides easy navigation of FTP servers and your local file system as well as drag – and – drop file transfers.

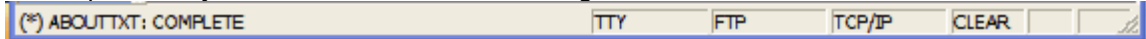


When actively transferring files, you may watch the progress of the individual and overall transfer in the progress bar: 

You may monitor or review FTP messages in the messages area:







```
PA5V
227 Entering Passive Mode (67.103.216.43.156.205)
RETR SHOWLOG
150 Opening data connection for SHOWLOG (67.103.216.43.1417d) [29232 bytes].
226 Binary Transfer complete.
```

Another way to check your FTP status is the status line at the bottom of the OutsideView window. This is particularly convenient when the FTP dialog is minimized.



### Menu Options

The menu options on this dialog provide the following functionality:

Menu Item	Functions	
File	<b>New FTP:</b> Opens the <a href="#">FTP Settings</a> window to define a new FTP session	
	<b>Open FTP:</b> Open a defined FTP session	
	<b>Save FTP:</b> Save the current FTP session	
	<b>Save As...:</b> Save current FTP session as another name	
	<b>Close FTP:</b> Shuts down FTP session	
Options	<b>FTP Settings...:</b> Opens the <a href="#">FTP Settings</a> dialog allowing changes only to File Extension and Initial Directories options. The FTP session file must be saved to retain any changes.	
	<b>Local Overwrite:</b> Allows overwrite of local files on downloads from the FTP server	
	 <b>ASCII:</b> Sets transfer mode to ASCII (default)	
	 <b>Binary:</b> Sets transfer mode to binary	
Commands	 <b>Upload:</b> Upload the currently selected local file(s) to the FTP server	
	 <b>Upload As...:</b> Prompts for a file name then uploads the currently selected local file to the FTP server	
	<b>NOTE:</b> The properties of the arriving host file can be specified using Upload As. Select the local file to send. Do an "Upload As..." In the dialog use the format: <i>FILENAME,FILECODE,EXTENTS</i> . For instance one can enter <i>BIGFILE,0,256</i> and have the extents to 256.	
	 <b>Download:</b> Download the currently selected files(s) from the FTP server	
	 <b>Download As...:</b> Prompts for a file name then downloads the currently selected file from the FTP server	





**Download and Edit:** Downloads the currently selected text file and opens it into Notepad.

**NOTE:** While editing the downloaded file the OutsideView 'parent' application will be unresponsive. You must complete the local editing operation to restore OutsideView to a receptive state

**Delete:** Attempts to delete the currently selected local or remote file(s). Delete permissions are controlled by the user's access rights.

**Rename:** Attempts to rename the currently selected local or remote file. Rename permissions are controlled by the user's access rights.

**New Folder:** Attempts to create a new local or remote folder. This capability is controlled by the user's access rights.

## View

**Toolbar:** Enables or disables display of the toolbar

**Local:** Allows definition of how local files are displayed

**Remote:** Allows definition of how remote files are displayed

**FTP Log:** Opens the FTP log showing all activity between the FTP client and server



**Refresh:** Updates the display with current information



**Toggle OSS/Guardian:** Changes file view type. Places the user into their default directory upon first use within the session.

## Window

**Local:** Show only the local files

**Remote:** Show only the remote files

**Tile Vertically:** Show the local files on the right and the remote files on the left in a vertically tiled window

**Note:** Unless the NonStop system also supports the OSS file system, graphical viewing of the NonStop Guardian file system requires creation of hint files. This process is automated by the FTPHints macro. Please see the System Administrators Guide for instructions on running this utility.

### 6.19.1.17.5 Transferring Files in Classic FTP

#### Transferring Files in "Classic" FTP (Please refer to SFTP for current behaviors)

Uploading (PC to host) or downloading (host to PC) files using the FTP Dialog may be performed by:






- Selecting one or more files (local or remote) and dragging the selection to the destination (remote or local).
- Your view into the NonStop file system can be either Guardian or OSS mode. You may switch between viewing mode by using the View/Toggle OSS/Guardian command or clicking on the



icon of the toolbar. The file viewing mode is displayed on the session title bar:

### FTP s72k.crystalpoint (OSS)


The file path display also changes with the mode. For instance, either Remote Path: \S72K.\$D00.JIMH or Remote Path: /G/d00/jimh

- Selecting one or more files (local or remote) and clicking on a toolbar Upload  or Download  button. If a single file is selected, the transfer may be initiated by clicking on the Upload As  or Download As  button.
  - Selecting one or more local files and selecting Commands/Upload or selecting one or more host files and selecting Commands/Download If a single file is selected, the transfer may be initiated by selecting Commands/ Upload As... or Commands/Download As...
  - You may also download text files from the host for editing in Notepad by:
    - Selecting the host text file and clicking on the Download and Edit  toolbar button.
    - Selecting the host text file and selecting Commands/Download and Edit
- The file will be transferred to your PC and opened in Notepad. A dialog to upload the file once your edits are complete is also opened.

**Note:** Unless the NonStop system also supports the OSS file system, graphical viewing of the NonStop Guardian file system requires creation of hint files. This process is automated by the FTPHints macro. Please see the System Administrators Guide for instructions on running this utility.

### Transfer Mode

The transfer mode (ASCII or binary) may be selected by:

- Clicking on the down arrow adjacent to the Transfer Type toolbar  button.
- Selecting Options and ASCII or Binary

### Local Overwrite

You may allow local files to be overwritten by those from the host by selecting Options/Local Overwrite.

#### 6.19.1.17.6 Classic FTP Trace

##### Classic FTP Trace

There is an FTP trace capability within 'classic' FTP. It is used only with newly created FTP sessions, not within saved FTP sessions (since it will not capture session initiation). To activate the trace function, select the classic FTP icon, but rather than initiating the session (after you configure it) by simply clicking on the OK button, hold down Control+Shift when clicking on the OK button. The trace file will be locally created as C:\ftptrace.cap

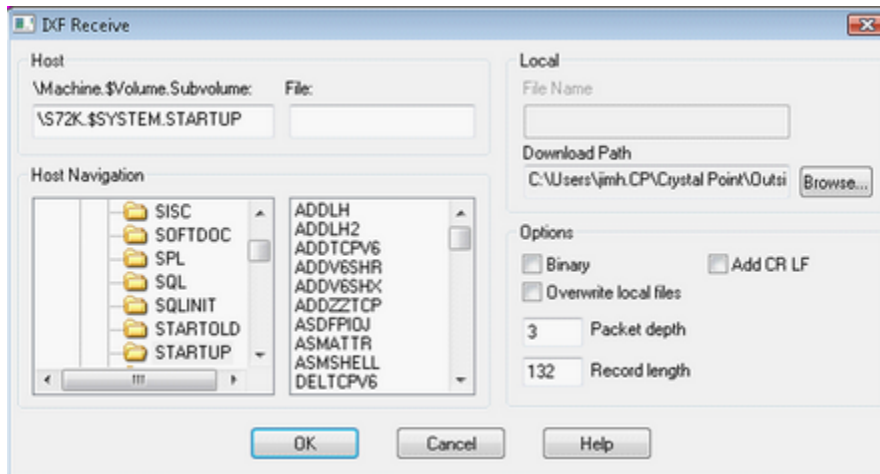
## 6.19.2 IXF

IXF is a proprietary NonStop file transfer facility. It operates by transferring files over an existing terminal session. IXF is rarely used, but still supported for operations that don't lend themselves to FTP or SFTP. It requires a host component called \$SYSTEM.SYSTEM.IXF. The IXF host component can be ordered from HPE as a separate product BE111AC (HPE NonStop IXF Host SW).

### 6.19.2.1 IXF Receive

#### IXF Receive

This dialog box is used to receive files on your local PC from the remote NonStop host using the IXF (Information Exchange Facility) protocol.



- You must have an active TACL session on a NonStop host to initiate an IXF transfer.
- For your convenience, closing sessions or closing OutsideView does not reset your IXF Transmit and Receive settings. These settings remain in effect until you explicitly change them; you don't have to re-specify your connection information each time you want to transfer files.

#### To receive a file (or files):

1. Specify the file or files you want to receive. There are two methods you can use:
  1. In the Host group box, enter the location in the \Machine.\$Volume.Subvolume field and the file name in the File field. Both of these fields support the use of wildcards (asterisk and question mark).
  2. You can easily browse the host file system using your mouse.

**Note:** Browsing of the Guardian file system requires the OVFSCAN utility to be running on the NonStop platform. Please see the topic [Guardian File System Graphical Navigation](#) for instructions on installing that utility.

2. In the Local group box, select the target directory where the received file or files will be saved. If you are receiving a single file, you can specify its file name. Multiple files are given the same file name as on the host.
3. Set the desired options for the transfer. If you are receiving text files, make sure the Binary option is not checked.
4. Click OK to initiate the transfer.

A dialog box informs you of the status of the transfer in progress.

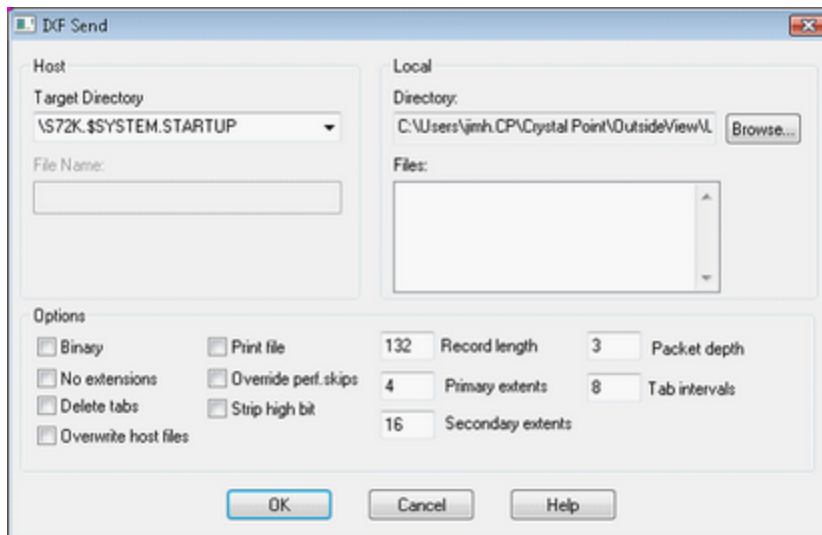
The transfer status dialog box can be minimized (onto the desktop) while the transfer is in process. This allows you to access other sessions within OutsideView. But the session in which the transfer is occurring is "locked" (not permitting any keyboard activity) until the transfer finishes and you exit the transfer status dialog box.

### 6.19.2.2 IXF Send

#### IXF Send

**Note:** Browsing of the Guardian file system requires the OVFSCAN utility to be running on the NonStop platform. Please see the topic [Guardian File System Graphical Navigation](#) for instructions on installing that utility.

This dialog is used to send files from your local PC to the remote NonStop host using the IXF (Information Exchange Facility).



- You must have an active TACL session on a NonStop host to initiate an IXF transfer.
- For your convenience, closing sessions or closing OutsideView does not reset your IXF Transmit and Receive settings. These settings remain in effect until you explicitly change them; you don't have to re-specify your connection information each time you want to transfer files.
- If you attempt to send a file that has a file name that does not begin with an alphabetic character – for example, 123myfile.txt – OutsideView will add the letter "N" to the beginning of the file name. For example, this file name would now be N123myfile.txt.

#### To Send a File to the Host:

1. Select the target directory (where the sent file will be saved) in the Target Directory box.
  - There is a checkbox that specifies the behavior when overwriting files. If checked, files being transmitted overwrite (replace) existing host files with the same name. If unchecked, the action depends on the file type. A text file with the same name as an existing host file causes an error and cancels the transfer. A binary file with the same name as an existing host file appends to the existing host file.
  - Wildcard characters ( \* and ? ) are supported for both File and Hostname; all files matching the criteria will be sent.
2. Set the desired options for the transfer.
  - If you are transferring a text file, make sure the Binary option is not checked.
3. Click OK to initiate the transfer.

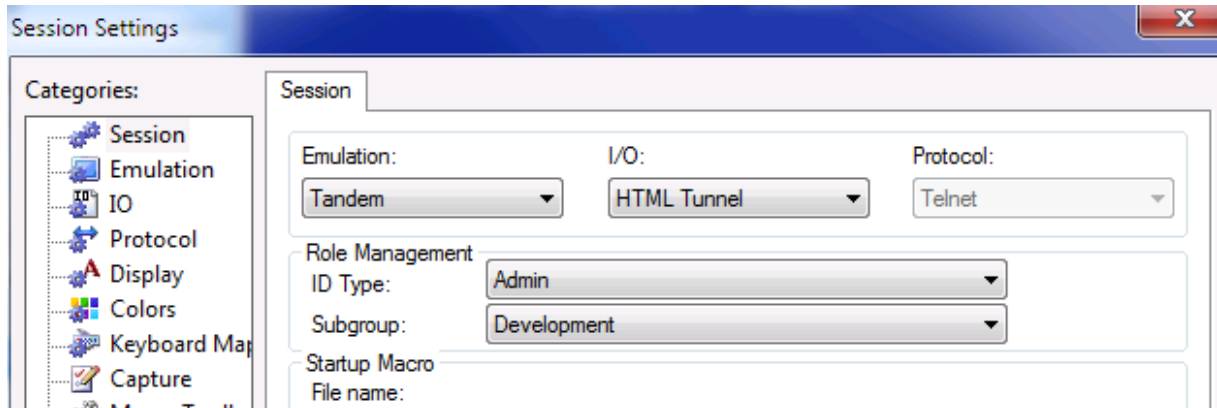
A dialog box informs you of the status of the transfer in progress. The transfer status dialog box can be minimized (onto the desktop) while the transfer is in process. Minimizing the window allows you to access other sessions within OutsideView, but the session in which the transfer is occurring is

"locked" (not permitting any keyboard activity) until the transfer finishes and you exit the transfer status dialog box.

## 6.20 HTML Tunnel

### HTML Tunnel

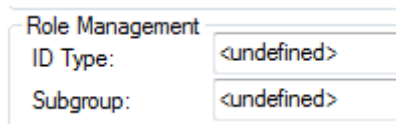
When creating a new HTML Tunnel session, use the Session tab to select HTML Tunnel as the I/O method:



Thereafter, all HTML Tunnel specific settings are found within the I/O category.

### 6.20.1 ID Management and HTML Tunnel

#### Role Management and HTML Tunnel



Selection of an ID type is **Optional** in HTML Tunnel.

