Manual - Xmanager

Version 8 Help

1 Xmanager Manual

The manual describe how to use the program's interface and will guide you through the basics.

2 Content

2.1 About Xmanager

2.2 Start

2.3 Session Management

2.4 Connection

3 About Xmanager

Xmanager® is a powerful, convenient PC X server software package that operates in the Windows® environment. Users can bring the UNIX/Linux desktop to their Windows PC via **Xmanager**. Additionally, the X application can be safely executed through SSH (secure shell) even when a user's PC is inside a private network or there is a firewall in between a user PC and remote server.
Xmanager offers diverse functions, such as setting multiple servers, multi-visual, multi-monitor, multiple user settings, multiple XDMCP sessions, and SSH security reinforcement. **Xmanager** provides a variety of premium options for advanced users and a simple user interface for first-time users.
Xmanager is comprised of **Xmanager**, **Xmanager Classic**, **Xconfig**, **Xstart** and several other utilities. In Version 8, the new X server based on X11R7.7 is referred to as Xmanager, while the legacy X server for older UNIX/Linux environments is referred to as Xmanager Classic.

- **Xmanager** has several meanings:
  - An X server program for PC.
  - Xmanager as a server. Graphical applications, X clients, of remote UNIX/Linux hosts can be displayed on a Windows Screen via **Xmanager Server**.
  - A session utility which manages sessions and session files (Until Version 5, this was referred to as Xbrowser). This allows you to create, run, and delete Xstart and XDMCP sessions as well as Xshell and Xftp sessions if the respective programs are installed. Also, if users install the XmanagerRDP utility, RDP sessions can be managed from within Xmanager. From here, users can launch and run multiple session simultaneously and create shortcut icons for each host.
- **Xconfig** creates and manages **Xmanager** server profiles. These server profiles determine various **Xmanager** options such as window modes, font catalogs, colors, etc.
- **Xstart** enables the direct execution of single remote X applications on a user's PC. Supported protocols include SSH, TELNET, RLOGIN, REXEC, RSH, and LOCAL when connecting to remote hosts. A remote host command can be conveniently executed on a user's Windows PC via **Xstart**.

3.1 Key Functions

This section provides descriptions of the key **Xmanager** functions.
Connection and Startup

- Manage Xmanager (Xstart and XDMCP), Xshell, and Xftp sessions all in one place
- Supports RDP and VNC sessions
- Session Manager for easily running and managing multiple sessions
- XDMCP, SSH, RSH, REXEC, RLOGIN and TELNET connection protocols
- Up to 128 X client connections per Xmanager session
- Shortcut to Xstart and XDMCP sessions
- Advanced prompt recognition settings and remote command script in Xstart
- Secure XDMCP for XDMCP connections to beyond firewalls and private networks
- IPv6 support
- Kerberos(MIT Kerberos, Microsoft SSPI) authentication support
- Multi tabs in a single window
- Multi tab groups in a single window
- Authentication Profile that manages authentication information instead of scattered authentication information in session files
- Windows Notifications

Installation and Distribution

- Supports Windows terminal server and Citrix MetaFrame for Windows

- Session sharing for Windows terminal service
- Silent Installation
- Multi-user setting
- Simple session and server profile distribution
- User-designated session path
- Program theme selection

Security

- SSH1/SSH2 protocols supporting public key authentication
- Creates SSH public key
- SSH user authentication agent
- Access control by host
- XDMCP connections using SSH secure tunnel(SecureXDMCP)
- User defined Master Password to add additional security to session passwords

X Server

- High-performance X11R7 PC X server
- GLX 1.3, OpenGL 1.2 extension protocol
- X Rendering extension protocol
- Supports RandR Exension
- Multi-server setting
- Multi-user setting
- Multi-monitor
- Multi-network adapter
- Multi-XDMCP sessions
- Automatic display number allocation
- Single & Multiple Window mode
- Panning and auto-raise in local window manager
- Multi-visual
- 256-color visuals in True Color video device
- Automatic color substitution for PseudoColor visuals
- Backing Store
- Complete Planemask function for 256-color applications
- Wheel mouse
- 3-button mouse emulation
- GUI keyboard editor
- Real-time keyboard change using shortcut key
- Sound files for XBell requests
- Local resources database
- Window printing in Multiple Window mode
- Automatic copy & paste between X applications and Windows applications
- Notification area icon

Font

- Font compiler
- Font server
- BDF, PCF font formats
- Automatic font substitution
- Additional fonts packages for various languages and X applications

3.2 Recommendations

- **Processor:** Intel® compatible
- **Operating System:** Windows 8 or higher, Windows Server 2012 or higher
- **Storage Space:** 100MB or more reserve space
- **Network:** TCP/IP network

3.3 Install and Uninstall

The **Xmanager** installation program was created using InstallShield®. A variety of installation options can be changed during installation. However, it is often sufficient to simply click [Next].
To uninstall **Xmanager**, use the standard Windows add/remove functions. Run the Control panel program regarding programs(control appwiz.cpl) and select to uninstall **Xmanager** from the list.
Even when the program is uninstalled, the registry information, log files and data files created by the user are not removed. The information and files are available for reuse when the program is reinstalled. If you want to remove all the files and registry information completely, remove the following explicitly:
Registry Information:

- \HKEY_CURRENT_USER\Software\NetSarang\Xmanager

File and Folder:

- User's Documents Folder\Netsarang Computer\8\Xmanager

4 Start

Xmanager provides **Xmanager** and **Xstart**, two basic tools for accessing a remote UNIX/Linux host. **Xmanager** brings the entire remote desktop via XDMCP (X display manager control protocol) to the user's Windows PC. Other users who only need access to single X applications, as opposed to an entire desktop environment, can opt to us **Xstart** as it is simpler and quicker than an XDMCP connection.

Note
Run **Xmanager - Passive** from the Tools folder under the **Xmanager** installation folder to have **Xmanager server** enter standby mode for X application connections. Users can then run a remote X application using **Xstart** or other tools.

4.1 Starting with XDMCP

To use **Xmanager sessions**, set a remote UNIX/Linux host to support the XDMCP service for a remote X server. In general, **dtlogin**, **kdm**, **gdm, lightdm**, or **xdm** must be running on the host. For details about XDMCP service settings, refer to the proper UNIX/Linux manual.

1. Open **Xmanager** folder on your desktop.

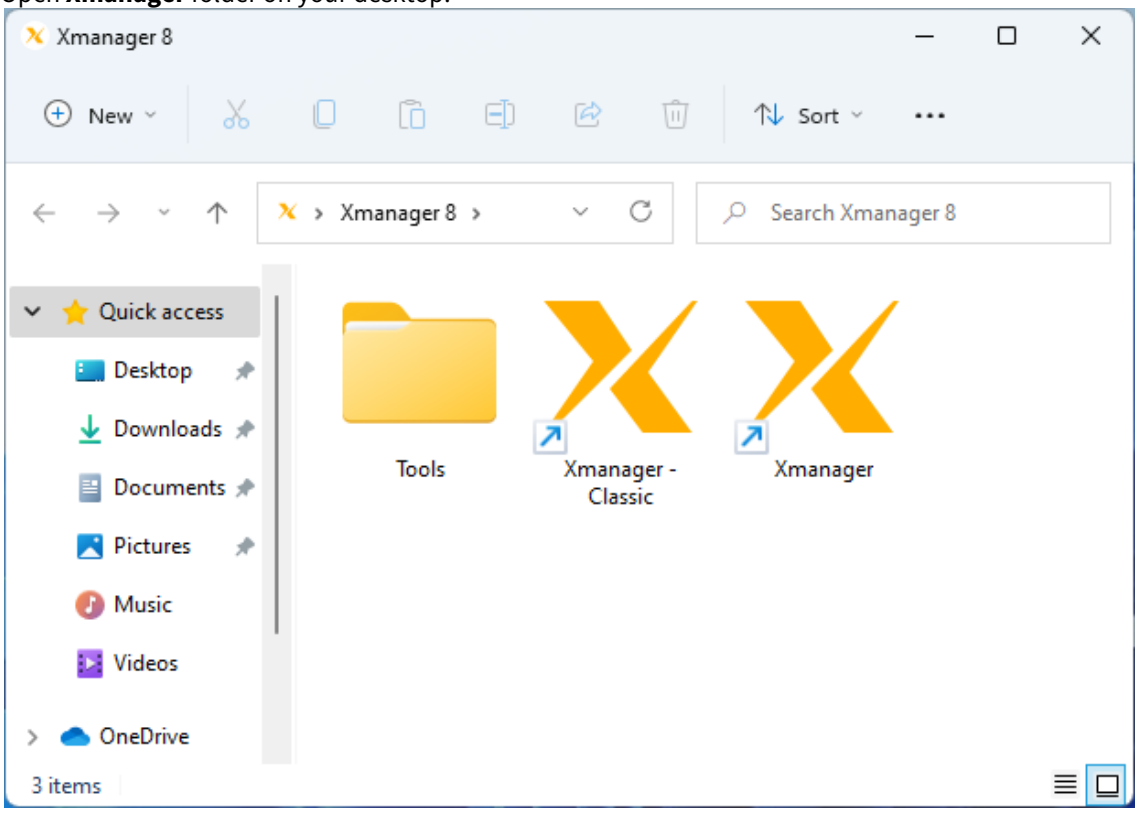

Fig. 1: Xmanager Folder

2. Run **Xmanager**.

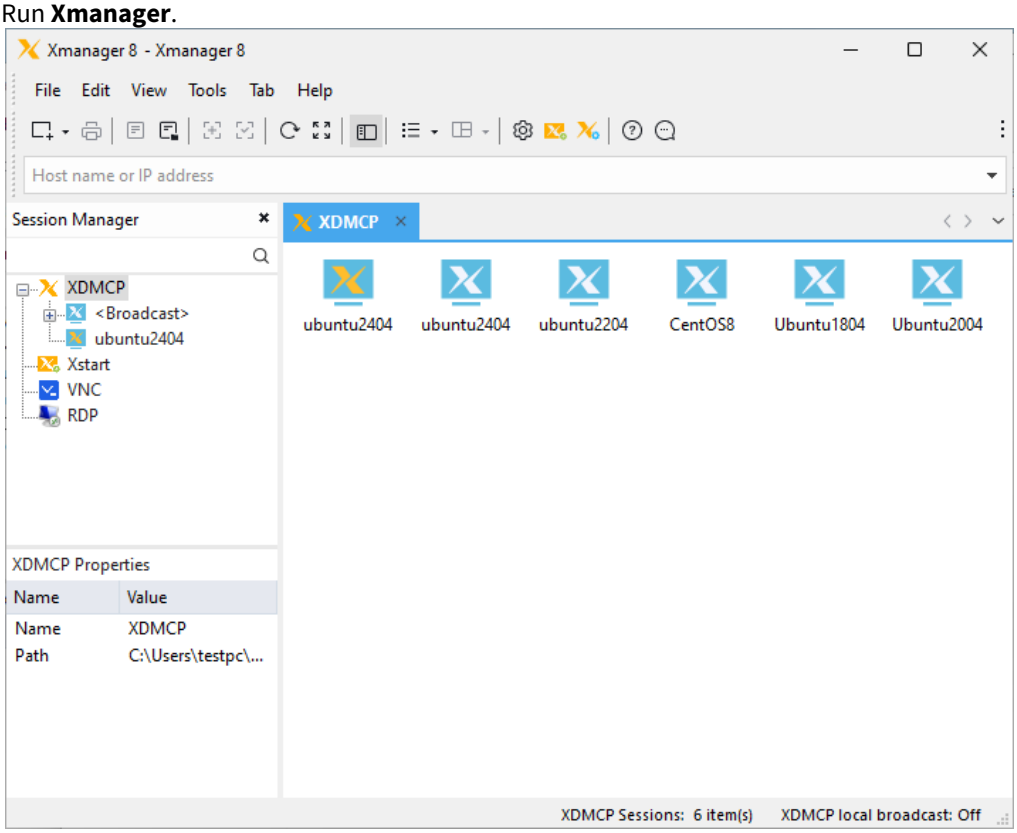

Fig. 2: Xmanager main window

Note

Xmanager automatically finds all UNIX/Linux hosts in the local network. If the UNIX/Linux host to access is on a different network than the user's PC, register the UNIX/Linux host IP address or broadcast address in the **Options** dialog box. For setting details, see **'**Automatic XDMCP Session**'.** If a UNIX/Linux host is not displayed in the **Xmanager** window, it means that the host is not prepared for an XDMCP connection.

3. Double-click a host to connect to. A graphic login screen opens.

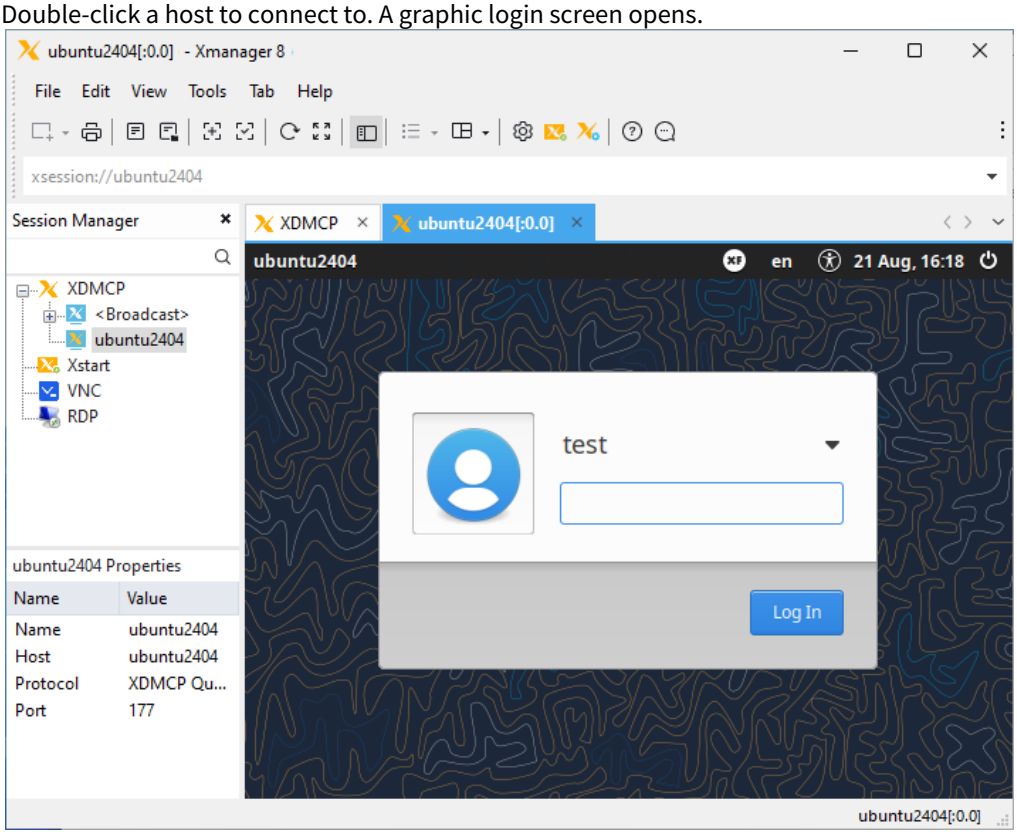

Fig. 3: CentOS login screen via an XDMCP connection

Note

If graphic login screen is not displayed, it is possible there is a firewall between the user's PC and the remote host.

