Rocket BlueZone Desktop

Administrator's Guide

Version 6.1

August 2013
BZD-0601-AG-04

Notices

Edition

Publication date: August 2013

Book number: BZD-0601-AG-04

Product version: Rocket BlueZone Desktop Version 6.1

Copyright

Trademarks

Examples

This information might contain examples of data and reports. The examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

License agreement

Note

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

Contact information

Website: www.rocketsoftware.com

Rocket Software, Inc. Headquarters
77 4th Avenue, Suite 100
Waltham, MA 02451–1468
USA
Tel: +1 781 577 4321
Fax: +1 617 630 7100

Contacting Global Technical Support

If you have current support and maintenance agreements with Rocket Software, you can access the Rocket Customer Portal and report a problem, download an update, or read answers to FAQs. The Rocket Customer Portal is the primary method of obtaining support.

To log in to the Rocket Customer Portal, go to:

www.rocketsoftware.com/support

If you do not already have a Rocket Customer Portal account, you can request one by clicking **Need an account?** on the Rocket Customer Portal login page.

Alternatively, you can contact Global Technical Support by email at support@rocketsoftware.com.

Contents

What's new in this release

This section summarizes the significant improvements or enhancements for BlueZone Desktop Version 6.1 and refers you to relevant sections of this book for more information. Minor modifications to the text are not listed.

BZD-0601-AG-02 December 2012

- You can set the feature locks at the session level with command line switches. Refer to Locking features using command line switches, on page 41 for more information.

BZD-0601-AG-02 September 2012

- The operating system requirements have been updated. Refer to Minimum installation requirements, on page 21 for more information.
- "Installing BlueZone Plus VBA" has been updated to include the new installer information. Refer to Installing BlueZone Plus VBA, on page 33 for more information.
- The registry locations are new for BlueZone 6.1. Refer to BlueZone registry entries, on page 19 for more information.
- You can now hide the dialog configuration profile toolbar buttons. Refer to Configuring the dialog configuration profile locks, on page 41 for more information.
- "Changing the BlueZone Display and Printer language" is a new topic. Refer to Changing the language in BlueZone, on page 65 for more information.
- PasswordVault is installed as a stand-alone application through an MSI. You cannot install PasswordVault through the BlueZone Desktop installation process. Refer to PasswordVault installation, on page 111 and the *BlueZone PasswordVault User's Guide* for more information.
- The `[BZSetup]` section of the `setup.ini` file has the following changes:
  - `DestinationDir=` and `WorkingDir=` now specify the version number.
  - `WorkingDirType=` is a new entry. This entry eliminates the need for the following entries:
    - `UsePersonalFolderAsWorkingDir=Yes`
    - `UseAllUsersCommonFolderAsWorkingDir=No`
    - `UseCurrentUserAppDataFolderAsWorkingDir=No`
  - `CopyPrevWorkingDir=` is a new entry.

  Refer to BZSetup section, on page 118 for more information.
- In the `[Program Group]` section of the `setup.ini` file, the `GroupName=` setting now specifies the version number. Refer to Program Group section, on page 124 for more information.
- The `global.ini` file has the following new information:
  - `AppendVersionToWorkingDir=` and `AllowCrossVersionInterop=` are new settings in the `[BlueZone]` section. Refer to BlueZone section, on page 130 for more information.
  - The `[Help]` section is new. Refer to Help section, on page 132 for more information.
- The `language.ini` file is now shipped with BlueZone. Refer to Default language.ini file, on page 133 for more information.

Chapter 1: BlueZone Desktop introduction

Welcome to the *BlueZone Desktop Administrator's Guide*. This guide provides information on installing, configuring, and distributing BlueZone Desktop.

BlueZone is a comprehensive, fully featured Windows-based secure LAN/WAN to host connectivity product. BlueZone can be installed on any Microsoft Windows Server 2003, Windows Server 2008, Windows XP SP3, Windows Vista, or Windows 7 system where users require secure (using SSL and TLS encryption) and non-secure access to Telnet and FTP hosts. BlueZone can be preconfigured for distribution to users from a web server, file server, terminal server, or through email.

BlueZone Desktop is Windows XP SP3, Windows Vista, and Windows 7 certified.

BlueZone emulation clients include:

- BlueZone IBM 3270 Display emulator
- BlueZone IBM 3270 Printer emulator
- BlueZone IBM 5250 Display emulator
- BlueZone IBM 5250 Printer emulator
- BlueZone VT - VT100, VT220, VT320 emulator
- BlueZone Secure FTP client
- BlueZone ICL 7561 Display emulator *
- BlueZone Unisys UTS Display emulator *
- BlueZone Unisys T27 Display emulator *

* Available as an additional cost option

Intended audience

This manual was written for system administrators and systems programmers responsible for installing, configuring, and deploying BlueZone Desktop to users. This guide is not intended for users. Directed your users to the *BlueZone Display and Printer User's Guide* for help with the BlueZone emulation clients.

It is assumed that you have a working knowledge of Microsoft Windows operating systems, basic local area and wide area networking concepts, file and directory structures, and some familiarity with the IBM host systems and other hosts and networks to which your users will be connecting.

Overview

BlueZone is compliant with Federal Information Processing Standards (FIPS) 140-2 - Security Requirements for Cryptographic Modules. FIPS is a set of standards that describe document processing, provide standard algorithms for searching, and provide other information processing standards for use within government agencies. FIPS also provides requirements for the encryption of data. FIPS is a standard that describes requirements for cryptography modules and components. The standard is published by the National Institute of Standards and Technology (NIST).

BlueZone for the Mainframe

BlueZone for the Mainframe provides secure LU2 Display emulation and LU1 and LU3 Printer emulation. BlueZone was designed and implemented using industry standard APIs, allowing it to communicate through leading SNA Gateways and TN3270/TN3270E connections.

BlueZone for the Mainframe ships with the following communication links:

- TN3270/TN3270E
- Microsoft SNA Server and Host Integration Server
- IBM Communications Server for NT
- Novell IntraNetware for SAA

BlueZone for the iSeries

BlueZone for the iSeries provides secure LU7 Display emulation, LU4 SCS Printer emulation, and supports iSeries Host Print Transform.

BlueZone for the iSeries ships with the TN5250/TN5250E communication link.

BlueZone VT

BlueZone VT provides secure (through SSL and SSH) and non-secure VT100, VT220, VT320, and VT420 emulation for UNIX, Linux, VAX, and other ASCII hosts through Telnet connections.

BlueZone VT also supports Kerberos Authentication Protocol. Kerberos is a computer network authentication protocol that allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. Kerberos prevents eavesdropping or replay attacks and ensures the integrity of the data. It provides mutual authentication; both the user and the server verify each other's identity.

BlueZone Secure FTP

BlueZone Secure FTP provides secure and non-secure file transfer protocol with a graphical user interface to transfer files over TCP/IP networks between the user's computer and any FTP server including Mainframe and iSeries FTP hosts.

Other BlueZone products

The following BlueZone products are included in the standard BlueZone distribution.

BlueZone PasswordVault
: Provides a convenient, easy-to-use means of storing, managing, and accessing your host account logon information. BlueZone PasswordVault is an optional, no cost feature that is installed as a stand-alone application.

BlueZone Security Server
: A Windows OS-based application that provides SSL connectivity and redirection for the entire family of BlueZone emulation clients if SSL is not available on the host system.

BlueZone License Manager
: A Windows OS-based application that manages the BlueZone concurrent user licensing method.

Optional BlueZone products

The following BlueZone products are available as extra cost options and are not part of the standard BlueZone distribution image. These items are supplied to customers who have purchased the appropriate licenses.

BlueZone Visual Basic for Applications

BlueZone ICL 7561
Provides secure and non-secure access to ICL hosts supporting the 7561 data stream using the RFC1006 specification through TCP/IP.

BlueZone T27
Provides secure and non-secure access to UNISYS hosts.

BlueZone UTS
Provides secure and non-secure access to UNISYS hosts.

Display emulator features

The BlueZone Display emulators are fully featured and comprehensive emulation software programs that emulate a variety of IBM and other terminal types. BlueZone can emulate the following terminal types:

- IBM 3270 Mainframe TN3270E
- IBM 5250 iSeries (AS/400) TN5250E
- Virtual Terminal (VT52, VT100, VT220, VT320, VT420, SCOANSI, WYSE60, VAX/AIX, HP2392A, HP70092/6, HP70094/8, LINUX, and IBM3151)
- ICL 7561
- Unisys T27
- Unisys UTS

Emulation features

BlueZone emulators contain the following features:

- Screen buffer sizes from 1,920 to 9,920 bytes, equivalent to IBM models 2 through 5, and model 3290
- Screen colors and keys that can be mapped, changed, or deleted by the user
- GUI editing of EBCDIC to ASCII translation tables
- Fully featured customizable Terminal status bar
- Selectable code page
- Customizable translation table
- Mainframe Vector Graphics Support (IBM Mainframe only)
  - Vector Graphics Screen Printing

Encryption and security

BlueZone emulators provide the following encryption and security:

- SSL 3.0
  - Implicit mode
  - Explicit (Telnet negotiated) mode
- TLS 1.0
  - Implicit mode
  - Explicit (Telnet negotiated) mode
- SSH-2 (BlueZone VT only)
- FIPS mode support
- Kerberos Authentication Protocol (BlueZone VT only)

File transfer features

BlueZone emulators provide the following file transfer features:

- FTP secure file transfer
- IND$FILE transfer (IBM Mainframe only)
- iSeries file transfer (IBM iSeries and AS/400 only)
- iSeries LIPI file transfer (IBM iSeries and AS/400 only)
  - SQL Statement Building feature

Program features

- Compatible with Windows 7
- BlueZone PasswordVault
- Internet Protocol v4 and v6 support
- Language support
  - English
  - French
  - German
  - Dutch
  - Japanese
- Double-byte character support
- Bidirectional language support (BiDi) for Arabic
- Up to 99 sessions per computer
- Mapping session IDs to LU names support
- Customizable main program menu bar feature
- Configuration management features include saving and opening of configuration files
- Profile schemes feature
- User-definable and sizable Windows Vista style iconic toolbars
  - Pixel sizes of 16 x 16, 24 x 24, 32 x 32 and 48 x 48 are supported
- User definable and sizeable status bar
  - Pixel sizes of 16 x 16, 24 x 24, 32 x 32 and 48 x 48 are supported

- User definable and fully configurable Power Pads with buttons, images and text
- Optional user-definable and dockable Power Keys
- Intelligent edit, copy, cut, and paste with columns aligned
- Robust print screen capability
- Macro/script recording for easy scripting of repetitive tasks
- Script Editor to modify and extend the functionality of BlueZone scripts
- Visual Basic Scripting through BlueZone Scripting Host
- BlueZone Plus VBA (Visual Basic for Applications) support *
- Customizable desktop colors and fonts
- Customizable background watermark feature
- Configurable host bell support
- Configurable mouse scroll wheel support
- Windows application sounds support

* BlueZone is available with the Microsoft VBA development environment and runtime license as BlueZone Plus VBA. BlueZone Plus VBA is required for everyone who develops and/or runs BlueZone Plus VBA applications. Existing BlueZone customers can upgrade their existing BlueZone license to BlueZone Plus VBA. Contact your BlueZone Account Executive for more information about upgrading to BlueZone Plus VBA.

Printer emulation features

The BlueZone printer emulators are fully featured and comprehensive IBM printer emulation printer software programs that emulate several printers.

Printer emulations

- IBM 3287
  - LU1 SCS
  - LU3 DSC
- IBM 3812-1 single-byte
  - Host print transform
  - Extended SCS
- IBM 5553 double-byte
  - Host print transform
  - Extended SCS

Emulation features

- Passthrough printing feature for direct output to printer
- Host print transform support (iSeries only)
- Full support of line density and print density SCS character formatting
- Override host formatting capabilities
- Fully featured customizable terminal status bar
- Selectable code page
- Customizable translation table

Encryption and security

- SSL 3.0
  - Implicit mode
  - Explicit (Telnet negotiated) mode
- TLS 1.0
  - Implicit mode
  - Explicit (Telnet negotiated) mode
- FIPS mode support

Program features

- Compatible with Windows 7
- Internet Protocol v4 and v6 support
- Language support:

  - English
  - French
  - German
  - Dutch
  - Japanese

- Double-byte character support
- Up to 99 sessions per workstation
- User-definable and sizeable Windows Vista style iconic toolbars
- User sizeable toolbars: 16 x 16, 24 x 24 (default size), 32 x 32, and 48 x 48 are supported
- User sizeable status bar: 16 x 16 (default size), 24 x 24, 32 x 32, and 48 x 48 are supported
- Configuration management features include saving and opening of configuration files
- View print queue and print log lists for easy print job management
- Drag-and-drop print job icon feature
- Robust printer and page layout configuration settings
- Precise use of host page margins by printing to unprintable region of page
- GUI editing of EBCDIC to ANSI translation tables
- Change printer profiles with a single click
- Robust print to file options
- Customizable desktop colors
- Customizable background watermark

BlueZone TCP/IP Print Server features

BlueZone TCP/IP Print Server is a Windows application that supports the Line Printer Daemon (LPD) protocol that enables users to receive and customize print jobs from a Line Printer Request (LPR) client on any AS/400, Mainframe, UNIX, or Windows-based system, to any Windows defined printer, whether locally attached or remote.

BlueZone TCP/IP Printer Server provides the following features:

- Easy to configure multi-panel graphical user interface
- Has the same look and feel as the BlueZone Printer emulation clients
- Supports multiple printer queues
- Supports multiple printing methods:
  - Passthrough
  - Passthrough with a printer definition file
  - Windows API
- Runs unattended and listens for print jobs
- Runs in the Windows taskbar

PasswordVault features

BlueZone PasswordVault is an automatic password storage program that is included in the standard BlueZone distribution. BlueZone PasswordVault is installed as a stand-alone application through an MSI.

BlueZone PasswordVault provides the following features:

- Easy to configure floating graphical user interface
- Stores all of your account logon credentials in a single encrypted file
- Automatic host logon screen detection
- Automatic credential application
- On-the-fly credential creation
- Wire feature for non standard host logon fields
- Strong password generator
- Secret question feature in case of forgotten PasswordVault password
- Supports multiple user authentication methods:
  - Password-based authentication
  - Windows-based authentication
  - Standard Windows user name and password
  - Windows fingerprint recognition
  - Windows Smart Card support

BlueZone licensing

BlueZone supports two licensing methods: concurrent user and single user licensing.

Concurrent user license

The concurrent user license is for pools of users with variable connection requirements and is based on the number of simultaneous, or concurrent users. It provides an unlimited license to copy and distribute BlueZone.

The BlueZone License Manager must be installed on a server or PC in the network to control the number of concurrent licenses. A license key is provided to activate the License Manager with the purchased number of concurrent users.

Refer to BlueZone License Manager, on page 88 for details on how to configure BlueZone to work with the BlueZone License Manager.

Single user license

The single user license is for an individual and can only be installed on one computer. The single user license requires the use of a Software Activation File (SAF). A Software Activation File can be obtained by running the BlueZone Registration Wizard.

Refer to Registering BlueZone, on page 25 for details on how to obtain a Software Activation File and register it.

File system

BlueZone saves all of its settings in files, called configuration files. All of the parameters for each session are saved in a single file. BlueZone registers the file extensions to Windows during setup. Double-clicking a configuration file starts the corresponding BlueZone emulator, and

loads the saved settings. Double-clicking the configuration file multiple times, opens multiple, identical BlueZone sessions.

Users can open their saved configuration files in Session Manager. Session Manager displays the configuration files that are in the `\Config` folder in the user's working directory. Refer to Chapter 6: BlueZone Session Manager for more information on Session Manager.

Starting new BlueZone sessions

When starting new BlueZone sessions without specifying a session profile (using Session Manager or `/F` switch) the user is prompted to select an existing session profile or create a new one.

Saving in profile mode

The configuration file used to launch the session displays on the session title bar. **File** ® **Save** saves any changes made to the session to the session profile. **File** ® **Save As** prompts the user to create a new file which saves all the current settings in the emulator.

BlueZone can automatically create a backup of the session profile each time a save is performed. When this feature is enabled, the last version of a session profile contains the words `Backup of` added to the beginning of the file name.

For example: `Test.zmd` becomes `Backup of Test.zmd`

Important

If multiple sessions are open using the same session profile, the last session to perform a save overwrites any settings saved from previously saved sessions.

This feature can be turned on by selecting the **Auto-Backup settings in Profile Mode** check box, which is located on the **Options** tab in File Properties.

Opening session profiles in profile mode

Performing a **File** ® **Open** in a BlueZone session loads the settings from the selected session profile into the session. The session profile name displays on the BlueZone title bar.

Cloning sessions in profile mode

To clone the current session, select **File** ® **Open Session** ® **Same Session Type** and BlueZone launches a new session window using the session profile from the current session. Using the **Open Session** tool bar button is a convenient way to clone sessions.

Note

If you want to prevent end users from opening more than one session from a particular profile, you can make a change to the `setup.ini` file. Refer to Profile sharing feature, on page 34 for more information.

Opening different session types

File ® **Open Session** ® **Different Session Type** prompts the user to select a session profile for the new session.

Auto-launching sessions using File ® **Properties** ® **AutoLaunch**

The user can automatically launch up to four additional sessions by selecting the check box and selecting the session type to launch. The session profile to use when launching each session must be specified in the **Switches** field using the `/F` command line switch. For example, `/Fmysession.zmd`.

CAUTION

Failure to specify a session profile results in an unconfigured session launching.

Launching BlueZone FTP from a BlueZone Display session

BlueZone FTP sessions can be launched from a BlueZone Display emulator session using **Transfer** ® **FTP**. The first time a FTP session is launched, the user is prompted to select a FTP session profile. Upon subsequent launches, BlueZone FTP loads the previously selected session profile.

Launching a pre-configured BlueZone FTP session

If you prefer to launch a preconfigured BlueZone FTP session, create a BlueZone FTP profile with the same name as the display session profile you want to launch it from.

For example, if you want to launch BlueZone FTP from a Mainframe Display session, and the name of the profile used to launch the Mainframe session is `MAINFRAME.ZMD`, then create a BlueZone FTP profile called `MAINFRAME.ZFT`.

Base registry setting

BlueZone settings are saved in the Windows registry. The registry location where they are saved depends on the value for the base registry setting in the `setup.ini` file.

By default, the base registry setting is 0.

Base registry 0

Global settings are saved in the Local Machine key. User-level settings are saved in the Current User key. This is the default setting for BlueZone Desktop. By using this mode, you can configure BlueZone so that each individual user can store their own user-level settings.

Base registry 1

Global and user settings are saved in the Local Machine key. Use this mode if all of the users of the computer must share both global and user settings.

Base registry 2

Global and user settings are saved in the Current User key. This mode is typically not used for BlueZone Desktop.

Global settings

Global settings apply to the BlueZone product as a whole. For example, the location of the BlueZone Windows installation directory is a global setting because it applies to the entire BlueZone application, which is by default stored in the HKEY_LOCAL_MACHINE key.

Other examples are specific feature settings, lock settings, and mode settings that apply to all BlueZone sessions.

User-level settings

User-level settings apply to individual BlueZone sessions. For example, the location of the user's `My Documents` folder, which is by default stored in the HKEY_LOCAL_USER key.

Other examples are individual BlueZone session keys like Mainframe Display S1, that contains all of the information about a specific BlueZone session.

Setting the base registry value

Use a text editor to edit the `setup.ini` file. From the table below, choose the value, and type it in the `BaseRegisrty=`*`value`* entry.

0	HKEY_CURRENT_USER (Session Settings - Default)
1	HKEY_LOCAL_MACHINE (All Settings)
2	HKEY_CURRENT_USER (All Settings)

For example:

```
[BZSetup]
BaseRegistry=0
```

BlueZone registry entries

BlueZone creates the following entries in the Windows registry:

In Windows XP SP3

- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1
- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1\About
- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1\Support
- HKEY_CURRENT_USER\Software\BlueZone\6.1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Session Manager

  Note

  Additional Registry sub keys are created for each BlueZone session when they are first started and are numbered sequentially: S1, S2, S3, … S99; or P1, P2, P3, … P99; or T1, T2, T3, … T99. They are deleted from the Registry when the session is closed.

- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\VT S1

In Windows 7 or Vista (32-bit)

- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1
- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1\About
- HKEY_LOCAL_MACHINE\SOFTWARE\BlueZone\6.1\Support
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Session Manager

  Note

  Additional Registry sub keys are created for each BlueZone session when they are launched and are numbered sequentially: S1, S2, S3, … S99; or P1, P2, P3, … P99; or T1, T2, T3, … T99. They are deleted from the Registry when the session is closed.

- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\VT S1

In Windows 7 or Vista (64-bit)

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlueZone\6.1
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlueZone\6.1\About
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BlueZone\6.1\Support
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Session Manager

Note

Additional Registry sub keys are created for each BlueZone session when they are launched and are numbered sequentially: S1, S2, S3, … S99; or P1, P2, P3, … P99; or T1, T2, T3, … T99. They are deleted from the Registry when the session is closed.

- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\AS/400 Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Display S1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\Mainframe Printer P1
- HKEY_CURRENT_USER\Software\BlueZone\6.1\VT S1

Chapter 2: BlueZone installation

BlueZone is distributed through a downloaded CD image.

The following steps are a high-level overview of the standard installation process:

1. Review and ensure that your system meets the installation requirements.
2. Install, upgrade, or modify BlueZone.
3. Register BlueZone (first time installations only).

BlueZone has a number of features that cannot be installed unless the feature is configured before the installation process. Some features require that an entry in the `setup.ini` file be edited. Other features require moving a file or files to a particular location. In either case, it is recommenced that you review the BlueZone optional installation features first, before performing your first BlueZone installation. Refer to Configuring optional features, on page 27 for more information.

After you complete these steps, you can distribute BlueZone to a large number of users, control BlueZone file location, create a BlueZone distribution image, push out a quiet mode installation to your users, and so on. Refer to Distributing BlueZone, on page 76 for more information.

BlueZone setup program

The BlueZone setup program, `setup.exe`, opens the installation wizard that installs BlueZone.

The file names and a description of every file that is included in the BlueZone image, is provided in the BlueZone file listing. This information is useful when planning the deployment of BlueZone to your users. If a function or feature is not required for an installation, then the associated files can be omitted from the distribution image.

The BlueZone setup program works in conjunction with the `setup.ini` file which is located in the same folder on the BlueZone CD image as the `setup.exe` program.

Refer to Creating a distribution image, on page 77 for more information.

Minimum installation requirements

The BlueZone emulation clients are designed specifically for computers that are running a Windows operating system using the WIN32 API to allow computers in a LAN/WAN environment to communicate with a wide variety of host systems. To function properly, BlueZone must be installed on a computer that meets the following minimum hardware and software requirements:

Operating system requirements

Microsoft Windows XP SP3, Windows Vista, Windows 7, Windows Server 2003, or Windows Server 2008

Hardware requirements

- A processor capable of supporting one of the above operating systems
- At least the minimum amount of memory required by your operating system
- Typically 30 MB of disk space (or less) for installation
- VGA Display or better

Communications library requirements

- SNA Server Client 3.0 or higher (LUA/RUI only)
- Communications Server for NT 6.0 or higher (LUA/RUI only)
- Netware for SAA 2.2 or IntraNetware for SAA 3.0 (LUA/RUI only)

.NET Framework requirements

- Microsoft .NET Framework 3.5 (for BlueZone UTS and T27 Display emulators only)

Windows Vista and Windows 7 support

BlueZone has undergone third-party testing to become Microsoft Certified for Windows Vista. This means that BlueZone passed all of the tests to ensure smooth installation and operation, as well as a user experience consistent with the Windows Vista operating system. Some of the hallmarks of Windows Vista include User Access Control, Protected Mode, and the ActiveX Installer Service. The following guide describes using BlueZone with Windows Vista or Windows 7.

- BlueZone is installed using the Microsoft Installer (MSI).
- BlueZone uses the permissions **As-Invoker** when running and does not require administrator permission to perform any regular BlueZone function.
- Installing for All Users under an administrator account is recommended.
- BlueZone configuration files, scripts, macros, and so on can be deployed with the BlueZone MSI automatically by including them in the BlueZone installation source directory image. Refer to Creating a distribution image, on page 77 for more information.
- All user files are written to `All Users\Application Data\BlueZone\` at installation time.
- On the first run, BlueZone copies the files from `All Users\Application Data\BlueZone\` to the user's working directory.
- At run time, BlueZone compares the files in the user's working directory to those in `All Users` and updates the user's working directory with any new files found in `All Users\Application Data\BlueZone\`.

Installing BlueZone 6.1

Prerequisite

- Ensure that your environment meets the installation requirements. Refer to Minimum installation requirements, on page 21 for more information.
- Locate the software activation file (SAF) that was sent to your by Rocket Software. You will need to access this file during the installation process.
  If you do not have an SAF, or if you are evaluating BlueZone, you can skip the Choose Activation File window, and install the SAF at another time.

  Note

  If you are a single user license holder, you do not receive a software activation file; you receive a BlueZone installation key. Single user license holders must run the BlueZone Registration Wizard to complete the installation process. Refer to Registering BlueZone, on page 25 for more information.

Procedure

1. Download the BlueZone CD image.
2. Open the `BlueZone Desktop` folder.
3. Double-click the `setup.exe` file.
4. The wizard guides you through the installation process. It is recommended to use the default settings.
5. When the installation is complete, click **Finish**.

Upgrading to BlueZone 6.1

There are two methods to upgrade BlueZone: upgrade to a new major version or upgrade within the same major version.

Upgrading to a new major version

You can upgrade from any earlier major version of BlueZone to BlueZone 6.1. For example, you can upgrade from version 5.2 to 6.1. BlueZone 6.1 is installed as a new product, and it can run side-by-side with any earlier major version of BlueZone.

The upgrade procedure is identical to installing a new installation. Refer to Installing BlueZone 6.1, on page 22 for the upgrade procedure.

If you do not want the old version installed, you can uninstall the old version. Refer to Uninstalling BlueZone, on page 25 for more information.

Upgrading within the same major version

If a patch is available, you can upgrade within the same major version. For example, you can upgrade from version 6.1.1 to 6.1.2. If a patch is not available, the `\Patches` folder will be empty.

As the BlueZone administrator, you can push the patch file out to your users. This allows your users to upgrade with a single file.

1. Download new BlueZone CD image.
2. Open the `BlueZone Desktop\Patches` folder.
3. Perform one of the following options:
   - To upgrade a single installation, double-click the `BlueZone Patch 6.1.`*`x`*`.`*`xxxx`*`.exe` file. The wizard guides you through the upgrade procedure.
   - To push the patch upgrade out to your users, distribute the patch file to your users, and instruct them to run the file.

Modifying BlueZone

BlueZone consists of multiple components. Most likely, you do not need to install all of the BlueZone components. By default the BlueZone installation wizard installs the following components (they are listed in the order that they display in the installation wizard Component Selection window):

- BlueZone Session Manager
- Mainframe - BlueZone Mainframe Display
  - Mainframe Printer

- iSeries - BlueZone iSeries Display
  - iSeries Printer
- VT - BlueZone VT
- FTP - BlueZone FTP
- BlueZone Scripting and Automation Components
- HLLAPI Components

The following BlueZone components are not installed by default and must be selected during the installation process in order for these components to be installed:

- Kerberos - Installs Kerberos Single Sign-on Protocol
- ICL - BlueZone ICL Display emulation
- Unisys T27 - BlueZone Unisys T27 Display emulation *
- Unisys UTS - BlueZone Unisys UTS Display emulation *
- BlueZone TCP/IP Print Server

* These components require an additional cost license and may not be present in your installation.

BlueZone has a number of features that cannot be installed unless the feature is configured in some way before the installation process takes place. Some features require that the `setup.ini` file be edited. Some features require moving a file or files to a particular location. In either case, it is recommenced that you review the BlueZone optional installation features first, before performing your first BlueZone installation. Refer to Configuring optional features, on page 27 for more information.

When BlueZone is installed, you can add any of the BlueZone components that were not installed during the initial installation or you can remove any of the BlueZone components that you no longer need.

For example, if you are an IBM 3270 Mainframe user and you accidentally installed BlueZone for the iSeries (IBM 5250 emulation), you can remove the BlueZone iSeries component.

Procedure

1. Open the `BlueZone Desktop` folder.
2. Double-click `setup.exe`.
3. Select your language from the menu and click **OK**.
4. Select the **Modify** radio button and click **Next**.
5. In the Component Select window, select the features that you want to modify:
   a. Review the list of your currently installed components.

      The components that have a diskette icon are currently installed. The components that have a red X icon are available for installation.

      Note

      For a description of a particular component, highlight the component and read the **Feature Description** in the right pane.

   b. Click the BlueZone components that you want to change and select an installation option.
6. Click **Next**.
7. Click **Install**.

The Wizard installs the required BlueZone files on your computer. When the installation is complete, you receive a message that the BlueZone installation was completed successfully.

8. Click **Finish**.

Registering BlueZone

If you have a BlueZone single user license, you received a BlueZone installation key. Single user license holders must run the BlueZone Registration Wizard to complete the installation process.

The first time you start a BlueZone session you receive a message that you need an activation file to start BlueZone. If you have a software activation file, follow the instructions in the message. If you do not have an activation file, run the Registration Wizard.

1. Start a BlueZone session.

   A message opens asking if you want to run the Registration Wizard.
2. If you do not have an activation file or you have a single user license, click **Yes**.
3. Enter the appropriate information in all of the fields. All of fields are required.
4. Click **Next**.
5. Select the **via Web (requires direct Internet connection)** radio button and click **Next**.

   The Registration Wizard connects to the Registration Wizard server, exchanges information, and downloads the Software Activation File.
6. Click **Next**.

   The Registration Wizard shows the full path where it saved the Software Activation File in your BlueZone installation directory.
7. Click **Finish**.

Note

If you have purchased multiple BlueZone Desktop licenses, install the software and run the Registration Wizard on each machine using the same Installation Key. The Registration Wizard keeps track of the number of installations and does not allow any more than the number of licenses purchased. The Software Activation File that is generated is unique to each machine and does not work if copied to another machine.

Uninstalling BlueZone

The process of uninstalling BlueZone is very similar to installing BlueZone.

Note

In addition to using the BlueZone installation wizard to uninstall BlueZone, you can also uninstall BlueZone through Add or Remove Programs in the Windows Control Panel. If this method is used, the BlueZone working directory is not removed. The BlueZone working directory can be manually deleted.

1. Open the `BlueZone Desktop` folder.
2. Double-click `setup.exe`.
3. Select your language from the menu and click **OK**.
4. Click **Next**.

   The Program Maintenance screen opens and the **Remove** radio button is automatically selected.

5. Click **Next**.
6. Click **Remove**.

   A message opens asking if you want to remove your working directory and its contents.
7. Click the **Yes** or **No** depending on whether or not you need the contents of the working directory.

   CAUTION

   The working directory contains BlueZone Profiles (configuration files) and scripts. If you click **Yes**, these files are deleted.
8. Click **Finish**.

Chapter 3: Configuring BlueZone

You can configure many aspects of BlueZone. For example, you can create preconfigured sessions that automatically connect to the host, create desktop shortcuts, automatically generate LU or device names, or map unique keyboards.

The following topics describe the parts of BlueZone that you can configure.

BlueZone working directory

The BlueZone setup program creates a directory structure to store the BlueZone working files: configuration, scripts, keyboard, macro files, and so on. This directory is known as the BlueZone working directory.

By default, the BlueZone working directory is created in the user's `My Documents` personal folder.

BlueZone setup does not place files in any common Windows directories other than the font files, eliminating the problems created by other emulators that install files in the Windows System directory.

Table 1: Default working directory locations lists the default locations of the working directory by operating system.

Table 1: Default working directory locations

Operating system	Location
Windows XP SP3	`C:\Documents and Settings\`*`Username`*`\My Documents\BlueZone`
Windows 7 and Vista	`C:\Users\`*`username`*`\Documents\BlueZone`

Table 2: Working directory subfolders lists the subfolders in the working directory.

Table 2: Working directory subfolders

Subfolder	Contents
`\Certs`	SSL certificate files
`\Config`	BlueZone configuration and keyboard map files
`\Macros`	BlueZone macro files
`\Scripts`	BlueZone script files
`\Spool`	BlueZone Printer spool files
`\Traces`	Traces taken using the trace facility in the TN3270/5250 driver
`\Transfer`	Files transferred using the IND$FILE utility, BlueZone Secure FTP, or Kermit

Configuring optional features

BlueZone has several optional features. Some of the BlueZone optional features can be installed using the standard installation wizard. However, there are several additional options and features that require manual configuration.

1. Determine the features that you want to enable/disable. The optional features that can be set are:
   - Customize the main BlueZone menu bar, on page 28
   - Customize the main BlueZone title bar, on page 29
   - Enable the power key feature, on page 31
   - Enable Kerberos Authentication Protocol, on page 32
   - Enable FIPS mode support, on page 32
   - Install Unisys T27 and UTS Terminal emulators, on page 32 *
   - Install BlueZone Plus VBA (Visual Basic for Applications), on page 33 *
   - BlueZone ActiveX control
   - Control file location, on page 33
   - Disable profile sharing, on page 34
   - Install script player only feature, on page 34
   - Add Session Manager in the startup folder, on page 35
   - Add Session Manager in the Windows taskbar, on page 35
   - Enable the LU name mapping feature, on page 36
   - Disable the append to clipboard feature, on page 36
   - Enable BlueZone feature locking, on page 38
   - Lock the License Server tab, on page 38
   - Enable the Telnet locking feature, on page 39
   - Enable the display locking feature, on page 39
   - Enable the font locking feature, on page 40
   - Disable the show locked dialogs feature, on page 40
   - Enable the dialog configuration profile toolbar locking feature, on page 41
   - Enable the BlueZone Secure FTP locking feature, on page 42

   * These features are available as additional cost options.
2. Make the necessary change for each feature.
3. Double-click `setup.exe` to reinstall BlueZone.

   If you have enabled any new emulator types, like the UTS terminal emulator, you must select it in the Component Selection window.

Customizing the main menu bar

Starting with BlueZone Version 5.1, you can control the appearance of the main BlueZone menu bar located at the top of the BlueZone application desktop. You can select the menu bar items that you want to be displayed or hidden. You also have the option of hiding the menu bar altogether.

To customize the menu bar, you must edit the settings in the `global.ini` file.

Note

Starting with BlueZone Version 5.1, the **Macro** menu item is no longer displayed on the BlueZone menu bar. If you want to enable the **Macro** menu item, you must modify the `global.ini` file in your installation image.

You can remove one or all of the items that appear on the menu bar. In addition, there is also a **View Properties** pop-up menu that can be accessed from the main BlueZone application

window by right-clicking anywhere in the main window. This pop-up menu can also be turned off through a setting in the `global.ini` file.

When a BlueZone Session is launched, the BlueZone program checks the `global.ini` file in the BlueZone installation directory. The contents are read in and the BlueZone application desktop is changed accordingly.

Note

The BlueZone Installation Wizard automatically places the modified `global.ini` file in the user's BlueZone installation directory.

1. Open the `global.ini` file in a text editor.
2. Locate the `[Menu]` section.
3. Make any desired changes. Refer to Menu section, on page 128 for the possible menu bar settings.
4. Save and close the file.

Customizing the main title bar

You can control the appearance of the main BlueZone title bar located at the top of the BlueZone application desktop. You can select the title bar items that you want to be displayed or hidden. You also have the option of displaying a custom title bar and/or a custom icon.