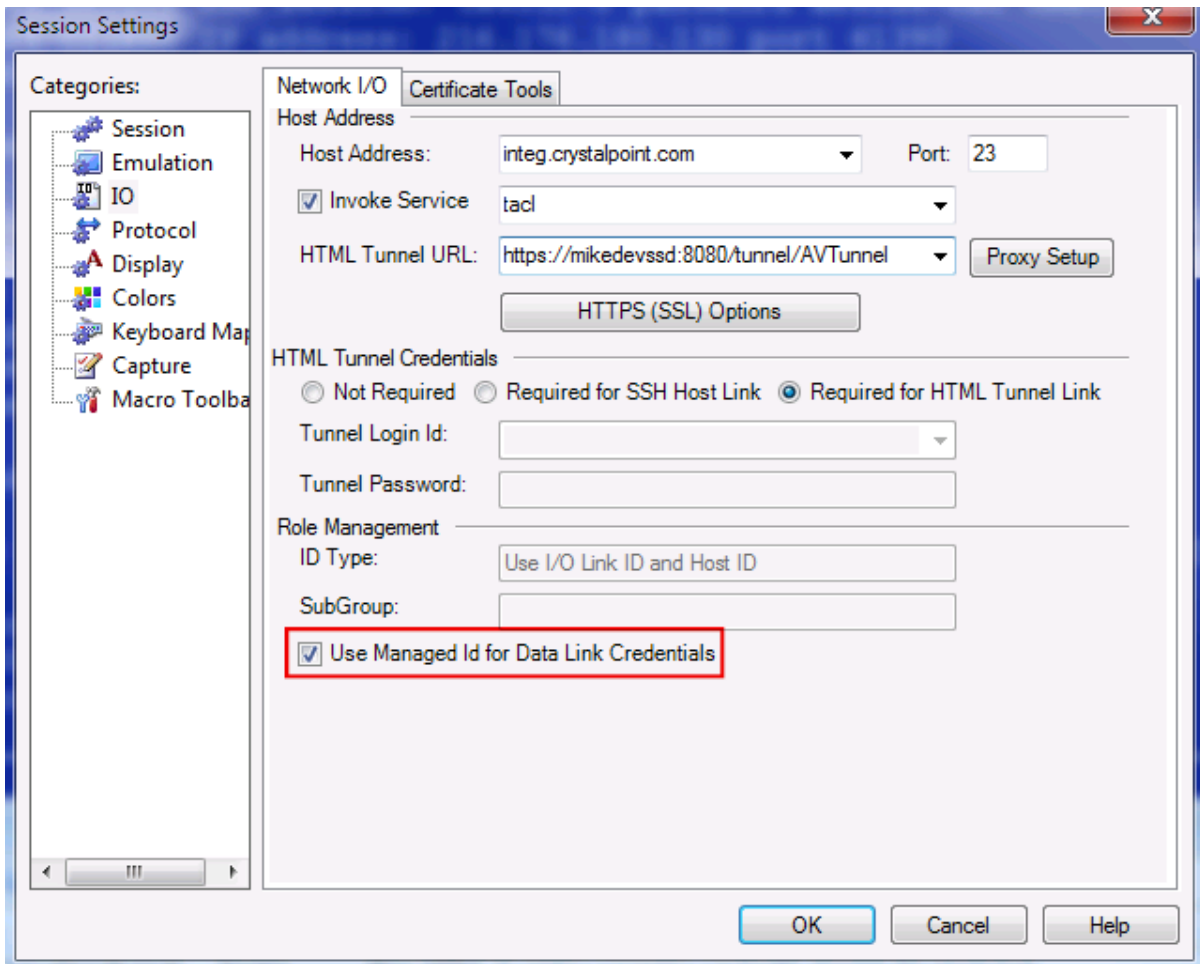
If an ID Type is specified, then the selected ID type and Subgroup will be displayed in the I/O tab. The ID Type and SubGroup credentials can be used with Invoke Service enabled and set to tacl.

#### New ID Type introduced in OutsideView 9.0

- I/O Link ID
- Use I/O Link ID and Host ID

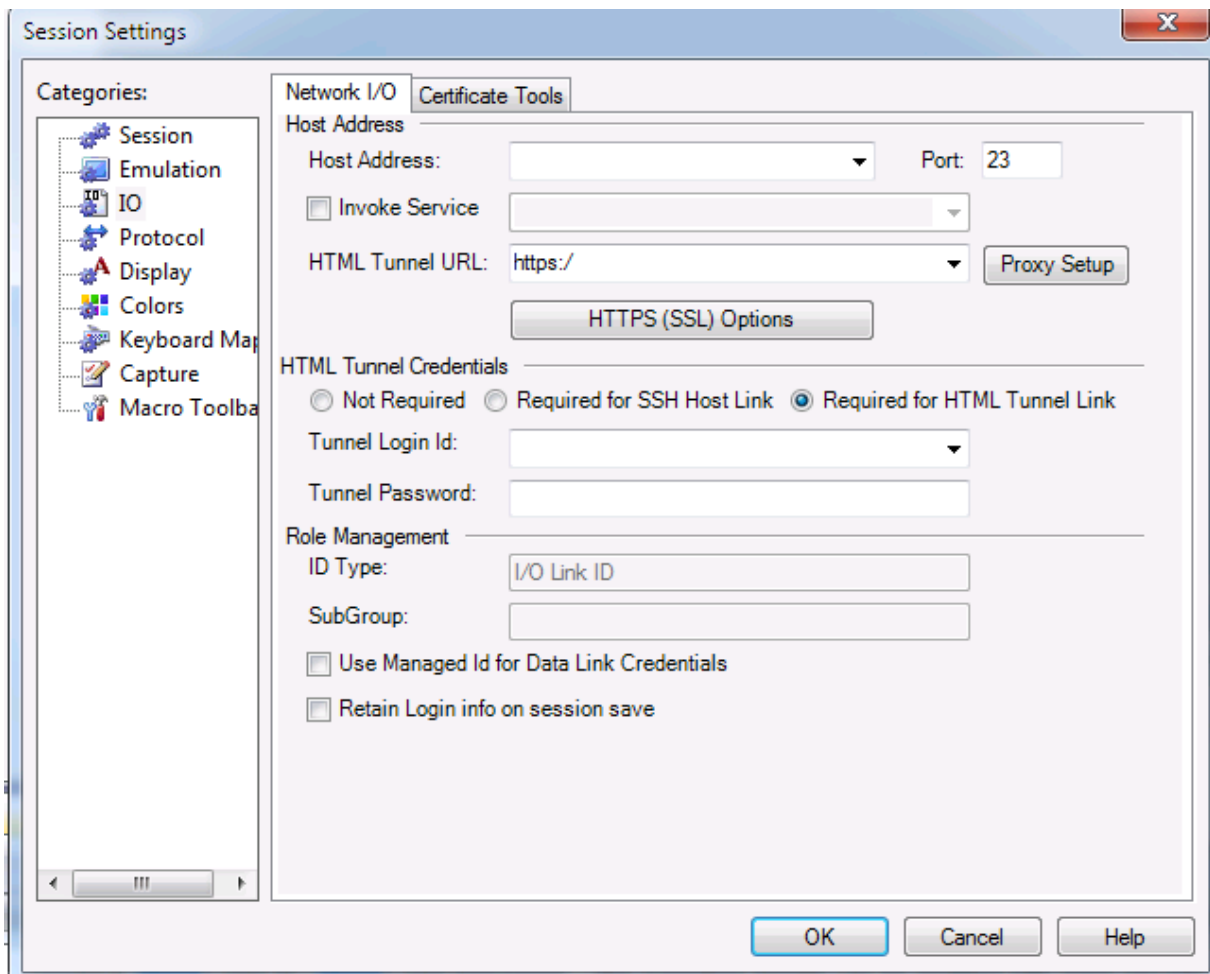
These two new ID types are used with the "Use Managed Id for Data Link Credentials" to provide login credentials for the data link and also for the host.

When using separate logins for the SSH data link level and host application interactions, it might be appropriate in your organization to use common credentials for securing the data link and save this information in the host configuration file that you distribute to the users. In this case you can still set a managed ID to prompt the user for their personal credential and enable the entering/retention of the link level credentials by **unchecking** "Use Manage Id for Data Link Credentials" checkbox.



### 6.20.2 Configuring HTML Tunnel

This communications transport method was introduced in OutsideView 9.0 and permits routing (tunneling) through one intermediate host to reach the final destination.



**NOTE:** HTML Tunnel requires a companion product called AVTunnel, AVTunnelSSH, or AVTunnelSSL. These tunneling servlets are a separate down-loadable product from Crystal Point. Contact [sales@crystalpoint.com](mailto:sales@crystalpoint.com) for further information.

- **Host Address** -- This is the URL that you would enter to the host (Do not include the port in this field)
- **Port** -- The port on the host you want to connect to.
- **Invoke Service** -- Host service to launch
- **HTML Tunnel URL** -- This is the Tunneling Servlet URL that OutsideView communicates with to wrap the data using http/https protocol. **Note** to ensure that this segment of the circuit is secure, it is recommended that you use the HTTPS protocol.
- **Tunnel Login Id / Tunnel Login Password** -- The Tunneling Servlet can be enabled with extra security step requiring users to authenticate themselves before the connection is allowed through the tunneling servlet.
- **SSH Host Login Id / SSH Host Password** -- Visible when Required for SSH Host Link is selected. These credentials are used to negotiate a secure connection to host.
- **HTML Tunnel Credentials:**

- **Not Required** -- This option is used when connecting through a tunneling servlet that is configured with userAuthentication set to false (AVTunnel and AVTunnelSSL).
- **Required for SSH Host Link** -- This option is used when connecting through the SSH version of the tunneling servlet (AVTunnelSSH). **Note** that the SSH Tunneling servlet must be configured with userAuthentication set to false. When using this option you will need to specify your SSH login name and password into the HTML Login Id and HTML Password field. These credentials are used by the SSH version of the tunneling servlet to connect to the SSH port on the host.
- **Required for HTML Tunnel Link** -- This option is used when connecting to a regular tunneling servlet and SSL version of tunneling servlet (AVTunnel and AVTunnelSSL) with the userAuthentication set to true and the session configured to use Role Management for auto login. You will need to specify the values for Tunnel Login Id and Tunnel Password that were configured for the tunneling servlet.
- **Role Management** -- The User ID Type and Subgroup can be used for logging into your session on the host. Note you may need to enable the Invoke Service and set that value to something like tacl for autologin function correctly.
- **Use Managed Id for Data Link Credentials** -- Use Managed ID (ID Type) to provide credentials to host. There are two new ID types (I/O Link ID and Use I/O Link ID and Host ID) that can be used with the "Use Managed Id for Data Link Credentials" feature to provide login credentials for the data link and also for the host application. When using separate logins for the SSH data link level and host application interactions, it might be appropriate in your organization to use common credentials for securing the data link and save this information in the host configuration file that you distribute to the users. In this case you can still set a managed ID to prompt the user for their personal credential and enable the entering/retention of the link level credentials by **unchecking** "Use Manage Id for Data Link Credentials" checkbox.
- **Retain Login info on session checkbox** -- Note that this checkbox is visible when the Use Managed Id for Data Link Credentials is **unchecked!** This option saves the current values in the HTML Login Id and HTML Password fields. Otherwise the value for HTML Password will be erased. **Note** when using Role Management this property is hidden.

## 6.21 Macros

### 6.21.1 Macro Editor

OutsideView now offers two means of automation. The Visual Comm Basic proprietary macro language is the original method provided. It continues to work, but support is limited to assuring the verbs works in newer environments.

Our **newer, more powerful and flexible automation method is a .NET API**. For more information, see the .NET API Help topic, in OutsideView.

#### Macro Editor

The Visual CommBASIC integrated development environment may be opened by selecting Macro/Macro Editor.... For a comprehensive guide on creating macros in the Visual CommBASIC environment please see the Visual CommBASIC Reference.

### 6.21.2 Running Macros

#### Running Macros

A Visual CommBASIC macro may be executed within OutsideView by:

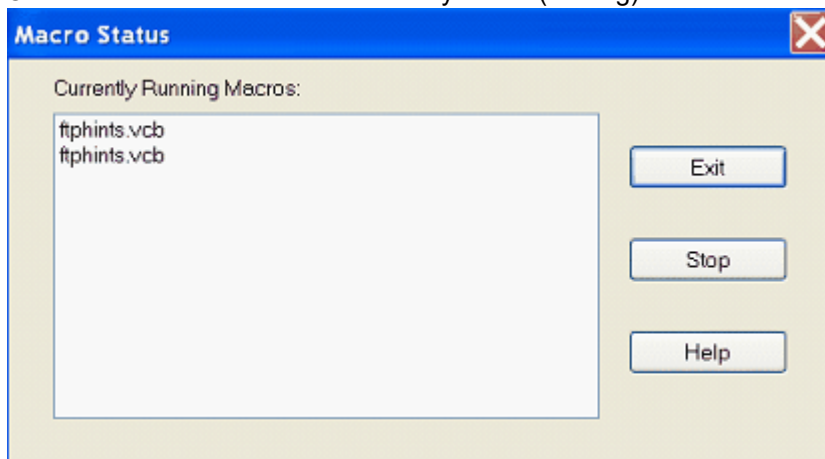


- Selecting Macro/Run Macro...: Then selecting the desired macro and clicking Open
- Opening a workspace with a startup macro: See the topic [Workspaces](#) for instructions how to define a workspace startup macro.
- Opening a Session with a startup macro: See the [Session tab](#) topic for instructions on defining a session startup macro.
- Clicking on a toolbar button: See the [Macro Toolbar](#) topic for instructions on mapping a macro to a toolbar button.
- Pressing a key sequence: See the [Keyboard Mapping](#) topic for instructions on mapping a macro to a key sequence.
- Including the macro in the OutsideView command line: See the [Command Line Options](#) topic for instructions on how to include a macro in the OutsideView command line.

### 6.21.3 View Macro Status

#### View Macro Status

The Macro Status dialog box is accessed by selecting Macro/Macro Status.... This dialog allows you to see the status of all your macros and easily terminate an active macro. The list contains all OutsideView macros that are currently active (running).



- To terminate a macro, click on the unwanted macro, then click the Stop button. The macro immediately halts its execution, unloads, and is no longer listed in the dialog box.
  - To leave the Macro Status dialog box at any time, click Exit.
- For detailed information on Visual CommBASIC and creating macros, refer to the comprehensive Visual CommBASIC Reference.

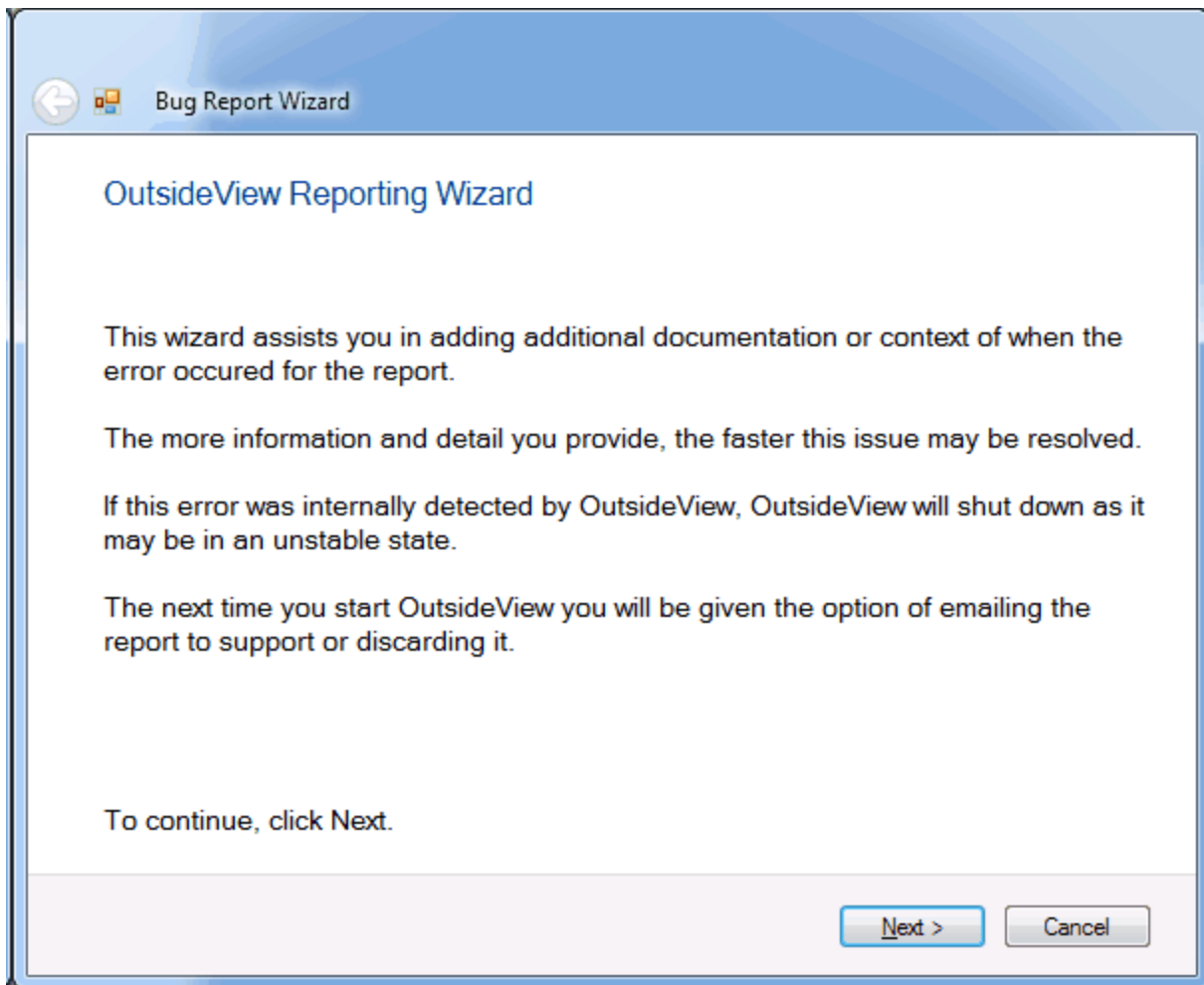
## 6.22 OV Automated Error Reporting

Error reports can be triggered automatically from internal errors detected by OutsideView or submitted manually by the user from the help menu.