4. Log in to the host by entering the account name and password. The remote desktop opens.

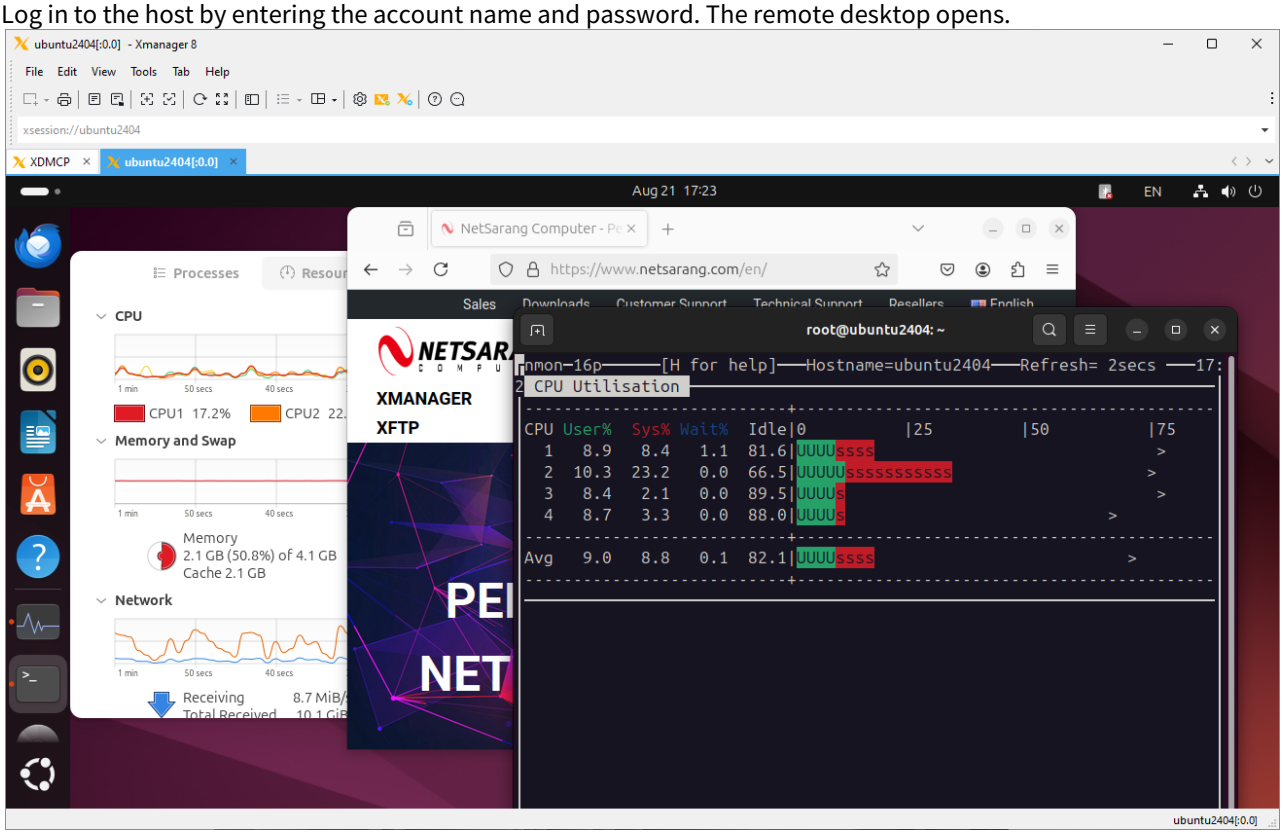

Fig. 4: Ubuntu desktop executed in Windows

Note

If the remote desktop does not display after entering the account and password, there may be a problem in the user account login shell script.

If you experience problems using **Xmanager**, visit our customer support page
Additional information about XDMCP settings in UNIX/Linux servers and related tips can be found in the customer support page.

4.2 Starting with Xstart

Xstart allows users to run a remote X application. Once an Xstart session is created, the remote X application can be executed any time in the future by simply clicking the session file in Windows.

1. Run **Xstart** located in Tools of the **Xmanager** folder.

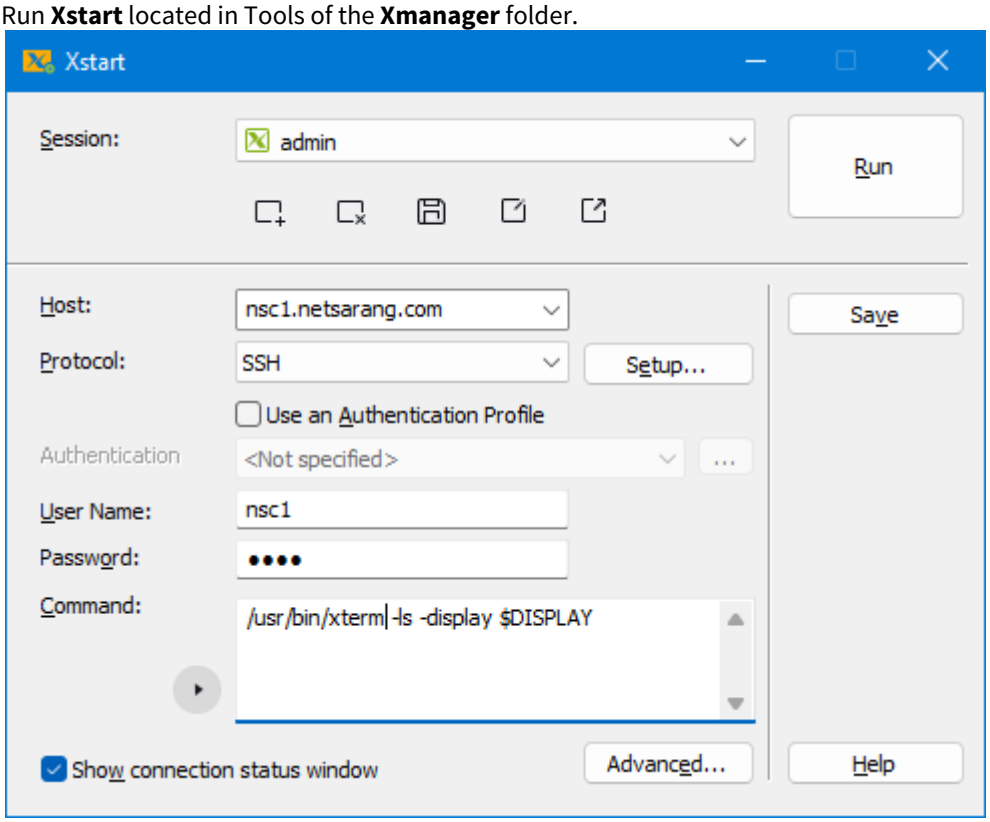

Fig. 1: Xstart main window

2. Click [New]. The **New Session** dialog box is displayed.

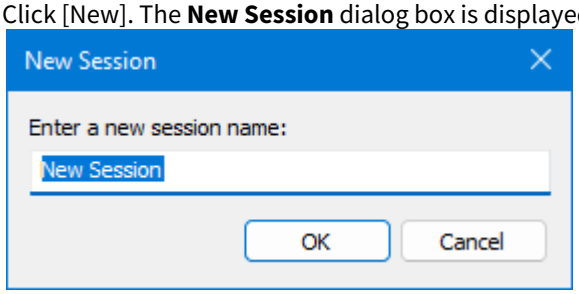

Fig. 2: Xstart New Session dialog box

3. Enter new session name and click [OK].
4. Enter the remote UNIX/Linux host name or IP address in [Host].
5. Select one of the protocols supported by the host from [Protocol].
6. Click [Setup] to set protocol options, such as port or timeout.
7. Enter remote host user account in [User Name].
8. Enter remote host *Password* in [Password].
9. Enter a command to be executed in the host in [Command]. To run **xterm**, enter the following command: /usr/bin/X11/xterm –ls –display $DISPLAY

> **Note**
> By pressing the button below the [Command] label, a convenient list of generally used sample xterm commands registered by UNIX/Linux types will be displayed. Select the xterm command suited to the UNIX/Linux distro to connect to. You can also add/remove frequently used commands by opening the **Registered Commands** dialog box.

10. Click [Run]. **xterm** window opens.

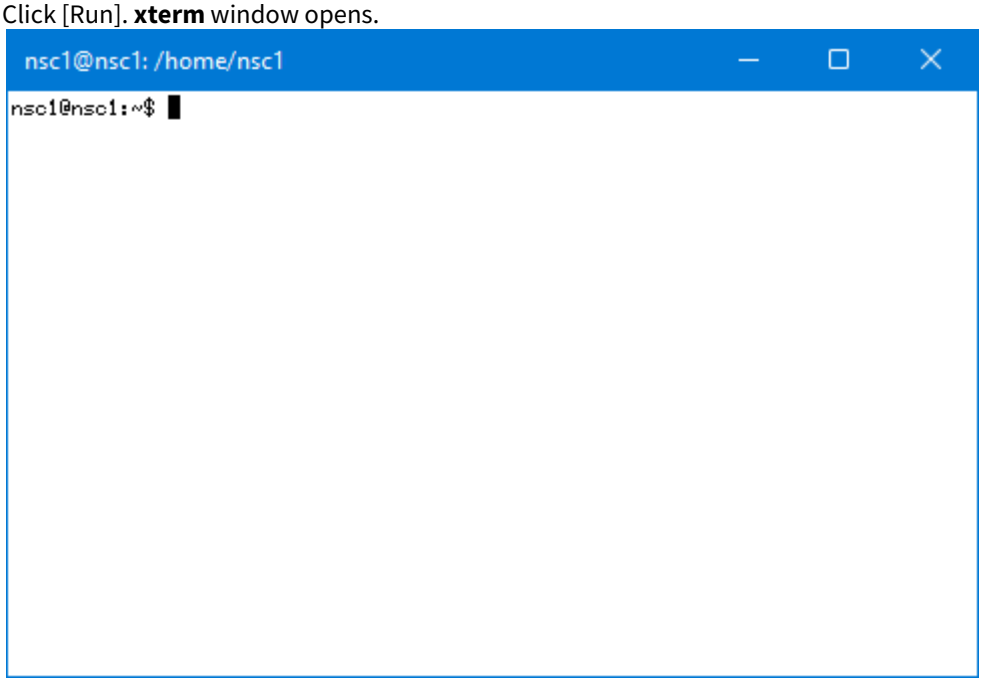

Fig. 3: xterm window

If you experience problems using **Xstart**, visit our customer support page
Most problems are typically caused by a firewall, the user PC, or network settings. In some cases, users may have to consult with network or system administrators.

4.3 Exit Xmanager

To end a remote X application started by **Xstart** or **Xmanager**, select [Close] from **Xmanager server's** system menu. For **Xmanager** system menu, see 'Window Mode'.
To Automatically Exit Xmanager server when All Remote X Applications are closed:

1. Select [Properties] from **Xmanager server's** system menu. The **Profile Properties** dialog box is displayed.
2. Select [Exit Xmanager when all connections are closed] from the [General] tab.
3. **Xmanager server** exits when all X application windows are closed.

Note
If the [Exit Xmanager when all connections are closed] option is not selected, **Xmanager** initializes when all remote X applications are closed and stands by for a new X application connection.

5 Session Management

Sessions have connection information to connect to a remote host. Users can designate different options and server profiles for each connection by creating a session.
Session types are divided into automatic XDMCP sessions, static XDMCP sessions, and Xstart sessions.

Icon	Session Type	Description
	Automatic XDMCP	**Xmanager** sends a broadcast message to local LAN and dynamically finds the hosts. To find another subnet host, enter host IP address in the **Options** dialog box. All automatic sessions use the same settings. However to change session settings, users can right-click on a session, select [Save As], and save the session. Then, right-click on the newly created session and select [Properties]. In this case, the newly created session becomes a static XDMCP session.
	Static XDMCP	Static session is a session created by a user. Static sessions can be created by copying (saving) an automatic session or using the New Session Wizard. If a remote host does not respond to an XDMCP request message, the displayed icon will be dim. Users can create shortcuts, change settings for this session, and send this session to other users via e-mail, etc.
	Xstart	**Xmanager** can create and manage Xstart sessions. Additionally, users can also manage these sessions from directly within **Xstart**. **Xmanager** and **Xstart** share all **Xstart** sessions. By double-clicking Xstart sessions, users can conveniently run a remote X application in their Windows PC.

Note
Xstart session is useful when running remote X applications one by one. This session connects to a remote host, automatically executes a designated command, and opens an X application in the user's Windows PC. XDMCP session is useful for bringing the GUI login screen and the entire remote host desktop environment to the user's Windows PC. **Xmanager** supports all UNIX/Linux GUI desktop environments including CDE, KDE and GNOME.

5.1 Xstart Session

By creating an Xstart session, a remote host X application can be executed in a user's PC. **Xstart** automatically processes the remote host login process and executes remote X applications designated by the user.
Users can create Xstart sessions in both **Xstart** and **Xmanager**.

To Create a Session with Xstart:

1. Run **Xstart** located in the **Xmanager** Folder.
2. Click [New]. The **New Session** dialog box is displayed.
3. Enter a new session name and click [OK].
4. Enter the remote UNIX/Linux host name or IP address in [Host].
5. Select one of the host supported protocols from [Protocol].
6. Click [Setup] to set options by protocol, such as port or timeout.
7. Enter remote host user account in [User Name].