To customize the title bar, you must modify the Title Bar options located on the File Properties window.

1. Click **File** ® **Properties**.
2. Click the **Title Bar** tab.

Figure 1: Title bar properties

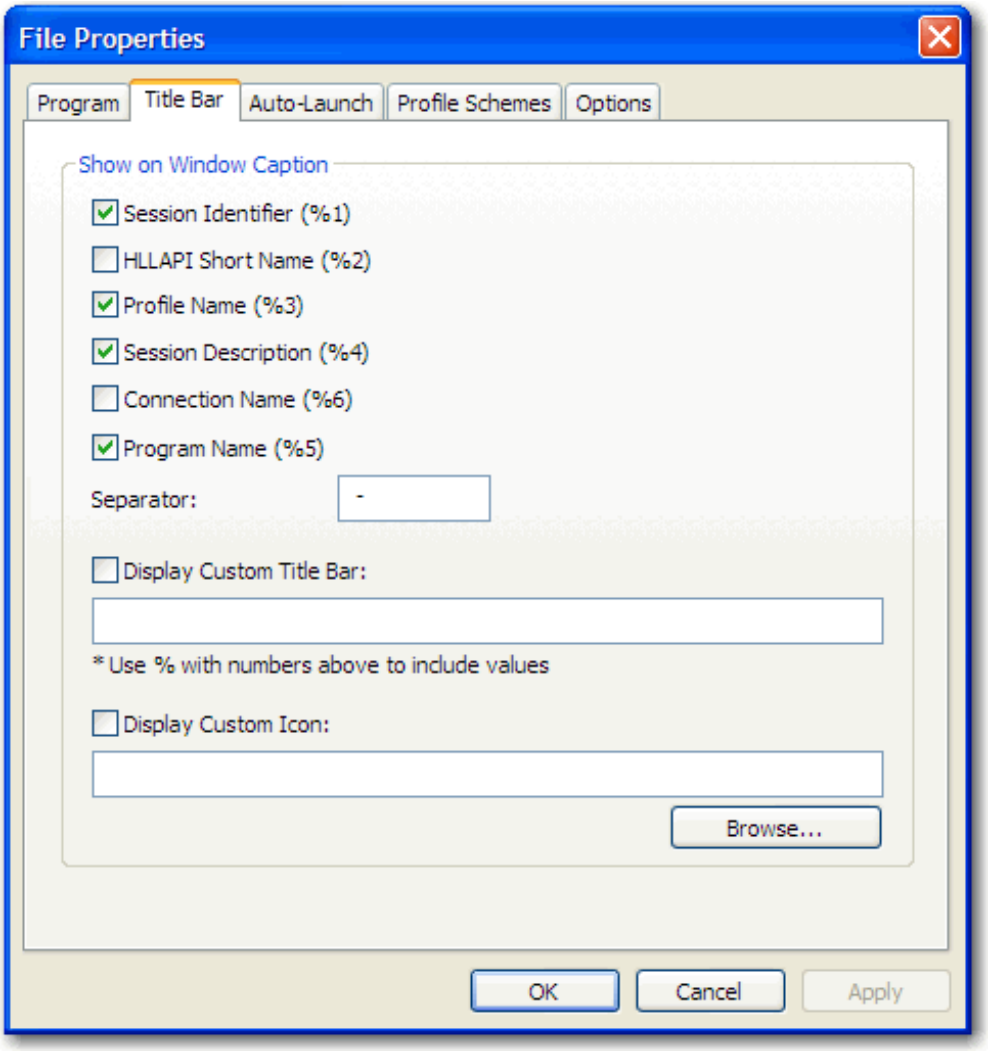


Figure 1: Title bar properties shows all of the title bar options. The default settings (items that are selected) are Session Identifier, Profile Name, Session Description, and Program Name. You can turn off these items or you can create you own custom title bar by using the variables (%1, %2, %3 and so on) in the **Display Custom Title Bar** field.

- **Session Identifier (%1)**: Includes the standard BlueZone Session Identifier in the title bar. For example, S1, S2, S3 and so on.
- **HLLAPI Short Name (%2)**: Includes the standard BlueZone HLLAPI Short Name Session Identifier in the title bar.
- **Profile Name (%3)**: Includes the name of the current BlueZone profile that was used to open this session in the title bar.
- **Session Description (%4)**: Includes the value of the **Session Description** field located on the **Program** tab in the title bar.

Note

If the **Use Connection Name as Session Description** check box in the **Connections** tab (**Session** ® **Configure** and click **Properties**) is selected, the Connection Name that was used to create the session is displayed on the title bar instead.

- **Connection Name (%6)**: Includes the value of the **Connection Name** field located in the Edit Connection window in the title bar.

  Note

  If the **Use Connection Name as Session Description** check box in the **Connections** tab (**Session** ® **Configure** and click **Properties**) is selected, the Connection Name is displayed twice in the title bar.

- **Program Name (%5)**: Includes the standard BlueZone program name in the title bar. For example, BlueZone Mainframe Display, BlueZone iSeries Display, and so on.
- **Separator**: Type a character to be used to separate the above values. Spaces are valid separators and can be used in conjunction with other characters. The default separator is space hyphen space (-).
- **Display Custom Title Bar**: If selected, any text that is placed in this field display on the title bar instead of the selected values above. This feature overrides any of the above items. You can build a custom title bar with the above variables in any order that you want You can also mix in your own text as well.

  For example, if you want the session description followed by the session identifier followed by the words `Claims Application` to display in the title bar, type the following in the field:

  ```
  %4 - %1 - Claims Application
  ```

  Important

  If the **Display Custom Title Bar** check box is selected and the field is left blank, the result is a blank title bar.

- **Display Custom Icon**: If you want to change the icon that displays on the BlueZone title bar, select this check box and browse to the location where the desired icon is located. It is suggested to keep the icon in a predicable location like the BlueZone installation directory.

Enabling the power keys feature

Starting with BlueZone Version 4.0, the power keys feature has been replaced with a new feature called power pads. By default the power pads feature is enabled when BlueZone is installed.

However, the power keys feature has not been eliminated from BlueZone; it has only been turned off. If you want, you can enable the old power keys feature.

To enable the power keys feature:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file with a text editor.
3. In the `[BZSetup]` section, locate the `EnablePowerKeys=No` entry.
4. Change `No` to `Yes`.
5. Save and close the file.

After the installation is complete, the power keys feature is enabled for all BlueZone emulation clients.

Note

You cannot enable the new power pads feature and the old power keys feature at the same time. You can only have one or the other enabled.

Enabling Kerberos Authentication Protocol

Kerberos Authentication Protocol is available as an optional, no additional cost feature. By default, Kerberos is not included as part of the standard BlueZone installation and is not available in the Components Selection window when installing BlueZone.

To enable Kerberos Authentication, you must copy the Kerberos CAB file to the `BlueZone Desktop` installation source directory:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `\Kerberos` folder.
3. Copy the `bzkerb.cab` file from the `\Kerberos` folder to the `BlueZone Desktop` folder.

   When you install BlueZone, Kerberos is available in the Component Selection window.

Enabling FIPS mode support

Starting with version 4.2, BlueZone has the option of supporting FIPS mode. By default, the FIPS mode feature is turned off.

To enable FIPS mode support:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `FIPSMode=No` entry.
4. Change `No` to `Yes`.
5. Save and close the file.

   After the installation is complete, FIPS mode is enabled for all BlueZone emulation clients and sessions.

If you already have BlueZone installed, you can check if FIPS mode support is enabled:

1. Open the BlueZone emulator that you want to check.
2. From the BlueZone menu bar, click **Session** ® **Configure**.
3. Click **Properties**.
4. Click the **About** tab.
5. Under the SSL information, either **FIPS Mode Enabled** or **FIPS Mode Disabled** displays.

Installing T27 and UTS terminal emulation

BlueZone T27 and BlueZone UTS Display emulators are available as additional cost options. By default, they are not included as part of the standard BlueZone installation and are not in the Components Selection window.

Note

You must have a special Software Activation File (SAF) called `bzallwin.saf` in order to run BlueZone T27 or BlueZone UTS. If you do not have the `bzallwin.saf` file, contact your BlueZone account executive.

To install either of these products, you must copy their respective CAB files to the BlueZone installation source directory.

1. Open the `BlueZone Desktop` folder you that created on your hard drive.
2. Open the `\Unisys` folder.
3. Copy the following files from the `\Unisys` folder to the `BlueZone Desktop` folder:

- BZT27.CAB
- BZUTS.CAB
- UNISYS.CAB

4. Double-click the setup.exe file to reinstall BlueZone.

   BlueZone T27 Display and BlueZone UTS Display will be available in the Component Selection window.

Installing BlueZone Plus VBA

BlueZone Plus VBA is available as an additional cost feature. You must obtain a BlueZone Plus VBA license in order to use BlueZone Plus VBA. If you do not have this license, contact your BlueZone account executive.

To install BlueZone Plus VBA:

1. Obtain the BlueZone Plus VBA installation file (bzvbai.exe) from your BlueZone account executive.
2. Save bzvbai.exe in the same folder that contains bzvba.cab.
3. Use one of the following methods to install BlueZone Plus VBA:
   - Install from bzvbai.exe (verbose mode). Double-click the executable to open an installation wizard.
   - Install from command line in verbose mode: bzvba /i
   - Install from command line in quiet mode: bzvba /i /q

There are the three different ways that the program can be used to uninstall BlueZone Plus VBA:

- Uninstall from Windows Add or Remove Programs (verbose mode)
- Uninstall from command line in verbose mode: bzvba /u
- Uninstall from command line in quiet mode: bzvba /u /q

Refer to the *BlueZone Advanced Automation Developer's Guide* for more information on developing applications with BlueZone Plus VBA.

Controlling file locations

During the installation of BlueZone, you can control the location of the BlueZone program and user-level files. Both types of files can be stored in the same location or different locations.

You can control these locations two ways:

- By using the BlueZone Desktop setup.exe installation program.
  During the BlueZone installation, you can change the default locations to a locations of your choice.
- By modifying the setup.ini file so that the default locations match your requirements before starting the BlueZone installation.

File location options

Destination directory

Can be any location on your machine. It is recommended to use the default value:
C:\Program Files\BlueZone\6.1

Use personal folder as working directory

Yes: Places all user-level files like BlueZone configuration files and scripts in the user's `My Documents` folder.

No: Places all user-level files like BlueZone configuration files and scripts in the BlueZone installation directory unless the value of the **Use all users common folder as working directory** (see below) is set to **Yes**.

Use all users common folder as working directory

Yes: Places all user-level files like BlueZone configuration files and scripts in the `All Users` common folder.

No: Follows the value for **Use personal folder as working directory** described above.

Profile sharing feature

If you are using profile mode, by default your users can open multiple BlueZone sessions from a single profile (configuration file). In other words, multiple BlueZone sessions can share a single profile. If you do not want your users have this option, you can configure BlueZone so that only one session can be opened per profile. This is accomplished by turning off profile sharing in the BlueZone `setup.ini` file.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `ProfileSharing=` setting.
4. Change the value from `Yes` to `No`.

```
[BZSetup]
ProfileSharing=No
```

5. Save and close the file.

Refer to Default setup.ini file, on page 118 for a complete example of the `setup.ini` file.

If profile sharing is disabled, when a user attempts to open a second BlueZone session from the same profile, no error message displays. Instead, the BlueZone session that is already open is given focus.

Installing the Script Player Only feature

During the BlueZone installation, if the scripting and automation feature is selected, users can play, edit, and record scripts.

If you do not want your users to be able to record or edit BlueZone scripts, but you still want them to be able to play BlueZone scripts, you can turn off the script editing and recording functions.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `InstallScriptPlayerOnly=No` entry.
4. Change the value from `No` to `Yes`:

```
[BZSetup]
InstallScriptPlayerOnly=Yes
```

5. Save and close the file.

Refer to Default setup.ini file, on page 118 for a complete example of the `setup.ini` file.

The BlueZone Scripting CAB (`bzsc.cab`) file contains the BlueZone Script Host (`bzsh.exe`), the BlueZone Script Host Player Only (`bzshp.exe`) , and the BlueZone Script Editor (`bzse.exe`) files. If the BlueZone Scripting CAB is deployed with `InstallScriptPlayerOnly=No`, all three files are deployed. When all three files are present in the installation, users can record, edit, and play all BlueZone script types. By setting the value to `Yes`, only the `bzshp.exe` file is deployed. When only this file is present in the installation, users can only play BlueZone scripts and not record or edit them.

Note

If you are manually creating a BlueZone distribution image file, `bzsc.cab` must be part of the BlueZone distribution image in order for this setting to have any affect.

Adding Session Manager in the startup folder

You can have a shortcut for the BlueZone Session Manager automatically added to the user's Windows startup folder. This causes the BlueZone Session Manager program to automatically start each time the computer is started.

By default, this feature is disabled. To enable this feature:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[Desktop Shortcuts]` section, locate the `SessionManagerInStartupFolder=No` entry.
4. Change `No` to `Yes`:

```
[Desktop Shortcuts]
SessionManagerInStartupFolder=Yes
```

5. Save and close the file.

Refer to Default setup.ini file, on page 118 for a complete example of the `setup.ini` file.

Adding Session Manager in the Windows taskbar

You can have Session Manager automatically added to the Windows taskbar when the Session Manager program is opened. By default, this feature is not enabled.

The Windows taskbar is located at the lower right corner of your Windows desktop. After Session Manager opens, the Session Manager icon displays in the Windows taskbar. When the icon displays in the Windows taskbar, it means that the program is running in the background. This makes it easier to access Session Manager. It also makes it possible to use the Session Manager Quick Launch feature.

Refer to the *BlueZone Session Manager User's Guide* for more information on the Quick Launch feature.

After BlueZone Session Manager is running, user's can turn this feature on or off. As the BlueZone Administrator, you can decide whether or not you want this feature turned on by default.

To enable this feature:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. Locate the `SessionManagerRunInTray=No` setting.
4. Change `No` to `Yes`:

```
[BZSetup]
SessionManagerRunInTray=Yes
```

5. Save and close the file.

Refer to Default setup.ini file, on page 118 for a complete example of the `setup.ini` file

Enabling LU name mapping feature

BlueZone Mainframe Display and iSeries Display emulators can map LU names to the BlueZone session identifier. This is accomplished by creating an LU map in the `global.ini` file.

Note

This feature can also be used to map Device names for AS/400 and iSeries systems as well.

This feature is similar to using the `/L` command-line switch to set the LU name.

1. Open the `BlueZone Desktop` installation source directory.
2. Open `global.ini` in a text editor.
3. Locate the `[LuMap]` section:

```
[LuMap]
;xD_Sy_Lu="LuName"
```

4. Delete the semicolon at the beginning of the entry and modify the entry to match your requirements.
   Where *x* is:
   - M for Mainframe
   - A for AS/400

   y is the session ID: 1, 2, 3, and so on.
   LuName is the LU name to be mapped.
5. Save and close the file.

Examples

To always associate the S1 Mainframe Display primary connection with LU name `LuS1`, modify the `[LuMap]` section to:

```
[LuMap]
MD_S1_Lu="LuS1"
```

To always associate the S1 iSeries Display primary connection with device name `BOBDISP`, modify the `[LuMap]` section to:

```
[LuMap]
AD_S1_Lu="BOBDISP"
```

Refer to Default global.ini file, on page 128 for a complete example of the `global.ini` file.

Configuring the disable append to clipboard feature

The disable append to clipboard feature controls the ability for users to be able to use the append to clipboard feature of BlueZone. By default, the ability to append is turned on.

To disable the append to clipboard feature:

1. Open the `BlueZone Desktop` installation source directory.

2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `DisableAppendToClipboard=No` entry.
4. Change `No` to `Yes`:

```
[BZSetup]
DisableAppendToClipboard=Yes
```

5. Save and close the file.

Note

Disabling this feature does not affect the ability to use the copy to clipboard feature. Only the append to clipboard feature is disabled.

BlueZone feature locking

BlueZone provides a feature locking capability. You can distribute preconfigured versions of BlueZone that prevents your users from making changes to some or all of the BlueZone features. BlueZone feature locking is controlled by several settings in the `setup.ini` file.

When the `setup.ini` file is configured to lock features, all of those features are locked in the distributed sessions. If this is too restrictive, you can use command line switches to lock features in specific sessions. Refer to Locking features using command line switches, on page 41 for more information.

There are two levels of feature locking: dialog and sub-dialog level.

Dialog-level

This feature uses a system that can lock BlueZone configuration features at the dialog-level. For example, if you lock the Display Options window, users cannot change any of the settings in the entire Display Options window. Locked windows can be viewed by your users, but they cannot save any changes. Dialog-level locking is accomplished by disabling the **OK** button.

You can also determine whether or not you want the locked windows to be displayed. By default, if you lock a window, your users can still view the locked window and its current settings. By setting the show locked dialogs feature to `No`, your users cannot view any of the locked windows. If they try to view a locked window, an error message opens.

For a complete list of BlueZone windows that can be locked, refer to BlueZone feature locks, on page 155.

Sub-dialog level

If locking an entire window is too restrictive, you can hide individual window tabs. This prevents your users from being able to see or change configuration options that are stored in those tabs. You can view and configure the options on all of the tabs and save them to your BlueZone top-level configuration file.

There are two windows that you can lock specific tabs:

- Telnet Properties window
  Refer to Configuring the Telnet locking feature, on page 39 for more information.
- Display Options window
  Refer to Configuring the display locking feature, on page 39 for more information.

If you are also using BlueZone Secure FTP client, you can configure the BlueZone Secure FTP client to inherit certain BlueZone lock values and can also prevent users from executing certain FTP commands.

Configuring feature locking

Using the BlueZone `setup.ini` file to lock BlueZone features is the easiest method and is recommended unless you are performing an automated installation in which case, setting the lock values in the Windows Registry is required.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `Lock=` entry.

   To set the BlueZone configuration lock, the `Lock=` value is set to the sum of the features to be locked. When BlueZone is installed, it reads the `Lock=` value from `setup.ini` and prevents the end user from making any changes by disabling the **OK** buttons for those locked features.
4. Determine the features that you want to lock. Refer to BlueZone feature locks, on page 155 for the features and their values.
5. To lock all of the features listed in the BlueZone feature lock table, type a value of `-1`:

   ```
   [BZSetup]
   Lock=-1
   ```

6. To lock a single feature, enter the value of the feature in the `Lock=` value.

   For example, if you want to lock the Display configuration settings, add the DISPLAYLOCK value of 16:

   ```
   [BZSetup]
   Lock=16
   ```

7. To lock multiple features, add the values of the features together and type the sum in the `Lock=` value.

   For example, if you want to lock the Translate Tables and Keyboard configuration settings, add the KEYBOARDLOCK value of 8 and the TRANSLATELOCK value of 512 together for a total of 520:

   ```
   [BZSetup]
   Lock=520
   ```

8. Save and close the file.

Locking the License Server tab

You can prevent your users from changing the values in the **License Server** tab in the Session Configuration window with the LICENSELOCK feature. This tab contains settings such as the license server IP address and group names.

Note

If you enable the session lock feature (SESSIONLOCK), the **License Server** tab is automatically locked.

The LICENSELOCK feature was specifically added so that it is possible for you to configure BlueZone so that users can change Telnet session information but not change any information stored in the **License Server** tab.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `Lock=` setting.
4. To enable the LICENSE LOCK feature, set `Lock=` to 32768:

```
[BZSetup]
Lock=32768
```

Refer to BlueZone feature locks, on page 155 for a complete listing of all the BlueZone lock features and their values.

5. Save and close the file.

Configuring the Telnet locking feature

If locking all of the BlueZone session configuration settings through the SESSIONLOCK feature is too restrictive, you can use the Telnet locking feature to hide the Telnet Configuration window tabs that you do not want your users to access.

For example, you can allow your users' to change the Connections and the Device settings but none of the other Telnet settings.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. Determine the Telnet configuration features that you want to lock. Refer to Telnet feature locks, on page 158 for the list of features and their values.
4. To hide a single feature, type the value of the feature in the `LockTelnet=` value.

   For example, if you want to hide the **Security** tab, set the `LockTelnet=` to 4:

   ```
   [BZSetup]
   LockTelnet=4
   ```

5. To hide multiple features, add the values of the features together and type the sum in the `LockTelnet=` value.
   For example, if you want to hide the **Firewall** and **Security Server** tabs, add the value of 64 and 128 together and set the `LockTelnet=` to 192:

   ```
   [BZSetup]
   LockTelnet=192
   ```

6. Save and close the file.

CAUTION

Do not use the LOCKALLCONFIG (Lock=-1) or the SESSIONLOCK (Lock=64) settings in conjunction with the Telnet locking feature. Using either of these settings makes it impossible for your users to access the BlueZone Telnet settings which defeats the purpose of the feature.

Configuring the display locking feature

If locking all of the BlueZone Display configuration settings through the DISPLAYLOCK feature is too restrictive, you can use the display locking feature to hide the Display Configuration window tabs that you do not want your users to access.

For example, you can allow your users to change the Font and Cursor settings but not the Colors, GUI, Watermark, or Advanced settings.

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. Determine the display configuration features that you want to lock. Refer to Display feature locks, on page 158 for a list of the features and their values.
4. To hide a single feature, type the value of the feature in the `LockDisplay=` value.

   For example, if you want to hide the **Colors** tab, set the `LockDisplay=` to 4:

```
[BZSetup]
LockDisplay=4
```

5. To hide multiple features, add the values of the features together and type the sum in the `LockDisplay=` value.

   For example, if you want to hide the **GUI** and **Advanced** tabs, add the value of 8 and 32 together and set the `LockDisplay=` to 40:

   ```
   [BZSetup]
   LockDisplay=40
   ```

6. Save and close the file.

Configuring the font locking feature

By default, users can change the configured font. If you do not want your users to change the font, you can use the BlueZone DISPLAYLOCK feature lock to disable all of the options in the Display Options window. Refer to Configuring feature locking, on page 38 for more information.

However, if you only want to lock the currently configured font and do not want to disable the other options in the Display Options window, use the font locking feature.

To lock the configured font:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `FontLock=` setting.
4. Change `No` to `Yes`:

   ```
   [BZSetup]
   FontLock=Yes
   ```

5. Save and close the file.

When the font lock feature is enabled, the **Change** button in the **Font** tab of the Display Options window is disabled. The **Font** tab is accessed by selecting **Options** ® **Display** from the BlueZone menu bar.

Configuring the show locked dialogs feature

If you set the `Lock=` entry, you can also disable the show locked dialogs feature. By default, the show locked dialogs feature is enabled. When enabled, this feature allows the BlueZone windows to display even when they are locked. The user can see the values in the windows but the **OK** button is disabled so they cannot save any changes.

When the show locked dialogs feature is disabled, the locked windows are not displayed. If a user tries to open a locked window, an error message opens.

To disable the show locked dialogs feature:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `ShowLockedDialogs=Yes` entry.
4. Change the value from `Yes` to `No`:

   ```
   [BZSetup]
   ShowLockedDialogs=No
   ```

5. Save and close the file.

Note

This feature only works in conjunction with the `Lock=` feature and not the `LockTelnet=` or `LockDisplay=` features.

Configuring the dialog configuration profile locks

Many BlueZone windows contain configuration profile toolbar buttons. Refer to BlueZone dialog configuration profiles, on page 57 for more information.

You can hide some or all of the configuration profile toolbar buttons:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `global.ini` file in a text editor.
3. In the `[BlueZone]` section, locate the `;HideDialogButtons=` entry.
4. Delete the semicolon at the beginning of the entry.
5. To hide a single button, type the value of the button in the `HideDialogButtons=` entry. For example, to hide the Save As button, set `HideDialogButtons=` to 8:

   ```
   [BlueZone]
   HideDialogButtons=8
   ```

6. To hide multiple buttons, add the button values together and type the sum in the `HideDialogButtons=` entry. For example, to hide the Open and Save As buttons, set `HideDialogButtons=` to 10:

   ```
   [BlueZone]
   HideDialogButtons=10
   ```

7. Save and close the file.

Locking features using command line switches

You can use command line switches to lock BlueZone features, BlueZone display features, and BlueZone Telnet features. You can use any method that passes a command line switch to the program. For example, you can set the command line switch through a desktop shortcut, DOS prompt, open settings in the registry, and so on.

For example, to start the Mainframe Display session `Session1.zmd` with the keyboard settings locked, use the `Bzmd.exe /fSession1.zmd /.8` command.

Table 3: Feature lock command line switches

Feature	Command line switch
BlueZone features	/.*x* Where *x* is the lock feature value. Refer to BlueZone feature locks, on page 155 for a list of the available values.
BlueZone display features	/,*x* Where *x* is the lock feature value. Refer to Display feature locks, on page 158 for a list of the available values.
BlueZone Telnet features	/`*x* Where *x* is the lock feature value. Refer to Telnet feature locks, on page 158 for a list of the available values.

BlueZone Secure FTP locking

BlueZone Secure FTP locking is slightly different from BlueZone feature locking because there are multiple levels of BlueZone Secure FTP locking.

Inheriting common lock values from BlueZone

There are several features that BlueZone and BlueZone Secure FTP have in common. The locking of one or more of these common features can be inherited by BlueZone Secure FTP.

For example, if you want to lock the BlueZone Session settings, you can configure BlueZone Secure FTP to inherit the session lock setting from BlueZone.

Locking specific FTP functions

BlueZone Secure FTP has FTP functionality that does not exist in BlueZone. You can configure BlueZone Secure FTP to lock one or more specific FTP functions. Some of the functions are program related and some are FTP commands.

For example, if you are using BlueZone Secure FTP to upload files only, you can prevent your end users from being able to use BlueZone Secure FTP to download files by locking the FTP Retrieve (RETR) command.

Locking individual BlueZone Secure FTP features

If for any reason, using the inherit feature is too restrictive, you can choose to configure BlueZone Secure FTP features on a more granular basis.

Inheriting common lock values from BlueZone

By default, BlueZone Secure FTP does not inherit any of the BlueZone lock settings. BlueZone Secure FTP can inherit three of the BlueZone lock settings. These common settings are shown in the BlueZone feature lock table.

Refer to BlueZone feature locks, on page 155 for more information.

1. If you want BlueZone Secure FTP to inherit these lock settings from BlueZone, type `1024` in the `LockFTP=` setting:

```
[BZSetup]
LockFTP=1024
```

2. If you want any additional BlueZone Secure FTP function lock options, add those values to 1024 and type the sum in the `LockFTP=` setting.

Locking BlueZone Secure FTP commands and features

There are two categories of specific BlueZone Secure FTP features:

- The ability to lock (or block) FTP commands
- The ability to lock (or block) BlueZone Secure FTP program features

Refer to BlueZone Secure FTP command and feature locks, on page 155 for the lock values.

Each FTP command or program feature listed in the table can be locked individually or if you want to lock more than one item, add the values of the items together and place the sum in the `LockFTP=` setting.

For example, if you want to prevent your end users from being able to create a new directory and prevent them from changing the BlueZone Secure FTP host configuration settings, add the Block Make Directory Command value of 32 and the Lock Configuration Settings value of 8 together for a sum of 40. Replace the 0 value with 40:

```
[BZSetup]
LockFTP=40
```

Locking individual BlueZone Secure FTP features

In some cases, the inheriting common lock values from BlueZone feature can be too restrictive. If this is the case, you can choose to lock BlueZone Secure FTP features on a more granular basis. Several BlueZone Secure FTP dialogs can be locked item by item where others can be disabled completely.

Locking is a way to disable or "gray out" one or more features or an entire dialog. In most cases, users can still see the locked features, but they cannot change or otherwise access them.

The following dialogs can be customized by disabling each individual item.

In Session Configuration:

Connections dialog

Options dialog

In the New, Edit or Copy dialogs:

Connection dialog

Miscellaneous dialog

The remainder of the dialogs can only be completely disabled:

Initial Commands dialog

Schedule dialog

Firewall dialog

Security dialog

Certificate dialog

1. Open the `setup.ini` file in a text editor.
2. Edit the desired FTP features. The options listed above are shown in red:

```
[BZSetup]
LockFTPSession=0
LockFTPConnection=0
LockFTPInitialCommands=0
LockFTPMiscellaneous=0
LockFTPSchedule=0
LockFTPFirewall=0
LockFTPSecurity=0
LockFTPCertificate=0
```

3. Save and close the file.

Locking the Session Configuration dialog

The session configuration lock table contains the values required to lock one or more individual features of the Session Configuration dialog. The Session Configuration dialog in BlueZone Secure FTP consists of multiple tabs. Only the items located on the **Connections** tab and the **Options** tab can be locked.

To lock the **License Server** tab, refer to Inheriting common lock values from BlueZone, on page 42 for more information.

Note

Typing a −1 locks all the items located on the **Connections** and **Options** tabs.

1. Open the `setup.ini` file in a text editor.
2. To lock a single item, type the value assigned to that item in the `LockFTPSession=` setting.

For example, to lock only the New button, type a 2 in the LockFTPSession= setting as shown here:

```
LockFTPSession=2
```

3. To lock more than one item, add the values together and type the sum in the LockFTPSession= setting.

   For example, to lock the New, Edit and Copy buttons, add 2, 4 and 8 together and type the sum in the LockFTPSession= setting:

   ```
   LockFTPSession=14
   ```

4. Save and close the file.

Refer to the session configuration lock table in BlueZone Secure FTP individual feature locks, on page 156 for a complete list of values.

Locking the Connection dialog

In addition to the **Connections** and **Options** tabs, there are items located on several tabbed dialogs located inside the main Session Configuration dialog. These additional dialogs can be accessed through the New, Edit or Copy buttons.

Note

Typing a -1 locks all the items located on the Connections dialog.

1. Open the setup.ini file in a text editor.
2. To lock a single item, type the value assigned to that item in the LockFTPConnection= setting.

   For example, to lock the host address field only, type 2 in the LockFTPConnection= setting as shown here:

   ```
   LockFTPConnection=2
   ```

3. To lock more than one item, add the values together and type the sum in the LockFTPConnection= setting.

   For example, to lock the host address, host type, and TCP port fields, add 2, 4, and 8 together, and type the sum in the LockFTPConnection= setting:

   ```
   LockFTPConnection=14
   ```

4. Save and close the file.

Refer to the connection lock table in BlueZone Secure FTP individual feature locks, on page 156 for a complete list of values.

Locking the Miscellaneous dialog

Note

Typing a -1 locks all the items located on the Miscellaneous tab.

1. Open the setup.ini file in a text editor.
2. To lock a single item, type the value assigned to that item in the LockFTPMiscellaneous= setting.

   For example, to lock enabling passive mode only, type 16 in the LockFTPMiscellaneous= setting as shown here:

   ```
   LockFTPMiscellaneous=16
   ```

3. To lock more than one item, add the values together and type the sum in the `LockFTPMiscellaneous=` setting.

   For example, to lock enabling passive mode and enabling keep alive timer, add 16 and 32 together, and type the sum in the `LockFTPMiscellaneous=` setting:

   ```
   LockFTPMiscellaneous=48
   ```

4. Save and close the file.

Refer to the miscellaneous lock table in BlueZone Secure FTP individual feature locks, on page 156 for a complete list of values.

Locking additional dialogs

The following dialogs can only be completely locked. The individual items cannot be individually locked as in the above dialogs.

1. Open the `setup.ini` file in a text editor.
2. To lock a dialog, type `1` in the corresponding setting.
3. Save and close the file.

Refer to the additional items table in BlueZone Secure FTP individual feature locks, on page 156 for a complete list of values.

Configuring sessions

You can configure the following types of sessions:

- Mainframe or iSeries Display, on page 45
- Mainframe or iSeries Printer, on page 46
- BlueZone VT Display, on page 47
- ICL Display, on page 47
- Unisys T27 Display, on page 48
- Unisys UTS Display, on page 49

Configuring Mainframe or iSeries Display sessions - Profile mode

1. Start a BlueZone Mainframe or iSeries Display session from Session Manager or from the desktop icon.

   A window displays prompting you for a profile name.

   Note

   If this is the first time you are starting a BlueZone session, the above window does not open. Instead, a BlueZone session starts and the Define New Connection window opens.

2. In the **File name** field, type in the desired name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.
3. A message opens asking you if you want to create the file. Click **Yes**.

   The session starts and the Define New Connection window opens.
4. Enter the host information:

a. In the **Connection Name** field, type any name for the session.

b. In the **Host Address** field, type the IP address or DNS name.

c. In the **TCP Port** field, type the port number.

All of the other fields are optional.

5. Click **OK** twice to return to the BlueZone Display Emulation screen.
6. From the BlueZone Display menu bar, click **Session** ® **Connect**.

   You are now connected to your host. **Ready** displays on the BlueZone status bar.

Additional configuration

You can also control the behavior of the host session that you just created. For example, you can control many aspects of the host session like auto-connecting and prompting on disconnect.

1. From the BlueZone Mainframe Display menu bar, click **Session** ® **Configure**.

2. From this window you can select the **Auto-Connect Session**, **Auto-Reconnect Session**, if the session was deactivated by the host, **Prompt on Disconnect**, **Auto-Close Session on Disconnect**, and/or **Connect Retry** check boxes.

There are additional configuration options that can be configured in this window. For additional information on session configuration, refer to the *BlueZone Display and Printer User's Guide*.

Configuring Mainframe or iSeries Printer sessions

1. Start a BlueZone Mainframe or iSeries Printer session from Session Manager or from the desktop icon.

   A window opens prompting you for a profile name.
2. In the **File name** field, type a name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.

   The session starts and the Define New Connection window opens.
3. Enter the host information:

   a. In the **Connection Name** field, type a name for the session.

   b. In the **Host Address** field, type the IP address or DNS name.

   c. In the **TCP Port** field, type the port number.

   All of the other fields are optional.

   Note

   Your host may require an LU Name in order to properly route print jobs to your job queue. In this case, you must enter an LU Name or the connection to your mainframe fails.

   If you are configuring an iSeries host, the configuration window has **Device Name** instead of **LU Name**. The same rule applies as stated above. Your iSeries host may require a Device Name (sometimes referred to as Terminal ID) in order route print jobs correctly. In this case, you must type a Device Name or the connection to your host fails.
4. Click **OK** twice to return to the BlueZone Printer Emulation screen.
5. From the BlueZone Mainframe Printer menu bar, click **Session** ® **Connect**.

   You are now connected to your host. **Connected** and **Ready** display on the BlueZone status bar.

Configuring BlueZone VT Display sessions

1. Start a BlueZone VT Display session from Session Manager or from the desktop icon.

   A window opens prompting you for a profile name for the session.

   Note

   If this is the first time you are starting a BlueZone VT session, the above window is not displayed. Instead, a BlueZone VT session starts and the Define New Connection window opens.

2. In the **File name** field, type a name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.

   A message opens asking you if you want to create the file.

3. Click **Yes**.

   The session starts and the Edit Connection window opens.

4. Enter the host information:

   a. In the **Connection Name** field, type a name for the session.

   b. In the **Host Address** field, type the IP address or DNS name.

   c. In the **TCP Port** field, type the port number.

   All of the other fields are optional.

5. Click **OK** twice until you return to the BlueZone Display Emulation screen.

6. From the BlueZone VT menu bar, click **Session** ® **Connect**.

   You are now connected to your host. **Connected** displays on the BlueZone status bar.

Additional configuration

You can also control the behavior of the host session that you just created. For example, you can control many aspects of the host session like auto-connecting and prompting on disconnect.

1. From the BlueZone VT Display menu bar, click **Session** ® **Configure**.

2. From this window you can select the **Auto-Connect Session**, **Auto-Reconnect Session**, if the session was deactivated by the host, **Prompt on Disconnect**, **Auto-Close Session on Disconnect**, and/or **Disable Exit While Connected to Host** check boxes.