### 6.22.1 Bug Report Wizard

Users can manually submit a report from the Help | Report Bug or RFE menu option if they want to request an RFE or report an issue with OutsideView. If OutsideView crashes this reporting process is started and a wizard appears to lead the user through the reporting process.

The image below is the initial dialog screen that is presented to the user when a crash event has occurred in OutsideView and the user shuts down and restarts OutsideView.

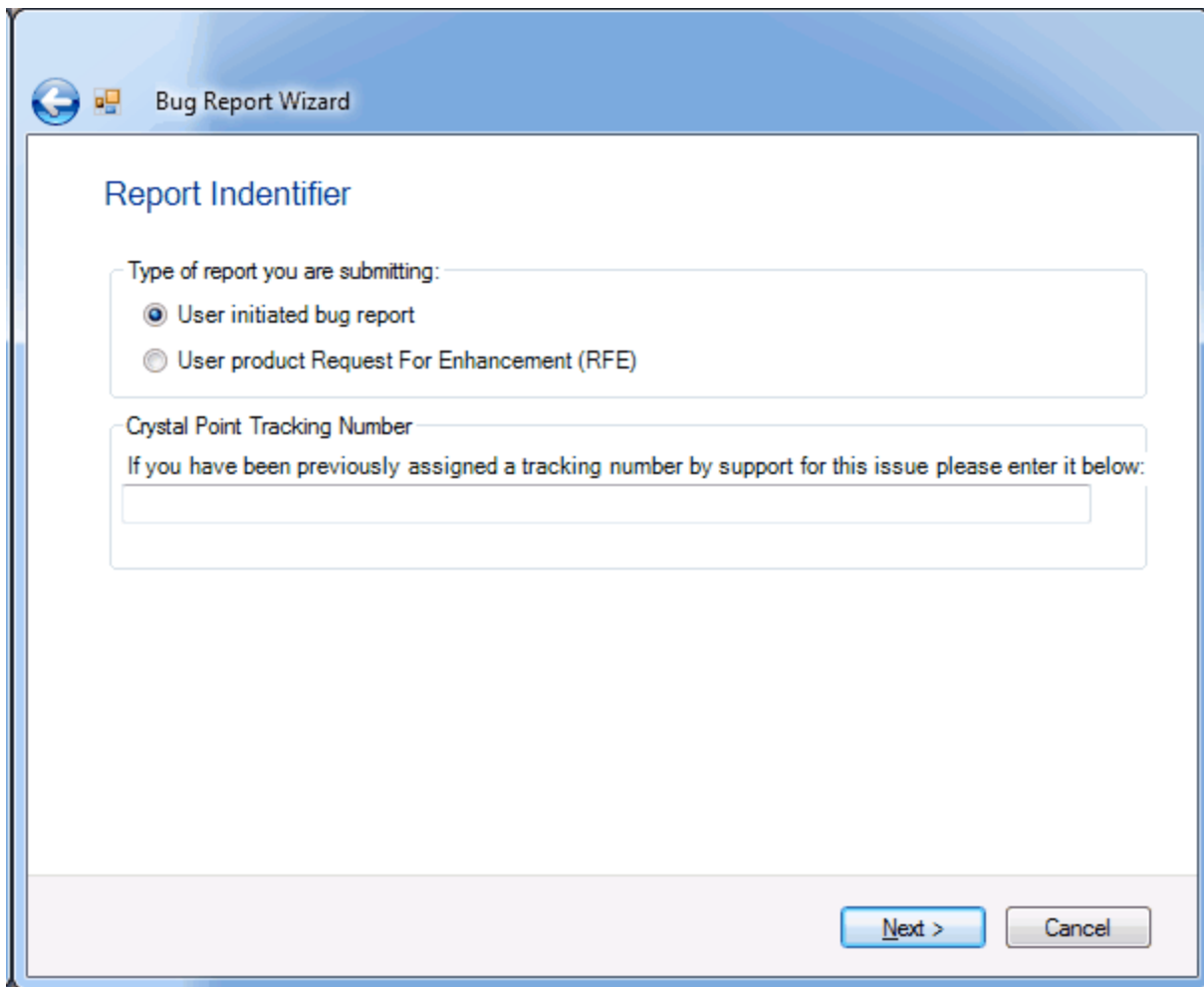


After clicking the next button the **Report Identifier** page appears. If this report was started by the user then they are prompted if it's an actual bug report or request for enhancement.

If the report is triggered by an internal error then the only dialog that will appear is a prompt for them to enter the tracking number if this is a reoccurring problem.

If the user selects RFE the tracking number panel will disappear replaced by a panel asking them for title of the RFE which will appear as part of the email subject line when the report is sent.

Also when RFE is selected the order of wizard pages they will visit is changed to a smaller subset for the user.



The image shows a screenshot of a software dialog box titled "Bug Report Wizard". The dialog has a blue header bar with a back arrow icon and a small icon to the left of the title. The main content area is white and contains the following elements:

- Report Identifier**: A section header in blue text.
- Type of report you are submitting:**: A label above a rounded rectangular container.
  - User initiated bug report
  - User product Request For Enhancement (RFE)
- Crystal Point Tracking Number**: A label above another rounded rectangular container.
  - Text: "If you have been previously assigned a tracking number by support for this issue please enter it below:"
  - A text input field below the text.

At the bottom right of the dialog, there are two buttons: "Next >" (highlighted in blue) and "Cancel" (disabled).

If a graphics image is detected on the system clipboard this page will appear to ask the user if they wish to include the image in the report that is sent:

Clipboard Image Detected, Include in Report?

Report Identifier

Type of report you are submitting:

- User initiated bug report
- User product Request For Enhancement (RFE)

Crystal Point Tracking Number

If you have been previously assigned a tracking number by support for this issue please

Include clipboard image into bug report data?

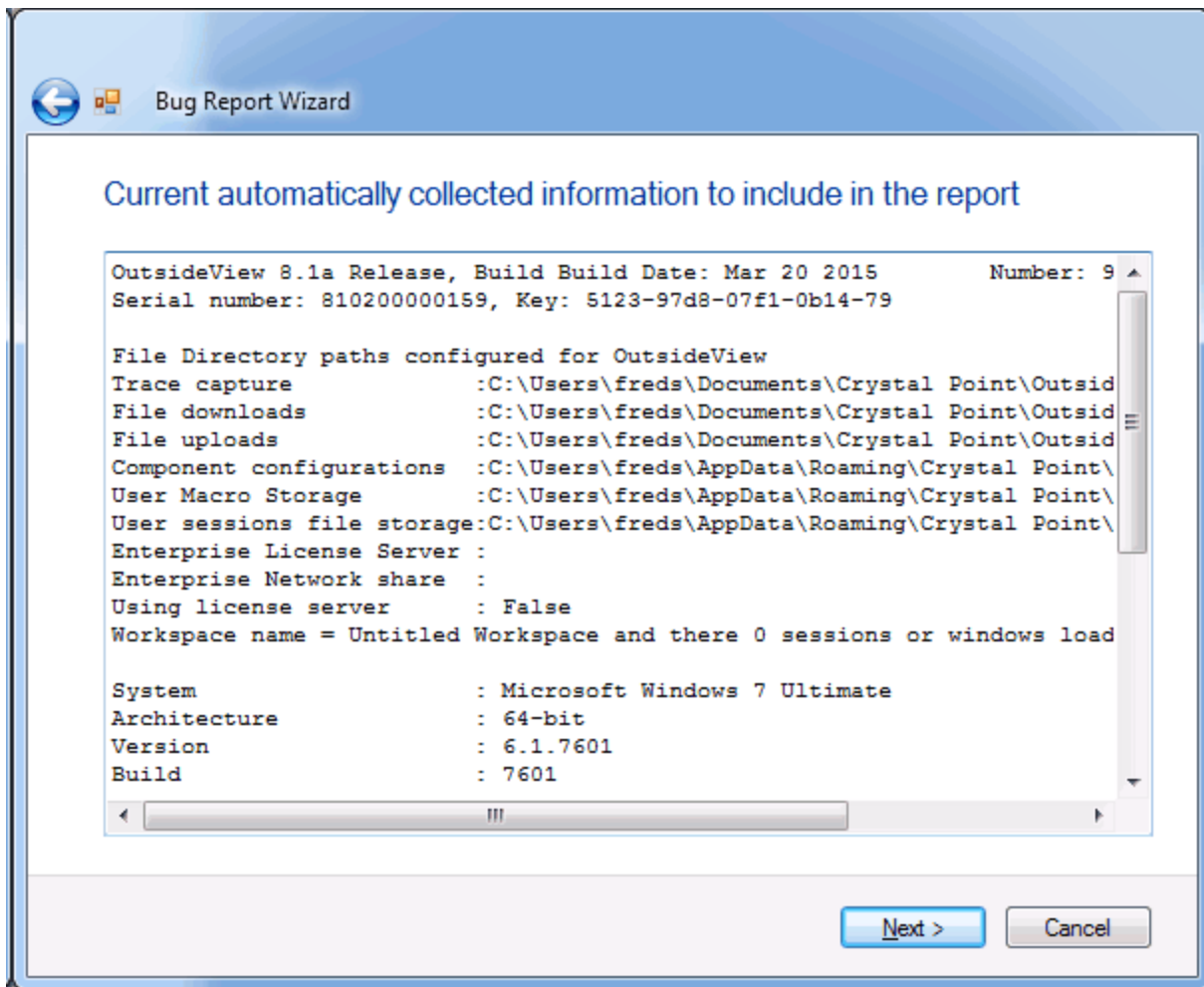
Next > Cancel

The **Description of Problem** page is where the .NET error is disclosed on internally detected errors this will obviously have more information visible.

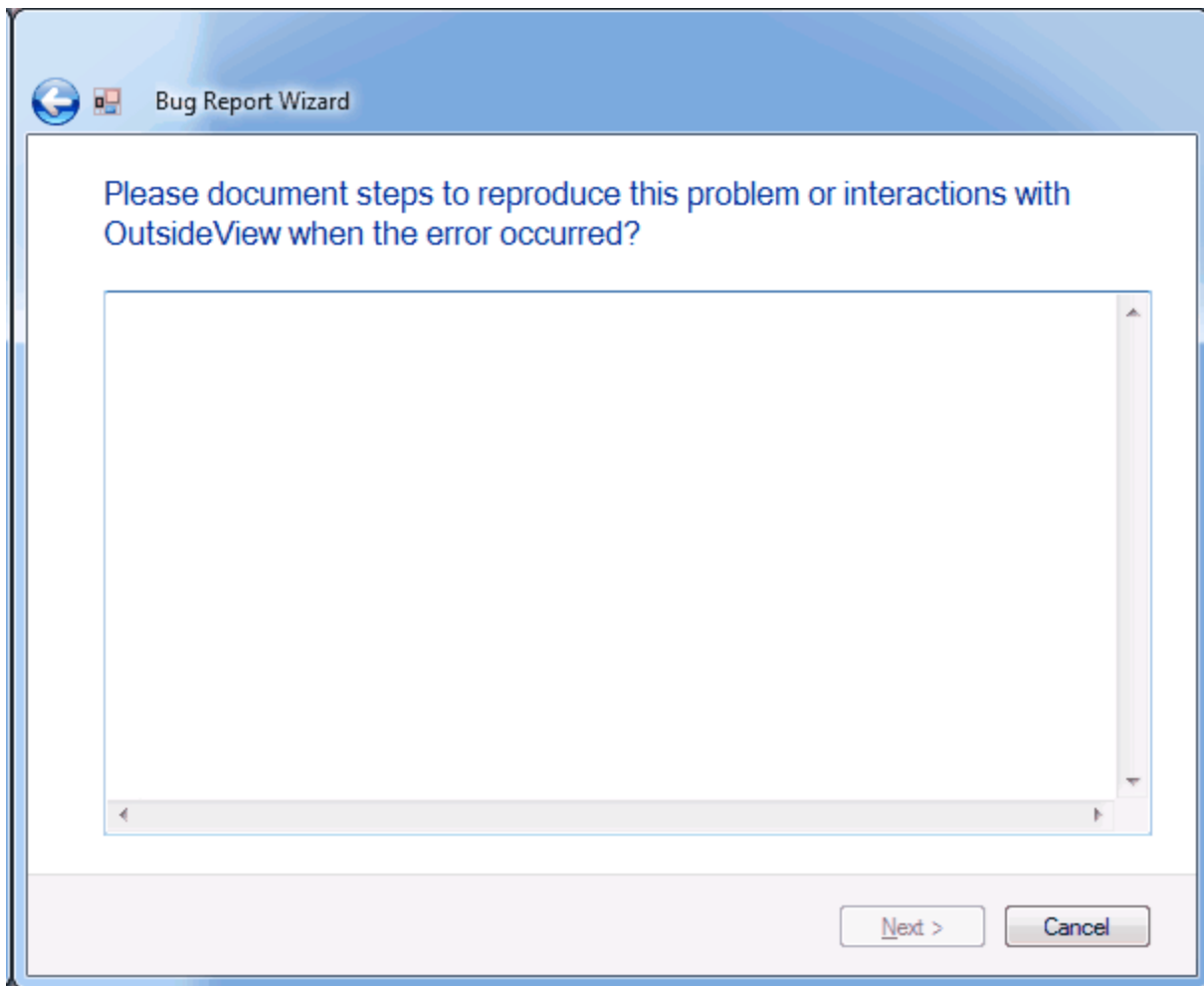
The last input field on this page is asking them for title of the error which will appear as part of the email subject line when the report is sent. Note the next button is greyed out until they start entering text into the field.