8. To save user password in session, set [Authentication] as *Password* and click the [Setup] button on the right. The **Password Setup** dialog box is displayed.
9. Enter a command to be executed in the remote host in [Command]. To run **xterm**, enter command as follows:
   /us**r/bin**/X11/xterm –ls –display $DISPLAY
   - **Note**
     Press the button below the [Command] label to see a list of generally used sample xterm commands registered by different UNIX/Linux types. Select the xterm command suited to the UNIX/Linux to connect to. User can also add/remove frequently used commands by opening the **Registered Commands** dialog box. $DISPLAY is converted to the PC's IP address and the display number that the Xmanager server is waiting for. However, if the SSH Protocol is being utilized, DISPLAY is automatically specified according to the X11 forwarding protocol, so the '-display $DISPLAY' option is not required. Xstart will not convert $DISPLAY while delivering the command.
10. Click [Save].

To Create a Session with Xmanager:

1. Run **Xmanager** in the **Xmanager** Folder.
2. Point to [New] in the [File] menu and select [Xstart Session]. The **New Session Properties** dialog box is displayed.
3. Enter [Session] name in [General] tab. Make sure not to enter a duplicate session name with an existing session file.
4. Enter the remote UNIX/Linux host name or IP address in [Host].
5. Select one of the host supported protocols from [Protocol].
6. Click [Setup] to set options by protocol, such as port or timeout.
7. Enter remote host user account in [User Name].
8. Enter the password to the user account in [Password].
9. Enter a command to be executed in the remote host in [Execution Command]. For example, enter command as follows to run **xterm**:
   /usr/bin/X11/xterm –ls –display $DISPLAY
10. Click [OK].

- **Note**
  Users can also create Xstart sessions using the **New Session Wizard** provided in **Xmanager**. Make sure the **Xmanager** session category is set as **Xstart**, then point to [New] in the [File] menu and select [New Session Wizard] to open the wizard.

To Create Shortcuts to Xstart Sessions:

1. Run **Xstart**.
2. Select a session from [Session] list.
3. Click the arrow button to view more menus and click [Create Shortcut]. The **Browse For Folder** dialog box is displayed.
4. Select a folder in which to create the shortcut.

5.2 Automatic XDMCP Session

Xmanager sends an XDMCP Broadcast message to the local network or a network designated by a user and shows the hosts that respond to the message. These sessions are automatically created by **Xmanager** and users do not need to create them manually. Therefore, these sessions are referred to as automatic sessions.
In general, all UNIX/Linux systems support the XDMCP service, and there should be no problem finding hosts in the **Xmanager** window. In some cases, a remote host is set not to support the XDMCP service and, as a result, it is not displayed in **Xmanager**. In this case, contact the system administrator of the concerned host and request to have the XDMCP service supported.

Xmanager provides an option to find hosts in other networks. Additionally, it offers an option to turn off the broadcast function in case there are too many hosts in the local network.

To Find Hosts in Another Network:

1. Run **Xmanager**.
2. Select [Options] in the [Tools] menu. The **Options** dialog box is displayed.
3. Enter the host name or IP address to find in [Search] section of the [XDMCP] tab or enter the network broadcast address to find all hosts available (e.g. 192.168.0.255)
4. Click [Add].
5. Click [OK].

To Turn off the Local Broadcast Option:

1. Run **Xmanager**.
2. Select [Options] in the [Tools] menu. The **Options** dialog box is displayed.
3. Unselect [Search for local hosts (XDMCP Broadcast)] in the [XDMCP] tab.
4. Click [OK].

Note
If there are too many hosts in the user's local network and there are a limited number of hosts to use, it may be convenient to turn off the [Search for local hosts (XDMCP Broadcast)] option and add only the necessary hosts to the list of search addresses.

5.3 Static XDMCP Session

In addition to automatic sessions, **Xmanager** provides support for static sessions, such as Passive, XDMCP Query, XDMCP Broadcast, XMDCP Indirect, and Secure XDMCP. Unlike automatic sessions, static sessions are displayed in the **Xmanager** window at all times and can be created, modified, or deleted by users. Unlike XDMCP sessions, passive sessions wait passively for an X application's request, but are grouped with XDMCP sessions based simply on the fact that they are not Xstart sessions.

To Create Passive Sessions:

1. Run **Xmanager**, and select [Session Manager] from the [View] menu.
2. Select XMDCP in the sessions category on the left.
3. Point to [New] in the [File] menu and select [New Session Wizard]. The **New Session Wizard** is displayed.
4. Select *None (Passive)* in [Method] and click [Next].
5. Select a server profile from [X Server Profile] and click [Next].
6. Enter a session name in [Name].
7. Click [Finish].

Note
When a passive session is executed, Xmanager enters a mode in which it stands by for an X application connection. Users can then run a remote X application by using Xstart or a terminal program, such as telnet.

To Create XDMCP Query/Broadcast/Indirect/Secure XDMCP Session:

1. Run **Xmanager**, and select [Session Manager] from the [View] menu.
2. Select XDMCP in the sessions category.
3. Point to [New] in the [File] menu and select [New Session Wizard]. **New Session Wizard** is displayed.
4. Select *XMDCP Query*, *XDMCP Broadcast*, *XDMCP Indirect,* or *Secure XDMCP* in [Method].
    Note
    XDMCP Query connections are made directly with a designated host and the GUI login screen can be brought to a user's window.
    XDMCP Broadcast connections are a method where Xmanager opens the Chooser dialog box and lists hosts available for connection.
    XDMCP Indirect connections are similar to XMDCP Broadcast connections. However, the Chooser

dialog box is displayed by a designated remote host, not Xmanager.
Secure XDMCP connections can be used when Xmanager is inside a firewall or a private network and the remote host is outside the firewall or the private network and thus users cannot make a direct XDMCP connection. If the SSH server is in operation on this remote host, XDMCP connections with the remote host can be achieved utilizing SSH tunneling of the Secure XDMCP connection.

5. Enter the remote host name or IP address in [Host] and click [Next].
6. Select server profile from [X Server Profile] and click [Next].
7. Enter a session name in [Name].
8. Click [Finish].

To Create Shortcuts to Static Sessions:

1. Run **Xmanager**.
2. Right-click on a session.
3. Select [Create Shortcut].

To Send Sessions through E-mail:

1. Run **Xmanager**.
2. Right-click on a session.
3. Point to [Send To] and select [E-Mail Recipient].

To Bring Sessions into Xmanager:

1. Drag a session from an external folder.
2. Drop it into the **Xmanager** window.

Note
Only static sessions saved in a file can be dragged and dropped. Automatic sessions cannot be brought in.

To Share Sessions with Other Users:

1. Run **Xmanager**.
2. Right-click on a session.
3. Select [Sharing].

Note
This task requires administrative permissions. Shared sessions are moved to a shared folder. By default, Xmanager has Shared sessions disabled. Shared sessions can be shown by navigating to the [Tools] menu and selecting [Options].

To Save Automatic Sessions as a Static Session:

1. Run **Xmanager**.
2. Select an automatic session and right-click on it.
3. Select [Save As].

5.4 RDP Sessions

Xmanager allows users to manage XDMCP, Xstart sessions as well as Xshell and Xftp sessions conveniently in one location. Users can also create, launch, and manage Microsoft Remote Desktop (RDP) sessions directly from within Xmanager.

How to Create an RDP Session:

1. Open **Xmanager**
2. Point to ‘New’ under the ‘File’ Menu and select ‘Xmanager RDP Session.’
   Result: A new session properties box will appear.
3. In the ‘Session’ field enter the session’s name. Enter characters suitable for a file name.
4. In the ‘Host’ field enter the name or IP address of the Windows device you want to connect to.

5. In the ‘Port Number’ field enter the listening port of the remote desktop you want to connect to. The default port is 3389.
6. Under [Login] enter the remote desktop’s username and password.
7. Click ‘OK’ to save the session.

How to Run an RDP Session in a New Window/New Tab:

1. Open **Xmanager**
2. Select Xmanager RDP in the Session Manager.
3. Right click the RDP session file you want to run from the Xmanager RDP session list.
4. From the context menu, select ‘Open in new window’ or ‘Open in new tab.’

- **Note**
  If a session is opened via a mouse double-click, the session file opens in either a new window or new tab depending on the select default open behavior. The default open behavior can be changed under ‘Tools’ -> ‘Default Open Behavior.’

RDP Session Properties

- **Window Size**
  The window size of the remote desktop.
  - **Full Screen**
    Local desktop size.
  - **Work space**
    This is the size of the Xmanager tab window.
  - **Custom**
    If you don't see the size you want among the sizes listed, you can designate your own.
- **Change Screen size**
  You can determine how to change the screen size of the remote desktop window when the size of the Xmanager window changes.
  - **Not used**
    Regardless of the size of Xmanager's work area, the size determined by the Window Size is used. If the Xmanager workspace is larger, the remote desktop appears in the middle of the screen. If it is smaller, a scroll bar appears.
  - **Use Smart Resizing**
    The size determined in the window size above is adjusted to the size of the Xmanager window through the picture zoom function. If the size of the remote desktop is larger than the work area, the large horizontal and vertical portions are displayed reduced. However, the opposite case is not shown enlarged. Because the picture reduction function is used, the aspect ratio of the remote desktop may not be correct or the image quality may not be clear.
  - **Use Smart Reconnect**
    The size of the remote desktop is the same as that of the Xmanager window. If the size of the Xmanager window changes, it changes the size of the remote desktop accordingly. No reconnection required.
  - **Use legacy Reconnect**
    The size of the remote desktop is the same as the Xmanager window. If the size of Xmanager has changed, it terminates the session and runs the session again with the changed size. It may take some time to reconnect after the session ends.
- **Screen Scale**
  You can set the screen scale of the remote desktop. Monitors with high pixel density require increased desktop scaling. When using an RDP session, you can select Auto to match the default scaling for your monitor, or to launch the remote desktop at a scaling that you specify.
- **Color**
  You can choose the color depth for your remote sessions. If you limit the color depth, the picture quality may

be slightly lower or you may not be able to use the graphical effects of the remote window, but you can expect fast operation if the network is slow.

- **Keyboard**
  Determines whether the remote desktop uses the combination keys used in Windows, such as the Alt+Tab and Window+Tab keys.
  - **On the remote computer**
    Have the remote desktop use the combination keys.
  - **On this computer**
    Remote Desktop does not use the combination keys.
- **Share this computer's drives with the remote computer**
  You can use the drives of the PC where Xmanager is installed by sharing it on a remote desktop.
- **Remote audio playback**
  You can choose where to play sounds originating from the remote desktop.
  - **Play on this computer**
    Play locally.
  - **Do not play**
    Does not process sound.
  - **Play on remote computer**
    The remote desktop processes that sound.
- **Remote audio recording**
  You can use your local microphone in a remote desktop session.
  - **Record from this computer**
    Use the local microphone for recording or voice chatting in remote sessions.
  - **Do not record**
    No local microphone is used, so any recording or voice chatting is not available.

5.5 VNC Sessions

Xmanager allows users to create, launch, and manage VNC(Virtual Network Computing) sessions directly from within Xmanager.

How to Create an VNC Session:

1. Open **Xmanager**
2. Point to 'New' under the 'File' Menu and select 'VNC Session.'
   Result: A new session properties box will appear.
3. In the 'Session' field enter the session's name. Enter characters suitable for a file name.
4. In the 'Host' field enter the name or IP address of the device you want to connect to.
5. In the 'VNC Port' field enter the listening port of the remote server you want to connect to. The default port is 5901.
6. In the [VNC Password], enter the password set on the VNC server running on the remote device.
7. Click 'OK' to save the session.

How to Run an VNC Session in a New Window/New Tab:

1. Open **Xmanager**
2. Select VNC in the Session Manager.
3. Right click the VNC session file you want to run from the VNC session list.
4. From the context menu, select 'Open in New window' or 'Open in New tab.'

- **Note**
  If a session is opened via a mouse double-click, the session file opens in either a new window or new tab depending on the select default open behavior. The default open behavior can be changed under 'Tools' -> 'Default Open Behavior.'

5.6 Session Properties Setting

A session file has basic connection information, such as a host name and the port number. Additionally, users can configure XDMCP settings, a connection address, a server profile, and a display number.

To Change a Session File's Connection Information:

1. Run **Xmanager**.
2. Right-click on a session file.
3. Select [Properties]. The **Session Properties** dialog box is displayed.
4. Modify connection information in the [Connection] section of the [General] tab.

Note
For details about XDMCP session and Xstart session properties, see 'XDMCP Session Properties' and 'Xstart Session Properties' respectively.

To Allocate a Display Number:

1. Start **Xmanager**.
2. Right-click on a session file.
3. Select [Properties]. The **Session Properties** dialog box is displayed.
4. Click [X Server] tab.
5. Turn off [Allocate display number automatically].
6. Enter a display number in [Display Number].
7. Click [OK].

Note
In case the display number is automatically allocated, each session holds an intrinsic display number starting from the default display number set in the profile. When several Xmanager sessions are executed, each session gets a unique display number and it is displayed on the title bar of Xmanager (e.g. [:0.0]). The first number is the display number and the second number is the screen number. In Xmanager, the screen number is always 0.
Display numbers must be a value between -4976 and 32767. Xmanager obtains TCP port numbers by adding 6000 to a display number. For example, if a user enters the number 10 in [Display Number], Xmanager communicates with X applications using TCP port 6010. Some UNIX servers cannot recognize a three-digit number. Therefore, it is recommended to use a number smaller than 100. Some systems do not support X window's default starting port of 6000. In this case, users can utilize negative values (-) such as port 5999(-1), 5998(-2), etc.

To Designate a Specific Profile to a Session:

1. Run **Xmanager**.
2. Right-click on a session file.
3. Select [Properties]. The **Session Properties** dialog box is displayed.
4. Click [X Server] tab.
5. Select a profile from [Server Profile] list.
6. Click [OK].

5.6.1 XDMCP Session Properties

The following are descriptions of connection-related items in the XDMCP Session Properties. The items are displayed in the [General] tab of the **XDMCP Session Properties** dialog box.

Method
The session connection methods are *None (Passive)*, *XDMCP Query*, *XDMCP Broadcast*, *XDMCP Indirect,* and *Secure XDMCP*.
For descriptions of each connection method, see 'Static XDMCP Session'.

Host
Enter the remote host name or IP address for connection.
Check if a display manager is in operation in the remote host. Most UNIX/Linux distros use **dtlogin**, **kdm**, **gdm, lightdm**, or **xdm** as the display manager.

Port Number
Enter remote display manager port number. The default value is UDP 177.

Use Default
Set port number as the UDP 177 default value.

Connection Address
This option is necessary when users connect using port forwarding in a limited network environment such as a firewall or proxy server and when automatic connection address does not function properly due to XDM server settings even if *Secure XDMCP* connection is selected. When the user's Windows resides in a private network with a firewall, Xmanager cannot get a remote login window with an XDMCP connection since the firewall blocks incoming connections. Thus, the remote display manager will not be able to reach Xmanager on the user's Windows PC. To use this feature, users need to allocate a listening port in the firewall and forward incoming connections to your Windows.

