



System Administrators Guide

© 2023 Crystal Point

Table of Contents

Foreword	0
Part I System Administrators Guide	5
1 What's New in OutsideView 9.1	5
2 System Requirements	6
3 Version Compatibility	6
4 Asian Usage Notes	6
Part II Installation and Maintenance	8
1 Desktop Installation	9
2 Corporate Licensing	10
3 SCCM (SMS) Installation Desktop	11
4 HTML Tunneling Servlet	12
5 Enterprise Installation	17
Enterprise Overview	17
Enterprise Failover (Disaster Recovery)	19
.NET Requirement	20
Create Network Shares	20
Enterprise Installation onto Share	21
Standard OutsideView Enterprise Installation	21
SQL OutsideView Enterprise Installation	26
Creating Multiple Profiles	36
Client Installation	37
SCCM (SMS) Installation Enterprise Client	38
WTS/Citrix Server Installation	39
Example Installation	41
6 License View Installation	42
Installing LicenseView	42
Connecting SQL LicenseView to SQL-based License Pools	44
7 Enterprise Updates and Upgrades	47
Maintenance updates	48
Feature Upgrades	49
Major Upgrades	50
Citrix \ Windows Terminal Server Updater Notes	51
8 Moving Enterprise Installations	51
Part III Enterprise Administration	54
1 User Profile Administration	54
Supervisor Mode	54
Override Mode	55
Override Application Settings	56
Directories tab	57
User Privileges	58
Detailed Control over User Privileges	62

Detailed User Privileges Control - Implementation notes	65
Additional User Privileges	68
Client Administration	69
Settings tab	71
New Session Defaults tab.....	72
Assigning Users to Profiles	73
Automating Users' Service Names	76
2 Licensing.....	77
Licensing Overview	77
License Administration	79
Traditional LicenseView.....	79
View License Status	79
Creating License Pools	80
Importing Licenses	80
Exporting Licenses	81
Releasing Licenses	82
Release All Licenses	83
Checking a License Out	83
Synchronize the License Pool.....	84
Make a license available offline.....	84
License Reports	85
License Alerts	85
PACK the License Pool	86
SQL LicenseView	87
Open	87
License Pool Properties	89
Print	91
Recent	91
Close and Exit	91
Find	92
Refresh	92
Checkout	92
Undo Checkout	93
Export License	93
Import License	95
Delete the Selected License.....	96
Options	97
Diagnostic Log	98
Help Topics	98
About LicenseView	98
Monitoring Multiple License Pool Databases.....	99
Make a License Available Offline for an Extended Period.....	99
Error Messages	101

Part IV Seamless Guardian/OSS support 103

1 Seamless Guardian/OSS support.....	103
2 Requirements.....	103
3 Background.....	104
4 Global OSS TERMCAP setup.....	105
5 Personal OSS TERMCAP setup.....	109
6 TERMINFO Support.....	110

7	Guardian File System Graphical Navigation.....	114
Part V Support		117
1	Contact Support.....	117
2	Pre-Compilation of .Net components.....	117
3	Diagnostic Tools.....	119
Index		120

1 System Administrators Guide

System Administrators Guide

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

System Administrators Guide

This guide is intended to help those responsible for **installation and administration** of OutsideView.

For assistance on **configuring and using** OutsideView, please refer to the OutsideView Users Guide.

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

For assistance with .Net interactions with OutsideView, please consult the .Net API Reference manual.

NonStop is a trademark of Hewlett-Packard Development Co.

1.1 What's New in OutsideView 9.1

What's New in OutsideView 9.1

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

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

1.2 System Requirements

System Requirements

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

System Requirements

Operating Systems:

Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022

.Net component 4.5 or higher

.Net component 3.5 SP1 for Macros

Hardware Requirements:

- TCP/IP
- 200 MB available disk space
- Optional Enterprise SQL Licensing requires Microsoft SQL Server 2012 to SQL Server 2022

1.3 Version Compatibility

Version Compatibility

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

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.

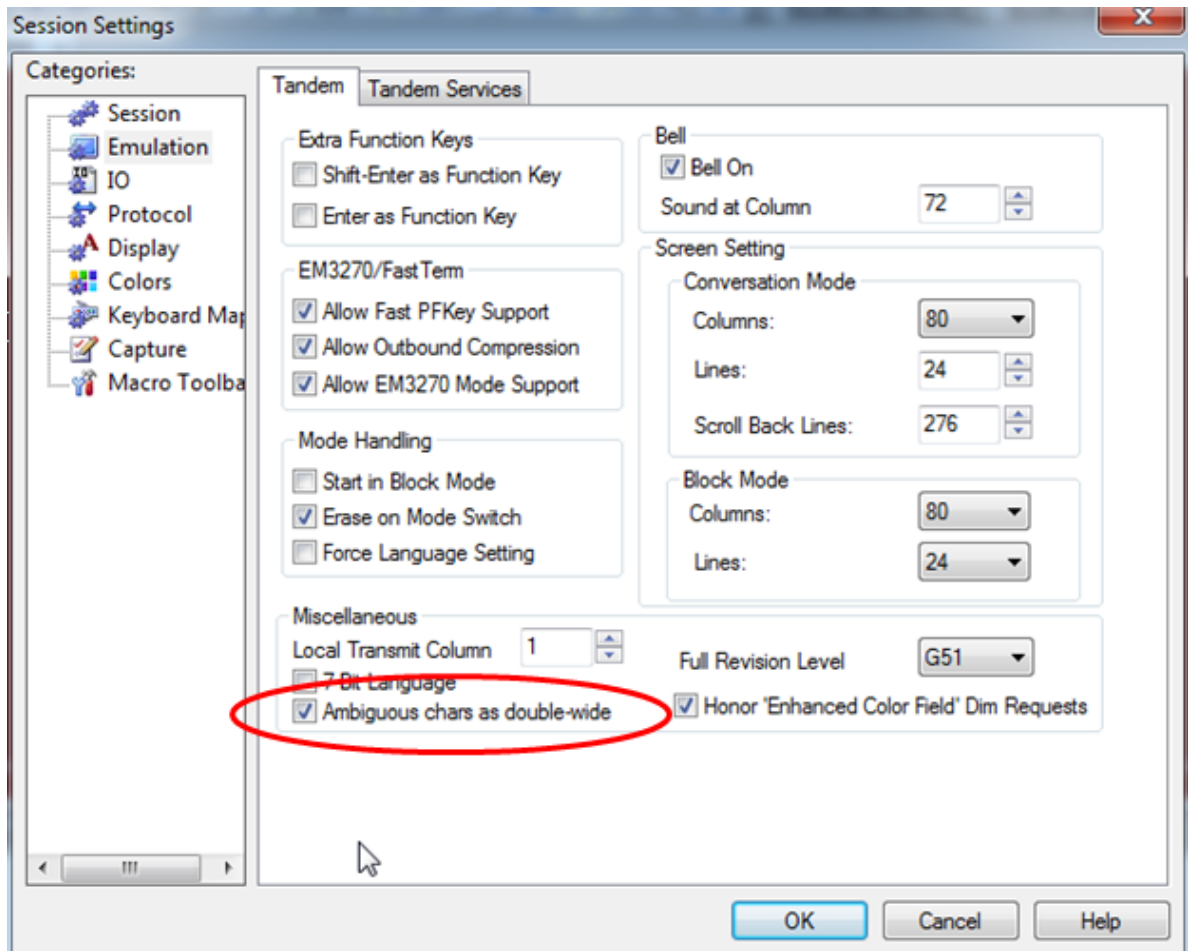
1.4 Asian Usage Notes

Asian Usage Notes

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

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"



2 Installation and Maintenance

Installation and Maintenance

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

Installation

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

Installation

Installation Overview

OutsideView installations have been updated to support true 64bit installs. The installations can detect your Operating System type and install the correct version of the OutsideView client onto your machine.

OutsideView may be installed in either Desktop or Enterprise mode. Desktop mode is installation per individual workstation, with control of the application entirely workstation-based.

Enterprise mode combines local installation and execution with centralized oversight and controls.

Enterprise Mode Overview

If you are deploying OutsideView to several networked computers, an Enterprise mode installation simplifies the initial deployment and your ongoing client administration. With an Enterprise installation, you will be able to:

- Reduce your administrative costs/effort by automatically installing and updating OutsideView Enterprise software across your organization from centralized network locations.
- Simplify user training and support by defining and administering user configurations and privileges from anywhere on the network.
- Maximize operational control over sensitive connectivity settings, while preserving user's ability to modify 'preference' settings.
- Monitor application usage and ensure license compliance with license administration tools (using WINS/NetBIOS).

For Enterprise installation instructions, click [here](#).

Enterprise Administration:

For instructions on administration of user configurations, click [here](#).

For instructions on license management, click [here](#).

Desktop Mode Overview

A Desktop mode installation is appropriate when installing to a few workstations or when centralized administration functions are not desired. Centralized administrative functions NOT available in desktop mode include central 'pools' of licenses, centrally maintained and automatic end-user distribution of software updates, connectivity parameters, user permissions, session settings, etc.

For Desktop installation instructions, click [here](#).

2.1 Desktop Installation

Desktop Installation

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

Desktop or Corporate Installation

Note: *If you are installing OutsideView onto several networked workstations, and want central oversight of user permissions and configurations, or want centralized, concurrent licensing 'pools', you should consider an [Enterprise](#) installation. If you are using OutsideView in either Windows Terminal Server, or Citrix environments, then OutsideView requires Enterprise concurrent licensing mode.*

The serial numbers used for typical Desktop installations are unique per each PC, to assist organizations in software inventory control.

To install OutsideView Desktop:

1. Use Add/Remove Programs from your Windows Control Panel to uninstall any prior versions of OutsideView
2. Navigate to the OutsideView folder of the OutsideView CD (or CD image on your disk).
3. Launch **OutsideViewSetup.exe**. Note that the OutsideViewSetup.exe will detect your Operating system type (32bit or 64bit) and install the corresponding OutsideView application onto your computer.
4. If the Installer detects a pre-existing version of OutsideView, it will offer to Repair or Remove the software. Select Remove. After that completes, start setup again.
5. Proceed by following the instructions on each screen. Once you have completed a screen, click Next to go to the next screen.
 - Make sure you read and accept the terms in the End-User License Agreement (EULA) by clicking "I accept the terms..."
 - The installation process will prompt you for a **Serial Number** and **License Key**. These numbers may be found on the CD packaging, or may have been mailed to you by Crystal Point
 - Serial numbers have 12 digits and look similar to '91000 00055 01'
 - Keys are in hexadecimal format (0 – 9 and a – f). If the characters "oh" or "el" appear to be present, they are actually either a zero (0) or a one (1). Keys appear similar to 'adb3-814c-07d7-0501-62'
 - You may modify the Destination folder if you wish.
 - Check 'Use shared directory for session configurations' checkbox if you want all users to share a single set of session configuration files instead of having, as per default, their own folders to store their own session files. Using a shared directory also disables multiple-profile support (only on Windows XP, Windows 2003 and better) **This option is NOT normally used when installing a single PC.**
6. After collecting all the necessary information, the Windows installer will install OutsideView.
7. When installation is complete, click "Finish".
8. Restarting your PC after installation is not usually required. If a restart is necessary, a notice will appear on your screen.

Notes on desktop file locations:

A default installation places the OutsideView application files under C:\Program Files\Crystal Point. Each OutsideView user on the PC will have an individual location automatically created

to contain their personal OutsideView configuration files and Edit files. For Vista, Windows 7 and newer systems, these configuration files are located at C:\Users\[User_Name]\AppData\Roaming\Crystal Point and C:\Users\[User_Name]\Documents\Crystal Point

NOTE: If the option to “Use shared directory for session configurations” is selected during installation, all OutsideView configuration files will be stored, in common, under C:\Users\All Users\ and on down.

Installation Issues

If the Installation package for whatever reason will not install OutsideView onto your machine then try the following steps as a work around:

1. Extract the packages from the OutsideViewSetup.exe file via the Dos Command:
OutsideViewSetup.exe /stage_only FILE="Extract_ALL"
2. You will see a dialog panel come up that says "Change Current Destination Folder". You can specify the directory where you want to extract the packages. Click on the Install button to extract the packages.
3. You will see the following packages extracted in the folder specified from step 2:
 - {1BEC2EE4-CD3E-4FDD-84A6-8855F4F8C55F}-- OutsideView 32bit Installer
 - {2C7DB961-C49F-491E-8D6C-AC92D3B163C0}-- OutsideView 64bit Installer
 - {47C4119B-3ADD-4803-B278-9ABA39415D83} -- VC_Runtime 32bit Installer
 - {D093EE4D-527D-4CC7-AB3C-DCE3219FA508}-- VC_Tuntime 64bit Installer
4. Install the following in this order:
 - a. VC_Runtime 32bit Installer (install on both 32 and 64bit OS)
 - b. VC_Runtime 64bit installer (If you are on a 64bit OS)
 - c. OutsideView 32bit (If you are on a 32bit OS)
 - d. OutsideView 64bit (If you are on a 64bit OS).

2.2 Corporate Licensing

Corporate Licensing

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

Corporate Licensing

*If you are installing multiple PCs, do **not** want centralized control over user permissions and configurations, but do want to use Push software such as SMS to distribute and update OutsideView, you should use a Corporate serial number. Contact Crystal Point Sales for*

these. A corporate license-based installation is identical to a desktop installation, with the exception that the same serial number and key can be used over and over.

2.3 SCCM (SMS) Installation Desktop

SCCM (SMS) Installation Desktop

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

OV Desktop Installation

The new OutsideViewSetup.exe installer contains both 32bit and 64bit OutsideView installations wrapped within. The installer has the capability to detect your operating system and install the correct version of OutsideView onto your machine. In the previous versions of OutsideView, users were required to extract the msi package from the installation but that is no longer required with the updated OutsideView Installation Setup.

SCCM Desktop installation requires the following 4 parameters:

1. SERIALNUM
2. SERIALKEY
3. SERIALKEY2
4. COMPANYNAME

The SERIALNUM and SERIALKEY is provided by Crystal Point via the License. Use your company name for the COMPANYNAME value. **Note that SERIALKEY2** is almost the same value as SERIALKEY except that it does not contain the last two digits. For example SERIALKEY is "17cb-2069-07f0-0404-96". Then SERIALKEY2 is "17cb-2069-07f0-0404-"

Desktop installation:

```
OutsideViewSetup.exe /silent SERIALKEY2="17cb-2069-07f0-0404-"  
COMPANYNAME="CrystalPoint" SERIALNUM="910100009008" SERIALKEY="17cb-2069-  
07f0-0404-96"
```

Installation Logging

If you run into installation issues, users can turn on the logging for the installations:

```
OutsideViewSetup.exe /debuglog /silent SERIALKEY2="17cb-2069-07f0-0404-"  
COMPANYNAME="CrystalPoint" SERIALNUM="910100009008" SERIALKEY="17cb-2069-  
07f0-0404-96" /log"/"
```

This will generate two separate log files in the same directory where you launched the OutsideViewSetup.exe application. The two log files are:

1. InstallShield.log
2. OVX64Compont.log or OVX86Component.log depending on your Operating System.

If you are under a Star Support Contract, collect these two log files and send them over to support@crystalpoint.com for further help regarding installation issues.

2.4 HTML Tunneling Servlet

HTML Tunneling Servlet

Contact sales@crystalpoint to purchase the license and to download the tunneling servlet application!

OutsideView has a companion product called HTML Tunneling Servlet. The Tunneling Servlet is used with the HTML Tunneling option from a OutsideView client to tunnel through a single intermediate host to reach the final host target.

The Tunneling Servlet requires the following environment to run:

- Java Development Kit 1.6 or higher (JDK1.6+)
- Web Application Container such as Apache Tomcat Application Server
- Computer that can access the final host target

There are 3 different versions of the tunneling servlet. They are:

- Tunnel
- Tunnelssl – wraps the data into SSL data stream
- Tunnelssh – wraps the data into SSH data stream

They each come packaged in their own WAR files. Installation of these WAR files are very straight forward. You will need to deploy them into your Web Application server. For example on the Tomcat Application server, all you need to do is copy and paste (tunnel.war, tunnelssl.war, or tunnelssh.war) file into the webapps folder in the Tomcat installation directory. These war files are standard Java Web Application war files and will work in various different Web Application Servers.

After you copy the WAR file into the deployment location and startup the Web Application server, you will notice that the contents of the WAR file is expanded out into a directory with the same name. For example you should see a folder name tunnel, tunnelssl, or tunnelssh.

You will now need to install the licensing file ([rqntun.reg](#)). You should have received the licensing file from CrystalPoint. You will need to place this file into the following location based on the tunneling servlet version:

- Tunnel – place the rqntun.reg file into the deployed folder location. For example on Tomcat: C:\Apache-tomcat-7.0.42\webapps\tunnel\WEB-INF\classes\at2custom\at2wsp
- Tunnelssl – place the rqntun.reg file into the deployed folder location. For example on Tomcat: C:\Apache-tomcat-7.0.42\webapps\tunnelssl\WEB-INF\classes\at2custom\at2wsp
- Tunnelssh – place the rqntun.reg file into the deployed folder location. For example on Tomcat: C:\Apache-tomcat-7.0.42\webapps\tunnelssh\WEB-INF\classes\at2custom\at2wsp

Configuring the Tunnel servlet

All three versions of the tunnel servlet have the same parameters that can be configured in the web.xml file. The web.xml file can be located in the deployed directory's WEB-INF folder. For example: C:\Apache-tomcat-7.0.42\webapps\tunnelssl\WEB-INF\ folder.

The configurable parameters for the tunneling servlets are:

- **profileDirectory** – this is a relative path to the at2wsp directory. It should be able to look this path up without any manual configurations. **Note on some platforms this relative pathing may not work**, we then suggest you manually set the absolute path to the at2wsp directory. This directory must contain the tunneling license (rqntun.reg).
- **debug** – Set to true to enable debugging. Generates tunnel log file in the profile directory listed in the parameter for profileDirectory. The value is defaulted to true. Please turn this value off when going into production mode.
- **sessionTimeout** – The amount of time (in seconds) tunneling servlet will wait for a response from the user before the session times-out.
- **userAuthentication** – User authentication on the Tunnel servlet. Set this value to true if you want to enable userid and password authentication on the tunneling servlet. The client credentials must match the values configured prior to gaining access to the servlet. Administrators will need to create profiles that contains the credential information for this to work. This default value is set to false.
- **host** – This parameter enables the administrator to hard code the target destination instead of retrieving the destination host address from the Client connection. Note that all connections routing through this tunneling servlet with this parameter set will go to the hard coded host address. This parameter is disabled by default.
- **trace** – This parameter turns on the feature to generate a data trace from the tunneling servlet. This feature is usually used by tech support to gather information to help debug and issue. The parameter is defaulted to false.

Accessing the tunnel servlet

The tunneling servlet URL is partially configured in the web.xml file through the servlet mapping parameter. For the three versions of tunneling servlet running Tomcat hosted on port 8080 they are:

1. `http(s)://YOUR_SERVER_NAME:8080/tunnel/AVTunnel`
2. `http(s)://YOUR_SERVER_NAME:8080/tunnelssh/AVTunnelSSH`
3. `http(s)://YOUR_SERVER_NAME:8080/tunnelssl/AVTunnelSSL`

Enabling HTTPS

To ensure that the data is encrypted from the browser to the tunneling servlet via HTTPS protocol you will need to configure Tomcat or the integrated Web Server with an SSL certificate. These steps are beyond the scope of this instructions. You should be able to get your Administrator to configure the Web Server or Web Application Server to handle HTTPS protocol for secure traffic.

Tunneling servlet user authentication configuration

To use the Tunneling Servlet User Authentication feature, you must set the `userAuthentication` property in each tunneling servlet's `web.xml` file to `true`. The Tunneling servlets have the capability to perform basic user authentication through the use of files with the `.upf` extensions. These files are stored in the Tunneling Servlet's profile directory (Example: `C:\Apache-tomcat-7.0.42\webapps\tunnelssh\WEB-INF\classes\at2custom\at2wsp`).

In this location you will find a file named "admin.upf" which you can use a template for creating more user ids that are valid for user authentication. Simply use a text editor to create these files with the ".upf" extension. The filename should be in lowercase and is the user's login id, with the password inside of the file.

The example format of the sample "admin.upf" file is:

```
#  
#Wed Jan 24 13:00:06 PST 2001  
password=admin  
profile=
```

However it works with just a single line of text for the password value. Create as many id files as you need. Note you should delete or change the password for the "admin.upf" file at this time since a user id of "admin" with a password of "admin" is very easy to guess.

User Id Manager for Tunneling Servlet

There is a administrator tool that will allow the administrator to manage the different userID access for the tunneling servlet. The tool will also save the password as encrypted text in a upf file. This tool is located in the same peer folder as the classes folder. For example (C:\Apache-tomcat-7.0.59\webapps\tunnel\WEB-INF\classes) folder you will find a jar file named useradmin.jar. **This tool requires JDK 1.6 or higher to work.** Next you will need to launch a DOS cmd box and navigate to the directory where the useradmin.jar file is located and type the command “**java -jar useradmin.jar**”. This will launch the user admin application tool. After adding the userID and password don't forget to click the save button to create the upf files for your users. To save time, you can copy those created files (*.upf and users.lst) in the folder C:\Apache-tomcat-7.0.59\webapps\tunnel\WEB-INF\classes\at2custom\at2wsp into the other tunneling servlet version of the matching location.

- **Note:** if the java application does not start because of java environment issue, you can try and launch the useradmin.jar file by using the JDK packaged with the included demo apache-tomcat-7.0.59 from Crystal Point. In your DOS cmd box, make sure you are still in the classes folder (IE. C:\Apache-tomcat-7.0.59\webapps\tunnel\WEB-INF\classes). Enter the command:

```
..\..\..\jdk1.8u31\bin\java -jar useradmin.jar
```

- **Note:** if you have problems with this tool you can enable debug mode to generate a log file: “**java -jar useradmin.jar -debug > useradmintool.log**”. For PCI compliance, it is strongly recommended that you use the User Id manager tool for the Tunneling Servlet to create the User ID and password credentials instead of a plain text editor. The tool will encrypt the password and save it to the property file.

After you have completed the process of managing the different user id's you will need to either restart the tomcat server or the appropriate tunnel application. If using the tomcat web management page you must stop the servlet and then start it again. The reload option will not cause a refresh of the setting values.

When the servlet restarts it scans the configuration folder for files that end in “upf” and adds the ids that it finds.

Note do not enable login security (userAuthentication) for the SSH Tunnel servlet! -- When using SSH Tunneling, connectivity will be terminated if the SSH circuit to the host fails access control via the user supplied credentials.

Tunneling Monitor

The tunneling servlets also include a servlet called a tunneling monitor. This servlet allows you to view the active connections into the tunneling servlet. The configurable parameters for the RQNTunnelMonitor servlet are:

- **debug** – option to view the generated tunneling log file from the Monitor servlet. By default this is set to false.
- **work_dir** – directory the servlet looks into if you modify user access credentials. **Note** if you forget what you saved, just delete this file and the Monitor will use its default credentials login "rqs" pwd "zx11". **Note2** – if this servlet does not startup check this parameter and try using hard coded path to the directory specified in the web.xml. The default value is using relative pathing to the folder at2custom/at2wsp.
- **addr_list** – secure access to this servlet via IP Address filter. Values are separated by a semicolon ";". You can have wild cards like:
 - * -- this means let anyone have access to the Monitor servlet
 - xxx.* -- check the first block of address for match and then the following railing blocks are wild card.
 - xxx.xxx.xxx.xxx – specific address. You can add multiple address separated by semicolon.
- **time_out** – Time in minutes that the connection to the Monitor servlet will timeout.

URL to access the RQNTunnelingMonitor: [http\(s\)://Your-machine:8080/tunnel/RQNTunnelMonitor](http(s)://Your-machine:8080/tunnel/RQNTunnelMonitor)

Security Notes

The tunneling servlets have the following layers of security:

- Magic number – client side must match the server side. This is a static value. This provides defense against brute force attack. If the number does not match the request is denied.
- Tunnel Servlet feature userAuthentication – Administrators can configure userID and password in the form of upf files in the tunneling servlet's at2custom/at2wsp directory. These files are read into the tunneling servlet on web application start up. The user authentication feature offers another line of protection against brute force attack. Note that in Tunnel SSH version that the userID and password used for the user authentication with the tunneling servlet will need to match with the credentials to logon to the NonStop Host. In retrospect, you are better off disabling the tunnelSSH userAuthentication feature and leverage host credential to provide host control access.
- Configure WebServer or Application Server to handle HTTPS protocol to encrypt data stream from browser to tunneling servlet.
- Tomcat Remote Address Filter – You can use this filter to block out IP Addresses

2.5 Enterprise Installation

2.5.1 Enterprise Overview

Enterprise Overview

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

Enterprise Overview

An Enterprise installation should be used whenever OutsideView is to be installed to several networked workstations. With an Enterprise installation, you will be able to:

- Reduce your administrative costs by automatically installing and [updating](#) OutsideView Enterprise software across your organization from centralized network locations.
- Simplify user training and support by defining and administering user configurations and privileges from anywhere on the network.
- Maximize operational control over sensitive connectivity settings, while preserving user's ability to modify 'preference' settings.
- Monitor application usage and ensure license compliance with license administration tools (using WINS/NetBIOS).

Note: An Enterprise installation requires a different form of license than a Desktop installation. An Enterprise installation requires an NLPC license. NLPC licenses begin with the characters "NLPC" and contain multiple, imbedded per-seat or concurrent licenses.

The appearance of an NLPC license is similar to: NLPC-9100-0000-5565-2639-39be-07d7-0501-0001-11

Desktop licenses consist of a serial number and key value pair, such as

Serial Number: Key:

91000 00055 01 adb3-814c-07d7-0501-62.

and CANNOT be used for Enterprise installations.

The administrative features available in an Enterprise installation are determined by choices made during its installation. To create an installation that best suits the needs of your users, the following issues should be considered:

Does your user community contain groups with differing host access requirements?

If so, you may need multiple profiles.

Is there a need to control or track OutsideView usage per business unit, or cost center, or user group?

If so, you may want to maintain multiple, separate license pools.

Is there a need to control unauthorized modification of connectivity parameters?

If so, you may need to define user rights and privileges (per profile)

- Would some user groups be best served if connectivity files are created and maintained centrally, then automatically sent to the users with only selected parameters (i.e. colors) available for users to modify?

If so, you will probably want to use Supervisor mode to create files centrally, and define which setting users may modify.

Enterprise installation now supports two different licensing infrastructures. During the installation process, the installer will select the licensing option they wish to install:

Standard OutsideView Enterprise installation – This is the classic version of the OutsideView Enterprise and LicenseView installation. It requires a Windows “Shared” folder in order to run and perform Enterprise profile and licensing operations, and uses NetBIOS (WINS) for license collision detection

OutsideView Enterprise Installation with SQL-based Licensing – This new version of the Enterprise and LicenseView installation moves licensing operations into a SQL database. It requires a Windows “Shared” folder to run and perform Enterprise (profile and configuration) operations, and requires a Microsoft SQL Server 2012 - SQL Server 2022 database, with ODBC connectivity between the share and the SQL database in order to run and perform licensing tasks.

If your organization uses Microsoft SQL servers and conducts OutsideView Enterprise operations across a Wide Area Network (WAN) or multiple domains, Crystal Point recommends use of the SQL-based licensing. (Note that you must have a SQL Server installed and running before you can run the Enterprise Installation with the SQL-based licensing option.)

If you have questions about these or other installation options, please contact Crystal Point technical support at (+1) 425 806 1119.

Enterprise Installation Process

The process of installing OutsideView Enterprise consists of three basic steps:

1. Create at least one network share point (accessible by our OutsideView users).
2. Use the Enterprise setup process to populate the network share point(s) with Media, Profile and (for non-SQL installations) Licenses folders

The Media folder contains the OutsideView application code.

The Profile folder contains one or more Profile sub-folders, each containing their relevant installation shortcut and configuration files for that group of OutsideView users.

If Standard Licensing is desired, the Enterprise installation process will create and populate a license pool within the network shared folder Licenses.

- If SQL-based Licensing is selected, the Enterprise installation process will guide your installation of the license pool within a SQL database.
3. Installation of OutsideView onto client workstations through execution of the 'Install OutsideView' shortcut

2.5.2 Enterprise Failover (Disaster Recovery)

Enterprise Failover (Disaster Recovery)

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

Enterprise Failover (Disaster Recovery)

The Enterprise end-use instance of OutsideView communicates with the Enterprise share via UNC (Universal Naming convention) pathing. Each end-user OutsideView stores the UNC path for its Enterprise share point.

The Enterprise installation can be configured to automatically fail over between multiple Enterprise share locations, thus preventing the Enterprise Share server from becoming a single point of failure, as well as providing Automatic Disaster Recovery capability.

To configure this capability:

1. Install the primary Enterprise share normally, as described elsewhere
2. Install another instance of the Enterprise share, with identical profiles. It is not necessary to create the various configuration files.
 - a. Give the second location identical share and security permission as the original location
 - b. Define an internal process to synchronize the shares periodically (this can be automated or manual) by
 - i. Copying the config sub-folder of each profile from the primary to the secondary location.
 - ii. Copying the contents of the License folder from the primary to the secondary location
3. Create the file failover.txt in the primary share's Profile folder

The content of failover.txt is of the form:

```
\\[primary server]\[primary share]\profile  
\\[secondary server]\[secondary share]\profile
```

Upon a first, successful access to the primary share, the fail over information is replicated to each end-use PC. That information is automatically updated as necessary upon each subsequent access.

NOTE: Use of the Pristine mode supervisor mode setting can disrupt failover, by removing the failover.txt file. See the topic [Client Administration](#) for more information.

Each time the end-use instance of OutsideView starts, it attempts to contact its primary share point. If that location does not respond before the timeout values expires, then that copy of OutsideView resets itself to use the secondary share location values, and re-attempts contact.

This re-direction will persist for the duration of that OutsideView copy. Upon termination and restart of that end-use OutsideView instance, it will restore its settings to point to the primary share, and attempt access again. (This constitutes the fail back capability).

2.5.3 .NET Requirement

.NET Prerequisite

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

The platform selected for the shared Windows folder, which will be the shared 'hub' for OutsideView Enterprise must have the .NET framework installed. The minimum required level is .NET framework 4.5. The recommended level is .NET framework 4.5.

2.5.4 Create Network Shares

Create Network Shares

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

Create Network Share(s)

Enterprise installation requires at least one shared folder (for instance, OV91_Ent) on a Windows 10, Windows 11, or Windows 2012 - 2022 server. OutsideView users must be able to 'see' this network share. This must be a **root level share**; that is, visible directly below system name in the form \\system\share. Lower level shares (e.g., \\system\corporate share\sub-folder\sub-folder\Enterprise share) are not supported.