The screenshot shows a 'Bug Report Wizard' window with a blue header bar containing a back arrow icon and the text 'Bug Report Wizard'. The main content area is titled 'Discription of Problem' (note the typo). Below the title are two tabs: 'General' and 'Exception'. The 'Exception' tab is selected. The content of the 'Exception' tab includes the text 'The current information is know about the problem.' (note the typo). Below this text are several input fields: 'Exception Type:' with the value 'System.Exception', 'User Submitted problem report' (empty), 'Target Site:' (empty), 'Date/Time:' with the value '3/29/2015 7:27:35 PM', and 'CLR:' with the value '2.0.50727.5485'. Below these fields is a paragraph of instructions: 'Please provide a short descriptive email subject title of the error such as "Connection error under SSH" or "error copying to clipboard". Another page will allow you to enter more detail.' Below this text is an empty text box. At the bottom right of the window are two buttons: 'Next >' and 'Cancel'.

This next page is information that we can automatically determine about the environment that OutsideView is executing under. Including workspace name and basic information on each active session.

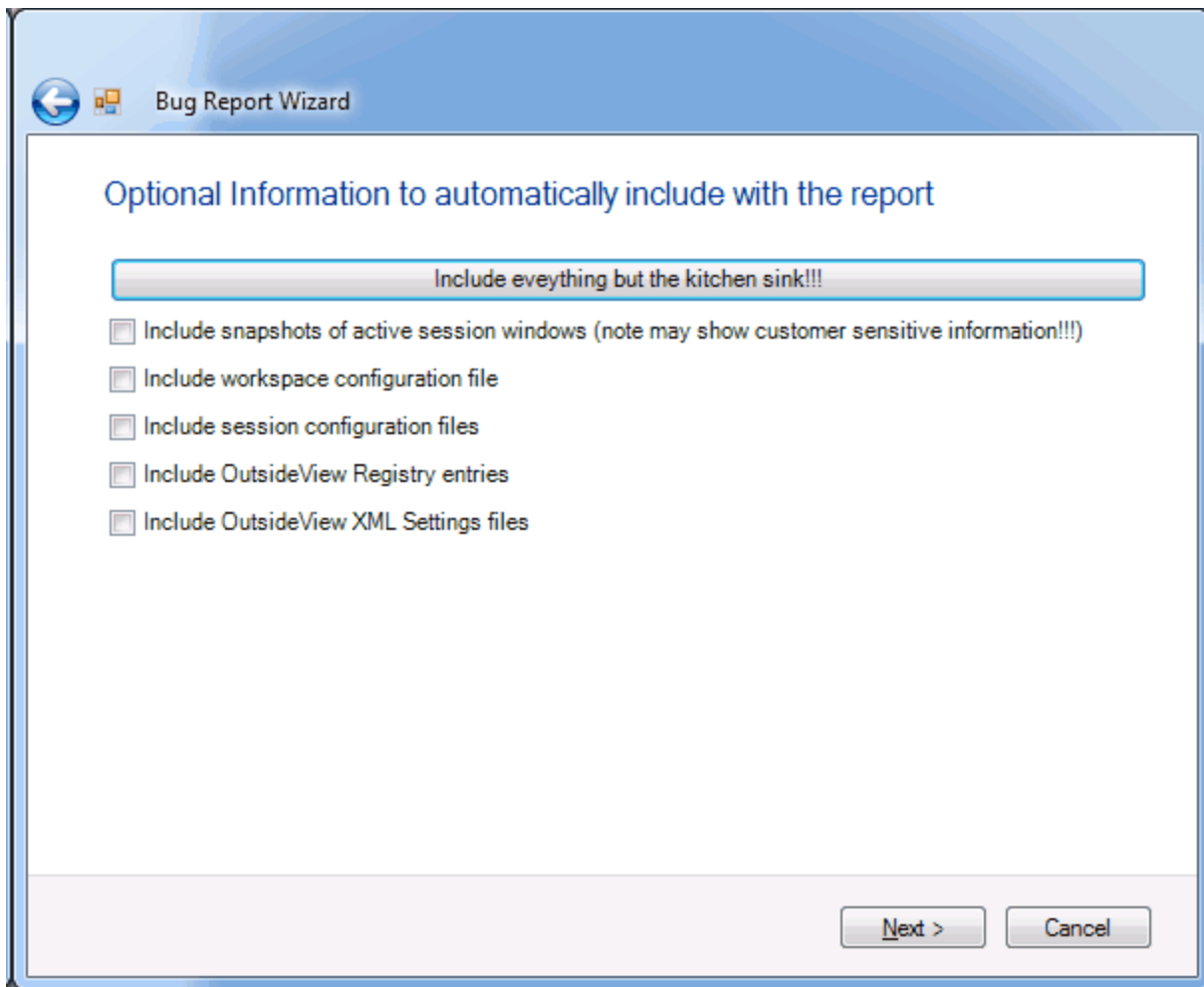


Users are then taken to a page where they can enter more information about how they got OutsideView to produce the error and hopefully reproduction steps:



The image shows a screenshot of a software dialog box titled "Bug Report Wizard". The dialog has a blue header bar with a back arrow icon and a close button. The main content area contains the text: "Please document steps to reproduce this problem or interactions with OutsideView when the error occurred?". Below this text is a large, empty text input field with a vertical scrollbar on the right and a horizontal scrollbar at the bottom. At the bottom right of the dialog, there are two buttons: "Next >" and "Cancel".

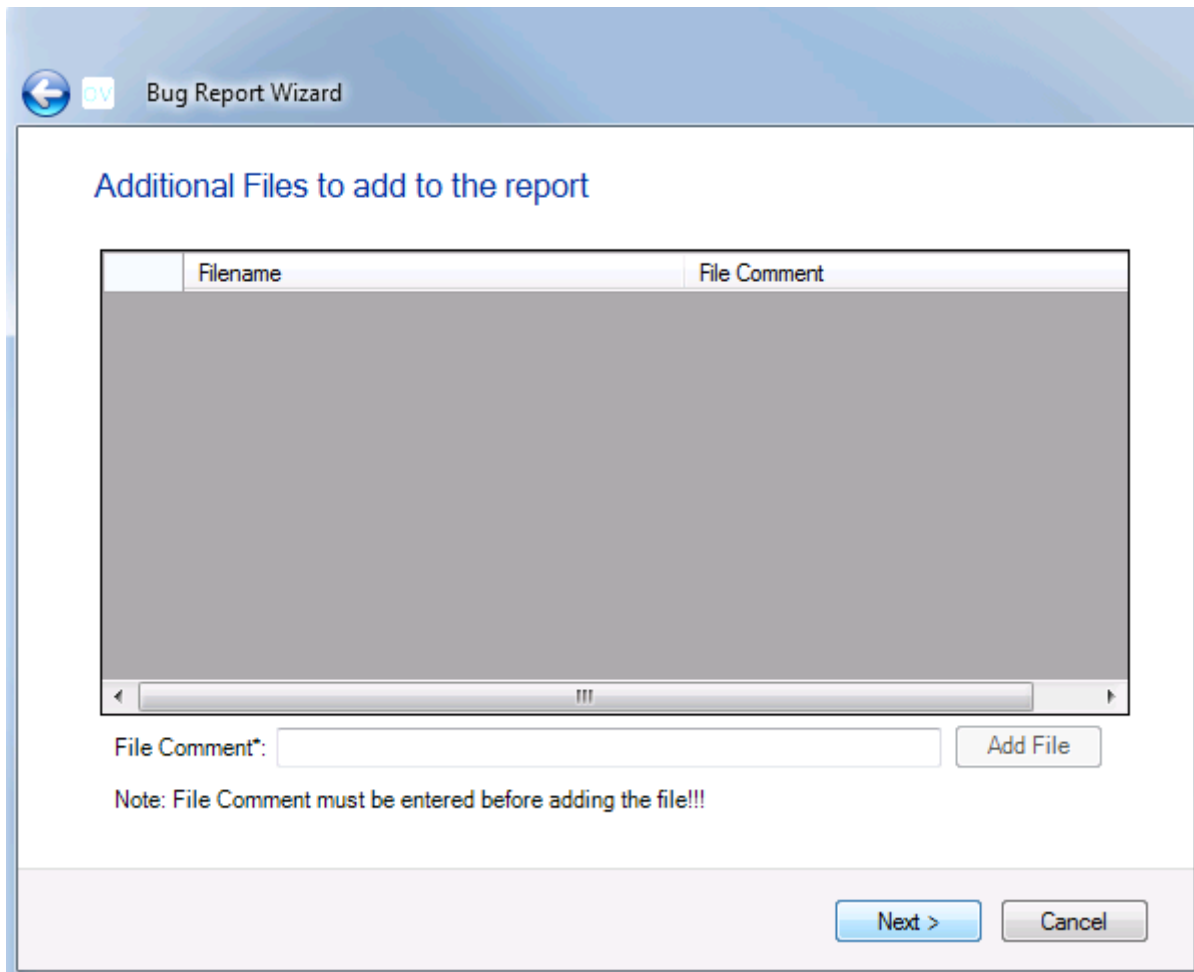
They are then taken to a page to specify optional information to automatically include with the report.



Users can then add any additional files that they would like to the report. Maybe they have a word document where they have taken other snapshots or maybe a history of how often the problem occurs, etc.

Note the GUI interactions with the Add File button and the next button. Users first have to describe why the file is being included before they can add.





The screenshot shows a software window titled "Bug Report Wizard" with a blue header bar. Below the header, the text "Additional Files to add to the report" is displayed in blue. A table with two columns, "Filename" and "File Comment", is shown with a greyed-out body. Below the table is a "File Comment\*" text input field and an "Add File" button. A note below the input field reads "Note: File Comment must be entered before adding the file!!!". At the bottom right, there are "Next >" and "Cancel" buttons.

Filename	File Comment
----------	--------------

File Comment\*:

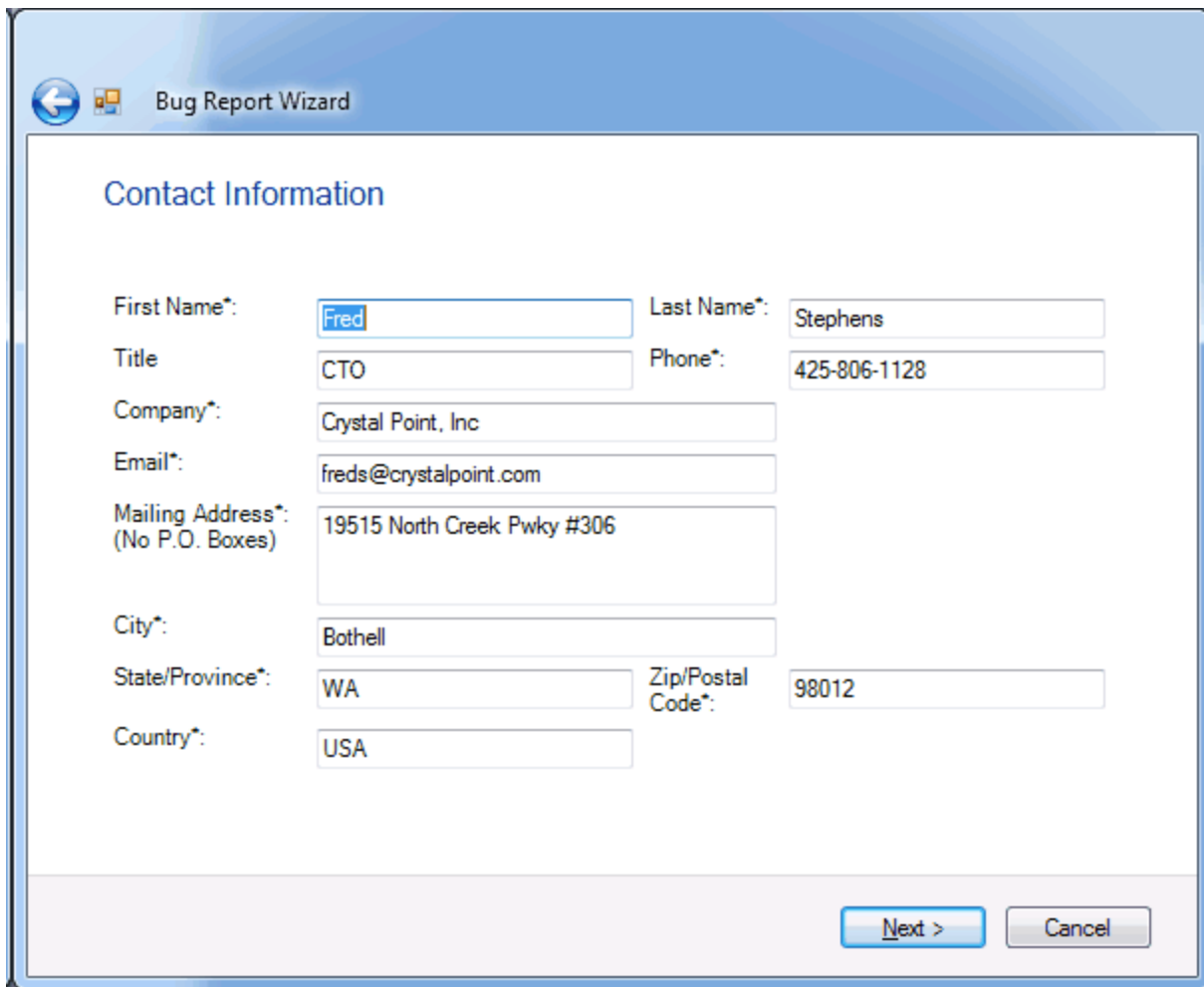
Note: File Comment must be entered before adding the file!!!

Next > Cancel

The last input panel users see is the Contact Information page, all the fields on this screen are required input except for Title just like they are on our web site.

We attempt to seed this information from Active directory when OutsideView is first run for the user.