Address Type
Select *User Defined* when using a proxy server or attempting XDMCP connection in an environment blocked by a firewall. When using Secure XDMCP, if *Automatic* of connection address fails, select *IP address of SSH server* or *Loopback Address (127.0.0.1)*.

IP Address
If [Address Type] is selected as *User Defined*, enter proxy server or firewall server IP address. The remote display manager attempts the connection using this address and the proxy server forwards the connection to the user's system.

Port Number
If [Address Type] is selected as *User Defined*, designate a TCP port number allocated to a proxy server and standing by for port forwarding.
For example, let's assume that a user's computer uses 192.168.1.100, a private IP address, and the firewall server uses 192.168.1.1, a private IP address. Additionally, the firewall uses 210.100.xxx.10, a public IP address, for an external Internet connection, and the UNIX host IP address is 210.100.xxx.100.
In this case, you need to configure the firewall to forward incoming connections (210.100.xxx.10, port number 6010) to **Xmanager** (192.168.1.100, port number 6010) on your Windows. This is called port forwarding. For this setting, make an inquiry to the firewall system administrator.
Now, enter 210.100.xxx.100 in the [Host] box of [Connection] field, and select *User Defined* as [Address Type] in [Connection Address]. Then, enter 210.100.xxx.10 in [IP Address] and enter 6010 in [Port Number]. Click [X Server] tab, clear [Allocate display number automatically] option and enter 10 (TCP 6010) in [Display Number].
The [Connection Address] setting process when connecting with an external host through a router is described in 'Firewall-related Setting'.

5.6.2 Xstart Session Properties

The following are descriptions of connection-related items in Xstart session properties. The items are displayed in the [General] tab of the **Xstart session properties** dialog box.

Host
Enter the remote UNIX/Linux host name or IP address. It is faster and more stable to enter an IP address than a host name, because Xstart does not have to connect to a name server.

Protocol
Select a protocol for remote host connection. **Xstart** supports *SSH*, *TELNET*, *RSH*, *REXEC*, *RLOGIN* and *LOCAL* protocols. Before selecting a protocol, be sure to check whether or not the remote host supports the protocol.

SSH is a protocol for secure connections with a remote host. SSH provides Public Key User Authentication, powerful data encryption, and X11 forwarding functions. Using the SSH protocol, a remote X application can be executed securely using the powerful encryption, even in a network environment vulnerable to security. Additionally, SSH allows for convenient connections to a host located on the other side of a firewall. A user on a private network can thus run an X application on another network using the X11 forwarding function.

TELNET is a legacy protocol for using a remote terminal. It is supported by most servers, such as UNIX, Linux and VMS. It is not typically utilized in modern systems because of its weak security.

RSH is a simple protocol for connecting with a remote host and running a designated command. It does not require a password and should be used cautiously when security is a concern.

REXEC is a protocol for running a command in a remote host. Although the functions are almost similar to those of RSH, REXEC requires a password for connection.

RLOGIN is a simple program for connecting with a remote host and obtaining login shells. Although similar to TELNET, RLOGIN authenticates users in a similar method to RSH.

LOCAL is for running an X application installed on a user's PC, not a remote host.

- **Note**
  For TELNET, RSH, REXEC, and RLOGIN, the latest UNIX/Linux versions do not permit connections with the default configurations.

Setup
Open the **Protocol Setup** dialog box in relation to the protocol selected and set the connection port, timeou,t and options by protocol.

User Name
Enter the remote host user account.

Authentication
Select an authentication method among *Password, Public Key, Keyboard Interactive*, GSSAPI and PKCS11. If the selected authentication method is not supported by the SSH server, a dialog box asking about the user authentication method is displayed during connection.

- **Note**
  If the PC running Xshell is utilizing an Xshell supported Kerberos module, Xshell can only automatically authenticate to the SSH server if GSSAPI authentication is selected.

Execution Command
Enter a command to be executed in the remote host.
For example, if a user executes **xterm**, the execution command is as follows:
/usr/bin/X11/xterm –display $DISPLAY
The "$DISPLAY" variable is converted to an appropriate value by **Xstart**. In general, it is converted to "192.168.1.100:0.0" when the IP address of your Windows is "192.168.1.100". To designate the value directly, the following command is executed:
/usr/bin/X11/xterm –display 192.168.1.100:0.0
Additionally, the '$PCADDR' variable and the '$DISPNO' variable can be converted. In this case, the execution command is as follows.
/usr/bin/X11/xterm –display $PCADDR:$DISPNO
If a user's PC uses several IP addresses, **Xstart** automatically changes them to appropriate values.
If utilizing the SSH protocol, the DISPLAY is automatically set according to the X11 forwarding protocol, so the '-display $DISPLAY' option is not required. In this case, attempting to change the $DISPLAY variable via the command box will be ignored by Xstart.

Registered Command (Direction Key Button)
Click this button to select a predefined command on a menu. By selecting a command on the menu, users can enter a long commands with just a single click.

Select [Add/Remove] to display the **Registered Commands** dialog box. In the dialog box, register frequently used commands.

Show connection status window
Select this option to check the connection status or messages transferred from a remote host. This option is useful when diagnosing why **Xstart** fails to run an X application. While the connection status window allows for simple input/output, it is not suitable for terminal work related to the connection status or error messages.

5.6.3 SSH Protocol Setting

Set the following SSH-related options for an Xstart session or a Secure XDMCP session in which the SSH protocol is selected.

> **Note**
> To set the SSH protocol, designate the protocol as *SSH* in the 'Xstart Session Properties' [General] tab and click [Setup]. Alternatively, users can designate the connection method as *Secure XDMCP* in the 'XDMCP Session Properties' [General] tab and click [Setup].

Secure XDMCP Setup

Set the following SSH-related options for an Xstart session or a Secure XDMCP session in which the SSH protocol is selected.

SSH Tab

The SSH server host is different from the XDMCP server
Secure XDMCP is a connection method that allows X clients to connect to the PC's **Xmanager** through SSH tunneling. If the SSH server is not running on the XDM host server, a proxy server for SSH tunneling is required. This option is to configure this SSH proxy server.

Host
Enter the host name or IP address of the proxy server for SSH tunneling. In this case, users need to configure the SSH proxy server so that it can bind to not only loopback address (127.0.0.1) but also to external connections.

Port Number
Enter port number to use in SSH connection.

Use Default
Set [Port Number] as 22, the SSH protocol default port.

Preferred Version
Select an SSH protocol version to use. SSH2 is recommended since it provides better security and more functionalities than SSH1.

Send keep alive signal
Send a keep alive signal to a remote host. This function is used to prevent disconnection while a user is temporarily absent. In some network environments, a gateway or a firewall system may terminate connections without notice when the connection is idle for a specified period of time.

User Name
Set the user name used to connect to the SSH server.

Method
Select the method to use for user authentication. Support SSH authentication methods include Password, Public Key, Keyboard interactive, GSSAPI, and PKCS#11. If using the GSSAPI or PKCS#11 methods, click the [Setup] button and enter the required information.

Password
If the Password or Keyboard interactive method has been selected, the password should be entered here.

User Key
If the Public Key method has been selected, the user can specify which user key to use. Click [Browse] to select the user key. Users can also create, modify, delete, import, and export user keys from the User Key dialog box. For more information regarding Public Keys and user key management, please see "**Public Key User Authentication**"and "**User Keys Dialog Box".**

Passphrase
If the Public Key method has been selected, the user key's passphrase should be entered here. The passphrase of the user key can be changed in the User Key dialog box.

Use SSH authentication agent (Xagent)
If opting to use Xagent, Public Key authentication is attempted initially.
Xagent is an SSH authentication agent. **Xagent** holds user keys that are used for public key authentication and passes the key to the SSH client when required.
Xagent maintains a list of all SSH client user keys, and if required, prompts the user for a key passphrase. Once the correct key passphrase in inputted, Xagent unencrypts the key and it is stored in memory. Therefore, with **Xagent**, users can enter a passphrase once and use the key multiple times.

Options Tab

Encryption
Encryption algorithms are used to encrypt and decrypt network traffic. Users can select their preferred algorithms from the list. If <*Cipher List*> is selected, several algorithms can be tried in order of preference. To modify <*Cipher List*>, click [Edit].

MAC
MAC(Message Authentication Code) ensures that data transferred through a network is not changed by a third person. It provides increased security of the SSH2 protocol over SSH1. Users can select their preferred MAC algorithms from a list. If <*MAC List*> is selected, several algorithms can be tried in order of preference. To modify <*MAC List*>, click [Edit].

Key Exchange
These are the options for the SSH initial key exchange. User can select the desired algorithm from the list. Keep in mind that if the server does not support the selected algorithm, the connection will fail.

Compress network data(using ZLIB compression)
Select this option to compress all data traffic with the ZLIB algorithm. Compression will provide better performance in a slow network environment. Depending on the X application being used, network data can be reduced between 15%-80%.

Tunneling Tab

Secure XDMCP sessions or Xstart SSH protocol sessions utilize X11 forwarding (TCP/IP forwarding using the SSH protocol) to use X applications. User can also use general forwarding (SSH tunneling) and can list, add, edit, and remove SSH tunneling channels registered in the session.

List Box
This area list the TCP/IP forwarding rules stored I nthe current sessoin file.

Add
Users can add a new TCP/IP forwarding rule.

Type(Direction):

- When using Local Forwarding, the connection through the local PC's listening port is forwarded to a specific port of the destination host.

- When using Remote Forwarding, the connection through the remote host's listening port is forwarded to a specific port of the destination host.
- Dynamic Forwarding works in the same way as Local Forwarding except the destination host is not specified. For reference, Dynamic Forwarding uses the SOCKS protocol with a default port number of 1080.

Source Host: This is the host to receive packets during forwarding. If the using Locol Forwarding, users can generally enter localhost here. If an IP address is entered, it can be set seperately for each network device.

Listening Port: This is the port number of the host to receive packets during forwarding. If an IP address was entered as the source host, this can be set separately for each network device.

Accept local connections only: If this option is turned on, access to the specified port will be blocked for other PCs or hosts. Only the locally requested forwarding will be processed.

Destination Host: Enter the host name or ip address where the arrived packets at the source port of the source host will be forwarded.

Destination Port: This is the port number of the destination host to which arriving packets at the source port of the source host will be forwarded.

Description: Enter a description of this forwarding rule.

Edit
Edit the selected forwarding rule from the list box.

Remove
Removes the selected forwarding rule from the list box.

SSH Protocol Setup of Xstart sessions

Set the following SSH-related options for an Xstart session or a Secure XDMCP session in which the SSH protocol is selected.

General Tab

Preferred Version
Select an SSH protocol version to use. SSH2 is recommended since it provides stronger security and more functionalities than SSH1.

Port Number
Enter port number to use in the SSH connection.

Use Default
Set [Port Number] as 22, the SSH protocol default port.

Send keep alive signal
Send a keep alive signal to the remote host. This function is used to prevent disconnection while a user is temporarily absent. In some network environments, a gateway or a firewall system may terminate connections without notice when the connection is idle for a specified period of time.

Method
Select the method to use for user authentication. Support SSH authentication methods include Password, Public Key, Keyboard interactive, GSSAPI, and PKCS#11. If using the GSSAPI or PKCS#11 methods, click the [Setup] button and enter the required information.

User Key
If the Public Key method has been selected, the user can specify which user key to use. Click [Browse] to select the user key. Users can also create, modify, delete, import, and export user keys from the User Key dialog box. For more information regarding Public Keys and user key management, please see "**Public Key User Authentication**"and "**User Keys Dialog Box".**

Passphrase
If the Public Key method has been selected, the user key's passphrase should be entered here. The passphrase of the user key can be changed in the User Key dialog box.

Use SSH authentication agent (Xagent)
If opting to use Xagent, Public Key authentication is attempted initially.
Xagent is an SSH authentication agent. **Xagent** holds user keys that are used for public key authentication and passes the key to the SSH client when required.
Xagent maintains a list of all SSH client user keys, and if required, prompts the user for a key passphrase. Once the correct key passphrase in inputted, Xagent unencrypts the key and it is stored in memory. Therefore, with **Xagent**, users can enter a passphrase once and use the key multiple times.

Options Tab

Encryption
Encryption algorithms are used to encrypt and decrypt network traffic. Users can select their preferred algorithms from the list. If <*Cipher List*> is selected, several algorithms can be tried in order of preference. To modify <*Cipher List*>, click [Edit].

MAC
MAC(Message Authentication Code) ensures that data transferred through a network is not changed by a third person. It provides increased security of the SSH2 protocol over SSH1. Users can select their preferred MAC algorithms from the list. If <*MAC List*> is selected, several algorithms can be tried in order of preference. To modify <*MAC List*>, click [Edit].

Key Exchange
These are the options for the SSH initial key exchange. User can select the desired algorithm from the list. Keep in mind that if the server does not support the selected algorithm, the connection will fail.

Compress network data(using ZLIB compression)
Select this option to compress all data traffic with the ZLIB algorithm. Compression will provide better performance in a slow network environment. Depending on the X application being used, network data can be reduced between 15%-80%.

Allocate a terminal before executing the command
This option is selected when you want to allocate a virtual terminal on the remote host and then run a command on the terminal. Virtual terminals are required by several X applications. When virtual terminals are allocated, shell environment variables are set as per the general login envirorment.

Tunneling Tab

Secure XDMCP sessions or Xstart SSH protocol sessions utilize X11 forwarding (TCP/IP forwarding using the SSH protocol) to use X applications. User can also use general forwarding (SSH tunneling) and can list, add, edit, and remove SSH tunneling channels registered in the session.

List Box
This area list the TCP/IP forwarding rules stored I nthe current sessoin file.

Add
Users can add a new TCP/IP forwarding rule.

Type(Direction):

- When using Local Forwarding, the connection through the local PC's listening port is forwarded to a specific port of the destination host.
- When using Remote Forwarding, the connection through the remote host's listening port is forwarded to a specific port of the destination host.
- Dynamic Forwarding works in the same way as Local Forwarding except the destination host is not specified. For reference, Dynamic Forwarding uses the SOCKS protocol with a default port number of 1080.

Source Host: This is the host to receive packets during forwarding. If the using Locol Forwarding, users can generally enter localhost here. If an IP address is entered, it can be set seperately for each network device.

Listening Port: This is the port number of the host to receive packets during forwarding. If an IP address was entered as the source host, this can be set separately for each network device.

