Gio 5

User Manual for J Series

Information in this document is subject to change without prior notice and does not represent a commitment on the part of the manufacturer. No part of this guide may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying and recording, for any purpose, without the express written permission of the manufacturer.

Registered trademarks are properties of their respective owners.

Every effort is made to make this guide as complete and as accurate as possible, but no warranty of fitness is implied. The authors and the publisher shall have neither responsibility nor liability to any person or entity with respect to loss or damages arising from the use of information contained in this guide.

Last Updated: October, 2013.

Version: GIO5J/UM-40-13

VXL Instruments Ltd.,
House of Excellence,
No. 17, Electronics City,
Hosur Road,
Bangalore– 560 100, INDIA.
www.vxl.net

Table of Contents

1 Introduction

Gio 5 is the latest Linux based thin client operating system offering from *VXL Instruments*. *Gio 5* offers flexibility, connectivity, security, multimedia and peripheral capabilities that make it ideal for mainstream corporate and small-business use.

This user manual provides information and instructions to configure and use *Gio 5*. For installing or restoring the *Gio 5* image on your thin client, refer to the *Gio 5* Installation Guide.

Features

The Salient features of Gio 5 are as follows:

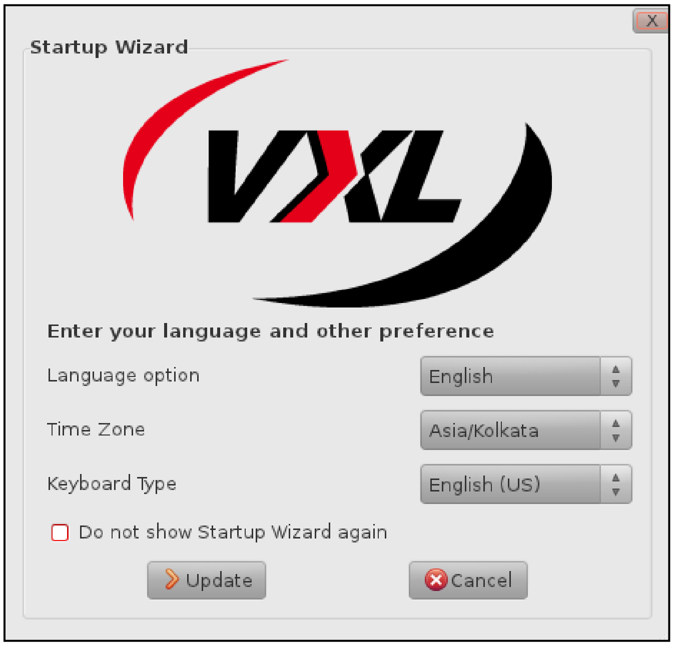
- Local Language Support :
  - English
  - French
  - German
  - Spanish
- Available Connections:
  - Citrix ICA 12.5.1
  - VMware View 2.0
  - Rdesktop 1.7.1
  - xFree Rdp 1.0.1
  - Standard open SSH & SFTP
  - Browser FireFox 16.0.2
  - WFCMGR
  - PNagent
  - XDMCP
  - NFS
  - SAMBA
  - NX 0.9.2
- Network Support :
  - TCP/IP supports IP V4 & IP V6
  - Network Security 802.1 is supported
    - WLAN supports the following encryptions
    - WEP 40/128-bit
    - WEP 128-bit passphrase
    - Dynamic WEP(802.1 x)
    - WPA & WPA2 Personal
    - WPA & WPA2 Enterprise
  - DHCP client support with IPV4 & IPV6
  - Auto Negotiable network speed
- Network Drive Support :
  - Samba (user can create it as a connection)
  - NFS (user can create it as a connection)