This results in the creation of a new XML configuration file named AutoErrorReporting:



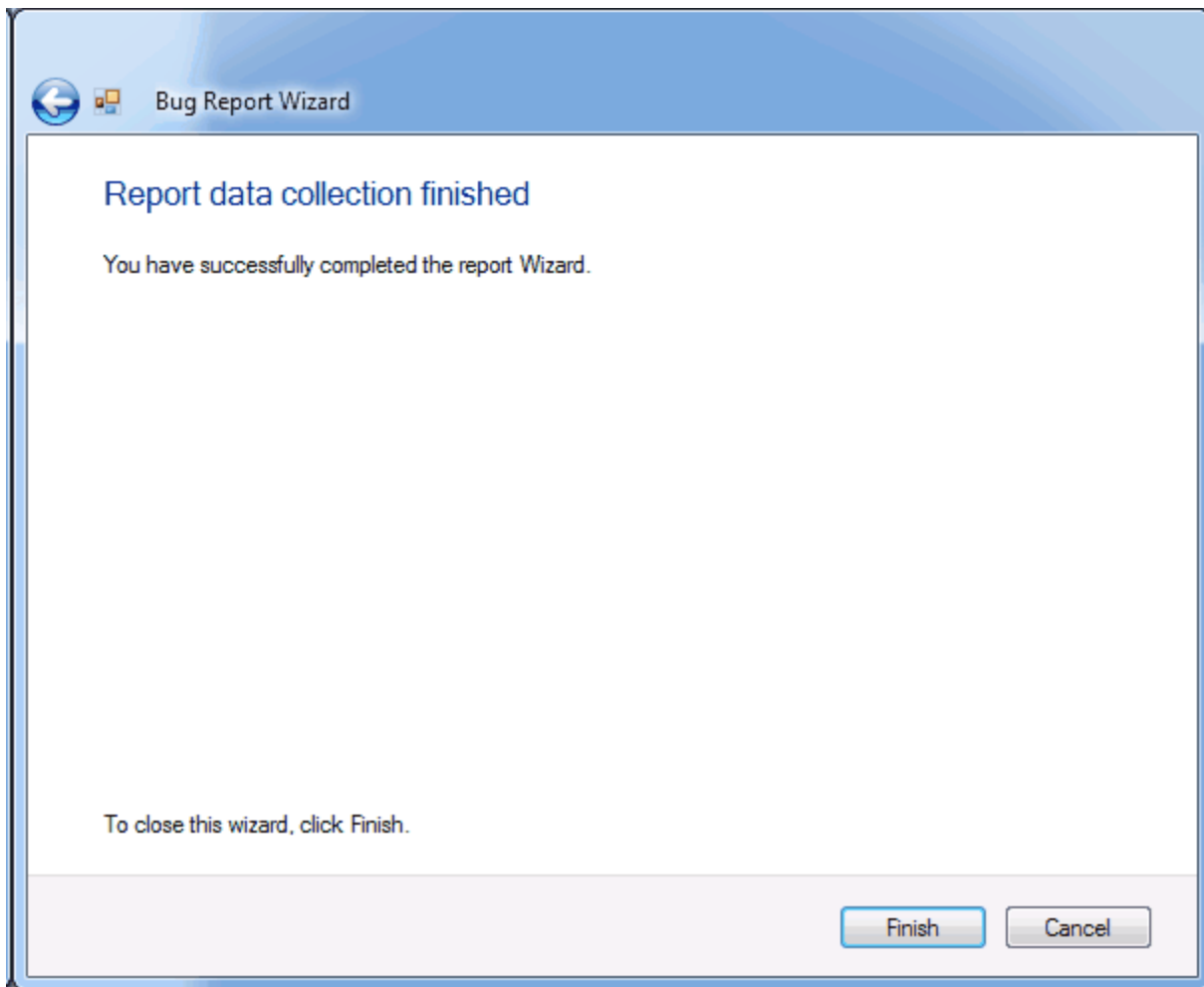
The screenshot shows a 'Bug Report Wizard' window with a 'Contact Information' section. The form contains the following fields and values:

Field	Value
First Name*	Fred
Last Name*	Stephens
Title	CTO
Phone*	425-806-1128
Company*	Crystal Point, Inc
Email*	freds@crystalpoint.com
Mailing Address* (No P.O. Boxes)	19515 North Creek Pwky #306
City*	Bothell
State/Province*	WA
Zip/Postal Code*	98012
Country*	USA

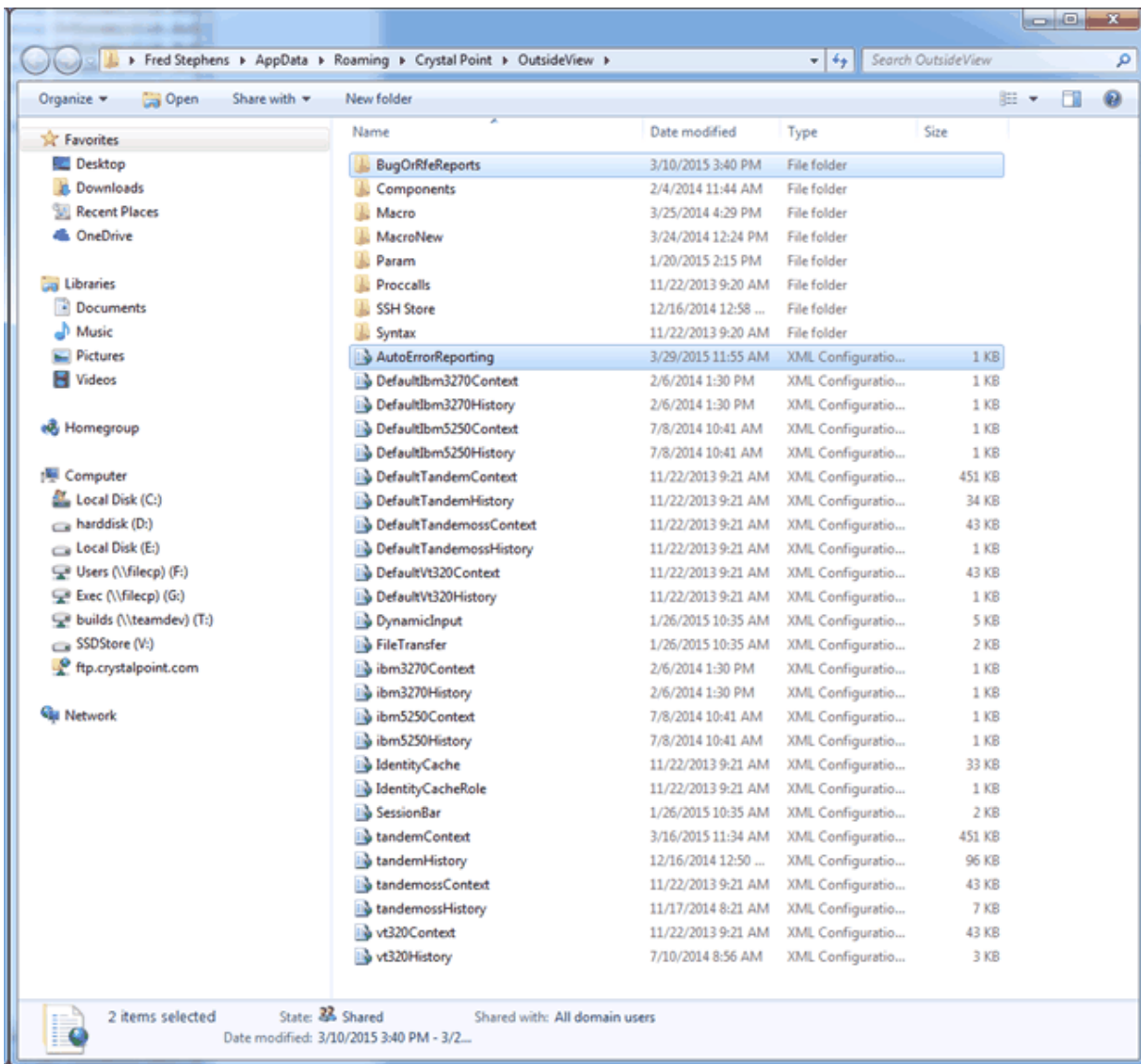
At the bottom right of the form, there are two buttons: 'Next >' and 'Cancel'.

At this point the data collection process is finished.

Since OutsideView may be unstable we do not attempt to send the report, but detect its presence the next time OutsideView is started and as the first task offer to send it at which time we run another wizard for the submission process.

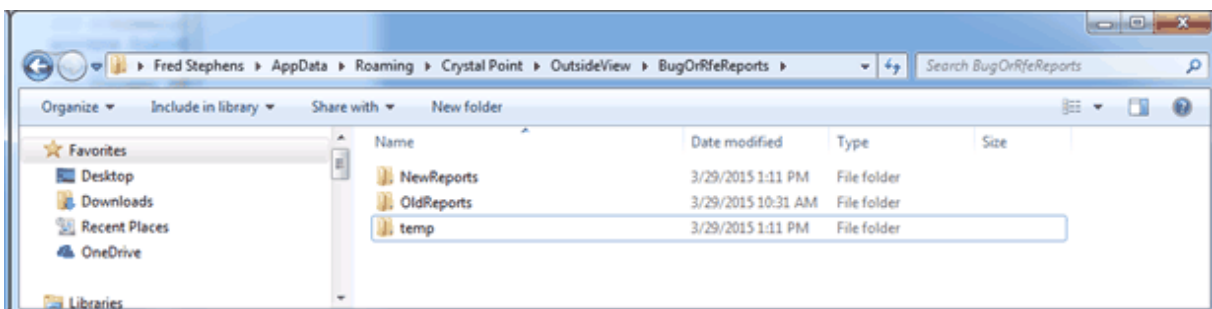


Under the configuration data folder we have the new configuration file `AutoErrorReporting` and a new directory `BugOrRfeReports` which is used by the error reporting logic.

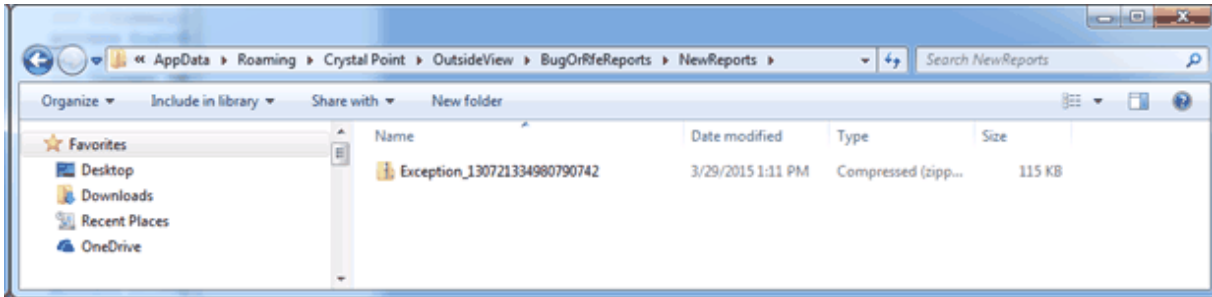


The top level folder has three sub folders for new reports, old reports and temporary files. Note the temporary files directory is cleared after each report is created.

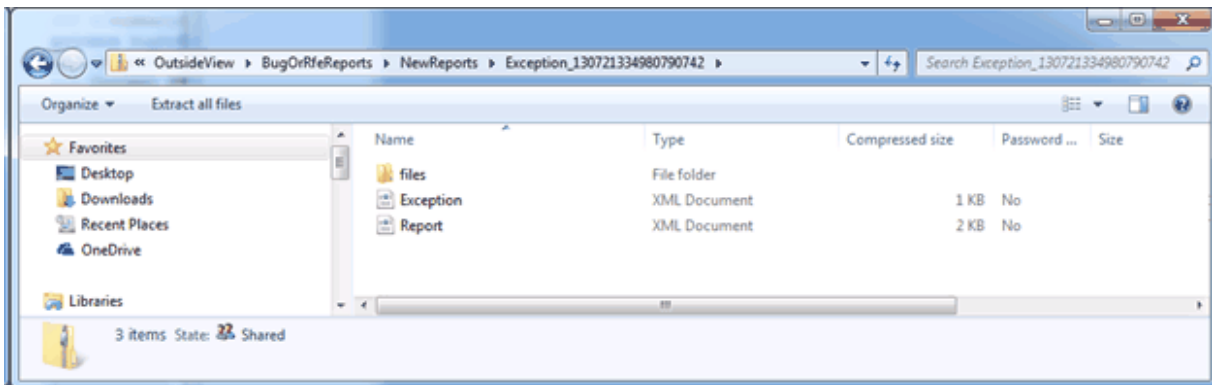
After a report has been emailed it is moved to the old reports directory:



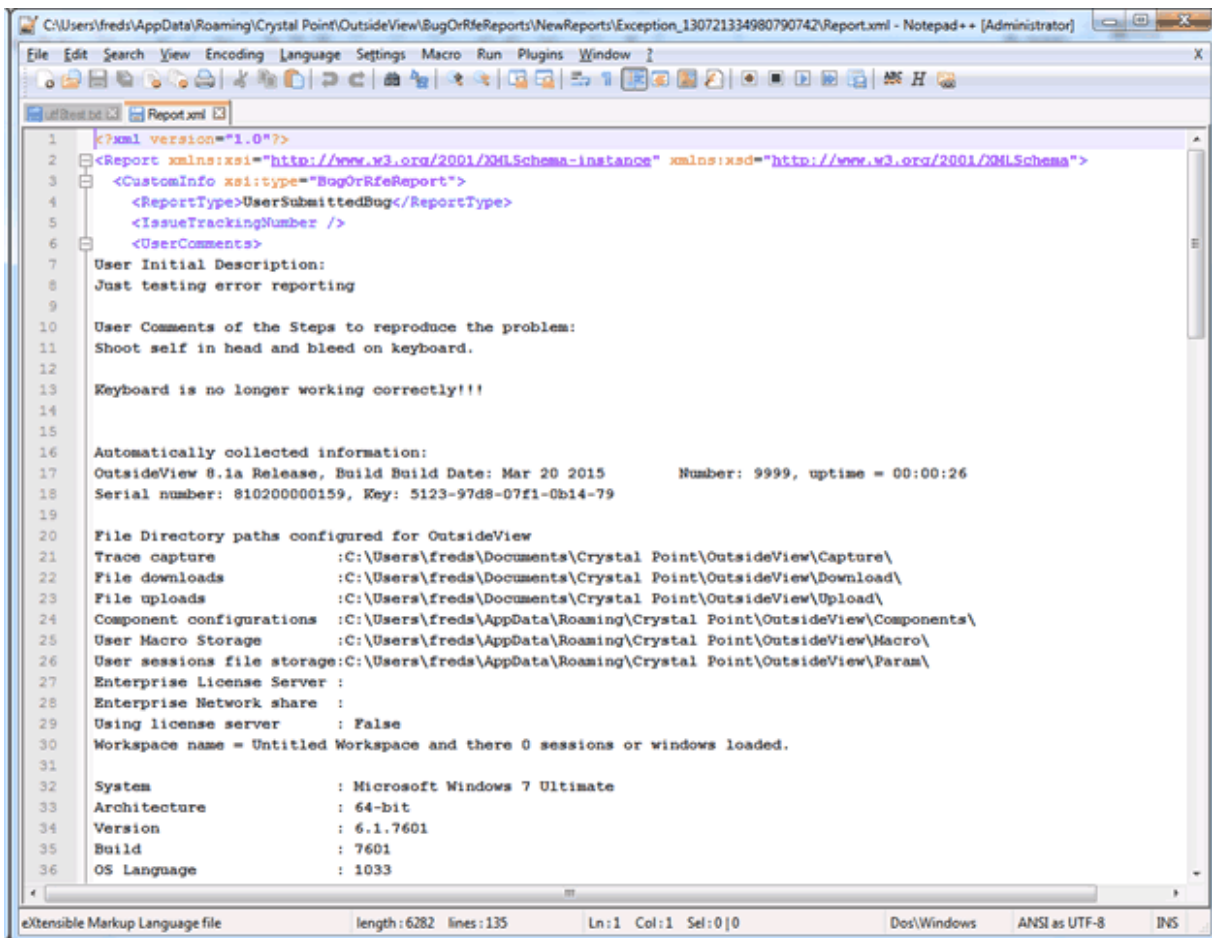
Each report is a zip file that is created with unique ID that is generated from a time stamp:



The meat of the report which is a zip file that we rename and send as a “Z” file type. The first two XML files are the .NET Exception and the Report file:



The report file is in XML formation and includes the information collected from the user:

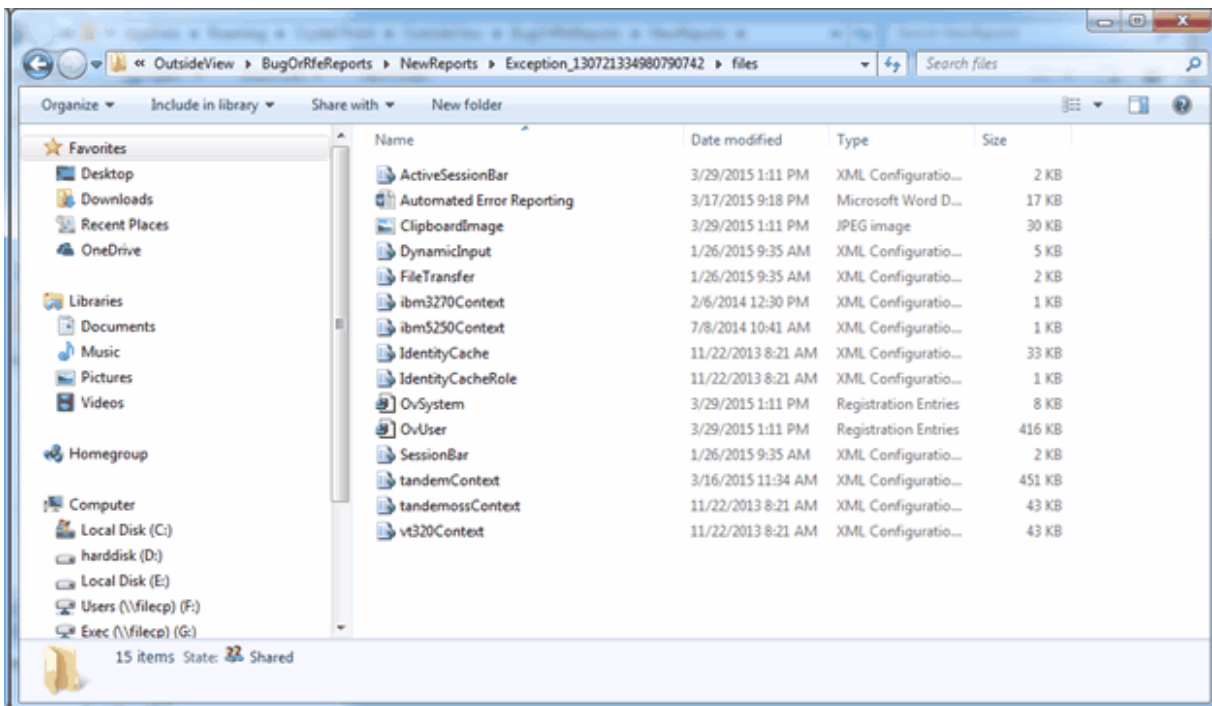


```
1 <?xml version="1.0"?>
2 <Report xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
3   <CustomInfo xsi:type="BugOrRfeReport">
4     <ReportType>UserSubmittedBug</ReportType>
5     <IssueTrackingNumber />
6     <UserComments>
7       User Initial Description:
8       Just testing error reporting
9
10      User Comments of the Steps to reproduce the problem:
11      Shoot self in head and bleed on keyboard.
12
13      Keyboard is no longer working correctly!!!
14
15
16      Automatically collected information:
17      OutsideView 8.1a Release, Build Build Date: Mar 20 2015          Number: 9999, uptime = 00:00:26
18      Serial number: 810200000159, Key: 5123-97d8-07f1-0b14-79
19
20      File Directory paths configured for OutsideView
21      Trace capture           :C:\Users\freds\Documents\Crystal Point\OutsideView\Capture\
22      File downloads         :C:\Users\freds\Documents\Crystal Point\OutsideView\Download\
23      File uploads           :C:\Users\freds\Documents\Crystal Point\OutsideView\Upload\
24      Component configurations :C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Components\
25      User Macro Storage      :C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Macro\
26      User sessions file storage:C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Param\
27      Enterprise License Server :
28      Enterprise Network share :
29      Using license server    : False
30      Workspace name = Untitled Workspace and there 0 sessions or windows loaded.
31
32      System                  : Microsoft Windows 7 Ultimate
33      Architecture            : 64-bit
34      Version                  : 6.1.7601
35      Build                    : 7601
36      OS Language              : 1033

```

Under the files sub directory is all the attached files that were included in the report.

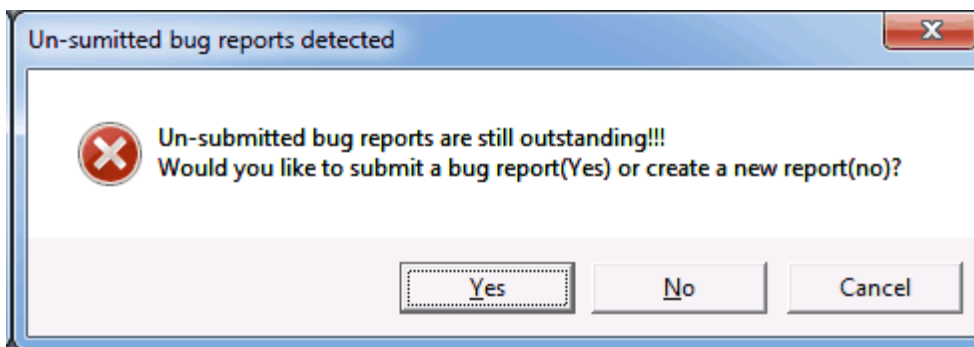
In this case you see an additional file named "ActiveSessionBar" which is the current setting the session bar is working with and which may have come from the workspace not the configuration data folder "SessionBar" configuration values.



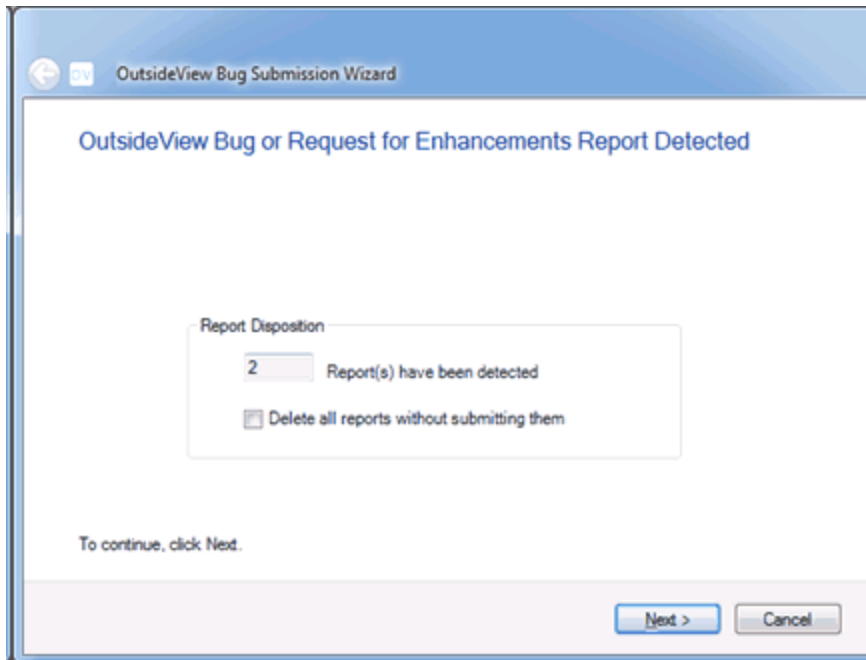
## 6.22.2 Report submission Process

When OutsideView starts up it checks the new bug reports directory to see if there are any reports active, if so it starts the reporting wizard which the user can cancel out of.

If the user starts manual report and there are previous reports that haven't been submitted they get the following dialog:

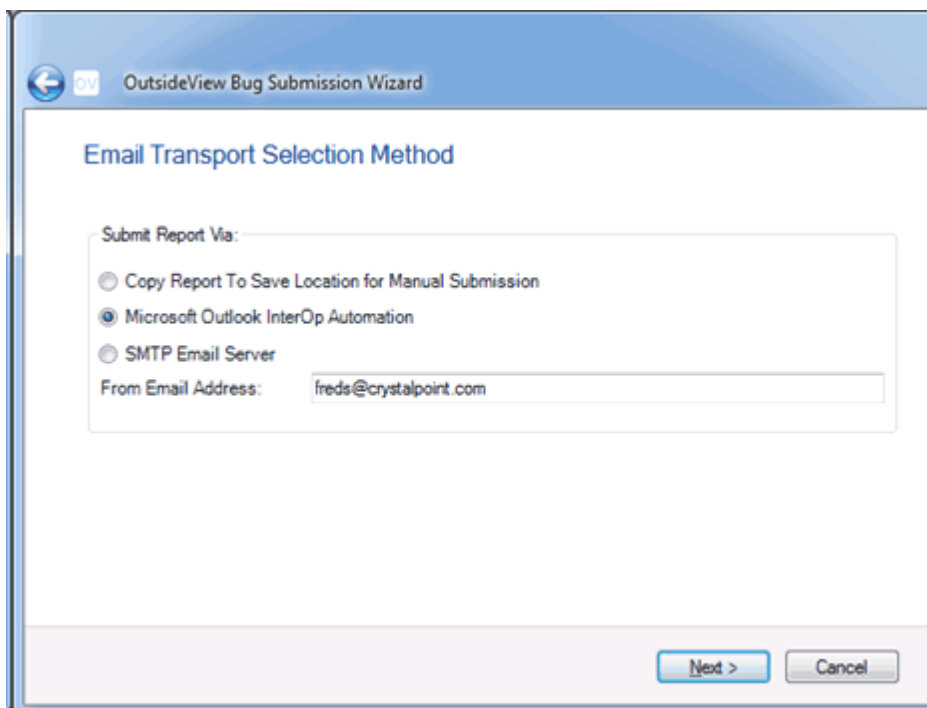


Clicking "Yes" takes them to the submission wizard and "No" lets them create a new report.



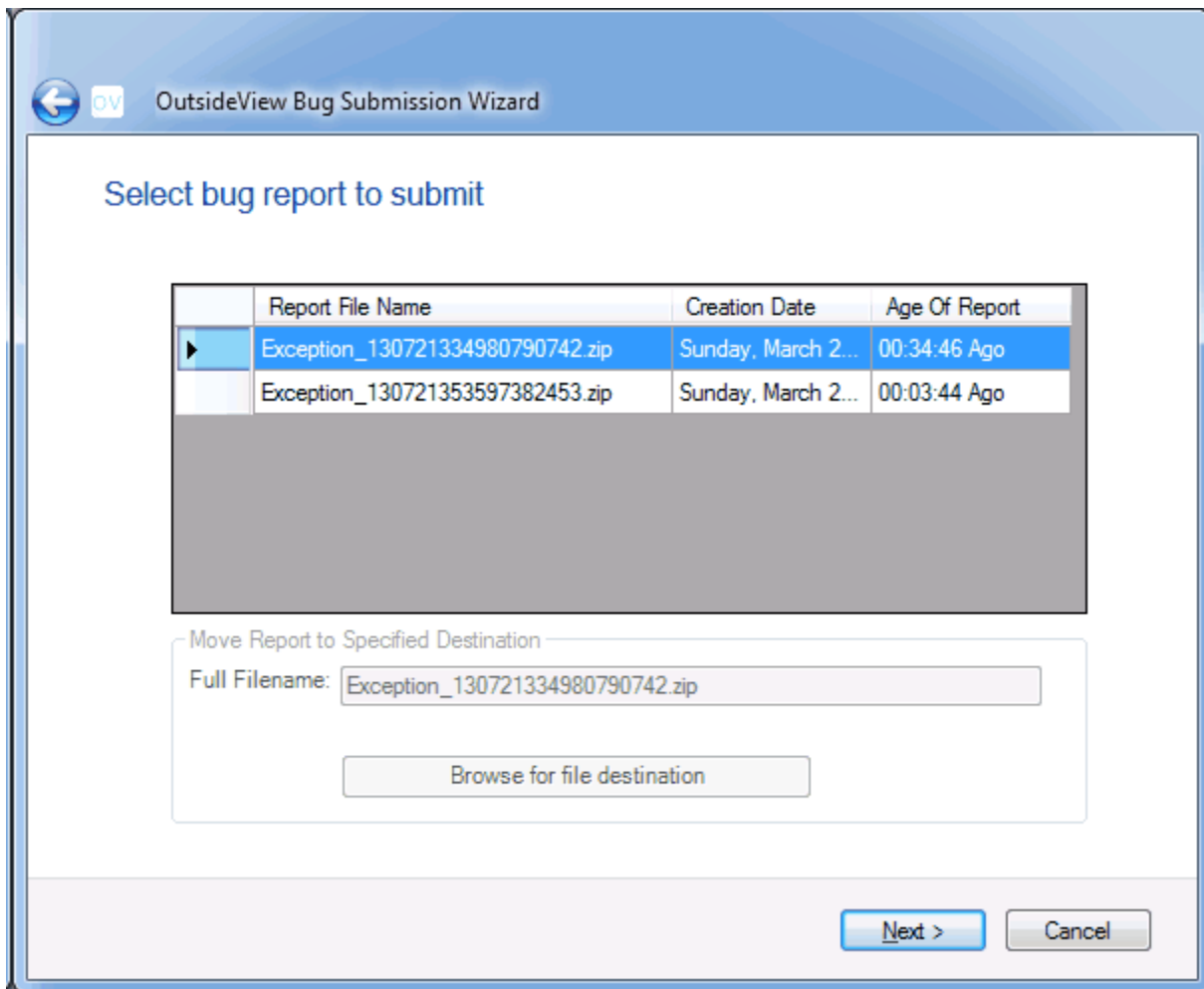
This wizard starts out by telling users how many reports are outstanding and gives them the option to simply delete them.

They then have a number of option on how to send the report:

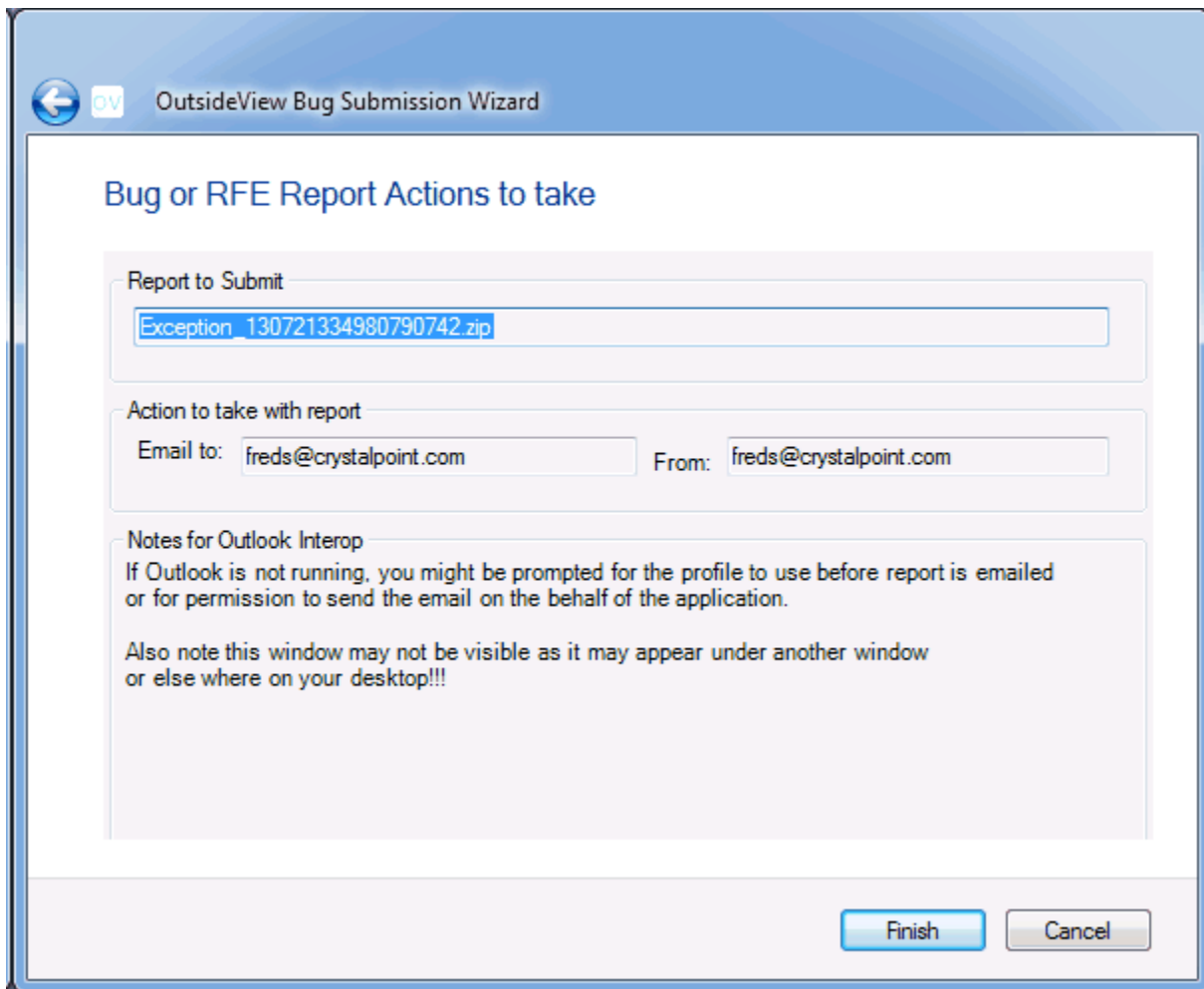


If multiple reports are present or they have elected to copy the report elsewhere this panel will appear. In the case of sending by email and only one report is available it will be skipped.