Accept local connections only: If this option is turned on, access to the specified port will be blocked for other PCs or hosts. Only the locally requested forwarding will be processed.

Destination Host: Enter the host name or ip address where the arrived packets at the source port of the source host will be forwarded.

Destination Port: This is the port number of the destination host to which arriving packets at the source port of the source host will be forwarded

Description: Enter a description of this forwarding rule.

Edit
Edit the selected forwarding rule from the list box.

Remove
Removes the selected forwarding rule from the list box.

5.7 Xmanager Window Settings

The **Xmanager Window** is similar to Explorer and consists of menus, standard buttons, an address bar, workspace, and a status bar.
The Workspace consists of a session category tree and icons list. Session categories include XDMCP session, Xstart session, Xshell session, and Xftp session.
An option to show or hide Xshell and Xftp sessions is provided in the **Options** dialog box [Sessions] tab.
Additionally, the XDMCP session folder and Xstart session folder can be designated. When several users designate a network folder as a session path, all users can use the same sessions.

To Change Session Path:

1. Run **Xmanager**.
2. Select [Options] in [Tools] menu. The **Options** dialog box is displayed.
3. Click [Sessions] tab.
4. Enter a session folder to change in [Session Path].

Note
To restore the original session path, click [Restore Default Session Path].

5.7.1 Column Setting

The **Columns** dialog box allows you to adjust the columns of **Xmanager** when it is in the [Details] view.
To Change Column Information:

1. Run **Xmanager**.
2. Select [Columns] from [View] menu. The **Columns** dialog box is displayed.
3. Select or unselect a column to show or hide.

5.8 Create a Session Folder

Users can connect all sessions at once by managing sessions with a folder. Additionally, session management, creations, deletion, categorization, etc. becomes much easier when using session folders.

To Create a New Session Folder:

1. Run **Xmanager**.
2. Point to [New] in the [File] menu and select [Folder].
3. Enter folder name.

5.9 Export

Exported sessions are saved into a single convenient file. When this file is imported from another computer where Xmanager is installed, the imported sessions may be used without additional setup.

To Export Sessions:

1. Run **Xmanager**.
2. Select [Export] from the [File] menu. The Import/Export Sessions wizard is displayed.
3. Select a product for which to export sessions and click [Next].
4. Select a location to save the exported sessions file and click [Next]. The sessions export results are displayed.
5. Click [Finish] to complete sessions export.

5.10 Import

Xmanager can import sessions from prevoius versions or session files exported from other computers.

To Import Sessions:

1. Run **Xmanager**.
2. Select [Import] from the [File] menu. The Import/Export Sessions wizard is displayed.
3. Directly enter file location or click […] to browse for a session file.
4. Under [Action] user can select how to convert the session file. Certain information from the original session file may not be converted during the conversion.
5. Select how to handle session files [If session exists].
6. Click [next] to move to the next stage. Products included in the file and session counts are displayed.
7. Select a product for which to import a session and click [Next]. Sessions are imported and the results are displayed.
8. Click [Finish] to complete the session import.

6 Connection

The following details how to use **Xmanager** and **Xstart** for a connection to a remote host. In general, **Xmanager** is used for connections to a remote host using the XDMCP protocols. **Xstart** is used when running single X applications in a remote host.

6.1 Connect using Xmanager

Xmanager broadcasts an XDMCP query message to the local network or a designated host and automatically displays hosts that respond to the query message.

To Connect to an XDMCP Host:

1. Run **Xmanager**. Hosts available for connection are automatically displayed.
   - **Note**
     To list hosts available for connection on the local network, the [Search for local hosts (XDMCP Broadcast)] option must be turned on. For settings on local host search, see 'Automatic XDMCP Session'.
2. Double-click a host for connection. **Xmanager server** is initialized and a connection to the host is made with the XDMCP protocol.
   - **Note**
     To refresh the list of hosts available for XDMCP connection, click [View] -> [Refresh].

To Connect to a Host from the Address Bar:

1. Run **Xmanager**.
2. Enter host name or IP address for connection in the address bar.
3. Press the Enter key.

- **Note**
  For additional details on using the address bar, see 'Xmanager Address Bar'.

6.2 Xmanager Address Bar

The Xmanager address bar is a convenient way to connect to a host on the fly. The rules for addresses entered in address bar are outlined as follows.
hostname (or ipaddress)
xdmcp://*hostname*
xstart://*sessionname*
xsession://*sessionname*
rdp://[username[:password]@]hostname[/]
vnc://hostname[: *port*][?VncPassword= *password*]
ssh://[*username*[:*password*]@]*hostname*[:*port*][/]
telnet://[*username*[:*password*]@]*hostname*[:*port*][/]
rlogin://[*username*[:*password*]@]*hostname*[:*port*][/]
ftp://[*username*[:*password*]@]*hostname*[:*port*][/]
sftp://[*username*[:*password*]@]*hostname*[:*port*][/]

The usable protocols are *xdmcp*, *xstart*, *xsession*, *ssh*, *telnet*, *rlogin*, *ftp, rdp* and *sftp*. When no protocol is designated, xdmcp is used as the default protocol. The *xdmcp* protocol uses UDP 177 port as the default port.

Default port values for the protocol

프로토콜	기본값 및 설명
xdmcp	UDP 177. This value can be changed in the remote server's XDMCP daemon settings.
rdp	TCP 3389
vnc	TCP 5901. TCP 5900 is the default in the VNC protocol, but 5901 is the default in Xmanager's VNC. This is because VNC servers usually run on Unix/Linux starting at number 5901.
ssh	TCP 22
telnet	TCP 23
rlogin	TCP 513
ftp	TCP 21
sftp	TCP 22

Examples:

URL	Description
myhost xdmcp://*myhost*	Connect to *myhost* using XDMCP protocol.
xstart://*mysession*	Run an Xstart session named *mysession*.
xsession://*cdesession*	Run a static session named *cdesession*.
rdp://*user:pass@myhost/*	Connect with myhost's **RDP** (Remote Desktop Protocol) protocol. The username and password are automatically sent after connection.
vnc://*myhost*:5902? VncPassword=*secret*	Connect to the server waiting on TCP port 5902 among *myhost*'s VNC servers. The password to access this server is 'secret'.
ssh://*myhost*:*22*/	Run **Xshell** and connect to *myhost* port 22 using an SSH protocol. To run this command, the **Xshell** program must be installed in the computer.

URL	Description
telnet://*user*:*pass*@*myhost*	Run **Xshell** and connects to *myhost* using a TELNET protocol. User name and password are automatically transferred after connection. To run this command, the **Xshell** program must be installed in the computer.
rlogin://*user*@*myhost*	Run **Xshell** and connect to *myhost* using an RLOGIN protocol. User name is automatically transferred after connection. To run this command, the **Xshell** program must be installed in the computer.
ftp://*anonymous*@*myhost*	Run **Xftp** and connect to *myhost* using an FTP protocol. User name is automatically transferred after connection. To run this command, the **Xftp** program must be installed in the computer.
sftp://*user*:*pass*@*myhost*/	Run **Xftp** and connect to *myhost* port 22 using an SFTP (secure shell fire transfer protocol). User name and password are automatically transferred after connection. To run this command, the **Xftp** program must be installed in the computer.

6.3 Secure XDMCP Connection

A Secure XDMCP connection is a safer and simpler XDMCP connection using the SSH protocol.
SSH protocols allow for, not only a secure connection, but also a convenient X11 connection in network environments blocked by a firewall, a masquerade server, or an NAT gateway.
To use Secure XDMCP, an SSH server must be in operation on a remote server and the X11 forwarding function must be activated.
For an OpenSSH server, modify the setup file (/etc/ssh/sshd_config) as follows.
X11Forwarding yes
For a Secure Shell Communications Security server, modify the setup file (/etc/ssh2/sshd2_config) as follows.
AllowX11Forwarding yes

To Create a Secure XDMCP Session:

1. Run **Xmanager**.
2. Click [XDMCP Session] in [New].
3. Select [Method] as *Secure XDMCP* in the **Session Properties** dialog box and enter the necessary information in [Connection Address].

Note
If a host is displayed in the list of XDMCP sessions, you can easily create a Secure XDMCP session by right clicking the host and selecting [Save as SSH Connection] in the context menu.

To Set a Secure XDMCP Session When the XDMCP Host is Different from SSH Server:

1. Right click the desired XDMCP session and click [Properties]. The **Session Properties** dialog box is displayed.
2. Set [Method] as Secure XDMCP, and click [Setup] on the right. The **Secure XDMCP Setup** dialog box is displayed.
3. Activate [Host] by selecting [The SSH server host is different from the XDMCP server].
4. Enter the SSH server host name or IP address in [Host].
5. Enter user information in the [User Authentication] field.

6. Click [OK] to save.

Note
If the SSH server is different from the XDMCP host, enter the SSH server host name or IP address for tunneling. In this case, the user needs to configure the SSH proxy server so that it can bind to not only loopback address (127.0.0.1), but also external connections. For OpenSSH, set the GatewayPorts value to yes in the SSH server setup file.

To Connect with a Secure XDMCP Session:

1. Run **Xmanager**.
2. Double-click the Secure XDMCP session.

6.4 Connect with Xstart

Xstart supports SSH, TELNET, RLOGIN, REXEC, RSH, and LOCAL protocols. To use each protocol, the corresponding service daemon must be executed in the remote host. The LOCAL protocol is used when an X application is in the user's PC.

To Run X Application with SSH Protocol:

1. Run **Xstart** from the **Tools** folder of the **Xmanager** folder.
2. Click [New]. The **New Session** dialog box is displayed.
3. Enter new session name and click [OK].
4. Enter remote UNIX/Linux host name or IP address in [Host].
5. Select *SSH* from [Protocol] list.
6. Click [Setup] to set SSH protocol options, such as port number or encryption options.
   Note
   For more information on SSH Protocol Settings, see '**SSH Protocol Setup of Xstart sessions**'.
7. Enter remote host user account name in [User Name].
8. Select an authentication method in [Authentication] and set password, etc.
   Note
   For more information on each authentication method's settings, see '**Xstart User Authentication Setting**'.
9. Enter a command to run in the remote host in [Command]. To run **xterm**, enter a command as follows: /usr/bin/X11/xterm –ls
   Note
   For SSH connections, the DISPLAY variables are automatically set with the values decided by the SSH server.
10. Click [Run].

To Run Remote X Application with the TELNET Protocol:

1. Run **Xstart**.
2. Click [New]. The **New Session** dialog box is displayed.
3. Enter a new session name and click [OK].
4. Enter the remote UNIX/Linux host name or IP address in [Host].
5. Select *TELNET* from [Protocol] list.
6. Click [Setup] to set TELNET protocol options, such as port or timeout.
   Note
   The connection method for RLOGIN, REXEC, and RSH protocols is similar to connections with the TELNET protocol. Set port and timeout in the **Protocol Setup** dialog box. The default port numbers in each protocol are as follows TELNET: 23 REXEC: 512 RLOGIN: 513 RSH: 514
   After a successful login, a shell is allocated by the TELNET and RLOGIN server in the remote host and **Xstart** executes the command in the shell prompt. **Xstart** closes the connection after the designated

timeout and the login shell is ended at the same time. If timeout is 0, connection is not closed while **Xmanager** is running. If a shell is closed, X applications executed on the shell may also close.

7. Enter the remote host user account in [User Name].
8. Only *Password* can be selected in [Authentication]. Click [Setup] to enter the password.
9. Enter a command to be executed in the remote host in [Command]. To run **xterm**, enter the following command: /usr/bin/X11/xterm –ls –display $DISPLAY
10. Click [Run].

To Run Local X Applications with Xstart:

1. Run **Xstart**.
2. Click [New]. The **New Session** dialog box is displayed.
3. Enter a new session name and click [OK].
4. Select *LOCAL* from the [Protocol] list.
5. Enter overall local command path in [Command].
6. Click [Run].

6.4.1 Xstart User Authentication Settings

To Set Password or Keyboard Interactive:

1. Run **Xstart**.
2. Select *Password* or Keyboard Interactive in [Authentication] and click [Setup]. The **Password Setup** dialog box is displayed.
3. Enter password.
4. Select [Save password] and click [OK] to save the entered password in the session.
5. To remove the password, click [Reset password].

Note
Keyboard Interactive authentication works by entering the required value in the message sent from the SSH server. It is typically used when the password changes often or if OTP is utilized. Unless otherwise specified by the server, the initial password value is the same as the user account's password.

To Set Public Key:

1. Run **Xstart**.
2. Select *Public Key* in [Authentication] and click [Setup]. The **Public Key Authentication Setup** dialog box is displayed.
3. Select a user key to use in authentication.
4. Enter passphrase.

Note
For more information on public key settings, see 'Public Key User Authentication'.
For maximum security, directly enter a passphrase upon each connection instead of saving it in a session. When opting to enter the password each time, the 'SSH User Authentication Dialog Box' will prompt for a password when attempting to connect.

To Set Kerberos: Xmanager supports MIT Kerberos and Microsoft's SSPI. This article assumes that you have a working Kerberos server and client. When this session opens, it will attempt to use the Kerberos credentials for the specified user. It must be the same user you defined in the Network Identity Manager.

1. Run **Xstart**.
2. For [Authentication], select GSSAPI and click [Setup]. The **Setup GSSAPI** dialog box appears.
3. Select the type of GSSAPI authentication to use.

Note
If the PC running Xxmanager is utilizing an Xmanager supported Kerberos module, Xmanager can only automatically authenticate to the SSH server if GSSAPI authentication is selected. To connect to another

server using Kerberos authentication from a server using Kerberos authentication, select the 'Allow GSSAPI credential delegation' option.

To set PKCS #11:

1. Run **Xstart**.
2. For [Authentication], select PKCS#11 and click [Setup]. The **Setup PKCS#11** dialog box appears.
3. Enter the path of the middleware program that can connect to the hardware token that contains the user key. Or click […] to browse for it.
4. If the pin number is set in the hardware token, enter the pin number.

6.4.2 Xstart Command Tag Definition

Xstart provides a command tag function to automate repetitive commands. Command tags are entered in [Command].

Tag	Description
<%CR%>	Send CR (Carriage Return, \r) character.
<%LF%>	Send LF (Line Feed, \n) character.
<%SEND="*string*"%>	Send a character string. Xstart does not convert DISPLAY and PCADDR variables in the character string.
<%WAIT="*string1*|*string2"*%>	Stand by for string1 or string2.
<%SLEEP=*n*%>	Sleep for n seconds.
<%POPUP="s*tring*"%>	Open the **Remote execution result** window if a designated character string is received.

All tags are processed in sequence except for the POPUP tag which is valid till the command is completed in its entirety.