- Display Support:
    - Display support for Cloned & Extended mode
    - Minimum Resolution for J series is 1024x768.
    - Maximum Resolution for J series is 1920x1200.
    - Rotations of single display like left, right, top ,bottom
    - Rotations of dual display like left, right, top ,bottom
    - Color depth is 16/24 bit
    - Display Power management System (DPMS) : default value 10 min
- Printing Support
    - Server side printing (using windows printer driver name used in ICA / RDP).
    - Network printing.
    - Local Printing through Common Unix Printing System (CUPS).
    - Ports supported for printing is USB.
    - Print queue and print status view.
    - Shared printing through IPP.
- External Device Support
- USB HDD, Flash drives , USB CD/DVD drive
    - USB Web camera
    - USB Audio Speaker, Audio Headset
- Client Security Functionality :
    - Windows Active Directories Authentication
    - Multi user support
- Keyboard :
    - USB Keyboard support
    - 93 Keyboard layouts are supported.
    - Controllable Repeat rate.
    - Controllable Delay time.
    - Various keyboard models and variants are supported.
    - Numlock on boot up
- Mouse
    - USB Mouse support
    - Controllable Mouse speed acceleration
    - Left hand mouse click on/off
    - Mouse Pointer auto hide
- Local Applications :
    - Gedit Text Editor
    - Evince PDF reader
    - Alsa mixer volume control
    - Touch Screen Calibrator
- Graphics Driver Support
    - Supports Inbuilt TI Chipset for DM814X
    - Supports Dual display and Rotation
- Firmware upgrade :
    - Individual component upgrade
- Thin Clint Device Management Support

- Configuration File Generator tool to generate INI files.

Startup Wizard

The **Startup Wizard** window appears immediately after installing Gio 5. This wizard allows you to set the system language, time zone and keyboard language on start-up.



Startup Wizard

Enter your language and other preference

Language option: English

Time Zone: Asia/Kolkata

Keyboard Type: English (US)

□ Do not show Startup Wizard again

To set the system language, time zone and keyboard language on start-up:

1. From the **Language option** spin box select the system language.
2. From the **Time Zone** spin box select the requuired time zone.
3. Drom the **Keyboard Type** spin box select the keyboard language.

Note: Select **Do not ask this again** option to not view the startup wizard next time.

User Manual Organization

The content in this manual is organized as shown in the following table:

Chapter No.	Chapter	Description
1	Introduction	Introduction to Gio 5
2	Gio 5 Desktop	Description of the various desktop components and the interface.
3	Connectivity	Description of the configuration procedures for network and server connections.
4	Local Settings	Description and procedure to set various local settings. Configuring input and output devices such as mouse, printer.
5	Security	Description of setting up security and server management.
6	Diagnostics	Description and procedure to use the diagnostic tools in Gio 5.
7	User Applications	Description of the various user applications installed in Gio 5
8	Glossary	Alphabetically sorted list of keywords/topics used in this manual.
9	Index	Definitions of technical terminology used in this manual

Table 1: List of Chapters

Terminologies

This user manual uses the following expressions to represent a few commonly used terminologies:

Terminologies	Description
Gio 5	A Linux based thin client specific operating system developed by *VXL Instruments*®.
Thin Client/thin client	*VXL Thin Client*

Table 2: Terminologies

Typographical Conventions

This manual uses the following typographical conventions:

Text Type	Usage
Bold text	Field names, user interface elements such as dialog boxes and windows
SMALL CAPS text	System messages
Italics text	Proper nouns and examples
`courier new` text	Syntax and user inputs
Bold and UPPER CASE text.	Keyboard shortcuts. For example, **CTRL+ C**
Blue underlined Italic text	External Hyperlinks (will open your default browser)