If a single shared folder is created, the installation will automatically create Media, Profile and (if using standard licensing) Licenses subfolders beneath that shared location. All users must be given a minimum of read/change permissions to the license database if using standard licensing. Because all subfolders of a share inherit the access rights of the top-level share, all users must therefore be given at least read/change access to this sharepoint. If using SQL-Based licensing, the top-level share may be given rights that are more restricted; such as Read-only.

To create a more secure installation, even when using the standard licensing, separate folders for the Media, Profile and License files may be created and shared with the following properties:

Folder	Minimum Access
Media	Users: Read Only Administrators: Full Control
Profile	Users: Read Only Administrators: Full Control
License	Users: Read/Change Administrators: Full Control

NOTE: *If there is a possibility for multiple License Pools (this should apply only when multiple profiles are in use), it is desirable to create each License share individually (e.g., DataLics, SysLics etc.). The same permissions are required for each of the individual License shares. Multiple license pools may also be created within subfolders of a top-level share (e.g. OVLICENSE\DataLics and OVLICENSE\SysLics).*

The next step is to [populate the network Share\(s\)](#) , creating at central resource that OutsideView end-users will draw from. This is accomplished by running the Enterprise installation process one or more times , in order to create one or more license pools, and one or more Profiles (or User Groups).

2.5.5 Enterprise Installation onto Share

Enterprise Installation onto Share

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

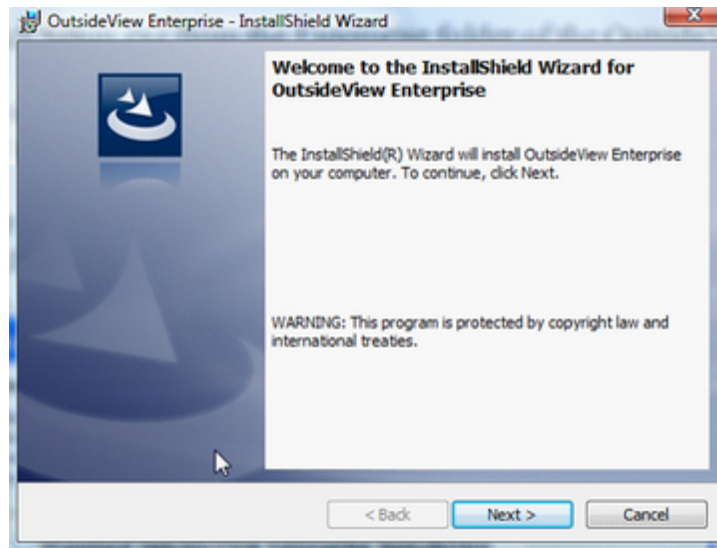
2.5.5.1 Standard OutsideView Enterprise Installation

Standard OutsideView Enterprise Installation

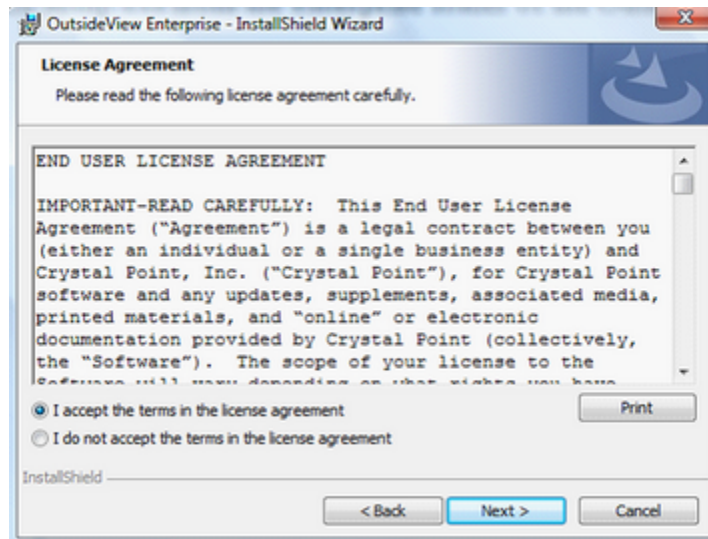
[Top](#) [Previous](#) [Next](#)

Standard OutsideView Enterprise Installation

1. Launch Setup.exe from the Enterprise folder of the OutsideView CD or CD image.



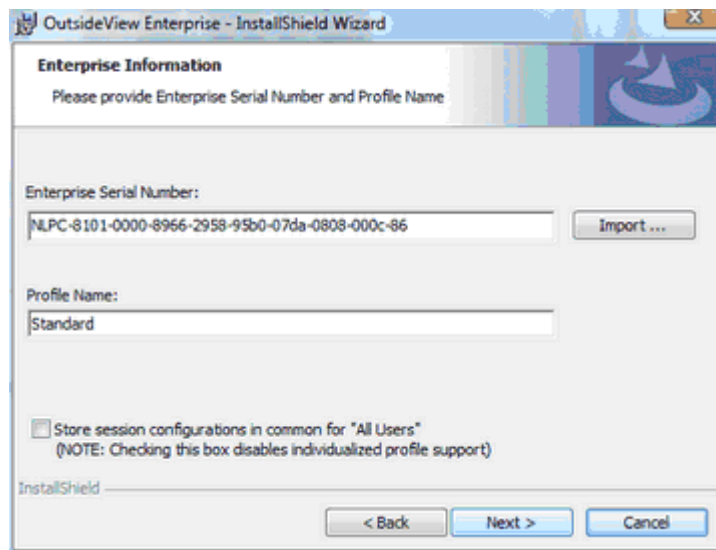
2. When prompted, click Next.



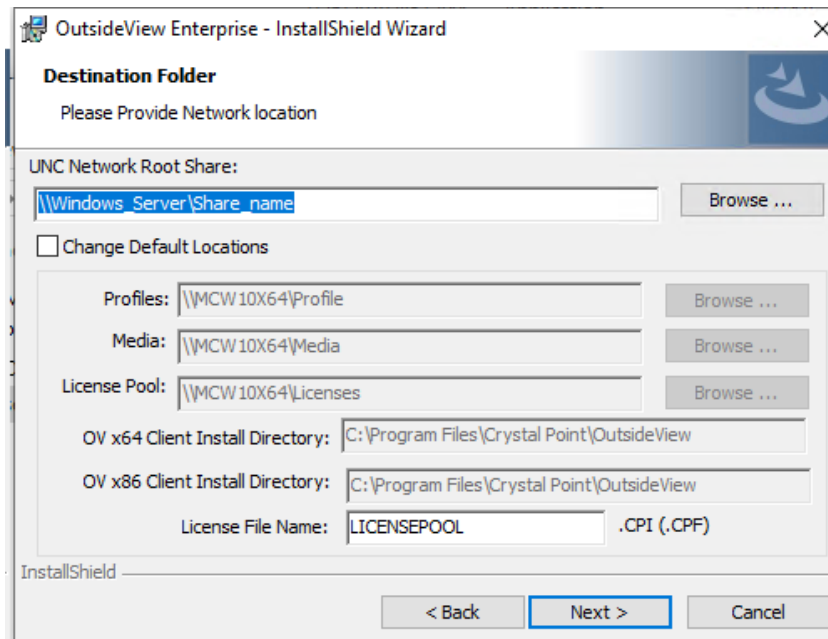
3. Read and accept the terms in the End-User License Agreement (EULA) by selecting "I accept the terms in the license agreement" and click Next.



4. Select the Standard OutsideView Enterprise Installation option then click Next.



5. If you have an NLPC number, enter it at the dialog where it says "NLPC-". If you received a License File, click the "Import" button. The Installer will prompt you to browse for your License File (.lic). The Installer will automatically extract the correct NLPC License Code from the License File.
6. **Profile Name** If you're not creating multiple profiles, it's simplest to just use the default profile name "Standard". If you are using multiple profiles, you should use a name descriptive of the group (e.g., "Data_Entry"). Continue following these instructions to create your first User Profile.
7. Click "Next" button to go to the next screen.



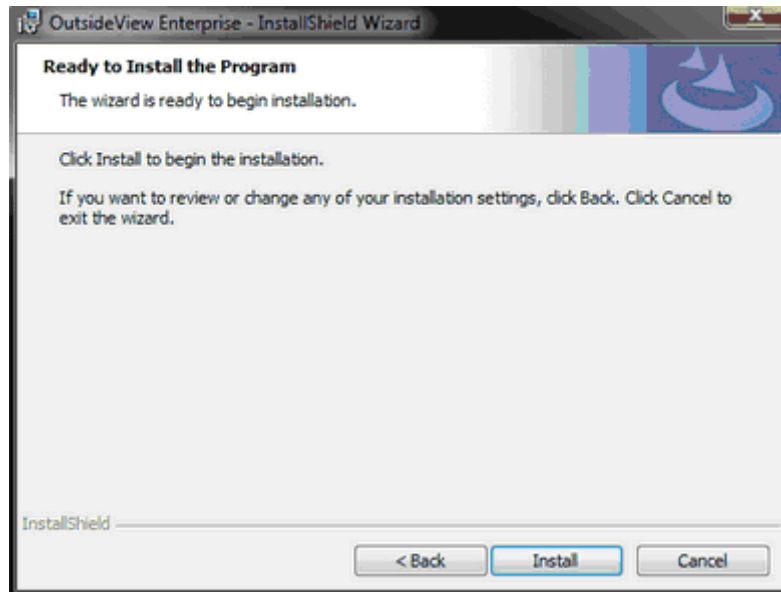
8. If you created a single top-level network share, enter the UNC path or browse to that share. OutsideView will automatically create the directories it needs within that share. If you created three (or more) individual shares, checking the "Change Default Locations" checkbox will allow you to specify the location/name of each share individually.

CAUTION: *It is essential that the share location be specified in UNC format. If the share is located on the local machine, however, the path may be returned in mapped drive format, such as D:\OV. In that case, correct the returned value by typing in the UNC path, such as \\servername\OV.*

9. Enter the License File name (the default name is LICENSEPOOL). If you are using multiple profiles, use a name descriptive of the group.

10. Select the location, on the user PC to which OutsideView is to be installed. (Typically, this is C:\Program Files\Crystal Point\OutsideView but frequently varies in Terminal Server or Citrix environments).

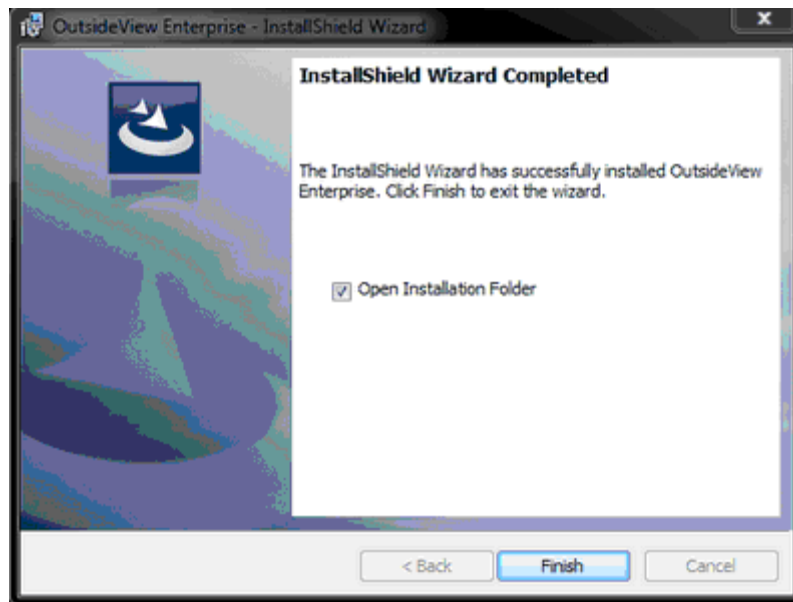
11. Click "Next" button.



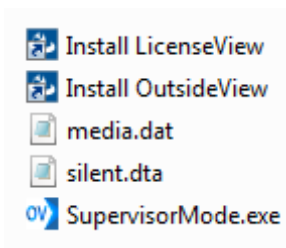
12. Click "Install". Be patient - this step may take a few moments as the Installer will now: Automatically copy an image of the installation files to the location you defined for the Media share.

Create a License Pool in the folder you defined for the License share and fill your License Pool with licenses from the License File.

Create a Profile directory containing the profile you just finished configuring



13. When the Installer has finished, leave the "Open Installation Folder" checked and click "Finish". The Installation Icons [three shortcuts and two configuration (.dat) files] will appear in their own window (the Install folder of the specified profile).



Prior to actually deploying OutsideView to end users, you may wish to define OutsideView configuration files (e.g. sessions, workspaces, and macros) and user privileges for members of each Profile. For the instructions on this task, see the [Supervisor Mode](#) topic. Definition of Profile settings may also be performed after client installation.

For instructions about installing the end-user workstations, click [here](#).

For instructions about installing Windows Terminal Server or Citrix application servers, click [here](#).

NOTES on default Enterprise file locations (non-SQL):

The central shared folder of an Enterprise installation will have three sub-folders:

- Media, containing the OutsideView and LicenseView applications.
- Profile, containing one or more individual profiles, default profile name is Standard.
- Licenses, containing one or more license pools (default name Licensepool.cpf)

Each time end-user or 'client' instances of OutsideView are initiated on outlying PCs, the OutsideView software will attempt to access the central Enterprise share to update its local permission settings, acquire or update its local copy of the application software and acquire or update any configuration files that exist on the central share.

The central configuration files are created using OutsideView's Supervisor Mode. For more information, click [here](#)

If the central share is NOT accessible for any reason, OutsideView will display a warning message that it could not access the Enterprise resource (to assure it has the latest configuration information,etc.) but it will continue to operate, using its local information, for a period of 7days after its last successful access of the share.

2.5.5.2 SQL OutsideView Enterprise Installation

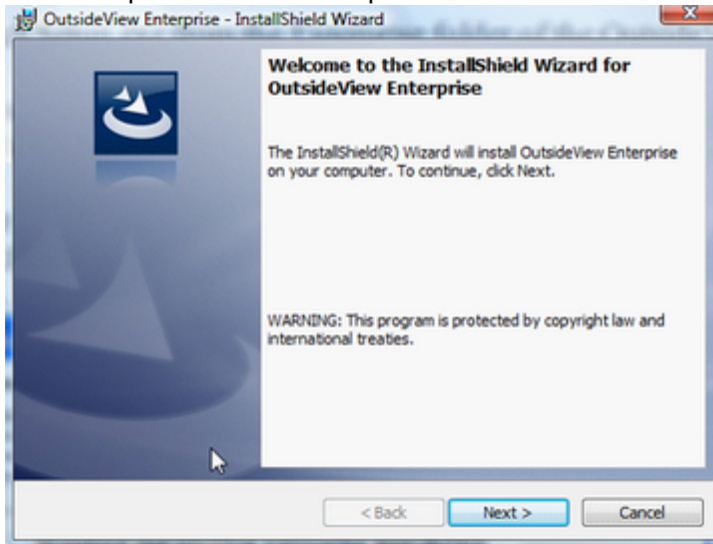
SQL OutsideView Enterprise Installation

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

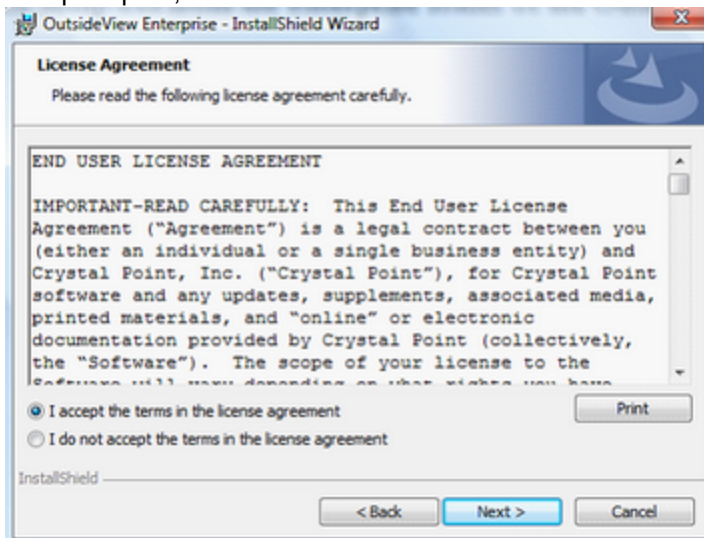
OutsideView Enterprise Installation with SQL-based Licensing.

Note: SQL Server compatibility is supported for SQL Server 2012 up to SQL Server 2022

1. Launch Setup.exe from the Enterprise folder of the OutsideView CDROM.



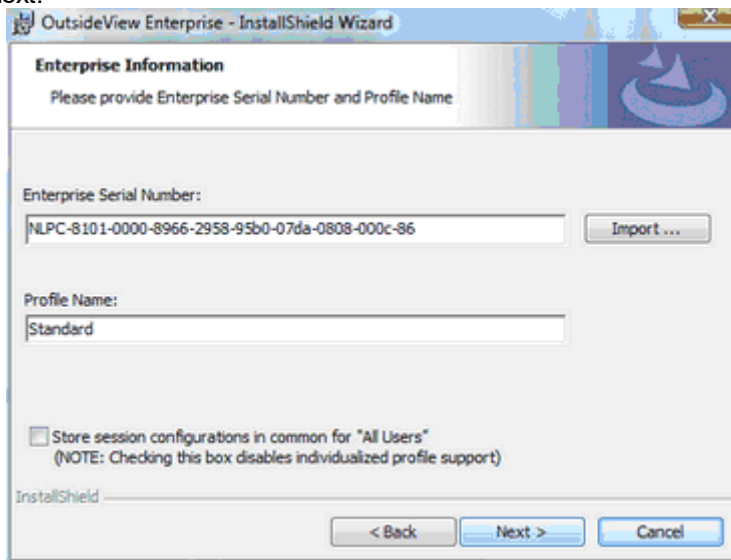
2. When prompted, click Next.



- 3 Read and accept the terms in the End-User License Agreement (EULA) by selecting "I accept the terms in the license agreement" and click Next.



4. Select the OutsideView Enterprise Installation with SQL-based Licensing option then click Next.

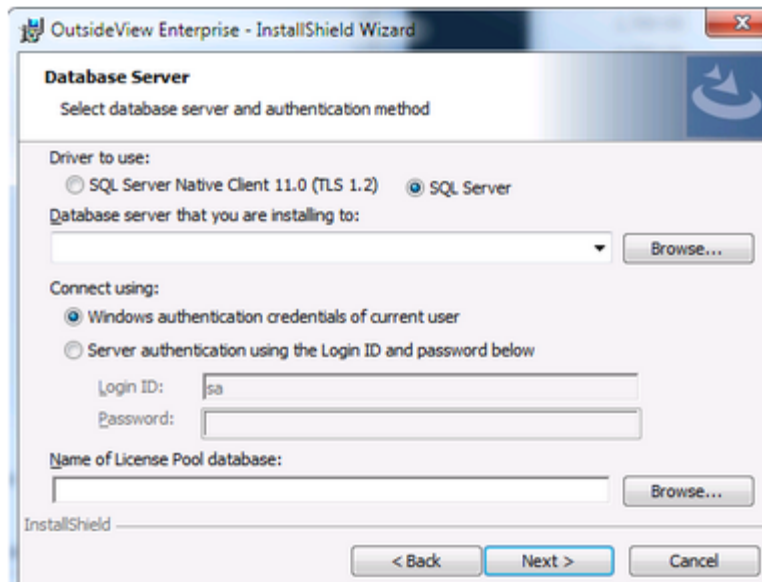


5. If you have an NLPC number, enter it at the dialog where it says "NLPC-". If you received a License File, click the "Import" button. The Installer will prompt you to browse for your License File (.lic). The Installer will automatically extract the correct NLPC License Code from the License File.

NOTE: Do not mix PerSeat and Concurrent licenses in the same SQL LicensePool.

6. If you are creating a single user profile, it's simplest to just use the default profile name "Standard". If you are creating multiple profiles, enter a descriptive profile name, such as "Data_Entry". To create multiple profiles, simply conduct the Enterprise installation as many times as needed.

- 7.



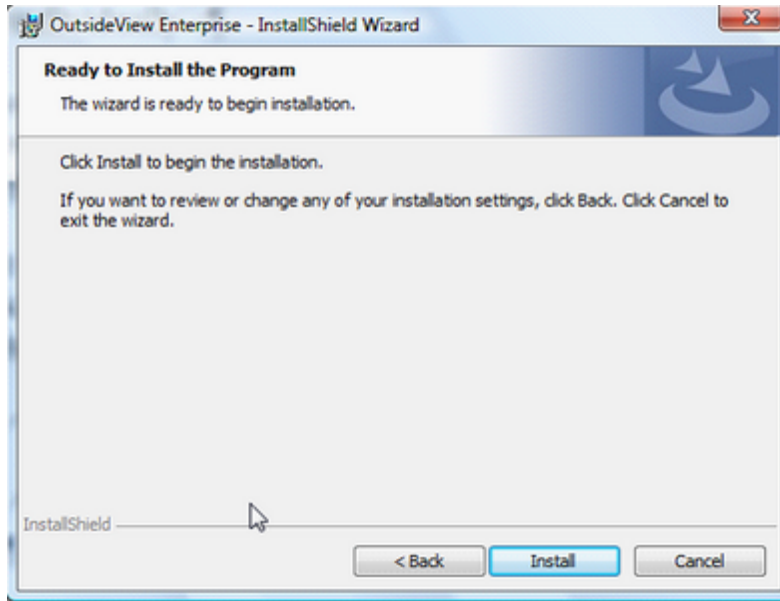
8. Select the SQL Server driver to use for the OutsideView clients. Note that SQL Server Native Client 11.0 ODBC Driver requires Microsoft SQL Server 2012 Native Client to be installed on your computer prior to using this driver. If your SQL Server machine is configured to use TLS 1.2 encryption, then you will need to use SQL Server Native Client 11.0 ODBC driver which is now installed as a prerequisite part of OutsideView 9.0.
9. Enter the name of the computer that the Database server is running on. Note that you can click on the Browse button if your SQL servers are configured with the SQL Browse service. The Browse button will display the computers that are hosting SQL Server.
CAUTION: Use of 'localhost' disables all remote access into the database. If you are browsing from the SQL server itself, you may see a selection in the list of computers hosting SQL Server 2005 such as "(localhost)/sqlexpress" You must substitute in the DNS qualified name for the server rather than use 'localhost'.
- 10 Select the authentication you will be using to connect to the database server. There are only two available options:
 - Windows authentication – this uses the users' Windows credentials to gain access to the database.
 - SQL Server configured Login and Password – this option is for users' who may not have Windows credentials. A credential is created for the user on the SQL Server. Then this credential is used to gain access into the SQL Server to install the database.
- 11 Enter the name of the database to be created on the database server. In the image above, the name of the database to be created is LicensePool. Clicking on the Next button will trigger creation of the LicensePool database on the database server.
- 12 After the database has been successfully created the following message box will be appear letting the user know that the database was installed:



Click OK

- 13 If you created a single top-level network share, enter the UNC path or browse to that share.
 - OutsideView will automatically create the directories it needs within that share. If you created two (or more) individual shares, checking the "Change Default Locations" checkbox will allow you to specify the location/name of each share individually.

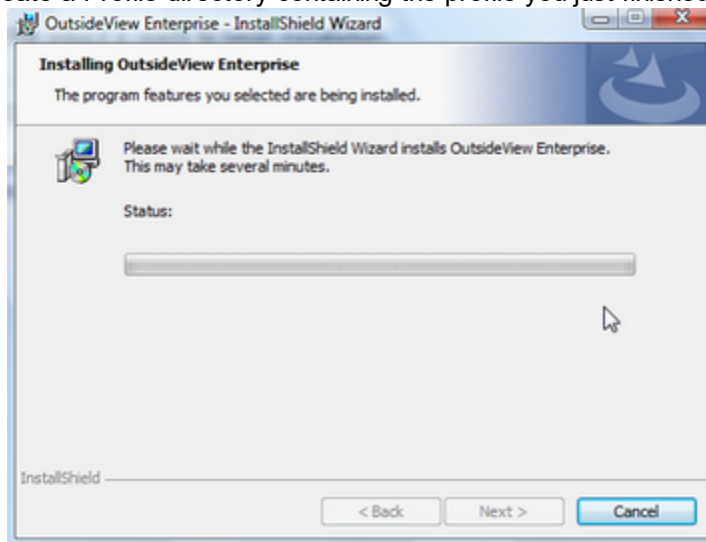
CAUTION: It is essential that the share location be specified in UNC format. If the share is located on the local machine, however, the path may be retrieved in mapped drive format, such as C:\OV. In that case, type in the UNC path, such as \\servername\OV.
- 14 Select the location to which OutsideView is to be installed, on the user PC (Typically, this is C:\Program Files\Crystal Point\OutsideView but this may vary, particularly in Terminal Server or Citrix environments)
- 15 Click "Next" button.

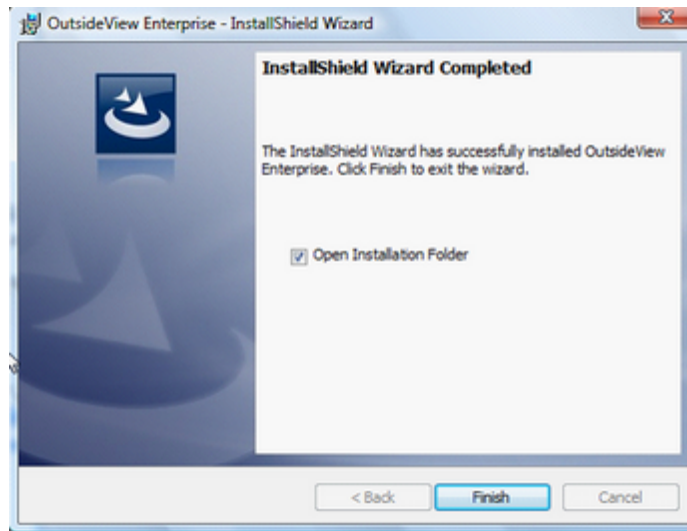


16 Click "Install". Be patient - this step may take a few moments, as the Installer will now:






Automatically copy an image of the installation files to the location you defined for the Media share.

Create a Profile directory containing the profile you just finished configuring

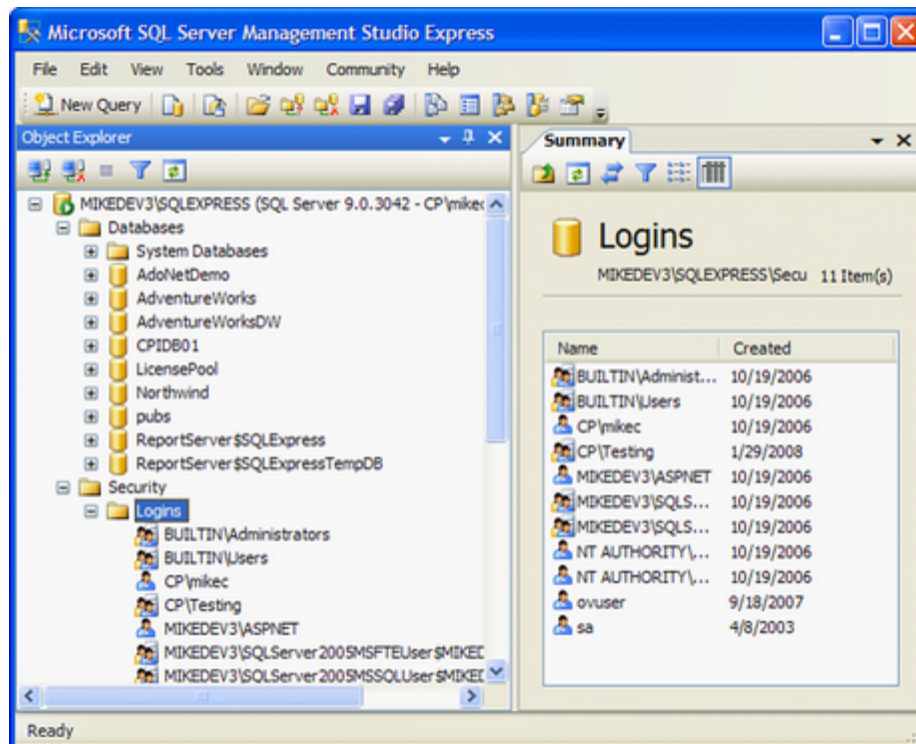




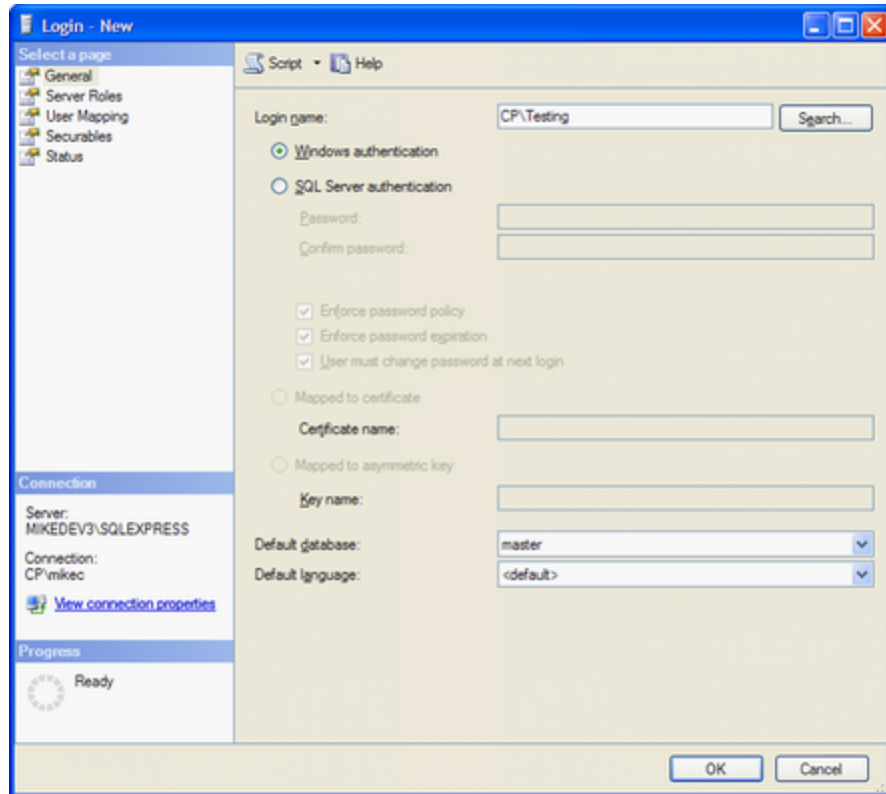
- 17 When the Installer has finished, leave "Open Installation Folder" checked and click "Finish". The Installation Icons [two shortcuts, one executable, and two configuration (.dat) files] will appear in their own window (the specific Profile's Install sub-folder.)