Note
Command tags are supported by TELNET and RLOGIN protocols. To use this function in an SSH protocol, select [Allocate a terminal before executing the command] in the [Options] tab of **the SSH Protocol Setup** dialog box. When a terminal is allocated, shell environment variables are set as per the general login environment.

Example

1. The following command is an example of a multi-login. Log in to a host with **Xstart**, and connect to another host using **telnet** and run **xterm**: telnet host2<%CR%><%WAIT="login:"%>root<%CR%> <%WAIT="Password:"%>password<%CR%><%WAIT="$"%>xterm –ls –display $DISPLAY
2. The following command is an example of the display **Remote execution result** window when a character string "assword:" is displayed. This command is useful when password expires in a fixed cycle and a new password must be entered before a command line prompt is displayed: <%POPUP="assword:"%>xterm –ls –display $DISPLAY

6.5 Firewall-related Settings

Special settings are required if a remote host is in another network on the opposite side of a gateway or if there is a firewall between the user's PC and a remote host. This is because **Xmanager** is a server program and remote X applications connect to **Xmanager** in a user's PC.
The keep alive option to retain connections, which is supported by SSH protocols, is useful when a firewall forcefully ends a connection that is idle for a set period of time.
Port-forwarding is required for XDMCP connections when you are in a private network and you connect to a remote host over a router. Once you have configured port-forwarding on the router, you should configure the connection address for XDMCP connections.

To Use Keep Alive Option for SSH Connections in a Firewall Environment:

1. Run **Xstart**.
2. Select a session from the [Session] list.
3. Select *SSH* from the [Protocol] list.
4. Click [Setup]. **SSH Protocol Setup** dialog box is displayed.
5. Click the [General] tab.
6. Select [Send keep alive signal].
7. Click [OK].

To Set Router Port Forwarding:

1. Connect to a router and move to port forwarding setup page.
2. Forward external router ports TCP 6000 ~ 6010 to the 6000 ~ 6010 ports in the user PC. If the user PC IP address is 192.168.1.2: **Router Port PC Port Address**6000 6000192.168.1.2 6001 6001192.168.1.2…6010 6010192.168.1.2
   - **Note**
     The router port number does not need to be the same as the PC port number. However, X applications attempt connection with the IP address and the corresponding router port. Since router forwards packets to a PC port according to the port forwarding rules, the display number designated in **Xmanager** session files must be the same as the port designated in router port forwarding rules. The **Xmanager** display number added with 6000 becomes the port number.
3. Save settings.
4. In the Xstart session, values relating to –display options must be designated as display numbers relevant to the router IP address and port number of the PC designated in the router port forwarding settings. For XDMCP session, [Connection Address] must be set.
   - **Note**
     For port forwarding settings, see your router's manual.

To Set XDMCP Session Connection Address:

1. Run **Xmanager**.
2. Right-click on a session for which to set the connection address.
3. Select [Properties].
4. Click the [General] tab.
5. Select *User Defined* as [Address Type] in the [Connection Address] field.
6. Enter router IP address in the [Connection Address] field [IP Address] box.
7. Enter a port designated in the router port forwarding setting in of the [Connection Address] field [Port Number] box.
   - **Note**
     The port number is a router side port number which is configured to perform port-forwarding from router to PC.
8. Click the [X Server] tab.
9. Unselect [Allocate display number automatically] in the [Display Number] field.

10. Enter a display number in [Display Number] relevant to the port number of the PC designated in the router port forwarding setting.
    - **Note**
      The display number is from the PC port number designated for forwarding from the router to a PC. The port number minus 6000 is the display number.
11. Click [OK].

6.6 Solve Connection Problem

Even if the steps listed above are followed, connection with a remote host may not be successful according to user environments. This section briefly introduces the methods to solve connection-related problems.

To Solve XDMCP Connection Problem:

1. Check the following:
   - Is **dtlogin**, **kdm**, **gdm, lightdm**, or **xdm** being executed in the remote host?
   - Is a login window displayed?
   - Is the remote host in another network?
   - Is there a firewall in between the remote host and user's PC?
   - Is a firewall set in the user's PC?
   - User's PC address may be incorrectly set in the name server.
   - DISPLAY variables may be configured in the user account shell script.
2. Refer to the log message.
   - To view an **Xmanager** log file, point to [Log] in the **Xmanager server** main window system menu and select [File].
   - If a login screen is not displayed in the CDE environment, check /var/dt/Xerrors file. If login fails, check $HOME/.dt/startlog and $HOME/.dt/errorlog files.

- **Note**
  For details on log files, see 'Session Log'.

To Solve Xstart Connection Problems:

1. Run **Xstart**.
2. Select [Show connection status window].
3. Click [Run]. The **Xrcmd: Remote execution result** window opens.
4. Read the message and identify causes of the problem.

- **Note**
  The **Remote execution result** window is a message window showing the connection progress status. A simple command input is possible. However, there are many restrictions in performing tasks, such as terminal emulation. This window only shows the process until a program including an execution command starts, which is **Xstart's** objective.

6.7 Xmanager server Command Line Options

Xmanager server (Xmanager.exe) supports command line options to interface with other user applications. When a user directly executes **Xmanager**, the connection methods and display numbers must be designated as options. The **Xmanager** command line rules are as follows:
Xmanager [-query *hostname*|-broadcast|-indirect *hostname*] [:*digit*]

Command	Description
Xmanager	Run in passive mode using [Default Xstart Profile]. Display number is set as 0, the default value. If it is not available, another value is automatically allocated.
Xmanager :*1*	Run in passive mode using [Default Xstart Profile]. Display number is set as 1. If it is not available, execution is stopped.
Xmanager –query *host*	Connect to a designated host using XDMCP Query connection method. [Default XDMCP Profile] is used. Display number is set as 0, the default value. If it is not available, another value is automatically allocated.
Xmanager –query *host* :*2*	Connect to a designated host using XDMCP Query connection method. [Default XDMCP Profile] is used. Display number is set as 2. If it is not available, execution is stopped.
Xmanager –broadcast	Display XDMCP hosts available for connection in **Chooser** dialog box by forwarding XDMCP Broadcast messages to local network. [Default XDMCP Profile] is used. Display number is set as 0, the default value. If it is not available, another value is automatically allocated.
Xmanager –indirect *host*	Connect to a host using XDMCP Indirect connection method. Remote host opens Chooser window through **Xmanager server**. [Default XDMCP Profile] is used. Display number is set as 0, the default value. If it is not available, another value is automatically allocated.

6.8 Xrcmd Command Line Options

Xstart provides command line option, which enables advanced users to integrate the program with their applications. In reality, **Xstart** only provides a user interface for session creation and management. When a user opens a session using **Xstart**, it executes the **Xrcmd.exe** command and forwards the session information. Therefore, for direct connections, **Xrcmd.exe** must be used, not **Xstart**. **Xrcmd** is found in the folder where **Xmanager** is installed.

The Xrcmd Command Line Rules are As Follows:

Xrcmd –protocol ssh|telnet|rexec|rsh|rlogin|local –host *hostname*
[–user *username*] [-password *password*] [-userkey *keyname*]
[-passphrase *userkeypass*] [-shell] [-zlib] [-status]
[-result] [-dispno *nnn*] [-timeout *nnn*] [-port *nnn*]
-command *remote_command*

***Note**: –command option must be at the end.*

Options:

Tag	Description
-protocol *protocol*	Designate a connection protocol.

Tag	Description
-host *hostname*	Designate a remote host.
-user *username*	Designate remote host user account.
-password *xxxx*	Designate user account password.
-userkey *keyname*	Designate user key name. This option is used only for SSH connection.
-passphrase *userkeypass*	Enter user key passphrase. This option is used only for SSH connection.
-shell	Run a command after shell (terminal) starts. This option is applied only to SSH connection.
-zlib	Compress network data using zlib algorithm. This option is applied only to SSH connection.
-status, -result	Show **Remote execution result** window.
-dispno *nnn*	Designate a display number to be used by **Xmanager server**. If this option is not set, **Xmanager server** automatically allocates an appropriate value.
-timeout *nnn*	Close connection after *nnn* seconds.
-port *nnn*	Designate connection protocol port number. If this option is not set, the default protocol port number is used.
-command *command*	Designate a command to be executed in a remote host.

Ex.:
Xrcmd –protocol telnet –host mylinux –user myname –status
–command /usr/bin/X11/xterm –ls
Xrcmd connects to *mylinux* using a *telnet* protocol and logs in with *myname*. It then executes the *xterm* command on the remote host. The connection status can be checked through the **Remote execution result** window during the course of connection.

7 Server Profile Setting

Server profiles contain **Xmanager server** options such as window modes, fonts, colors, and security options. **Xconfig** displays all **Xmanager** profiles available for use. Users can individually designate a profile for XDMCP and Xstart sessions.
The shared profile is displayed with a hand-shaped icon and can be modified only by users with system administrator permissions. For the default XDMCP profile or the default Xstart profile, the icon is marked with a black tick on top. Double-click an icon to modify the properties of each profile.

7.1 Profile Management

When a user creates a session, initially the default profile is designated to the session. As default profiles, **Xmanager** supports the default Xstart profile and the default XDMCP profile. The default Xstart profile is applied when [Server Profile] is set as *Auto Select* in an Xstart session. The default XDMCP profile is applied when [Server Profile] is set as *Auto Select* in an XDMCP session. All automatic XDMCP sessions use the default XDMCP profile.

To Create a Server Profile:

1. Run **Xconfig**.
2. Select [New] from the [File] menu. A new profile is created in the **Xconfig** window.
3. Double-click the new profile. The **Profile properties** dialog box is displayed.
4. Set options.
5. Click [OK].

To Set a Profile as the Default Xstart Profile:

1. Run **Xconfig**.
2. Right-click on a profile to be used as the default **Xstart** profile.
3. Select [Set as default **Xstart** profile].

To Set a Profile as the Default XDMCP Profile:

1. Run **Xconfig**.
2. Right-click on a profile to be used as the default XDMCP profile.
3. Select [Set as default XDMCP profile].

To Share a Profile with Other Users:

1. Run **Xconfig**.
2. Right-click on a profile to share with other users.
3. Select [Sharing]. A hand-shaped icon is added to the server profile icon.

To Export Profile to Folder:

1. Run **Xconfig**.
2. Drag a profile and drop it into an external folder.

To Import Profile to Xconfig:

1. Run **Xconfig**.
2. Drag a profile from an external folder and drop it into **Xconfig**.

7.2 Window Mode

Xmanager supports Single Window Mode (mainly used in XDMCP sessions) and Multiple Window Mode (mainly used in Xstart sessions). In Single Window Mode, you can customize the size of the root window and add a scroll bar when the X desktop is larger than your Windows desktop.

In Multiple Window Mode, you can select a window manager and the desktop background. Additionally, you can set panning and an auto-raise function to activate a window on mouse focus.

Note
In Single Window Mode, **Xmanager server** opens one large main window. Opening a session with 'Open in new window,' which opens in an entirely new window, and 'Open in new tab,' which opens a new tab within Xmanager, both utilize Single Window Mode. The system menu can be accessed via the title bar when 'Opening in new window' and via the tab menu when 'Opening in new tab.'
In Multiple Window Mode, an **Xmanager server** icon is created in the notification area. To aceess the Xmanager system menu, right-click the icon in the notification area.

To Use Xmanager in Single Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Single Window Mode* from the [Window Mode] list.
5. Click [OK].

To Set Root Window Size in Single Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Single Window Mode* from the [Window Mode] list.
5. Click [Settings]. The **Window Mode Settings** dialog box is displayed.
6. Click the [Single Window Mode] tab.
7. Select an appropriate size from the [Window Size] list.
8. Click [OK].

Note
For *Desktop Size*, run Xmanager server as large as the desktop excluding the task bar.
For *Full Screen*, run Xmanager server as large as the entire screen without the title bar and window frame. Windows task bar is also not displayed.

To Use Multiple Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Multiple Window Mode* from the [Window Mode] list.
5. Click [OK].

To Use Panning in Multiple Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Multiple Window Mode* from the [Window Mode] list.
5. Click [Settings]. The **Window Mode Settings** dialog box is displayed.
6. Click the [Multiple Window Mode] tab.
7. Select [Use Panning].
8. Click [Panning Settings] to set panning options.
9. Set velocity and position in the **Panning Settings** dialog box.
10. Click [OK].

Note
Panning can be used only when the local window manager is used.
This option is useful when the window size is larger than the desktop and some window areas are located

outside the desktop. Each time the mouse pointer moves on a panning position, the panning window moves inside the desktop area by pixels designated in panning velocity.

To Use Auto-Raise in Multiple Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Multiple Window Mode* from the [Window Mode] list.
5. Click [Settings]. The **Window Mode Settings** dialog box is displayed.
6. Click the [Multiple Window Mode] tab.
7. Select [Raise Window Automatically].
8. Click [OK].

To Select Background in Multiple Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Multiple Window Mode* from the [Window Mode] list.
5. Click [Settings]. The **Window Mode Settings** dialog box is displayed.
6. Click the [Multiple Window Mode] tab.
7. Select Background from the [Background] list.
8. Click [OK].

Note

For *Windows Background*, the background is managed by Windows. In this mode, the X root window background cannot be used.
For *X Window Background,* the background is managed by Xmanager. The background changes to the X root window and the mouse pointer changes to an X pointer. In this mode, the Windows icons in the desktop cannot be used.
X Window Background(Transparent) operates the same as X Window Background mode. It looks like Windows Background and you can still see the Windows icons on the desktop, but the icons are not active.

To Select Window Manager in Multiple Window Mode:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [General] tab.
4. Select *Multiple Window Mode* from the [Window Mode] list.
5. Click [Settings]. The **Window Mode Settings** dialog box is displayed.
6. Click the [Multiple Window Mode] tab.
7. Select a window manager from the [Window Manager] list.
8. Click [OK].

Note

The Window manager manages X applications. It adds a title bar, a frame, and system menu to the window. Additionally, it provides functions to change window size, to move window, and to close window. The local window manager looks like Windows and adds a title bar and a frame to an X application just like Windows applications. Remote window managers, such as dtwm, mwm and fvwm, are executed on a remote host and look different from the local window manager.
Xmanager provides *Automatic Switch*, *Remote Only*, and *Local Only* for the window manager modes.
In *Automatic Switch* mode, the window manager is automatically converted. Initially, Xmanager runs a local window manager, and when a remote window manager tries to connect to Xmanager, the local window manager is automatically closed. And if the remote window manager is closed by the user, the local window manager will run once again.
In *Remote Only* mode, the local window manager is not executed. Run remote window manager to manage X

application windows.
In *Local Only* mode, a connection by a remote window manager is not permitted. All X application windows are managed in the same way as Windows applications.
When using remote user desktop environments by running the gnome-session, startkde, etc. commands, the window manager must be set to *Automatic Switch* or *Remote Only* for a smooth experience.