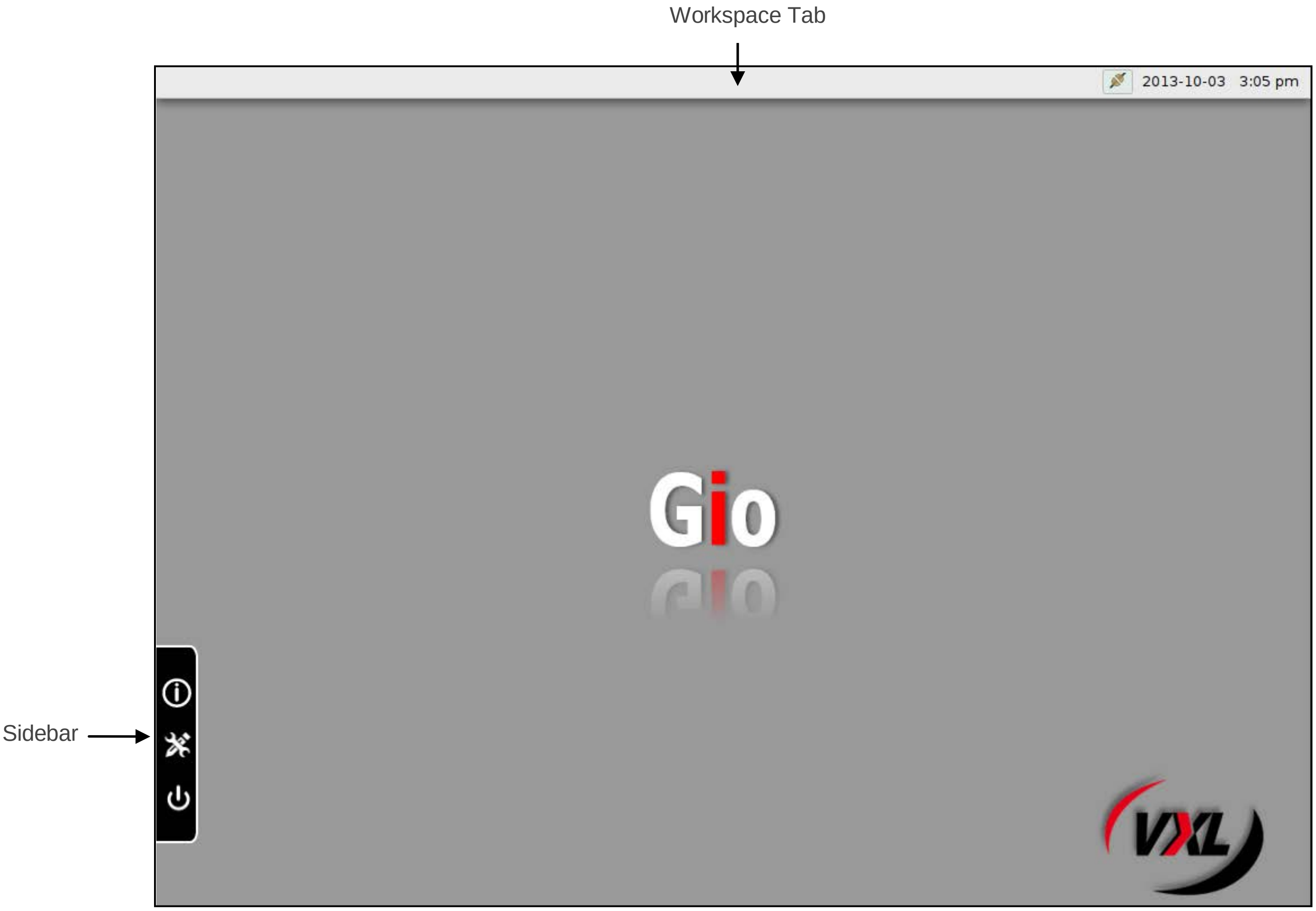
Table 3: Typographical Conventions

2 Gio 5 Desktop

A graphical user interface desktop environment provides menus and icons for interaction with the operating system. *Gio 5* is a Graphical User Interface (GUI) based operating system. *Gio 5* desktop supports 3D and composite acceleration. It also supports network video acceleration. The *Gio 5* desktop consists of:

- Desktop icons and widgets on the home screen.
- Sidebar that provides access to the features of the operating system
- Active applications and services on the workspace tab.

The *Gio 5* desktop environment consists of the following components:



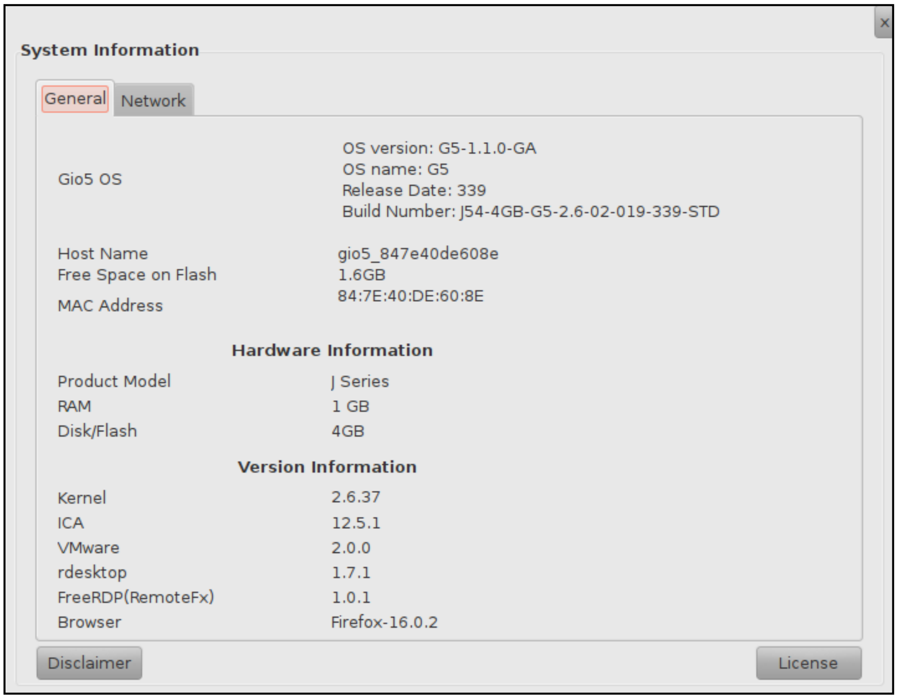
- Workspace Tab: User applications that are minimized appear in the workspace tab for quick access.
- Sidebar: The sidebar provides access to the operating system functionality and applications.

Sidebar Icons	Description
ⓘ	Information
⚒	Settings
⏻	Power

System Information

You can view the various system specific information such as Kernel version, IP address from the system information option. You can view the system information by clicking on the **Information** icon in the sidebar. Click **Disclaimer** or **License** to view the disclaimer and license details.

System Information – General



Gio5 OS	OS version: G5-1.1.0-GA OS name: G5 Release Date: 339 Build Number: J54-4GB-G5-2.6-02-019-339-STD
Host Name	gio5_847e40de608e
Free Space on Flash	1.6GB
MAC Address	84:7E:40:DE:60:8E

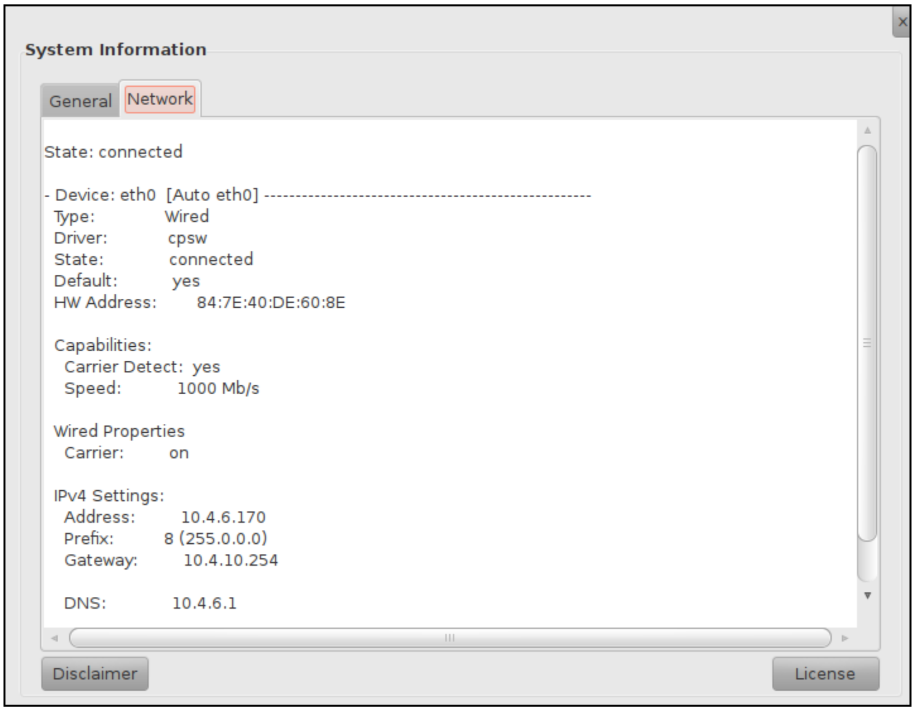
Hardware Information

Product Model	J Series
RAM	1 GB
Disk/Flash	4GB

Version Information

Kernel	2.6.37
ICA	12.5.1
VMware	2.0.0
rdesktop	1.7.1
FreeRDP(RemoteFx)	1.0.1
Browser	Firefox-16.0.2