Name	Date modified	Type
 Install LicenseView	03/19/17 4:47 PM	Shortcut
 Install OutsideView	03/19/17 4:47 PM	Shortcut
 media.dat	03/19/17 4:47 PM	DAT File
 silent.dta	03/19/17 4:47 PM	DTA File
 SupervisorMode.exe	03/17/17 5:23 PM	Application

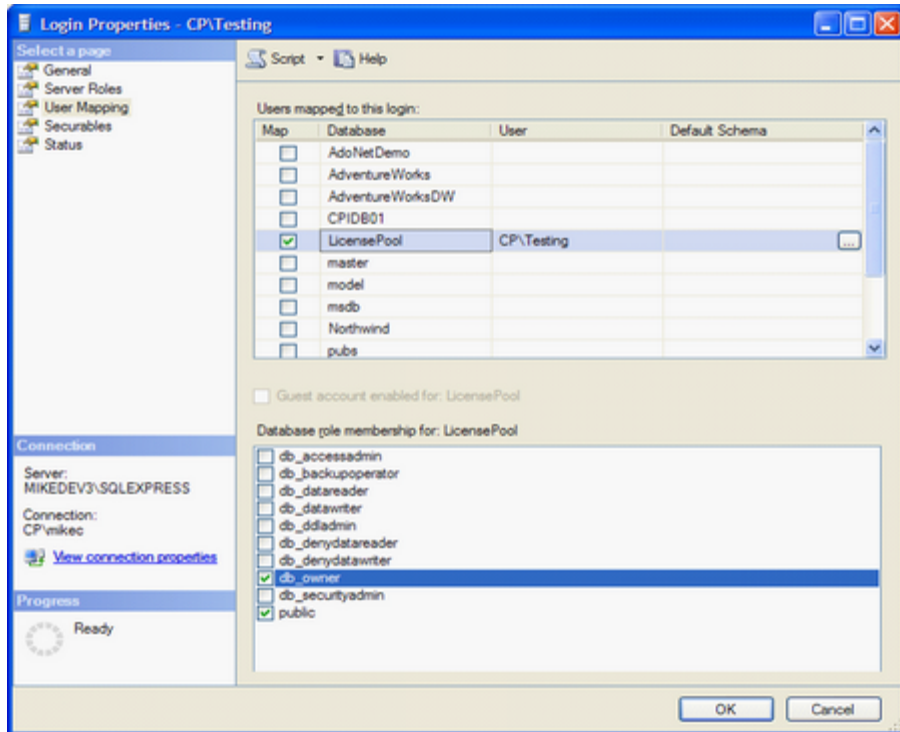
Note: In SQL Server 2005, users have limited permissions to access the database and perform operations on them. Even with Windows authentication, the database administrator will need to configure the Security aspect of the database once the License Pool database is installed. For instance, the default behavior for users allows them to connect to the database but not perform other functions such as writing to the database or reading from the database. To resolve this in a Windows authentication environment, the database administrator will need to create a group domain in which all the users that need to use the database are added to that group domain. For example, a group domain called CP\Testing could be created. In this domain all the users that belong in the CP\Testing area are added to this domain. Then in the SQL Server Management tool, the group domain is added by selecting the Logins folder and right clicking it to launch the command "New Login...".



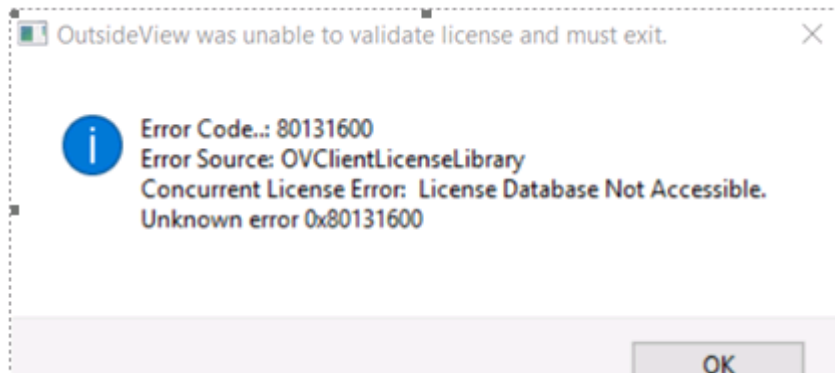
A Login panel will appear and you will need to enter the CP\Testing or as an alternative search for the group and enter the name into the Login Name text box.



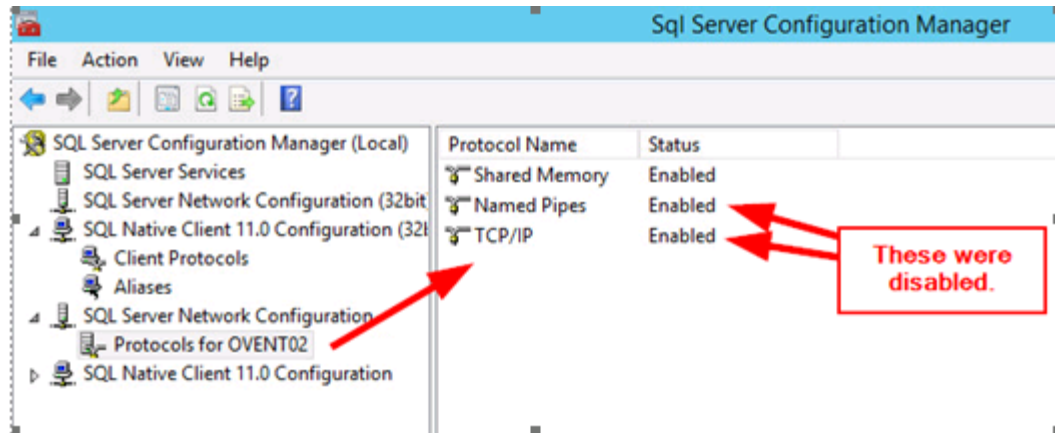
After entering the Login name, you will need to configure the User Mapping. This option allows us to map the role membership for the domain group to a specific database. For this example, the database we are mapping to is LicensePool and the database role membership for LicensePool is db_owner. This will provide the users of CP\Testing domain the ability to read, write, and update functions to the LicensePool database.



NOTE - If you are running into connectivity issues from the client to the SQL Server and getting this error:



Open the SQL Server Configuration Manager and navigate to the SQL Server Network Configuration and see if the Protocols listed there are enabled. These settings are usually set to disabled by default:



Enable the protocols and restart the SQL Server and see if that resolves your connectivity issue.

NOTES on default Enterprise file locations (SQL):

The central shared folder of an Enterprise installation will have two sub-folders:

Media, containing the OutsideView and LicenseView applications.

Profile, containing one or more individual profiles, default profile name is Standard.

Each time end-user i.e. 'client' instances of OutsideView are initiated on outlying PCs, the OV software will attempt to access the central Enterprise share to update its permission settings, and acquire or update its local copy of the application software and any configuration files that exist on the central share.

The central configuration files are created using OutsideView's Supervisor Mode. For more information, [click here](#)

If the central share is NOT accessible for any reason, OutsideView will display a warning message that it could not access the Enterprise resource (to assure it has the latest configuration information, etc.) but it will **continue to operate**, using its local information, for a period of 7 days after last successful access to the share.

2.5.6 Creating Multiple Profiles

Creating Multiple Profiles

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

Creating Multiple Profiles

If your population of OutsideView users includes groups with different host access or application usage requirements (e.g. developers versus data entry personnel), you should consider defining separate OutsideView user profiles for each such group. Defining multiple user profiles will allow you to easily deploy and manage host connectivity tools that are tailored to the needs of diverse user groups. Each new user profile contains its unique installation script, and (potentially) unique user configuration files, user privileges and license pool.

To create additional user profiles, it is necessary to re-execute the [Enterprise installation process](#). In that process, the Enterprise serial number must be re-entered (no duplicate licenses are created), and a unique name must be assigned to the profile (e.g. DataEnt, SysAdmin`).



The more-advanced technical types may, if they wish, bypass the install wizards and GUIs to replicate profiles in a more direct manner. Merely copy an entire existing profile folder (i.e., Standard) to a folder of another name (i.e. New_profile) on the same level. Then edit the silent.dta file (in Notepad) within the newly created folder to point to the new locations, and edit the properties of the Install OutsideView shortcut within the new profile to point to their new locations. You may then modify any existing permissions, configurations files, and profile membership data via the Supervisor mode of the new profile.

2.5.7 Client Installation

Client Installation

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

Client Installation

These instructions are for installation onto end-user workstations. For instructions to install onto a WTS/Citrix application server, click [here](#).

NOTE: *In Windows 2000 and later later environments, administrative or power user privileges are required to install the client-side product, even via the "Install OutsideView" shortcut. OutsideView installation will automatically detect if your Operating system is 32bit or 64bit versions and install the corresponding version of OutsideView.*

To install OutsideView on a workstation, simply double-click on the 'Install OutsideView' shortcut located in the "Install" subfolder of appropriate user profile. No user intervention (e.g. entry of license information) is required to accomplish this installation. After installation, when OutsideView is *launched* for the first time on a client PC, it will 'check out' a license from the License Pool defined for the user's profile. If this is a static, or per-seat license, the client will retain that license until it is manually recovered via the LicenseView utility. If the license is a concurrent license, it will be released each time the client properly exits the OutsideView application.

Notes on Client workstation file locations

A default installation places the OutsideView application files under C:\Program Files\Crystal Point. Each OutsideView user on the PC will have an individual location automatically created to contain their personal OutsideView configuration files and Edit files. For XP systems, these are under C:\Documents and Settings\[User_Name]\Application Data\Crystal Point and C:\Documents and Settings\[User_Name]\My Documents\Crystal Point. For Vista systems, these are at C:\Users\[User_Name]\AppData\Roaming\Crystal Point and C:\Users\[User_Name]\Documents\Crystal Point

NOTE: If the option to “Use shared directory for session configurations” is selected during installation, all OutsideView configuration files will be stored, in common, under C:\Users\All Users\ and on down.

2.5.8 SCCM (SMS) Installation Enterprise Client

SCCM (SMS) Installation Enterprise Client

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

The following instructions assumes that you have already installed the Enterprise installation onto your Network Share folder.

The new OutsideViewSetup.exe installer contains both 32bit and 64bit OutsideView installations wrapped within. The installer has the capability to detect your operating system and install the correct version of OutsideView onto your machine. In the previous versions of OutsideView, users were required to extract the msi package from the installation but that is no longer required with the updated OutsideView Installation Setup.

The Enterprise SCCM Installation has been updated so that admins only need to provide a single parameter instead of 11 params! This command will work for either SQL Enterprise Licensing or the Traditional OutsideView Licensing.

SCCM Enterprise Installation requires a single parameter:

1. CUSTOMSILENTPATH

Enterprise Installation Command

```
OutsideViewSetup.exe /silent CUSTOMSILENTPATH="\
\MIKEDEVSSD\OV\Install\NONSQ\OV90\Profile\Standard\install\silent.dta"
```

Installation Logging

If you run into installation issues, users can turn on the logging for the installations:

```
OutsideViewSetup.exe /debuglog /silent CUSTOMSILENTPATH="\
\MIKEDEVSSD\OV\Install\NONSQ\OV90\Profile\Standard\install\silent.dta" /log"./"
```

This will generate two separate log files in the same directory where you launched the OutsideViewSetup.exe application. The two log files are:

1. InstallShield.log
2. OVX64Compont.log or OVX86Component.log depending on your Operating System.

If you are under a Star Support Contract, collect these two log files and send them over to support@crystalpoint.com for further help regarding installation issues.

2.5.9 WTS/Citrix Server Installation

WTS/Citrix Server Installation

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

Windows Terminal Server or Citrix Server Installation

Overview:

There are two forms of OutsideView which can be used in Citrix or Windows Terminal Server environments.

An OutsideView corporate license is available to organizations with software inventory controls in effect. This license mode will allow a public version to be published on a Windows Terminal Server or Citrix environment, but does not provide automatic configuration control and synchronization, nor concurrent licensing options.

The more powerful and flexible OutsideView Enterprise, with Concurrent licensing, is the only preferred mode of OutsideView supported within the Windows Terminal Server or Citrix environments. OutsideView Enterprise runs within a WTS/Citrix server as a 'client.'

1. Follow the instructions to conduct an Enterprise installation of OutsideView, perhaps merely creating a separate profile configured for Citrix/WTS use.

NOTE: *When operating OutsideView in WTS/Citrix environments, it is frequently necessary to modify the default local program files installation location from C:\Program Files\Crystal Point\OutsideView to some other location – e.g., M:\Program Files\Crystal Point\OutsideView. Consult your organization's WTS/Citrix administrators.*

2. Have the WTS/Citrix server, in Install mode, browse to and execute the "Install OutsideView" short cut within the appropriate OutsideView Enterprise profile.

Uninstalling previously published OutsideView instances from Citrix

NOTE: *As with any Citrix-hosted application, the installation or uninstall of the OutsideView application must be performed in an identical manner on all members of a Citrix server farm.*

1. Logon as Administrator
2. Open Citrix Management Console (Start -> Programs -> Citrix -> Management Console)
3. Log into Management Console as administrator
4. To delete a published instance of OutsideView, select Application
5. Select the specific OutsideView application to uninstall, right-click and select Delete
Published Application

Installing OutsideView to Citrix

NOTE: *If you have more than one server in the Citrix server farm, all servers need to have identical installations/configurations of OutsideView. Just follow the steps below to set up each server.*

Option 1:

1. Open Control Panel, select Add/Remove Programs

2. Choose Add New Programs
3. Select CD or floppy, click Next and go to Browse (set file type to 'All files')
4. Browse to the 'Install OutsideView' shortcut
5. Select the file, click Open, click Next
6. OutsideView installation will start
7. When completed, back out and click Finish

Option 2:

1. Select Start -> Run
2. Enter 'change user /install'
3. Navigate to 'Install OutsideView' shortcut and double-click on the file to start the installation
4. After installation is completed, select Start -> Run
5. Enter 'change user /execute'

After installing OutsideView onto each server, test the successful installation

1. Select Start -> Programs -> Crystal point -> OutsideView -> OutsideView
2. Configure OutsideView 'Edit -> Application Settings' to be identical on all servers
3. Click Ok and close OutsideView

Publishing OutsideView client for use by Citrix clients

NOTE: Only needs to be done once, it applies to entire farm.

1. Open Citrix Management Console
2. Select Application and right-click
3. Select Publish Application
4. Wizard Screen 1 - Welcome to the Application Publishing Wizard:
5. Display Name: OutsideView
6. Application Description: Mainframe connection tool
7. Click Next

Wizard Screen 2 - Specify What to Publish:

8. Select Application
9. Command Line: i.e.: C:\Program Files\Crystal Point\OutsideView\outside.exe
10. File of Type: Executable
11. Working directory: Leave as displayed; i.e.: C:\Program Files\Crystal Point\OutsideView (set file type to 'Executable')
12. Click Next

Wizard Screen 3 - Program Neighborhood Settings:

13. Accept all defaults
14. Click Next

Wizard Screen 4 - Specify Application Appearance:

15. Accept all defaults
16. Click Next

Wizard Screen 5 - Specify ICA Client Requirements:

17. Accept all defaults
18. Click Next

Wizard 6 - Specify Servers:

19. Add all farm members
20. Accept all defaults otherwise
21. Click Next

Wizard Screen 7 - Specify Users:

22. Specify users as per company policies
23. Click Finish

2.5.10 Example Installation

Example Installation

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

Example Multiple-profile, Multiple License Pool Installation

To give you some idea of the flexibility and capabilities of an OutsideView Enterprise installation, here is a description of an installation that meets the needs of two user groups with widely different requirements. We will call these two groups “Salespeople” and “Programmers”.

- Programmers
 - Are frequent users of OutsideView
 - Require access to the full capabilities of OutsideView, including multiple types of emulation.
- Salespeople
 - Are intermittent users of OutsideView with limited PC or Windows skills
 - Require access to a single host application for their tasks.
 - Will be permitted to make only ‘cosmetic’ changes to their session settings.
 - For security purposes, screen snapshots and screen prints will be disabled from within OutsideView
- Members of both groups travel around the office(s) and may need host access from any convenient workstation.
- Corporate security initiatives mandate both groups will use only encrypted sessions.

To meet these differing needs; we would

1. Create a single network share point (as described in the [Create Network Shares](#) topic).
2. Create a "Sales" user profile with a separate license pool containing concurrent licenses (as described in the [Enterprise Installation](#) topic).
3. Create a "Programmers" user profile with a separate license pool containing per-seat licenses (as described in the [Enterprise Installation](#) topic).
4. Install OutsideView to the administrator's PC using the 'Install OutsideView' shortcut in either profile (as described in the [Client Installation](#) topic).
5. Using OutsideView launched in the Supervisor mode of the **Programmers** profile (As described in the topic Supervisor Override Mode):
 - Define and save a workspace containing a single session that starts a TACL command prompt.
 - Leave User Privileges completely open (full rights)
 - Assign members to the Programmers profile.
6. Using OutsideView launched in the Supervisor mode of the Sales profile:
 - Define and save a workspace containing a single session
 - The single session will be SSL-encrypted, and have a defined service or startup macro (as described in the OutsideView Users Guide).
 - Set User Privileges (as described in the [User Privileges](#) topic) so that:
 - OutsideView will automatically start a specified workspace and session
 - Only a single session can be run at a time
 - User cannot modify Workspaces, Macros
 - User can modify only Color settings and Toolbars within the session
 - Screen Print, Screen snapshot, and right-click menus are disabled.
 - Assign members to the Sales profile (as described in the [Assign Users to Profiles](#) topic).
7. Using LicenseView, set e-mail alerts for the two different License Pool Database (as described in the [License Alerts](#) topic).

2.6 License View Installation

License View Installation

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

License View Installation

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

LicenseView Installation

LicenseView is a utility for management of OutsideView license pools. There are two different versions of LicenseView. The standard version of the LicenseView application is designed to administer standard (non-SQL) license pools. The SQL LicenseView application is designed to administer SQL-based license pools.

To install LicenseView, simply click on the shortcut in the Profile Install subfolder. During the LicenseView installation process, you will have the option of selecting which type of LicenseView application that you want to install. The version of LicenseView you install should match the version of licensing that you installed during the Enterprise installation process. If you installed the traditional License Pool, then you would select LicenseView. However, if you installed the License Pool onto a SQL server database, then you would select SQL LicenseView.

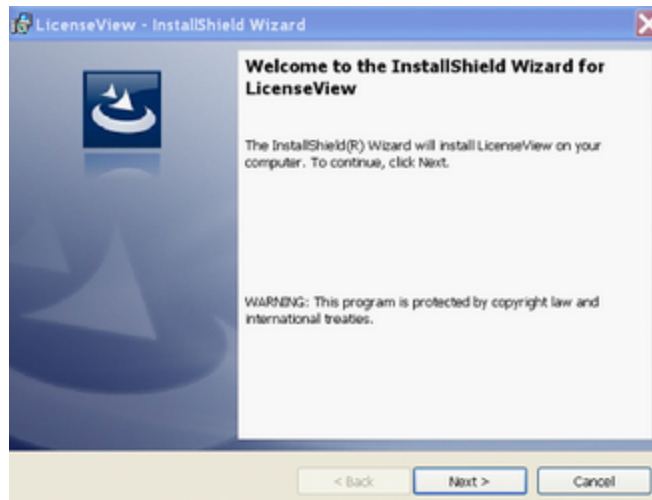
2.6.1 Installing LicenseView

Installing LicenseView

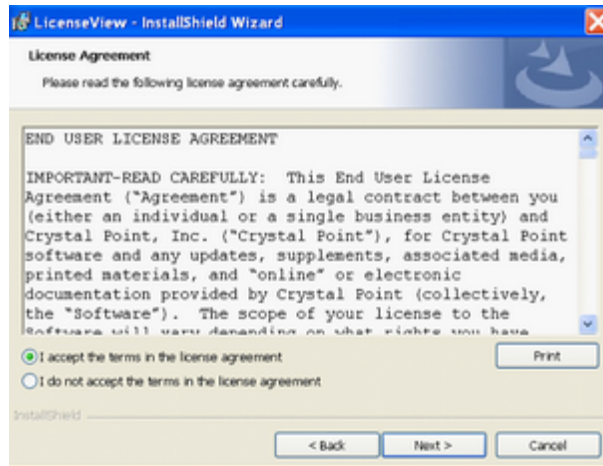
[Top](#) [Previous](#) [Next](#)

Installing LicenseView.

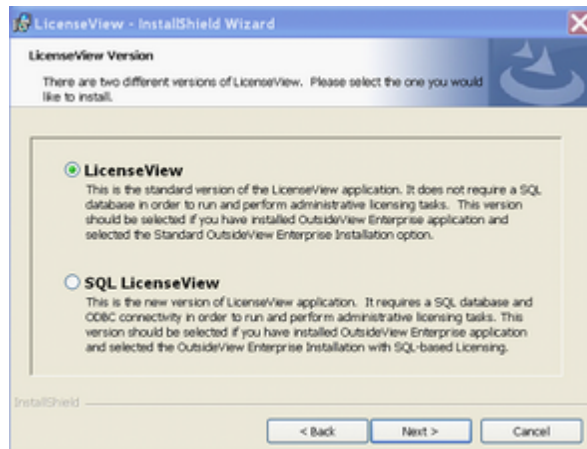
1. Navigate to the folder LicenseView on the OutsideView CD and click on LicenseViewSetup.exe.



2. Click Next



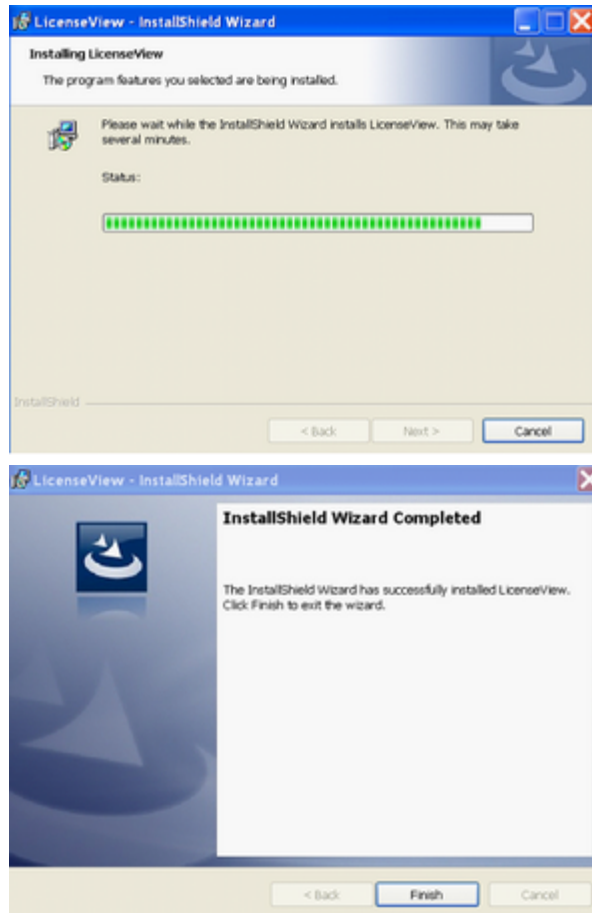
3. Accept the terms of the License Agreement and click Next.



4. Select the appropriate LicenseView type, standard or SQL, and click on Next.

5. Modify the LicenseView installation directory if desired, and then click Next.

6. When prompted, click Install.



LicenseView, whether for standard or SQL licensing is now ready for use. In the standard LicenseView, merely select File Open, and navigate to your standard license pool. With SQL LicenseView, you must first connect it to the appropriate SQL-based license pool.

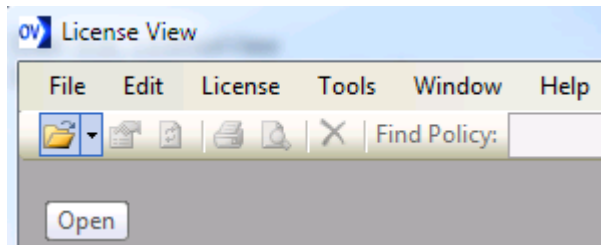
2.6.2 Connecting SQL LicenseView to SQL-based License Pools

Connecting SQL LicenseView to SQL-based License Pools

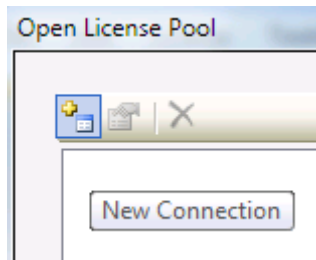
[Top](#) [Previous](#) [Next](#)

Connecting SQL LicenseView to SQL-based License Pools

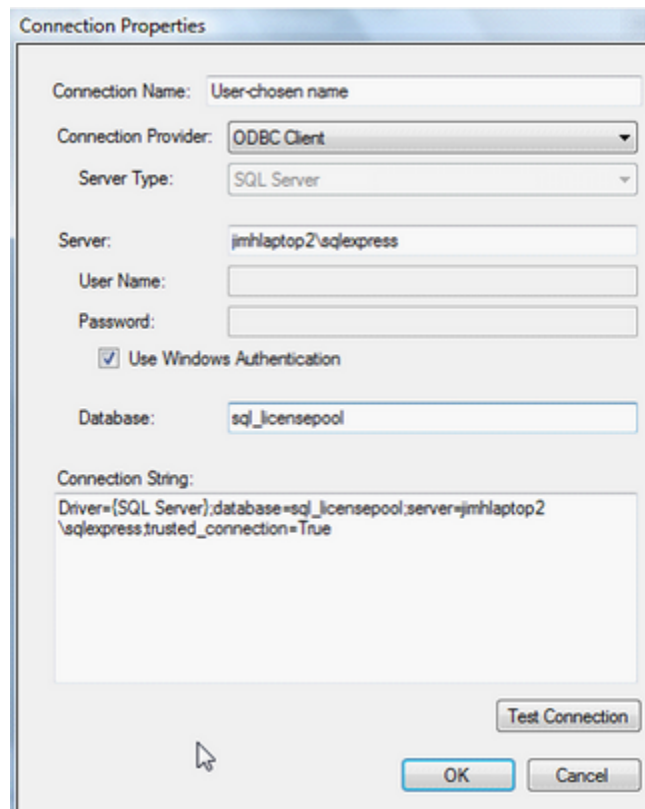
1. Start SQL LicenseView
2. Select File, Open or click on the Open icon



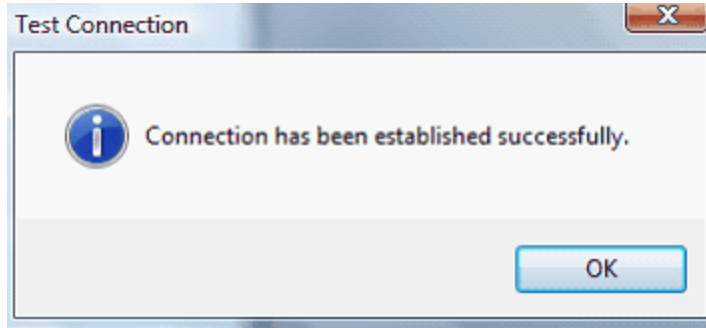
3. Select New Connection



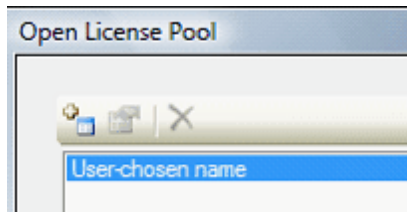
4. Enter the SQL server name, connection provider (database driver), and database identification information (as requested in the form shown below), to automatically generate a connection string. **Note** if your SQL Server is configured to use TLS1.2 encryption then you will need to set the connection provider to be SQL Server Native Client in the drop down list box.



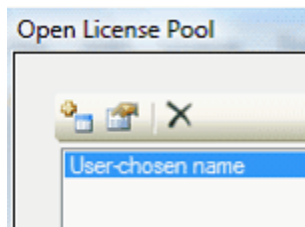
5. Click on “Test Connection”



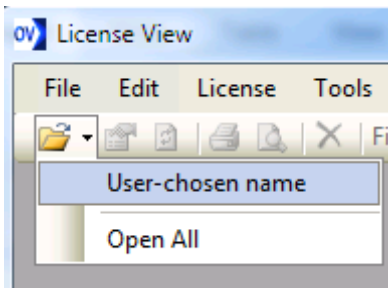
6. Once you receive notification of a successful test connection, click on OK within the notice and on OK within the main Connection Properties dialog to register the new database connection information into LicenseView.



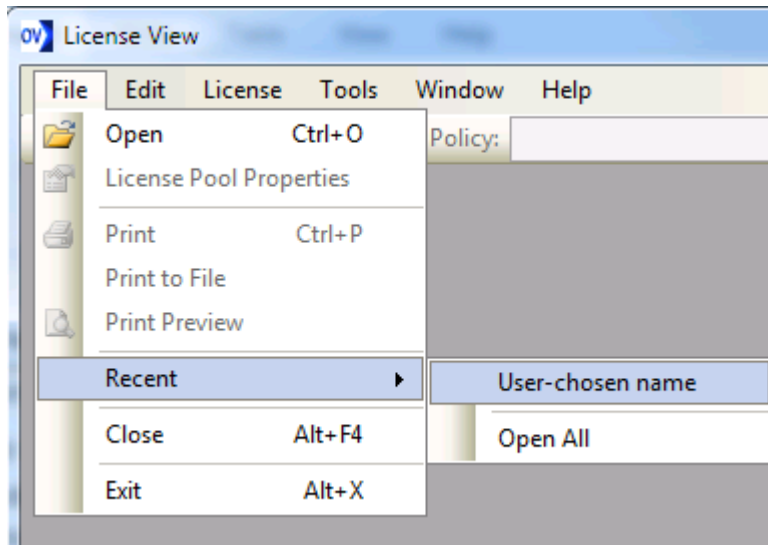
7. Thereafter, open the database via File, Open



OR the Open icon,



OR File, Recent



To see the license pool:

Serial Number	User ID	Machine Name	Terminal Session ID	License Expiration	Lease Expiration	Lease Obtained	Last Logged In
900100000272				11/23/36	12/14/16	12/07/16 8:51 AM	12/07/16 8:51 AM
900100000373				11/23/36	01/01/00		

2.7 Enterprise Updates and Upgrades

Enterprise Updates and Upgrades

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

Updates and Upgrades

Enterprise architecture provides the convenience of **automatic updates of maintenance releases**.

Each time a user launches OutsideView, the program checks the user's local files against those contained in the network Profile share. If the Profile share files have been changed through [Supervisor Mode](#), the new files are automatically downloaded to the client workstation.

If the Media share has been updated with a new maintenance version, all members of the Profile whose Windows user account permits software installation can automatically update to that new version. For cases where the user may be on a low-bandwidth connection, an option in the User Privileges definition will allow the user to postpone the update.

The contents of the default OutsideView Profile folders (Capture / Components / Download / Macro / Param / SSH Store / Upload) are also automatically updated. However, if you have created subfolders within these default folders, the subfolders will not automatically copy down to the local machines.