There are additional configuration options that can be configured in this window. For additional information on session configuration, refer to the *BlueZone Display and Printer User's Guide*.

Configuring ICL display sessions

1. Start a BlueZone ICL Display session from Session Manager or from the desktop icon.

   A window opens prompting you for a profile name.

   Note

   If this is the first time you are starting a BlueZone ICL session, the above window is not displayed. Instead, a BlueZone ICL session starts and the Define New Connection window opens.

2. In the **File name** field, type a name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.

   A message opens asking you if you want to create the file.

3. Click **Yes**.

   The session starts and the Define New Connection window opens.

4. Enter the host information:
   a. In the **Connection Name** field, type a name for the session.
   b. In the **Host Address** field, type the IP address or DNS name.
   c. In the **TCP Port** field, type the port number.

   All of the other fields are optional.
5. Click **OK** twice until you return to the BlueZone Display Emulation screen.
6. From the BlueZone menu bar, click **Session** ® **Connect**.

   You are now connected to your host. **Connected** and **Ready** display on the BlueZone status bar.

Additional configuration

You can also control the behavior of the host session that you just created. For example, you can control many aspects of the host session like auto-connecting and prompting on disconnect.

1. From the BlueZone ICL Display menu bar, click **Session** ® **Configure**.
2. From this window you can select the **Auto-Connect Session**, **Auto-Reconnect Session**, if the session was deactivated by the host, **Prompt on Disconnect**, **Auto-Close Session on Disconnect**, and/or **Connect Retry** check boxes.

There are additional configuration options that can be configured in this window. For additional information on session configuration, refer to the *BlueZone Display and Printer User's Guide*.

Configuring Unisys T27 Display sessions

1. Start a BlueZone T27 display session from Session Manager or from the desktop icon.

   A window opens that prompts you for a profile name.
2. In the **File name** field, type a name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.

   A message opens asking you if you want to create the file.
3. Click **Yes**.

   The BlueZone T27 Display opens.
4. On the BlueZone menu bar, click **Session** ® **Configure**.
5. Click **Properties**.
6. Click **New Screen**.
7. In the **Screen connection name** field, type a name for the screen.
8. Click **Configure Connections**.

   A message opens asking if want to generate the initial connection route to host.
9. Click **Yes**.
10. Double-click **MYHOST**.
11. Enter the host **IP address** and **IP Port Id**.

    The IP address can be a numeric IP address or a DNS name.
12. Click **OK**.
13. Click **Save and Close**.
14. From the **Connection Route** menu, select an available route.

    If you followed the previous steps, **ROUTE1** is available.
15. Click **Save and Close**.

16. Click **OK** in the Session Configuration window.
17. From the BlueZone menu bar, click **Session** ® **Connect**.

    You are now connected to your host. **Connected** displays on the BlueZone status bar.

Configuring Unisys UTS Display sessions

1. Start a BlueZone UTS display session from Session Manager or from the desktop icon.

   A window opens prompting you for a profile name.
2. In the **File name** field, type a name and click **Save**. BlueZone automatically assigns the correct file extension for the session type.

   A message opens asking you if you want to create the file.
3. Click **Yes**.

   The BlueZone UTS Display opens.
4. On the BlueZone menu bar, click **Session** ® **Configure**.
5. Click **Properties**.
6. Click **New Screen**.
7. In the **Screen connection name** field, type a screen name.
8. Click **Configure Connections**.

   A message opens asking if you want to generate the initial connection route to the host.
9. Click **Yes**.
10. Double-click **MYHOST**.
11. Enter the host **IP address** and **IP Port Id**.

    The IP address can be a numeric IP address or a DNS name.
12. Click **OK**.
13. Click **Save and Close**.
14. From the **Connection Route** menu, select an available route.

    If you followed the previous steps, **DEMAND1** is available.
15. Click **Save and Close**.
16. Click **OK** in the Session Configuration window.
17. From the BlueZone menu bar, click **Session** ® **Connect**.

    You are now connected to your host. **Ready** and **Connected** display on the BlueZone status bar.

Saving and opening session configurations

Opening sessions

BlueZone sessions can be started several ways:

- using the BlueZone Session Manager
- using the BlueZone Desktop icons that are created during installation
- using the auto-launch session feature found on the Auto-Launch tab in **File** ® **Properties**
- from a command prompt using a command line switch

Each of these methods takes advantage of the command line switches used to load configuration files, override configuration settings, and control the BlueZone session number. Refer to BlueZone command line switches, on page 162 for more information.

Opening saved BlueZone configuration files

Saved configurations can be used on a single installation or transferred to another BlueZone installation by copying the configuration file to that system.

1. From the BlueZone menu bar, click **File** ® **Open**.
2. Select the configuration file that you want to launch.
3. Click **Open**.

CAUTION

Opening a saved configuration file in an active session automatically overwrites the configuration settings saved in the Registry for that active session. To prevent the loss of the active session's configuration settings, save them to a file first using the **File** ® **Save As** command.

Note

The BlueZone Session Manager allows session configurations to be opened during session creation or launch. Refer to BlueZone Session Manager, on page 90 for more information.

Creating preconfigured configuration files

If you want to deliver BlueZone to your users with one or more preconfigured BlueZone profiles, you must create the required number of BlueZone profiles (configuration files) and include them in the BlueZone distribution image.

During the installation, the BlueZone installation program automatically copies any profiles to the user's `BlueZone\Config` folder.

If you are using BlueZone Session Manager, the BlueZone profiles that you create automatically display in Session Manager the first time it is opened.

If you are not using Session Manager and the user is opening BlueZone from program files or a desktop icon, the profiles automatically display in the Select or Create New Profile window that opens when a BlueZone client is started.

Tip

This feature also works for BlueZone script files. Add your script files to the distribution image.

Refer to Creating a distribution image, on page 77 for more information on distributing files to your users.

Creating BlueZone desktop shortcuts

There are two types of desktop shortcuts that can be created:

- A desktop shortcut that starts a unconfigured BlueZone session
- A desktop shortcut that starts a preconfigured BlueZone session

You can also add the shortcut to the BlueZone program group.

Creating an unconfigured BlueZone session shortcut

You can create a desktop shortcut that starts an unconfigured BlueZone session. A standard Windows file window opens listing the available BlueZone profiles (configuration files) to choose from. If no BlueZone profiles exist, the Define New Connection window automatically opens, allowing the user to configure the host connection settings at that time.

In a default installation of BlueZone Desktop, only one desktop shortcut is created; the shortcut for BlueZone Session Manager. If however, you want to have a desktop shortcut that starts one or more BlueZone emulators, follow this procedure:

1. Open the `BlueZone Desktop` folder.
2. Open the `setup.ini` file in a text editor.
3. Locate the `[Desktop Shortcuts]` section.
4. For each emulator that you want a desktop shortcut created, change the `No` value to `Yes`. For example:

```
[Desktop Shortcuts]
MainframeDisplay=Yes
MainframePrinter=Yes
```

5. Save and close the `setup.ini` file.

   When BlueZone is installed through the `setup.exe` program, the desktop shortcuts are created.

Creating a preconfigured BlueZone session shortcut

You can create a desktop shortcut that launches a BlueZone session along with an preconfigured BlueZone profile (configuration file). In order for this feature to work, you must create at least one BlueZone profile along with an associated desktop shortcut. These files must be added to your BlueZone distribution image so that they are available during the BlueZone installation process.

Prerequisites:

- In `setup.ini`, under `[Program Group]`, the `UseGroup=` entry must be set to `Yes`. Yes is the default value.

1. Install BlueZone Desktop using the default settings. Refer to BlueZone installation, on page 21 for more information.

   Verify that you have installed all of the BlueZone emulators that you want to make shortcuts for. Verify that you have installed the BlueZone Session Manager.
2. For each shortcut that you want to create, start the appropriate BlueZone emulator, configure, save, and name each session. Refer to Configuring sessions, on page 45 for more information.

   The profile names that you create are also the names that are assigned to the shortcut.
3. Open the BlueZone Session Manager.

   An icon for each session you created displays.
4. Highlight a session and click the **Create Desktop Shortcut** icon on the Session Manager toolbar.

   A desktop shortcut is created for each session and placed on your desktop.
5. Repeat step 4 for each session.
6. Locate the following files and save them in your `BlueZone Desktop` distribution image folder:

- BlueZone profiles for each session

  The profiles are saved to: `C:\Documents and Settings\`*`username`*`\My Documents\BlueZone\Config`

- Shortcut files for each session

  The shortcut files are saved to: `C:\Documents and Settings\`*`username`*`\Desktop`

  Note

  Windows does not display the file extensions of desktop shortcut files in Windows Explorer; however, if you use the Windows command prompt to display your files, the desktop shortcuts have a file extension of `.LNK`.

7. On a test machine, install BlueZone using your BlueZone distribution image. Verify that the desktop shortcuts are created and start the configured BlueZone sessions.

Adding a BlueZone shortcut in the program group

In addition to being able to place preconfigured BlueZone session shortcut(s) on the desktop, you can also add the shortcut(s) to the BlueZone program group.

1. Open the `BlueZone Desktop` folder.
2. Open `setup.ini` in a text editor.
3. Locate the `[Desktop Shortcuts]` section.
4. Locate the `CopyShortcuts2ProgramGroup=No` entry.
5. Change `No` to `Yes`.
6. Save and close the file.

This causes any BlueZone session desktop shortcuts (`.LNK`) files that are present in the BlueZone distribution image, to be automatically added to the BlueZone program group during the installation process.

BlueZone command line switch support

Opening BlueZone sessions from the registry using the /S command line switch

BlueZone sessions can be started out of sequence by using the `/S`*`x`* command line switch where *`x`* is the session identifier.

The following sample steps open Session S3 without starting session S1 or session S2:

1. Right-click on the BlueZone icon and select **Properties**.
2. In the **Target** field, add `/S3` to the end of the command:

   ```
   "C:\Program Files (x86)\BlueZone\6.1\bzmd.exe" BZMD.EXE /S3
   ```

   Session S3 starts without session S1 or session S2 being started first. If a configuration for session S3 is not in the registry, the session is created with default settings.

Note

The BlueZone Session Manager allows sessions to start out of sequence. The command line switches can be used for specific applications where the BlueZone Session Manager is not installed. Desktop icons created by the BlueZone Session Manager use the /S*x* command line switch to start the associated session. Right-click on a desktop icon, select **Properties**, and to view or modify the **Target** field.

Refer to BlueZone command line switches, on page 162 for more information.

Opening saved configuration files using the /F command line switch

You can open a specific configuration file with the /F*x* command line switch, where *x* is the configuration file name.

For example, BZMD.EXE /F"MY CONFIG1.ZMD" opens the BlueZone Mainframe Display and loads the MY CONFIG1.ZMD configuration file.

Note

The BlueZone Session Manager allows saved configuration files to be loaded when the session is created or starts. The command line switches can be used for specific applications where the BlueZone Session Manager is not installed.

This command line switch can be used with the session command line switch, /S*x*, where *x* is the session identifier, to load a specified session number and a specified configuration file.

For example, BZMD.EXE /S9 /FCONFIG1.ZMD opens session S9 and loads the configuration file named CONFIG1.ZMD.

Refer to BlueZone command line switches, on page 162 for more information.

Saving a configuration file to the registry using the /Q command line switch

The /Q command line switch is used in conjunction with the /S*x* and /F*x* command line switches to load the configuration file specified with /F without starting BlueZone. This is useful when performing remote installations where the configuration must be loaded from a batch file or DOS session.

For example, BZMD.EXE /S9 /FCONFIG1.ZMD /Q loads the configuration in CONFIG1.ZMD into the session S9 Registry Key without starting BlueZone.

Refer to BlueZone command line switches, on page 162 for more information.

Prompting for an LU or device name using the /L command line switch

When the /L command line switch is used, the user is prompted to enter an LU name or device name which is then sent to the host during the connection negotiation.

If an LU name or device name is specified after the /L switch, the name specified is automatically entered into the current TN3270 or TN5250 configuration. This switch is designed to be used with BlueZone Web to allow a single configuration file to be distributed to all users yet allow individual LU or device names to be specified.

Refer to BlueZone command line switches, on page 162 for more information.

Starting a session with a dialog configuration file using the /R command line switch

You can start a BlueZone session with a specific dialog configuration file. This is accomplished by using the `/R` command line switch.

For example, if you wanted to start a BlueZone Mainframe session with a specific keyboard map file, you can use the `/R` command line switch to load a BlueZone keyboard map file that you created.

Because BlueZone supports more than one type of dialog configuration file, you can load multiple dialog configuration files by using multiple `/R` commands.

The following example starts Mainframe Display session S10 with a session configuration and keyboard dialog configuration profiles:

```
"C:\Program Files\BlueZone\6.1\BZMD.EXE" /S10 /Rsession.mds /Rkeyboard.mdk
```

Refer to BlueZone command line switches, on page 162 for more information.

Controlling SSL/TLS using the /~ command line switches

You can use the `/~` command line switches to enable or disable SSL/TLS encryption. Table 4: Encryption command line switches lists the available `/~` command line switches.

Table 4: Encryption command line switches

Switch	Function
`/~0`	Disables SSL/TLS encryption
`/~2`	Enables SSL/TLS encryption

If you want to start a BlueZone Mainframe session with SSL/TLS encryption enabled, use the `/~2` command line switch when starting the session. The `/~2` command line switch has the same affect as selecting the **Enable Secure Sockets Layer** check box on the **Security** tab when you are configuring a host connection. Any additional SSL or TLS settings that are required, must be set and saved in the BlueZone configuration first.

The following example starts a BlueZone Mainframe session with SSL/TLS encryption enabled:

```
"C:\Program Files\BlueZone\6.1\BZMD.EXE" /~2
```

If you want to start a BlueZone Mainframe session with encryption disabled, use the `/~0` command line switch to disable encryption. The `/~0` command line switch has the same affect as clearing the **Enable Secure Sockets Layer** check box on the **Security** tab.

The following example starts a BlueZone Mainframe session with encryption disabled:

```
"C:\Program Files\BlueZone\6.1\BZMD.EXE" /~0
```

This feature applies to the following products:

- BlueZone Mainframe Display
- BlueZone Mainframe Printer
- BlueZone iSeries Display
- BlueZone iSeries Printer
- BlueZone VT
- BlueZone ICL Display

Refer to BlueZone command line switches, on page 162 for more information.

BlueZone Secure FTP also supports encryption through command line switches. Refer to BlueZone Secure FTP command line switches, on page 167 for more information.

Associating Mainframe Printer sessions with Mainframe Display sessions

You can use the `/L!` command line switch to associate a Mainframe Printer session with a Mainframe Display session. This command line switch directs print jobs that are queued up using the Display emulator to a specific Printer emulator, so the print jobs can be spooled and printed. This feature requires Printer Association to be configured on your Mainframe host.

1. In a Mainframe Display sessions, configure the LU Name:
   a. From the Mainframe Display menu bar, click **Session** ® **Configure**.
   b. In the **Connection Type** list, select **TN3270/TN3270E**, and click **Properties**.
   c. In the **Connection List** list, select the session that you want to edit, and click **Edit**.
   d. In the **LU Name** field, type an LU name for the Mainframe Display. For example, type `WS123`.
   e. Click **OK** three times.
   f. Save and close the Mainframe Display session.
2. Use the `/L!` command line switch to start a Mainframe Printer session.

   For example, `"C:\Program Files (x86)\BlueZone\6.2\bzmp.exe" /FRS73.zmp /L!WS123` starts the Mainframe Printer session `RS73.zmp`, and associates it to the Mainframe Display session with the LU name WS123.

BlueZone Secure FTP command line switch support

BlueZone Secure FTP also has support for command line switches. They work exactly the same way as with the other BlueZone emulators. Some of the commands are repeated, but they do not necessarily perform the same function.

BlueZone Secure FTP and batch files

BlueZone Secure FTP can be started from a DOS batch file. Because BlueZone Secure FTP supports command line switches, you can control how BlueZone Secure FTP starts.

Use there `/F` command line switch if you want to start BlueZone Secure FTP from a batch file and include a configuration file named `config.zft` to start the BlueZone Secure FTP session:

```
"C:\Program Files\BlueZone\6.1\BZFTP.EXE" /Fconfig.zft
```

Use the `/I` command line switch if you want to start BlueZone Secure FTP from a batch file and set the Initial PC Directory to a folder, for example, `C:\MyFiles`:

```
"C:\Program Files\BlueZone\6.1\BZFTP.EXE" /Ic:\MyFiles
```

You can also combine command line switches in one statement:

```
"C:\Program Files\BlueZone\6.1\BZFTP.EXE" /Fconfig.zft /Ic:\MyFiles
```

Other examples

Initial commands (/L command line switch) are used to configure FTP to perform specific FTP commands upon connect. For example, you can configure BlueZone Secure FTP to perform an upload of a file named upload.txt and then a download of a file named download.txt during your batch execution with the following command:

```
BZFTP.EXE /L"STOR upload.txt" /L"RETR download.txt" /L"EXIT"
```

The /L"EXIT" command line switch closes BlueZone Secure FTP after the initial commands complete. There are sometimes issues with getting double quotes to appear inside other double quotes through a batch file. In BlueZone Secure FTP, there are two characters that translate into double quote and a blank space. The ampersand symbol (&) translates into a double quote (") and the percent sign (%) translates into a blank space. The following is an example:

```
BZFTP.EXE /L"STOR &upload.txt& upload" /L"EXIT"
```

This translates the STOR command to "STOR "upload.txt" upload", which uploads the local file upload.txt to the host as upload.

Some scripting and programming languages support the use of double double quotes. The following example shows the use of double double quotes when you are calling BlueZone Secure FTP to run from a program or script using the /Z and /L commend line switches.

```
Run "C:\Program Files\BlueZone\6.1\BZFTP.EXE /Z0 /L""RETR F1201.CSV""
```

Controlling SSL/TLS and SSH using the /~ command line switches

You can use the /~ command line switches to disable encryption or enable Explicit SSL/TLS, Implicit SSL/TLS, and SSH encryptions.

Table 5: FTP encryption command line switches lists the available /~ command line switches.

Table 5: FTP encryption command line switches

Switch	Function
/~0	Disables encryption
/~1	Enables Explicit SSL/TLS encryption
/~2	Enables Implicit SSL/TLS encryption
/~3	Enables SFTP encryption

If you wanted to start a BlueZone Secure FTP session with Explicit SSL/TLS encryption enabled, use the /~1 command line switch when starting the session. The /~1 command line switch has the same affect as selecting **Explicit FTPS (SSL/TLS)** from the **Security Options** menu on the **Security** tab when you are configuring a host connection. Any additional SSL or TLS settings that are required, must be set and saved in the BlueZone Secure FTP configuration first.

The following example starts a BlueZone Secure FTP session with Explicit SSL/TLS encryption enabled:

```
"C:\Program Files\BlueZone\6.1\BZFTP.EXE" /~1
```

If you wanted to start a BlueZone Secure FTP session with encryption disabled, use the /~0 command line switch to disable SSL/TLS encryption. The /~0 command line switch has the same affect as clearing the **Enable Secure Sockets Layer** check box on the **Security** tab.

The following example starts a BlueZone Secure FTP session with encryption disabled:

```
"C:\Program Files\BlueZone\6.1\BZFTP.EXE" /~0
```

Refer to BlueZone Secure FTP command line switches, on page 167 for a complete listing of command line switches.

BlueZone dialog configuration profiles

Many BlueZone configuration dialogs have toolbar icons that you can use to save, import, and export configuration files for values associated with that specific dialog. You can save subsets of session configurations and transfer them between sessions or users. These files are called dialog configuration profiles.

Dialog configuration profiles commonly used are keyboard map settings, color settings, and session settings.

The dialog configuration profile toolbar is located in either the upper right or lower left corner of the dialog.

Figure 2: Sample dialog configuration profile toolbar

From left to right, the toolbar functions are:

- Default: Opens the default dialog configuration profile.
- File Open (Import File): Open an existing dialog configuration profile.
- File Save As (Export File): Save a new dialog configuration profile.
- Help: Opens the help system to the relevant topic.

Any BlueZone dialog that contains a dialog configuration profile toolbar can have that dialog's settings defaulted, imported, or exported to a file (as a subset of the main BlueZone configuration file) with its own file extension. Dialog configuration profiles for each dialog have unique file extensions. Refer to Dialog-level configuration profile extensions, on page 153 for a complete listing of the dialog configuration profile file extensions.

Dialog configuration profiles can also be used with the following BlueZone features:

- Profiles schemes. Refer to Profile schemes, on page 58 for detailed information on how to use dialog configuration profiles to override BlueZone configuration settings.
- Command line switches. Refer to Starting a session with a dialog configuration file using the /R command line switch, on page 54 for more information on how to use the dialog command line switch feature.
- Hiding toolbar buttons. Refer to Configuring the dialog configuration profile locks, on page 41 for information on how to hide some or all of the dialog configuration profile buttons.

Hotkey support

In addition to being able to start the various functions from the toolbar icons, you can also invoke these functions from a keyboard Hotkey.

Table 6: Hotkey assignments

Function	Hotkey
Default Settings	1
Import Settings	2
Save Settings	3
Export	4
Transfer Send	5
Transfer receive	6
Help Topics	7

By supporting Hotkeys, these functions are accessible through a BlueZone script.

Profile schemes

The profile schemes feature can be used to automatically import dialog configuration profiles. When this feature is used, the values stored in the dialog configuration profile overrides certain values stored in the main BlueZone configuration file that was used to start the session.

Dialog configuration profiles are subsets of the main BlueZone configuration file. There are up to eight types of dialog configuration profiles that can be used in any combination with the main BlueZone configuration file.

Note

This feature is used primarily with a push technology, like Microsoft SMS, to install and update BlueZone files on users' computers.

Use the profile schemes feature to control certain aspects of the BlueZone configuration while allowing your users to be able to control all of the other aspects of the configuration.

The following examples shows how to change the IP address (or DNS name) of an IBM 3270 Mainframe host, with and without the profile schemes feature:

Without using the profile schemes feature

If you are not using the profile schemes feature, you must

1. Modify the master BlueZone configuration file (`.zmd`) with the new IP address or DNS name.
2. Push the modified configuration file to all of your users' computers.
   Modifying the master BlueZone configuration file accomplishes this, but all your users' customizations, like keyboard map changes and font/color changes, are overwritten.

Using the profile schemes feature

When using the profile schemes feature, your master BlueZone configuration file already has the profile schemes window configured to import a TN3270E profile (`.tn3`). This profile contains all of the BlueZone Mainframe Display TN3270E configuration settings like, host IP address (DNS name), and TCP port.

1. Modify the TN3270E profile (`.tn3`) with the new IP address or DNS name.
2. Push the modified TN3270E profile to your users' computers.
   By modifying and updating only the TN3270E profile, you do not disturb any of your users' customizations.

Configuring profile schemes

1. Click **File** ® **Properties** from the BlueZone menu bar.
2. Click the **Profile Schemes** tab.
3. Determine which aspects of the BlueZone configuration you want to override using the profile schemes feature.
4. Select the corresponding check box(es) of the features that you want to enable.
5. Determine how you want the dialog configuration profiles created:
   - You can leave the file names blank. BlueZone creates a profile configuration file (based on your current configuration settings) with the same name as the master BlueZone configuration file, but with the corresponding file extension.
   - You can create you own dialog configuration profiles by going to each dialog, making the necessary customizations, and exporting the changes to a dialog configuration profile using your own naming convention.
6. Depending on which method you want to use, either leave the file name blank or click **Browse** to locate the dialog configuration profile(s) that you created.
7. Click **OK**.

From now on, when this BlueZone Mainframe Display session starts, BlueZone applies all of the configuration settings stored in the main BlueZone configuration file (`.zmd`) first, then it applies the dialog configuration profiles that are selected in the Profile Schemes window, and overrides the configuration settings with the values stored in the enabled dialog configuration profiles.

Refer to Dialog-level configuration profile extensions, on page 153 for a complete listing of the dialog configuration profile file extensions.

Automatically generate LU names

BlueZone can generate LU names internally, based on the workstation name. You can send a single BlueZone configuration to your users and have them automatically request an LU name that contains the first seven characters of their workstation name plus a D for display sessions or P printer sessions then append the session number. BlueZone is configured to create the names based on %1, %2, and %3 values entered in the **LU Name** field of the Edit Connection window.

Table 7: Substitution text values lists the available substitution values and their description.

Table 7: Substitution text values

Value	Description
%1	Uses the first seven characters of the computer name as the base device name.
%2	Appends a D for display sessions or P for printer sessions.
%3	Appends the BlueZone session identifier. Session S1 appends 00, Session S2 appends 01 and so on.

Examples

Display session using the computer name as the base name

For a computer with computer name WS1234.

An LU Name of %1%2%3 results in WS1234D00 being sent to the mainframe for Session S1. WS1234D01 is sent for Session S2.

Display session using a standard base name

Using a base name of GROUP1.

An LU Name of GROUP1%2%3 results in GROUP1D00 being sent to the mainframe for Session S1. GROUP1D01 is sent for Session S2.

Printer session using the computer name as the base name

For a computer with computer name WS1234.

An LU Name of %1%2%3 results in WS1234P00 being sent to the mainframe for Session P1. WS1234P01 is sent for printer Session P2.

Printer using a standard base name

Using a base name of GROUP1.

An LU Name of GROUP1%2%3 results in GROUP1P00 being sent to the mainframe for printer Session P1. GROUP1P01 is sent for printer Session P2.

Using TN3270E printer LU association

Printer association provides an automated means to match display LUs with printer LUs. By enabling printer association and selecting the number of the display session to associate the printer with, the host automatically assigns the appropriate printer LU Name during the TN3270E negotiation.

Note

If the associated display session disconnects, the associated printer will also disconnect to prevent another user's print job from displaying on the wrong system.

Automatically generate device names

BlueZone can automatically create iSeries device names dynamically and retry the devices until the iSeries determines that the requested device is not in use. BlueZone is configured to create the names based on %1, %2, and %3 values entered in the **Device Name** field of the Edit Connection window.

Table 8: Substitution text values lists the substitution values and their description.

Table 8: Substitution text values

Value	Description
%1	Uses the first seven characters of the computer name as the base device name.
%2	Appends a D for display sessions or P for printer sessions.
%3	Appends an automatically incrementing number beginning with 00 and ending with 99.

Examples

Display session using the computer name as the base name

For a computer with computer name WS1234.

A device name of %1%2%3 results in WS1234D00 being sent to the iSeries. If the requested device name is in use, WS1234D01 is requested.

Display session using a standard base name

Using a base name of GROUP1.

A device name of GROUP1%2%3 results in GROUP1D00 being sent to the iSeries. If the requested device name is in use, GROUP1D01 is requested.

Printer session using the computer name as the base name

For a computer with computer name WS1234.

A device name of %1%2%3 results in WS1234P00 being sent to the iSeries. If the requested device name is in use, WS1234P01 is requested.

Printer session using a standard base name

Using a base name of GROUP1.

A device name of GROUP1%2%3 results in GROUP1P00 being sent to the iSeries. If the requested device name is in use, GROUP1P01 is requested.

Using printer device association

Printer association provides a mechanism to automatically request a printer device name based on the existing display device name. By predefining pairs of printer and display devices in the iSeries, users may dynamically request a display device using a base name plus %2%3 and automatically get a matching printer device.

For example, using a base name of GROUP1.

Using the associate printer with display feature.

A device name of GROUP1%2%3 configured in the display results in GROUP1D00 being sent to the iSeries. If the requested device name is in use, GROUP1D01 is requested.

Once the display successfully obtains a device name, the printer is assigned the matching device name by the display emulator. If the display gets GROUP1D01, it gives the printer GROUP1P01.

Note

This feature only works with predefined display and printer device name pairs where the printer device is assigned to the display device rather than the user.

Configuring API support

BlueZone supports DDE and HLLAPI to allow external applications, such as GUI interfaces, scripting engines, and input automation programs, to input data to and extract data from IBM host screens. The primary interface is through the DDE server. The BlueZone implementation of HLLAPI communicates with BlueZone through this DDE interface and is EHLLAPI/WHLLAPI compliant.

Typical applications that use the BlueZone API interface use a HLLAPI interface to communicate with BlueZone. For BlueZone to communicate with a HLLAPI application through the BlueZone DDE interface, you must enable the BlueZone DDE Interface:

1. Click **Options** ® **API**.
2. In the **Dynamic Data Exchange DDE)** section, enter the following information:
   a. Select the **Enable DDE Interface** check box to allow the BlueZone session to function as a DDE Server.

      DDE client applications can communicate with DDE servers to exchange data. This option must be enabled in order for BlueZone to communicate with HLLAPI client applications.

The **Server / Service Name** field displays the server/service name as **BlueZone**.

The **Topic Name** field displays the session's DDE topic name. The topic name can be changed by configuring the HLLAPI Short Name Session Identifier.

b. Select the **Enable Network DDE Initialization** check box to enable DDE client applications to communicate with BlueZone over a Local Area Network (LAN). BlueZone will modify the registry settings and invoke `netdde.exe`.

Note

Only use this option when the HLLAPI application is on a computer separate from the computer that BlueZone is running on.

The **DDE Share** field displays the DDE share name that NETDDE uses to establish a DDE connection over the Local Area Network (LAN).

3. In the **High Level Language API (HLLAPI)** section, select the necessary check boxes:
   - **Auto-Assign HLLAPI Names**: Select to have BlueZone automatically associate the Short Name Identifier to a session number, for example, A for S1, B for S2, and so on. When this check box is selected, you cannot edit the **Short Name Session Identifier** and **Session Long Name** fields.
   - **Auto-Launch the BlueZone DOS HLLAPI Redirector**: Select to have BlueZone run/close the BlueZone DOS HLLAPI Redirector program each time that the BlueZone DDE Server initializes/deinitializes.
   - **Allow Multiple Simultaneous Connections**: Select to allow multiple simultaneous connections.
4. Click the **Trace** tab:
   a. Select the necessary check boxes:
      - **Trace DDE Interface**: Select to trace the DDE conversation transactions.
      - **Trace HLLAPI Interface**: Select to trace the HLLAPI function calls and return values.
      - **Trace RUI Interface**: Select to trace the RUI conversation transactions.

   b. In the **Trace File** field, type a file name for the API trace. By default, the traces are saved in the `\Traces` folder in the working directory. Click **Browse** to select a different location.

Important

This field must contain a valid path or the trace feature does not work.

   c. Click **Start Trace** to start the API trace.
   d. Click **Stop Trace** to stop the API trace.
5. Click **OK**.

Mapping keyboards

BlueZone keys are mapped to a standard BlueZone keyboard map.

Note

If you have installed a non-English version of BlueZone, the default keyboard map is based on your currently selected language in the Windows Regional and Language Options.

To determine the functions that a key is mapped to:

1. Click **Options** ® **Keyboard**.

2. Click any key in the image.

   A window opens that displays the key's mappings.

Refer to the following topics to modify the keyboard maps:

- Creating key mappings, on page 63
- Editing existing key mappings, on page 63
- Mapping combination keys, on page 64
- Mapping overstrike keys, on page 64
- Importing keyboard maps, on page 64
- Exporting keyboard maps, on page 65

Creating key mappings

1. In the Keyboard Options window, select a group from the **Functions Group** list.

   When you select a group, all of the functions associated with that group display in the **Functions** list.
2. In the **Functions** list, select a function.

   Any existing key mappings for that function display in the **Key Mappings** list. If there are no keys currently mapped to this function, `<No Keys Mapped to Function>` displays in the list.
3. Click **New**.

   BlueZone creates a new blank highlight bar in the **Key Mappings** list. If there are existing key mappings, the new blank highlight bar displays below the existing key mappings.
4. In the keyboard image, click the key that you want to associate with the function that you selected in step 2.

   The name of the selected key displays in the **Key Mappings** list.
5. Click **OK**.

   The selected function is now mapped to the new key. Any other keys that are mapped to this function are also displayed in the **Key Mappings** list.
6. Repeat steps 1-5 as needed.
7. Click **OK** to close the Keyboard Options window.

Editing existing key mappings

1. In the Keyboard Options window, select a group from the **Functions Group** list.
2. In the **Functions** list, select a function.

   Any existing key mappings for that function display in the **Key Mappings** list.
3. In the **Key Mappings** list, select the mapping that you want to edit.
4. Click **Edit**.
5. In the keyboard bitmap, click the new key that you want to associate with the function that you selected in step 2.

   The highlighted key changes to the key that you just selected.
6. Click **OK**.

   The function is now mapped to the new key.
7. Click **OK** to close the Keyboard Options window.

Note

If you want to map a function to a multiple key sequence, you must select the active key first, then select the Ctrl or Alt key last. For example, if you want to map the New Line function to the keypad Enter key, click the keypad Enter key first, then click the Ctrl key last.

Mapping combination keys

The Alt and Ctrl keys have dual modes. They can be mapped to a function by themselves or they can be used in combination with other keys.

For example, to map the 3270 function Print Screen to Ctrl+P:

1. In the **Functions** list, select **Print Screen**.
2. Click **New**.
3. Click the right **Ctrl** image twice.

   In the **Key Mappings** list, the first time you click the right Ctrl image, it displays as **Right Ctrl**. The second time you click the image, it changes to **Ctrl+**.
4. Click **P**.

   The **Key Mappings** list displays **Ctrl+P**.
5. Click **OK**.

Mapping overstrike keys

The 3270 Function Overstrike Sequence allows a non-ASCII character in the EBCDIC character set, such as è, to be entered from the keyboard.

Overstrike causes the emulation to enter overstrike mode, after which two ANSI characters, such as e and `, are typed to represent the character. If the two characters represent a valid combination, the resulting EBCDIC character is entered into the device buffer. An uncompleted overstrike can be canceled with the Reset key.

Importing keyboard maps

By default, BlueZone uses the standard BlueZone keyboard map. However, there are additional keyboard maps that can be imported in to BlueZone. These additional keyboard map files are configured to the default keyboard map settings for several popular emulators and keyboards.

Note

If you have installed a non-English version of BlueZone, the default keyboard map that displays is based on your currently selected language in the Windows Regional and Language Options.

After you have installed BlueZone, the following keyboard map files are created in the `\Config` folder of the working directory.

Table 9: Additional BlueZone keyboard map files

File name	Configured like	Host type
extra101.mdk	Attachmate EXTRA!	Mainframe
keytronic122.mdk	KeyTronic 122 Key Keyboard Map	Mainframe
ibm3270.mdk	IBM 3270 Terminal Keyboard Map	Mainframe
pcomm101.mdk	IBM Personal Communications	Mainframe
rumba101.mdk	Netmanage RUMBA	Mainframe
unicomp122.mdk	Unicomp 122 Key Keyboard Map	Mainframe
putty.vdk	Putty Telnet client	BlueZone VT

To import one of these keyboard files:

1. Open a BlueZone Display session.
2. From the BlueZone menu bar, click **Options** ® **Keyboard**.
3. In the bottom left corner, click the **Import Keyboard Options** icon.
4. Select the keyboard map file that you want to import and click **Open**.

Note

If there are no keyboard map files in the window, then there are no additional keyboard map files for this particular BlueZone emulator.

You are now using the imported keyboard map file.

Refer to the *BlueZone Display and Printer User's Guide* for information on how to make changes to your BlueZone keyboard map.

Exporting keyboard maps

By default, BlueZone uses the standard BlueZone keyboard map. However, you can create a unique keyboard to meet your requirement and export the keyboard file.