System Information – Network


System Information

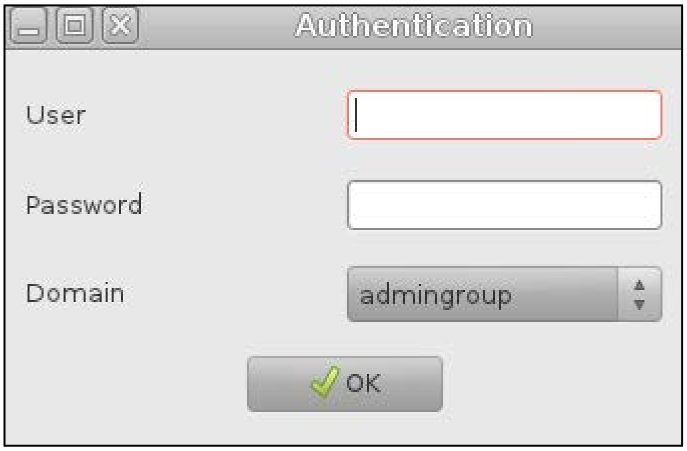
```
State: connected

- Device: eth0  [Auto eth0] --------------------------------------------------
  Type:            Wired
  Driver:          cpsw
  State:           connected
  Default:         yes
  HW Address:      84:7E:40:DE:60:8E

  Capabilities:
    Carrier Detect:  yes
    Speed:           1000 Mb/s

  Wired Properties
    Carrier:         on

  IPv4 Settings:
    Address:         10.4.6.170
    Prefix:          8 (255.0.0.0)
    Gateway:         10.4.10.254

    DNS:             10.4.6.1
```

Settings

You can view and configure settings of your *Gio 5* operating system using the settings option. This option allows you to configure your network, connections, input/output devices etc. The following chapters in this user manual provide instructions and information about various settings.

To access the various settings:

1. Click the **Settings** icon on the sidebar. The **Authentication** dialog box appears.


Authentication

User

Password

Domain: admingroup

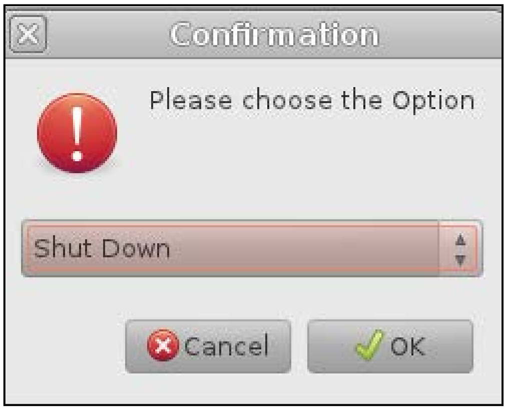
2. Enter user name and password.
3. Select the domain and click **OK**.

Note: In the **Domain** field select **Local** for local authentication; select a particular LDAP domain for authentication on the LDAP server. For more information on creating LDAP refer section ‘To create LDAP ‘on page 92.

Shutting down and Restarting Gio 5

To shut down your thin client:

1. From the sidebar, click **Power** icon.
2. From the drop-down menu, select **Shut Down.**



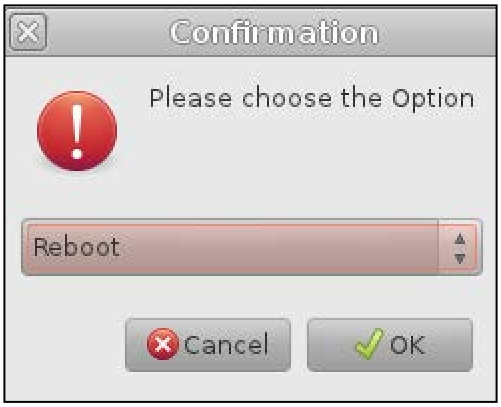
Please choose the Option

Shut Down

3. Click **OK**.

To restart your thin client:

1. From the sidebar, click **Power** icon.
2. From the drop-down menu, select **Reboot**.



Please choose the Option

Reboot

3. Click **OK**.

3 Connectivity

Gio 5 provides several connectivity options to configure your network and connect your client to a server. Network connection options such as wired, wireless and VPN allow you to connect your thin client to different network infrastructure environments; you can configure your network based on your preferences using the **Configure Network** option.