2.7.1 Maintenance updates

Maintenance updates

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

Automatic Updates of OutsideView Maintenance releases

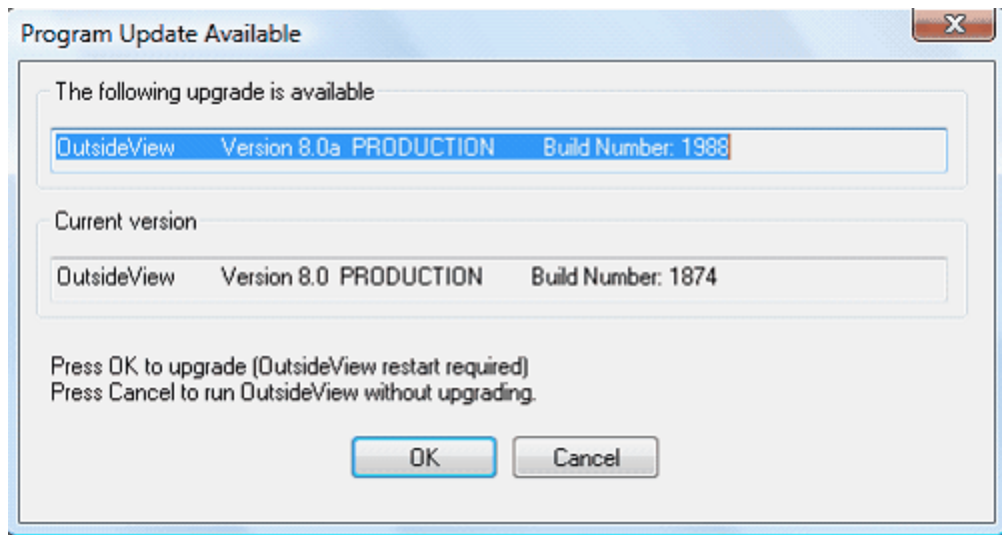
OutsideView Enterprise will automatically present an update option to all end-users of an Enterprise profile (except WTS and Citrix users) after the Media folder at the Enterprise share is updated with a new **maintenance** (e.g. 9.0a to 9.0b) update.

NOTE: Increased user controls implemented by Microsoft limit this capability, in recently released operating systems, to users permitted to install software. For instance under Vista, users must have been given membership in the Administrators or Power Users group.

To update all OutsideView Enterprise clients to a new **maintenance update (patch)** of the application, simply:

- Obtain the new release and navigate to its \Enterprise\MEDIAFOLDER folder.
- Copy the **OutsideViewSetup.exe**, and the **version.dat** file from that location to the Enterprise installation's Media folder.
- Copy the file UpdateNNNN.exe to the Enterprise installation's Media folder.

Enterprise end-users running the prior release will, upon their next start of OutsideView, be notified of the new release's availability and given the opportunity to update:



Note: These instructions apply only for updating to new Maintenance releases (e.g. moving from version 9.0 to version 9.0a or b or c). They do not apply to upgrading to new Major releases, such as from OutsideView 8.2 to OutsideView 9.0. or Feature Upgrades (e.g., 9.0 to 9.1) **Major** and **Feature** Upgrade releases typically require reinstallation.

Note: The auto-update feature has been disabled for Citrix and Windows Terminal Server environments due to the fact that there can be no active users while performing an auto-

update. In those environments, update each terminal or Citrix server in the same manner that the applications were originally installed:

- While no users are using OutsideView, uninstall OutsideView
- Run the 'Install OutsideView' via the Add Programs wizard within the Control Panel.
- If the descriptive Information contained in the Published Citrix Application becomes out of date, delete and re-publish the application.

2.7.2 Feature Upgrades

Feature Upgrades

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

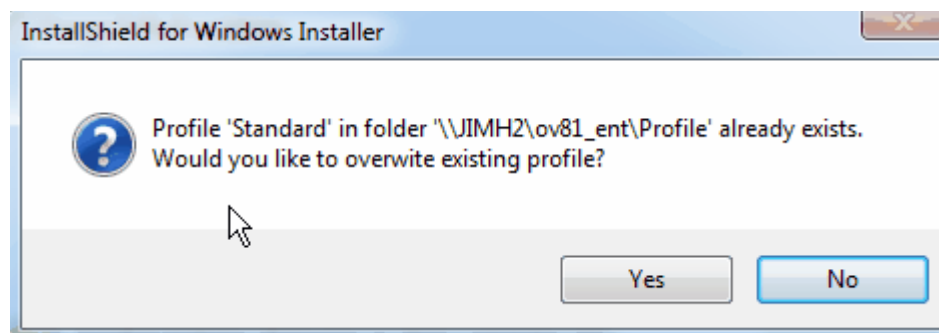
It is not necessary to create a new sharepoint when installing a new Feature (9.0 to 9.1) release.

New Feature upgrades can be installed over existing, earlier versions. You can retain your Profiles data and easily import your new License information..

- 1) Assure you have an NLPC number containing licenses of the appropriate level (The first two digits of the NLPC number indicate release level)
- 2) Rename the existing Media folder (for example, to Media_81c).
- 3) If you are using classic licensing, rename the existing License folder (for example, to Licenses_81)
- 4) Conduct a standard Enterprise Installation, specifying the same share point

If you want to retain your existing profile(s) you may. Simply fill in the installation prompt for profile name appropriately.

When installing over an existing profile, the installation process will caution you:



Select "Yes" to continue, with the new installation referencing to the pre-existing profile and its contents.

- 5) Conduct your end-users installations, as per usual.

Users with software installation rights may navigate to, and click on, the installation shortcut:

```
\\[server_name]\[sharepoint_name]\Profile[profile_name]\install\Install OutsideView
```

Administrators may also 'push' the installation shortcut to end-users' workstations.

2.7.3 Major Upgrades

Major Upgrades

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

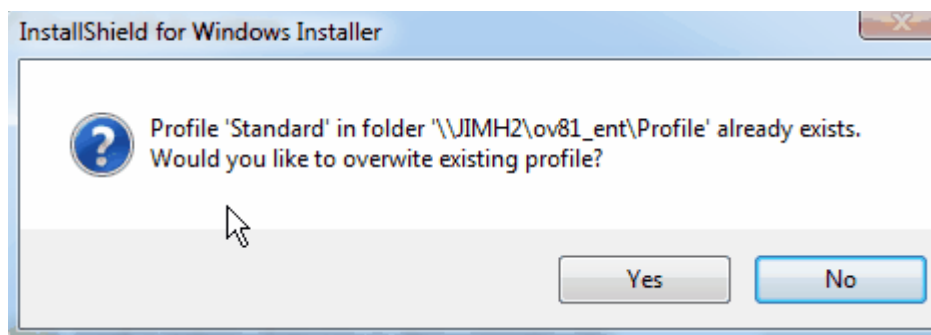
It is not necessary to create a new sharepoint when installing a new Major (8.x to 9.0) release.

New Major upgrades can be installed over existing, earlier versions. You can retain your Profiles data and easily import your License information..

- 1) Assure you have an NLPC number containing licenses of the appropriate level (The first two digits of the NLPC number indicate release level)
- 2) Rename the existing Media folder (for example, to Media_80c).
- 3) Rename the existing License folder (for example, to Licenses_80)
- 4) Conduct a standard Enterprise Installation

If you want to retain your existing profile(s), such as Standard, you may. Simply fill in the installation prompt for profile name appropriately.

When installing over an existing profile, the installation process will caution you:



Select "Yes" to continue, with the new installation referencing to the pre-existing profile and its contents.

- 5) Conduct your end-users installations, as per usual.

Users with software installation rights may navigate to, and click on, the installation shortcut:

```
\\[server_name]\[sharepoint_name]\Profile[profile_name]\install\Install OutsideView
```

Administrators may also 'push' the installation shortcut to end-users' workstations.

2.7.4 Citrix \ Windows Terminal Server Updater Notes

Citrix \ Windows Terminal Server Updater Notes

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

The auto-update feature has been disabled for Citrix and Windows Terminal Server environments due to the fact that there can be no active Citrix or WTS clients while performing an auto-update. In Citrix and WTS environments, update each terminal or Citrix server in the same manner that the applications were originally installed:

- While no users are using OutsideView, uninstall OutsideView
- Run the 'Install OutsideView' via the Add Programs wizard within the Control Panel.
- If the descriptive Information contained in the Published Citrix Application becomes out of date, delete and re-publish the application.

2.8 Moving Enterprise Installations

Moving Enterprise Installations

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

At times, organizations may need to move their OutsideView Enterprise installations from one server to another.

To move the shared Windows folder containing the Enterprise central configuration information and profiles, this may be done one of two ways;

- If the original Enterprise share point (windows shared folder) is replicated, with identical properties, onto a new server **with the same UNC name** as the original server, the relocation will be transparent to OutsideView.
- If the new server must have a new UNC name, end users may be automatically notified of the change, by creating a file named redirect.dat, and placing it into the original sharepoint's Media subfolder. Once this file is in place, then the next time a user starts their end-user Enterprise copy of OutsideView, the PC will automatically download the redirect file, and update its internal OutsideView registry settings - causing it to permanently point to the new server share point.

- Over time, therefore, all users pointing to the original server will be redirected automatically and permanently to the the new server.
- Once all users have been redirected, the original Enterprise share point is no longer needed.
- The redirect.dat file is a text file with the structure;

```
NETWORKPATH = \\W7bit64\OV81GEnt_New\Profile
LicenseDatabase = \\w7bit64\ov81gent_New\Licenses\LICENSEPOOL.cpf
```

For Enterprise installations using **SQL licensing**, the license database may (or may not) also need to be moved.

- Clone the original OutsideView Enterprise license database, with all users rights and permissions exactly preserved, onto the new SQL server.
- Create the file redirect.dat, and place it into the original server's Profiles folder. Once this file is in place, then the next time a user starts their end-user Enterprise copy of OutsideView, the PC will automatically download the redirect file, and permanently update its internal OutsideView registry settings, for both the share point and the license database.
- Over time, therefore, all users pointing to the original server will be redirected automatically and permanently to the the new server and new SQL server.
- Once all users have been redirected, the original Enterprise share point and original SQL database is no longer needed.
- The redirect.dat file is a text file with the structure;


```
DBCONNECTIONSTRING = Driver = {SQL
Server};server=SERVER_NAME;trusted_connection=True;database=DATABASE_
NAME
NETWORKPATH = \\W7bit64\OV81GSQL_New\Profile
```

Steps to use this feature:

1. Create a text file named 'redirect.dat' following the format shown in the sample above. Note the following for the redirect.dat file:
 - An exclamation point prefix character defines a comment line.
 - Leading/trailing whitespace is ignored for both comments and data lines.
 - Valid key words (left side of first '=') are not case sensitive.
 - Non-valid key words and blank lines in the file are ignored.
 - Configuration data strings (right side of first '=') are case sensitive.
 - For multiple valid key word entries, the last entry in the file will be used.
 - The key words are independent of each other. Use one, the other, or both.
 - The order of the key words does not matter.
 - A file with no valid key words or all comments results in no action taken.
 - Cannot use DBCONNECTIONSTRING and LICENSEDATABASE in the same file.
2. Create a new network sharepoint at the location specified by NETWORKPATH. Give this new sharepoint the same permissions as the original sharepoint. Remember to include the '...\Profile' suffix in the NETWORKPATH line in 'redirect.dat'.
3. Place the 'redirect.dat' file into the original sharepoint's Media subfolder. This is the same location as the 'version.dat' file.

4. Launch OV via SplashScreen. If OV is executed directly from 'outcore.exe' the redirection will not occur.
5. After OV start-up, check the following registry locations. Each one should refer to the new network sharepoint as defined in the 'redirect.dat' file under the NETWORKPATH key word. Note that the 'Failover' value should always be '0' after a successful redirection operation. The HKLM keys will be located under the 'HKLM\Software\Wow6432Node' registry key for 32 bit version of OutsideView on 64-bit machines:
 - a. HKCU\Software\Crystal Point\Licensing\OutsideView\9.0 -> LicenseDatabase
 - b. HKCU\Software\Crystal Point\OutsideView\9.0 -> NetworkPath
 - c. HKLM\Software\Crystal Point\Licensing\OutsideView\9.0 -> DBConnectionString
 - d. HKLM\Software\Crystal Point\Licensing\OutsideView\9.0 -> LicenseDatabase
 - e. HKLM\Software\Crystal Point\OutsideView\9.0 -> Failover (always = '0')
 - f. HKLM\Software\Crystal Point\OutsideView\9.0 -> Name
 - g. HKLM\Software\Crystal Point\OutsideView\9.0 -> NetworkPath
6. As mentioned above, redirection is a permanent operation. The only way to move back to the original network sharepoint would be to create a new 'redirect.dat' configuration file that points back to the original sharepoint and place it into the new (now current) Media subfolder and restart OV.
7. Because this is not a failover operation, it is possible to also perform a patch update operation together with a redirection operation. Just prepare the redirect file normally, then before copying it to the original Media subfolder first place the patch update files into the new sharepoint location as normal. After 'redirect.dat' is in place, running OV will then first redirect from the original sharepoint to the new sharepoint, then the patch update will be applied from the new sharepoint, all in a single OV start-up. Note that patch updates located in the original sharepoint will be ignored, since the sharepoint redirection operation occurs first.

3 Enterprise Administration

3.1 User Profile Administration

3.1.1 Supervisor Mode

Supervisor Mode

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

Supervisor Mode

After an Enterprise install has created a profile, OutsideView may be installed to a workstation by executing the "Install OutsideView" shortcut in the install subfolder of that profile.

Once OutsideView has been installed to a workstation, that workstation may invoke a special Supervisor Mode to create or modify OutsideView configuration files (sessions, workspaces, macros, etc.) within a specific profile of the Enterprise share location or 'hub'. Once created or modified, such files are thereafter automatically deployed to all members of that specific profile.

"Supervisor Mode" is invoked via an executable automatically created in the Install subfolder of each specific Profile. When Supervisor mode is started, it initiates the regular OutsideView software, but with specific run-time switches, to automatically set file location pointers to the relevant profile sub-folders at the Enterprise share point.

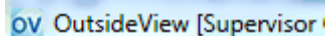
Caution: Do NOT run simultaneous instances of OutsideView - mixing Supervisor mode and client mode, or mixing Supervisor mode for differing profiles. Whichever instance of OutsideView is initiated last will reset file location pointers for ALL instances, causing confusion.

Running the Supervisor Mode executable for a particular profile will launch OutsideView in Supervisor Mode for that profile. Any configuration files created or modified via Supervisor mode are stored within the Config subfolder of that specific profile. For instructions on creating OutsideView sessions, workspaces and other user configuration files, please see the OutsideView Users Guide. For instructions on creating or editing Visual CommBasic macros, please see the Visual CommBASIC Reference manual.

Each time members of a profile start their local copy of OutsideView, it will automatically replicate (or update) any configuration files in the Config subfolder of their profile down to their own local storage, where it is immediately available for use.

This allows administrators to create or modify configuration files ONCE, and know that all members to that profile will automatically acquire those files (or updates) when they next start OutsideView. There is no need to distribute or update the files via any other methodology. Many organizations use this capability to assure that end-users have 'known-good' configuration files, in addition to whatever configuration files the end user might create for himself. Other organizations remove the user privilege of creating their own configuration files to enforce the end-users will only use the centrally-supplied, Supervisor mode created files.

The OutsideView title bar will indicate "[Supervisor]" when launched in Supervisor Mode.

The image shows a close-up of a window title bar. The text in the title bar is "OV OutsideView [Supervisor]". The "OV" is in a blue box, and "OutsideView" is in a light blue box. The "[Supervisor]" part is in a darker blue box.

The Privileges defined for a profile will apply whenever OutsideView is launched, including within Supervisor Mode (to allow testing).

If “Privileges” are to be defined or modified for members of a user profile, it will be necessary to enter [Override Mode](#) to allow that functionality.

NOTE: Be careful if using SUPERVISOR MODE in combination with the Application setting “Open Last Workspace”. If you use Supervisor mode to open a workspace (from the central share) and later start OutsideView on that same workstation in client mode with “Open last workspace” checked ON, the last workspace is STILL the Enterprise share one, even though your current settings are pointed locally. Either do not use “Open Last Workspace” on the PC where you use Supervisor mode or get in the habit of an explicit “File, Open Workspace” each time you start OutsideView following a Supervisor mode session.

3.1.2 Override Mode

Override Mode

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

Override Mode

Troubleshooting a user’s local OutsideView configurations may require overriding the permissions defined in the Profile’s Privileges. An Override Mode is provided to allow full local rights to modify or create OutsideView configuration files regardless of the permissions defined. The only exception to this capability is lockdown mode in which virtually all user menus and permissions are disabled.

To enter Override Mode:

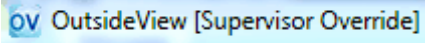
1. Start OutsideView
2. Select Default Application Settings and click on the Settings tab.
3. In the Settings tab, select the check box for "Enable Override Mode" and click "OK".
4. In the "Enter Override Password" dialog, enter the password (the default password is "crystal") and click "OK".
5. Once you have entered Override Mode, the OutsideView title bar will indicate "[Override]"

Supervisor Override Mode

In OutsideView’s Supervisor mode, profile permission restrictions are in effect so that Administrators may test configurations efficiently. Therefore, modification of those user permissions and/or profile membership is conducted in a special Supervisor sub-mode; Supervisor Override Mode.

To enter Supervisor Override Mode:

1. Start Supervisor Mode
2. Select Default Application Settings and click on the Settings tab.
3. In the Settings tab, select the check box for "Enable Override Mode" and click "OK".
4. In the "Enter Override Password" dialog, enter the password (the default password is "crystal") and click "OK".

5. Once you have entered Override Mode, the OutsideView title bar will indicate "[Supervisor Override]". 
6. Select Default Application Settings (Again) and click on the newly-visible User Privileges or Client Administration tabs.

It is strongly recommended to change the Override Mode password to something other than the default. To change the Override Mode password:

1. Select Default Application Settings and click on the "Client Administration" tab.
2. Select the "Change Override Password" checkbox and click "OK".
3. Complete the fields in the "Change Supervisor Override Password" dialog and click "OK".

3.1.3 Override Application Settings

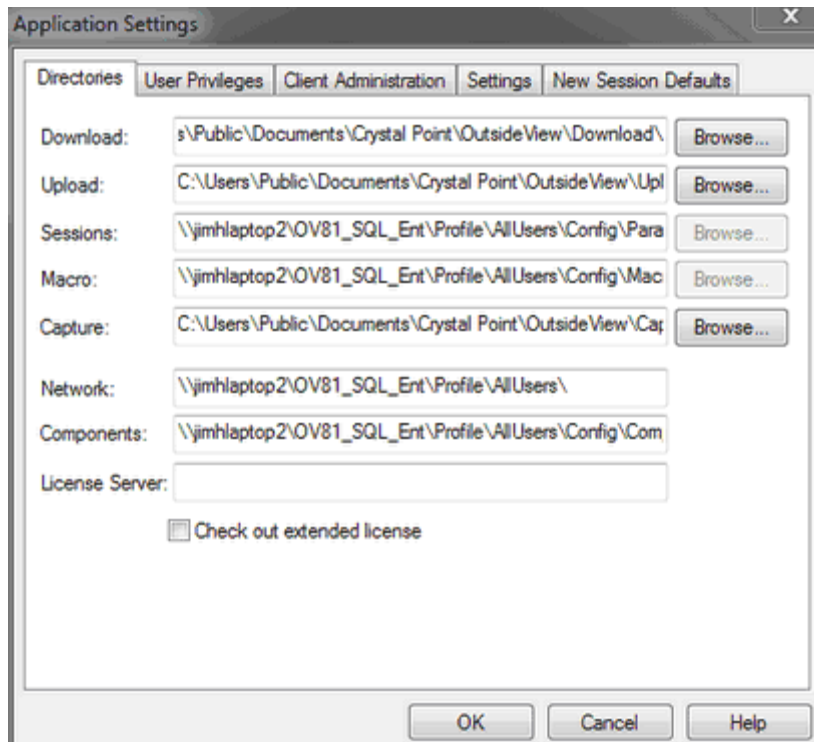
Override Application Settings

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

Override Application Settings

When you enter Edit, Application Settings the second time, after enabling override mode, your available choices have changed.

You now see:



The tabs for **Directories**, **Settings** and **New Session Defaults** apply only to the workstation on which you are running OutsideView.

These three tabs are primarily displayed for informational purposes. However, any changes made to these tabs will take effect within that specific workstation.

The tabs for **User Privileges** and **Client Administration** are the key dialogs for controlling Profile behavior.

3.1.3.1 Directories tab

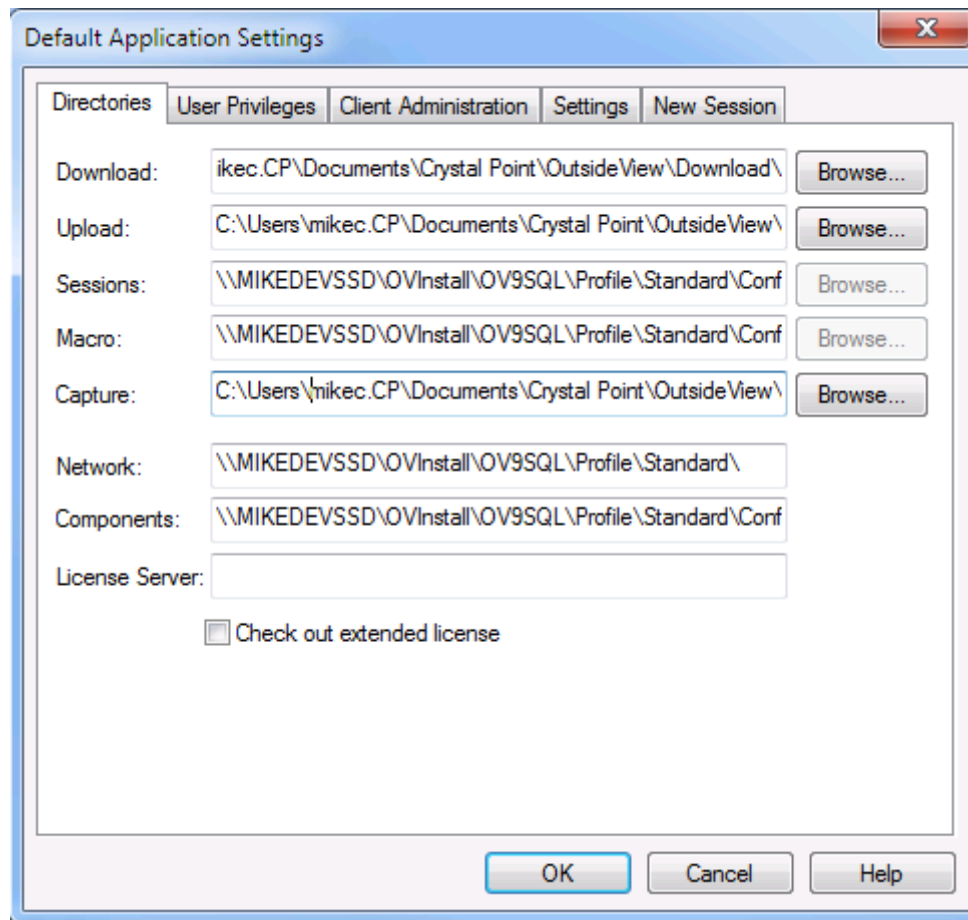
Directories tab

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

Directories tab

The **Directories** tab lets you see 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 application data area. This tab is displayed within Supervisor Override mode in case you need the information within. However, any changes you make in this tab apply only to this specific workstation and this specific instance of OutsideView. These settings are **not** propagated to all profile members.



3.1.3.2 User Privileges

User Privileges

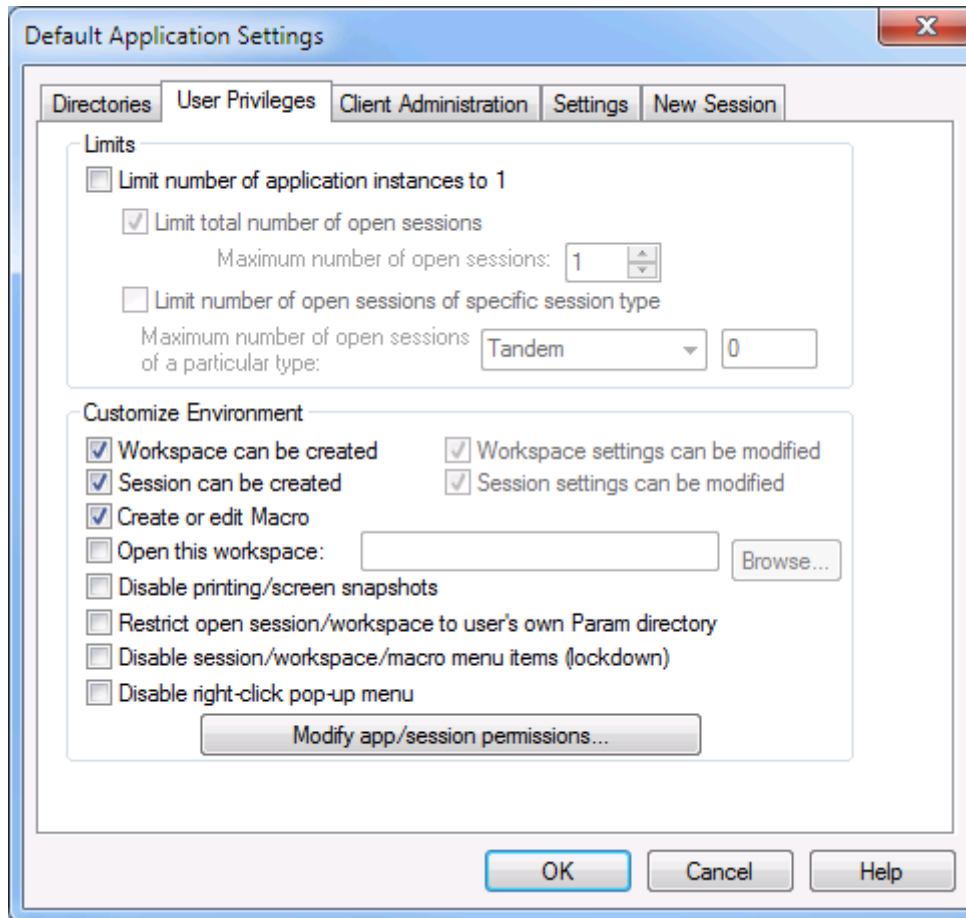
[Top](#) [Previous](#) [Next](#)

User Privileges

To modify the User Privileges (i.e, user permissions)for members of an OutsideView user profile, OutsideView must be in Supervisor Override mode.

- For instructions on launching OutsideView in Supervisor mode, click [here](#)
- For instructions on entering Supervisor Override mode, click [here](#).

To access the User Privileges dialog, first enter Supervisor, Override mode, then select **Edit: Application Settings** and click on the User Privileges tab.



This is an itemized description of the User Privileges settings and their impact on OutsideView behavior on client PCs.

User Privileges – Interpretation of Settings

- **Limit number of application instances to 1:** This allows users to start only one instance of OutsideView at a time. One instance must be closed before another can be opened.
- **Limit total number of open sessions:** This is a restriction to be applied on Open Session and New Session to restrict the number of sessions a user can have open simultaneously. (If an attempt is made to open any session (including a retained but not-yet-open session) which would exceed the limit, a dialog box displays stating that the limit would be exceeded and the user must first close a session before proceeding. The number of independent FTP sessions is not limited by this setting; users can have any number of FTP-only sessions open.
- **Limit number of open sessions of specific session type:** Like the previous restriction, this restricts the number of sessions of a particular emulation type that a user can open. Use the drop down button to select the emulation of interest and then enter the maximum number of active sessions of that type in the text box. If this setting is changed, it will take effect the next time OutsideView is launched.
- **Workspace can be created / workspace can be modified:** The valid combinations of these settings are listed below.

Workspace can be created?	Workspace can be modified?	Disallowed operations	Allowed operations
---------------------------	----------------------------	-----------------------	--------------------

Yes	Yes	No restrictions	All
Yes	No	<invalid setting combination>	<invalid setting combination>
No	Yes	New Workspace... Close Workspace Session: Load Session: Unload Changing of workspace startup macro	Save Workspace... Save Workspace As... Modification of toolbars (including macro bindings) Modification of workspace settings
No	No	New Workspace... Close Workspace Session: Load or Session: Unload Changing of workspace startup macro Save Workspace... Save Workspace As... Editing of toolbars (including macro mappings)	Repositioning and changing active set of toolbars Modification of workspace settings

- **Session can be created / session settings can be modified:** The valid combinations of these settings are:

Session(s) can be created?	Session settings can be modified?	Disallowed operations	Allowed operations
Yes	Yes	No restrictions	Everything
Yes	No	<invalid setting combination>	<invalid setting combination>
No	Yes	New Session... Changes to IO, Protocol or Emulator types (on Session tab of Session Settings dialog box) Changing of session startup macro Changing of language setting Modifications to any IO and Protocol settings	Save Session... Save Session As... Supervisor selection of Modifiable User settings Repositioning and sizing session window, including maximizing, minimizing and closing the session window
No	No	New Session... Save Session... Save Session As... Changing of session startup macro Changing of language setting All Session Settings are read-only. This means the following are not allowed:	Repositioning and sizing session window, including maximizing, minimizing and closing the session window Repositioning and changing active set of toolbars via View: Toolbars)

1. Modifications to Emulator, I/O or Protocol settings
 2. Modifications to or creation of color scheme and keyboard map
 3. Modifications to toolbars via the Session Settings dialog box
 4. Modifications to property pages (Summary Information) of color, toolbar, keyboard map and session files
- Editing of toolbars (including mapping macros)

- **Create or Edit macro:** If unchecked, the Macro Editor menu item is disabled.
- **Open this workspace:** This allows a network administrator to specify what workspace a client PC should open when the OutsideView application is launched. This setting is overridden by command line arguments that start a specific session, workspace, or macro.
- **Disabling Printing and Screen Snapshots:** Check ON “Disable printing/screen snapshots” to activate this restriction for all members of this profile.
- **Restrict users to opening parameter (session and workspace) files from within their own directories only:** Check ON “Restrict open session/workspace to user’s own Pram directory” to activate this restriction for all members of this profile
- **Disable session/workspace/macro menu items (lockdown):** Within the User Privileges dialog, accessed via Supervisor, Override mode, if the checkbox to “Disable session/workspace/macro menu items (lockdown)” is checked ON, then members of this profile will only have access to the menu items File->Exit OutsideView, and the Windows and Help menu items. All other Menu items will be disabled (grayed out)

It is the intention for this mode that users are not able to do anything but operate whatever software is presented to them within the workspace and session(s) opened automatically for them. In lockdown mode users cannot even select session or workspace files to open. OutsideView administrators must pre-create any desired workspace and session files, using Supervisor Mode, and identify (via the User Privileges dialog) which workspace is to be automatically opened by users.