1. Open a BlueZone Display session.
2. From the BlueZone menu bar, click **Options** ® **Keyboard**.
3. Edit the keyboard map as needed.
4. In the bottom left corner, click the **Export Keyboard Options** icon.
5. Type a name for the keyboard map file that you want to export and click **Save**.

The keyboard map file is saved in the `\Config` folder in the working directory.

Changing the language in BlueZone

In a standard installation, you select a language at the beginning of the process. The BlueZone installation program unzips `common.cab`, which contains the language DLLs, and the selected language file is renamed to `bzstring.dll`. The information contained in `bzstring.dll` is used to populate the BlueZone menus and dialogs in the selected language.

To switch to a different language without the `language.ini` file, you must uninstall and reinstall BlueZone with the new language selected. Configuring the `language.ini` file removes the need to uninstall and reinstall BlueZone with the new language. You can easily switch between two or more BlueZone supported languages.

Note

Changing the language with the `language.ini` file does not change the keyboard layout; it only affects the menus and dialogs. If you want to change the keyboard layout to support a specific language, you must modify the **Keyboard Type** option in the Keyboard Options dialog. For more information, refer to the "Keyboard Options dialog" topic in the *BlueZone Display and Printer User's Guide*.

To change the language in the BlueZone menus and dialogs:

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `language.ini` file in a text editor.
3. In the `[Language]` section, locate the `;Language=English` entry.
4. Delete the semicolon at the beginning of the entry.
5. Change `English` to the new language. The valid language values are:
   - `Dutch`
   - `French`
   - `German`
   - `Japanese`

   For example,

   ```
   [Language]
   Language=French
   ```

6. Save the `language.ini` file in the `\Config` folder of the BlueZone working directory. For example, `C:\Users\`*`username`*`\Documents\BlueZone\Config`.
7. Open to the `BlueZone Desktop` installation source directory and open the `common.cab` file.
8. Extract `english.dll` and the other necessary language `.dll` file, for example `french.dll`, to the BlueZone installation directory.

   If you accept the default locations during installation, the installation directory is `C:\Program Files\BlueZone\6.1`.

When BlueZone starts, it loads the language `.dll` file that is specified in the `language.ini` file.

Power pads

BlueZone power pads are fully customizable groups of buttons that can be configured to start BlueZone host and menu functions. You can create and edit power pads that contain frequently used functions.

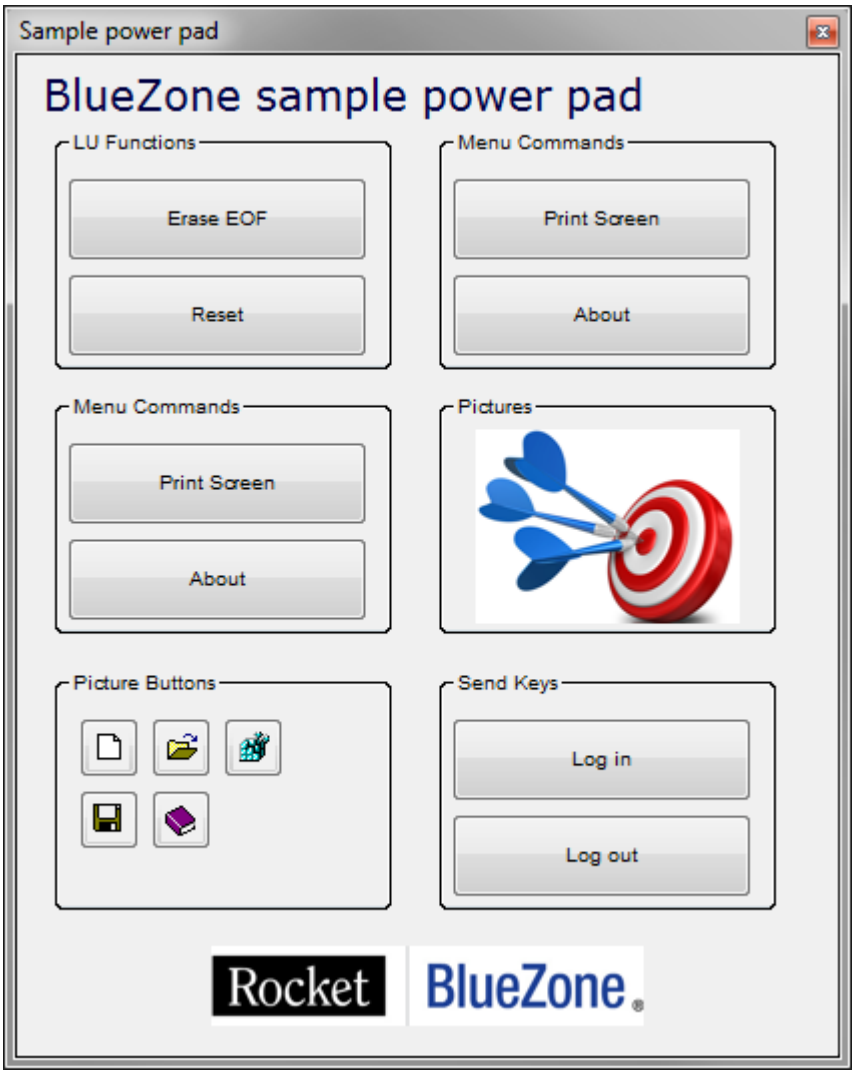
Note

Starting with BlueZone version 4.0, power keys have been replaced by power pads. The power keys feature is not enabled by default. To enable the power keys feature, refer to Enabling the power keys feature, on page 31.

Power pads open as a separate application window that can be positioned anywhere on the Windows desktop. When the power pad window is opened, it always displays on top of the BlueZone Display session. If you do not want it to overlap or block your view of the BlueZone session, drag the power pad off to one side.

A power pad can consist of one simple button or it contain multiple controls, as shown in the example in Figure 3: Sample power pad.

Figure 3: Sample power pad



Power Pad Editor

Power pads are created and edited using the standalone graphical desktop application, Power Pad Editor. The Power Pad Editor is opened from a BlueZone Display session.

To open the Power Pad Editor:

1. Click **View** ® **Properties**.
2. Select the **Power Pads** tab.
3. Click **New** or highlight an existing power pad and click **Edit**.

The power pad canvas is where you create your Power Pads. The control icons are used to select and place the various controls that can be placed on the power pad canvas, such as buttons, text, pictures, and group boxes.

Using the Power Pad Editor you can:

- Specify the size, title, color, and specific layout of the power pad.
- Add objects: buttons, text, group boxes, and pictures.

- Configure buttons to perform actions such as sending keystrokes; running an application, script or macro; and performing any commands that appear in the BlueZone menus, such as connecting to a host, transferring a file, or printing.
- Make single or multiple copies of objects on a grid.
- Align and size the objects on the grid as needed.
- Resize the power pad.

Note

A maximum of 128 objects can be created per power pad.

For help using the Power Pad Editor, refer to the *BlueZone Display and Printer User's Guide*.

Configuring power pads

Power pads are configured in the **Power Pads** tab in the View Properties window.

To make an existing power pad open with your BlueZone session:

1. From the BlueZone menu bar, click **View** ® **Properties**.
2. Click the **Power Pads** tab.

   In the **Available Power Pads** list there is a list of sample power pads. These power pads mimic the old default power keys. The **bzmenu** power pad contains all of the default BlueZone menu power keys. The other sample power pads contain all of the default function power keys for each BlueZone emulation client. The names of the sample power pads match the emulation client.
3. In the **Settings** section, select the **Show Power Pads** check box.

   This check box must be selected in order for the power pads shown in the **Active Power Pads** list to be displayed on the desktop. If this check box is not selected, the power pads remain in the **Active Power Pads** list but are not displayed on the desktop.
4. In the **Available Power Pads** list, select the power pad that you want to use and click **Add**.

   The power pad is added to the **Active Power Pads** list on the right.
5. Repeat step 4 as needed.
6. Click **OK**.

   All of the active power pads open. If you selected the **Enable Docking** check box, you can dock one or more of your power pads.
7. Save and close the BlueZone session.

The next time you open this BlueZone session, all of the power pads that you added to the **Active Power Pads** list open at the same time and in the same positions.

Docking power pads

You can choose to make the power pads dockable. When the **Enable Docking** check box is selected, you can drag one or more power pads into the BlueZone session window and dock it. Power pads can be docked to the top, sides, or bottom of the inside of the BlueZone session window. If the power pad is very tall, you will only be able to dock it to the left or right side. If the power pad is very wide, you will only be able to dock it to the top or bottom. After the power pad is docked, if the power pad is large, you may have to adjust the size of the BlueZone Session window to display the whole power pad.

To drag a power pad, point to the title bar with your left mouse button. Then, while holding down the left mouse button, drag it to the desired spot within the BlueZone Session window.

You will see the outline of the power pad change, and the title bar disappear, when it is in a "dockable" position.

Note

Closing a power pad, by clicking the power pad's X, during a BlueZone session will not remove it from the **Active Power Pads** list. This only temporarily closes the power pad.

Controlling power pads

You can temporarily turn off all power pads, without removing them from the **Active Power Pads** list.

1. Click **View** ® **Properties**.
2. Select the **Power Pads** tab.
3. Clear the **Show Power Pads** check box.

   You can also add a Toggle Power Pads button to the BlueZone toolbar to toggle the power pads in your **Active Power Pads** list on and off.

   Refer to the *BlueZone Display and Printer User's Guide* for help with customizing the BlueZone toolbar settings.

HLLAPI support

High Level Language Application Program Interface (HLLAPI) was developed so external programs can be written to interact with a host session. This is accomplished by using the BlueZone emulator acting as the middleware between the HLLAPI application and the host session.

BlueZone is fully 32-bit WHLLAPI, EHLLAPI, and EEHLLAPI compatible allowing easy migration of many custom or third-party applications used with other emulators. BlueZone HLLAPI is compatible with third-party HLLAPI applications including, but not limited to, those from Shared Medical (Siemens), Neasi-Webber, Real Vision, and Decision Technology.

To support older HLLAPI applications on 32-bit systems, BlueZone also supports DOS HLLAPI and 16-bit HLLAPI conversations with 32-bit BlueZone.

BlueZone ships with the following HLLAPI DLL files:

DLL	Environment	Description
WHLLAPI.DLL	BlueZone 32-bit HLLAPI DLL	Provides compatibility with Windows HLLAPI. Uses the DDE Server interface to communicate with the BlueZone emulator. The BlueZone DDE Server interface must be enabled in order for this DLL to work. Refer to Configuring API support, on page 61 for more information.
PCSHLL.DLL	BlueZone 32-bit HLLAPI DLL	Provides compatibility with IBM PCOMM HLLLAPI. Uses shared memory to communicate with the BlueZone emulator.
EHLAPI32.DLL	BlueZone 32-bit HLLAPI DLL	Provides compatibility with IBM EHLLAPI. Uses shared memory to communicate with the BlueZone emulator.
EEHLLAPI.DLL	BlueZone 32-bit HLLAPI DLL	Based on the IBM EEHLLAPI specification. Uses shared memory to communicate with the BlueZone emulator.
BZHLLVDD.DLL	BlueZone Virtual Device Driver	Used with Windows 2003 Server and Windows XP SP3 only.

Note

If you intend to write a program that interfaces with BlueZone through the HLLAPI interface, the following documents are provided in the `DOCS\WHLLAPI` folder of the BlueZone CD image:

- `BZWHLL.H`
- `BZWHLL_I.C`
- `WOSA HLLAPI 1.1.DOC` - Sometimes referred to as Windows HLLAPI.

Configuring HLLAPI application prerequisites

Before you can configure HLLAPI applications, you must:

- Configure the BlueZone installation, on page 70
- Configure the HLLAPI application requirements, on page 71

Configuring the BlueZone installation for HLLAPI

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. In the `[BZSetup]` section, locate the `SetPath=No` entry.
4. Change `No` to `Yes`:

```
[BZSetup]
SetPath=Yes
```

5. Save and close the file.
6. Restart your computer.
7. Run the `setup.exe` program to install BlueZone.
8. In the Component Selection window, ensure that the HLLAPI component is selected.

During installation, the BlueZone Setup program adds the BlueZone Program Directory to the Windows Path environment variable if the computer is using Windows XP SP3 or Windows Vista.

You can also configure three optional HLLAPI features. Refer to Configuring optional HLLAPI features, on page 73 for more information.

Configuring HLLAPI application requirements

To ensure that BlueZone works correctly with your HLLAPI application, you must point your HLLAPI application to the BlueZone `whllappi.dll` file, which by default is installed in the `C:\Program Files\BlueZone\6.1` directory.

1. To avoid HLLAPI DLL conflicts, change the name and location of your HLLAPI application DLL by using one of the methods shown in the following table:

To change existing HLLAPI DLL	Action
If your HLLAPI application provides a way to change the name and location of the existing HLLAPI DLL	Start the application configuration interface and point to the BlueZone `whllappi.dll` file in the `C:\Program Files\BlueZone\6.1` directory.
If your application does not provide a way to change the name and location of your HLLAPI application DLL	Rename the BlueZone `whllappi.dll` and copy it to the directory where the application expects to find it.
If your workstation has a competitor emulator HLLAPI DLL installed (how do users know what a competitor is? And why is a competitor DLL different from the other kind of DLL that might be installed?)	Temporarily rename the competitor DLL during your testing of BlueZone to prevent conflicts or consider installing and testing BlueZone on a workstation that does not have a competitor emulator installed.

2. Configure your HLLAPI application by using one of the methods in the following table, depending on your Windows environment:

Environment	Configuration topic
Windows 32-bit	Configuring for Windows 32-bit HLLAPI application, on page 71
Windows 16-bit	Configuring for Windows 16-bit HLLAPI application, on page 72
DOS on Windows 95/98/ME	Configuring for DOS HLLAPI application - Windows 95/98/ME, on page 72
DOS on Windows XP SP3	Configuring for DOS HLLAPI Application - Windows XP SP3, on page 73

Configuring HLLAPI applications

BlueZone supports the following types of third-party HLLAPI applications:

- Windows 32–bit HLLAPI application, on page 71
- Windows 16–bit HLLAPI application, on page 72
- DOS HLLAPI application for Windows 95, 98, or ME, on page 72
- DOS HLLAPI application for Windows XP SP3, on page 73

Configuring for Windows 32-bit HLLAPI application

1. On the BlueZone menu bar, click **Options** ® **API**.
2. Select the **Enable DDE Server Interface** check box.

3. Click **OK**.

   BlueZone is now listening for a DDE connection.
4. Click **Session** ® **Connect** to establish a connection to your host.
5. Configure your 32-bit HLLAPI application to connect to the BlueZone HLLAPI DLL (WHLLAPI.DLL).

   This can involve changing the applications settings so that it is looking for the BlueZone DLL called WHLLAPI.DLL or you may have to rename the BlueZone DLL to the name that your application is programmed to look for.
6. Open your HLLAPI application and execute a command that sends or receives data from your host.
7. Check to see if your HLLAPI application is interacting with BlueZone.

Configuring for Windows 16-bit HLLAPI application

1. On the BlueZone menu bar, click **Options** ® **API**.
2. Select the **Enable DDE Server Interface** check box.
3. Click **OK**.

   BlueZone is now listening for a DDE connection.
4. Click **Session** ® **Connect** to establish a connection to your host.
5. Configure your 16-bit HLLAPI application to connect to the BlueZone Thunking DLL (WHLAPI16.DLL).

   This could involve changing the application's settings so that it is looking for the BlueZone DLL called WHLAP16I.DLL, or you may have to rename the BlueZone DLL to the name that your application is programmed to look for.
6. Open your 16-bit HLLAPI application and execute a command that sends or receives data from your host.
7. Check to see if your HLLAPI application is interacting with BlueZone.

Configuring for DOS HLLAPI application - Windows 95/98/ME

1. On the BlueZone menu bar, click **Options** ® **API**.
2. Select the following check boxes:
   - **Enable DDE Server Interface**
   - **Auto-Launch the BlueZone DOS HLLAPI Redirector**
3. Click **OK**.

   BlueZone is now listening for a DDE connection.
4. Click **Session** ® **Connect** to establish a connection to your host.

   Important

   Ensure that the DOS HLLAPI Redirector is running by checking the Windows taskbar for a small yellow light bulb. This is the indication that the DOS HLLAPI Redirector is running.
5. Open a DOS shell.
6. Change to the working directory of where your DOS HLLAPI application is located.
7. At the DOS command prompt, type `VECT7F.EXE` to open the BlueZone VxD application.

   The following message opens: `DOS Virtual Machine Vector 0x7f Redirector`.
8. Open your DOS HLLAPI application and execute a command that sends or receives data from your host.

9. Check to see if your DOS HLLAPI application is interacting with BlueZone.

Configuring for DOS HLLAPI Application - Windows XP SP3

1. On the BlueZone menu bar, click **Options** ® **API**.

   The API Properties window opens.
2. Select the **Enable DDE Server Interface** check box.
3. Click **OK**.

   BlueZone is now listening for a DDE connection.
4. On the BlueZone menu bar, click **Session** ® **Connect** to establish a connection to your host.
5. Launch a DOS shell. Change to the working directory of where your DOS HLLAPI application is located.
6. At the DOS command prompt, launch the BlueZone VxD application by typing `BZHLLINT.EXE`.
   The following message appears: `The DOS HLLAPI interrupt has been successfully intercepted`.
7. Launch your DOS HLLAPI application and execute a command that sends or receives data from your host.
8. Check to see if your DOS HLLAPI application is interacting with BlueZone.

Configuring optional HLLAPI features

You can configure the following optional HLLAPI features:

Feature	Description
Connection retry time, on page 73	Defines the number of milliseconds to retry the BlueZone session connect when `ConnectPresentationSpace` is called. This setting is used by the `whllapi.dll` and `whlapi32.dll` DLLs and in conjunction with BlueZone scripting.
Telnet host wait time, on page 73	Defines the number of milliseconds to wait when a HLLAPI application calls the WAIT function. This setting is used by the `whllapi.dll` and `whlapi32.dll` DLLs.
HLLAPI auto-launch, on page 74	Automatically starts a BlueZone session when the HLLAPI DLL is accessed by a third-party HLLAPI application. HLLAPI applications require an active BlueZone session for the HLLAPI application to connect to the host. Configuring the HLLAPI application to start at the same time as the host session eliminates the need for the user to perform two steps; users must only start the HLLAPI application.

Enabling connection retry and Telnet host wait time features

1. Open the `BlueZone Desktop` installation source directory.
2. Open the `setup.ini` file in a text editor.
3. Locate the `[HLLAPI]` section:

```
[HLLAPI]
ConnectRetryMilliseconds=0
TelnetHostSettleMilliseconds=0
```

4. To enable the connection retry time feature, in the `ConnectRetryMilliseconds=` entry, type the time (in milliseconds) to retry the BlueZone session connect when `ConnectPresentationSpace` is called.
5. To enable the Telnet host wait time, in the `TelnetHostSettleMilliseconds=` entry, type the time (in milliseconds) to wait when a HLLAPI application calls the `WAIT` function.
6. Save and close the file.

Enabling HLLAPI auto-launch

1. Create a BlueZone session that is configured to start automatically.

   Refer to Configuring sessions, on page 45 for more information.
2. Save and close the session.
3. Open the `BlueZone Desktop` installation source directory.
4. Open the `global.ini` file in a text editor.
5. Locate the `[HLLAPI]` section:

   ```
   [HLLAPI]
   ;SessionA=
   ```

6. Delete the semicolon at the beginning of the entry.
7. Type the profile name that you want to automatically start. For example:

   `SessionA=mainframe.zmd\`
8. Save and close the file.
9. Add the location of your BlueZone HLLAPI DLL to your Windows PATH statement. By default, it is installed in the `C:\Program Files\BlueZone\6.1` directory.
10. If necessary, rename the BlueZone HLLAPI DLL to the name that your HLLAPI application is configure to start. If this is a configurable option in your HLLAPI application and you changed this value when configuring your HLLAPI application, this is not necessary.

Testing auto-launch

To test the auto-launch feature:

1. Start the BlueZone session and ensure that it is connects to your host.
2. While the BlueZone session is running, start the HLLAPI application.
3. Ensure that your application connects to the host system through BlueZone.
4. Close both the HLLAPI application and the BlueZone session.
5. Start the HLLAPI application.

   The BlueZone session named in the `global.ini` file starts and automatically connects to your host. The HLLAPI application also starts and connects through BlueZone to the host.

If the BlueZone session does not start, ensure that the following is true:

- The `global.ini` file exists.
- The `global.ini` file is in the `BlueZone Desktop` folder.
- The semicolon was not deleted from the `SessionA=` entry.
- The BlueZone session specified in `global.ini` exists and is configured to automatically start.

If the HLLAPI application does not connect to the host, ensure that following is true:

- The HLLAPI session hard coded to the correct session in the `global.ini` file.
- The `SetPath=` entry in the `setup.ini` file is set to `Yes`.

Capturing HLLAPI traces

This procedure assumes that you already have your HLLAPI application and BlueZone installed on the same computer.

1. On the BlueZone menu bar, click **Options** ® **API**.
2. Click the **Trace** tab.
3. Ensure that only the **Trace HLLAPI Interface** check box is selected.
4. Ensure that you have a valid path to a trace file. For example:

   `C:\Documents and Settings\`*`username`*`\My Documents\BlueZone\Traces\hllapi.trc`
5. Click **Start Trace**.
6. Start your HLLAPI application and execute a command that sends or receives data from your host.
7. When you are finished, click **Options** ® **API** and click the **Trace** tab.
8. Click **Stop Trace**.
9. Browse to the location where your trace file is stored. To view the trace, open it with a text editor.

Reviewing HLLAPI traces

The following is the beginning of a BlueZone HLLAPI trace. The return code in this example is 0 (`RetCode:0`). This means that the HLLAPI application successfully connected to the BlueZone session.

```
BlueZone v3.4 Build 455 API Trace Started 08/26/2004 at 13:47:47.701

Time:  13:47:53.605
Event: WinHLLAPI-In Task:0 Status:0 Func:21 Data:1384668 Len:0 RetCode:0

Time:  13:47:53.605
Event: WinHLLAPI-Out Task:0 Status:0 Func:21 Data:1384668 Len:0 RetCode:0
```

A return code of 1 indicates that the HLLAPI application is not connected to the BlueZone session.

Possible causes of a return code of 1 are:

- The `SetPath=Yes` in the `setup.ini` file is not configured, omitting BlueZone from the computer PATH environment variable.
- Your computer was not rebooted after changing the `SetPath=Yes` setting.
- The BlueZone DDE Server Interface is not enabled.
- The HLLAPI application is still trying to connect to a competitor's HLLAPI DLL installed on the computer.
- If your HLLAPI application is looking for a specific HLLAPI DLL name, the correct BlueZone HLLAPI DLL can be renamed with the wrong name.
- The wrong BlueZone HLLAPI DLL was renamed. Ensure that you rename the correct DLL. If your HLLAPI application is 32-bit, you must rename `whllapi.dll` (DDE) or `whlapi32.dll` (shared memory). If your HLLAPI application is 16-bit, you must rename `whlapi16.dll`.

Chapter 4: Distributing BlueZone

After you install and configure BlueZone to meet your users requirements, you can distribute a customized version of BlueZone. You can distribute BlueZone through a network server, push technology, or email.

Installation mechanics

During the installation process, the installation wizard automatically creates a BlueZone folder in the `All Users` common folder. Table 10: All Users common folder locations lists the available operating systems and the `All Users` location.

Table 10: All Users common folder locations

Operating system	Location
Windows XP SP3	`C:\Documents and Settings\All Users\Application Data\BlueZone\6.1`
Windows 7 and Vista	`C:\Users\All Users\BlueZone\6.1`

Any BlueZone profiles (configuration files) that you placed in the image are automatically copied from the `All Users` folder to the `\BlueZone\Config` folder in the working directory. The first time a user starts a BlueZone session or starts the BlueZone Session Manager, the BlueZone profiles are automatically copied to the working directory location specified during installation.

For example, if during the installation you used the default settings, your user's working files are placed in their `My Documents` folder.

```
...\My Documents\BlueZone\Config
```

Any BlueZone Scripts (`.bzs`, `.vbs`, and so on) that you placed in the image are automatically copied to the `\BlueZone\Scripts` folder. The first time a user starts a BlueZone session or starts the BlueZone Session Manager, the BlueZone scripts are automatically copied to the location specified during installation.

For example, if during the installation you used the default settings, your user's working files are placed in their `My Documents` folder.

```
...\My Documents\BlueZone\Scripts
```

In addition to the above mentioned files, any other included files are copied to their respective folders.

This feature is very helpful when you are pushing out a BlueZone installation image using software management software to many desktop machines and you want each user's working files to be stored in their own `My Documents` folder, even if multiple users use the same machine.

Important

Keep in mind that when you are finished creating your distribution image, it must have a completely flat file structure. It must not contain any folders. All BlueZone files must be at the same level.

Tip

You can use the BlueZone distribution image to create a self-extracting installation file by using a combination of WinZip and WinZip Self Extractor. To do this, change the quiet mode installation setting in the `setup.ini` file to `Yes`.

Creating a distribution image

The BlueZone installation and configuration process can be completely customized to meet the needs of your users without creating an unnecessary administrative burden. You can select only the BlueZone program files necessary for distribution. This collection of files is called a BlueZone distribution image.

Installing BlueZone from a distribution image is similar to performing a standard BlueZone installation. It differs in the following ways:

- You can customize your installation beyond the limits of the standard installation.
- You can include optional features that are not available during a standard installation.
- You can limit the files in the image to include only the files that you require.
- You can customize the look and feel of the BlueZone emulation clients to more closely match your user requirements.
- You can include BlueZone configuration files so that the BlueZone emulation clients are completely configured and automatically connect to your hosts.
- You can include BlueZone script files, Power Pad files, keyboard map files, or any other dialog-level configuration file.
- You can include the Software Activation File (SAF) which is necessary for licensing purposes.
- You can use the distribution image to create a quiet mode installation for use with software management programs that install desktop software using push technology.

To create a distribution image, you must:

1. Back up the installation source directory. Refer to Backing up the installation source directory, on page 77 for more information.
2. Delete any files that you do not need. Refer to Editing the distribution image contents, on page 78 to determine the files you can delete.
3. Configure the optional features and files. Refer to Configuring optional BlueZone features, on page 80 for more information.
4. Add any other additional files such as the Software Activation File, BlueZone configuration files, scripts, or macros. Refer to Adding optional files to the distribution image, on page 80 for more information.
5. Distribute the image to your users. They can then double-click `setup.exe` to install BlueZone using the standard installation wizard. Or, you can further automate the installation process using the quiet mode installation feature. Refer to Quiet mode installation, on page 80 for more information.

Backing up the installation source directory

The installation source directory is the `BlueZone Desktop` folder that you downloaded and its contents.

In case you need to go back to the original version of the files or create multiple distribution images, it is highly recommended that you create a backup copy of the installation source directory.

To do this, copy the entire `BlueZone Desktop` folder to a new location and rename it. For example, `BlueZone Desktop-Original`.

Editing the distribution image contents

To avoid distributing unnecessary files, you can decide which files are needed for your installation and which files can be deleted.

1. Open the `BlueZone Desktop` installation source directory.
2. Do not delete any of the files listed in Table 11: BlueZone files. They are all required, except for `readme.htm`.

Table 11: BlueZone files

File name	Purpose	Status
`0x040c.ini`	MSI initialization file - French	Required
`0x0407.ini`	MSI initialization file - German	Required
`0x0409.ini`	MSI initialization file - English	Required
`0x0411.ini`	MSI initialization file - Japanese	Required
`0x0413.ini`	MSI initialization file - Dutch	Required
`1031.mst`	MSI configuration file	Required
`1033.mst`	MSI configuration file	Required
`1036.mst`	MSI configuration file	Required
`1041.mst`	MSI configuration file	Required
`1043.mst`	MSI configuration file	Required
`BlueZone.msi`	Main BlueZone MSI file	Required
`common.cab`	Contains required files	Required
`common2.cab`	Contains required files	Required
`global.ini`	Global initialization file	Required
`setup.ini`	Setup initialization file	Required
`language.ini`	Language initialization file	Required
`setup.exe`	BlueZone installation program	Required
`readme.htm`	BlueZone Desktop readme file	Optional

3. Determine the folders that you want to keep. Delete any unnecessary folders.

   Table 12: BlueZone folders lists the folders in the installation source directory, their purpose, and required or optional status. These folders contain files that are either not used at all for installation or contain files that can be added to the installation as options.

Table 12: BlueZone folders

Folder name	Purpose	Status
\Assets	Contains images for the readme.htm file.	Optional
\Docs	Contains BlueZone Help and Administrator guides.	Optional
\Kerberos	Contains the Kerberos program CAB file.	Optional
\Patches	Contains BlueZone patch files (if any).	Optional – used for patching
\Unisys	Contains the T27, UTS, and Unisys program CAB files.	Optional
\Utils	Contains utilities that are not used during installation.	Optional
\Web2Host	Contains the Web-to-Host program CAB file.	Optional

4. If you keep any of the above folders, copy their contents to the parent BlueZone Desktop folder. The BlueZone Desktop folder must have a completely flat file structure.
5. Determine the CAB program files that you want and delete any unnecessary files. At least one BlueZone Program CAB file is required in a BlueZone distribution image.

   Table 13: BlueZone program CAB files lists the CAB files that you can choose to keep or delete from the distribution image as needed.

Table 13: BlueZone program CAB files

File name	CAB file contents	Status
bzadp.cab	BlueZone IBM 5250 iSeries Display files	Optional
bzap.cab *	BlueZone IBM 5250 iSeries Printer files	Optional
bzftp.cab	BlueZone FTP files	Optional
bzhllapi.cab	BlueZone HLLAPI files	Optional
bzicl.cab	BlueZone ICL Display files	Optional
bzmdp.cab	BlueZone IBM 3270 Mainframe Display files	Optional
bzmp.cab *	BlueZone IBM 3270 Mainframe Printer files	Optional
bzpwvlt.cab	BlueZone PasswordVault files	Optional
bzsc.cab	BlueZone Scripting support files	Optional
bzsm.cab	BlueZone Session Manager files	Optional
bztcpip.cab	BlueZone TCP/IP Print Server	Optional
bzvt.cab	BlueZone VT CAB	Optional
bzwhll.cab	BlueZone Scripting Object DLL	Optional

* The Printer CAB files cannot be installed by themselves. They are dependent upon their Display counterparts in order to operate properly. In other words, the Display CAB can be installed by itself but the Printer CAB requires the Display CAB.

Configuring optional BlueZone features

BlueZone has several optional features. Some of the BlueZone optional features can be installed using the standard installation wizard. However, there are several additional options and features that require manual configuration.

Refer to Configuring optional features, on page 27 for a list of the optional features and the steps to configure them.

Adding optional files to the distribution image

You can customize the distribution image even further by adding optional configuration files. You can add the following file types to the distribution image:

- Configured sessions
  Refer to Configuring sessions, on page 45 and Creating preconfigured configuration files, on page 50 for more information on configuring sessions.
- Desktop shortcuts
  Refer to Creating BlueZone desktop shortcuts, on page 50 for more information on configuring desktop shortcuts.
- Dialog configuration profiles
  Refer to Profile schemes, on page 58 for more information on configuring the profile schemes feature.
- Keyboards
  Refer to Mapping keyboards, on page 62 for more information on configuring keyboards.
- Power pads
  Refer to Configuring power pads, on page 68 for more information on configuring power pads.
- Scripts
- Macros

To include any additional files in the distribution image, copy the files to the `BlueZone Desktop` distribution image folder.

Creating a compressed distribution image file

You can distribute BlueZone by compressing the files in the BlueZone distribution image into a single, self-extracting, executable file using an archiving program such as ZIP2EXE in the PKZIP family of products or WINZIP Self Extractor. These archiving programs also protect the files from becoming corrupted during the transfer.

Use compressed files to distribute BlueZone from File Servers, FTP Servers, email, and any other method where the files must be transferred to the user prior to installation. When the user downloads the file to the desktop, running the executable unzips the files allowing access to the BlueZone `setup.exe` file.

Quiet mode installation

BlueZone can be completely configured and installed on a user's computer without the BlueZone installation interface being displayed. This is called quiet mode installation.

Quiet mode installation is a technique that is used by many customers who want to install BlueZone on a large number of users computers through a remote software installation and management program. For example, Microsoft Systems Management Server (SMS).

Because there is no user interface during a quiet mode installation, there is no opportunity for the user to select or change the installation options.

To perform a quiet mode installation, you must use the Windows Installer (`msiexec.exe`) through a DOS command line. The Windows Installer works in conjunction with the `BlueZone.MSI` and `setup.ini` files to control the BlueZone installation. Before running the Windows Installer, you must become familiar with the BlueZone settings that are controlled by the `setup.ini` file.

Edit the setup.ini file

There are several key features that are controlled by the BlueZone `setup.ini` file. Some features are related to the installation of BlueZone and other are related to the behavior of BlueZone.

Use a text editor to edit the `setup.ini` file. To enable some features, you must uncomment the line by deleting the semicolon (;) at the beginning of the line. Others features are modified by changing the value of an entry.

Refer to Default setup.ini file, on page 118 for format details and default values.

The following is a list of items that are typically used in conjunction with quiet mode installation. To make it easier to find these items in the `setup.ini` file, the items are listed in the order that they appear in the file:

- Destination directory
- Use personal folder as working directory
- Use all users common folder as working directory
- Use current user application data folder as working directory
- Set working directory
- Set default connection type
- Locking BlueZone emulation features
- Locking BlueZone Secure FTP features and commands
- Locking BlueZone Telnet features
- Show locked dialogs
- Disable append to clipboard feature
- Base registry setting
- Profile mode
- Profile sharing
- Setting BlueZone in the Windows path
- Enabling the power keys feature
- Enabling FIPS mode support
- Install script player only
- Session Manager run in tray
- Browser-based help
- Install BlueZone in a program group
- Create desktop application shortcuts
- Session Manager in startup folder

Installing BlueZone in quiet mode

1. Install BlueZone for the desktop using the standard installation method.

   Refer to BlueZone installation, on page 21 for more information.

2. Start the BlueZone emulation clients that you need for you application and create your BlueZone configuration files. Configure the configuration files to connect to your host systems and are ready to be used by your users. Save these configurations to your BlueZone working directory or some other convenient location your computer.

   Refer to Configuring BlueZone, on page 27 for more information.

3. Optional: Create the necessary BlueZone desktop shortcut files.

   Refer to Creating BlueZone desktop shortcuts, on page 50 for more information.

4. Create a BlueZone distribution image.

   This step is not mandatory, however, by creating a distribution image, you eliminate unnecessary BlueZone files and install only the BlueZone files that are necessary for your particular installation.

   Refer to Creating a distribution image, on page 77 for more information.

5. Optional: Copy the following files to the distribution image:

   - Configuration files
   - Script files
   - Desktop shortcuts

6. Edit the `setup.ini` file and make any necessary changes.

   By editing this file, you are able to control exactly how and where BlueZone is installed.

   Refer to Edit the setup.ini file, on page 81 and Default setup.ini file, on page 118 for more information.

7. Open a DOS command window and type:

   ```
   msiexec /i BlueZone.msi QUIET_INSTALL=1 ADDLOCAL=ALL
   ```

   Refer to MSI command line switch support, on page 83 for more information.

   Note

   You can also install BlueZone VBA by itself using the following command:

   ```
   msiexec /i BlueZoneVBA.msi QUIET_INSTALL=1
   ```

   This command assumes that the `bzvba.cab` file has been copied to the BZ install image folder.