The finish panel then tells them what actions are going to take place and in the case of Outlook warn them of actions that might not make immediate sense like the following message:



The screenshot shows a dialog box titled "OutsideView Bug Submission Wizard". The main heading is "Bug or RFE Report Actions to take". There are three sections:

- Report to Submit:** A text box containing "Exception\_130721334980790742.zip".
- Action to take with report:** Two text boxes. "Email to:" contains "freds@crystalpoint.com" and "From:" contains "freds@crystalpoint.com".
- Notes for Outlook Interop:** A text area containing the following text:  
If Outlook is not running, you might be prompted for the profile to use before report is emailed or for permission to send the email on the behalf of the application.  
  
Also note this window may not be visible as it may appear under another window or else where on your desktop!!!

At the bottom right, there are two buttons: "Finish" and "Cancel".

The report subject is:

[Support Request] UserSubmittedBug "Just testing error reporting", report  
Exception\_130721334980790742

The email is sent with the following body of text:

Attached zip file renamed to Z type is a bug report for OutsideView , Build  
From [freds@crystalpoint.com](mailto:freds@crystalpoint.com), report was created on Sunday, March 29, 2015  
Submitted by:  
Fred Stephens CTO  
Crystal Point, Inc  
19515 North Creek Pwky #306  
Bothell, WA, 98012  
USA  
425-806-1128

User Initial Description:  
Just testing error reporting

User Comments of the Steps to reproduce the problem:  
Shoot self in head and bleed on keyboard.

Keyboard is no longer working correctly!!!

Automatically collected information:

OutsideView 8.1a Release, Build Build Date: Mar 20 2015      Number: 9999, uptime = 00:00:26  
Serial number: 810200000159, Key: 5123-97d8-07f1-0b14-79

File Directory paths configured for OutsideView

Trace capture            :C:\Users\freds\Documents\Crystal Point\OutsideView\Capture\  
File downloads         :C:\Users\freds\Documents\Crystal Point\OutsideView\Download\  
File uploads            :C:\Users\freds\Documents\Crystal Point\OutsideView\Upload\  
Component configurations :C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Components\  
User Macro Storage     :C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Macro\  
User sessions file storage:C:\Users\freds\AppData\Roaming\Crystal Point\OutsideView\Param\  
Enterprise License Server :  
Enterprise Network share :  
Using license server    : False  
Workspace name = Untitled Workspace and there 0 sessions or windows loaded.

System                 : Microsoft Windows 7 Ultimate  
Architecture          : 64-bit  
Version                : 6.1.7601  
Build                  : 7601  
OS Language           : 1033  
Service Pack          : 1.0  
Total Virtual Memory   : 47326.46 MB  
Free Virtual Memory    : 37986.32 MB  
Free Physical Memory   : 7620.64 MB

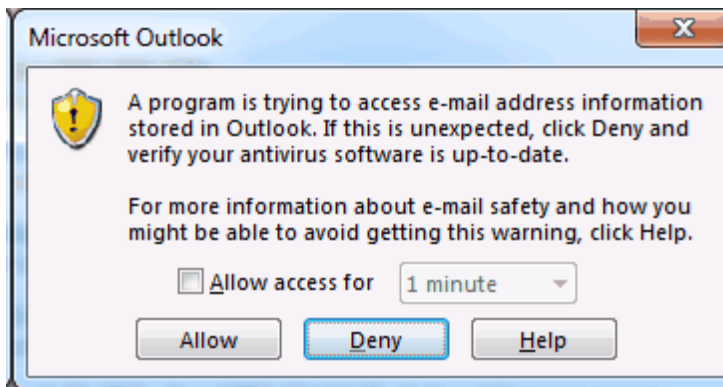
Processor              : Intel(R) Core(TM) i7-4510U CPU @ 2.00GHz  
Number of Cores        : 2  
Processor Load Percentage : 37

Name                 : C:

File System : NTFS

Size                 : 228933.00 MB

Free Space : 79662.27 MB



### 6.22.3 Optional Directory Settings

It is envisioned that some customers might not want the reports to go directly to Crystal Point, but to their own help desk for internal tracking.

If so they can create a group policy to set the email destination.

The following registry settings are honored by OutsideView and automatically overwrite any values the user has previously entered.

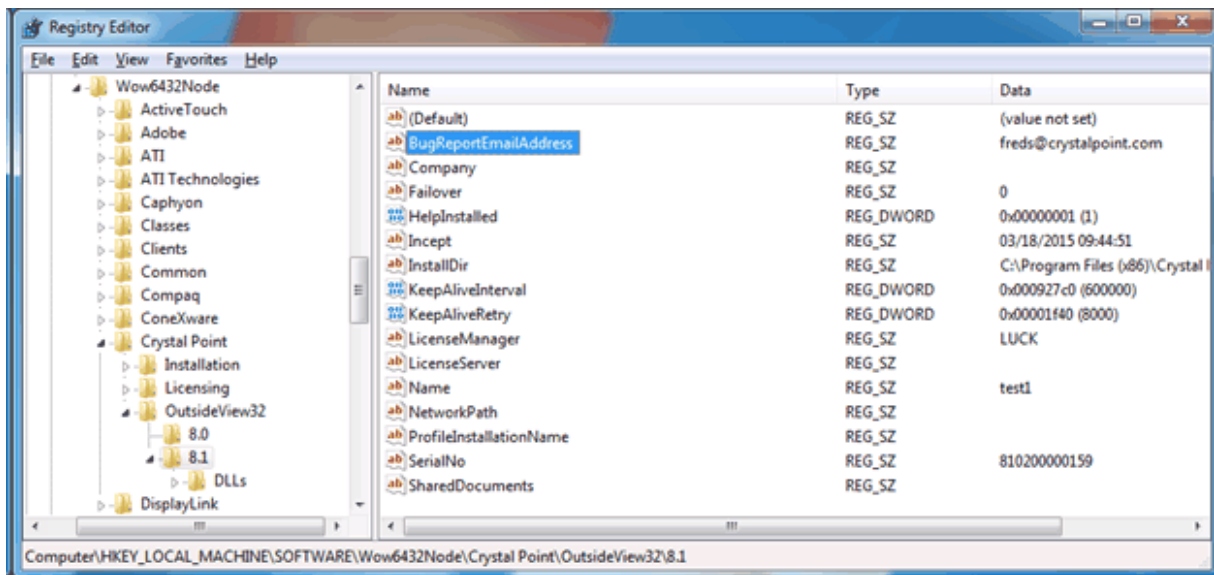
```

        TestRegistryKey("BugReportEmailAddress", ref
m_BugReportEmailAddress);
        if (string.IsNullOrEmpty(BugReportEmailAddress))
        {
            BugReportEmailAddress = "support@crystalpoint.com";
        }
        TestRegistryKey("EmailViaOutlook", ref m_EmailViaOutlook);
        TestRegistryKey("SMTPserver", ref m_SMTTPserver);
        TestRegistryKey("SMTPport", ref m_SMTTPport);
        TestRegistryKey("SMTPLogin", ref m_SMTPLLogin);
        TestRegistryKey("SMTPPassword", ref m_SMTPPassword);
        TestRegistryKey("SMTPuseSSL", ref m_SMTPUseSSL);

```

It first checks the OutsideView user registry and then the machine registry for these values.

In this example we set the value "BugReportEmailAddress" to a personal email to not litter the support email inbox during testing.



## 6.22.4 MFC Support

The MFC side should detect the error and write the mini dump and other files to error reporting temporary directory.

It then can call the following function from in mainfrm.cpp see

```
CMainFrame::OnReportBugOrRequestForEnhancement ()
m_wndThumbnailBar.ReportBugOrRequestForEnhancement (false);
```

A value of false means the report was not started by a user. At which time the wizard will lead the user though providing more information and creating the report zip file. It will also request that the application be terminated.

## 7 Troubleshooting

### 7.1 OutsideView File Locations

File Locations:

On each workstation, the OutsideView Application code is installed to the location specified to the Install Wizard. By default, that location is

C:\Program Files\Crystal Point\OutsideView

Each user is provided a separate file location\* for their individual configuration files. This permits users to share a workstation without having to share their OutsideView 'set up'. Typically, these configuration files are located at:

Windows 11, Windows 10 C:\Users\[User\_Name]\AppData\Roaming\Crystal Point\OutsideView

To quickly and easily access this are, users may select View, Configuration Data Folder. (This view is disabled for Citrix and Windows Terminal Server clients.)

Files considered text or text-like in nature, such as Upload, Download, or Capture files are stored, in accordance with Microsoft standards, under My Documents;

Windows 11, Windows10 C:\Users\[User\_Name]\Documents\Crystal Point\OutsideView

\*There is an option, when installing via Enterprise mode, to have all configuration files stored in common for all users of a given workstation. In that case, the configuration files are located at: C:\Users\All Users\AppData\Roaming\Crystal Point\OutsideView

## 7.2 UTF-8 Support

### Potential problems using UTF-8 with a NonStop system

UTF-8 is a variable length encoding system which generally has implications when used with Asian character sets.

Previously internationalization had a one to one correspondence between the data stream and the text display width on the screen. Depending on nomenclature; normal or half width characters used one byte of terminal screen data to cause one screen character of screen text to be displayed/occupied. Full width or DBCS (double byte character sets) characters would use two bytes of terminal stream data and occupy two screen positions.

Under UTF-8 encoding depending on the displayed character the host data stream could use between three to six bytes of terminal screen data depending on the position of the displayed character/glyph inside of the Unicode encoding space.

This presents a problem for Legacy applications which were written with the assumption that a 40 position input field on the emulation screen can be stored/represented with 40 bytes of memory or disk storage. Where it might range from 50 to 300 percent more data to represent the users input.

OutsideView has a legacy application mode insures that user is unable to enter more text in to an input field than can be stored by the legacy application. In most cases for this mode the user will have visual empty space at the end of a field when the limit is reached. The emulator prevents them from entering any more text into the field when this limit is reached. They receive a warning message that the field limits has been reached because of UTF-8 encoding.

Note for the TEDIT application. The Legacy Application Support setting is automatically enabled even if it has been turned off by a previous application or the user.

### UTF-8 Operational Notes

While it is desired that an environment have uniform character set encoding, it might take an organization some time to reach that standard. It is recommended that separate OV sessions be used for the differing applications.

One operational pattern might be to configure OutsideView for the traditional country value and DBCS so it can be used with existing applications with UTF-8 support turned off. All new UTF-8 applications

can then be coded to detect UTF-8 support in OutsideView and automatically change the 6530 terminal configuration to support it for the duration of the applications lifetime.

**Emulation Escape Sequence Changes**

The Read Terminal Configuration (Esc ?) and Set Terminal Configuration (Esc v) commands have a new configuration values to support UTF-8 interactions

UTF-8 Values

Set or Configuration Reply	UTF-8 Support Enabled	Legacy Application Support Enabled
u00	no	no
u01	yes	no
u02	no	no
u03	yes	yes

On issuing a Read terminal Configuration (Esc ?) if the response contains a configuration value that starts with the lower case letter 'u' than the emulator support the UTF-8 data stream.

If the desired UTF-8 mode is not enabled then the Set Terminal Configuration (Esc v) can be issued to the emulator to set the desired mode.

It is suggested that the initial state of this configuration be stored on application startup and restored on application shutdown.

**7.3 Recovering Unavailable Components**

**Recovering Unavailable Components**

Reopening a session is usually simple: go to File: Open Session and select the session to reopen. If one or more session components - such color scheme or key map - are unavailable, however, you will see warning messages when you reopen the saved file.

Components are unavailable if:

- They have been deleted from the network
- They have been moved to a different location
- The network itself has gone down

**Recovering Unavailable Color Schemes and Key Maps**

OutsideView will prompt you for a decision if the color scheme or Key Map files specified within the session are unavailable.

"One or more schemes (or Key Maps) associated with this session are missing. Do you wish to restore the missing scheme/Key Map? Yes/No"

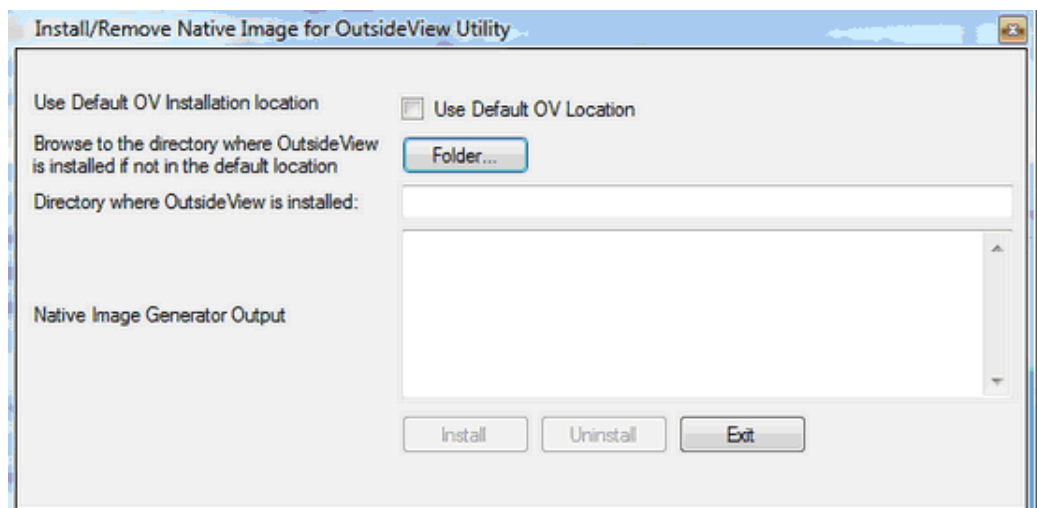
- If you answer "Yes," OutsideView will attempt to restore the missing scheme from the cache within the session file.
- If you answer "No," OutsideView will replace the missing scheme or Key Map with the default settings.

Each time this session is loaded, the whole process of trying to use the scheme specified in the session will begin again until the specified scheme becomes available or the scheme is reset to the defaults.