This mode of operation in combination with a SSL/SSH encrypted circuit is suitable for an extremely high-security environment, effectively eliminating all avenues for transfer of data from OutsideView via copy/paste, logging, printing, or network trace.

NOTE: Once lockdown mode is enabled, you must enter Supervisor Override mode to modify these settings.

- **Disable right-click pop-up menu:** Clicking this option ON to disable right-click menus.

Detailed Control over User Privileges

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

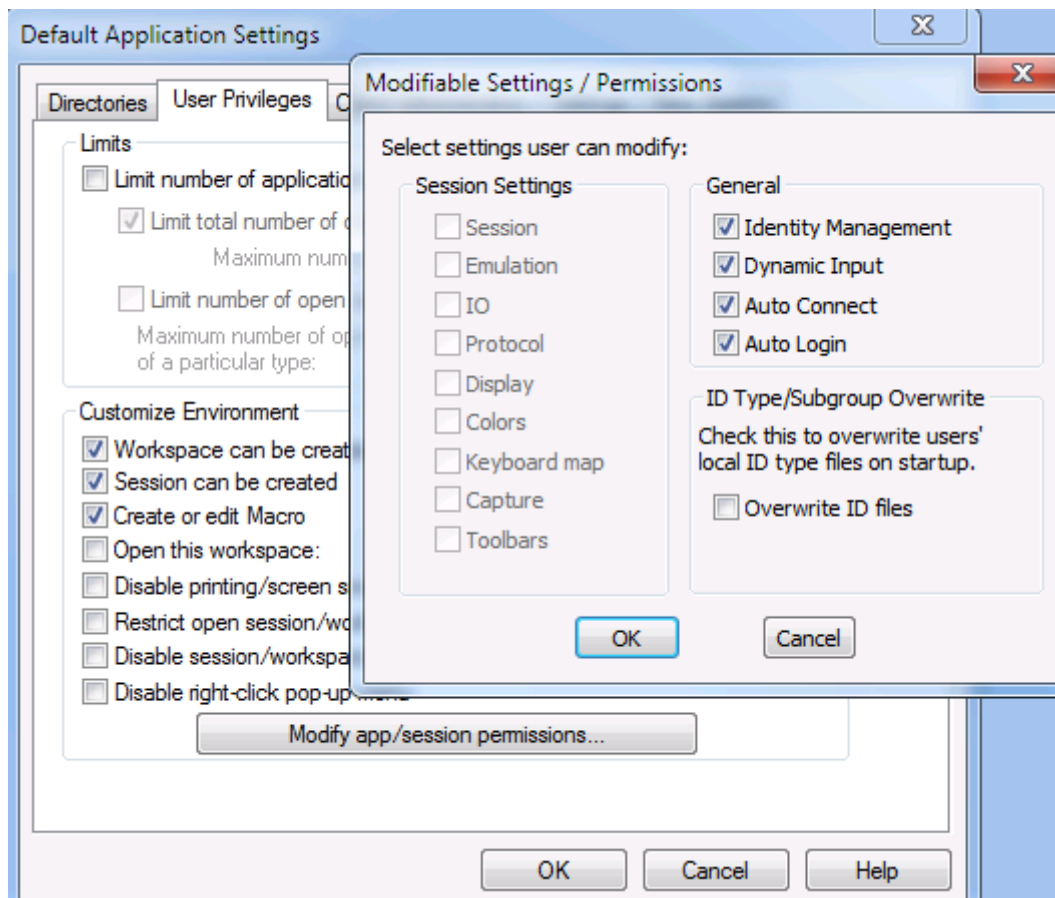
Detailed Control over User Privileges

To enable detailed user privileges control, the “Session can be created” checkbox must be OFF, and the “Session settings can be modified” checkbox must be ON.

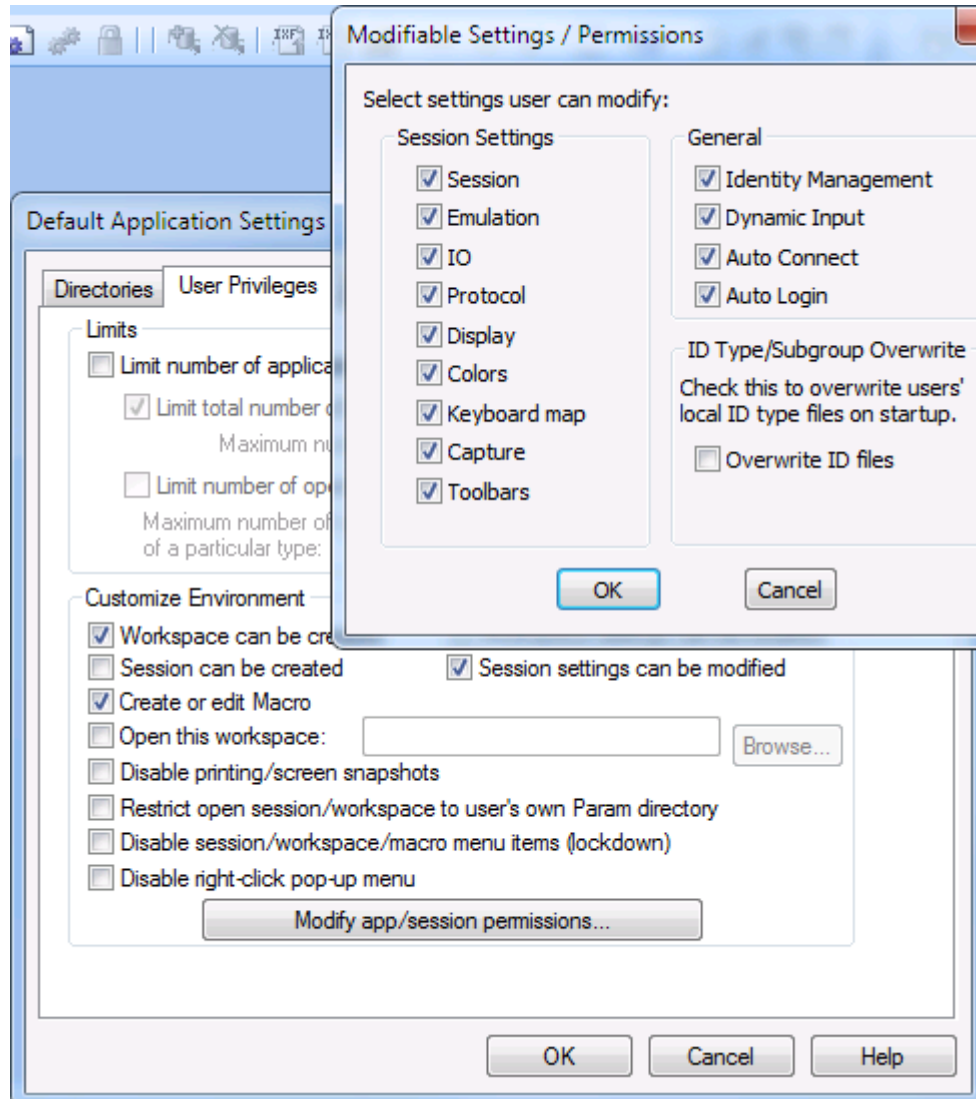
NOTE: Enabling the “Session can be created” checkbox overrides the “Select modifiable session settings” dialog, and give users permission to set all settings.

NOTE: Checking ON the option to “Disable sessions/workspace/macro menu items (lockdown)” which is discussed in the topic [Additional User Privileges](#), will remove user access to both preference and configuration settings. When detailed user privilege control is desired, therefore, we recommend a customized toolbar (containing only preference settings icons) rather than a complete disabling of all menu and toolbar items (lockdown mode).

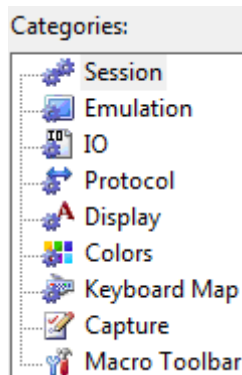
With “Session can be created” **ON**, click on the “Modify app/session permissions...” button, to see the Modifiable Settings dialog, below:



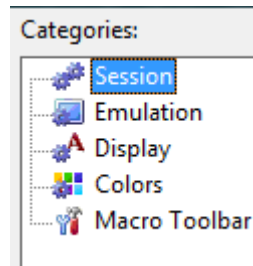
With “Session can be created” **OFF**, and “Session settings can be modified” **ON**, click on the Modify app/session permissions...” button, to see the Modifiable Settings dialog, below:



Those configuration categories checked ON as Modifiable would be available to end-user members of this profile, when they select Session, Session Settings from their toolbar, as illustrated below.



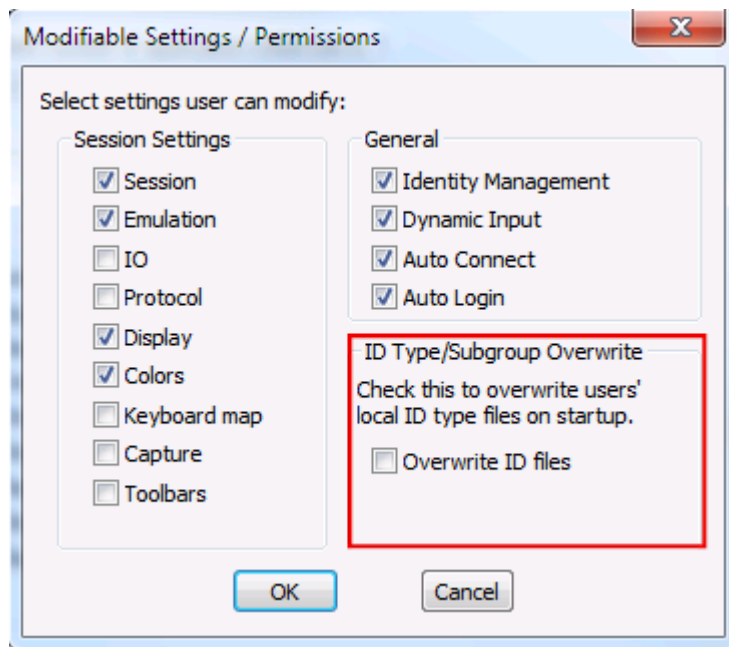
Potentially available User Configurable Categories
Configurable Categories



Example Customized

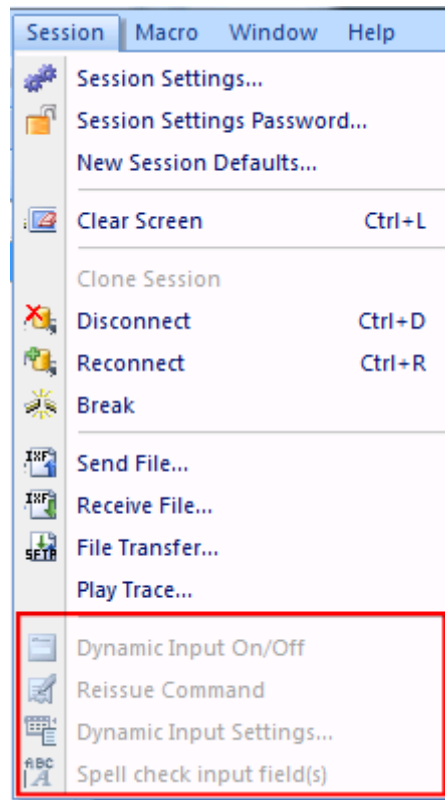
ID Type Centralized Control

By checking the box shown below, each time the Supervisor uses Supervisor mode to create/modify the central list of ID types or Roles, that list will be distributed (overwriting) to all end-users. When this box is checked on, the General Setting permission for users over Identity Management is typically off.



The **General Settings**, when not checked ON, will be disabled for end-users. For instance, if Dynamic Input is not checked, users will see their Dynamic Input icons disabled, and the menu option Session will have its Dynamic Input choices disabled;





3.1.3.2.2 Detailed User Privileges Control - Implementation notes

Detailed User Privileges Control - Implementation notes

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

Detailed User Privileges Control - Implementation notes

Privileges file

The file PRIVILEGES.CPG contains the user privileges settings, for each profile. (Different profiles can have different permissions.) The structure, size, and format of this file have not changed. The detailed user privileges control feature was engineered in such a way as to permit the use of an old PRIVILEGES.CPG file, applying the default settings for the new privileges.

The new settings are read from and written to the existing structure of the file. Whatever levels of user privilege are afforded by that file will apply to the new settings.

Changes made to the privileges.cpg file will be recognized by each OutsideView 'client' the first time OutsideView is restarted after all other active copies of OutsideView on a given workstation have been closed.

User Preference Files

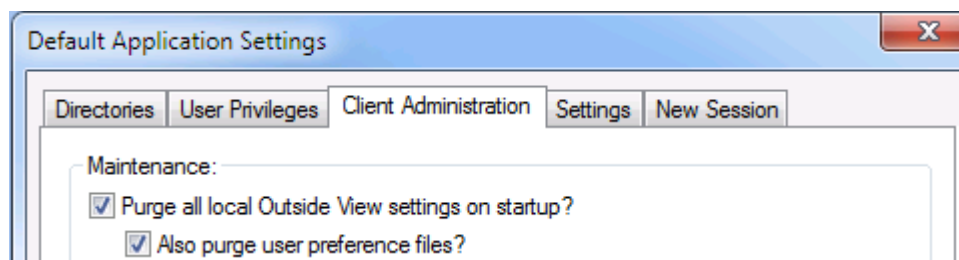
Workspace files are stored as .cpw (Crystal Point Workspace) files. Workspace files record which sessions are to be started, and how they are to allocate screen space. Sessions are

stored as .cps (Crystal Point Session) files. In an environment where detailed user control is implemented, such files would typically be created and maintained by the OutsideView administrator, using Supervisor Override mode. The administrator creates or maintains a single instance of each needed session or workspace file (per profile) at the network-shared, central Enterprise installation location.

Configuration of a session may automatically generate component sub-files when values such as colors, toolbars, or keyboard map are customized. These files are stored in the Component folder. Such Color or Toolbar and Keyboard sub-files are stored with .cpc, .cpt, and .cpk extensions respectively (Crystal Point Color, Crystal Point Toolbar, Crystal Point Keyboard).

Whenever OutsideView is started by an end-user, that end-user receives (or updates) a local copy of all configuration files from their Enterprise profile. Session and workspace files are stored in each end user's local Param folder. Any component sub-files are stored in the end user's local Component folder.

When an end-user modifies **any** 'Preference' settings within a session file, **all** user-controlled 'Preference' settings are saved, using the same base file name as that of the modified file, but with a new extension. For instance, session_one.cps is stored as session_one.cus. At this point, the end-user has taken control of all preference settings. Even user settings not explicitly changed are treated as 'confirmed' and stored on the user's behalf. Supervisors can retrieve control over those settings only by using Supervisor, Override mode to reset (i.e., delete) the local user preference file:



User-modified session files have a .cus (CrystalPoint User Session) extension, and are stored in the Param folder. User-modified color, toolbar or keyboard map settings are stored as .cuc, .cut or .cuk (CrystalPoint User Color, CrystalPoint User Toolbar or CrystalPoint User Keyboard) files, in the Component folder.

These files are simply configuration files with a different extension, never seen or manipulated directly by the user. A .cus file will have a one-to-one correlation with a .cps, and will only exist if the user makes and saves changes to session settings.

In previous releases, OutsideView Supervisors and Users had to choose between using centrally supplied and updated sessions, or using local sessions with locally defined settings, but no automatic updating. That is no longer the case.

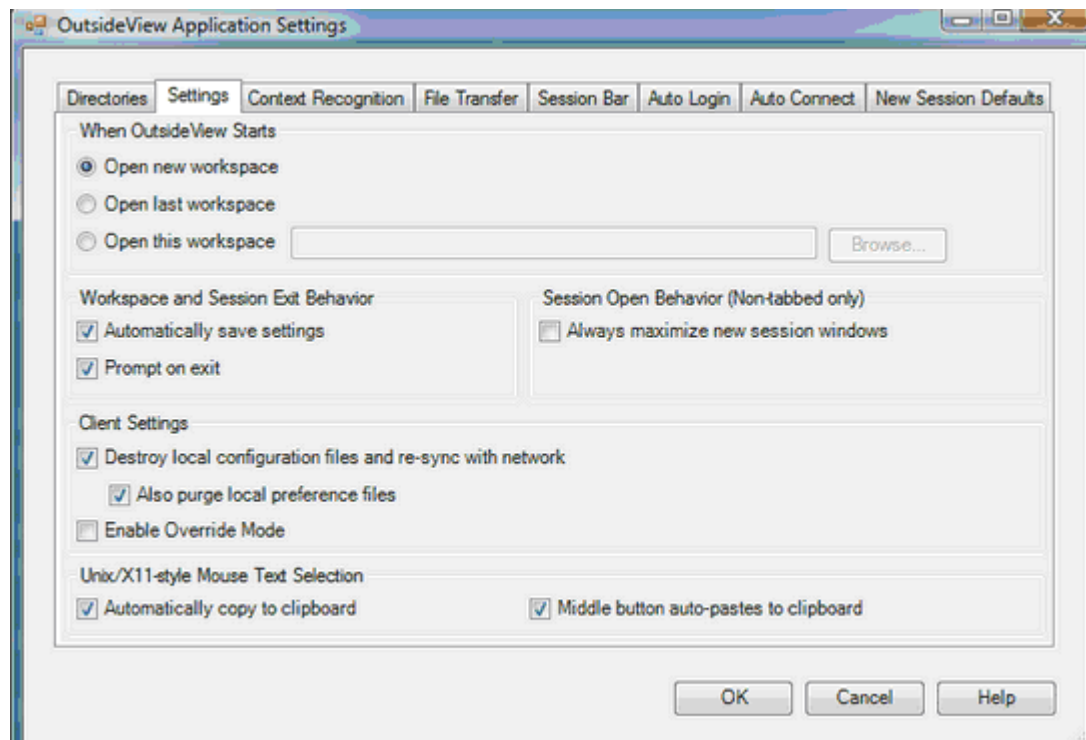
These 'user modifier' files enable an optimum operational environment; maximizing administrative efficiency and operational control while preserving the desired level of user flexibility. An OutsideView Supervisor defines/modifies a single session file that is automatically available and dynamically updated for all profile members, while those profile members retain the flexibility to modify those settings – WITHOUT LOSING THE AUTOMATIC UPDATE linkage with the base session settings.

If an end-user does modify any of the 'user preference' settings, the automatic update linkage back to the profile-level session file is still preserved. Any changes the administrator subsequently makes to the profile-level session file will still automatically be distributed to the appropriate end-users. The user preference files will remain effective, too, modifying the updated session file.

Session and User Preference File Housekeeping

Workspace, session, and user preference files may be purged from all users (profile-wide) by the Supervisor, if desired, by entering Supervisor Override mode and the Client Administration tab. There, the Supervisor can impose a 'housekeeping' cycle (in effect until the switch is unchecked) where end-user workspace, session and sub-component files are deleted and reacquired – profile-wide - upon each OutsideView start. There are separate options to include the user preference files or not.

The purpose of this capability, called 'pristine-mode,' is so that Supervisors can clear out old files that may be in use within a profile group. For instance, when implementing Enterprise level controls, it might be appropriate to clear out previous user-built session files. Session and user preference files may also be cleared out by the User, if desired, by entering Edit, Application Settings, and choosing the Settings tab. There, the user can impose a 'housekeeping' cycle (in effect until the switch is unchecked) where workspace, session and sub-component files, for that individual user only, are deleted and reacquired upon each OutsideView start. There are separate options to include the user preference files or not.



Client Settings User dialog for forcing individual purge of local settings files (with or without user preference files)

The purpose of this capability is to let individual end-users 'clean house' and force a fresh download of session files from the central Enterprise location.

3.1.3.2.3 Additional User Privileges

Additional User Privileges

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

Additional User Privileges

In Supervisor, Override mode, there are additional user privileges that can be fine tuned.

- Disable printing/screen snapshots
- Restrict open session/workspace to user's own Param directory
- Disable session/workspace/macro menu items (lockdown)
- Disable right-click pop-up menu

These settings work in the following way:

Disable printing/screen snapshots

Just as implied, checking this option ON will disable the user's permission to print OutsideView screens.

Restrict open session/workspace to user's own Param directory

This option prevents users, when attempting to open a session or workspace, from browsing outside their default folders for session or workspace files located elsewhere.

Disable session/workspace/macro menu items (lockdown)

This option sets users into 'lockdown' mode, our most restrictive user environment. In lockdown mode, users have very few permissions. Supervisors **MUST** specify a specific workspace to open for the user. While in that workspace, users only have the ability to access Help, rearrange sessions windows, and exit OutsideView. The OutsideView Menu bar appears, but virtually all options are disabled, with the exception of Exit, Text Select options, the ability to select the in-focus window, and Help options.

CAUTION: Since lockdown users do not have the option to open sessions or workspaces, Supervisor **MUST** specify a workspace to open.

In Lockdown mode, it is likely Supervisors will also want to uncheck the "Workspaces can be modified" and "Session settings can be modified" options that would, otherwise, permit transient changes to sessions and workspaces.

Lockdown privileges, typically, would look like:

Customize Environment

- Workspace can be created
- Workspace settings can be modified
- Session can be created
- Session settings can be modified
- Create or edit Macro
- Open this workspace: \OutsideView\Param\ENT_ws1.cpw
- Disable printing/screen snapshots
- Restrict open session/workspace to user's own Param directory
- Disable session/workspace/macro menu items (lockdown)
- Disable right-click pop-up menu

and would be accompanied by a customized toolbar.

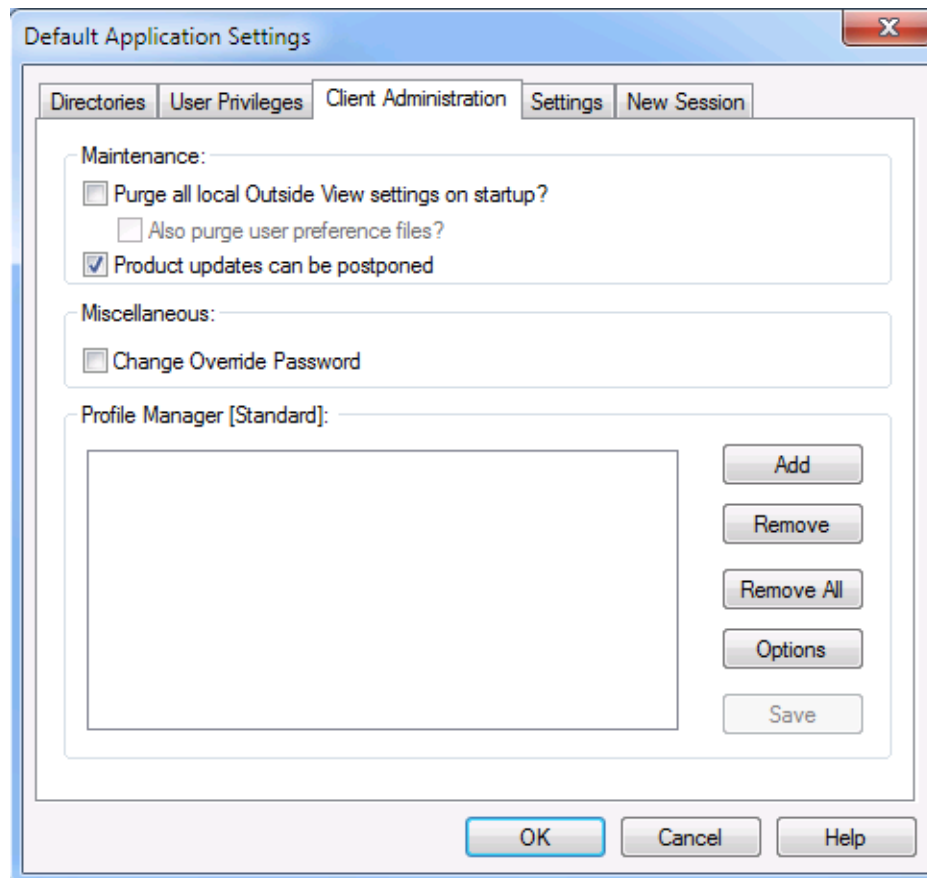
3.1.3.3 Client Administration

Client Administration

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

Client Administration

While in Supervisor Override Mode, select Edit, Application settings, then select the Client Administration Tab:



Supervisor Override tab for Client Administration

- **Purge all local OutsideView settings on startup?** If this "pristine mode" setting is enabled, all local Component, Param, and Macro files are purged (including any created locally) and all Enterprise-provided files are reloaded from the network when OutsideView starts up.

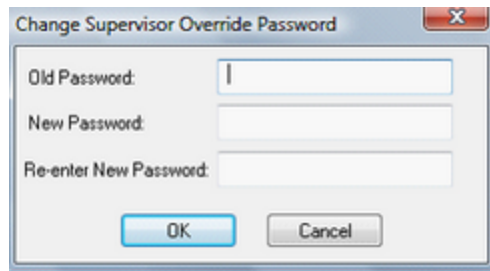
NOTE 1: Pristine mode also removes the failover.txt file essential to correct automatic failover/failback. For that reason, it is recommended that this switch be used intermittently or periodically and not simply left on continuously.

NOTE 2: If it is essential to leave the Pristine Mode switch on at all times, you can move the failover.txt file from the single, global location of the ...\\Profile folder into the multiple locations of ...\\Components subfolder of EACH profile.

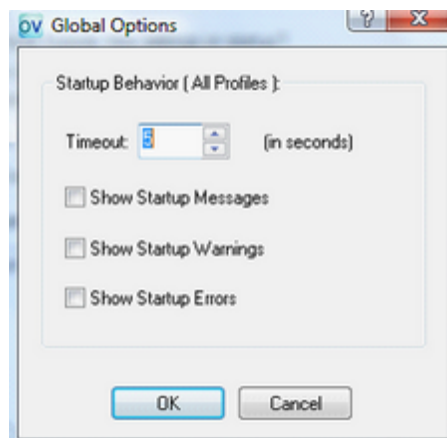
- **Also Purge user preference files?:** User preference files are exempt from a routine 'Purge all' to protect local preference settings. Set this switch to ON to include them when purging local files
- Files marked read-only will NOT be deleted. Nothing is deleted if there is a problem in copying files down from the network.
- **Product updates can be postponed?** This enables the Update Available query box. If this option is not checked, the user is not offered the option of declining the program update. Program updates can be postponed, but network configuration file updates cannot. Since there are so few network configuration files, the download time will be almost unnoticeably short. To allow for different clock settings across machines, and to prevent the clients from spoofing configuration files, the network files are copied down to the PC if they have different modified dates (earlier or later) or different file sizes. Only files that differ in one or both of

these values are copied. This copying feature allows you to roll back configuration changes network-wide; simply change the configuration on the Profile Server and let OutsideView propagate it down through the network as users launch the program. The update and pristine-mode settings are executed before program files are launched; these settings are always applied to the local configuration even if the user attempts to run in supervisor mode. Processing these settings before redefining the network path ensures that, once OutsideView has launched, a user's changes to these settings cannot disable them.

- **Change Override Password?:** This brings up the Password Change dialog where the default password (crystal) can be reset.



- **Options:** Click on this button to bring up the Enterprise licensing options



- Timeout value is how long the OutsideView 'client' will wait for a response from the Enterprise share point. The default value is 5 seconds. In complex LANs or WANs, this figure should be increased.
- Show Startup Messages or Warning or Errors enables a verbose mode where messages are displayed at the OutsideView workstation as the startup process looks for a specific user profile assignment and downloads/updates local configuration files.

3.1.3.4 Settings tab

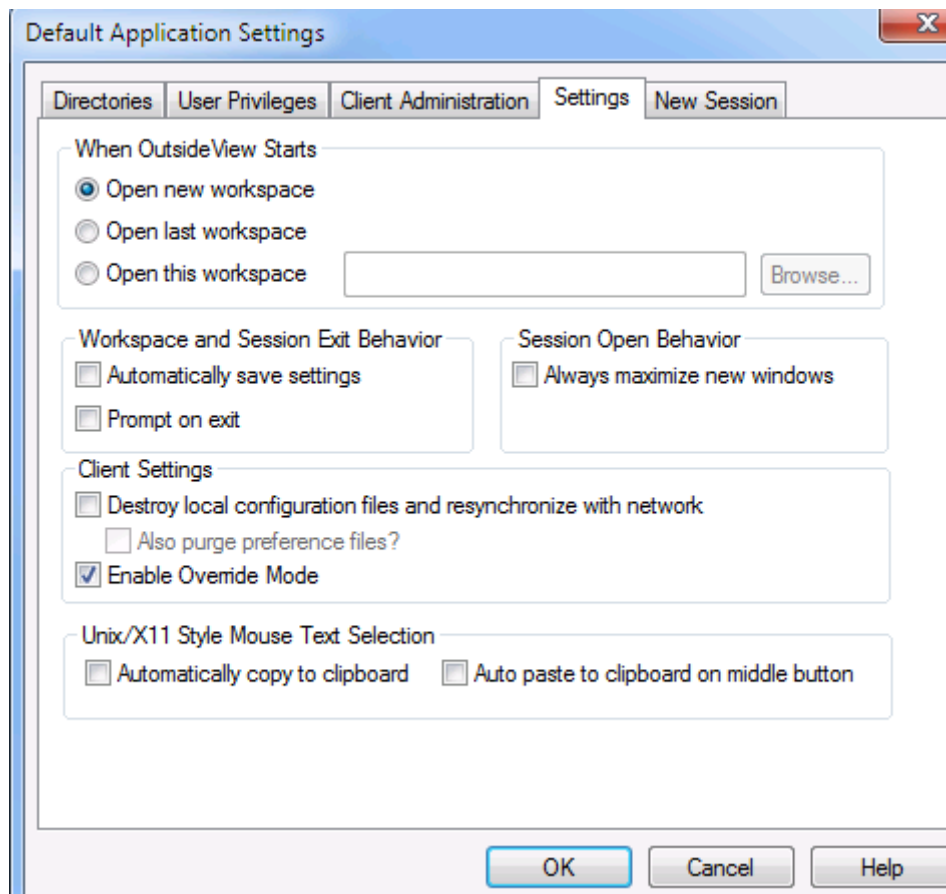
Settings tab

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

Settings tab

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.

This tab is displayed within Supervisor Override mode in case you need the information within. However, any changes you make in this tab apply only to this specific workstation and this specific instance of OutsideView. These settings are **not** propagated to all profile members.



The Unix/X11 mouse text selection is fairly new. When checked, 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.