   BlueZone Plus VBA is a separately licensed product and is not a component of the standard BlueZone Terminal Emulation Suite. Contact BlueZone sales for information about upgrading to BlueZone Plus VBA.

BlueZone installs quietly, and very quickly, without displaying any windows. If you enabled any desktop shortcuts, they automatically display on the desktop at the end of the installation process.

BlueZone configuration files are automatically placed in the `All Users` common folder:

```
C:\Documents and Settings\All Users\Application Data\BlueZone\Config
```

When a user starts BlueZone for the first time, any BlueZone configuration files that were copied to the `\All Users\Application Data\BlueZone\Config` folder, are automatically copied to the location that was specified in the `setup.ini` file. The default location is for the users working files to be stored in their `My Documents` folder.

This feature is helpful when you are pushing out a BlueZone installation image to many computers and you want each user's working files to be stored in their own `My Documents` folder even if multiple users use the same machine.

Installing BlueZone from a network server

The distribution image can also be used to distribute BlueZone over a network connection. This is accomplished by placing the BlueZone distribution image in a folder that is accessible by your users.

As long as the users can browse the Network Neighborhood to the folder that contains the BlueZone distribution image, BlueZone can be installed over the network.

1. Distribute (perhaps though email) the server name, drive, and distribution image directory name to your users.
2. From the distribution image directory, instruct users to double-click `setup.exe`.
3. The user can enter setup information during the course of the installation or it can be preconfigured with the `setup.ini` file.
4. The BlueZone setup program installs BlueZone on the user's computer.

MSI command line switch support

You can also use the Windows Installer program (`MSIEXEC.EXE`) to install BlueZone. Windows Installer uses a command line interface.

`BlueZone.msi` is designed to be used in conjunction with the supplied `setup.ini` file. Many BlueZone features and options can be modified or changed by editing the `setup.ini` file. The advantage to this is that you do not have to know the Windows Installer command line syntax to modify or change BlueZone features and options.

Refer to Default setup.ini file, on page 118 for default values.

Note

This procedure assumes that you are already familiar with Microsoft's Windows Installer. Also, this procedure assumes that you are already familiar with the concept of a BlueZone distribution image. Refer to Creating a distribution image, on page 77 for more information.

As you learned in Creating a BlueZone distribution image, it is possible reduce the size of the BlueZone distribution image by deleting any BlueZone components that you do not need. However, it is important to know that you must keep any BlueZone components that you think you might need in the future, as part of the image.

The reason for this is because the Windows Installer makes a list of all of the BlueZone components that are present in the BlueZone distribution image during a BlueZone installation. Even if all the components are not installed during the initial installation, they are tracked in the list. Later, if you want to install a BlueZone component that was not installed during the initial BlueZone installation, just add the component to the Windows Installer command line and run an installation. The new component is added to your BlueZone installation.

If you add a component to the BlueZone distribution image (that was not there during the initial BlueZone installation) and perform an installation, the new component is not recognized and therefore, is not installed.

Note

If you want to add a BlueZone component to a machine where BlueZone has already been installed, the only option is to uninstall BlueZone first and install it again with the new component added to the BlueZone distribution image.

BlueZone specific command line switches

As mentioned above, `BlueZone.msi` is designed to work in conjunction with the BlueZone `setup.ini` file. Because BlueZone has a number of optional settings, using the `setup.ini` file simplifies the task of performing a command line installation.

However, it is possible to use the Windows Installer to set a particular BlueZone feature, like the BlueZone keyboard lock feature, using a BlueZone specific command line switch.

To accomplish this, you must know the exact name assigned to the keyboard lock feature (which is LOCK), and you must know the lock value to set the keyboard lock (which is 8), so that you can include this feature in the command line statement.

Refer to BlueZone MSI features, on page 160 for the specific feature values.

The following example creates a Windows Installer command line that installs BlueZone with the following features:

- No transform file
- No logging
- Prompt the user for restart if necessary
- Basic (semi- quiet) interface (displays a progress bar with cancel button) `/qb`

  Note

  If you want a completely quiet installation, use `/qn`.

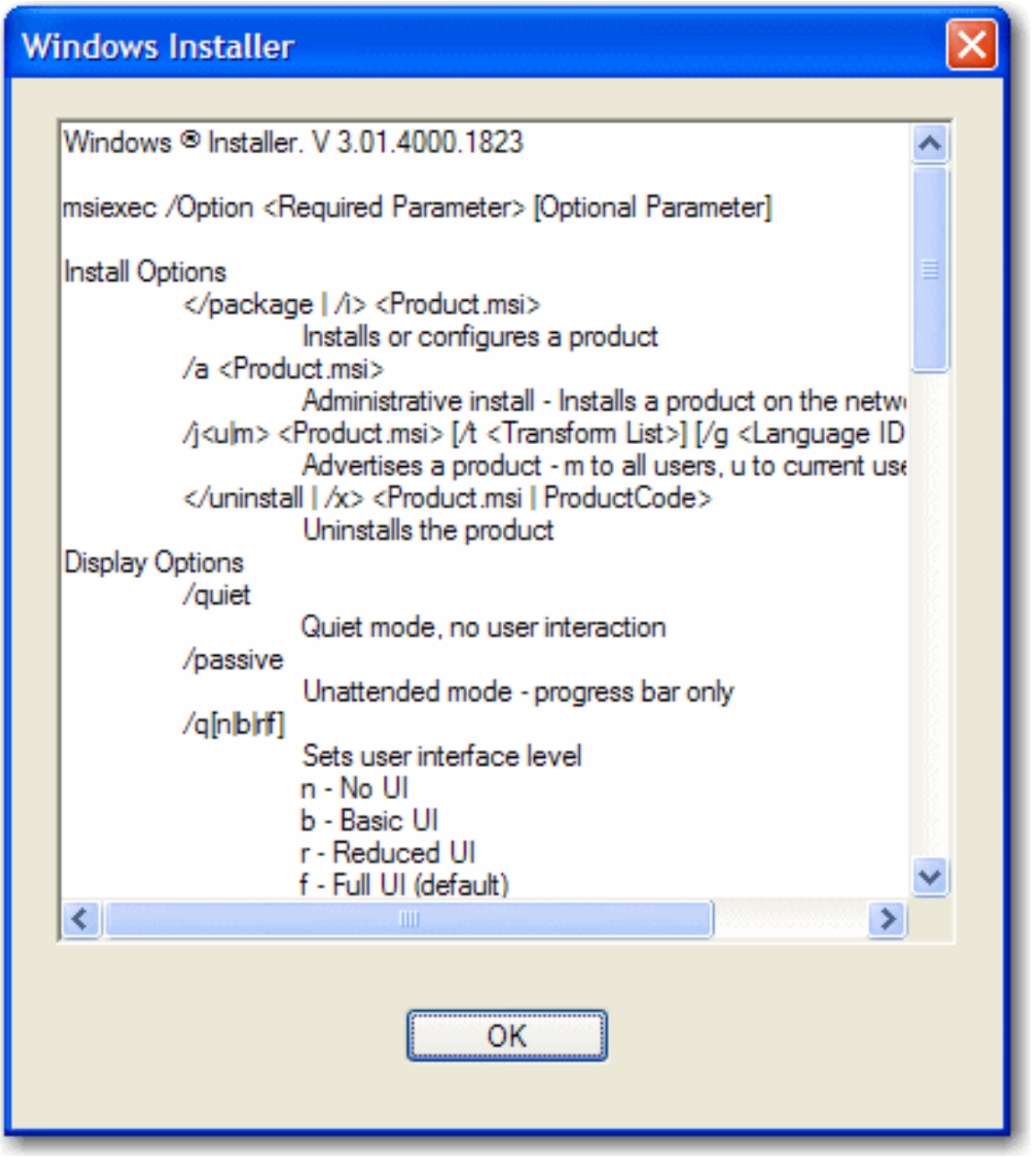
- BlueZone feature lock (LOCK) - Keyboard Lock = 8 (Locks BlueZone Keyboard map settings)

Command line switch example:

```
C:\>MSIEXEC /i "BlueZone.msi" LOCK="8" /promptrestart /qb
```

Note

If you need help with the Windows Installer command line options and switches, simply type MSIEXEC at a DOS prompt, and the following window will automatically be displayed:



Keep in mind that this is only an example of what can be done. Since the BlueZone keyboard lock feature is a standard part of the `setup.ini` file, you may find it easier to set the keyboard lock feature by editing the `setup.ini` file and not including `LOCK="8"` in the command line.

Using MSIEXEC to install specific BlueZone components

Using Windows Installer, you have the ability to select exactly which BlueZone components to install. This is accomplished by using the ADDLOCAL command line switch to control which BlueZone components get installed.

In order to use the ADDLOCAL feature, you must know the names of the individual BlueZone components so that you can include them in the Windows Installer command line. To keep things as simple as possible, the BlueZone component names use the same names as their CAB file names.

Refer to Editing the distribution image contents, on page 78 for a complete list of the BlueZone CAB files.

The following example uses a fictitious company with the following requirements:

Company XYZ has users who require the following BlueZone components:

- BlueZone Session Manager
- BlueZone Mainframe Display
- BlueZone Mainframe Printer
- BlueZone VT
- BlueZone Secure FTP

However, company XYZ has no users that require all of the above BlueZone components. Table 14: Sample user groups and required components lists company XYZ user groups and the BlueZone components that they require.

Table 14: Sample user groups and required components

User group	Component(s)
1	BlueZone Mainframe Display
2	BlueZone Session Manager BlueZone Mainframe Display BlueZone Mainframe Printer BlueZone Secure FTP
3	BlueZone VT
4	BlueZone Session Manager BlueZone VT BlueZone Secure FTP

Step 1: Creating a BlueZone distribution image

The first step is to create a BlueZone distribution image. It is recommended that you create one BlueZone distribution image that works with all of the above situations. In other words, your BlueZone distribution image contains all of the CAB files necessary to install all four groups. The advantage to this is that you only have to manage one BlueZone distribution image and in addition, in the future, if any of company XYZ's users want to add a BlueZone component to their installation, this can be accomplished without having to uninstall and reinstall BlueZone.

Note

You may even want to include additional CAB files for components that are not being installed now, but you may want to install in the future, like the BlueZone Mainframe Printer CAB and the BlueZone Scripting CAB. The advantage to this is that you do not have to uninstall BlueZone in order to install the new component.

Add any necessary BlueZone configuration profiles or desktop shortcut files to this image. Refer to Creating a distribution image for more information.

Step 2: Creating a command line for each group

To install BlueZone, use standard Windows Installer command line syntax using the ADDLOCAL feature to install the individual BlueZone Components. ADDLOCAL is standard Windows Installer syntax. You must know the names of the individual BlueZone components. They are the same names as the CAB file names.

Table 15: Installation command line syntax

User group	Command line syntax
1	C:\>MSIEXEC /i "BlueZone.msi" ADDLOCAL=bzmdp,common,common2 /qb
2	C:\>MSIEXEC /i "BlueZone.msi" ADDLOCAL=bzsm,bzmdp,bzmp,bzftp,common,common2 /qb
3	C:\>MSIEXEC /i "BlueZone.msi" ADDLOCAL=bzvt,common,common2 /qb
4	C:\>MSIEXEC /i "BlueZone.msi" ADDLOCAL=bzsm,bzvt,bzftp,common,common2 /qb

Note

You must include the common.cab and common2.cab files in all cases. Also, these examples assume that the DOS prompt is already in the same folder as the BlueZone.msi file. Otherwise, you must include the path to the BlueZone.msi file. For example, C:\>MSIEXEC /i "C:\Program Files\BlueZone\6.1\BlueZone.msi"

Tip

To execute a Windows Installer command line, one option is to type the Windows Installer command line at the DOS prompt. Another option is to place each of the above Windows Installer command lines into a separate text file that ends in .BAT. Give each file a name like UserGroup1.bat. Batch files can be executed from Windows explorer by double-clicking the file.

Using MSIEXEC to install all BlueZone components

If you have a set of BlueZone components that you want to install across all of your users, you can use the ADDLOCAL=ALL command line switch to perform the installation:

```
C:\>MSIEXEC /i "BlueZone.msi" ADDLOCAL=ALL /qb
```

ADDLOCAL=ALL automatically installs all of the BlueZone components that are present in the installation image.

Chapter 5: BlueZone licensing

The administrators of the BlueZone license must ensure strict compliance with the BlueZone License Agreement.

Click **Help** ® **About BlueZone** in any BlueZone emulation client to determine what type of license is installed.

Click **License Info** to view more information on the license.

BlueZone license types

BlueZone has the following license types:

Evaluation License
A temporary license that allows you to test BlueZone prior to purchase.

Single User License (SUL)
Holders can only install BlueZone on one computer. Each user is supplied with a unique BlueZone key, which is used to register BlueZone through the BlueZone Registration Wizard. The BlueZone Registration Wizard supplies a Software Activation File that is required in order for BlueZone emulation clients to operate.

Refer to Registering BlueZone, on page 25 for more information.

Concurrent User License (CUL)
Holders can make and distribute unlimited copies of BlueZone, but must ensure the proper use of the BlueZone License Manager software that limits the number concurrent BlueZone users. A Software Activation File is required in order for BlueZone emulation clients to operate.

The concurrent user license is the preferred licensing model for public Internet distribution of BlueZone. Concurrent user licensing eliminates the need to track user installations since this is automatically done by the BlueZone License Manager.

Refer to Configuring BlueZone with License Manager, on page 89 for more information.

BlueZone License Manager

BlueZone emulation clients can be licensed on a concurrent user basis under the control of the BlueZone License Manager. The License Manager is a 32-bit Windows application that can reside on any Microsoft Windows Server 2003, Windows Server 2008, Windows XP SP3, Windows Vista, Windows 7, or Windows 8 computer.

This application must be installed somewhere on the network that is accessible by BlueZone users. The License Manager requires little processing power to handle thousands of client license requests. Therefore, it can be installed on a system running the web server, BlueZone Security Server, or any other Windows PC with excess processing capability.

Note

It is recommended to use a Windows server instead of a Windows PC whenever possible.

Refer to the *BlueZone License Manager Administrator's Guide* for more information.

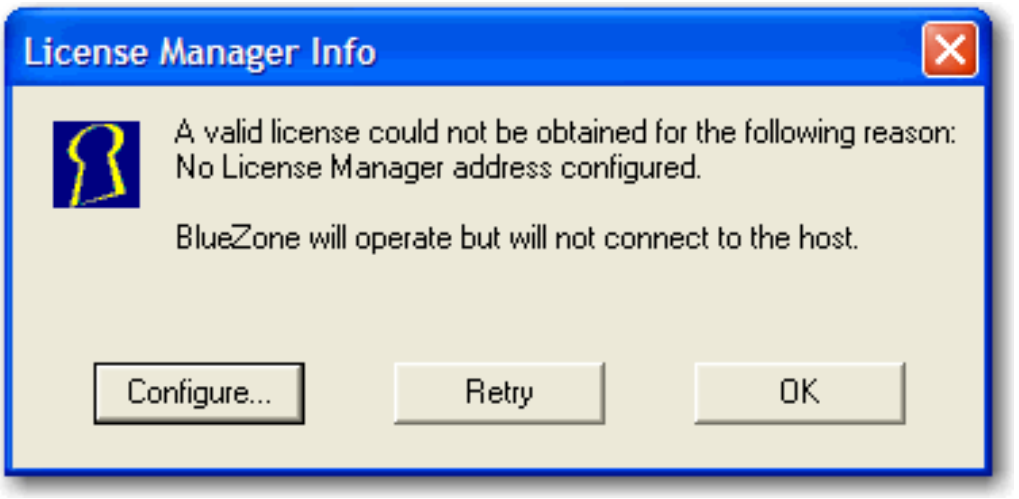
Configuring BlueZone with License Manager

When the installation of the BlueZone License Manager is complete, you must configure the IP Address of the License Manager in your BlueZone emulators.

To configure BlueZone for licensing with the License Manager:

1. Open the BlueZone Display emulator that you want to configure to work with the License Manager.

   When the emulator starts, you cannot obtain a license or make a host connection. The following message opens:



2. Click **Configure**.
3. Click the **License Manager** tab.
4. In the **Add Server** field, type the IP address of the License Manager server and click **Add**.

   The IP address displays in the **Server List**.
5. Click **OK**.
6. Click **Retry** on the License Manager Info window.

   You can now obtain a license.
7. On the BlueZone menu bar, click **File** ® **Save**.
8. Repeat steps 1-7 for each BlueZone Display emulator that you are using.

Note

There is no need to perform this procedure on the BlueZone Printer emulators. Only the BlueZone Display emulators require the License Manager IP address.

Chapter 6: BlueZone Session Manager

Starting with BlueZone Version 3.3, BlueZone Session Manager has been completely redesigned. The new Session Manager retains most of the features of the old Session Manager and adds a few new features as well. The new Session Manager has a presentation interface that is easier to use and more up-to-date in terms of its look and functionality.

BlueZone Session Manager is an optional component and is by default automatically selected to be installed by the installation wizard during the installation of BlueZone. If you do not want to install the BlueZone Session Manager, you can clear it from the list of optional components on the Components Selection window when you install BlueZone.

When you upgrade to BlueZone 5.0 or higher, the old Session Manager is replaced with the new one.

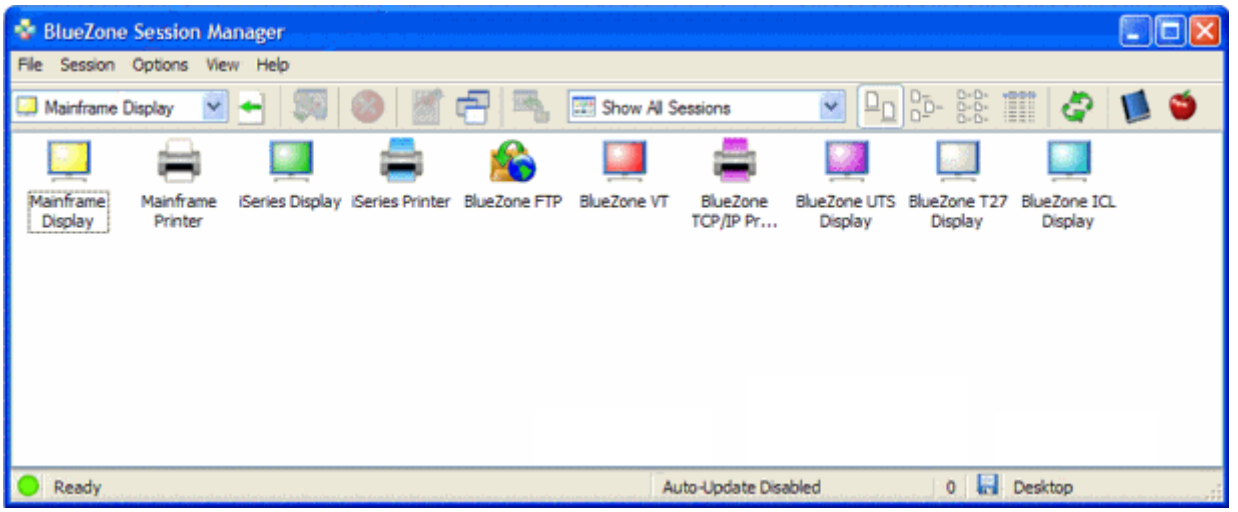
Interface overview

The BlueZone Session Manager provides a graphical environment for the purpose of viewing and managing BlueZone emulation client sessions. BlueZone Session Manager can be used to start preconfigured sessions, create new sessions, delete sessions, and create desktop icons.

When used in conjunction with BlueZone Desktop, BlueZone Session Manager provides the ability to automatically download and install BlueZone maintenance updates on users' workstations.

BlueZone Session Manager provides a simple user interface for creating and maintaining BlueZone session configurations. Figure 4: Session Manager interface is an example of the new BlueZone Session Manager showing one session for each of the BlueZone emulation clients:

Figure 4: Session Manager interface



Note

When you open BlueZone Session Manager for the first time, no icons are displayed because you have not created any BlueZone profiles (configuration files), unless you are upgrading BlueZone version 3.3 to version 5.0. If this is the case, your profiles are displayed in Session Manager.

Features overview

The major features of Session Manager are:

- Easy-to-use graphical interface
- Start individual BlueZone sessions
- Start multiple BlueZone sessions simultaneously
- Start all BlueZone sessions
- Create custom BlueZone session labels
- Start or create BlueZone sessions with an associated configuration file (profile mode)
- Create BlueZone desktop shortcut icons for selected sessions
- Session layout feature - start multiple sessions from one desktop shortcut
- Delete one or more BlueZone sessions simultaneously
- Monitor the status of BlueZone sessions
- Filter BlueZone sessions by session type
- Change the BlueZone session icon view
- Change from Windows Vista style icons to traditional BlueZone icons
- Quick launch feature works from the Windows system tray
- Can be automatically started with Windows

Installation

By default, BlueZone Session Manager is automatically installed during the BlueZone Desktop installation process. Session Manager is an optional feature. If you do not want to install BlueZone Session Manager, you must clear it from the BlueZone Components window during the BlueZone installation process.

There are two optional features that can be configured through the `setup.ini` file:

- Session Manager in Startup Folder , on page 35
- Session Manager Run in Windows System Tray, on page 35

If you want to change either of these options from their default settings, you must edit the `setup.ini` file before you install BlueZone.

Starting Session Manager

There are three methods available to start Session Manager:

- from a desktop shortcut
- from the Windows taskbar
- on system start

Launching from a desktop shortcut

By default, the BlueZone installer creates a desktop shortcut for the Session Manager. To start the Session Manager, double-click the Session Manager desktop shortcut.

Launching from the Windows taskbar

Session Manager has a feature called Quick Launch. By default, Session Manager automatically runs from your Windows taskbar tray. The advantage to using quick launch is that you can have Session Manager running without taking up space on your desktop, yet you can still access many of the Session Manager features with a simple right-click.

To use quick launch, look for the Session Manager icon  and right-click the icon. The Session Manager quick launch pop-up menu opens.

To use the Session Manager pop-up menu, click on the desired item.

Also, clicking on the Session Manager icon in the taskbar tray, causes the Session Manager to launch on your desktop. If you prefer not to launch Session Manager from the taskbar tray, you can turn this feature off by clearing this feature in the **Options** menu on the Session Manager menu bar or from the Session Manager taskbar menu.

Launching on system start

If you used the default settings, the BlueZone setup program adds the Session Manager to your Windows startup folder. When you start up your workstation, Session Manager automatically launches. If you prefer not to launch Session Manager when Windows starts, you can turn this feature off by clearing this feature in the **Options** menu on the Session Manager menu bar or from the Session Manager taskbar menu.

Creating sessions

1. Open Session Manager.
2. In the **Session Type** menu, select the BlueZone session type that you want to create.
3. Click the **New *session type*** icon.

   The BlueZone session starts and the Session Configuration window opens.
4. In the Session Configuration window, configure the session. Refer to Configuring sessions, on page 45 for more information.
5. Click **OK**.
6. Save the session.

Creating session layouts

You can start multiple sessions at the same time by creating session layouts.

1. Open Session Manager.
2. Select the BlueZone sessions that you want to add to the layout.

   To select multiple sessions, hold the Ctrl key and click the BlueZone sessions.
3. When you have all of the BlueZone sessions selected that you want in the layout, click the **Add Session Layout** icon.
4. Type a name for the session layout and click **Save**.

   A session layout icon is created in Session Manager using the file name as the label.

   When you double-click the session layout, all of the sessions start.

Starting sessions

1. Open Session Manager.
2. To start a single session, double-click on the BlueZone session icon.
3. If you want to start multiple sessions, press the Ctrl key and click the sessions you want to open. Click the **Launch Selected** icon .
4. If you want to start all of the sessions, click the **Launch All** icon.

Creating shortcut icons

You can use Session Manager to create desktop shortcut icons for any or all the BlueZone sessions in Session Manager.

1. Open Session Manager.
2. Select the BlueZone session icon that you want to create a desktop shortcut.

   To create multiple shortcuts, hold the Ctrl key and select all of the sessions that you want.
3. Click the **Create Desktop Shortcut** icon .

Filtering sessions

1. Open Session Manager.
2. In the **Session Filter** menu, select the BlueZone session type that you want to be displayed.

   Only BlueZone sessions of that type are displayed.

Deleting sessions

1. Open Session Manager.
2. Select the BlueZone session icon that you want to delete.
   To delete more than one session, press the Ctrl key and click all of the sessions that you want to delete.
3. Click the **Delete** icon.

Chapter 7: BlueZone Security Server

BlueZone Security Server is a Windows-based server software package designed primarily to provide Secure Sockets Layer (SSL/TLS) encryption for the BlueZone terminal emulator product line as well as other SSL/TLS enabled products. SSL/TLS is the standard for secure Internet communications and provides a cost effective solution ensuring data integrity, confidentiality, and authentication.

Security Server is required only if encryption is desired and SSL or TLS is not available on the host Telnet or FTP server.

Note

Security Server requires a license key in order to operate. If you are evaluating BlueZone and would also like to evaluate the Security Server, you can install and run the Security Server without a license key. When installed without a license key, the Security Server will automatically operate in the “evaluation mode” by limiting the number of connections to the Security Server to three. All other functions of the Security Server are available in the "evaluation mode".

If you must install the Security Server, refer to the *BlueZone Security Server Administrator's Guide*.

Note

BlueZone Security Server includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. Refer to http://www.openssl.org/ for more information.

Secure Sockets Layer (SSL)

BlueZone provides additional security features beyond those supplied through the network operating systems (NOS) or the native host security systems. The primary security function is a full implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption protocols that provides privacy, authentication, and message integrity. When used in conjunction with the BlueZone Security Server, BlueZone provides RSA SecurID Authentication and NT Domain Authentication. The iSeries also provides password encryption through the TN5250E server, referred to as the Encrypted Substitute Password feature, which BlueZone also supports.

SSL v3 and TLS v1 are the current Internet standards to insure privacy, message integrity, and authentication. This standardization ensures that BlueZone emulation clients work with any SSL/TLS enabled Telnet server including OS/390, z/OS, IBM CSNT, Novell NWSAA, and OS/400. If an SSL or TLS enabled Telnet server is not available, the Security Server can SSL enable any Telnet server.

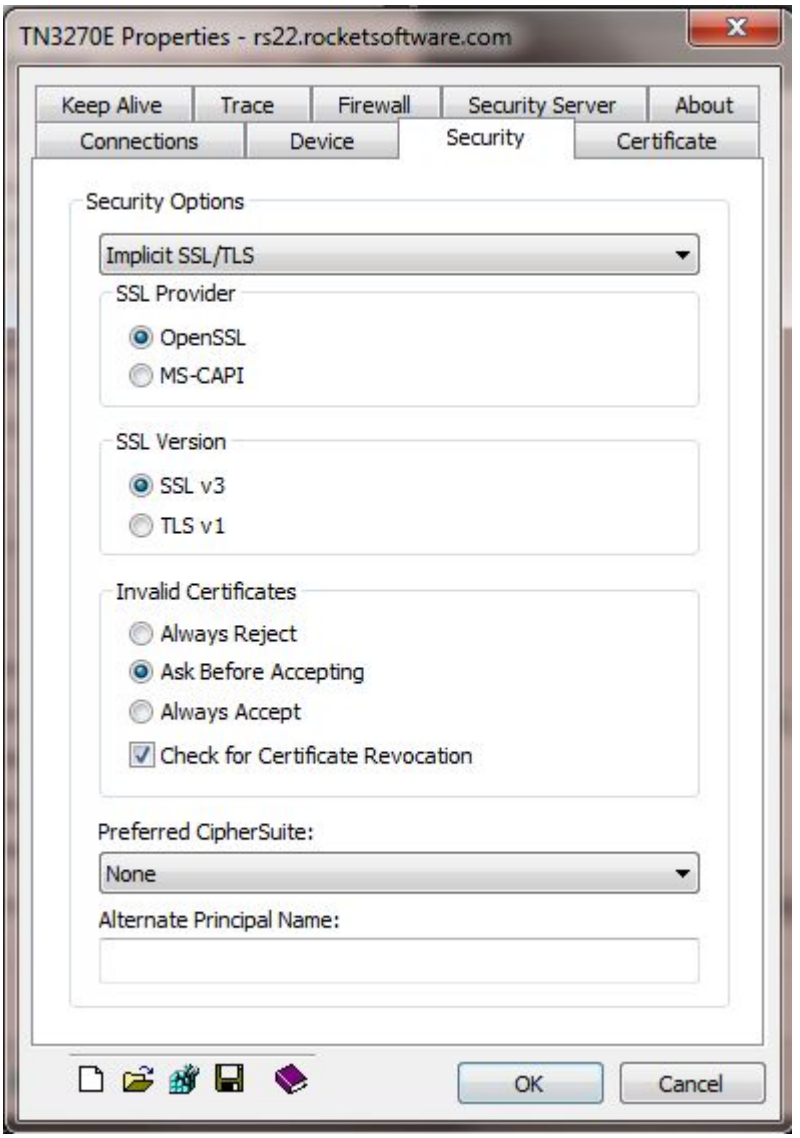
BlueZone Mainframe Display and Printer emulators, and the iSeries Display and Printer emulators support both Implicit SSL/TLS and Explicit SSL/TLS encryption. The SSL/TLS feature can be implemented in BlueZone on a connection-by-connection basis during the configuration process. BlueZone can also be distributed preconfigured with the encryption settings, eliminating user intervention in the installation and configuration process.

Refer to SSL/TLS configuration for the Telnet server being used for additional information. If the Security Server is being used, see the *BlueZone Security Server Administrator's Guide* for more information.

Refer to the *BlueZone Display and Printer User's Guide* for more information about configuring the Implicit SSL/TLS and Explicit SSL/TLS encryption feature in the Session Configuration.

The following screen shot shows the Security tab of the BlueZone IBM Mainframe Display emulator configured for Implicit TLS v1 encryption.

Figure 5: Security tab



RSA SecurID Token authentication

BlueZone provides built-in support for RSA SecurID Token Authentication. To enable this feature, BlueZone must be used with the BlueZone Security Server and have Secure Sockets Layer enabled. No additional configuration is necessary in BlueZone.

When BlueZone connects to the Security Server port, secured using SecurID, the end user is presented with the appropriate SecurID dialog. The end user types their user ID and token generated passcode. This is sent to the Security Server which in turn authenticates to the SecurID Ace Server. If authenticated, the end user is passed through to the host session. If the authentication fails, the connection is closed by the Security Server. All SecurID tokens and token modes are supported.

Refer to the *BlueZone Security Server Administrator's Guide* for more information about configuring for SecurID Authentication.

Windows Domain authentication

BlueZone provides built-in support for Windows Domain Authentication. To enable this feature, BlueZone must be used with the BlueZone Security Server and have Secure Sockets Layer enabled. No additional configuration is necessary in the BlueZone client.

When the BlueZone client connects to a Security Server port, secured using Windows Domain Authentication, the end user is presented with a standard Windows domain login dialog. The end user enters their user ID and password. This is sent to the Security Server, which in turn authenticates to the Windows Domain. If authenticated, the user is passed through to the host session. If the authentication fails, the connection is closed by the Security Server.

Refer to the *BlueZone Security Server Administrator's Guide* for more information about configuring for Windows Domain Authentication.

Encrypted substitute password configuration

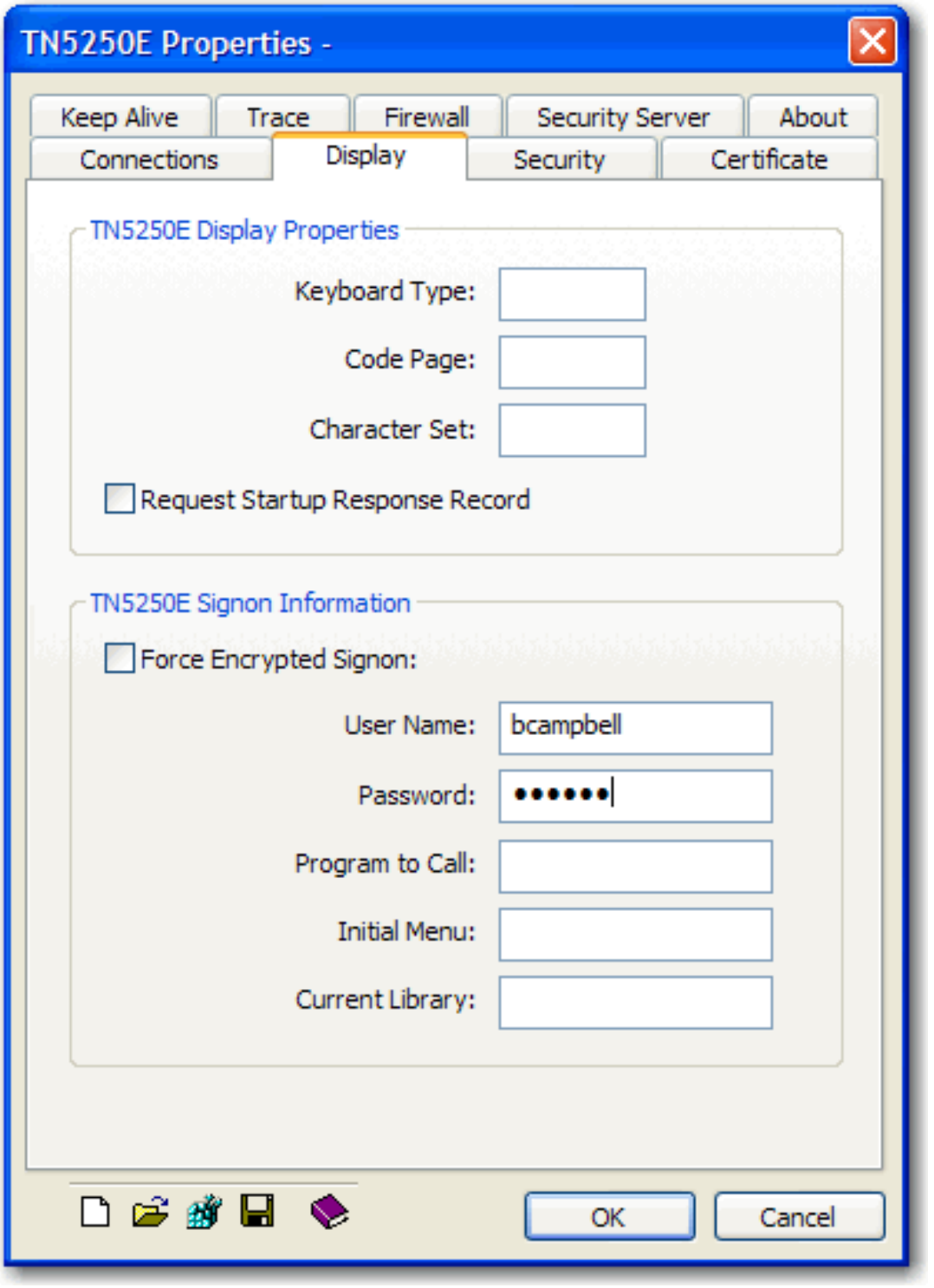
BlueZone for the iSeries supports a feature called Encrypted Substitute Password. This feature is enabled on the iSeries (by the iSeries administrator) by setting QRMTSGN to *Verify.

The end user types their name and password in the BlueZone Session Configuration. Upon connection, a negotiation takes place that sends this password securely to the iSeries, bypassing the main iSeries Sign on Screen. This is especially useful on Local Area Networks where data encryption is not required, but sending passwords in the clear is not desirable.