## 7.4 Pre-Compilation of .Net components

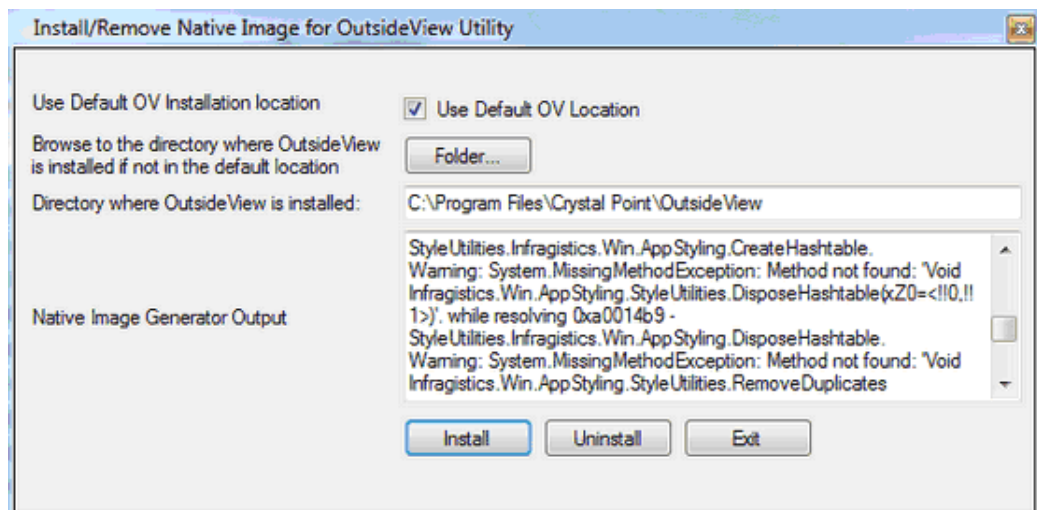
OutsideView makes extensive use of .Net technology. It is typical when using .Net components that they are compiled upon installation by the Microsoft Installer package. However, the last three releases of Microsoft installer have had defects in this area that prevent correct compilation of newly installed .Net components. Therefore, a .Net Just-In-Time (JIT) compiler must run upon each 'first use since reboot' of a .Net component, to create native (machine specific) executable code. The significance of this is that Users may experience a delay depending on the computer, each time OutsideView is started following a reboot or power off. This delay may be avoided by compiling the .Net components on your specific PC into Native code. To do that:

- 1) Navigate to the OutsideView installation media's Utilities folder
- 2) Double-click to execute the file InstallOVNativeImage



A) Click to accept the default installation location(C:\Program Files\Cystal Point\OutsideView) or browse to your OutsideView installation location

B) Click Install to create the native code





NOTE 1: When uninstalling OutsideView, these files will need to be **manually** uninstalled, as they are necessarily created after the Installer process completes

NOTE 2: Each time a new version of OutsideView is installed, the .Net components will need to be re-compiled.

## 7.5 Diagnostic Traces

### Diagnostic Traces

A diagnostic trace file may be requested by Crystal Point Technical Support to resolve an issue that goes beyond basic troubleshooting. The trace file will contain all telnet traffic between your host and OutsideView for the duration that tracing is active.

If the trace file by the same name already exists, OutsideView will ask for confirmation before replacing the existing file. If the answer is Yes, a fresh password is requested, and the saved file is overwritten. If the answer is No, the trace process is canceled.

If any other errors occur opening a trace file, or opening and writing to a save file, then an error message displays describing the error, and the trace file setting will be turned off automatically.

#### To Create a Trace File

1. If there is no active session, either open a previous session or initiate a new session. Bring the session that you will run the trace on into focus.
2. Click the Session Settings button on the toolbar, or select Session: Session Settings from the menu.
3. Click the Capture link on the Category list.
4. In the Diagnostic Trace group box, click the To File checkbox. This will enable the Trace function.
5. Specify a file name. Trace information will be saved in this file. You can also click the Browse button to navigate to a different drive or directory
6. Click the OK button.
7. OutsideView will prompt for a password (must be at least 6 characters) :



8. Upon filling in the password information and clicking OK, OutsideView will close this dialog box and begin the diagnostic trace.
8. Starting from a command prompt (e.g., a TACL prompt) perform the steps required to duplicate the error.
9. To terminate tracing, open the Capture dialog box once again (by following steps 2 and 3) and uncheck the To File checkbox in the Diagnostic Trace group box. This will close the trace file. The trace file will be located in the Capture folder (the default) or the folder set in step 5.

Once you have created a trace file, you can email it – and the password used when creating it - to our Technical Support staff (support@crystalpoint.com) as an attachment.

## 7.6 Extended Diagnostics for Auto Login

**Log Extended Diagnostic messages for auto login process** This is a Crystal Point internal debugging switch, found on the Applications Settings, Auto Login screen. Only activate if directed by Crystal Point Technical Support.

## 7.7 Additonal Tracing Capabilities

Crystal Point engineering has the ability to provide custom product builds, with specific, custom, and highly detailed tracing imbedded. If your issue requires this level of investigation, rest assured it is available.

## 7.8 Contacting Support

### Contacting Support

Help us help you. Crystal Point is committed to supporting all users running the current version of OutsideView who are within 90 days of their purchase of the product or who have purchased STAR support. We strive to maintain a turnaround of one business day for help requests.

In order to maintain this high level of quality support, we ask that you help us by:

- Trying to find the solution in the online help.
- Checking the OutsideView [error](#) or [session logs](#). These logs may have information that help identify where your problem is occurring.
- Checking our online Technical Support site. In addition to various publicly available resources, we also have a searchable AnswerBook online available to those with STAR support.
- Asking your System Administrator or Help Desk. Administrators are likely to be familiar with your particular question or problem – they're your best source for immediate answers or solutions.
- If none of the above steps work, you or your Administrator can contact Crystal Point. Our Technical Support staff may ask you to create a trace file; for directions, you can read the section on creating a trace file.

For your convenience, there are several methods for contacting Technical Support. Voice services are available from 7:00 AM to 5:00 PM Pacific time, Monday through Friday (except holidays). You can also access our electronic services, including the AnswerBook, on our website at [www.crystalpoint.com](http://www.crystalpoint.com) 24 hours a day, seven days a week.

Crystal Point, Inc.  
15833 Mill Creek Blvd.  
#12247  
Mill Creek, WA 98082 USA

Email: [support@crystalpoint.com](mailto:support@crystalpoint.com)  
Tech Support (Toll free): (800) 982-0881  
Tech Support (Direct): (425) 806-1119  
Main Phone: (425) 487-3656  
Fax: (425) 487-2880

# Index

## - . -

.Net API 6  
.Net JIT compiler 212

## - 1 -

132 column mode 40

## - 8 -

80 or 132 column mode 40

## - A -

Active mode 154  
active workspace 25  
Add or Remove Buttons 55  
Adding user-generated key file to NonStop hosts 103  
Allow User override of errors 109  
Ambiguous characters 7  
Application Data Folder 34, 209  
application log 125  
Application Look 9  
Application Message Log 125  
Asian 7  
Asian Usage Notes 7  
authentication 111  
Auto Connect tab 18  
Auto Login tab 17

## - B -

Block Mode Logon 77

## - C -

capture extended diagnostic trace 95  
Capture Tab 47  
Certificate Tools tab 93  
Certificate Validation 111

Certifying Authority 109  
Change Product License 7  
Changing Icon images 55  
Character Set Support 129  
China 7  
Chinese 7, 40  
cipher suite 111  
Clone Session 35  
cloud 106  
cloud computing 106  
Colors Tab 45  
Command Line Options 131  
compiling the .Net components 212  
Configuring HTML Tunnel 186  
Configuring Individual Workspace behavior 21  
Connection Types 95  
Contacting Support 214  
Context recognition 11, 70  
Context-Sensitive Toolbars 6  
convert an SSH key to SSH2 107  
Converting Evaluation licenses 7  
Copy to Clipboard 126  
Copy to Printer 126  
Copy/Paste 128  
Create New Context 70  
create new contexts 71  
Creating an SFTP file 148  
Creating Custom Toolbars 53  
Creating New Sessions 35  
creating public key certificates 148  
Custom toolbar 53  
Customize dialog 55  
Customizing Toolbars 53

## - D -

DBCS 129  
Desktop installation 8  
Diagnostic Traces 213  
Directories tab 10  
Display Tab 43  
docking 141  
Double-wide 7  
download 168  
download and edit 161  
download as 168  
Download-and-Edit 161, 168  
Dynamic Fonts 18

Dynamic Input Assistance 16  
 Dynamic Input Assistance - Main Settings 62  
 Dynamic Input Assistance - Cmd History 64  
 Dynamic Input Assistance - Main Settings 62  
 Dynamic Input Assistance - Spell Checking 67  
 Dynamic Input Assistance- Command Auto-completion Assistance 70  
 Dynamic Input Assistance Overview 60  
 Dynamic Lines 18, 43  
 Dynamic Toolbar 75  
 dynamic toolbar labels 72  
 Dynamic Windows 125  
 dynamically labeled function key toolbars 70

## - E -

Edit Context List 64  
 Editing Context List 73  
 Editor 169  
 Emulation Tab 40  
 Encryption 111  
 Enhanced Failover Abilities 6  
 extended diagnostic trace 95

## - F -

failover 6, 125  
 File Attributes During Transfer 163  
 File Transfer Defaults 147  
 File Transfer Progress Monitor 172  
 File Transfer tab 11  
 File Transfer:FTP 178, 179, 181  
 File Transfer:IXF 183, 184  
 Filtering Application Log 125  
 Find 128  
 Find Next 128  
 Find/Find Next 126  
 fixed pitch 43  
 fixed pitch font 43  
 Fonts:National Character Sets 129  
 Fonts:Session Font 43  
 FTP 142  
 FTP Command Mode 178  
 FTP Dialog Interface 179

## - G -

Graphical Navigation 132  
 Guardian mode 161  
 Guardian OS 142

## - H -

Hide warning messages 109  
 host-initiated IXF 40  
 Host-to-Host File Transfers 6  
 hover 13  
 Hover Time Period 13  
 HTML Tunnel 185, 186

## - I -

IBM 77  
 IBM TSO 77  
 icon image editor 55  
 Icon images 55  
 Icons 53  
 ID Management 185  
 ID Management and SSH 93  
 Identity 38  
 Identity Caching 6, 38  
 Identity Management 77  
 Imbedded Editor 169  
 Importing Root CA Certificates 113  
 Individual Workspace behavior 25  
 Individual Workspace Settings 25  
 in-progress file transfers 170  
 InstallOVNativeImage 212  
 Invoking "Classic" FTP 173  
 IO Tab 42  
 ipv6 95, 125  
 IXF Receive 183  
 IXF Send 184  
 IXF Transmit 184

## - J -

Japan 7  
 Japanese 7, 40  
 Japanese Usage Notes 7

## - K -

keepalive 95  
Keep-Alive 95  
Kerberos 95  
Kerberos/GSS-API 95  
key 106, 107  
Keyboard Input with Function Keys 75  
Keyboard Interactive 93, 95  
Keyboard Map Tab 46  
Keyboard Mapping 49  
Keyboard:Maps 46, 49  
Keyboard:Running Key Sequences 50  
Keyboard:Running Macros 51  
Keyboard:Send Terminal Function 50  
Korea 7  
Korean 7, 40

## - L -

Legacy Block 40  
legacy block mode 40  
log file name conflicts 130  
Log Incoming 130  
Log to File 130  
Log to Printer 130  
Log, Application 125  
Log, filtering 125  
Logging Session Activity 130  
Logging to Network Locations 130  
Logon Credentials 93, 148

## - M -

Macro Editor 188  
Macro Status 189  
Macro Toolbar 48, 58  
Macros:Editor 188  
Macros:Running 188  
Macros:Toolbars 58  
Mapping Key Sequences 50  
Mapping Macros 51  
Mapping Terminal Functions 50  
message authentication code 111  
modify an icon image 55  
mouse roller wheel 10

Multi Host Uploads 6  
Multi-Hop SSH Tunneling 6  
multilan 42  
Multiple Formatted Block Mode Logon Screens 77  
Multiple Formatted Screen Login 77  
Multiple Host file transfers 171  
Multiple Host Uploads 6  
Multiple SSH Hops 148  
Multiple SSH Tunneling hops 93

## - N -

National Character Set Support 129  
Net JIT Compiler 212  
New Session Defaults tab 18  
non-passive 154

## - O -

OCSP 111  
On Session Load 18  
Operating System 142  
OSS mode 161  
OutsideView Editor 169  
OutsideView File Locations 209  
OutsideView User Interface Overview 118

## - P -

Passive Mode 154  
passphrase 148  
password 148  
password protect 119  
Password/Passphrase 93  
performance tuning options 18  
Pre-Compilation of .Net components 212  
Print:Screen 128  
Print:Session Log 130  
Printing 128  
PRIVATE KEY 106, 107  
Protocol Tab 42  
pseudo-terminal 95  
pseudo-terminal connection 93  
Pseudo-terminal connections 95  
public key 95, 106, 107  
public key certificates 148  
public keys 103

**- Q -**

Quick Changes of your Dynamic Input Assistance Mode 61  
 Quick Start 8

**- R -**

raw printing 40  
 RAW view 161  
 recognize new contexts 71  
 Recovering Unavailable Color Schemes and Key Maps 211  
 Recovering Unavailable Components 211  
 Reset Toolbars 55  
 RFC 2434 111  
 RFC 5246 111  
 Right-Click Options 126  
 Role Management 38, 95, 185  
 Role Management and HTML Tunnel 185  
 Role Management and SSH 93  
 RSA 106, 107  
 Running Macros 188

**- S -**

Save Session As 126  
 Screen Visualizer 11  
 Secure Sockets Layer 111  
 Security 93, 109  
 Security Overview 93  
 Server Authentication 109  
 Session 31, 32, 119, 134, 140  
 Session Activation 31, 140  
 Session Activation Control 31, 140  
 Session and Workspace Overview 34  
 Session Bar 21, 26, 32, 134  
 Session Bar and ID Types 26, 134  
 Session Bar Color Coding 32, 134  
 Session Bar tab 13  
 Session Cloning 6  
 session password 119  
 Session Settings 36  
 session settings password 119  
 Session Tab 36  
 Session:Creating 35

Session:Settings 36, 40, 42, 43, 48  
 Setting File Attributes 163  
 Settings tab 10  
 SFTP 142  
 SFTP file transfer 148  
 SSH I/O tab 93  
 SSH key 107  
 SSH Security 93  
 SSH Tunneling 93  
 SSH2 key 107  
 ssh-keygen 107  
 SSL 111  
 SSL Authentication 109  
 SSL Server Authentication 109  
 SSL-secured file transfer 154  
 startup macro 24  
 Status Bar 33  
 Steps to add public keys to host 103  
 Support 214

**- T -**

tabbed group windows 121  
 Tabbed View 121  
 text search 128  
 Text Selection 126  
 thumbnail 13  
 TLS 111  
 TLS Cipher Suite Registry 111  
 Toggle Font 43  
 Toolbar 48  
 toolbar customization 55  
 Toolbar Icons 53  
 Toolbar Overview 51  
 Toolbar Tab 48  
 Toolbars 33, 51, 53, 58  
 Toolbars and Docking Windows 51  
 Trace 213  
 Transferring Files 181  
 Transport Layer Security 111  
 True Type fonts 43  
 Tunnel 185  
 Tunneled connections 93  
 tunneling connection 95  
 Tunneling Connections 95  
 tunneling SSH connection 93

## - U -

Unavailable Color Schemes and Key Maps 211  
Unavailable Components 211  
Universal Editor 6  
Unix/X11 mouse text selection 10  
Upload 163  
Upload As 163  
Upload to Multiple Hosts 163  
Upload with Attributes 163

## - V -

Validate Certificate 109  
Validate root CA fingerprint 109  
Version Compatibility 6  
View Macro Status 189  
View, Application Data Folder 209  
Visualize Screen 71  
Visualize Screen Layout 70, 71  
Visualizer 11  
VisualizeScreenLayout 72

## - W -

What's new 6  
when login data is available 18  
When session is selected 18  
Windows 7 6  
workspace startup macro 188  
Workspaces 24