3.1.3.5 New Session Defaults tab

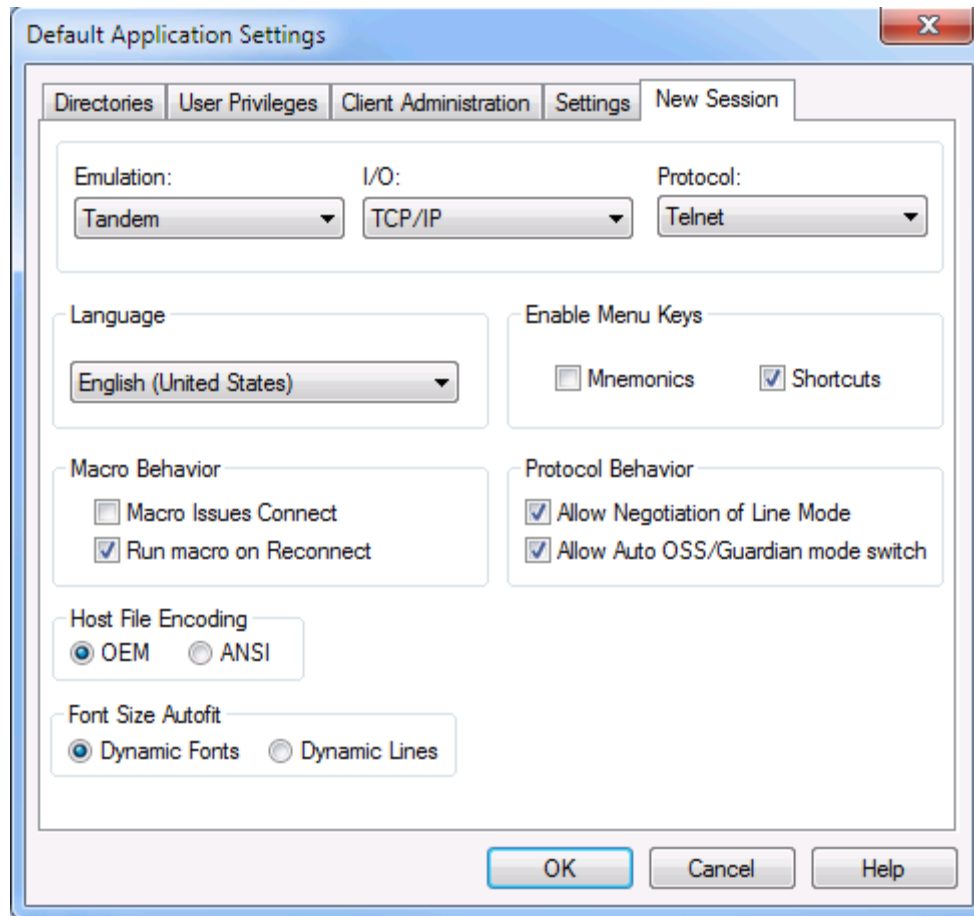
New Session tab

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

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.

This tab is displayed within Supervisor Override mode in case you need the information within. However, any changes you make in this tab apply only to this specific workstation and this specific instance of OutsideView. These settings are **not** propagated to all profile members.



3.1.4 Assigning Users to Profiles

Assigning Users to Profiles

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

Assigning Users to Profiles

Roaming Profile Capability

By default, an OutsideView user will receive the configuration files and privileges of the Profile from which the workstation was installed. As with Windows user profiles, however, an OutsideView user Profile can be 'roaming.' That is, OutsideView users can receive the

configuration and privileges assigned to their Profile, regardless of which workstation they are logged onto.

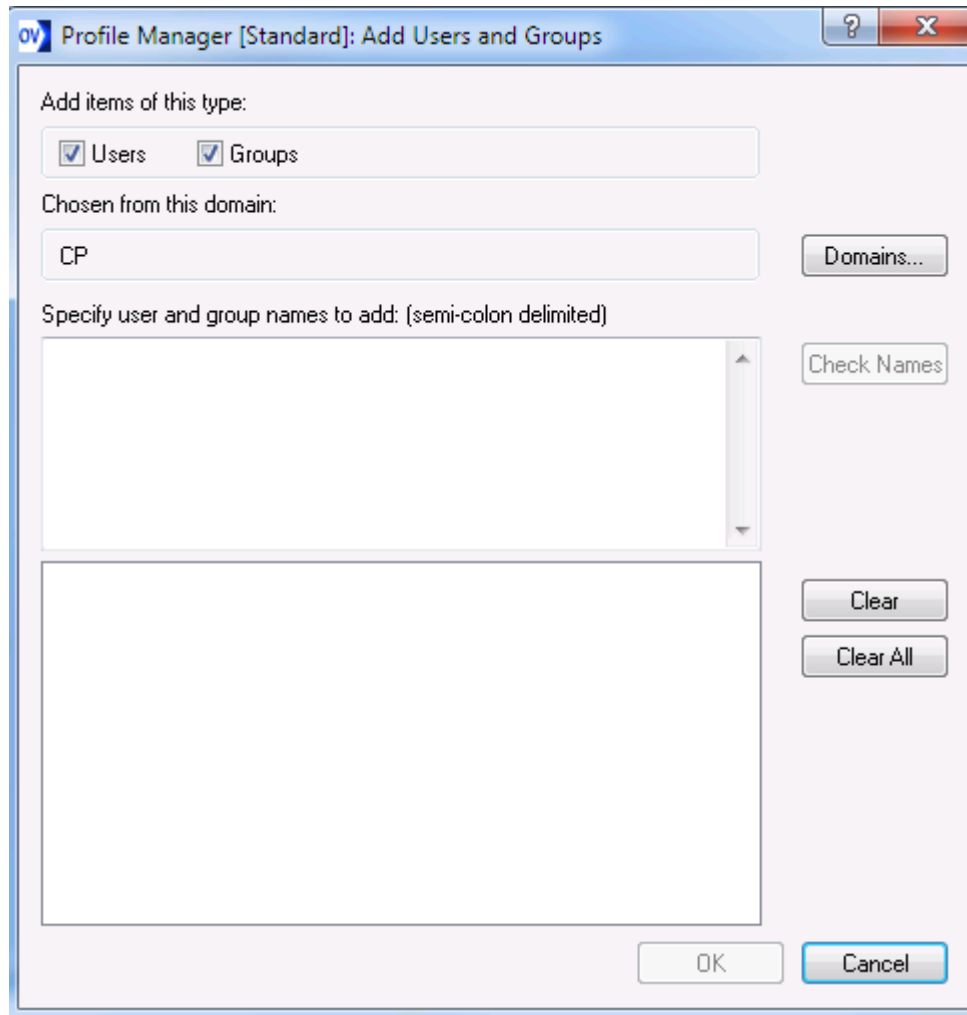
This capability is enabled through Supervisor Override mode to associate Windows Users or Groups with specific OutsideView profiles.

One example of this feature's usefulness is for a single workstation to be used across two shifts by two users who belong to different OutsideView profiles. Each user would still receive the specific sessions, workspaces, and permissions defined in their profile.

Assigning Users to Profiles

To assign Windows users or groups to an OutsideView Profile:

1. Launch OutsideView in [Supervisor Mode](#) for the target OutsideView Profile
2. Enter [Override Mode](#)
3. Enter Client Administration
(Edit, Application Settings, Client Administration tab)
4. Using the Add Button, add users or user groups



The user name and group assignments are stored in the file `profile_users` in the Profile folder (e.g. `\\servername\sharename\Profile`).

The format of `profile_users` file is:

```
[<Profile Name 1>
Path=<fully qualified UNC path to license pool e.g. \
server\OEnterprise\Licenses\LicensePool1.cpf>
User=<domain>\<user name1>
User=<domain>\<user name2>
User=<domain>\<user name3>
...
Group=<domain>\<group name1>
Group=<domain>\<group name2>
...
[<Profile Name 2>
Path=<fully qualified UNC path to license pool e.g. \
server\OEnterprise\Licenses\LicensePool2.cpf>
```

```
User=<domain>\<user name4>
User=<domain>\<user name5>
User=<domain>\<user name6>
...
Group=<domain>\<group name3>
Group=<domain>\<group name4>
```

Example file content:

```
<Global Options>
Timeout = 15
ShowMessages = 0
ShowWarnings = 0
ShowErrors = 0
```

```
[Standard]
```

```
Path = 1
User = CP\JimW
Group = CP\Domain Users
```

```
[Concurrent]
```

```
Path = \\EnterprisePC\ov80-ent\Licenses\LICENSEPOOL-PerSeat.cpf
User = CPX\BobS
User = CP3\MaureenG
Group = CPX\DataEntry
```

Note: This file may also be created and/or edited in any text editor such as Notepad.

The way the file is searched is that, on startup, the OutsideView client looks for the file and, if it exists, searches through it top-to-bottom for a **case-sensitive** match against User name. If it finds a match, it is satisfied (first match wins) and that is the profile used. If no match is found to User name, it starts again in a top-to-bottom **case-sensitive** search for a match with Group membership. Again, first match wins and that is the profile used. If no match is found for user or group name or if the file was not found, OutsideView will default to the Profile last used.

3.1.5 Automating Users' Service Names

Automating Users' Service Names

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

Automating Users' Service Names

In some environments, each end-user is required to sign on to the NonStop host using a unique service name.

To accommodate this, within the Enterprise framework, Crystal Point has developed a macro-driven mechanism to automate the service name selection. In summary, the macro is listed as the session's Startup Macro (under Session settings), and the session is informed that the

Macro Issues Connect . The macro determines the user's Windows user and domain names, then uses those values to interrogate a table at the Enterprise share and retrieve the desired <IP Address>, <Port>, and <Service> values. The macro then constructs a session open request using those values.

For detailed information, you may download information from our web site:

http://www.crystalpoint.com/cpdownloads/macros/VisualCommBasic/GetUserInfo-7_2.zip

http://www.crystalpoint.com/cpdownloads/macros/VisualCommBasic/GetUserInfo-7_3.zip

http://www.crystalpoint.com/cpdownloads/macros/VisualCommBasic/GetUserInfo-8_0.zip

http://www.crystalpoint.com/cpdownloads/macros/VisualCommBasic/GetUserInfo-8_1.zip

3.2 Licensing

3.2.1 Licensing Overview

Licensing Overview

[Top Previous Next](#)

Licensing Overview

All OutsideView Enterprise clients obtain their licenses from the license pool(s) identified in their profile. As of OutsideView release 8.0, there are two different versions of the license pool available. One is the traditional license pool created on a Windows shared folder, and the other is created within a SQL database. Both types of license pool are usually created during the Enterprise Install process. In the traditional Licensing model, additional license pools can be created after the fact using the LicenseView utility.

License Types

OutsideView Enterprise licenses are purchased as either per-seat or concurrent types.

Per-seat licenses are reserved by a workstation on the first launch of OutsideView Enterprise and will be permanently bound to that workstation unless manually released using LicenseView. There is a one-to-one relationship between PerSeat licenses and OutsideView Enterprise PerSeat users.

Concurrent licenses are reserved by a workstation when OutsideView is launched and released back to the pool when OutsideView is properly terminated by the user. That license then becomes available to another user. There is no one-to-one relationship between number of licenses and number of users when using concurrent licenses. One concurrent license will allow any number of users to (sequentially) take use of it.

SSL/TLS and SSH Encryption are supported for all license types.



Warning: You should not mix license types in a single pool. All licenses in a particular pool must be of the same type.

License Pool Operation

On each launch of OutsideView at a workstation, an attempt is made to contact the license pool. If a license is not available on the local workstation, an attempt is made to find an available license and check it out. If the workstation had previously checked out a per-seat license, the reservation is renewed for 7 days. If the workstation acquires a concurrent license on the launch of OutsideView, that license is checked back into the pool when OutsideView is properly terminated.

If the license pool cannot be accessed by an OutsideView client, OutsideView will continue to operate using its last acquired license for the length of the reservation period (7 days). This functionality eliminates license pool as a possible single point of failure.

If the workstation is to be removed from the network for an extended period (more than 7 days) and continued operation of OutsideView is required, the license may be made available offline. Click [here](#) for instructions on making a license available offline.

SQL License Pool Operation

On each launch of OutsideView at a workstation, an attempt is made to contact the license pool database. If a license is not available on the local workstation, an attempt is made to find an available license and check it out. If the workstation had previously checked out a per-seat license, the Lease Expiration Date is renewed for 7 days. If the workstation acquires a concurrent license on the launch of OutsideView, that license is checked back into the pool when OutsideView is properly terminated. The license pool database is only contacted once within every 24-hour period. Therefore, termination and re-launch of OutsideView within the 24-hour period does not involve re-contacting the license pool database.

If the license pool database cannot be accessed by an OutsideView client, the client will continue to operate using its last acquired license until the license's Lease Expiration Date (7 days). This functionality eliminates license pool as a possible single point of failure.

If the workstation is to be removed from the network for an extended period (more than 7 days) and continued operation of OutsideView is required, the license may be made available offline for an extended period. Click [here](#) for instructions on making a license available offline.

License Pool Administration

The LicenseView utility provides the following functionality:

[View license status](#): View the state of all licenses to determine the availability of any license.

Create new license pools

[Create New Pools](#): Multiple license pools will allow usage by different user groups or business units to be independently tracked and managed.

[Export Licenses](#): You may export Enterprise licenses for Desktop use or to other license pools.

Import Licenses: You may import Desktop licenses, licenses in other license pools or add new licenses to your existing pools.

[Import Licenses](#): You may import Desktop licenses, licenses from other pools or add new licenses to an existing pool.

[Releasing Licenses](#): Release licenses bound to particular users or workstations for use by other users.

[Synchronizing licenses](#) : The license pool may be synchronized to reflect the current license usage.

[Generating usage reports](#): Quickly generate reports of OutsideView license usage.

[Make a license available offline](#) for cases where the workstation will be disconnected from the network for an extended period.

SQL License Pool Administration

The SQL LicenseView utility provides the following functionality:

Open License Database: Open existing License Pool Database.

License Pool Properties: Configure the settings for the License Pool Database

Print: Prints out the License Information from the current active License Pool Database session.

Recent: Shortcut to open most recent databases

Close License Database: Closes the current active monitored License Pool Database session.

Exit: Shut down the LicenseView application.

Find: Search for a License using the Machine Name, User ID, or Serial Number.

Refresh: Refreshes the display with updated information from the License Pool Database.

Checkout: Reserve a license to a specific User ID or Machine Name.

UndoCheckOut: Release licenses bound to particular users or workstations for use by other users.

Export Licenses: You may export Enterprise licenses for Desktop use or to other License Pool Databases.

Import Licenses: You may import Desktop licenses, or license from an NLPC number.

Delete: Delete selected license(s) from the License Pool Database.

Options: Configure a notification email message to be sent when the available licenses reach a certain level or manage the database connections.

Diagnostic Log: If diagnostic tracing is turned on, view the diagnostic trace information of users accessing the License Pool Database.

3.2.2 License Administration

3.2.2.1 Traditional LicenseView

3.2.2.1.1 View License Status

View License Status

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

View License Status

The icons at the far left of the LicenseView table indicate the state of each license is in:

- A Checked Out license will typically show a red icon and the letter R (reserved)
- A Checked In license available for use, will show a green icon and the letter U (Unassigned)
- A Checked Out license whose Lease period has expired will be used only if no other license are available, and shows a green icon and R (reserved)
- A license whose internal validity date has passed (such as an evaluation license) cannot be used, and will display a gray icon and X (eXpired).



Checked Out



Checked In



Checked out and Expired



Expired

3.2.2.1.2 Creating License Pools

Creating License Pools

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

Creating License Pools

You can use the License Wizard to set up a new OutsideView license pool. You can then add licenses to the new pool.

1. On the menu bar, select File: New Pool.
2. In the dialog box, enter a path or browse to the location where you want the license pool to be located.
3. Type in a name for the new license pool, and click Next.

NOTE: Each license pool should be created in a separate folder.

You now have the option of leaving this pool empty or importing licenses immediately. If you want to leave the pool empty, you're done. In most cases, you will want to import the licenses right away.

4. To import licenses, click Import licenses from an enterprise license file/NLPC number. Then click Next.
5. In the Get Enterprise License File dialog box, enter an NLPC (Network License Pool Code) number or click Browse to locate a valid enterprise license file. Then click Next.
6. Read the information in the confirmation dialog box, and click Finish.

3.2.2.1.3 Importing Licenses

Importing Licenses

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

Importing Licenses

The Import feature of LicenseView may be used to:

- Import a Desktop License
- Import licenses from another Enterprise License Pool.
- Add new licenses from a supplied NLPC number or License file.

Should you purchase additional OutsideView licenses, these licenses will arrive as a license file or NLPC (Network License Pool Code) number.

To import licenses from another Enterprise License Pool

To import a Desktop license:

1. Open the target license pool in LicenseView then select Licenses: Import: Desktop License...
2. In the Import License dialog, enter the Serial Number and License Key values for the Desktop License.
3. Click OK.

To import licenses from another Enterprise License Pool:

Open the target license pool in LicenseView then select **Licenses: Import: Enterprise License(s) from a License Pool...**

1. In the License Wizard – Open License File dialog, enter the fully qualified UNC path to the external license pool and click OK.
2. In the License Wizard – Select Licenses dialog, select the licenses to be imported (use Ctrl+click to select multiple licenses).
3. Click OK.
4. Verify the information in the confirmation dialog box, and click Finish.

To add OutsideView licenses to an existing license pool from an NLPC number or license file:

1. Open the target license pool in LicenseView, and then click **Licenses: Import: Enterprise License(s) from a License File/NLPC number**.
2. Enter the NLPC number or click Browse to enter a path to the license.
3. Click Next.
4. Verify the information in the confirmation dialog box, and click Finish.

3.2.2.1.4 Exporting Licenses

Exporting Licenses

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

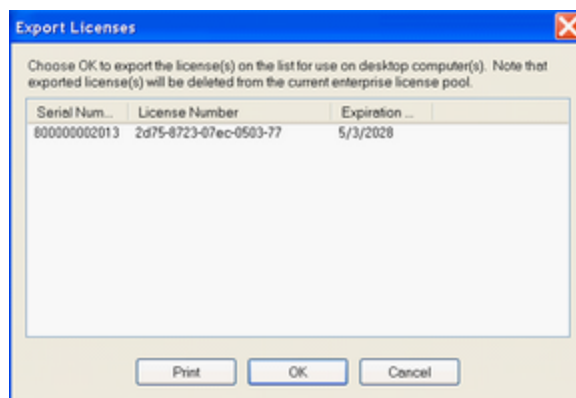
Exporting Licenses

The Export License feature of LicenseView may be used to:

- Export Enterprise licenses for Desktop installations
- Export licenses to another License Pool

To export Enterprise licenses for Desktop installations:

1. Open the license pool containing the licenses to be exported in LicenseView.
2. Highlight the available **U** licenses you wish to convert to Desktop licenses.
3. Select **Licenses: Export: License(s) to Desktop**.
4. The Export Licenses dialog will open displaying the serial number, License Number and Expiration Date values for the selected licenses.

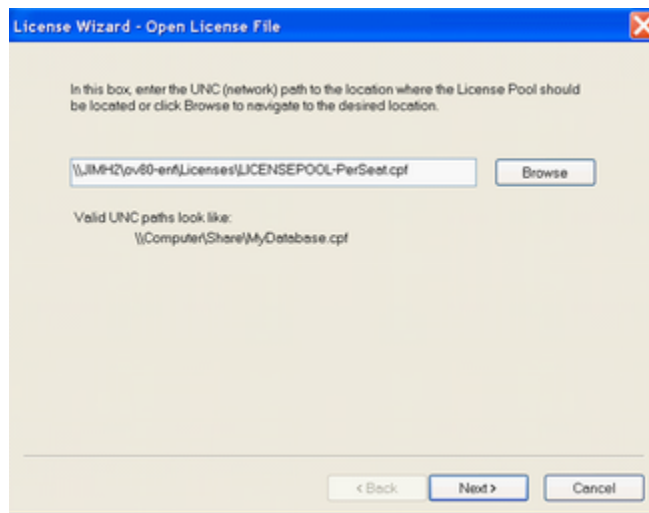


Selecting Print will print these values. Selecting OK will display a warning dialog verifying that the licenses are to be exported. Clicking Ok will close both dialogs and remove the licenses from the Enterprise pool.

NOTE: *It is highly recommended to Print and keep a record of this export. No other record of these exported licenses will exist within License View*

To export licenses to another license pool:

1. Open the license pool containing the licenses to be exported in LicenseView.
2. Select **Licenses: Export: License(s) to Enterprise Pool**.



3. In the License Wizard - Open License File dialog, enter the fully qualified UNC file name of the target license pool and click OK.
4. Verify the information in the Export to Enterprise dialog and click Next.
5. Verify the information in the Confirmation dialog and click Finish.

3.2.2.1.5 Releasing Licenses

Releasing Licenses

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

Releasing Licenses

Licenses can only be released when not actively in use – i.e., OutsideView is not running at the client workstation. There should be no need to manually release a concurrent license; this should occur automatically. To release the binding of a particular PerSeat license to a user/workstation:

1. Start LicenseView and open the license pool (*.cpf) containing the license.
2. Select the license from the list of licenses then select Licenses/Undo Check Out...
3. Click "OK" in the "Licenses Properties..." dialog
4. Click "Yes" in the "LicenseView – Undo Checkout" dialog

The binding of that license to a particular user/workstation will be released.

To release the bindings for all licenses in a pool:

1. Start LicenseView and open the license pool (*.cpf) containing the licenses.
2. Select Licenses/Release All Licenses.
Regardless of previous or current status, all licenses in the pool will become available for check-out.

NOTE: This utility is designed to be run no more frequently than every two weeks. If more frequent use arises, please contact Crystal Point technical support at support@crystalpoint.com or +1 425 806 1143.

3.2.2.1.6 Release All Licenses

Release All Licenses

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

Release All Licenses

Licenses, Release All Licenses is a powerful remedial action. It will reset your entire license pool to a brand-new state, regardless of active users, or other considerations. This can resolve problems, but can also generate certain user warning messages. For example, if you Release All Licenses while users are active, when such users later exit OutsideView and an automatic attempt is made to release their (already released) license they will receive an error message to the effect that the OutsideView program was unable to successfully release the license. Such a warning message may be ignored.

3.2.2.1.7 Checking a License Out

Checking a License Out

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

Checking a License Out

Although the process of assigning licenses to users is usually performed automatically whenever a user starts OutsideView, LicenseView also allows manual checkout of a license.

To check out a license to a particular user or computer:

1. Open the license pool and click to select any available unassigned  license.

NOTE: A red icon means that the license is already checked out to someone else and therefore not available.

2. On the menu bar, click Licenses: Check Out.
The license properties dialog box appears.
3. Under Check Out Information, click Browse to select the computer name. Then click OK.

3.2.2.1.8 Synchronize the License Pool

Synchronize the License Pool

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

Synchronize the License Pool

There are some cases when a license's reported status can become incorrect. For example, a server can crash or become corrupted by a virus. This can result in licensing errors, perhaps even repeated difficulty.

If you can identify which user or group of users are experiencing difficulty, then highlight those particular licenses, and select Licenses, Synchronize Selected

If you are unsure which licenses are experiencing difficulty, you may attempt to correct this condition with Licenses, Synchronize All.

When you synchronize the license pool, LicenseView sends a message across the network asking for the name of each of the machines currently connected to the license pool. Once that list is compiled, LicenseView then updates (checks out) the licenses in the pool, matching them with the appropriate machine name.

To synchronize a license pool:

1. Launch LicenseView and open the pool (File/Open Pool...)
2. Select Licenses, Synchronize All

3.2.2.1.9 Make a license available offline

Make a license available offline

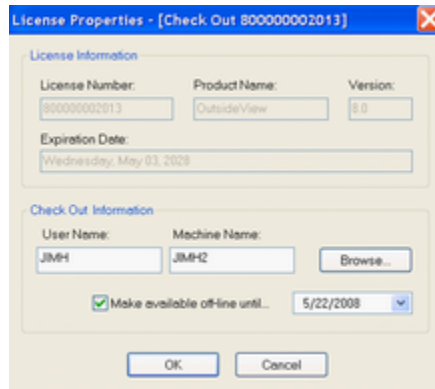
[Top](#) [Previous](#) [Next](#)

Make a License Available Offline (extended license checkout)

These instructions will allow a client Enterprise installation of OutsideView to continue operation when disconnected from the network for an extended period. The process of assigning licenses to users is usually performed automatically whenever a user starts OutsideView.

To make a license available offline:

1. Open the license pool in LicenseView
2. Select the license currently checked out to the workstation
3. Right click on the license and select Properties



4. Check the "Make available offline until..." box and define a date past the last date the workstation will be reconnected to the network.

3.2.2.1.10 License Reports

License Reports

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

License Reports

LicenseView provides various report options so you can better keep track of license activity. To quickly print the current state of the license pool, just click File: Print.

1. To Generate a Custom Report
2. On the menu bar, click Licenses: Report.
3. Select the criteria for your report:
 - To see all license activity that occurred on and between a set of dates, specify a date range.
 - To see all activity for a particular license, specify a license number.
 - To see all the license activity for a certain user, specify a user name.
4. Under Select column headers to view, select the information that you want to see on your report, and click OK. The report you asked for will be generated on-screen.
5. Click Cancel to close it or click Print to print it out.

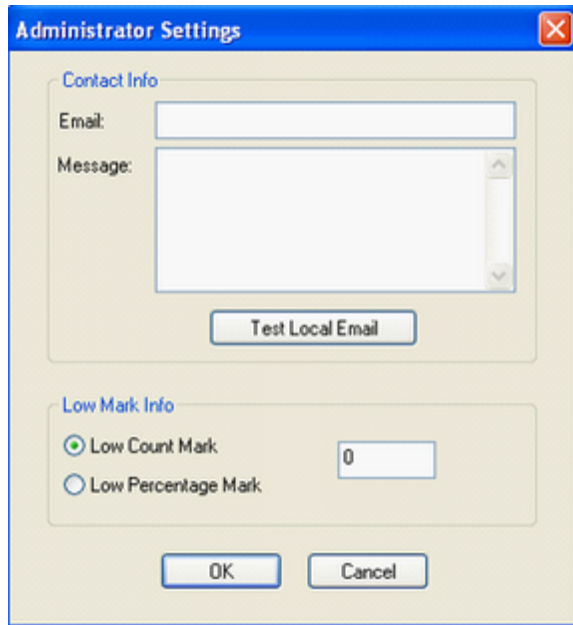
3.2.2.1.11 License Alerts

License Alerts

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

License Alerts

LicenseView supports automatic email alerts when the number of available licenses hits a low count mark or a percentage of all licenses. The email is sent by the client workstation when OutsideView is launched.



NOTE: This feature is supported only with the Outlook mail client.

To define an email license alert:

1. Open the license pool for which you wish to enable alerts in LicenseView
2. Select Edit/Administrator Settings to open the dialog shown above.
3. Enter the email address of the license administrator and a message to be included in the body of the email.
4. Select whether the alert will be on a Low Count Mark or Low Percentage Mark and enter the value to be tested.

NOTE: The email functionality may be tested by clicking the "Test Local Email" button. This will send a test message from the current user to the license administrator.

5. Click OK.

3.2.2.1.12 PACK the License Pool

PACK the License Pool

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

PACK the License Pool

Error 80042af7 "invalid or unknown error" may indicate the index file of the license pool database has become corrupted. To regenerate the index file, one must run the PACK utility against the license pool database file, usually named licensepool.cpf

STEPS:

1. Everyone else must be out of LicenseView
2. Open LicenseView
3. Open license pool
4. Select FILE, PACK

NOTE: *PACK takes exclusive use of pool)*

5. Exit LicenseView (to release pool from exclusive use mode)
6. Confirm users can check out licenses

3.2.2.2 SQL LicenseView

SQL LicenseView

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

SQL LicenseView

SQL LicenseView is a new version of LicenseView that enables an administrator to manage licenses residing in the License Pool on a Microsoft SQL Server 2012 - 2022 databases.

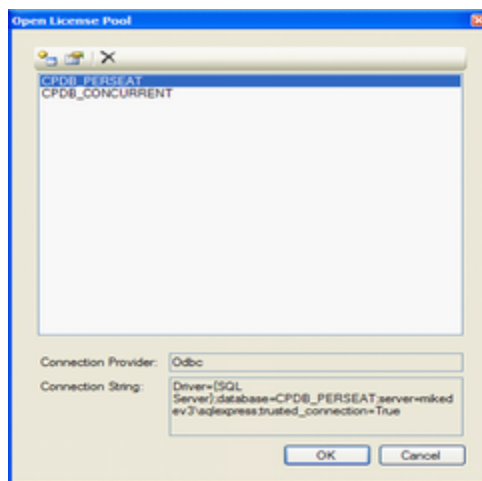
3.2.2.2.1 Open


Open

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

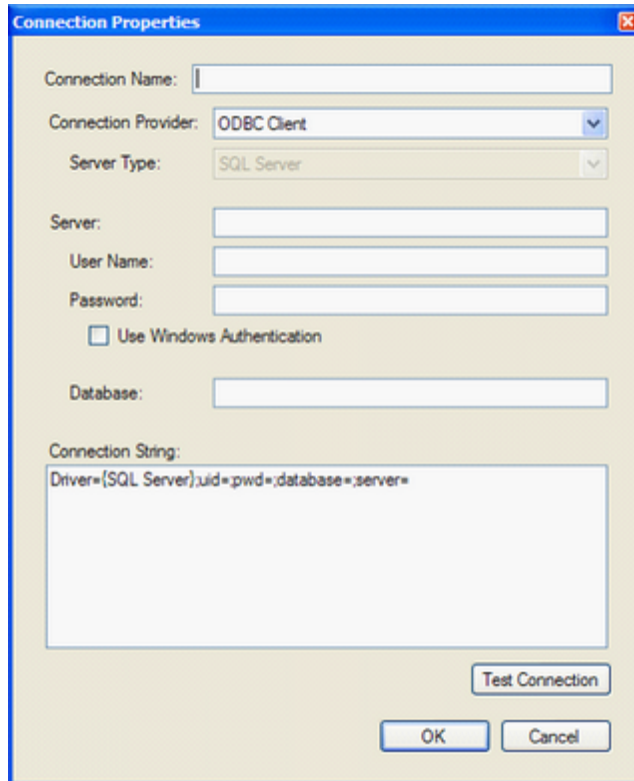
Open

The File --> Open menu function enables the administrator to open saved database connections or to open a new database connection. A database connection is a simple connection string that is used to connect to a SQL database server and point to the specific License Pool database. The connection string also specifies the type of authentication to be used for verification on the SQL database side. Upon clicking on the Open menu item, the Open License Pool window will appear displaying existing database connection string names, allowing the users to create new database connection string, modify existing database connection string properties, or delete the database connection string.



New database connection is a connection that has not yet been established to a newly created License Pool database. A new connection can be made by clicking on the icon: . 