It can be used when you want to make the sign on process easier or perhaps if you want to provide public access to an iSeries host where it is not desirable or necessary to have end users enter a User Name and Password to gain access. It also can be used to "force" an encrypted sign on by presenting end users with a user name and password dialog box.

Use the **Display** tab in the TN5250E properties dialog to configure the sign on bypass values as shown. The **Program to Call**, **Initial Menu** and **Current Library** values are optional.

Figure 6: Display tab



Important

If the sign on bypass fails, the user will be taken to the main iSeries login screen. This will defeat the purpose of Encrypted Substitute Password because the end user will be able to sign on and send their password in the clear. To prevent this, an "exit" program should be used so that if an end user signs off, the iSeries will automatically force BlueZone to disconnect from the host.

As an option, you can choose to use the force encrypted sign on feature by selecting the **Force Encrypted Signon** check box.

When you are using the force encrypted sign on feature, the end user will be presented with a login dialog box each time they launch a BlueZone iSeries Display session.

Refer to the *BlueZone Display and Printer User's Guide* for more information about configuring the iSeries sign on parameters.

BlueZone express logon feature

Beginning with BlueZone version 5.1, the BlueZone Mainframe Display emulator has support for the IBM Express Logon feature, known as Certificate Express Logon. The BlueZone express logon feature allows you to configure BlueZone Mainframe Display sessions that automatically connect to an IBM Mainframe without requiring a user ID and password. When this feature is enabled, the Telnet server on the Mainframe uses certificate information from an SSL connection and the application ID supplied by BlueZone to request a user ID and a PassTicket (a temporary password) from the IBM host access control program RACF.

In order to use this feature, an administrator must configure the host, install certificates if necessary on user computers, configure BlueZone connection settings, and create and modify a BlueZone connection script (`.bzs`).

- TN3270 changes
- RACF changes
- Importing the certificate
- Configuring BlueZone for express log on
- Record and modify an express logon script

TN3270 changes

In TelnetParms:

```
TelnetParms

;      DEBUG TRACE JOBLOG

       SECUREPORT 993

       KEYRING SAF   your RACF keyring name

       ENCRYPTION DEFAULT ENDENCRYPTION
```

Add the following three lines:

```
       EXPRESSLOGON

       CLIENTAUTH SAFCERT

       CONNTYPE ANY

       SSLTIMEOUT 120

       NOSEQUENTIALLU

EndTelnetParms
```

You can also find this information in the following IBM publications:

- APPENDIX1.3 Appendix C - Express Logon Feature
- z/OS V1R9.0 Comm Svr: IP Configuration Reference

RACF changes

1. Add Root certificate - if not already available:

```
RACDCERT CERTAUTH ADD('your CA dataset name') TRUST -
withlabel(' 'your CA label' ')
```

2. Add Server certificate, if not already available:

```
RACDCERT ID(TN3270) ADD('your datasetname') TRUST -  WITHLABEL('your
label') PASSWORD('password')
```

3. Create RACF keyring:

```
RACDCERT ID(TN3270) ADDRING('your RACF keyring name')
```

4. Add certificates to the keyring:

```
RACDCERT ID(TN3270) CONNECT(CERTAUTH) - LABEL('your CA label')  RING('your
RACF keyring name')  -USAGE(CERTAUTH))

RACDCERT ID(TN3270) CONNECT(ID(TN3270)  - LABEL('your label') -RING('your
RACF keyring name') DEFAULT USAGE(PERSONAL))
```

5. For testing, a self-signed client certificate has been created:

```
RACDCERT ID('RACF userid') -

GENCERT -

SUBJECTSDN(CN('Name of User') -

  O('Name of Organization') -

  C('US'))                    -

WITHLABEL('BlueZone Client for Username') -

SIGNWITH(CERTAUTH LABEL(''your CA label'))

RACDCERT EXPORT(LABEL('BlueZone Client for Name of User')) -

ID('RACF userid') -

DSN('your dataset name') -

PASSWORD('client password') -

FORMAT(PKCS12DER)
```

   This data set is then sent using FTP to the user's machine and imported into their personal certificate store.

Importing the certificate

1. On the client computer, start Internet Explorer.
2. Click **Tools** ® **Internet Options**.

3. Click the **Content** tab.
4. In the Certificates section, click **Certificates**.
5. In the Certificates dialog box, click **Import**.
6. In the Certificate Import Wizard, perform the following steps:
   a. On the Welcome to the Certificate Import Wizard page, click **Next**.
   b. On the File to Import page, click **Browse** and navigate to the location containing the saved certificates.
   c. In the File type drop-down menu, select **Personal Information Exchange (*.pfx, *.p12)**. This displays all files with `.pfx` and `.p12` extensions.
   d. Select the certificate (`.pfx` or `.p12`) file that you saved previously, click **Open**, and click **Next**.
   e. On the Password page, type the password in the **Password** field, and click **Next**.
   f. On the Certificate Store page, click **Place all certificates in the following store**. In the Certificate store box, specify **Personal**, and click **Next**.
   g. On the Completing the Certificate Import Wizard page, click **Finish**.
   h. In the message box that appears, click **OK**.
7. In the Certificates dialog box, click **Close**.
8. Click **OK** to close the Internet Options dialog box.

Configuring BlueZone for express log on

1. Launch an existing BlueZone Mainframe Display session that connects to the desired host.
2. From the BlueZone menu bar, click **Session** ® **Configure**.
3. Click **Properties**.
4. Click the **Security** tab.
5. Select the desired **Security type** from the drop-down menu.
6. Click the **Certificate** tab.

   The certificate can be either in a disk file or in the system certificate store. If the client certificate was generated on the Mainframe, transfer it to your machine through FTP or IND$FILE.
7. Select the certificate by file name (disk) or common name (certificate store). Type in the rest of the required information required by your certificate selection.
   Certificates generated by the Mainframe are usually in PKCS12 format, which does not require a private key file, since the certificate and private key reside together in one file. A PKCS12 file can be put into the certificate store using Internet Explorer. Refer to How to Import the Certificate above.
8. Click **OK** twice. Remember to save your changes.

Recording and modifying an express logon script

You have the choice of starting the script when the session is either disconnected or connected, so it can or cannot start with a `Connect` event.

1. From the BlueZone menu bar, click **Script** ® **Record** and type a name for the script.

   Note

   BlueZone express log on is only supported with BlueZone Script files (`.bzs`).

2. Click **Save**.
3. Record the steps necessary to connect to your host (if not already) and log on to the desired application.
4. Click **Script** ® **Stop** to end the script recording.
5. Click **Script** ® **Edit** and select the script you just recorded.

   The BlueZone Script Editor launches and your script displays.
6. In the script, find the Script Event where you typed your user ID `(Type "MYUSERID")`, double-click it to open the field.
7. Replace your user ID with `")USR.ID("` and click **OK**.
8. In the script, find the Script Event `(Type "RpvPassword")`, double-click it to open the field.
9. Replace `"RpvPassword"` with `")PSS.WD("`.
10. Directly before the `Type ")USR.ID("` command, insert an express logon script event, and enter the host application ID for the application you want to use.
    You must get this application ID from your system administrator who configured the host for express logon.
    a. To do this, select the Script Event before `(Type ")USR.ID(")`. In the Script Events box, locate the `Express_Logon` event and double-click. This opens the field where you can enter the application ID.
    b. Click **OK**. This places the `(Express_Logon "Application ID")` Script Event immediately before the `(Type ")USR.ID(")` Script Event.
11. Save the script and exit the Script Editor.

Configuring Smart Card support

BlueZone supports SSL/TLS authentication using certificates stored on Smart Cards that are Microsoft Crypto API compliant. The certificates from the Smart Card are automatically added to the user's personal store by Windows, and are available to BlueZone using the **Use Client Certificate in Certificate Store** radio button in the Certificate tab of the TN3270 configuration.

1. Click **Session** ® **Configure** from the BlueZone menu bar.
2. Click **Properties**.
3. Click the **Security** tab.
4. Enable some type of SSL/TLS security and select the **MS-CAPI** radio button.
5. Click the **Certificate** tab.
6. Select the **Client Certificate on Smart Card** radio button.

Note

The Smart Card must be inserted into its reader in order to access the certificate. Windows prompts the user to insert the Smart Card if an attempt is made to use the certificate without the Smart Card being inserted.

Enabling SSL on z/OS

There are a few basic tasks which will be described in detail then are referenced in the various configuration scenarios. This document is based on z/OS 1.4 and 1.5. The gskkyman program is documented in System SSL Programming V1R4.0 SC24-5901-03 and an online copy of the document can be found at:

http://publibfp.boulder.ibm.com/cgi-bin/bookmgr/BOOKS/gska1a21/CCONTENTS

Steps required for creating certificates

1. Create an HFS KEYRING file.
2. Create a self-signed certificate.
3. Create a server certificate.
4. Create a client certificate.

Steps required to implement SSL

1. SSL for Telnet using a server certificate.
2. SSL for Telnet using a client certificate.
3. SSL for FTP using server certificate.
4. SSL for FTP using a client certificate.
5. Express logon (ELF).
6. SSL for CICS using a server certificate.
7. SSL for CICS using a client certificate.

Creating HFS KEYRING files

1. Enter the OMVS environment.
2. Create a directory for all SSL objects and change to that directory.
3. Enter the following command:
   `gskkyman`
4. Select **Option 1** to create a new database.
5. Enter a name for the file, for example `key.kdb`.
6. Enter a password twice.
7. Enter a password expiration value.
8. Enter a database record length of `2500`.
9. Select **Option 10** to save the database password in a file.

   The database is ready for use.

Creating self-signed certificates

1. Select **Option 6** to create a self-signed certificate.
2. Select one of the **CA certificate types**, for example `1 - CA with 1024 RSA key`.
3. Enter a label for the certificate. For example, `SigningCA`.
4. Enter the certificate information:
   a. Common name, for example `Signing Certificate`
   b. Organization Unit, for example `Rocket Software`
   c. Organization, for example `PD`
   d. City
   e. State
   f. Country

g. Number of days that the certificate is valid. The certificate can be valid from 1 – 9999 days.

5. Select **Option 1** to manage keys and certificates.
6. Select **SigningCA**.
7. Select **Option 7** to export certificates and keys.
8. Select **Option 3** or **Option 4**.
9. File name `SigningCA.p12`.
10. Enter a password twice.
11. Enter `0` for export encryption.
12. Change to your PC.
13. FTP the `.p12` file to the PC using binary if option 3 was used to export or ASCII is option 4 was used.
14. Open Internet Explorer:
    a. Click **Tools** ® **Internet Options**.
    b. Select the **Contents** tab.
    c. Click **Certificates**.
    d. Click **Import**.
    e. Click **Next**.
    f. Select file that was FTPed to the PC.
    g. Click **Next**.
    h. Type the certificate password and select the **Mark this key as exportable** check box.
    i. Click **Next**.
    j. Place the certificate in the Trusted Signing store.
    k. Click **Next**.
    l. Click **Finish**.

Creating server certificates

1. Select **Option 4** to create new certificate requests.
2. Select one of the **Certificate Types**, for example **1 – CA with 1024 RSA key**.
3. Request a file name, for example `Server.arm`.
4. Enter the certificate information:
    a. Common name, for example `Server Certificate`
    b. Organization Unit, for example `Rocket Software`
    c. Organization, for example `PD`
    d. City
    e. State
    f. Country
5. Exit gskkyman.
6. Sign the request by issuing:
   `gskkyman -g -x 360 -cr Server.arm -ct Server.cer -k yourkey.kdb`
7. Enter yourkey.kdb password
8. Enter gskkyman
9. Select **Option 2** to open a database.

10. Yourkey.kdb
11. Enter the password.
12. Select **Option 5** to receive the requested certificate.
13. Enter the name of the certificate: `Server.cer`.

Creating client certificates

1. Select **Option 4** to create new certificate requests.
2. Select one of the certificate types, for example, **1 – CA with 1024 RSA key**.
3. Request a file name, for example, `Client.arm`.
4. Enter the certificate information:
    a. Common name, for example, `Client Certificate`
    b. Organization Unit, for example, `Rocket Software`
    c. Organization like PD
    d. City
    e. State
    f. Country
5. Exit gskkyman.
6. Sign the request by issuing the following command:
   `gskkyman -g -x 360 -cr Client.arm -ct Client.cer -k yourkey.kdb -l SigningCA`
7. Enter yourkey.kdb password.
8. gskkyman
9. Select **Option 2** to open a database.
10. Yourkey.kdb
11. Enter the password
12. Select **Option 5** to receive the requested certificate.
13. Enter the name of the certificate file: `Client.cer`
14. Select **Option 1** to manage the keys and certificates.
15. Select **Client**.
16. Select **Option 7** to export the certificate and key or **Option 6** to export the certificate without a key.
17. Select **Option 3** or **Option 4** PKCS #12 version 3 (if option 6 it will be PKCS #7)
18. File name `Client.p12`.
19. Enter password twice.
20. Enter `0` for export encryption
21. Change to your PC
22. FTP the p12 file to the PC using Binary if option 3 was used to export or ASCII if option 4 was used.
23. Open Internet Explorer:
    a. Click **Tools** ® **Internet Options**.
    b. Select the **Contents** tab
    c. Click **Certificates**.
    d. Click **Import**.

e. Click **Next**.
f. Select the file that was FTPed to the PC.
g. Click **Next**.
h. Enter the certificate password and select the **Mark this key as exportable** check box.
i. Click **Next**.
j. Place the certificate in the personal store.
k. Click **Next**.
l. Click **Finish**.

24. Open a BlueZone Display:
    a. Click **Session** ® **Configure**.
    b. Click **Properties**.
    c. Select the **Security** tab and select the **Enable Secure Sockets Layer** check box
    d. Select **SSL v3**.
    e. Select the **Certificate** tab and select the **Client Certificate in Disk File** radio button.
    f. Click **Browse** and select the `Client.p12` file.
25. FTP `Client.p12` back as an MVS dataset.
26. Go back to the Mainframe Display.
27. Go to ISPF 6 to enter a TSO command.
28. Enter the following RACF command:
```
RACDCERT ID(USERID) ADD('USERID.CLIENT.P12') TRUST WITHLABEL('Client')
PASSWORD('xxxxxxxx')
```

SSL for Telnet using server certificate

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.
2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.
3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.
4. OMVS change to your SSL directory.
    a. gskkyman
    b. Select **Option 2** to open a database.
    c. Enter the database name.
    d. Enter the password.
    e. Select **Option 1** to manage keys.
    f. Select the server certificate.
    g. Select **Option 3** to set the key as the default.
5. Add the following to TCPIP.PROFILE:
    a. TelnetParms
    b. SECUREPORT 992
    c. KEYRING HFS /ssl/key.kdb
    d. SSLTIMEOUT 120
    e. EndTelnetParms

SSL for Telnet using client certificate

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.
2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.
3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.
4. Create a client certificate. Refer to Creating client certificates, on page 104 for more information.
5. Add the following to TCPIP.PROFILE:
    a. TelnetParms
    b. SECUREPORT 992
    c. KEYRING HFS /ssl/key.kdb
    d. CLIENTAUTH SAFCERT
    e. SSLTIMEOUT 120
    f. EndTelnetParms

SSL for FTP using server certificate

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.
2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.
3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.
4. Modify the FTP configuration dataset, for example, TCPIP.FTP.DATA, and add the following:
    a. EXTENSIONS AUTH_TLS
    b. SECURE_LOGIN NO_CLIENT_AUTH
    c. TLSTIMEOUT 500
    d. KEYRING /ssl/key.kdb
    e. SECURE_CTRLCONN PRIVATE
    f. SECURE_DATACONN PRIVATE
    g. SECURE_FTP REQUIRED
    h. TLSPORT 0

Note

TLSPORT 0 was an undocumented parameter.

SSL for FTP using client certificate *

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.
2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.

3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.
4. Create a client certificate. Refer to Creating client certificates, on page 104 for more information.
5. Modify the FTP configuration dataset, for example, TCPIP.FTP.DATA, and add the following:
   a. EXTENSIONS AUTH_TLS
   b. SECURE_LOGIN VERIFY_USER
   c. TLSTIMEOUT 500
   d. KEYRING /ssl/key.kdb
   e. SECURE_CTRLCONN PRIVATE
   f. SECURE_DATACONN PRIVATE
   g. SECURE_FTP REQUIRED
   h. TLSPORT 0

Note

This configuration has not been attempted *

Express Logon (ELF)

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.
2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.
3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.
4. Create a client certificate. Refer to Creating client certificates, on page 104 for more information.
5. Add `EXPRESSLOGON` to the `TelnetParms` block.
6. Issue the following command:

   ```
   SETR CLASSACT(PTKTDATA)
   ```

7. Issue the following command:

   ```
   RDEF PTKTDATA TSOSYS1 SSIGNON(KEYMASKED(E001193519561977)) UACC(NONE)
   APPLDATA('NO REPLAY PROTECTION')
   ```

   Where:

   - `KEYMASKED` is any combination of 16 hexadecimal characters.
   - `TSOSYS1` is TSO concatenated with the value of SID in SMFPRMxx if VTAM generic resource naming is not being used. If VTAM generic resource naming is being used, see *z/OS V1R4.0 Security Server RACF Security Administrator's Guide*, 7.13.3.1 Determining Profile Names.
   - A passticket expires in 10 minutes, to make it expire after signing on add: `APPLDATA('NO REPLAY PROTECTION')`.

SSL for CICS using server certificate

1. Create an HFS KEYRING file. Refer to Creating HFS KEYRING files, on page 102 for more information.

2. Create a self-signed certificate if a trusted CA is not available. Refer to Creating self-signed certificates, on page 102 for more information.
3. Create a server certificate. Refer to Creating server certificates, on page 103 for more information.

   Note

   When creating the server certificate, the label name needs special attention. It is not required but it is better to name the label the same as the starting point of the host name: `https://cics14.bluezonesoftware.com` would have a label of `cics14`. If both are named the same it will eliminate a dialog box when the URL is accessed.

4. On the PC, locate the signing CA certificate and FTP it to the mainframe using binary or ASCII depending on which option was used when it was exported. FTP to an MVS dataset.
5. On MVS, select ISPF option 6, ISPF Command Shell, and issue the following RACF commands:
   - `RACDCERT ID(CICS USERID) ADDRING(RINGNAME)`
   - `RACDCERT ID(CICS USERID) CONNECT(CERTAUTH LABEL('Signing CA label') RING(RINGNAME))`
   - `RACDCERT ID(CICS USERID) CONNECT(LABEL('Server label') RING(RINGNAME))`
6. Edit the CICS SIP file as follows:
   a. ENCRYPTION=NORMAL, (56 bit) =STRONG (168 bit),
   b. KEYRING=RINGNAME,
   c. SSLDELAY=600,
   d. SSLTCBS=8,
7. Change the CICS startup JCL making sure that the SSL SGSKLOAD dataset is available by means of the STEPLIB, JOBLIB unless it is listed the LNKLST IPL parameter.
8. For the CICS TCPIPSERVICE resource:
   a. Set the port number. 684 is the well known port.
   b. Set the SSL property to YES.

SSL for CICS using client certificate

1. Follow SSL for CICS using server certificate, on page 107.
   a. `RACDCERT ID(CICS USERID) CONNECT(LABEL('Client label') RING(RINGNAME))`
2. For the CICS TCPIPSERVICE resource:
   a. Change the SSL property to `CLIENTAUTH`.
   b. Set the certificate to the label of the client certificate.

Chapter 8: TCP/IP print server

BlueZone TCP/IP Print Server is a Windows application that supports the Line Printer Daemon (LPD) protocol enabling users to receive and customize print jobs from an Line Printer Request (LPR) client on any iSeries, Mainframe, UNIX, or Windows-based system, to any Windows defined printer, whether locally attached or remote.

BlueZone TCP/IP Print Server is known as a Line Printer Daemon, or LPD for short. A daemon is a server or sometimes referred to as an agent. BlueZone TCP/IP Print Server is an LPD Server.

LPR/LPD is a printing method used in many TCP/IP networks. It is in wide use on university and business campuses where IBM Mainframe and iSeries systems as well as UNIX-based systems have been in place for a long time. LPR/LPD is a computer-to-computer printing method, rather than a host-to-PC method.

The LPR/LPD protocol is broken into two parts: LPR and LPD.

LPR (Line Printer Request)
This is the part that submits the print request. LPR is the client part of the protocol and is sometimes confused when used on a Mainframe. Any system submitting requests through an "LPR client" is referred to as a client.

LPD (Line Printer Daemon)
This is the piece that receives and processes the request. A "daemon" is a server or agent. BlueZone TCP/IP Print Server is an LPD server.

The LPD Protocol Specification is documented in RFC 1179.

Use the BlueZone TCP/IP Print Server where your host system is running a Line Printer Request (LPR) client that is configured to send print jobs to a specific user IP address.

The BlueZone TCP/IP Print Server is a Line Printer Daemon (LPD) that runs on the user's workstation that listens for print jobs that are being sent directly to it by the LPR client.

TCP/IP print server installation

The BlueZone TCP/IP Print Server is installed using the standard BlueZone Desktop installation wizard setup program. BlueZone TCP/IP Print Server is one of the components that can be selected during installation. BlueZone TCP/IP Print Server is not selected by default. You must select TCP/IP Print Server from the Component Selection list in order for it to be installed.

Refer to BlueZone installation, on page 21 for more information.

Starting the TCP/IP print server

1. Double-click the desktop icon that was created during the BlueZone installation.

   You can also start BlueZone TCP/IP print server from the BlueZone Program Group by going to **Start** ® **Programs** ® **BlueZone** and clicking on **BlueZone TCP/IP Print Server**.

   By default, the BlueZone TCP/IP Print Server automatically starts in the Windows System Tray without appearing on the Windows desktop.

   If you want to configure the BlueZone TCP/IP Print Server, start the BlueZone TCP/IP Print Server, then locate the BlueZone TCP/IP Print Server icon in the Windows system tray and click. The BlueZone TCP/IP Print Server desktop application opens.
2. From the BlueZone TCP/IP Print Server menu bar, click **Session** ® **Start**.

Listening... displays in the status bar when the BlueZone TCP/IP Print Server is started.

Note

The first time you start the BlueZone TCP/IP Print Server, you are prompted with a Print Setup window. You cannot proceed until you supply a Printer Queue Name.

Stopping the TCP/IP print server

From the BlueZone TCP/IP Print Server menu bar, click **Session** ® **Stop**.

You can also click the **Stop Session** icon from the BlueZone TCP/IP Print Server toolbar.

Stopped displays in the status bar when the BlueZone TCP/IP Print Server is stopped.

TCP/IP Print Server configuration

The first time you start the BlueZone TCP/IP Print Server, you are required to provide a Queue Name. This Queue Name must match the Queue Name that your LPR client is using to send print jobs to your LPD Server. The Queue Name uniquely identifies your BlueZone TCP/IP Print Server (LPD Server) running on your workstation.

Note

If you do not know the Queue Name that your LPR client is using to send jobs to your LPD Server, you can type any name you want and change it later.

Refer to *BlueZone Display and Printer User's Guide* Version 3.4, or higher, for detailed information on configuring and using the BlueZone TCP/IP Print Server.

Chapter 9: BlueZone PasswordVault

BlueZone PasswordVault is designed exclusively to work with the BlueZone family of terminal emulation products. BlueZone PasswordVault provides a convenient, easy-to-use means of storing, managing, and accessing your host account logon information. BlueZone PasswordVault stores all of your passwords in a single encrypted repository, unlocked by your Windows account, fingerprint, smart card, or password of your choosing.

BlueZone PasswordVault not only provides secure storage of account data but also automatically detects host logon screens and prompts. Upon detecting a prompt, BlueZone PasswordVault displays a window, preset to the appropriate stored account, allowing you to auto-fill the account information. If this is the first time you are accessing a particular host and an account has not yet been recorded, you can automatically create a new entry through the same window.

BlueZone PasswordVault has its own help file that can be opened from the application.

PasswordVault installation

BlueZone PasswordVault is installed as a stand-alone application through an MSI. Refer to the *BlueZone PasswordVault User's Guide* for more information on the installation process.

Enabling BlueZone PasswordVault

When BlueZone PasswordVault is installed, it is not automatically enabled. To enable BlueZone PasswordVault:

1. Click **File** ® **Properties** from the BlueZone menu bar.
2. Select the **Enable Password Vault** check box located at the bottom of the window.
3. Click **OK**.

Chapter 10: BlueZone scripts

BlueZone offers a wide variety of powerful tools for automating repetitive tasks, streamlining the user interface, and communicating with external applications. BlueZone scripts can be recorded in either a proprietary format, or in a text-based format recorded in either VBScript or JavaScript.

Note

Some applications refer to the function used to automate tasks as a macro. BlueZone refers to this function as a script and offers several automation technologies from the **Script** menu in the BlueZone emulators.

BlueZone proprietary scripts

BlueZone proprietary scripts are recorded and played back using a proprietary method. Scripts are created by recording keystrokes, but can be edited later to change the playback. BlueZone proprietary scripts are targeted at users with a basic understanding of scripting and logic, but without the skill sets required to write and edit VBScripts or JavaScripts.

Scripts are edited using the BlueZone Script Editor (`bzse.exe`) application, which is opened from the BlueZone emulator menu bar by selecting **Script** ® **Edit**, and selecting a `.bzs` script file.

BlueZone Script Editor is a GUI tool that allows users to drag script events into the script flow, change the order of events, and delete previously recorded events. BlueZone scripts support a proprietary mechanism called Wait_Ready that ensures that the host is ready to accept input, even when using TN3270 or TN3270E.

BlueZone proprietary scripts have the following features:

- Easy to record.
- Easy to edit with BlueZone Script Editor.
- Keyboard lock state aware.
- Support advanced functions like wait for, watch for, text input, and so on.
- Can execute other programs using the Run command.
- Can run BlueZone menu commands, for example, Copy, Paste, and Print Screen.
- Can accept variables passed from a BlueZone Web-to-Host Object Tag, for example, Login ID and Password generated dynamically by the web application and used to sign the user into the mainframe.
- The BlueZone administrator can control whether or not end users can record and play scripts or only play scripts. Refer to Controlling scripting access, on page 114 for more information on this feature.
- Do not support text input variables.
- Do not support file I/O.
- Does not have external application integration.

BlueZone text-based scripts

BlueZone text-based scripts can be written or recorded in either VBScript or JavaScript. Scripts are typically created by recording keystrokes, but can be edited later to change the playback. BlueZone text-based scripts are targeted at users who want to leverage their proficiency with either VBScript or JavaScript, and want to take advantage of being able to write and edit BlueZone scripts in a scripting language that they already know.

Scripts are edited using the BlueZone Script Host and Debugger (`bzsh.exe`) application, which is opened from the BlueZone emulator menu bar by selecting **Script** ® **Edit**, and selecting a `.vbs` or `.js` script file.

BlueZone text-based scripts have the following features:

- Easy to record or can be written from scratch.
- Written in VBScript or JavaScript.
- Easy to edit with BlueZone Script Host and Debugger.
- Support unique BlueZone methods that control the behavior of BlueZone.
- Require a working knowledge of VBScript or Java Script.

BlueZone scripting host

BlueZone scripting host is a language-independent host for ActiveX scripting engines on 32-bit Windows platforms. This tool allows you to run Visual Basic Scripting Edition (VBScript) and JScript natively within the base operating system, either on Microsoft Windows XP SP3, Windows Vista, Windows 7, or Windows 8 and acts as a host for other ActiveX-supported scripting languages such as Perl, Rexx, and Python.

In addition, BlueZone Script Host allows scripts to communicate with BlueZone Display emulation software products. Using the scripting languages you already know, you can write scripts to execute common tasks on a variety of host systems, automate user input, obtain data from host systems, initiate file transfers, and more.

Using BlueZone Script Host and Debugger, BlueZone can record and playback scripts using VBScript or JavaScript. Once recorded, these scripts can be played back as-is, or edited using the Script Host and Debugger. The record and playback feature makes using VBScript and JavaScript available to the non-technical user.

BlueZone Script Host and Debugger is also a general purpose VBScript and JavaScript debugger that supports break points, stepping, and color-coding of scripts providing a powerful interface for script development.

The BlueZone Script Host and Debugger and Dialog Editor contain the following features:

- Very powerful.
- Can control multiple host sessions simultaneously.
- Use of industry standard scripting languages.
- Direct access to read from and write to the host screen.
- File I/O support.
- Support of scripted variables.
- COM compliance allows any other COM complaint component to be loaded by the script to extend its functionality.
- Powerful editing and debugging features.
- Ability to view the value of script variables while executing/debugging the script.
- Dialog support to create Windows dialogs for user interaction.
- Attachmate Extra! Basic and NetManage Chameleon macro compatibility to provide easy migration from those emulators to BlueZone.
- Complex, text-based scripting language.
- Requires a relatively high degree of scripting ability.

Refer to the *BlueZone Advanced Automation Developer's Guide* for more information on using the Script Host and Debugger and the Dialog Editor.

Controlling scripting access

You can control scripting by making several scripting files available or unavailable during the BlueZone installation process. This method of making files available or unavailable is controlled by editing a setting in the `setup.ini` file.

- Users can record, edit, and play BlueZone proprietary scripts and text-based scripts. This is the default setup. You do not need to make any modifications to the `setup.ini` file.
- Users can only play BlueZone proprietary scripts and text-based scripts.

  1. In the BlueZone distribution image, open the `BlueZone Desktop` folder.
  2. Open the `setup.ini` file in a text editor.
  3. Locate the `InstallScriptPlayerOnly=No` entry.
  4. Edit the entry value to `InstallScriptPlayerOnly=Yes`.
  5. Save and close the file.

  Refer to Creating a distribution image, on page 77 for more information on creating a BlueZone distribution image, and Default setup.ini file, on page 118 for more information on the `setup.ini` file.

File	Description
`bzse.exe`	Include the file in the BlueZone distribution image to include the BlueZone Script Editor. Users can record, edit and play BlueZone proprietary scripts (`.bzs`). If the `bzse.exe` file is not included in the BlueZone distribution image, users are only able to play BlueZone proprietary scripts (`.bzs`).
`bzsh.exe` `bzshp.exe`	Include the file in the BlueZone distribution image to include the BlueZone
`setup.ini`	The `InstallScriptPlayerOnly=` entry ... For users to be able to record, edit and play scripts, do nothing. To change to play only mode, edit the `setup.ini` file and change `InstallScriptPlayerOnly=No` to `InstallScriptPlayerOnly=Yes`. This causes only the `bzshp.exe` file to be installed.

BlueZone text-based scripting

BlueZone text-based scripting is controlled by the BlueZone Script Host (`bzsh.exe`) file and the BlueZone Script Host Player (`bzsh.exe`) file.

If the `bzsh.exe` file is included in the BlueZone distribution image, then end users are able to record, edit and play BlueZone text-based scripts (`.vbs`, `.js`, and so on).

If the `bzsh.exe` file is included but the `bzsh.exe` file is not included in the BlueZone distribution image, then end users are only able to play BlueZone text-based scripts (`.vbs`, `.js`, and so on).

If neither the `bzsh.exe` file nor the `bzsh.exe` files are included in the BlueZone distribution image, then end users are not able to record, edit or play BlueZone text-based scripts (`.vbs`, `.js`, and so on).

Note

By default, both the `bzsh.exe` and the `bzshp.exe` files are installed if you included the `bzsc.cab` file in the BlueZone distribution image.

Controlling script passwords

The BlueZone Script Recorder does not allow passwords (sometimes referred to as hidden fields or hidden text) to be captured and inserted into the script while the script is being recorded. This feature is referred to as the automatic password prompting feature.

Scripts that contain passwords can be shared with other users. The automatic password prompting feature prevents scripts from being recorded with actual passwords. Without this feature, a user can record a logon script and save it. Then this user can share the script with another user. If that user runs the logon script, they would be logging on with the original author's user name and password. You are depending on the author to be savvy enough to remove his or her password before sharing the script.

By default, the automatic password prompting feature is enabled. When a hidden field is encountered during the recording process, the password (or hidden text) is not actually stored as part of the script. Instead, the BlueZone Script Recorder automatically inserts an "Input Command" with the label "BlueZone Recorded Prompt" and the "hidden" attribute turned on. The password that was entered during the recording process is discarded.

The end result of using this feature is that when the script is run and a hidden field is encountered, the script prompts all users, including the author, for a password.

This is the same as manually inserting a "prompt for password" command into the script in lieu of the actual password.

Note

In BlueZone text-based scripts, the actual command that is inserted into the script is a little different, but the end result is the same.

Disabling the automatic password prompting feature

If you want to disable the automatic password prompting feature and allow BlueZone to capture and record passwords during the script recording process, you must add the `ScriptRecordHiddenText=` entry in the `setup.ini` file.

This is a global feature change that affects all types of BlueZone scripting regardless of the script format: proprietary or text-based.

To disable the automatic password prompting feature:

1. In the BlueZone distribution image, open the `BlueZone Desktop` folder.
2. Open the `setup.ini` file in a text editor.
3. Add the following entry at the bottom of the `[BZSetup]` section:

   ```
   ScriptRecordHiddenText=Yes
   ```

4. Save and close the file.

   Note

   Any changes made to the `setup.ini` file only take effect after `setup.exe` is run and BlueZone has gone through the installation process. Refer to Creating a distribution image, on page 77 and BlueZone installation, on page 21 for more information.

Refer to BZSetup section, on page 118 for more information on the editing the `setup.ini` file.

Chapter 11: OLE automation

Object Linking and Embedding (OLE) is a Microsoft Windows standard for communications between applications. BlueZone can be linked to Windows applications like Microsoft Word and Microsoft Excel that support OLE.

In addition, BlueZone Host Automation Object can be used as a language-independent programmatic interface to BlueZone.

Using OLE, it is possible to use link Word to BlueZone in support of a "mail merge" application where the names and addresses are stored on a Mainframe and the text of the form letters are stored and formatted in Word. You could link Word to BlueZone and "pull" the names and addresses into Word from the Mainframe through the OLE interface.

BlueZone Host automation object

The BlueZone Host Automation Object is a Component Object Model (COM) software component for 32-bit Windows platforms. BlueZone Host Automation Object is essentially a programmatic interface to BlueZone.

BlueZone Host Automation Object can be utilized by any COM container application like Visual Basic, Microsoft Excel, and Microsoft Word to enable communications between PCs running BlueZone Display emulation software products and IBM mainframe and iSeries systems as well as other ASCII hosts. With BlueZone Host Automation Object, applications can execute common tasks on various host systems, automate user input, obtain data from host systems, initiate file transfers, and more.

The BlueZone Host Automation Object is a language-independent software component. Programs written in Visual Basic, Pascal, C, C++, and so on can invoke the BlueZone Host Automation Object to communicate with the host system. In addition, the BlueZone Host Automation Object can be incorporated into many popular word processing, database and spreadsheet macros, and run by any ActiveX scripting engine, including the BlueZone Scripting Host.

The BlueZone Host Automation Object utilizes capabilities of the BlueZone File Mapping (Shared Memory), DDE (Dynamic Data Exchange), and HLLAPI (High-Level Language API) interfaces. In addition to the container's properties and methods, the BlueZone Host Automation Object adds objects, properties and methods that enable interaction with the BlueZone session and the host system.

Using OLE/DDE to link BlueZone to other applications

BlueZone supports OLE/DDE links to other applications, which can be used to automate copy and paste operations.

When enabled, BlueZone establishes a link with the other application. Possible uses include; automatically copying Customer information from a BlueZone emulation screen to a Microsoft Word document to perform mail merges or automatically copying data from a host screen through BlueZone, to a Microsoft Excel spreadsheet. Each time the host screen changes, the data are dynamically updated in the linked application.