7.3 Connection Option Settings

The keep alive function is useful when a connection is unexpectedly closed while the connection is idle. In some network environments, the gateway or firewall system forcefully disconnects with systems in situations where data transfer is not made for a set period of time.
The automatic closing function is used to automatically close Xmanager when user input is not detected for a set period of time.

To Retain Connections:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Connection] tab.
4. Select [Send TCP keepalive packets when network is idle].
5. Enter a waiting time (seconds) in the idle state in [Timeout].

To Set Automatic Closing:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Connection] tab.
4. Select [Close session when user is idle].
5. Enter a waiting time (minutes) in the idle state in [Timeout].

Note
When Xmanager closes due to automatic closing, all X applications may end unexpectedly and work data may be lost.

7.4 Font Management

Xmanager provides fonts necessary in most systems and applications. However, users may need to directly add new fonts.

To Download and Install Additional Fonts Pack:

1. Go to the **Xmanager** download page: https://www.netsarang.com/en/font-download/
2. Download additional font packs to install.
3. Run the font packs in the user's system.
4. Install fonts pack according to the instructions provided by the install wizard.

Note
When additional font packs are installed, a fonts folder is automatically added to all server profiles, so a new fonts folder does not need to be registered separately in each server profile when using **Xconfig**.

To Change BDF Font to PCF Font:

1. Run **bdftopcf.exe** program as in the following example:
   C:\tmp> %XMANAGER_INSTALL_DIR%\bdftopcf new.bdf –o new.pcf

To Create or Renew FONTS.DIR File Using the Mkfntdir.exe Program:

1. Move to fonts folder and run the **mkfntdir.exe** program:
   %XMANAGER_INSTALL_DIR%\Fonts\NewFonts> ..\..\mkfntdir

To Create and Use Fonts Folder:

1. Create a new folder under the following folder:
   %XMANAGER_INSTALL_DIR%\Fonts
2. Copy new font files to the created folder.
3. Run the **mkfntdir.exe** program in the created folder:
   %XMANAGER_INSTALL_DIR%\Fonts\NewFonts> ..\..\mkfntdir
4. Run **Xconfig**.
5. Double-click a profile to which the new fonts folder is to be added. The **Profile Properties** dialog box is displayed.
6. Click the [Font] tab.
7. Click [Add Font Folder]. The **Browse For Folder** dialog box is displayed.
8. Select a new font folder.
9. Click [OK].
10. Restart **Xmanager**.

To Use Font Server:

1. Run **Xconfig.**
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Font] tab.
4. Click [Add Font Server]. The **Add Font Server** dialog box is displayed.
5. Enter the font server name or IP address in [Host].
6. Enter the font server port number in [Port].
7. Click [OK].

Note
Check if a font server is executed on the remote server. In general, the font server program name is **xfs** and the default port number is 7100.

To Change Default Font:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Font] tab.
4. Enter the name of the font to use as the default font in [Default Font].
5. Click [OK].

Note
The default font is used when an X application does not designate a font for text display.

To Replace a Font with another Font when the Font Cannot be Found:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Font] tab.
4. Select [Automatic Font Substitution].
5. Click [OK].

To Display the Font Error Dialog Box:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Font] tab.
4. Select [Show Missing Font Dialog].

Note
The missing font message is used to find a font when the font used by a remote X application is not available in Xmanager. The missing font information is always recorded in the Xmanager log. Even if a font is unavailable in Xmanager, the missing font message may not be displayed by some X

applications. In this case, find the necessary fonts by referring to the log or error messages of the concerned X application.

5. Click [OK].

7.5 Color Management

Visual is a device-independent color system, which defines **Xmanager's** color format and the numbers of colors supported. **Xmanager** supports *PseudoColor*, *StaticColor*, *DirectColor*, *TrueColor*, *GrayScale,* and *StaticGray*, the six visuals defined in X window standards.
In *PseudoColor* visual, all X applications can only use 256 colors and thus application execution may fail due to an inadequate number of colors. Use the [Automatic Color Substitution(PseudoColor)] option to successfully run the application in case the color palette is insufficient due to another program.
Windows uses 20 system colors in 256-color mode to display title bars, window frames and icons. In some X applications, the whole 256-color palette is used to display the colors properly. In this case, the Windows desktop and icons may blink. Select the [Preserve System Colors (20 colors)] option to prevent this.
Additionally, **Xmanager** provides an RGB database, which is used to change color names to appropriate RGB values. Users can edit the database using a text editor.

To Change Default Server Visual:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Color] tab.
4. Select an appropriate visual from the [Choose Default Visual] list.
5. Click [OK].

Note
If the default visual is set as *Auto Detect*, Xmanager selects an appropriate visual according to the video device. In 256-color (8 bit) mode, it is set as PseudoColor. In true color (16 bit or higher) mode, it is set as TrueColor. The default visual is used by X root window and most applications.

To Support Exact StoreColor Request (PseudoColor):

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Color] Tab.
4. Select [Exact StoreColor (PseudoColor)].
5. Click [OK].

Note
When the true color video device operates with PseudoColor visual, StoreColor requests overloads and deteriorates overall performance. Xmanager provides an option to turn off Exact StoreColor.

To Operate True Color Video Device with 256-color Visual:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Color] tab.
4. Select PseudoColor from the [Choose Default Visual] list.
5. Click the [Advanced] tab.
6. Select [When Mapped] in [Backing Store].
7. Click [OK].

Note
Some older CAD programs operate in the 256-color system thus the default visual must be changed to PseudoColor to ensure successful execution.

To Change to RGB Format in TrueColor Visual:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Color] tab.
4. Select [RGB in Reverse Order(TrueColor)].
5. Click [OK].

Note
This function is useful when an X application requires a special RGB format.

To Change or Edit the RGB Color Database:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Color] tab.
4. Click [Change] or [View] in the [Color Database] field.
5. Click [OK].

7.6 Keyboard Setting

Users can create or edit a keyboard file, designate a shortcut key to change a keyboard file in real-time, and edit the keyboard file using a keyboard editor. **Xmanager** provides keyboard files created in advance in relation to most languages and keyboards. Users can thus find and use a keyboard appropriate for their application. If an appropriate keyboard file cannot be found, a similar keyboard file can be selected and conveniently edited. If the XKEYBOARD extension is enabled in the 'Advanced Option Settings' of the 'Server Profile', the user-defined keyboard settings will not be applied.

To Add a Keyboard File to Keyboards List:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Keyboard Settings]. The **Keyboard Settings** dialog box is displayed.
5. Click [Add]. The **Add Keyboard** dialog box is displayed.
6. Select a keyboard file.
7. Click [OK].

To Set a Specific Keyboard as the Default Keyboard:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Keyboard Settings]. The **Keyboard Settings** dialog box is displayed.
5. Select a keyboard to use as the default keyboard from [Keyboards List].
6. Click [Set as Default].
7. Click [OK].

To Change a Keyboard File in Real-time:

1. Click Ctrl+Alt+K while running **Xmanager**. The **Keyboard Selector** dialog box is displayed.
2. Press 'K' key several times while pressing Ctrl+Alt to select a keyboard.
3. Release all keys.

Note
Users may view only the keyboard files in the **Keyboard Settings** dialog box [Keyboards List].

To Edit a Keyboard File:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.

3. Click the [Devices] tab.
4. Click [Keyboard Settings]. The **Keyboard Settings** dialog box is displayed.
5. Select a keyboard to edit from [Keyboards List].
6. Click [Edit]. The **Keyboard Editor** opens.
7. Double-click a key to edit in the keyboard layout. The **Edit Key** dialog box is displayed.

Note
In the **Edit Key** dialog box, change the key status and keysym.
Repeat continuously generates a same key event when a user presses a key. This function is used in most keys with the exception of auxiliary keys, such as Shift, Alt and Control.
Latch generates either a KeyPress or KeyRelease event when the key is pressed and then released. The key must be pressed and released twice to generate KeyPress and KeyRelease events. In general, this function is used for CapsLock key or NumLock keys.
In the [Keysym] field, Normal, Shift, ModeSwitch, and Shift ModeSwitch keysyms are set to a key.
Normal is used when pressing the key while pressing no other auxiliary keys.
Shift is used when pressing the key while pressing the Shift key.
ModeSwitch is used when pressing the key while pressing the ModeSwitch key.
Shift ModeSwitch is used when pressing the key while simultaneously pressing the Shift and ModeSwitch keys.

To Create a New Keyboard File:

1. Open the Keyboard Editor.
2. Select [New] from the [File] menu. The **Select Keyboard Type** dialog box is displayed.
3. Select an appropriate keyboard type and click [OK].
   Note
   In the **Select Keyboard Type** dialog box, [Keyboard Type] list shows all keyboard types available to use in Xmanager. Each keyboard has different keyboard layouts and key counts. A keyboard type similar to the one being used must be selected.
4. Edit keyboard in the selected keyboard layout.

7.7 Mouse Setting

Xmanager provides 3-button emulation: scroll using mouse wheel and changing the middle and right mouse buttons.

To Use 2-button Mouse as 3-button Mouse:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Mouse Settings]. The **Mouse Settings** dialog box is displayed.
5. Select [Click the left and right buttons simultaneously].
6. Adjust the time interval between the left and right buttons in [Click Speed].
7. Click [OK].

Note
In 3-button emulation mode, the mouse operates as if the middle button is pressed when the left and right buttons are pressed simultaneously. Click speed is the standby time from the pressing of one button to the pressing of the other.

To Scroll in X Applications Using Mouse Wheel:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Mouse Settings]. The **Mouse Settings** dialog box is displayed.

5. Select [Use Wheel Mouse].
6. Click [OK].

Note
For scrolling using a mouse wheel, a button4 event is generated when scrolling up and a button5 event is generated when scrolling down. Right-clicking may not be available in some X applications, such as CDE desktop.

To Change Right and Middle Button Positions:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Mouse Settings]. The **Mouse Settings** dialog box is displayed.
5. Select [Use Right Button as Middle Button].
6. Click [OK].

Note
Select this option if the middle button is used more frequently than the right button.

To Use Color Mouse Pointer:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Mouse Settings]. The **Mouse Settings** dialog box is displayed.
5. Select [Use Color at Mouse Pointer].
6. Click [OK].

7.8 Sound Setting

In the **Sound Settings** dialog box, select bell types and designate sound files. In the **Profile Properties** dialog box, open the dialog box by clicking the [Sound Settings] button in the [Devices] tab.

Bell Type
Select an appropriate audio device for bell requests by an X application. Select one from among three bell types: *Sound Card, PC Speaker, and None.*
If *Sound Card* is selected, an appropriate sound file (.wav) must be designated. If *None* is selected, no bell sound is generated.

Sound File
Show a sound file (.wav) to be used for bell requests of X applications.

Browse
Select a sound file by opening

Open dialog box.

7.9 Multi-monitor

Xmanager enables users to select a monitor for X Window desktop output on a multi-monitor systems. **Xmanager** may not operate successfully if one monitor is 8-bit color and other monitors are larger than 8-bit. It is therefore recommended that every monitor's color is set to 16-bit color or higher.

To Select Monitor for X Desktop:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.

3. Click the [Devices] tab.
4. Click [Monitor Settings]. The **Monitor Settings** dialog box is displayed.
5. Select a monitor from the [Monitor to use] list.
6. Click [OK].

Note
The monitor list shows all monitors available for use including *Auto detect* and *Virtual Screen*.
Virtual Screen is a virtual rectangular area that includes all monitors.
When *Auto detect* is selected, Xmanager selects *Virtual Screen* in Multiple Window Mode and the main monitor in Single Window Mode.

To Use All Monitors as a Single X Desktop:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Monitor Settings]. The **Monitor Settings** dialog box is displayed.
5. Select *Virtual Screen* from the [Monitor to use] list.
   Note
   Virtual Screen is listed only when there are several monitors on a system. The *Virtual Screen* created root window size and workspace are affected by the resolution and layout of each monitor. The root window is the largest rectangle comprising of several monitors.
6. Click [OK].

To Display Select Monitor Window at Startup:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Devices] tab.
4. Click [Monitor Settings]. The **Monitor Settings** dialog box is displayed.
5. Select [Show the Monitor Selector at startup].
6. Click [OK].

7.10 Advanced Option Setting

Set X protocol extensions and other advanced options in the [Advanced] tab of the **Profile Properties** dialog box. For copy and paste option usage, see 'Copy, Save and Print in X Application'.

Copy and Paste Automatically
When this option is turned on, **Xmanager** copies and pastes texts or images between an X application and a Windows application. When an X application copies texts or images, the contents are immediately forwarded to the Windows Clipboard. Reversely, when new contents are added to Windows Clipboard, the contents are immediately forwarded to X Selection. Texts and images can be copied to both or either the Cut Buffer or X Selection. Selectin one may be required depending on the X application.

X Selection
Use X Selection when copying and pasting contents between Windows and an X application.

Cut Buffer
Use Cut Buffer when copying and pasting contents between Windows and an X application.

Copy and Paste on Changing Focus
Run copy and paste only when focus changes between **Xmanager** and another Windows application. When the focus is in **Xmanager**, the contents can be copied several times from X applications. The contents are then pasted to the Windows Clipboard the moment input focus changes to another Windows program. If using this option while using **Xmanager** in the Windows terminal, copy and paste may not function properly.

Notify Display Change
Display a dialog box when the Windows desktop color or resolution is changed. If color or resolution is changed, **Xmanager** must be restarted.

Maximize Performance
Xmanager is executed at maximum performance. **Xmanager** selects the fastest method for complicated drawing operations.
However, some graphic images may not be displayed properly depending on the user's video device or applications.

Permit Old X11 Bugs
Select this option when a remote X application is created in version earlier than X11R6 and thus do not operate successfully in **Xmanager**.

Accept Esound Request
This is an option to process remote Esound requests. Esound uses TCP 16001 port.

Detailed Log Message
Use this option for detailed log messages if necessary for technical support.