After clicking on this icon, a Connection Properties dialogue window will come up so that administrator users can enter the connection information to create a database connection string:




- **Connection Name** – This is an identifier used to refer to this connection string. It can have whatever value you prefer. After this connection property has been specified, all future reference will be made to this connection via the Connection Name.
- **Connection Provider** – This is the database driver to be used to connect to the database. The SQL LicenseView application currently supports only the ODBC database driver.
- **Server** – This field is to specify the DNS qualified name of the Database server in which the License Pool database is residing on. For example if you have installed the SQL Express database on a computer named Machine, then this field would be: “Machine\SQLExpress”. Note that in the Server field, you must not append two backslashes prior to the server name (do not use “\”).
- **User Name** – this field is to specify a user login name that exists on the SQL database server.
- **Password** – this field is the corresponding password necessary for the User Name to gain access onto the SQL database server.
- **Use Windows Authentication** – A different option instead of using SQL database specific User Name and Password is to use the Windows Authentication option. This option uses the user’s window’s login name and password on a windows domain as their credential to access the SQL database. If you use this option, the User Name and Password fields will be grayed out.

- **Database** – This field should contain the name of the license pool, as specified during the Enterprise Installation process.
- **Test Connection** – This button is used to test the database connection string to verify that it is working.
- **OK** – This button should be clicked on once the connection string passes the Test Connection test. The new database connection string with the specified Connection Name will be displayed in the Open License Pool window and automatically saved to a configuration file.
- **Cancel** – This button will close the Connection Properties window and discard the connection string that the user was working on.

Saved database connections are prior connections that were defined by the administrator and saved. If there are saved database connections, the administrator will be able to select the database connection and then click on the OK button. Users can also modify existing database connection string properties by selecting the database connection name and then

clicking on the  icon. By clicking on this icon the Connection Properties dialogue window will appear containing the information for this specific database connection string. Users can modify any field, click on the test button and then the OK button to save the changes.

The delete icon  allows the user to remove unwanted database connections.

3.2.2.2 License Pool Properties

License Pool Properties

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

License Pool Properties

The File --> License Pool Properties menu function brings up the License Pool Properties dialogue window. This window displays the configuration information for the License Pool database that was installed during the Enterprise installation process. The configuration values for the License Pool database are installed with default values and some of these values (non grayed out fields) can be changed by the administrator.

License Pool Properties

Name: test

Type: concurrent

Minimum Checkout Period: 7 days

Maximum Checkout Period: 14 days

Server Outage Warning Period: 2 days

Extended Checkout Allowed

Help Desk Contact Info:

Diagnostic Tracing:

Off

Normal

QA Testing using client-side DateTime

Max Diagnostic Record: 1000

OK Cancel

The following list explains the configuration information used for the License Pool database:

- **Minimum Checkout Period** – This value represents the smallest number of days that a license can be checked out by OutsideView clients. Note that this value must be smaller than Maximum Checkout Period. This value, when set, dictates the Lease Expiration Date value in the License View window.
- **Maximum Checkout Period** – This value represents the largest number of days that a license can be checked out by OutsideView clients. Note that this value cannot be smaller than Minimum Checkout Period. This value is only used when the option for Extended Checkout Allowed is turned on.
- **Server Outage Warning Period** – This value sets the grace period time in days that the administrator has to bring back up a downed License Database before all the OutsideView client's license leases are expired. The max value for this variable is (Min Checkout Period - 2).
- **Extended Checkout Allowed** – This option allows the Administrator to toggle on using the Max Checkout Period. This is used when certain client PCs running OutsideView client are taken off the network for an extended period and therefore can't reach the License Pool Database. This feature is used with 'PerSeat' licenses only in the Enterprise environment. In order for this to work, the OutsideView client must also be configured to use Extended Checkout. This can be configured within OV's Edit --> Application Settings... menu. In the Application Settings dialogue box's Directories tab, check the extended checkout box to turn on the extended checkout feature for the OV application.
- **Help Desk Contact Info** – This option allows the administrator to enter contact information to reach when licensing issues are encountered.
- **Diagnostic Tracing** – This option enables the administrator to configure the tracing behavior of the License Pool database. When set to 'Normal Tracing', this records into the License Pool database all the activity in obtaining and releasing the licenses including using the time stamp of when the event happened on the database side. The administrator can also set to 'QA Testing Using Client Side Date Time' in which the tracing functionality records the time stamp of when the events happened in obtaining/releasing the licenses from the OutsideView Client's perspective instead of the License Pool database.

- **Max Diagnostic Record** – This value limits the number of records to record into the License Pool database.

3.2.2.2.3 Print

Print

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

Print

The File --> Print menu option prints the licenses displayed in the LicenseView application.

Print to File

The File --> Print to File menu option prints the licenses information onto a file.

Print Preview

The File --> Print Preview menu option allows the user to preview the printout prior to sending the print request to the printer.

3.2.2.2.4 Recent

Recent

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

Recent

The File --> Recent menu option allows the user to open previously closed database connection. If there are multiple database connection names listed, then there is an option to open all of them.

3.2.2.2.5 Close and Exit

Close and Exit

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

Close

The File --> Close menu option closes the current LicenseView application's connection to the License Pool database.

Exit

The File --> Exit menu option closes the LicenseView application.

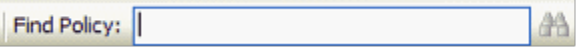
3.2.2.2.6 Find

Find

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

Find

The Edit --> Find menu option allows the user to search for a specific license. To find a license, the user can enter the License's Serial Number, the User ID or Machine Name into the

input field: . Once the search item is entered into this input field, then the user can click on the Edit --> Find menu option or click on the binocular icon.

Once the license has been found, the whole row is then highlighted in the LicenseView application.

3.2.2.2.7 Refresh

Refresh

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

Refresh

The Edit --> Refresh menu option updates the data displayed in the LicenseView application because the License Pool database sessions are not dynamically updated. This will poll the License Pool database on the SQL database server to obtain updated licensing information.

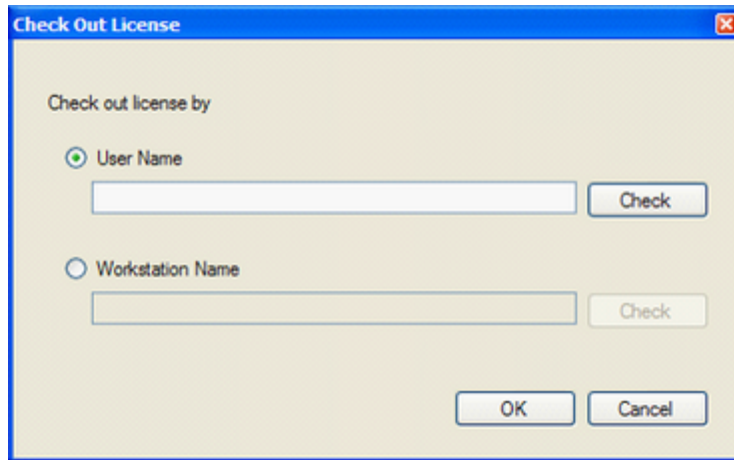
3.2.2.2.8 Checkout

Checkout

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

Checkout

The License --> Checkout menu option allows the administrator to reserve a license to a specific User ID or to a Machine Name. The Check Out License dialogue window will appear and the user can select whether to check out the license by User Name or Workstation Name.



After entering the information into the input field, click on the Check button to confirm that the User Name or Workstation Name exists on the domain network. Then click on the OK button to reserve the license or the Cancel button to exit out of the dialogue window without reserving a license.

3.2.2.2.9 Undo Checkout

Undo Checkout

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

Undo Check Out

The License --> Undo Check Out menu option releases the binding of a particular license to a user/workstation. Once this menu option is clicked, a Confirmation dialogue box will appear asking the user to confirm this action. If the user clicks on the Yes button then the license is released back to be used in the License Pool. If the user clicks on the No button then the undo checkout will be canceled.

3.2.2.2.10 Export License

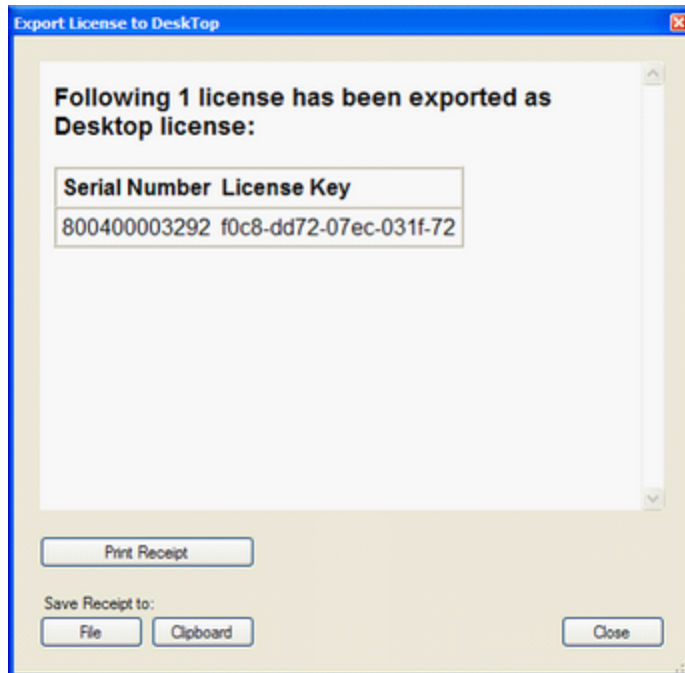
Export License

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

Export License

As Desktop License

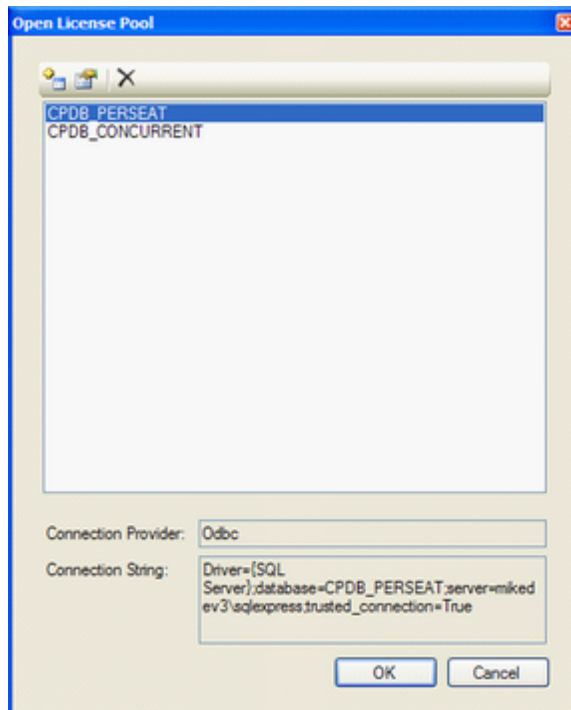
The License --> Export License --> As Desktop License menu item takes a highlighted license(s) within the License Pool database and exports it out of the pool to be used as a desktop license. When this menu item is selected, an Export License to Desktop dialogue window appears asking the user to make sure that they want to proceed with the export. If the user clicks on the Yes button, then the license is removed from the License Pool database and another dialogue box will come up displaying the information of the license that was exported:




The user can choose to either print out the information, save it to file or copy it to the clipboard.

To a License Database

The License --> Export License --> To a License Database menu option takes a highlighted license(s) within a license pool database and exports it out to a different license pool database. When the user clicks on this menu item, the Open License Pool dialogue window appears.



The user can select which license pool database they want to export to and then click on the OK button. If the license pool they want is not listed in this dialogue window, they can also create a new license pool database connection by clicking

on the icon: .

Once the OK button is clicked on, the license is exported from the source database over to the target database.

3.2.2.2.11 Import License

Import License

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

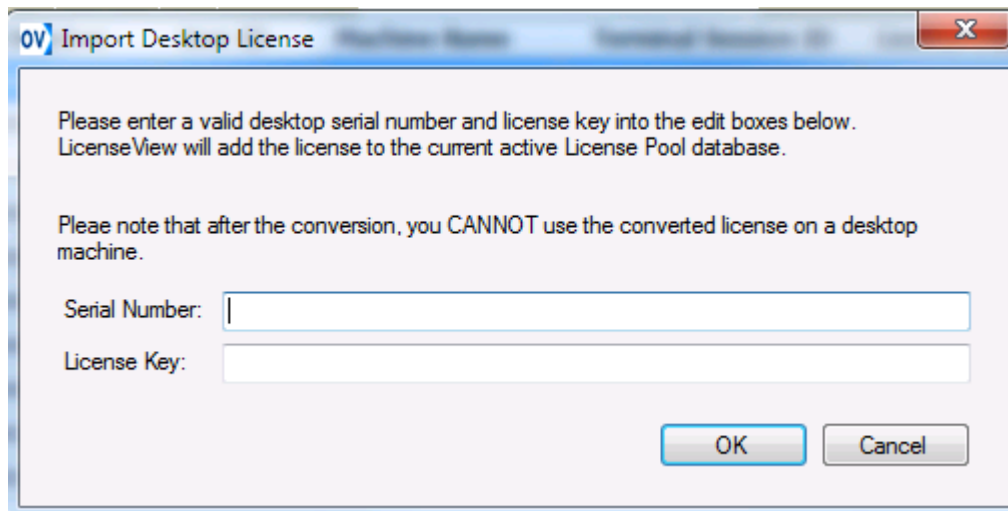
Import License

Desktop License

The License --> Import License --> Desktop License menu item takes a desktop license and imports that license into a license pool database. This imported license will then be able to be used in an enterprise setting.

NOTE: You can only import licenses of the same type. Therefore, if the license pool database has PerSeat licenses in there, then you can only import per-seat desktop licenses.

Upon clicking on this menu item the Import Desktop License dialogue window will appear:

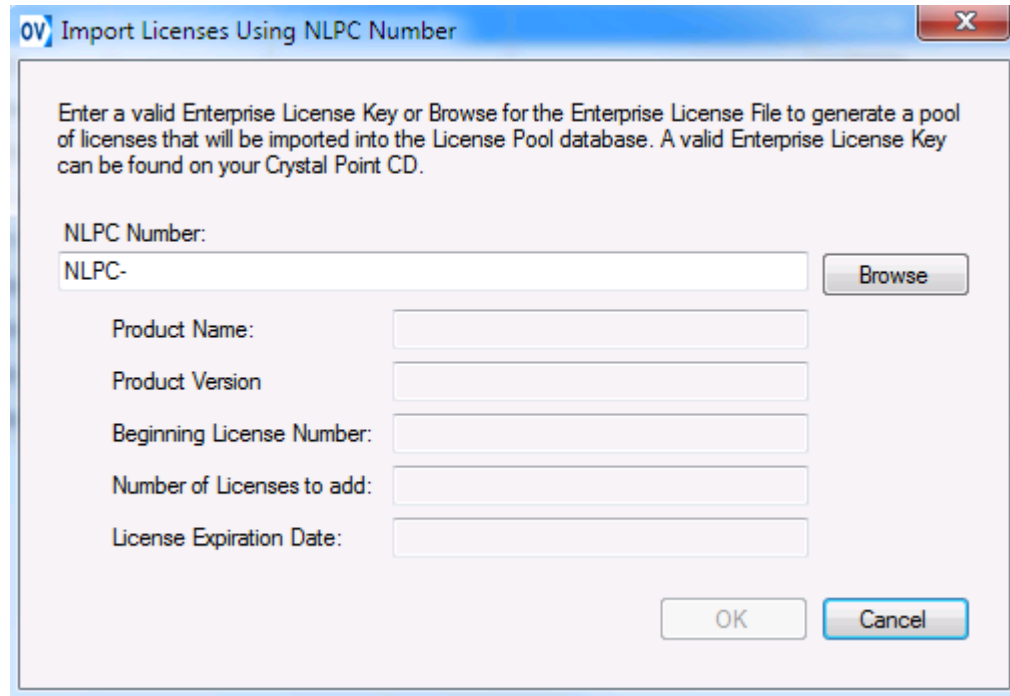


Enter the Serial Number and License Key information into the input fields and then click on the OK button to import that license into your current active license pool database. If the administrator clicks on the Cancel button then the import action will be canceled.

From NLPC Number

Should you purchase additional OutsideView licenses, these licenses will arrive as a license file or NLPC (Network License Pool Code) number. The License --> Import License --> From NLPC Number menu item will enable the administrator to import the license file or NLPC

number. Upon clicking on this menu item, the Import Licenses Using NLPC Number dialogue window will appear:



Enter the NLPC number or click on the Browse button to browse to a license file. After entering the NLPC number or license file, the information for the license should be displayed in the grayed out input fields and the OK button should become enabled for the user to click on. Clicking on the OK button will import the licenses into the current active license pool database. If the user clicks on the Cancel button, then the import license action will be canceled.

NOTE: *If there are duplicate licenses in the license file, then those duplicates will not be inserted into the license pool database.*

3.2.2.2.12 Delete the Selected License

Delete the Selected License

[Top Previous Next](#)

Delete the Selected License

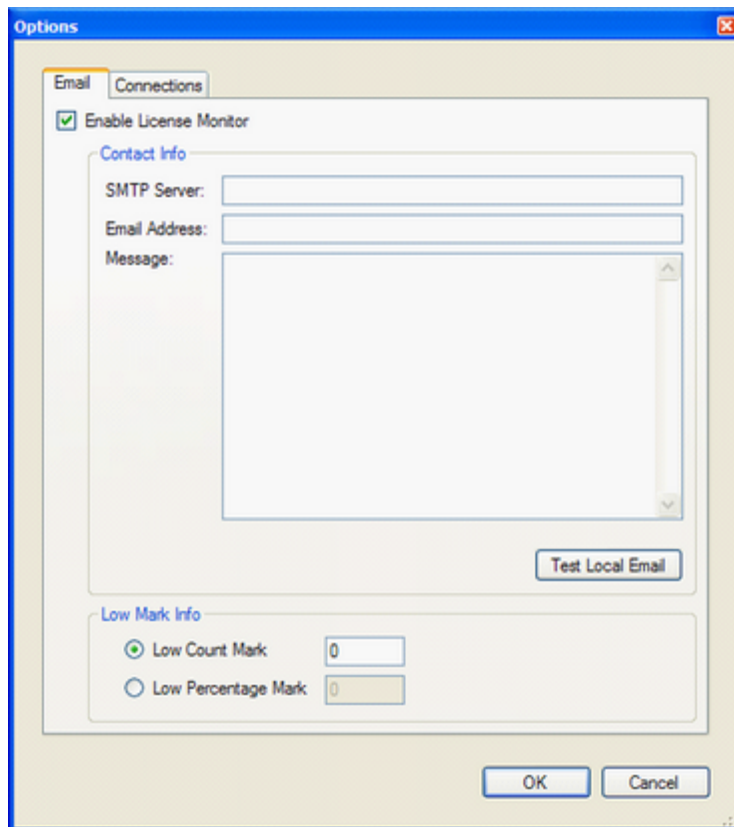
The License --> Delete the Selected License menu item takes the highlighted license(s) and deletes them from the current active license pool database. Clicking on this menu item will bring up the Confirmation dialogue box for the user to confirm that they actually want to delete this license from the license pool database. If the user clicks on the Yes button, then the license(s) will be deleted otherwise if they click on the No button, then the delete action will be canceled.

Options

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

Options

The Tools --> Options menu item lets the user configure database connection settings and email notification settings. When the user clicks on this menu item the Options dialogue window will appear:



Email

The email tab allows the administrator to configure and email notification to be sent when the free available licenses reach a certain count.

The information required for this feature to work correctly is

- SMTP Server – This is the email server
- Email Address – The email address to send the message to.
- Message – The message to include with this email.
- Low Count Mark – The number of free available license that is reached to trigger LicenseView to send out the email message.
- Low Percentage Mark – The percentage of free available license that is reached to trigger LicenseView to send out the email message.

After the information has been entered into this dialogue box and the user clicks on the OK button, the contents are saved into LicenseView.exe.configuration file. This allows the

notification to be persistent even after LicenseView has been restarted. To test if the email notification is configured correctly the user can click on the Test Local Email button.

NOTE: *The email notification only works when LicenseView is up and running.*

Connections

The connections tab allows the administrator to modify the existing database connection properties or add new database connection property. For more information about connections and how to create or modify them please refer to [File --> Open menu](#).

3.2.2.2.14 Diagnostic Log

Diagnostic Log

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

Diagnostic Log

The Tools --> Diagnostic Log menu item displays the diagnostic log information associated with the current active license pool database.

3.2.2.2.15 Help Topics

Help Topics

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

Help Topics

The Help --> Help Topics menu item brings up this help information otherwise known as System Admin help.

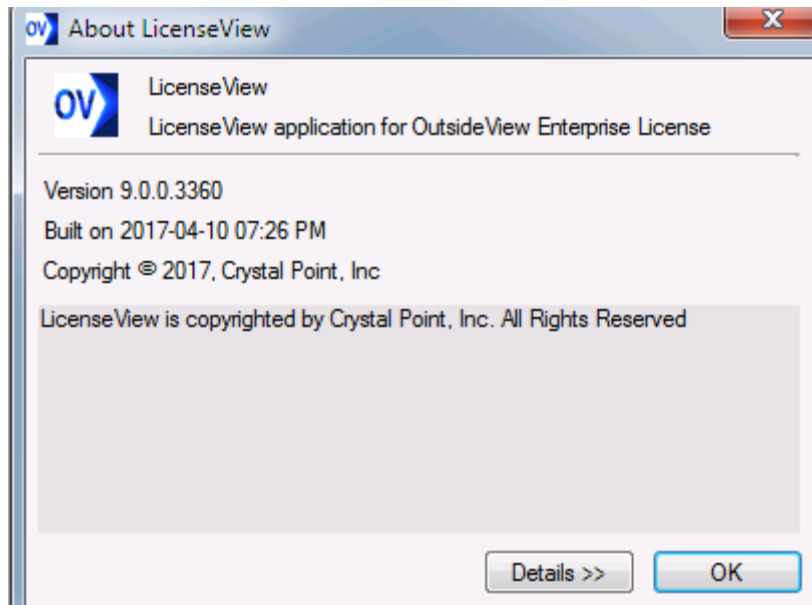
3.2.2.2.16 About LicenseView

About LicenseView

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

About LicenseView

The Help --> About LicenseView menu item brings up the about box for the LicenseView application.



3.2.2.2.17 Monitoring Multiple License Pool Databases

Monitoring Multiple License Pool Databases

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

Monitoring Multiple License Pool Databases

The SQL LicenseView application has the capability to open multiple license pool databases. For each license pool database open, a separate LicenseView window will come up. To toggle between the different LicenseView database connections, you can click on Window menu item and select from the list of open LicenseView database connections.

3.2.2.2.18 Make a License Available Offline for an Extended Period

Make a License Available Offline for an Extended Period

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

Make a License Available Offline for an Extended Period

Extended checkout is intended to serve the needs of those users who go off the network for an exceptionally long time - such as when traveling.

SQL Licensing;

To **enable extended checkout** at all, for a given SQL license pool, open the pool, using LicenseView,

Select, File, License Pool Properties.

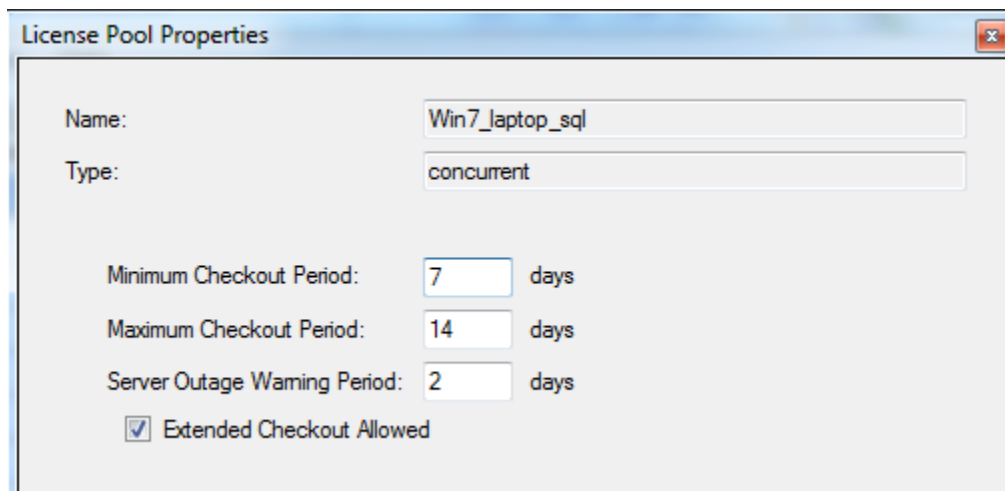
Use "Maximum Checkout Period" to set the duration you prefer for Extended Checkout to persist.

Check ON 'Extended Checkout Allowed.'

The Minimum checkout period is the default resiliency period; that is, the period of time since last accessing the license pool that normal users will continue to operate if the license pool becomes unavailable.

The Maximum checkout period is the duration clients having performed Extended Checkout will continue to operate if the license pool becomes unavailable, or When the user is off the network for reasons such as travel..

The Server Outage Warning Period specifies how far in advance, of the relevant checkout period expiration, OutsideView will begin displaying a warning message of impending expiration.



The screenshot shows a dialog box titled "License Pool Properties". It contains the following fields and settings:

- Name: Win7_laptop_sql
- Type: concurrent
- Minimum Checkout Period: 7 days
- Maximum Checkout Period: 14 days
- Server Outage Warning Period: 2 days
- Extended Checkout Allowed

To Check out a (SQL) license for an extended period;

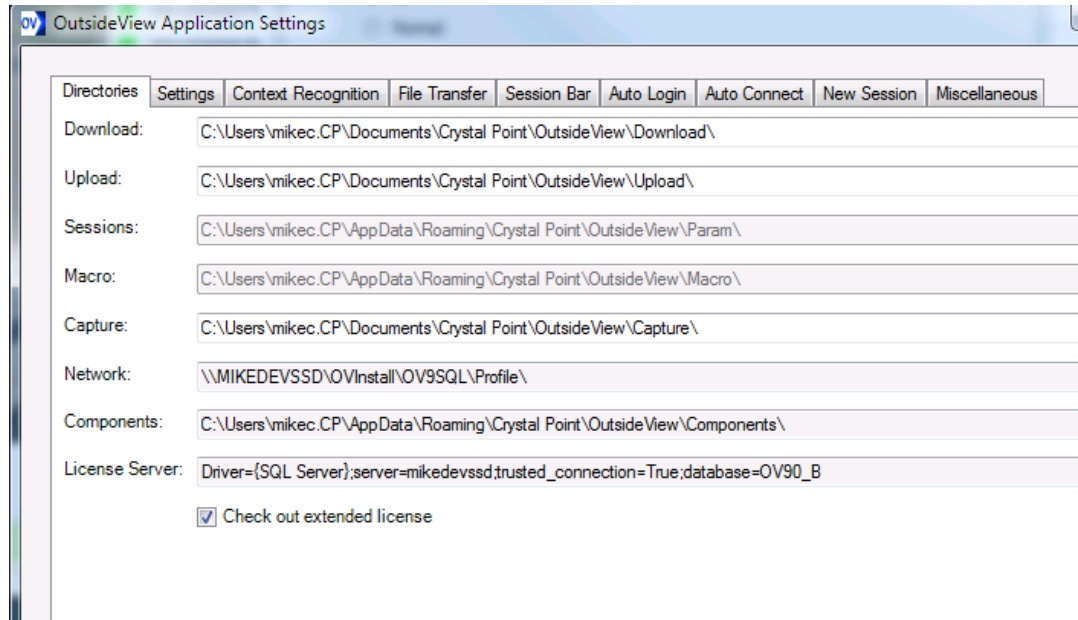
NOTES:

This capability is not available for 'classic' license pools, nor Citrix or Windows Terminal Server clients.

The extended checkout operation cannot be performed across a Remote Desktop link; it needs to be performed from the actual workstation itself.

Start OutsideView,

select **Edit, Application Settings** and, from the **Directories** tab, check ON "**Check out extended License**"



3.2.2.2.19 Error Messages

Error Messages

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

Error Messages

Error messages may arise during OutsideView client application startup. If error messages do occur, it is possible to have it include information as to whom the client user should contact. In order to include contact information in the error message dialogue box, the administrator needs to add the information into the License Pool Properties dialogue window. In this window, there is a input field labeled "Help Desk Contact Info" in which the administrator can set the contact information when these error messages occur.

Here is a list of possible licensing issues encountered by the OutsideView clients using the SQL Licensing scheme:

- **Error: Unable to open registry to create new registry values for current user.** -- This error means that the user does not have enough access privilege to write to the registry location: HKEY_CURRENT_USER\Software\Crystal Point\Licensing\ location. Check to make sure that the user can create this registry at the specified location.
- **Error: No licenses are available because all licenses are currently being used.** -- This error means that all licenses are being used and therefore no new users can use the OutsideView client application until either a license becomes available for use or more licenses are added to the License Pool database.
- **Error: No licenses are available because all licenses have expired.** -- This means that the license in the License Pool database have expired. Usually this occurs when the License Pool database have been populated with demo licenses.

- **Concurrent License Error: License Database Not Accessible.** -- This means that the License Pool database cannot be access by the OutsideView clients. Since the licensing type is concurrent, the OutsideView clients will not be able to launch until the License Pool database connection issue can be resolved.
- **Warning: Using cached license as this workstation has not been able to contact the license database server for the last...** -- This error message states that the OutsideView client have not been able to access the License Pool database for the last 'x amount of days'. Because the license type in the License Pool database is PerSeat, the OutsideView client application is still able to launch until the lease obtained expiration date expires.
- **Error: License Database Not Accessible and Your cached License Lease has Expired.** -- This error means that the License Pool database can not be reached and that the Lease Expiration Date has already expired. Therefore the OutsideView client application will not launch until the License Pool database issue has been resolved.
- **Error: License Database Not Accessible. Unable to get a License.** -- This error message means that the License Pool database is not accessible. This specific error message will only occur when the OutsideView client is ran the first time on a PC in which it does not have a license. In essence the client pc contains a virgin installation of OutsideView.

4 Seamless Guardian/OSS support

4.1 Seamless Guardian/OSS support

Seamless Guardian/OSS support

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

Seamless Guardian/OSS support

In OutsideView 7.3 or newer there is an enhanced sub mode "UNIX/OSS" that extends the basic 6530 emulation via operation differences and extensions to work optimally with UNIX environments that use TERMINFO and or TERMCAP files*to control the terminal behavior. OutsideView 7.3 or newer will now dynamically switch between modes depending on the application environment that is in use.

Notes:

K-series OSS environments typically use only the TERMCAP file to control terminal behavior, while S-Series or Integrity NonStop systems may use either TERMCAP or TERMINFO files.

The mode indicator in the lower right corner of your OutsideView screen will show either "UNIX/OSS" or "CONV" or "BLOCK". CONV and BLOCK are standard 6530 terminal emulation modes. UNIX/OSS indicates the extended functional mode is operative.

This functionality is predicated on the telnet connection to your host negotiating the NonStop specific telnet line mode protocol. This is the default connection option for OutsideView.. If you install TERMINFO support, then a command can be added to your profile file to switch the emulation mode when entering an OSS shell without line mode or from a service processor maintenance connection. There is more detail on this later in the document.