1. Enable linking in BlueZone:
    a. From the BlueZone menu bar, click **Options** ® **API**.
    b. Select the **Enable DDE Server Interface** check box.

c. Set the **HLLAPI Short Name Session Identifier** to a unique value. The default is **A**. If links to multiple BlueZone sessions are required, then each session must have a unique identifier.

d. Select the **Auto-assign HLLAPI Names** check box to eliminate having to configure each session separately.

e. Select the desired data in your BlueZone emulation session to be sent to the linked application by selecting it and copying it to the Windows clipboard.

Tip

Once you have the area highlighted, right-click and select **Copy to Clipboard**.

2. Establish the link in the linked application:

a. Position the cursor in the document where the BlueZone data must appear.

b. From the linked application's menu, click **Edit** ® **Paste Special**.

c. In the Paste Special dialog, select the **Paste link** radio button and **Unformatted Text** from the **As** list.

d. Click **OK**. The link is now established. Each time the BlueZone screen changes, the data is automatically updated in the linked application.

Appendix A: Default setup.ini file

The `setup.ini` file is processed during installation. You can use the `setup.ini` file to make many customizations to your BlueZone installation.

The following sections detail the `setup.ini` file with the default settings. The items in blue type, are values used by BlueZone during installation. The items shown in black type, are comments and never need to be edited or changed. Lines preceded by a semicolon are commented out and are ignored by the BlueZone installation program.

The `setup.ini` file is shipped with BlueZone and is located in the `BlueZone Desktop` installation source directory.

To edit the `setup.ini` file, use a text editor. Change any values necessary and save the file. You must run the BlueZone installation program (`setup.exe`), in order for the changes to take affect.

When editing the `setup.ini` file, you may only need to change a value. In other cases you may have to uncomment out an item by deleting the semicolon from the beginning of the line.

Important

The sections after the `[Activation]` section contain installation parameters and are not documented. They are only intended for internal use; do not change them.

BZSetup section

In the `[BZSetup]` section, you can customize the BlueZone installation process. The following code displays the default values in the `[BZSetup]` section

```
[BZSetup]
;default SourceDir is drive and directory of SETUP.EXE
;SourceDir=A:\
;DestinationDir="C:\Program Files\BlueZone\6.1"
WorkingDirType=1
;0 - Custom, 1 - User's Personal Folder (My Documents), 2 - All Users Shared Document Folder
;3 - User's AppData Folder, 4 - All Users AppData Folder
;WorkingDir="C:\Program Files\BlueZone\6.1"
;CopyPrevWorkingDir=Yes
;fourteen digit registration key
RegistrationKey=
;SNA Server, Renex Async Protocol, TN3270E, Communications Server, IntranetWare for SAA
Connection=TN3270E
;see Administrator's Guide for Lock values
Lock=0
LockFTP=0
LockFTPSession=0
LockFTPConnection=0
LockFTPInitialCommands=0
LockFTPMiscellaneous=0
LockFTPSchedule=0
LockFTPFirewall=0
LockFTPSecurity=0
LockFTPCertificate=0
LockTelnet=0
LockDisplay=0
LockFont=No
ShowLockedDialogs=Yes
DisableAppendToClipboard=No
;0-HKEY_CURRENT_USER (Session Settings - Default), 1-HKEY_LOCAL_MACHINE (All Settings)
;2-HKEY_CURRENT_USER (All Settings)
BaseRegistry=0
ProfileMode=Yes
ProfileSharing=Yes
SetPath=No
EnablePowerKeys=No
FIPSMode=No
InstallScriptPlayerOnly=No
SessionManagerRunInTray=No
ScriptRecordHiddenText=No
```

Table 16: BZSetup entries

Entry	Description
SourceDir=	Source directory is only used when installing BlueZone from a floppy diskette. Note that the value of SourceDir must be where SETUP.EXE is located. Default value: ;SourceDir=A:\ (commented out)
DestinationDir=	Controls the installation location of the BlueZone program files. This feature is typically used in conjunction with the quiet mode installation. If you want to install BlueZone in a specific location, uncomment this item and edit the value with the custom location. Default value: ;DestinationDir="C:\Program Files\BlueZone\6.1" (commented out)

Table 16: BZSetup entries (continued)

Entry	Description
`WorkingDirType=`	Controls the location of the working directory folder. The working directory contains the BlueZone working files: certificate, configuration, macro, script, spool, trace, and transfer files. BlueZone working files are connected to a specific user. The available `WorkingDirType=` values are: ▪ 0 - Custom Folder ▪ 1 - User's Personal Folder (My Documents) ▪ 2 - All Users Shared Document Folder ▪ 3 - User's AppData Folder ▪ 4 - All Users AppData Folder If you set `WorkingDirType=0`, use the `WorkingDir=` entry to control the exact location of the working directory. Default value: `WorkingDirType=1`
`WorkingDir=`	Controls the custom location of the working directory. If you set `WorkingDirType=0`, uncomment this entry and define the custom working directory location. This feature is also typically used in conjunction with quiet mode installation. Default value: `;WorkingDir="C:\Program Files\BlueZone\6.1"` (commented out)
`CopyPrevWorkingDir=`	Copies the previous version's working directory to the newly installed version's working directory. This allows the user to continue to use the same user configuration profiles from a previous version. Default value: `;CopyPrevWorkingDir=Yes` (commented out)
`Connection=`	Sets the BlueZone preferred connection type. This is the connection that BlueZone uses as a default when an end user selects **Session** ® **Configure** from the BlueZone menu bar. Possible values: ▪ Microsoft SNA Server = `SNAServer` ▪ Renex Async Protocol = `RenexAsync` ▪ TN3270 / TN3270E = `TN3270E` ▪ IBM Communications Server = `CommServ` ▪ IntranetWare for SAA = `Intranetware` For example, if you are a Microsoft SNA Server shop and you want to install BlueZone using Microsoft SNA Server as the preferred connection type, set `Connection=SNAServer`. **Note:** Some BlueZone emulation clients only support one connection type. Therefore, the value of `Connection=` is ignored during installation of these clients. Default value: `Connection=TN3270E`

Table 16: BZSetup entries (continued)

Entry	Description
Lock=	Controls the locking of one or more BlueZone features. The possible values for the lock feature are provided in the BlueZone feature lock table. Refer to BlueZone feature locks, on page 155 for a table of lockable BlueZone features and their values, and BlueZone feature locking, on page 37 for more information. A zero value indicates that no BlueZone features are locked. Default value: Lock=0.
LockFTP=	Controls the locking of one or more BlueZone Secure FTP commands. The possible values for the LockFTP feature are provided in the BlueZone Secure FTP lock table. Refer to BlueZone Secure FTP command and feature locks, on page 155 for a table of lockable BlueZone functions and their values. Also refer to BlueZone feature locking, on page 37 for more information. A zero value indicates that no BlueZone FTP commands are locked. Default value: LockFTP=0
LockFTPSession= LockFTPConnection= LockFTPInitialCommands= LockFTPMiscellaneous= LockFTPSchedule= LockFTPFirewall= LockFTPSecurity= LockFTPCertificate=	Controls the locking of one or more BlueZone Secure FTP features. The possible values for the above items, are provided in the BlueZone Secure FTP feature lock table. Refer to BlueZone Secure FTP individual feature locks, on page 156 for the tables of lockable BlueZone features and their values. Also refer to BlueZone feature locking, on page 37 for more information. A zero value indicates that no BlueZone Secure FTP features are locked. Default values: LockFTPSession=0 LockFTPConnection=0 LockFTPInitialCommands=0 LockFTPMiscellaneous=0 LockFTPSchedule=0 LockFTPFirewall=0 LockFTPSecurity=0 LockFTPCertificate=0
LockTelnet=	Controls the locking of one or more of the BlueZone Telnet features. The possible values for the lock feature are provided in the Telnet feature lock table. Refer to Telnet feature locks, on page 158 for a table of lockable BlueZone Telnet features and their values. Also refer to BlueZone feature locking, on page 37 for more information. A zero value indicates that no Telnet features are locked. Default value: LockTelnet=0

Table 16: BZSetup entries (continued)

Entry	Description
LockDisplay=	Controls the locking of one or more of the BlueZone Display features. The possible values for the lock feature are provided in the Display feature lock table. Refer to Display feature locks, on page 158 for a table of lockable BlueZone Display features and their values. Also refer to BlueZone feature locking, on page 37 for more information. A zero value indicates that no Display features are locked. Default value: LockDisplay=0
LockFont=	Controls the locking of the currently configured font. Possible values are Yes to lock the currently configured font and No to allow users to be able to change the configured font. When this value is set to Yes, the Change button on the Font dialog is disabled. Default value: LockFont=No
ShowLockedDialogs=	Controls whether the BlueZone dialog is displayed if that particular feature is locked using the BlueZone feature locking feature. Normally, if you lock a particular BlueZone feature, your end users are still able to access the associated BlueZone configuration dialog for that feature. They can view it and make changes to the settings. They cannot however apply or save those changes. The OK button will be grayed out. However, if would prefer for your end user's to not be able to see the dialogs at all, you can turn them off by setting this value of ShowLockedDialogs= to No. An message box displays instead. Refer to Configuring the show locked dialogs feature, on page 40 for more information. Default value: ShowLockedDialogs=Yes
DisableAppendToClipboard=	Disables the BlueZone append to clipboard feature. If you do not want your users to be able to append data to their Windows clipboard, you can turn this feature off by setting this value to Yes. Default value: DisableAppendToClipboard=No
BaseRegistry=	Controls how BlueZone uses the Windows registry. Possible values are 0, 1 or 2. Refer to Base registry setting, on page 18 for more information. Default value: BaseRegistry=0
ProfileMode=	Controls whether BlueZone operates in profile mode or registry mode. Possible values are Yes to enable profile mode and No to enable registry mode. Default value: ProfileMode=Yes
ProfileSharing=	Controls whether a BlueZone profile (configuration file), can be used to start more than one BlueZone session. The default value is for profile sharing to be enabled. This means that end users can use a single BlueZone profile to open up multiple BlueZone sessions. If for any reason you don't want your end users to be able to start more than one BlueZone session for a profile, disable this feature by setting the value to No. Refer to Profile sharing feature, on page 34 for more information. Possible values are Yes to enable profile sharing and No to disable profile sharing. Default value: ProfileSharing=Yes

Table 16: BZSetup entries (continued)

Entry	Description
SetPath=	Controls the placing of the BlueZone installation directory into the Windows "PATH" during the BlueZone installation. This feature is especially helpful if you are using a third-party HLLAPI application in conjunction with BlueZone. Default value: SetPath=No
EnablePowerKeys=	Turns on the old power keys feature. Changing this value to Yes enables the old power keys feature and disables the new power pads feature. Refer to Enabling the power keys feature, on page 31 and Power pads, on page 66 for more information. Default value: EnablePowerKeys=No
FIPSMode=	Enables FIPS mode. Changing this value to Yes enables FIPS mode. Refer to Enabling FIPS mode support, on page 32 for more information. Default value: FIPSMode=No
InstallScriptPlayerOnly=	This setting is used in conjunction with the BlueZone Scripting CAB file (BZSC.CAB). The default setting allows end users to record and play scripts. Changing this value to Yes deploys only the BlueZone Script Player only (BZSHP.EXE) program. The BlueZone Scripting CAB contains both the BZSH.EXE and the BZSHP.EXE files. If the BlueZone scripting CAB is deployed with InstallScriptPlayerOnly= set to No, both files are deployed. When both files are present in the installation, end users can run and edit BlueZone scripts. By setting the value to Yes, only the BZSHP.EXE file is deployed. When only this file is present in the installation, end users can only run BlueZone scripts and not edit or record them. **Note:** The BZSC.CAB file must be part of the BlueZone distribution image in order for this setting to have any effect. Default value: InstallScriptPlayerOnly=No
SessionManagerRunInTray=	Controls whether or not the BlueZone Session Manager automatically displays in a user's Windows system tray. By default this value is set to No. Setting this value to Yes causes the BlueZone Session Manager to automatically run out of the Windows system tray whenever BlueZone Session Manager is launched. Default value: SessionManagerRunInTray=No
ScriptRecordHiddenText=	Controls the automatic password prompting feature. This entry is not included in the default setup.ini file and must be added manually. Refer to Controlling script passwords, on page 115 for more information on the automatic password prompting feature.

HLLAPI section

In the [HLLAPI] section, you can configure the HLLAPI options.

```
[HLLAPI]
ConnectRetryMilliseconds=0
TelnetHostSettleMilliseconds=0
```

Entry	Description
ConnectRetryMilliseconds=	Used by Whllapi.dll and Whlapi32.dll to control the default number of milliseconds to retry the BlueZone session connect when ConnectPresentationSpace is called.
TelnetHostSettleMilliseco-nds=	

Program Group section

In the [Program Group] section, you can configure the program group options and change the names associated with the program group icons.

```
[Program Group]
UseGroup=Yes
GroupName=BlueZone 6.1
CopyShortcuts2ProgramGroup=No
MainframeDisplayText=Mainframe Display
MainframePrinterText=Mainframe Printer
iSeriesDisplayText=iSeries Display
iSeriesPrinterText=iSeries Printer
VTText=BlueZone VT
SessionManagerText=BlueZone Session Manager
ScriptEditorText=BlueZone Script Editor
FTPText=BlueZone FTP
HllapiRedirectorText=BlueZone HLLAPI Redirector
ScriptingHostText=BlueZone Scripting Host
TCP/IPPrintServerText=BlueZone TCP-IP Print Server
ICLDisplayText=ICL Display
UTSDisplayText=UTS Display
T27DisplayText=T27 Display
```

Entry	Description
UseGroup=	Controls the creation of a BlueZone program group in the Windows startup folder. Default value: UseGroup=Yes
GroupName=	Changes the name assigned to the BlueZone program group in Windows. Prerequisites: Set UseGroup=Yes. Default value: GroupName=BlueZone 6.1
CopyShortcuts2ProgramGroup=	Changing this value to Yes causes any BlueZone session desktop shortcuts (.LNK) files that are present in the BlueZone distribution image to be automatically added to the BlueZone Program Group during the installation process. These shortcuts are automatically copied to the user's desktop as well. Refer to Creating BlueZone desktop shortcuts, on page 50 for more information. **Important:** Do not confuse this feature with the [Desktop Shortcuts] feature which is located lower down in the setup.ini file. The [Desktop Shortcuts] feature allows you to create a BlueZone desktop shortcut that launches a non-configured BlueZone session. When a non-configured BlueZone Session is launched, the Windows common file dialog automatically displays, allowing the end user to choose a BlueZone profile (configuration file) to use. Default value: CopyShortcuts2ProgramGroup=No

Desktop Shortcuts section

In the [Desktop Shortcuts] section, you can configure the shortcuts that are created on the desktop. The shortcut names are the values configured in the [Program Group] section.

```
[Desktop Shortcuts]
MainframeDisplay=No
MainframePrinter=No
iSeriesDisplay=No
iSeriesPrinter=No
VT=No
SessionManager=Yes
ScriptEditor=No
FTP=No
ScriptingHost=No
SessionManagerInStartupFolder=No
TCP/IPPrintServerer=Yes
UTSDisplay=No
T27Display=No
ICLDisplay=No
```

SessionManagerInStartupFolder=

This setting is used to control whether or not the BlueZone Session Manager is added to the end user's Windows startup folder.

Changing this setting to `Yes` causes the BlueZone Session Manager to be added to the end user's Windows startup folder, which causes the Session Manager to launch whenever the machine is started.

Default value: `SessionManagerInStartupFolder=No`

WinJa and JWalk sections

In the `[WinJa]` and `[JWalk]` sections, you can configure the values associated with these products.

```
[WinJa]
;Version=2.2C9
;CabFile=WinJa.Cab
;DestDir=C:\Program Files\SEAGULL\WinJa Windows Client-Version 2.2C9

[JWalk]
;Version=
;CabFile=
;DestDir=
```

Note

In this example, only the WinJa section contains information. If you want to use BlueZone with JWalk, you would have to fill in the appropriate information in the JWalk section. Refer to your WinJa and JWalk documentation for more information about using BlueZone with WinJa and JWalk.

Support section

In the `[Support]` section, you can customize the message in the **Help ® Technical Support** window.

You can add your company's help information here (such as phone number or website) so your users see a custom message.

```
[Support]
Line1=
Line2=To contact Technical Support, go to:
Line3=http://www.rocketsoftware.com/support and submit your issue online.
Line4=
Line5=Note to BlueZone Administrators:
Line6=
Line7=Information displayed in this window can be preconfigured by editing
Line8=
Line9=the setup.ini file before installation.
```

About section

In the `[About]` section, you can customize the **Help ® About** window.

It is recommended to not change this section because important BlueZone contact information is displayed in the About window. Enter customized information in the `[Support]` section.

```
[About]
Info1=Discover more about genuine BlueZone business solutions
Info2=by visiting http://bluezone.rocketsoftware.com
Name=Rocket Software, Inc.
Address1=275 Grove Street
Address2=Suite 3-410
Address3=Newton, MA 02466-2272
Phone=
Fax=
INet=bluezone.rocketsoftware.com
```

Activation section

The `[Activation]` section is reserved for future use.

```
[Activation]
Address=
Email=
```

Important

The sections after the `[Activation]` section contain installation parameters and are not documented. They are only intended for internal use; do not change them.

Appendix B: Default global.ini file

You can customize the following BlueZone features in the `global.ini` file:

- Backup working directory feature
- Main menu bar appearance
- HLLAPI auto-launch feature
- LU name mapping feature
- VT Display font size
- FTP command timeout values

The `global.ini` file is shipped with BlueZone and is located in the `BlueZone Desktop` installation source directory.

When a BlueZone session is started, BlueZone checks the `global.ini` file; the contents are read and the BlueZone application desktop is changed accordingly.

Note

When you include a `global.ini` file as part of your BlueZone distribution image, the BlueZone installation wizard automatically places the `global.ini` file in the user's BlueZone installation directory.

Refer to the following topics for more information on each section of the `global.ini` file. The blue text are values you can configure to match your requirements and the text in black are comments; do not edit this text.

When editing the `global.ini` file, you may only need to change a value. In other cases you may have to uncomment out an item by deleting the semicolon from the beginning of the line. Lines starting with a semicolon are commented out and are ignored by the BlueZone installation program.

Menu section

In the `[Menu]` section, you can customize the appearance of the main menu bar. You can hide the entire menu, select menus, and/or the right-click menu.

```
[Menu]
; Used to display or hide BlueZone MenuBar items
HideMenuAll=No
HideMenuMain=No
HideMenuPopup=No
HideMenuFile=No
HideMenuEdit=No
HideMenuSession=No
HideMenuOptions=No
HideMenuTransfer=No
HideMenuView=No
;HideMenuMacro=Yes
HideMenuScript=No
HideMenuHelp=No
```

`HideMenuAll=`

Hides the entire menu bar and the right-click pop-up menu.

Default value: `HideMenuAll=No`

HideMenuMain=
Hides the entire menu bar.

Default value: `HideMenuMain=No`

HideMenuPopup=
Hides the right-click pop-up menu only.

Default value: `HideMenuPopup=No`

HideMenu *Name*=
If set to `Yes`, the corresponding menu is hidden.

Default values:

```
HideMenuFile=No
HideMenuEdit=No
HideMenuSession=No
HideMenuOptions=No
HideMenuTransfer=No
HideMenuView=No
;HideMenuMacro=Yes
HideMenuScript=No
HideMenuHelp=No
```

Refer to Customizing the main menu bar, on page 28 for more information.

HLLAPI section

In the `[HLLAPI]` section, you can enable the HLLAPI auto-launch feature.

```
[HLLAPI]
;SessionA=
```

SessionA=
Defines the profile you want to automatically launch. To enable the auto-launch feature, delete the semicolon and type the desired profile file name.

Default value: `;SessionA=` (commented out)

Refer to Enabling HLLAPI auto-launch, on page 74 for more information.

LuMap section

In the `[LuMap]` section, you can enable the LU name mapping feature.

```
[LuMap]
;xD_Sy_Lu="LuName"
```

Where *x* is:

- `M` for Mainframe
- `A` for AS/400

y is the session ID: 1, 2, 3,and so on

LuName is the desired LU name to map

Default value: ;*x*D_S*y*_Lu="*LuName*" (commented out)

Refer to Enabling LU name mapping feature, on page 36 for more information.

VT section

In the [VT] section, you can set the font size in BlueZone VT.

```
[VT]
; Used to set the size of the font that BlueZone VT will use
;FontSize80=13
;FontSize132=-1
```

FontSize80=
Sets the 80 column font size. To enable this feature, delete the semicolon and type a font size.

A value of -1 forces auto-size font on.

Default value: ;FontSize80=13 (commented out)

FontSize132=
Sets the 132 column font size. To enable this feature, delete the semicolon and type a font size.

A value of -1 forces auto-size font on.

Default value: ;FontSize132=-1 (commented out)

FTP section

In the [FTP] section, you can control the time out value of FTP commands.

```
[FTP]
;Command Timeout=value
```

Command Timeout=
Sets the FTP command time out, in seconds.

A value of 0 disables the time out.

If this option is not enabled, a value of 30 is used.

Default value: ;Command Timeout=value (commented out)

BlueZone section

In the [BlueZone] section, you can configure the backup working directory folder and set the time it takes for the BlueZone session to automatically disconnect. You can also hide specific configuration dialog buttons.

```
[BlueZone]
;BackupWorkingDir=PathOfBackupWorkingDirectory
;KeyboardInactivityTimer=NumberOfMinutes
AppendVersionToWorkingDir=No
AllowCrossVersionInterop=Yes
;HideDialogButtons=
```

BackupWorkingDir=

Sets the path to the back up working directory. This entry is commented out by default. You must delete the semicolon to enable this feature.

You can add a custom backup folder where BlueZone saves a backup copy of the working directory. If the backup working directory is configured, every time BlueZone writes to a file (creates or saves a profile, script, macro, VBA project, power pad file, dialog file, and so on), the file is also copied to the backup working directory.

If the primary working directory is unavailable, BlueZone automatically switches to the backup working directory.

You can also include environment variables in the path between angle brackets or percent characters. For example:

```
BackupWorkingDir=%USERPROFILE%\BlueZone
```

KeyboardInactivityTimer=

Sets the time that the BlueZone session automatically disconnects when the value is met. The value is time in minutes. This entry is commented out by default. You must delete the semicolon to enable this feature.

For example, if the following is set, after 20 minutes of inactivity, the BlueZone session will automatically disconnect:

```
KeyboardInactivityTimer=20
```

AppendVersionToWorkingDir=

Defines the working directory path name when you upgrade.

When set to `AppendVersionToWorkingDir=No`, the default value, no version number will be appended to the working directory path when BlueZone is upgraded. All of the user's previously created certificate, configuration, log, macro, script, spool, trace, and transfer files will be available to the newly installed version.

It is recommended that end users keep the default value of `No` so the files will be immediately available after an upgrade.

When set to `AppendVersionToWorkingDir=Yes`, the major version number is appended to the working directory.

Configuring this setting to `Yes` is useful for administrators who must run multiple version of BlueZone Web-to-Host or want to test a new version before going live.

If an end user configures this setting to `Yes`, the previously created certificate, configuration, log, macro, script, spool, traces, and transfer files are kept separate from the newly installed version. To continue to use these files, the user must copy the files to the new directory structure.

AllowCrossVersionInterop=

Controls whether different versions of BlueZone can communicate and interact with each other.

When set to `AllowCrossVersionInterop=Yes`, the default value, older versions of BlueZone can communicate with newer versions. For example, if you have versions 5.1 and 6.1 installed, version 5.1 will communicate with version 6.1.

This setting effects functionality such as **File ® Close All**, **View ® Jump Screen**, ActiveX events, and whether the host automation objects and HLLAPI DLLs can connect to a different version of BlueZone.

To specify a specific version, refer to "Multiple side-by-side versions of BlueZone" in the *BlueZone Advanced Automation Developer's Guide*. If no version is specified, the latest registered version of the BlueZone Host Automation Object is used.

When set to `AllowCrossVersionInterop=No`, different versions of BlueZone do not communicate.

HideDialogButtons=

Hides configuration dialog buttons. This entry is commented out by default. You must delete the semicolon to enable this feature.

The available buttons and their values are:

- Default button = 1
- Open button = 2
- Save As button = 8
- Help button = 16

To hide a single button, type the value. For example, to hide the Open button, type `HideDialogButtons=2`.

To hide multiple buttons, add the values together and type the sum. For example, to hide the Open and Save As buttons, type `HideDialogButtons=10`.

Help section

In the `[Help]` section, you can change from the locally installed `.chm` to Web-based help.

```
[Help]
UseWebHelp=No
WebHelpUrl=http://www.bluezonesoftware.com/help/v61
```

UseWebHelp=

Sets the help system type: `.chm` file or Web-based HTML help.

The default value is `UseWebHelp=No` which instructs BlueZone Desktop to use the locally installed `.chm` file.

`UseWebHelp=Yes` instructs BlueZone Desktop to use the Web-based HTML help. You must run `setup.exe` for this change to take affect.

WebHelpUrl

Displays the URL to the currently installed version's web help.

Appendix C: Default language.ini file

You can use the `language.ini` file to change the language of the BlueZone Display and Printer dialogs and menus. You can also configure the bidirectional language options for Arabic.

The `language.ini` file is located in the `BlueZone Desktop` installation source directory.

Language section

In `[Language]` section, you can change the default language of the dialogs and menus in BlueZone.

For the complete steps on changing the BlueZone language, refer to Changing the language in BlueZone, on page 65.

The following is the default `[Language]` section:

```
[Language]
;Language=English
```

Language=

Defines the language that BlueZone uses in the Display and Printer menus and dialogs. To change this value, delete the semicolon and modify the language value. The valid language values are:

- `Dutch`
- `English`
- `French`
- `German`
- `Japanese`

For example:

```
[Language]
Language=French
```

Bidi Options section

In the `[Bidi Options]` section, you can control the initial reverse text entry, auto push mode, numeric swapping, parentheses and bracket swapping, and the default Windows Arabic font. These settings are only applied if you use Arabic.

The following is the default `[Bidi Options]` section:

```
[Bidi Options]
ReverseTextEntry=Yes
AutoPushMode=Yes
NumericSwapping=Yes
SymmetricSwapping=Yes
DisplayInUnicode=Yes
```

ReverseTextEntry=

Reverses the direction of the text. The valid values are:

`ReverseTextEntry=Yes` (default)

`ReverseTextEntry=No`

AutoPushMode=
Enables auto push mode. The valid values are:

`AutoPushMode=Yes` (default)

`AutoPushMode=No`

NumericSwapping=
Controls if Latin digits are swapped for Hindi digits when the screen is reversed. The valid values are:

`NumericSwapping=Yes` (default)

`NumericSwapping=No`

SymmetricSwapping=
Controls if open parentheses and angle brackets are swapped for close parentheses and angle brackets and vice versa when the screen is reversed. The valid values are:

`SymmetricSwapping=Yes` (default)

`SymmetricSwapping=No`

DisplayInUnicode=
Enables BlueZone to use standard Windows Arabic fonts (fixed pitch only) for display and printing. Windows Arabic fonts scale better than the provided bitmap fonts BlueZone Arabic Terminal and Farabi Print 3. The valid values are:

`DisplayInUnicode=Yes` (default)

`DisplayInUnicode=No`

Appendix D: iSeries configuration example

The following device description is a virtual printer device necessary to connect the BlueZone Telnet 5250E Printer emulator. This is provided for reference purposes only. Device descriptions can vary from system to system.

```
Display Device Description                      Page     1

5769SS1 V4R2M0  980228                           Sys20  04/01/99  13:34:37

 Device description . . . . . :   DEVD        RNXPRT0001

 Option . . . . . :   OPTION      *ALL

 Category of device . . . . . :               *PRT

 Device class . . . . . :   DEVCLS      *VRT

 Device type  . . . . . :   TYPE        3812

 Device model . . . . . :   MODEL       1

 Advanced function printing . . . . :   AFP         *NO

 Online at IPL  . . . . . :   ONLINE      *NO

 Attached controller  . . . . . :   CTL         QVIRCD0001

 Font . . . . . :   FONT

   Identifier . . . . . :               010

   Point size . . . . . :               *NONE

 Separator drawer . . . . . :   SEPDRAWER   *FILE

 Separator program  . . . . . :   SEPPGM      *NONE

   Library  . . . . . :

 Printer error message  . . . . . :   PRTERRMSG   *INFO

 Message queue  . . . . . :   MSGQ        QSYSOPR

   Library  . . . . . :                 *LIBL

 Host print transform . . . . . :   TRANSFORM   *YES

 Manufacturer type and model  . . . :   MFRTYPMDL   *HP4

 Paper source 1 . . . . . :   PPRSRC1     *LETTER

 Paper source 2 . . . . . :   PPRSRC2     *NONE

 Envelope source  . . . . . :   ENVELOPE    *NONE

 ASCII code page 899 support  . . . :   ASCII899    *NO

 Image configuration  . . . . . :   IMGCFG      *NONE
```

```
Character identifier . . . . . :   CHRID       *SYSVAL

Workstation customizing object . . :   WSCST       *NONE

User-defined object  . . . . . :   USRDFNOBJ   *NONE

  Object type  . . . . . :              *NONE

Data transform program . . . . . :   USRDTATFM   *NONE

User-defined driver program  . . . :   USRDRVPGM   *NONE

Dependent location name  . . . . . :   DEPLOCNAME  *NONE

Allocated to:

Job name . . . . . :              *NONE

  User . . . . . :

  Number . . . . . :

Text . . . . . :   TEXT        prt01 test printer

User-defined options . . . . . :   USRDFNOPT

-----------------User-defined options------------------
```

Appendix E: Character sets

ASCII character set

Table 17: ASCII Device control codes

CTRL	DEC	HEX	CHAR	DESC
Ctrl-@	0	00	NUL	Null Prompt
Ctrl-A	1	01	SOH	Start of Header
Ctrl-B	2	02	STX	Start of Text
Ctrl-C	3	03	ETX	End of Text
Ctrl-D	4	04	EOT	End of Transmit
Ctrl-E	5	05	ENQ	Enquiry
Ctrl-F	6	06	ACK	Acknowledge
Ctrl-G	7	07	BEL	Audible Bell (Beep)
Ctrl-H	8	08	BS	Backspace
Ctrl-I	9	09	HT	Horizontal Tab
Ctrl-J	10	0A	LF	Line Feed
Ctrl-K	11	0B	VT	Vertical Tab
Ctrl-L	12	0C	FF	Form Feed
Ctrl-M	13	0D	CR	Carriage Return
Ctrl-N	14	0E	SO	Shift Out
Ctrl-O	15	0F	SI	Shift In
Ctrl-P	16	10	DLE	Data Link Escape
Ctrl-Q	17	11	DC1	Device Control1 (X-ON)
Ctrl-R	18	12	DC2	Device Control2
Ctrl-S	19	13	DC3	Device Control3 (X-OFF)
Ctrl-T	20	14	DC4	Device Control4
Ctrl-U	21	15	NAK	Negative Acknowledgement
Ctrl-V	22	16	SYN	Synchronous Idle
Ctrl-W	23	17	ETB	End Transmission Block
Ctrl-X	24	18	CAN	Cancel
Ctrl-Y	25	19	EM	End of Medium
Ctrl-Z	26	1A	SUB	Substitution
Ctrl-[	27	1B	ESC	Escape
Ctrl-\	28	1C	FS	File Separator (Right Arrow)

Table 17: ASCII Device control codes (continued)

CTRL	DEC	HEX	CHAR	DESC
Ctrl-]	29	1D	GS	Group Separator (Left Arrow)
Ctrl-^	30	1E	RS	Record Separator (Up Arrow)
Ctrl-_	31	1F	US	Unit Separator (Down Arrow)

Table 18: ASCII character set

DEC	HEX	CHAR	DESC
32	20	<SP>	Space
33	21	!	Exclamation Point
34	22	"	Double Quote
35	23	#	Number Sign
36	24	$	Dollar Sign
37	25	%	Percent Sign
38	26	&	Ampersand
39	27	'	Single Quote
40	28	(	Left Parenthesis
41	29	)	Right Parenthesis
42	2A	*	Asterisk
43	2B	+	Plus Sign (Addition)
44	2C	,	Comma
45	2D	-	Hyphen (Minus Sign)
46	2E	.	Period (Dot)
47	2F	/	Forward Slash (Divide)
48	30	0	
49	31	1	
50	32	2	
51	33	3	
52	34	4	
53	35	5	
54	36	6	
55	37	7	
56	38	8	
57	39	9	
58	3A	:	Colon
59	3B	;	semicolon
60	3C	<	Less-than Sign

Table 18: ASCII character set (continued)

DEC	HEX	CHAR	DESC
61	3D	=	Equals Sign
62	3E	>	Greater-than Sign
63	3F	?	Question Mark
64	40	@	At Sign
65	41	A	
66	42	B	
67	43	C	
68	44	D	
69	45	E	
70	46	F	
71	47	G	
72	48	H	
73	49	I	
74	4A	J	
75	4B	K	
76	4C	L	
77	4D	M	
78	4E	N	
79	4F	O	
80	50	P	
81	51	Q	
82	52	R	
83	53	S	
84	54	T	
85	55	U	
86	56	V	
87	57	W	
88	58	X	
89	59	Y	
90	5A	Z	
91	5B	[	Left Square Bracket
92	5C	\	Back Slash
93	5D	]	Right Square Bracket
94	5E	^	Caret (Circumflex)
95	5F	_	Underscore
96	60	`	Grave Accent
97	61	a	

Table 18: ASCII character set (continued)

DEC	HEX	CHAR	DESC
98	62	b	
99	63	c	
100	64	d	
101	65	e	
102	66	f	
103	67	g	
104	68	h	
105	69	i	
106	6A	j	
107	6B	k	
108	6C	l	
109	6D	m	
110	6E	n	
111	6F	o	
112	70	p	
113	71	q	
114	72	r	
115	73	s	
116	74	t	
117	75	u	
118	76	v	
119	77	w	
120	78	x	
121	79	y	
122	7A	z	
123	7B	{	Left Curly Brace
124	7C	|	Vertical Bar
125	7D	}	Right Curly Brace
126	7E	~	Tilde (Equivalency Sign)
127	7F	DEL	Delete

Table 19: Extended ASCII character set

DEC	HEX	CHAR	DESC
128	80	Ç	Latin capital letter C with cedilla
129	81	ü	Latin small letter u with diaeresis
130	82	é	Latin small letter e with acute

Table 19: Extended ASCII character set (continued)

DEC	HEX	CHAR	DESC
131	83	â	Latin small letter a with circumflex
132	84	ä	Latin small letter a with diaeresis
133	85	à	Latin small letter a with grave
134	86	å	Latin small letter a with ring above
135	87	ç	Latin small letter c with cedilla
136	88	ê	Latin small letter e with circumflex
137	89	ë	Latin small letter e with diaeresis
138	8A	è	Latin small letter e with grave
139	8B	ï	Latin small letter i with diaeresis
140	8C	î	Latin small letter i with circumflex
141	8D	ì	Latin small letter i with grave
142	8E	Ä	Latin capital letter A with diaeresis
143	8F	Å	Latin capital letter A with ring above
144	90	É	Latin capital letter E with acute
145	91	æ	Latin small letter ae
146	92	Æ	Latin capital letter AE
147	93	ô	Latin small letter o with circumflex
148	94	ö	Latin small letter o with diaeresis
149	95	ò	Latin small letter o with grave
150	96	û	Latin small letter u with circumflex
151	97	ù	Latin small letter u with grave
152	98	ÿ	Latin small letter y with diaeresis
153	99	Ö	Latin capital letter O with diaeresis