Backing Store
Select an appropriate Backing Store mode.
The Backing Store is a function to store a hidden window area in memory. When a window is hidden by another window, it must be redrawn when it is revealed later on. By saving the obscured area in memory, **Xmanager** can recover the area faster than the application can draw it again. Using this method, **Xmanager** reduces data transfer volume in a slow network environment.
Xmanager provides four Backing Store modes.
In *Do Not Use* mode, the Backing Store function is turned off and the hidden fields are always redrawn.
When Requested does not use the Backing Store function. However, when requested by an X application, Xmanager uses the Backing Store function limitedly for the X application windows.
In *When Mapped* mode, the Backing Store function operates in all windows excluding hidden or minimized windows.
In *Always* mode, the Backing Store function operates in all windows including hidden or minimized windows. This option requires a large system memory capacity and graphic resources.

X Extensions
Select X extensions to use.
Xmanager supports BIG-REQUEST, DAMAGE, DEC-XTRAP, DOUBLE-BUFFER, Extended-Visual-Information, MIT-SUNDRY-NONSTANDARD, Multi-Buffering, RandR, RECORD, RENDER, SECURITY, SHAPE, SYNC, TOG-CUP, XC-APPGROUP, XC-MISC, XEVIE, XFIXES, Xinerama, XInput, XKeyboard, and XTEST extension protocols. In particular, it supports Render extension protocol and an improved graphic enviornment for X applications.

X Resource Database
Show path to the X resource database to read when **Xmanager** is started.

Change
Display the **Open** dialog box to change the resource database to another file.

View
View the resource database contents using Notepad.

8 Security

Xmanager supports secure connections by providing host access control and SSH protocols.
Host access control prevents connections from unauthorized hosts. However, network packets between **Xmanager** and an X application are not encoded and are vulnerable to intrusions.
Xmanager also supports SSH protocols for security. SSH connections can be utilized in both Xstart and Secure XDMCP sessions.
Host key and user key databases generated in **Xmanager** can be used in **Xshell** and **Xftp** programs. Once a public key is created, it can be used in all programs without additional configurations.

8.1 Host Access Control

Host access control manages a list of reliable hosts and enables only X applications from reliable hosts to connect to **Xmanager**. When connections by an unauthorized host is requested, **Xmanager** displays an Alert dialog box asking whether to permit the connection.

To Use the Host Access Control Function:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Security] tab.
4. Select [Enable Access Control].
5. Enter authorized hosts in the [Trusted Hosts] list.
6. Click [OK].

To Display an Alert Message for Unauthorized Connection:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Security] tab.
4. Select [Warn Unauthorized Connections].
5. Click [OK].

8.2 Public Key User Authentication

To Open the User Key Manager:

1. Run **Xmanager**.
2. Click [User Key Manager] in the [Tools] menu.

Note
User can export, import, rename, delete, and create a user key in 'User Keys Dialog Box'.

To Create a User Key:

1. Run **Xmanager**.
2. Select [New User Key Wizard] from the [Tools] menu.
3. Create a user key according to the instructions provided by the New User Key wizard.

Note
Register a public key on a server at the last stage of key creation. Registration methods vary according to key formats.

- *SSH1*: Copy the public key text and save it to $HOME/.ssh/authorized_keys file. Run the following command to turn off the write permission of the files and directories.

```
$ cd
$ chmod go-w . .ssh .ssh/authorized_keys
```

- *SSH2-OpenSSH*: OpenSSH servers use this format. Copy the public key text and save it to $HOME/.ssh/authorized_keys2 file. Run the following command to turn off the write permission of the files and directories.

```
$ cd
$ chmod go-w . .ssh .ssh/authorized_keys2
```

- *SSH2-IETF SECSH*: Some commercial SSH servers, such as ssh.com server, use this format. Save a public key under an intrinsic name, such as mypublickey.pub and copy it to $HOME/.ssh2 directory. Add the following line to $HOME/.ssh2/authorization file: Key mypublickey.pub Run the following command to turn off the write permission of the files and directories.

```
$ cd
$ chmod go-w . .ssh2$ chmod go-w .ssh2/authorization .ssh2/mypublickey.pub
```

To Register a Public Key in Server:

1. Open the **User Keys** dialog box.
2. Select a user key to register.
3. Click [Properties]. The **User Key Properties** dialog box is displayed.
4. Click the [Public Key] tab.
5. Select a type that suits a remote SSH server from the [Public Key Format] list.
6. Save the public key by selecting [Save as a file] or copy the key contents and register the key in a server using the public key registration method listed above.

To Change a User Key Passphrase:

1. Open the **User Keys** dialog box.
2. Select a user key for which to change the passphrase.
3. Select [Properties]. The **User Key Properties** dialog box is displayed.
4. Select the [General] tab.
5. Select [Change Passphrase].

8.2.1 User Keys Dialog Box

The **User Keys** dialog box enables to users to create and manage user keys. Open this dialog box by selecting [User Key Manager] from the [Tools] menu.

Import
Select a user key file and import it by opening the **Open** dialog box. Currently, **Xmanager** can read the SSH1 protocol RSA key, the OpenSSH SSH2 protocol RSA/DSA/ECDSA/ED25519 key, the SSH.COM key, and NetSarang user key formats.

Export
Save a selected user key file by opening the **Save** dialog box. Exported file types are NetSarang user keys, OpenSSH SSH2. NetSarang user key format files can be used in programs developed by NetSarang Computer, Inc.

Delete
Delete a selected user key from the database.

Rename
Rename a selected user key. Key name must be a valid file name.

Properties
Show user key attributes. Type, length, fingerprint, and public key can be viewed. Additionally, the key passphrase can be changed.

Generate
Open the **New User Key wizard**.

8.3 SSH User Authentication Dialog Box

The **SSH User Authentication** dialog box enables users to select appropriate authentication methods. If a passphrase is not saved in a session, this dialog box is displayed in case it is necessary to obtain authentication-related information from the user.

Password
Password authentication is used to permit a user to log in to a server by entering the user account password. Due to security reasons, some servers do not support this authentication method.

Public Key
Public key authentication requires a user's public key to be registered in a remote SSH server. To log in using this method, select an appropriate user key from the user keys list.

Keyboard Interactive
Keyboard interactive acts as a server asking questions and the user replying with the correct messages.

8.4 Host Key Management

A host key is a remote host public key, through which users can verify hosts by their fingerprint. When a connection is made, the remote host sends its public key to **Xmanager**. For a host that is connected with for the first time or when a host key is not saved in the database, an **SSH Security Warning** dialog box is displayed upon connection. If a host key is valid and reliable, save the host key in the host key database.

To Open the Host Key Manager:

1. Run **Xmanager**.
2. Click [Host Key Manager] in the [Tools] menu.

8.4.1 SSH Security Warning Dialog Box

The **SSH Security Warning** dialog box is displayed when a remote host key is not saved in the host key database or when the fingerprint of a remote host key differs from the fingerprint of the saved host key.

Accept Once
Accept a host key for this connection only. The host key is not saved and the same dialog box will opens on the next connection. This function is useful when the server host key changes often or if the server is not frequently connected to.

Accept and Save
Save a host key and continuously process connection. The dialog box will not open on the next connection. This function is useful when a fingerprint is correct and the host is connected with frequently.

Cancel
A host key is not accepted and the connection is cancelled.

8.4.2 Host Keys Dialog Box

The **Host Keys** dialog box permits users to manage host keys of remote hosts to which connection is allowed.

Import
Import a host key by opening the **Open** dialog box. The imported host key is saved in the host key database. Imports are limited to keys saved in the SECSH public key format.

Export
Export a selected host key by opening the **Save** dialog box. Exported keys are saved in the SECSH public key format and can be used in other programs.

Remove
Remove a selected host key from the database.

View
Open a selected host key with Notepad.

Edit CA key
Check, add, or delete certificate-authenticated host keys. Unless the authenticated host key has had its authentication expire, a change to a server's host information does not require you to check the new host key information.

8.5 Master Password

Master password can be used to save passwords more securely using the user defined master password**. Xmanager** saves all password information in an encrypted format. However, since passwords are encrypted using a fixed key, it has a risk of being exploited by hackers. When the master password is enabled and set, it is mixed in during password encryption adding an additional layer of security.
Master password uses a user defined keyword to encrypt the password section of the session data. When the master password is enabled, Xmanager asks for the master password every time a new Xmanager instance is started and a session is open. If the correct master password in not inputted, the session's password is not able to be utilized and must be entered again manually preventing unauthorized access.

> **Note**
> Be sure to remember your master password. If you lose your master password, there is no way to retrieve the password information stored in the session files. Maser Password settings are applied simultaneously to Xmanager, Xshell, and Xftp sessions.

To Enable Master Password:

1. Click on the **Tools** menu of Xmanager and then select **Set Master Password**.
2. In the **Master Password** dialog box, enter a new master password in the **New Password** field.
3. In the **Confirm Password** field, enter the new password again.
4. Click **OK** to save the changes.

Once master password is enabled, all sessions saved in the default location are re-encrypted using the new master password.

To Change Master Password:

1. Click on the **Tools** menu of Xmanager and then select **Set Master Password**.
2. In the Change area click **Change** to open the Master Password Change dialog box..
3. Enter the current master password in the **Current Password** field.
4. Enter the new master password in the **New Password** field.
5. Enter the new password one more time in the **Confirm Password** field.
6. Click **OK** to save the changes.

To Disable Master Password:

1. Click on the **Tools** menu of Xmanager and then select **Set Master Password**.
2. Click the **Remove** button to open the Remove Master Password dialog box.
3. In the Remove Master Password dialog box, enter the master password and click **OK.**

To Reset the Master Password:

1. Click on the **Tools** menu of Xmanager and then select **Set Master Password**.
2. Click the **Reset** button to open the Reset Master Password dialog box.
3. In the Reset Master Password dialog box, click **Reset Master Password** and click **OK.**

Note
Reset of the master password can be used if your forgot your master password or if you would like to clear all the passwords stored in your sessions.

9 Tab Management

Xmanager includes a powerful tab management feature. Users can can connect to multiple hosts and compare them side by side from a single window. This tab management system is a unique Xmanager feature that cannot be found in other PC X Servers.
Each tab is associated to a single Xmanager server instance and it belongs to a tab group. At tab group is a collection of tabs. A single Xmanager window can have multiple tab groups can be organized in any way.

9.1 Tab

Tabbed sessions in Xmanager run according to the options as if the '**Window Mode**' is set to Single Window Mode.

To Open a Session in a New Tab

1. Click [Tools] from the File menu
2. For the Default Open action, select **Open in Tab**.
3. Double click on a session in Xmanager.

Note
You can manually open a session in a new window by right clicking on a session and then selecting the Open in a New Window option. What you select in the context menu will override the default open action setting.

To close a Tab

1. Click the **x** button on tab.

9.2 Tab Group

Tab group is collection of multiple tabs. Only one tab from the tab group is visible at any given moment. You can manage multiple tab groups in a single Xmanager window allowing for comparing different tabs side by side without switching between applications.

To Create a New Tab Group

1. Open a new session by right clicking on a session and then selecting **Open in New Tab**.
2. Click on the tab and drag it to an edge of the **Xmanager** window. This will create a drop zone that indicates how the new tab group will be created.
3. Drop the tab to an edge where you want to create the new tab group.

To Move a Tab to a Different Tab Group

1. Select a tab you want to move to a new tab group.
2. While holding down the left mouse button, drag the tab to a different tab group.
3. Drop the tab into the new tab group.

To Close a Tab Group

1. Select a tab group you want to close.
2. Right click on the tab group in the background.
3. Select the **Close This Tab Group** option.

To Arrange All Tabs Vertically

1. While multiple tabs are open, right click on a tab.
2. Point to **Arrange** and then select **Arrange Tabs Vertically**.

To Arrange All Tabs Horitzontally

1. While multiple tabs are open, right click on a tab.

2. Point to **Arrange** and then select **Arrange Tabs Horizontally**.

To Arrange All Tabs Stacked

1. While multiple tabs are open, right click on a tab.
2. Point to Arrange and then select **Arrange tabs Tiled**.

To Merge All Tab Groups

1. While more than one tab group is showing on a single window, right click on a tab.
2. Point to **Arrange** and then select **Merge All Tabs**.

10 Copy, Save, and Print in X Applications

Automatically copy character strings between an X application and the Windows Clipboard using **Xmanager**. Additionally, when using the local window manager, X application images can be copied to the Windows Clipboard, saved as bitmap files, and printed by a printer.

To Set Automatic Copy and Paste:

1. Run **Xconfig**.
2. Double-click a profile. The **Profile Properties** dialog box is displayed.
3. Click the [Advanced] tab.
4. Select [Copy and Paste Automatically] from the [Settings] list.
5. Click [OK].

To Copy Character Strings from Xterm to the Windows Notepad:

1. Select a character string to copy from the **xterm** window with the left mouse button.
2. Start Notepad.
3. Select [Paste] from the [Edit] menu.

To Copy Character Strings from Windows Notepad to Xterm:

1. Select a character string to copy from Notepad with the left mouse button.
2. Select [Copy] from the [Edit] menu.
3. Run **xterm**.
4. Click the middle mouse button or left and right buttons simultaneously in the **xterm** window.

To Copy the X Application Window to Clipboard:

1. Point to [Copy] in the title bar system menu and select [Window] or [Content]. The Window image is copied to the clipboard.

Note
This function can be used when the local window manager is in operation under Multiple Window Mode.

To Save the X Application Window as a Bitmap File:

1. Point to [Save] in the title bar system menu and select [Window] or [Content]. The **Save As** dialog box is displayed.
2. Enter an appropriate file name in [File Name].
3. Click [OK].

Note
This function can be used when the local window manager is in operation under Multiple Window Mode.

To Print X Application Window:

1. Point to [Print] in system menu on title bar and click [Window] or [Content]. The **Print** dialog box is displayed.
2. Click [Print].

Note
This function can be used when the local window manager is in operation under Multiple Window Mode.

11 Session Log

Xmanager sessions record debug information as files. When several **Xmanager** sessions are being used simultaneously, each session log is saved under a different name, such as X0.LOG and X1.LOG. The number in the log file refers to the display number of the **Xmanager** session.
Checking log files can be helpful when problems occur while using **Xmanager**.

To View a Log Files of the Current Session:

1. Right-click on the **Xmanager** notification area icon or click the **Xmanager** icon in the **Xmanager** main window title bar.
2. Point to [Log] in the system menu and select [File]. A log file is opened with Notepad.

Note
In Multiple Window Mode, the Xmanager icon is created in the notification area. In Single Window Mode, Xmanager opens a single main window.

To Open the Folder where All Session Log Files are Saved:

1. Right-click on the **Xmanager** notification area icon or click the **Xmanager** icon in the **Xmanager** main window title bar.
2. Point to [Log] in the system menu and select [Folder]. The log folder opens.

Note
Open a log folder by selecting [Open Log Folder] from the [File] menu in the **Xmanager**.