Note: the UNIX/OSS mode changes the operation of your keyboard. Various local action keys like page up and down are now function keys that are sent to the host to be interpreted. Therefore, if you are at a UNIX/OSS command prompt and you want to look back in the scroll back buffer you will now need to use the scroll bar and your mouse.

In addition, the mouse can no longer be used to reposition the cursor when in this mode.

4.2 Requirements

Requirements

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

Requirements

To configure your NonStop environment to take advantage of this new capability, you need the following items:

- OSS preinstalled and running on your NonStop host
- Administrator logon for super.super

- Example "tn653_termcap.txt" File from the OV installation CD.
- Example "tn653_terminfo.txt" File from the OV installation CD.
- Windows workstation running OutsideView 7.3 or above

If TERMINFO support is desired then you will need three additional files:

- "gzip.tar.Z" File from the FLOSS library
- "ncurses.tar.Z" File from the FLOSS library
- "vim.tar.Z" File from the FLOSS library

The FLOSS library is available from the [HP Connect Open Source Technical Library](#)

4.3 Background

Background

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

Background

In the UNIX environment support for terminal interaction has gone through three basic stages over the years.

- Applications that are hard coded for a specific terminal type
- Applications that are interfaced via a TERMCAP definition file
- Applications that are interfaced via a compiled TERMINFO file

UNIX first saw a lot of use in educational environments where every effort was made to use heterogeneous computer terminals acquired by the institution. This operational requirement led to the development of a terminal capabilities file so that programs could dynamically interact with different types of terminals connected to the same UNIX system.

The OSS personality on the NonStop is initially at the level of Berkley UNIX; which can be extended by installing various packages (like ncurses) out of the FLOSS (free library OSS) to add more modern capabilities and utilities. The FLOSS library can be accessed via the [HP Connect Open Source Technical Library](#) ITUG web site.

On most modern UNIX distributions when you invoke the VI text editor you are actually invoking an improved version of it named VIM; which is also available from the FLOSS library.

To support VIM you need to install "ncurses" and VIM as separate packages. Until the "ncurses" package is installed, TERMCAP is the controlling interface to the terminals under OSS. After installation of "ncurses" TERMINFO is the controlling interface for applications that are TERMINFO aware.

One of the drawbacks to the TERMCAP file was that it had to be dynamically scanned to locate the correct terminal definition and then parsed to locate the requested capabilities, this added significant overhead to start time for UNIX applications.

With newer versions of UNIX this transitioned to a new functional definition named TERMINFO that changed this format to be more easily maintained with expanded capabilities definitions and precompiled files that reduced the application startup overhead.

To prepare your NonStop OSS or UNIX system to use this new functionality takes some pre-configuration steps on the host to enable these enhanced interactions with OutsideView.

This can be done on an individual account basis or globally for everyone who connects to a NonStop and invokes the OSS personality. We will document the global procedure for TERMCAPE first.

4.4 Global OSS TERMCAPE setup

Global OSS TERMCAPE setup

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

Global OSS TERMCAPE setup

The procedure sets the OSS UNIX personality to default to a terminal type of "tn6530-8", rather than the initial value of "xterm". Doing this will allow your users to seamlessly move back and forth between the Guardian and OSS personalities on your NonStop system without changing the terminal emulation type that they are using.

On most UNIX systems, the host telnet process dynamically sets the terminal type through negotiation when the telnet connection is initiated to the host. Under OSS, this is a static value that is controlled via the global profile file in the "/etc" directory. If you have individual users who still need to use a different terminal type, this can be set by editing a personal profile file in their home directory or adding a simple script command to the profile file as we document in this document.

To make the OV 7.3 terminal definition globally available on your system perform the following steps from a command line window on a windows based workstation.

Note: *in the example below user commands/interactions are in bold text and assume we are working out of c:\tmp directory and have previously copied the tn653_termcap.txt file from the CD. You will find this file in the utilities directory on the installation CD image.*

Transfer 7.3+ plus TERMCAPE information to host

In the sequence of commands below, we open an FTP session to a host, log in as super.super, change over to the OSS file space and upload the new TERMCAPE for OV 7.3 as a file fragment.

```
C:\tmp> ftp [host name, e.g. s72k]  
Connected to s72k.cp.crystalpoint.com.  
220 s72k.crystalpoint.com FTP SERVER T9552G07  
(Version 3.w TANDEM 29JUL2005) ready.
```

```

User (s72k.cp.crystalpoint.com:(none)): super.super
331 Password required for SUPER.SUPER.
Password:
230 User SUPER.SUPER logged in.  OSS API enabled
ftp> quote oss
257 OSS API enabled.
ftp> cd /etc
250 CWD command successful.
ftp> put tn653_termcap.txt
200 PORT command successful.
150 Opening data connection for tn653_termcap.txt
(172.16.0.169,1279d).
226 Transfer complete.
ftp: 1020 bytes sent in 0.00Seconds 1020000.00Kbytes/sec.

```

Set the default terminal type for all users

We now open a terminal session to the NonStop host and perform the following steps:

```

TACL 1> logon super.super
Password:
Last Logon: 20 DEC 2005, 09:38
Last Unsuccessful Attempt: * NONE *
TACL (T9205D46 - 27JUN2005), Operating System G06, Release G06.27.00
(C)1985 Tandem (C)2005 Hewlett-Packard Development Company, L.P.
CPU 0, process has no backup
December 20, 2005 9:42:27
(Invoking $SYSTEM.SYSTEM.TACLLOCL)
(Invoking $SYSTEM.STARTUP.TACLCTSTM)

Loaded from $SYSTEM.STARTUP.TACLMACS:

V H F I P TYPE FI

Current volume is $SYSTEM.STARTUP
$SYSTEM STARTUP 1> osh

/home/super: cd /etc
/etc: ls -l

total 354
drwxrwxrwx 1 SUPER.SUPER SUPER 4096 Mar 3 2005 dns923
-rw-rw-rw- 1 SUPER.SUPER SUPER 1596 Jul 28 2003 inetd.conf
drwxrwxrwx 1 SUPER.SUPER SUPER 4096 Mar 29 2004 install_obselete
drwxrwxrwx 1 SUPER.SUPER SUPER 4096 Dec 6 18:59 install_obsolete
-rwxrwxrwx 1 SUPER.SUPER SUPER 488 Aug 31 1993 magic
-rwxrwxrwx 1 SUPER.SUPER SUPER 185 Dec 17 1993 printcap.sample
-rwxrwxrwx 1 SUPER.SUPER SUPER 268 Dec 6 18:59 profile
-rwxrwxrwx 1 SUPER.SUPER SUPER 268 Aug 9 1995 profile.sample
-rwxrwxrwx 1 SUPER.SUPER SUPER 166146 Jun 13 1994 termcap

```

```
-rw-rw-rw- 1 SUPER.SUPER  SUPER    1000 Dec 21 13:01 tn653_termcap.txt
/etc: cat profile
# Remove /bin/unsupported from  PATH if you DO NOT want to
# use the unsupported utilities on your system
# Note: /usr/ucb contains the OSS ftp client
#export PATH=/bin:/usr/ucb
export PATH=/bin:/bin/unsupported:/usr/bin:/usr/ucb
export TERM=xterm
export PS1='$PWD: '
/etc: cp profile profile.sav
/etc: cp termcap termcap.sav
/etc: cat tn653_termcap.txt >>termcap
/etc: mkdir /usr/local
/etc: mkdir /usr/local/bin
/etc:
```

In the above sequence of commands we open a terminal session, login as SUPER.SUPER and selected the OSS personality. We then change to the "/etc" directory, perform a directory listing and typed out the master profile file for our reference. Note that the default terminal type for OSS is "xterm". We then made a copy of the original profile file for future use/reference by copying it to profile.sav.

We then make a copy of the master TERMCAP file to TERMCAP.SAV and appended our new definition for OV 7.3 6530 terminal emulation to the end of the file.

As a final step we created the primary program execution directory for the FLOSS libraries on the assumption that we will also load the ncurses later and other packages in the future.

Change the default terminal type

Now we need to change the default terminal type from "xterm" to "tn6530-8", to do that we go back to our windows command window and perform the following additional steps:

```
ftp> get profile t1.txt
200 PORT command successful.
150 Opening data connection for profile (172.16.0.169,1282d) (392
bytes).
226 Transfer complete
ftp: 401 bytes received in 0.01Seconds 40.10Kbytes/sec.
ftp> !notepad t1.txt
```

While in notepad we make the following changes to the profile file:

```
# Remove /bin/unsupported from  PATH if you DO NOT want to
# use the unsupported utilities on your system
# Note: /usr/ucb contains the OSS ftp client
#export PATH=/bin:/usr/ucb
export PATH=/usr/local/bin:/bin:/bin/unsupported:/usr/bin:/usr/ucb
export TERM=tn6530-8
```

```
export PS1='$PWD: '
Once changes have been made, exit Notepad, saving the changes.
```

```
ftp> put t1.txt profile
200 PORT command successful.
150 Opening data connection for profile (172.16.0.169,1283d).
226 Transfer complete.
ftp: 401 bytes sent in 0.00Seconds 401000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

In the above series of commands we first bring the global profile file that applies to all users down to the local pc, we then use the notepad program to edit the file before transferring it back to the host.

Note: for the path value we specify the commands in the `/usr/local/bin` would take precedence over any like-named command in the standard OSS distribution/installation. A typical example would be the "grep" command that might be downloaded from the FLOSS library into the `/usr/local/bin`.

A more conservative value for the path definition would be:

```
export PATH=/bin/unsupported:/usr/bin:/usr/ucb:/usr/local/bin:/bin
```

At this point, to make the changes active for your terminal session, exit and re-invoke the OSS personality.

```
/home/super: exit
$SYSTEM STARTUP 3> osh
/home/super:
```

Notes

To confirm changes are in place, you may use the command `set` to see active settings:

```
/home/super: set
ERRNO=4010
FCEDIT=/bin/ed
HOME=/home/super
IFS='
'
LINENO=1
LOGNAME=SUPER.SUPER
MAILCHECK=600
OPTARG
OPTIND=0
PATH=/usr/local/bin:/bin:/bin/unsupported:/usr/bin:/usr/ucb
PPID=1
PS1='$PWD: '
PS2='> '
PS3='#? '
PS4='+ '
PWD=/home/super
RANDOM=1163074432
SECONDS=16
```



```
SHELL=/bin/sh
TERM=tn6530-8
TMOUT=0
_ =PS1='$PWD: '
```

4.5 Personal OSS TERMCAP setup

Personal OSS TERMCAP setup

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

Personal OSS TERMCAP setup

This procedure is very similar to the global setup procedure except that we are working with the user personal profile file and changes and file uploads are made to the users home directory.

```
C:\tmp>ftp ktenk
Connected to ktenk.cp.crystalpoint.com.
220 ktenk.cp.crystalpoint.com FTP SERVER T9552D40 (Version 3.e TANDEM
26FEB98) ready.
User (ktenk.cp.crystalpoint.com:(none)): tst.joe
331 Password required for TST.JOE.
Password:
230 User TST.JOE logged in. GUARDIAN API enabled
ftp> quote oss
257 OSS API enabled.
ftp> pwd
257 "/home/joe" is current directory.
ftp> put tn653_termcap.txt tn653termcap
200 PORT command successful.
150 Opening data connection for tn653termcap (172.16.0.169,2522d).
226 Transfer complete.
ftp: 1020 bytes sent in 0.00Seconds 1020000.00Kbytes/sec.
ftp> get .profile t1.txt
200 PORT command successful.
150 Opening data connection for .profile (172.16.0.169,2524d) (580
bytes).
226 Transfer complete
ftp: 598 bytes received in 0.01Seconds 59.80Kbytes/sec.
ftp> !notepad t1.txt
ftp> put t1.txt .profile
200 PORT command successful.
150 Opening data connection for .profile (172.16.0.169,2525d).
226 Transfer complete.
ftp: 598 bytes sent in 0.00Seconds 598000.00Kbytes/sec.
ftp> bye
221 Goodbye.
```

In the above sequence of commands we opened a FTP session to the host and then changed over to the OSS file space and uploaded the new TERMCAP definition for OV 7.3 as the file "tn653termcap".

We then edited the users personal profile file ".profile" by bringing it down to the local PC and using the notepad program. While in notepad we make sure that following two lines are present in the file to set the terminal type and to specify where the controlling TERMCAP file is located:

```
export TERM=tn6530-8
export TERMCAP=/home/joe/tn653termcap
```

Depending on how the user's OSS login account was created they may not have a personal profile file. One option is to simply copy the one from the "/etc" directory and modify that. Another option is to create a small one with just the above two configuration line in it.

4.6 TERMINFO Support

TERMINFO Support

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

TERMINFO Support

To advance to the next level of terminal support, which is TERMINFO, it is necessary to download certain binary files from the [HP Connect Open Source Technical Library](#). It is advised to read the web page for help in determining which files you need to download.

Typically, these are:

1. "ncurses.tar.z" which provides TERMINFO support.
2. "vim.tar.Z" which is the improved VI editor that supports function keys.
3. "gzip.tar.Z" which is the gzip utility that does an uncompress of files that end in a type of ".z" (lower case "Z").

Notes: the gzip package is not required, though since you are performing this process it is a good idea to do this right now.

If your system already features TERMINFO support, skip to the topic **COMPILE TERMINFO File** below.

For the following example we make the assumption that you pre-created a directory of "C:\TMP" and downloaded these files. The next step is to open a DOS style command window on your PC and use the intrinsic FTP to perform the following steps:

```
C:\Documents and Settings\support>cd \tmp
```

```
C:\tmp>dir
Volume in drive C has no label.
Volume Serial Number is 14A5-86F5
```

Directory of C:\tmp

```
12/19/2005 03:16 PM <DIR> .
12/19/2005 03:16 PM <DIR> ..
12/19/2005 03:16 PM          554,745 gzip.tar.z
12/19/2005 02:48 PM      7,810,397 ncurses.tar.z
12/19/2005 02:50 PM    12,322,753 vim.tar.z
12/22/2005 11:24 AM          1,020 tn653_termcap.txt
12/22/2005 11:23 AM          1,258 tn653_terminfo.txt
          5 File(s)      20,690,173 bytes
          2 Dir(s)     222,971,322,368 bytes free
C:\tmp>rename *.z *.Z
C:\tmp>ftp s72k
Connected to s72k.cp.crystalpoint.com.
220 s72k.crystalpoint.com FTP SERVER T9552G07
(Version 3.w TANDEM 29JUL2005) ready.
User (s72k.cp.crystalpoint.com:(none)): super.super
331 Password required for SUPER.SUPER.
Password:
230 User SUPER.SUPER logged in.  OSS API enabled
ftp> quote oss
257 OSS API enabled.
ftp> pwd
257 "/home/super" is current directory.
ftp> mkdir /home/super/floss
257 MKD command successful.
ftp> cd /home/super/floss
250 CWD command successful.
ftp> put tn653_terminfo.txt
200 PORT command successful.
150 Opening data connection for tn653_terminfo.txt
(172.16.0.165,3383d).
226 Transfer complete.
ftp: 1258 bytes sent in 0.00Seconds 1258000.00Kbytes/sec.
ftp> binary
200 Type set to I.
ftp> put gzip.tar.Z
200 PORT command successful.
150 Opening data connection for gzip.tar.Z (172.16.0.121,5006d).
226 Transfer complete.
ftp: 554745 bytes sent in 2.27Seconds 244.81Kbytes/sec.
ftp> put ncurses.tar.Z
200 PORT command successful.
150 Opening data connection for ncurses.tar.Z (172.16.0.121,5007d).
226 Transfer complete.
ftp: 7810397 bytes sent in 28.64Seconds 272.67Kbytes/sec.
ftp> put vim.tar.Z
200 PORT command successful.
150 Opening data connection for vim.tar.Z (172.16.0.121,5008d).
226 Transfer complete.
ftp: 12322753 bytes sent in 43.74Seconds 281.73Kbytes/sec.
ftp> bye
221 Goodbye.
```

```
C:\tmp>
```

In the above example the following steps occurred:

1. We changed to the directory from which we download the files from the ITUG user library.
2. We renamed all files that ended in lower case "Z" to an uppercase "Z". Note the three files that we downloaded the FLOSS library using Internet Explorer were more and likely saved with the lower case dot "Z" extension. If you download additional packages from the FLOSS library be sure to remember if they end in lower or upper case "Z" and rename them before transferring them to your host.
3. We then invoked the intrinsic command line FTP for windows and logged into the host as SUPER.SUPER
4. We issued the "quote oss" command to make sure that we are in the OSS file space even though the message had informed us that the OSS API was already enabled.
5. We created our upload directory at "/home/super/floss" and changed to that directory.
6. We upload our terminfo definition file for the OV, that we will compile later in this document.
7. We invoked binary file transfer mode so that future transfers would do a binary copy from our pc to the host.

We then uploaded the three archive files. Note it does not matter what case you use to specify the filename in the put command. The windows command line ftp uses the case of the filename as it is stored in the directory. That is why renamed them before transferring the files.

We then use OutsideView to connect to the NonStop system (as super.super) and invoke the open system shell and perform the following commands:

```
$SYSTEM STARTUP 1> osh
/home/super:cd /home/super/floss
/home/super/floss: ls -l
total 40407
-rw-rw-rw-  1 SUPER.SUPER      SUPER      554745 Dec 19 15:15
gzip.tar.Z
-rw-rw-rw-  1 SUPER.SUPER      SUPER      7810397 Dec 19 15:09
ncurses.tar.Z
-rw-rw-rw-  1 SUPER.SUPER      SUPER        1236 Dec 21 13:46
tn653_terminfo.txt
-rw-rw-rw-  1 SUPER.SUPER      SUPER     12322753 Dec 19 15:10
vim.tar.Z
/home/super/floss: uncompress gzip.tar
/home/super/floss: uncompress ncurses.tar
/home/super/floss: uncompress vim.tar
/home/super/floss: cd /
```

Note: It is correct behavior that some error messages display while the following commands take place. Also, be patient; these actions take a while to perform.

```
/: tar xvf /home/super/floss/gzip.tar
```

```
/: tar xvf /home/super/floss/ncurses.tar
```

```
/: tar xvf /home/super/floss/vim.tar
```

In the preceding example we performed these steps:

1. Switch from the TAACL to the OSS space
2. Changed to the upload directory that was made with the remote FTP client.
3. Uncompressed the TAR file that contains the GZIP file compress utility.
4. Uncompressed the TAR file that contains the NCURSES library.
5. Uncompressed the TAR file that contains the VIM editor utility.
6. Invoked TAR to unpack the GZIP package
7. Invoked TAR to unpack the NCURSES package
8. Invoked TAR to unpack the VIM package

COMPILE TERMINFO File

The final step is use the terminal information compiler (TIC) to compile the TERMINFO definition file for OV.

```
/: cd /home/super/floss
/home/super/floss: tic tn653_terminfo.txt
/home/super/floss:
```

After this is done the NonStop OSS has now been configured to support the OV 7.3 UNIX/OSS sub mode for both TERMCAP and TERMINFO aware UNIX programs.

If it is desired to replace the usage of VI with its more powerful and modern VIM you can add the following line to the appropriate profile file.

```
alias vi=vim
```

Changing Terminal Type on the FLY

With the addition of a simple script to the appropriate profile file you can add a command that can be executed by the user to change the terminal type on the fly.

The simple script for this adds a command (capital "T").

Type "T" alone tells you the term type, while type "T newterm" ("T ansi", for example) will show you what your TERM was and now is.

Caveats to remember: functions do not carry over to sub-shells, so if you shell out of an application this function will not be available. Functions run before any commands in the PATH with the same name, so if there were a /usr/local/bin/T command, the function T would run first unless you invoked it as "/usr/local/bin/T".

After making this change our /etc/profile file would have the following contents:

```
# Remove /bin/unsupported from PATH if you DO NOT want to
# use the unsupported utilities on your system
```

```
# Note: /usr/ucb contains the OSS ftp client
#export PATH=/bin:/usr/ucb
export PATH=/usr/local/bin:/bin:/bin/unsupported:/usr/bin:/usr/ucb
export TERM=tn6530-8
export PS1='$PWD: '
#
# Shell script to allow user to dynamically change their terminal
type
#
T() {
if [ -z "${1}" ]
then
echo "Your TERM type is set to $TERM"
else
echo "Your TERM was $TERM \c"
TERM=${1}
export TERM
echo "and is now $TERM"
fi ;
}
```

Adding support for Service Processor connections and non line mode operations

On "S" series systems the telnet connections to the service processor function differently and do not negotiate for line mode operations which are normally used by the emulator to detect the switch between the Guardian and OSS environment. Other power users may also de-select the telnet option to negotiate line mode on a normal telnet connection.

Automatic switching can still be accomplished when entering the OSS environment by adding another command to the appropriate profile file (global or personal). That command is:

```
tput is1
```

Note: This command is only available if you install TERMINFO support into your OSS environment.

4.7 Guardian File System Graphical Navigation

Guardian File System Graphical Navigation

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

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, FTPHINTS** or via the supplied **Host Scanning Utility, OVFSKAN**. 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.

Host hint files are required for graphical FTP file transfer and for navigation on NonStop systems without an OSS environment. 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 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 OVFSCAN. 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 OVFSCAN as an executable file. Make sure you are in the system area, and then type the command: `FUP ALTER OVFSCAN, CODE 100`

Notes

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

5 Support

5.1 Contact Support

Contact Support

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

Contact Support

Help us help you. Crystal Point is committed to supporting all users running the current version of OutsideView. 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 reduce call volumes by:

- Trying to find the solution in the online help.
- Checking the OutsideView error log. This log may have information that helps identify where your problem is occurring.
- Checking our online Technical Support site. We have a searchable AnswerBook online.
- 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 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
Tech Support (Toll free): (800) 982-0881
Tech Support (Direct): (425) 806-1119
Main Phone: (425) 487-3656
Fax: (425) 487-2880

5.2 Pre-Compilation of .Net components

Pre-Compilation of .Net components

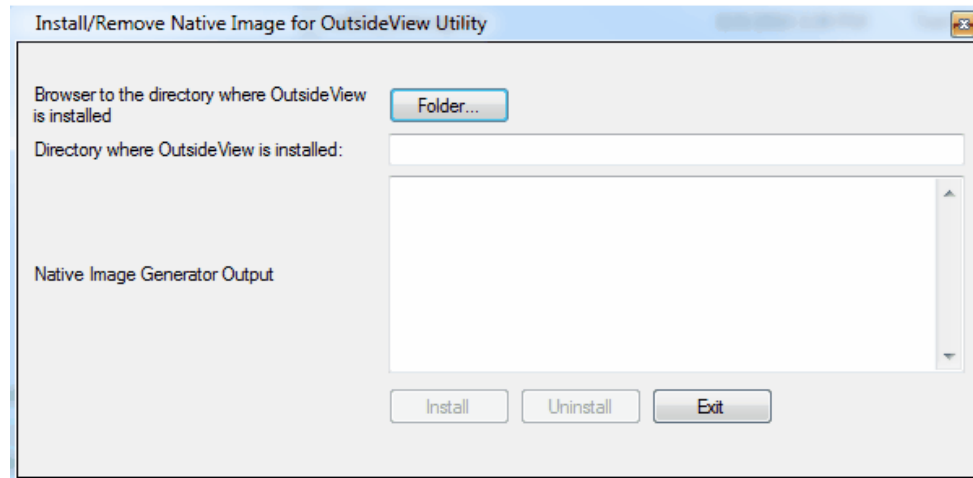
[Top](#) [Previous](#) [Next](#)

Pre-Compilation of .Net components

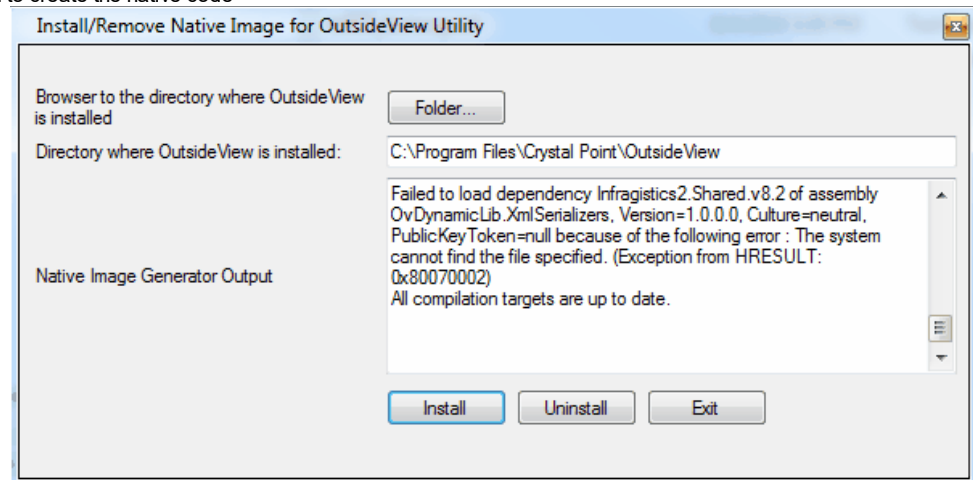
OutsideView makes extensive use of .Net technology. It is typical when using .Net components that they are compiled

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 and see the following dialog:



- A) Browse to your OutsideView installation location (typically C:\Program Files\Cystal Point\OutsideView)
- 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.

5.3 Diagnostic Tools

Diagnostic Tools

[Top Previous](#)

Diagnostic Tools

Diagnostic Traces

A diagnostic trace file may be requested by Crystal Point Technical Support when diagnosing a problem 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 overwriting the file. If the answer is Yes, the saved file is overwritten. If the answer is No, the trace process is cancelled.

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

- 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.
- Click the Session Settings button on the toolbar, or select Session: Session Settings from the menu.
- Click the Capture link on the Category list.
- In the Diagnostic Trace group box, click the To File checkbox. This will enable the Trace function.
- 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.
- Click the OK button. OutsideView will close this dialog box and begin the diagnostic trace.
- Starting from a command prompt (e.g., a TACL prompt) perform the steps required to duplicate the error.
- 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 to our Technical Support staff as an attachment.

There is also an FTP trace capability. It is designed for use only with new FTP sessions, not within saved FTP sessions (since it will not capture session initiation). To activate the trace function, select Session, FTP, NEW and rather than initiating the session 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

Index

- . -

.NET framework 20
 .Net interactions 5
 .Net JIT compiler 117

- A -

Ambiguous characters 6
 Application Publishing Wizard 39
 Asian 6
 Asian Usage Notes 6
 Automatic Updates of OutsideView Maintenance releases 48
 Automatic Updating 47

- B -

Background 104

- C -

Capture 119
 Change Override Password 55
 Check In 79, 82
 Check Out 79, 83
 Chinese 6
 Citrix 39
 Citrix Server Installation 39
 Client Installation 37
 Client Settings 65
 code editor 5
 Concurrent 77
 Concurrent Encrypted 77
 Connecting SQL LicenseView to SQL-based License Pools 44
 Contact Support 117
 controlling Profile behavior 56
 Corporate Licensing 10
 Create Network Shares 20
 Creating License Pools 80
 Creatng Multiple Profiles 36

- D -

Desktop 9, 77
 Desktop Installation 9
 Desktop License 9, 77, 80
 Diagnostic Tools 119
 Directories tab 57
 Disable printing/screen snapshots 68
 Disable session/workspace/macro menu items (lockdown) 68
 Disaster Recovery 19
 Double-wide 6

- E -

Enterprise Failover 19
 Enterprise Mode Overview 8
 Enterprise Overview 17
 Enterprise:Administration 54
 Enterprise:Installation 17
 Enterprise:Licensing 77
 Example Installation 41
 Example Multiple-profile, Multiple License Pool Installation 41
 Expired 79
 Export License 81
 extended license checkout 84

- F -

Failover 19
 Feature Release 49
 Feature Upgrade 49

- G -

General Settings 62
 Global OSS TERMCAP setup 105
 Groups:Multiple Profiles 36
 Groups:OutsideView Profile 36

- H -

Help Desk 117
 Housekeeping 65
 html tunnel 12

html tunneling 12

- I -

ID Type Centralized Control 62
Import a Desktop License 80
Importing Licenses 80
Installing:Client 37
Installing:Desktop 9
Installing:Enterprise 20
Installing:WTS/Citrix 21

- J -

Japan 6
Japanese 6
Japanese Usage Notes 6

- K -

Korean 6

- L -

License Alerts 85
License available offline 84
License File 21
License Pool:Add/Import Licenses 80
License Pool:Check License Out 83
License Pool:Create New Pool 80
License Pool:Export Licenses 81
License Pool:Make License Available Offline 84
License Pool:Releasing Licenses 82
License Pool:Reports 85
License Pool:Synchronize 84
License Pool:View Status 79
Licenses, Synchronize All 84
Licenses, Synchronize Selected 84
LicenseView 42, 81, 82, 84, 85
Licensing Overview 77
Limit 58
Lockdown 68
lockdown mode' 68
Lockdown privileges, typically 68

- M -

maintenance update 48
Major Release 50
Major Upgrade 50
Make a license available offline 84
Media 21
Modify 58
mouse roller wheel 71
Moving Enterprise Installations 51
Multi-Hop SSH Tunneling 5
Multiple Profiles 36

- N -

network share 20
network share point 17
New Session tab 72

- O -

OutsideView 21, 37
OutsideView CD:installing 9
OutsideView Desktop 9
OutsideView Enterprise 17
OutsideView Silent Installation Shortcut 54
OutsideView:installing 21
Override Mode 55, 58

- P -

Password 55
patch 48
PC 37
permissions 58
Personal OSS TERM CAP setup 109
Populate Share s 21
Pre-Compilation of .Net components 117
pristine mode 69
pristine-mode 65
Privileges 54, 55, 58
Profile 36, 54
Profile Name 21
Publishing 39
purge of local settings 65

- R -

redirect.dat 51
Releasing License 82
relocation 51
Requirements 103
Restrict open session/workspace to user's own
Param directory 68

- S -

SCCM (SMS) Installation 11, 38
Seamless Guardian/OSS support 103
Server Installation 21, 39
Settings tab 71
sharepoint 20
Silent Install 21, 37
SQL LicenseView 42, 87
SQL-based license pools 42
Supervisor Mode 54, 55, 58
Supervisor Override 55
Synchronize the License Pool 84

- T -

Technical Support 117
TERMINFO Support 110
Trace 119
tunnel 12

- U -

Unix/X11 mouse text selection 71
Updates 47
Upgrades 47
user permissions 58
User Preference Files 65
user privilege 54
User Privileges 58, 62
User Profile 21

- V -

Version Compatibility 6
View License Status 79

- W -

Windows Terminal Server 39
Windows Terminal Server or Citrix Server Installation
39
WTS/Citrix 21, 39

Endnotes 2... (after index)

Back Cover