Table 19: Extended ASCII character set (continued)

DEC	HEX	CHAR	DESC
154	9A	Ü	Latin capital letter U with diaeresis
155	9B	¢	Cent Sign
156	9C	£	Pound Sign
157	9D	¥	Yen Sign
158	9E	ž	
159	9F	ƒ	Latin small letter f with hook
160	A0		Non-Breaking Space
161	A1	¡	Inverted Exclamation Mark
162	A2	¢	Cent Sign
163	A3	£	Pound Sign
164	A4	¤	Currency Sign
165	A5	¥	Yen Sign
166	A6	¦	Pipe, Broken Vertical Bar
167	A7	§	Section Sign
168	A8	¨	Diaeresis (Umlaut)
169	A9	©	Copyright Sign
170	AA	ª	Feminine Ordinal Indicator
171	AB	«	Left Double Angle Quotes
172	AC	¬	Logical Not Sign
173	AD		Soft Hyphen
174	AE	®	Registered Trade Mark Sign
175	AF	¯	Spacing Macron - Overline
176	B0	°	Degree Sign
177	B1	±	Plus-or-minus Sign
178	B2	²	Superscript Two, Squared
179	B3	³	Superscript Three, Cubed
180	B4	´	Acute Accent - Spacing Acute
181	B5	µ	Micro Sign
182	B6	¶	Pilcrow Sign - Paragraph Sign
183	B7	·	Middle Dot - Georgian Comma
184	B8	¸	Spacing Cedilla
185	B9	¹	Superscript, One
186	BA	º	Masculine Ordinal Indicator

Table 19: Extended ASCII character set (continued)

DEC	HEX	CHAR	DESC
187	BB	»	Right Double Angle Quotes
188	BC	¼	Fraction, One Quarter
189	BD	½	Fraction, One Half
190	BE	¾	Fraction, Three Quarters
191	BF	¿	Inverted Question Mark
192	C0	À	Latin Capital Letter A with Grave
193	C1	Á	Latin Capital Letter A with Acute
194	C2	Â	Latin Capital Letter A with Circumflex
195	C3	Ã	Latin Capital Letter A with Tilde
196	C4	Ä	Latin Capital Letter A with Diaeresis
197	C5	Å	Latin Capital Letter A with Ring Above
198	C6	Æ	Latin Capital Letter AE
199	C7	Ç	Latin Capital Letter C with Cedilla
200	C8	È	Latin Capital Letter E with Grave
201	C9	É	Latin Capital Letter E with Acute
202	CA	Ê	Latin Capital Letter E with Circumflex
203	CB	Ë	Latin Capital Letter E with Diaeresis
204	CC	Ì	Latin Capital Letter I with Grave
205	CD	Í	Latin Capital Letter I with Acute
206	CE	Î	Latin Capital Letter I with Circumflex
207	CF	Ï	Latin Capital Letter I with Diaeresis
208	D0	Ð	Latin Capital Letter ETH
209	D1	Ñ	Latin Capital Letter N with Tilde
210	D2	Ò	Latin Capital Letter O with Grave
211	D3	Ó	Latin Capital Letter O with Acute

Table 19: Extended ASCII character set (continued)

DEC	HEX	CHAR	DESC
212	D4	Ô	Latin Capital Letter O with Circumflex
213	D5	Õ	Latin Capital Letter O with Tilde
214	D6	Ö	Latin Capital Letter O with Diaeresis
215	D7	×	Multiplication Sign
216	D8	Ø	Latin Capital Letter O with Slash
217	D9	Ù	Latin Capital Letter U with Grave
218	DA	Ú	Latin Capital Letter U with Acute
219	DB	Û	Latin Capital Letter U with Circumflex
220	DC	Ü	Latin Capital Letter U with Diaeresis
221	DD	Ý	Latin Capital Letter Y with Acute
222	DE	Þ	Latin Capital Letter THORN
223	DF	ß	Latin Small Letter Sharp S - Ess-zed
224	E0	à	Latin Small Letter a with Grave
225	E1	á	Latin Small Letter a with Acute
226	E2	â	Latin Small Letter a with Circumflex
227	E3	ã	Latin Small Letter a with Tilde
228	E4	ä	Latin Small Letter a with Diaeresis
229	E5	å	Latin Small Letter a with Ring Above
230	E6	æ	Latin Small Letter ae
231	E7	ç	Latin Small Letter c with Cedilla
232	E8	è	Latin Small Letter e with Grave
233	E9	é	Latin Small Letter e with Acute
234	EA	ê	Latin Small Letter e with Circumflex

Table 19: Extended ASCII character set (continued)

DEC	HEX	CHAR	DESC
235	EB	ë	Latin Small Letter e with Diaeresis
236	EC	ì	Latin Small Letter i with Grave
237	ED	í	Latin Small Letter i with Acute
238	EE	î	Latin Small Letter i with Circumflex
239	EF	ï	Latin Small Letter i with Diaeresis
240	F0	ð	Latin Small Letter eth
241	F1	ñ	Latin Small Letter n with Tilde
242	F2	ò	Latin Small Letter o with Grave
243	F3	ó	Latin Small Letter o with Acute
244	F4	ô	Latin Small Letter o with Circumflex
245	F5	õ	Latin Small Letter o with Tilde
246	F6	ö	Latin Small Letter o with Diaeresis
247	F7	÷	Division sign
248	F8	ø	Latin Small Letter o with Slash
249	F9	ù	Latin Small Letter u with Grave
250	FA	ú	Latin Small Letter u with Acute
251	FB	û	Latin Small Letter u with Circumflex
252	FC	ü	Latin Small Letter u with Diaeresis
253	FD	ý	Latin Small Letter y with Acute
254	FE	þ	Latin Small Letter Thorn
255	FF	ÿ	Latin Small Letter y with Diaeresis

EBCDIC character set

Table 20: EBCDIC character set

CTRL	DEC	HEX	EBCDIC	DESC
Ctrl-@	0	00	NUL	Null
Ctrl-A	1	01	SOH	Start of Heading
Ctrl-B	2	02	STX	Start of Text
Ctrl-C	3	03	ETX	End of Text
Ctrl-D	4	04	SEL/PF	Select / Punch Off
Ctrl-E	5	05	HT	Horizontal Tab
Ctrl-F	6	06	RNL	Required New-line
Ctrl-G	7	07	DEL	Delete
Ctrl-H	8	08	GE	Graphic Escape
Ctrl-I	9	09	SPS	Superscript
Ctrl-J	10	0A	RPT	Repeat
Ctrl-K	11	0B	VT	Vertical Tab
Ctrl-L	12	0C	FF	Form Feed
Ctrl-M	13	0D	CR	Carriage Return
Ctrl-N	14	0E	SO	Shift Out
Ctrl-O	15	0F	SI	Shift In
Ctrl-P	16	10	DLE	Data Link Escape
Ctrl-Q	17	11	DC1	Device Control 1
Ctrl-R	18	12	DC2	Device Control 2
Ctrl-S	19	13	TM	Tape Mark
Ctrl-T	20	14	RES/ENP	Restore / Enable Presentation
Ctrl-U	21	15	NL	New-line
Ctrl-V	22	16	BS	Backspace
Ctrl-W	23	17	POC	Program-Operator Communications
Ctrl-X	24	18	CAN	Cancel
Ctrl-Y	25	19	EM	End of Medium
Ctrl-Z	26	1A	UBS	Unit Backspace
Ctrl-[	27	1B	CU1	Customer Use 1
Ctrl-\	28	1C	IFS	Interchange File Separator
Ctrl-]	29	1D	IGS	Interchange Group Separator
Ctrl-^	30	1E	IRS	Interchange Record Separator
Ctrl-_	31	1F	IUS/ITB	Interchange Unit Separator /
	32	20	DS	Digit Select

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	33	21	SOS	Start of Significance
	34	22	FS	Field Separator
	35	23	WUS	Word Underscore
	36	24	BYP/INP	Bypass/Inhibit Presentation
	37	25	LF	Line Feed
	38	26	ETB	End of Transmission Block
	39	27	ESC	Escape
	40	28	SA	Set Attribute
	41	29		
	42	2A	SM/SW	Set Model Switch
	43	2B	CSP	Control Sequence Prefix
	44	2C	MFA	Modify Field Attribute
	45	2D	ENQ	Enquiry
	46	2E	ACK	Acknowledge
	47	2F	BEL	Bell
	48	30		
	49	31		
	50	32	SYN	Synchronous Idle
	51	33	IR	Index Return
	52	34	PP/PN	Presentation Position / Punch On
	53	35	TRN	
	54	36	NBS	Numeric Backspace
	55	37	EOT	End of Transmission
	56	38	SBS	Subscript
	57	39	IT	Indent Tab
	58	3A	RFF	Required Form Feed
	59	3B	CU3	Customer Use 3
	60	3C	DC4	Device Control 4
	61	3D	NAK	Negative Acknowledge
	62	3E		
	63	3F	SUB	Substitute
	64	40	SP	Space
	65	41		
	66	42		
	67	43		
	68	44		
	69	45		

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	70	46		
	71	47		
	72	48		
	73	49		
	74	4A	¢	Cent Sign
	75	4B	.	Period (Decimal Point)
	76	4C	<	Less-than Sign
	77	4D	(	Left Parenthesis
	78	4E	+	Plus Sign
	79	4F	|	Logical OR
	80	50	&	Ampersand
	81	51		
	82	52		
	83	53		
	84	54		
	85	55		
	86	56		
	87	57		
	88	58		
	89	59		
	90	5A	!	Exclamation Point
	91	5B	$	Dollar Sign
	92	5C	*	Asterisk
	93	5D	)	Right Parenthesis
	94	5E	;	Semicolon
	95	5F	¬	Logical NOT
	96	60	-	Subtraction Sign
	97	61	/	Forward Slash (Virgule)
	98	62		
	99	63		
	100	64		
	101	65		
	102	66		
	103	67		
	104	68		
	105	69		
	106	6A	¦	Pipe, Broken Vertical Bar
	107	6B	,	Comma

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	108	6C	%	Percent Sign
	109	6D	_	Underscore
	110	6E	>	Greater-than Sign
	111	6F	?	Question Mark
	112	70		
	113	71		
	114	72		
	115	73		
	116	74		
	117	75		
	118	76		
	119	77		
	120	78		
	121	79	`	Grave Accent
	122	7A	:	Colon
	123	7B	#	Number Sign
	124	7C	@	At Sign
	125	7D	'	Apostrophe
	126	7E	=	Equal Sign
	127	7F	"	Straight Double Quotation Mark
	128	80		
	129	81	a	
	130	82	b	
	131	83	c	
	132	84	d	
	133	85	e	
	134	86	f	
	135	87	g	
	136	88	h	
	137	89	I	
	138	8A		
	139	8B		
	140	8C		
	141	8D		
	142	8E		
	143	8F		
	144	90		

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	145	91	j	
	146	92	k	
	147	93	l	
	148	94	m	
	149	95	n	
	150	96	o	
	151	97	p	
	152	98	q	
	153	99	r	
	154	9A		
	155	9B		
	156	9C		
	157	9D		
	158	9E		
	159	9F		
	160	A0		
	161	A1	~	Tilde (Equivalency Sign)
	162	A2	s	
	163	A3	t	
	164	A4	u	
	165	A5	v	
	166	A6	w	
	167	A7	x	
	168	A8	y	
	169	A9	z	
	170	AA		
	171	AB		
	172	AC		
	173	AD		
	174	AE		
	175	AF		
	176	B0		
	177	B1		
	178	B2		
	179	B3		
	180	B4		
	181	B5		
	182	B6		

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	183	B7		
	184	B8		
	185	B9		
	186	BA		
	187	BB		
	188	BC		
	189	BD		
	190	BE		
	191	BF		
	192	C0	{	Left Curly Brace
	193	C1	A	
	194	C2	B	
	195	C3	C	
	196	C4	D	
	197	C5	E	
	198	C6	F	
	199	C7	G	
	200	C8	H	
	201	C9	I	
	202	CA		
	203	CB		
	204	CC		
	205	CD		
	206	CE		
	207	CF		
	208	D0	}	Right Curly Brace
	209	D1	J	
	210	D2	K	
	211	D3	L	
	212	D4	M	
	213	D5	N	
	214	D6	O	
	215	D7	P	
	216	D8	Q	
	217	D9	R	
	218	DA		
	219	DB		
	220	DC		

Table 20: EBCDIC character set (continued)

CTRL	DEC	HEX	EBCDIC	DESC
	221	DD		
	222	DE		
	223	DF		
	224	E0	\	Back Slash
	225	E1		
	226	E2	S	
	227	E3	T	
	228	E4	U	
	229	E5	V	
	230	E6	W	
	231	E7	X	
	232	E8	Y	
	233	E9	Z	
	234	EA		
	235	EB		
	236	EC		
	237	ED		
	238	EE		
	239	EF		
	240	F0	0	
	241	F1	1	
	242	F2	2	
	243	F3	3	
	244	F4	4	
	245	F5	5	
	246	F6	6	
	247	F7	7	
	248	F8	8	
	249	F9	9	
	250	FA	|	Vertical Line
	251	FB		
	252	FC		
	253	FD		
	254	FE		
	255	FF	EO	Eight Ones

Appendix F: File extensions

Top-level configuration profile extensions

Table 21: Top-level configuration profiles

Product Type	Display	Printer	Screen	Port	Character
BlueZone Mainframe	.ZMD	.ZMP	-	-	-
BlueZone iSeries	.ZAD	.ZAP	-	-	-
BlueZone VT	.ZVT	-	-	-	-
BlueZone ICL	.Z7D	-	-	-	-
BlueZone T27**	.ZTD	-	BZT27.INI*	T27QPORT.INI*	T27CHAR.INI*
BlueZone UTS**	.ZUD	BZUTSPTR.INI*	BZUTS.INI*	UTSQPORT.INI*	UTSCHAR.INI*
BlueZone Secure FTP	.ZFT	-	-	-	-
TCP/IP Print Server	-	.ZTP	-	-	-

* These names are assigned automatically

** BlueZone T27 and UTS require multiple files for a complete Top Level configuration

Dialog-level configuration profile extensions

The following table contains a list of menu bar commands along with their associated file extensions.

Table 22: Dialog level configuration profiles

Toolbar command	3270	5250	VT	ICL	UTS	T27
Session ® Configure	.MDS	.ADS	.VDS	.IDS	.UDS	.TDS
Session ® Configure ® Properties	.TN3	.TN5	-	.IDC	UTSQPOR-T.INI	T27QPOR-T.INI
Options ® Display	.MDD	.ADD	.VDD	.IDD	.UDD	.TDD
Options ® Keyboard	.MDK	.ADK	.VDK	.IDK	.UDK	.TDK
Transfer ® Configure	.MDF	*	.VDF	.IDF	.UDF	.TDF
View ® Properties ® ToolBars	.MDB	.ADB	.VDB	.IDB	.UDB	.TDB
View ® Properties ® PowerPads	.MDP	.ADP	.VDP	.IDP	.UDP	.TDP
View ® Properties ® Statusbar	.MDR	.ADR	.VDR	.IDR	.UDR	.TDR
File ® Print Setup	-	-	.VDI	.IDI	-	-

BlueZone host file transfer configuration profile extensions

The following table contains a list of menu bar commands along with their associated file extensions.

Table 23: BlueZone Host file transfer configuration profiles

Toolbar Command	3270	5250
File ® Save As	.MDF	.ADF
List ® Save As	.MDL	.ADL

Appendix G: Locking features

BlueZone feature locks

Table 24: Feature locks lists the features and their values that you can lock in the Lock= entry in the `setup.ini` file. Refer to Configuring feature locking, on page 38 for more information.

Table 24: Feature locks

Feature	Value	Description
TOOLBARLOCK	1	Locks the toolbar settings in **View** ® **Properties** *
POWERKEYSLOCK	2	Locks the power key settings in **View** ® **Properties**
STATUSBARLOCK	4	Locks the status bar settings in **View** ® **Properties**
KEYBOARDLOCK	8	Locks the keyboard map settings in **Options** ® **Keyboard**
DISPLAYLOCK	16	Locks the display settings in **Options** ® **Display**
FILELOCK	32	Locks the **File** ® **Properties** settings*
SESSIONLOCK	64	Locks the session settings in **Session** ® **Configure** *
PRINTERLOCK	128	Locks the printer screen settings in **File** ® **Print Setup**
EDITLOCK	256	Locks the cut and paste settings in **Edit** ® **Properties**
TRANSLATELOCK	512	Locks the translate table settings in **Session** ® **Configure**
MACROLOCK	1024	Locks the macro settings in **Macro** ® **Properties**
TRANSFERLOCK	2048	Locks IND$File settings in **Transfer** ® **Configure** (3270 only)
APILOCK	4096	Locks the settings in **Options** ® **API**
SCRIPTLOCK	8192	Locks the Script settings in **Script** ® **Properties**
QUEUELOCK	16384	Locks the print queue settings in the print emulators only
LICENSELOCK	32768	Locks the settings in **Session** ® **Configure** ® **License Manager** *
LOCKALLCONFIG	-1	Locks all settings

* These items can be inherited by BlueZone Secure FTP as an option. Refer to Inheriting common lock values from BlueZone, on page 42 for more information on how BlueZone Secure FTP inherits the BlueZone lock settings.

BlueZone Secure FTP command and feature locks

Table 25: Secure FTP command and feature locks lists the Secure FTP features and their values that you can lock in the LockFTP= entry in the `setup.ini` file. Refer to Locking BlueZone Secure FTP commands and features, on page 42 for more information.

Table 25: Secure FTP command and feature locks

Function	Value
Block changing directories (CWD)	1
Block uploads (STOR)	2
Block downloads (RETR)	4
Lock configuration settings	8
Block the SITE command (SITE)	16
Block the make directory command (MKD)	32
Block the remove directory command (RMD)	64
Block the custom/FTP command options	128
Block the initial commands	256
Block delete file (DELE)	512
Inherit the BlueZone feature lock settings *	1024

* Refer to BlueZone feature locks, on page 155 for the items that can be inherited by BlueZone Secure FTP.

BlueZone Secure FTP individual feature locks

Session lock table

Table 26: Session configuration locks lists the features and their values that you can lock in the Session Configure window. Set these locks in the `LockFTPSession=` entry of the `setup.ini` file. Refer to Locking the Session Configuration dialog, on page 43 for more information.

Table 26: Session configuration locks

Feature to lock	Value	Location
Lock all the following features	-1	
Connection List Window	1	Connections tab
New Button	2	Connections tab
Edit Button	4	Connections tab
Copy Button	8	Connections tab
Remove Button	16	Connections tab
Sort Button	32	Connections tab
Use Connection Name as Session Description	64	Connections tab
Auto-Connect Session	128	Connections tab
Prompt on Disconnect	256	Connections tab
Prompt to Reconnect to Last Directory when disconnected	512	Connections tab
Connect Retry	1024	Connections tab
Double-Click Settings	2048	Options tab
Logging Options Settings	4096	Options tab

Connection lock table

Table 27: Connection locks - New/Edit/Copy lists the features and their values that you can lock in the window. Set these locks in the `LockFTPConnection=` entry of the `setup.ini` file. Refer to Locking the Connection dialog, on page 44 for more information.

Table 27: Connection locks - New/Edit/Copy

Feature to lock	Value	Location
Lock all the following features	-1	
Connection Name	1	Connection tab
Host Address	2	Connection tab
Host Type	4	Connection tab
TCP Port	8	Connection tab
Backup Host	16	Connection tab
Initial PC Directory	32	Connection tab
Initial Host Directory	64	Connection tab
Username	128	Connection tab
Password	256	Connection tab
Anonymous signon	512	Connection tab
Do not send Username/Password	1024	Connection tab

Miscellaneous lock table

Use `LockFTPMiscellaneous=`*`value`*

Table 28: Miscellaneous locks

Feature to lock	Value	Location
Lock all the following features	-1	
Place folders on top when sorting	1	Miscellaneous tab
Prompt for destination name before file transfer	2	Miscellaneous tab
Disable automatic LIST after connect and uploads	4	Miscellaneous tab
Overwrite LIST command with	8	Miscellaneous tab
Enable Passive Mode	16	Miscellaneous tab
Enable Keep Alive Timer (Minutes)	32	Miscellaneous tab
Use directory prefix on Uploads	64	Miscellaneous tab
Use reduced buffer size	128	Miscellaneous tab

Additional items table

Table 29: Additional items

Dialog	Value	Location
Initial Commands	1	Initial Commands tab
Schedule	1	Schedule tab
Firewall	1	Firewall tab
Security	1	Security tab
Certificate	1	Certificate tab

Telnet feature locks

Table 30: Telnet feature locks lists the tabs and their values that you can lock in the `LockTelnet=` entry in the `setup.ini` file. Refer to Configuring the Telnet locking feature, on page 39 for more information.

Table 30: Telnet feature locks

Tab to hide	Value
Connections tab	1
Device tab in 3270 **Display/Printer** tab in 5250 *	2
Security tab	4
Certificate tab	8
Keep Alive tab	16
Trace tab	32
Firewall tab	64
Security Server tab *	128
Kerberos tab	256

* Tab does not apply to BlueZone VT

Display feature locks

Table 31: Display feature locks lists the tabs and their values that you can lock in the `LockDisplay=` entry in the `setup.ini` file. Refer to Configuring the display locking feature, on page 39 for more information.

Table 31: Display feature locks

Tab to hide	Value
Font tab	1
Cursor tab	2
Colors tab	4
GUI tab	8
Watermark tab	16
Advanced tab	32

Dialog-level configuration profile locks

Table 32: Dialog-level configuration profile locks lists the configuration profile buttons and their values that you can lock in the `HideDialogButtons=` entry in the `global.ini` file. Refer to Configuring the dialog configuration profile locks, on page 41 for more information.

Table 32: Dialog-level configuration profile locks

Button to hide	Value
New	1
Open	2
Save	4
Save As	8
Help	16

Appendix H: Command line switches

BlueZone MSI features

Features that are marked with a possible value of 1 or 0 are features that are either On or Off. In your MSIEXEC command line, use a 1 to indicate On and a 0 to indicate Off.

Keep in mind that if a feature's default value is acceptable, you do not have to include that feature in your command line statement.

Table 33: MSI feature values

MSI name	Function description	Possible values	Default value
INSTALLDIR	Sets the Installation Directory Path	<PATH>	See Note 1
WORKINGDIR	Sets the Working Directory Path	<PATH>	See Note 2
WORKINGDIR_MODE	Sets the Working Directory Mode	0 = Custom - Set your own path 1 = Use Personal Folder (Default) 2 = Use All Users Common Folder 3 = Use Current User Application Data Folder **Note:** When using the Working Directory Mode of "Custom" (WORKINGDIR_MODE = 0), you must also assign a path to WORKINGDIR, so that the BlueZone Installer knows where to create your Working Directory.	1
ADDLOCAL	Adds all available features to the installation	ALL	
CONNECTION_TYPE	Preferred Connection Type	0 = SNA Server 1 = Renex Asynchronous Protocol 2 = TN3270 / TN5250 (Default) 3 = IBM Communications Server 4 = IntranetWare for SAA	2
LOCK	BlueZone feature lock	Refer to BlueZone feature locks, on page 155 for values.	0
LOCK_FTP	BlueZone FTP feature lock	Refer to BlueZone Secure FTP command and feature locks, on page 155 for values.	0

Table 33: MSI feature values (continued)

MSI name	Function description	Possible values	Default value
LOCK_TELNET	Telnet feature lock	1 = Hides the Connections Tab 2 = Hides the Device Tab in 3270 and the Display/Printer Tab on 5250 * 4 = Hides the Security Tab 8 = Hides the Certificate Tab 16 = Hides the Keep Alive Tab 32 = Hides the Trace Tab 64 = Hides the Firewall Tab 128 = Hides the Security Server Tab * 256 = Hides the Kerberos Tab * Tab does not apply to BlueZone VT	0
SHOW_LOCKDLGS	Show locked dialogs	1 or 0	1
DISABLE_CLIPBOARD	Disable append to clipboard	1 or 0	0
BASE_REGISTRY	Base registry setting	0 = HKEY_CURRENT_USER (Session Settings Only) (Default) 1 = HKEY_LOCAL_MACHINE (All Settings) 2 = HKEY_CURRENT_USER (All Settings)	0
PROFILE_MODE	Profile mode	1 or 0	1
PROFILE_SHARING	Profile sharing	1 or 0	1
ENABLE_PWRKEYS	Enable power keys feature	1 or 0	0
FIPS_MODE	Enable FIPS mode	1 or 0	0
HLLAPI_CONNRETRY	HLLAPI connection retry in milliseconds	Value in ms HLLAPI_CONNRETRY=500, for example, represents one half second.	0
HLLAPI_TELNET	Telnet host settle time in milliseconds	Value in ms HLLAPI_CONNRETRY=500, for example, represents one half second.	0
SESSION_MANAGER_RUNIN-TRAY	Place the Session Manager icon in the Windows Tray	1 or 0	0
REMOVE_WORKINGDIR	Remove working directory during uninstall	1 or 0	0

Note 1

If no install directory (INSTALLDIR) is specified, BlueZone is installed in `C:\Program Files\BlueZone\6.1`.

Note 2

If WORKINGDIR is not specified in the command line and WORKINGDIR_MODE= is set to 1, then the installer makes the working directory the user's personal folder.

If WORKINGDIR is specified in the command line, for example, C:\WORKINGDIR="C:\Bluezone", then the installer forces WORKINGDIR_MODE= to 0, so it is not necessary to include WORKINGDIR_MODE=0 in the command line statement.

BlueZone command line switches

BlueZone supports many command lines switches that are used to control BlueZone during startup. Command line switches are added to the command line after the file name that loads the BlueZone application.

Table 34: BlueZone Mainframe Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/R	Dialog configuration profile
/L	LU name
/H	Host IP address or DNS name
/O	TCP port number
/T	Device type (used in Display session only)
/Q	Set Registry without starting
/I	Blockade user ID
/J	Blockade password
/K	Blockade message
/&	Auto-lock keyboard on start
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption
/1../9	Var1 through Var9

Table 35: BlueZone Mainframe Printer command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/L	LU name
/L!	Associates a Mainframe Display session LU name to the Printer session
/H	Host IP address or DNS name
/O	TCP port number
/Q	Set Registry without starting
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption

Table 36: BlueZone iSeries Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/R	Dialog configuration profile
/L	Device name
/H	Host IP address or DNS name
/O	TCP port number
/T	Device type (used in Display session only)
/N	User name
/P	Password
/G	Initial program to call
/M	Initial menu name
/B	Initial library name
/Q	Set Registry without starting
/I	Blockade user ID
/J	Blockade password
/K	Blockade message
/&	Auto-lock keyboard on start
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption
/1../9	Var1 through Var9

Table 37: BlueZone iSeries Printer command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/L	Device name
/H	Host IP address or DNS name
/O	TCP port number
/A	Queue name
/V	Queue library
/W	Font
/X	Formfeed
/Y	Host print transform
/Z	Printer model
/Q	Set Registry without starting
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption

Table 38: BlueZone VT Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session number
/F	Configuration file name
/R	Dialog configuration profile
/H	Host IP address or DNS name
/O	TCP port
/T	Terminal ID
/L	Answerback
/A	Number of columns
/R	Number of rows
/Q	Set Registry without starting
/I	Blockade user ID
/J	Blockade password
/K	Blockade message
/&	Auto-lock keyboard on start
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption
/1../9	Var 1 through Var 9
/[0	Sets auto-connect to False
/[1	Sets auto-connect to True

Table 39: BlueZone ICL 7561 Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/R	Dialog configuration profile
/H	Host IP address or DNS name
/O	TCP port number
/Q	Set Registry without starting
/~0	Disables SSL/TLS encryption
/~2	Enables SSL/TLS encryption
/1../9	Var1 through Var9

Table 40: BlueZone Unisys T27 Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/H	Host IP address or DNS name
/L	Station name
/O	TCP port number
/Q	Set Registry without starting
/1../9	Var1 through Var9

Table 41: BlueZone Unisys UTS Display command line switches

Switch	Function
/C	Connection name
/D	Session description
/S	Session identifier
/F	Configuration file
/H	Host IP address or DNS name
/L	Station name
/O	TCP port number
/Q	Set Registry without starting
/1../9	Var1 through Var9

Table 42: BlueZone Session Manager command line switches

Switch	Function
/F	Configuration file name
/T	Start directly in the Windows System Tray

Table 43: BlueZone TCP/IP Print Server command line switches

Switch	Function
/F	Configuration file name
/T	Start directly in the Windows System Tray

BlueZone feature lock command line switches

Table 44: BlueZone feature lock command line switches

Switch	Function
/.*x*	Locks the specified BlueZone feature or features. Where *x* is the lock feature value. Refer to BlueZone feature locks, on page 155 for a list of the available values.
/,*x*	Locks the specified BlueZone display feature or features. Where *x* is the lock feature value. Refer to Display feature locks, on page 158 for a list of the available values.
/`*x*	Locks the specified BlueZone Telnet feature or features. Where *x* is the lock feature value. Refer to Telnet feature locks, on page 158 for a list of the available values.

BlueZone Secure FTP command line switches

BlueZone Secure FTP supports many command lines switches which are used to control BlueZone Secure FTP during startup. Command line switches are added to the command line after the file name that loads the BlueZone Secure FTP application.

Table 45: Secure FTP command line switches

Switch	Function
/L	Initial commands
/S	Session number
/F	Configuration file
/C	Connection name
/D	Session description
/H	Host IP address or DNS name
/O	TCP port number
/T	Host type
/N	User name
/P	Password
/I	Initial PC directory
/R	Initial Host directory
/K	Private key password
/A	Play transfer list after connect and initial commands
/Z	Session number to select at startup
/!	License Manager address override
/#	License Manager group override
/~0	Disables encryption
/~1	Enables Explicit SSL/TLS encryption
/~2	Enables Implicit SSL/TLS encryption
/~3	Enables SFTP encryption
/1../9	Var 1 through Var 9
/[0	Sets auto-connect to False
/[1	Sets auto-connect to True

Common supported FTP commands through the command line

The following FTP commands are supported through the command line:

STOR

Uploads a local file to the host. If `str2` is in the command then the file name on the host is set to `str2` instead of `str1`.

Format: `STOR str1`

Format: `STOR "str1" str2`

STOU

This command behaves like STOR except that the resultant file is to be created on the host under a name unique to that directory.

Format: STOU str1

Format: STOU "str1" str2

APPE

This command behaves like STOR except that if the resultant file already exists on the host the contents of the local file are appended to the host file.

Format: APPE str1

Format: APPE "str1" str2

PUT

This command behaves like STOR.

Format: PUT str1

Format: PUT "str1" str2

RETR

Downloads str1 from the host and stores it on the local computer. If str2 is in the command then the file name is stored on the local computer as str2.

Format: RETR str1

Format: RETR "str1" str2

GET

This command behaves like RETR.

Format: GET str1

Format: GET "str1" str2

MPUT

Uploads multiple files to the host. Wildcards (*) are supported in this command. Ex. MPUT *.txt uploads all the text files in the current directory to the host.

Format: MPUT str1

Format: MPUT str1 str2 str3 and so on (long file names containing spaces are not supported in this command, use multiple STOR commands instead).

MGET

Downloads multiple files from the host. Wildcards (*) are supported in this command. Example: MGET *.txt downloads are the text files in the current host directory from the host.

Format: MGET str1

Format: MGET str1 str2 str3 and so on (long file names containing spaces are not supported in this command, use multiple RETR commands instead).

LIST

Performs a listing of the current host directory.

Format: LIST

LS

Performs a listing of the current host directory. Not all hosts support this command.

Format: LS

DIR

Performs a listing of the current host directory. Not all hosts support this command.

Format: DIR

EXIT
Closes the BlueZone FTP program.

Format: `EXIT`

QUIT
Disconnects the connection to the host.

Format: `QUIT`

CWD
Changes the current working directory on the host.

Format: `CWD str1`

CD
This command behaves like `CWD`.

Format: `CD str1`

CDUP
Changes the current directory to its parent directory.

Format: `CDUP`

TYPE
Changes the data type used for file transfer.

Format: `TYPE A` (Sets Type to ASCII)

Format: `TYPE I` (Sets Type to Binary)

Format: `TYPE E` (Sets Type to EBCDIC)

Format: `TYPE F` (Sets Type to Double-Byte EBCDIC)

Format: `TYPE B` (Sets Type to Double-Byte ASCII)

REIN
Terminates a USER, the state is now the same as after a connection is opened. A `USER` command can be expected to follow.

Format: `REIN`

SITE
Used by the server to provide services specific to the system that may be essential to file transfer. The nature of these services and the specification of their syntax can be stated in a reply to the `HELP SITE` command.

Format: `SITE`

DELE
Deletes the file specified in `str1` on the host.

Format: `DELE str1`

MKD
Creates the directory specified in `str1` as a directory (if `str1` is absolute) or as a subdirectory of the current working directory.

Format: `MKD str1`

RMD
Removes the directory specified in `str1`. If the directory is not empty then BlueZone FTP tries to recursively delete the contents in any subfolders.

Format: `RMD str1`

AUTH

Starts an SSL handshake between BlueZone Secure FTP and the host.

Format: `AUTH`

Format: `AUTH SSL`

Format: `AUTH TLS`

Format: `AUTH TLS-C`

Format: `AUTH TLS-P`

SMNT

Allows the user to mount a different file system data structure. Format depends upon the host.

Format: `SMNT str1`

Format: `SMNT str1 str2`

Format: `SMNT str1 str2 str3`

IFTD

A unique command to BlueZone Secure FTP. An iSeries File Transfer download is started with this command.

Format: `IFTD Library iSeries_File FFD Type PC_FileName`

Where: `Library` is the library on the iSeries server.

Where: `iSeries_File` is the data file to use for the transfer.

Where: `FFD` is the file field descriptor.

Type: `0` for XLS, `1` for CSV, `2` for Tab-delimited(txt).

Where: `PC_FileName` is the destination file name for the XLS, CSV, or TXT file.

IFTU

A unique command to BlueZone Secure FTP. An iSeries File Transfer upload is started with this command.

Format: `IFTU Library iSeries_File FFD PC_FileName`

Where: `Library` is the library on the iSeries server.

Where: `iSeries_File` is the data file to use for the transfer.

Where: `FFD` is the file field descriptor.

Where: `PC_FileName` is the destination file name for the XLS, CSV, or TXT file.

Related information

You might need to refer to other sources of information when you are using BlueZone products. This section lists the documentation that supports BlueZone.

Version 6 Release 1 product information:

- *BlueZone Advanced Automation Developer's Guide*, BZAA-0601-DG-02
- *BlueZone Desktop Administrator's Guide*, BZD-0601-AG-03
- *BlueZone Display and Printer User's Guide*, BZDP-0601-UG-03
- *BlueZone Integration Server Administrator's Guide*, BZIS-0601-AG-01
- *BlueZone License Manager Administrator's Guide*, BZLM-0601-AG-01
- *BlueZone PasswordVault User's Guide*, BZPV-0601-UG-01
- *BlueZone Secure FTP User's Guide*, BZSF-0601-UG-01
- *BlueZone Security Sever Administrator's Guide*, BZSS-0601-AG-01
- *BlueZone Session Manager User's Guide*, BZSM-0601-UG-01
- *BlueZone Web-to-Host Administrator's Guide*, BZWH-0601-AG-01

Index

E

F

G

H

I

J

K

L

M

O

P

R

S

T

U

V

W