Gio 5 allows your thin client to connect to a server using popular protocols and tools such as ICA, RDP, VMware View and Citrix Receiver; you can configure these settings using the **Connection Manager** option.

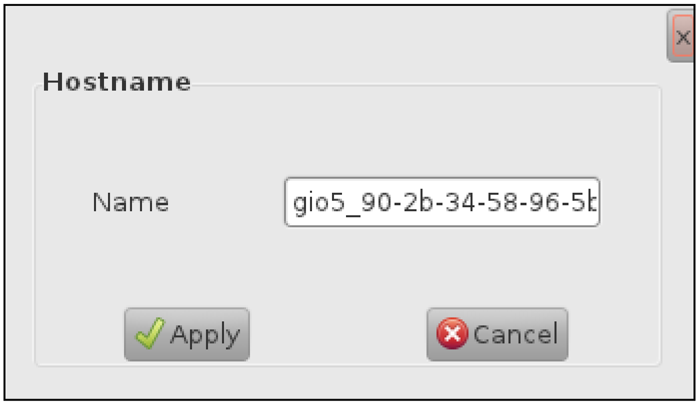
You can manage your *Gio 5* based thin client using the *VXL Instruments XLmanage* thin client management application. You can establish a connection with the *XLmanage* application server using the **XLM Connect** option.

Configure Hostname

Host name is a custom name used to identify your thin client on the network.
You can change the host name based on your preference. *For example, Lab Thin Client.*
The host name is displayed in the information page and in the DHCP server.

To change the host name:

1. On the desktop sidebar, click the **Settings** icon**.**
2. Click **Connectivity** drop-down arrow.
3. Click **Configure Hostname.** The **Hostname** dialog box appears**.**



Hostname

Name gio5_90-2b-34-58-96-5b

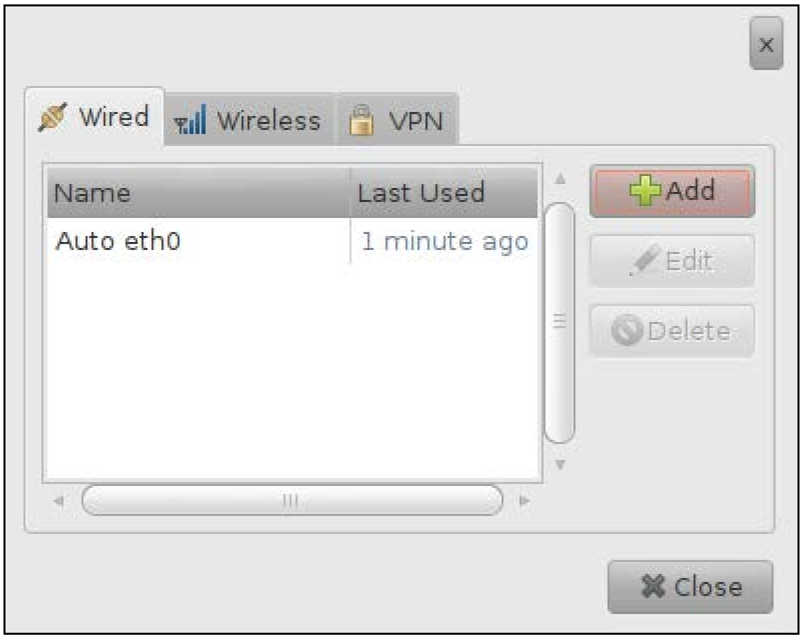
4. Enter a host name and click **Apply.** The client will restart.

Configure Network

The **Configure Network** option allows you to configure your network connection. Configuring your network is necessary to connect your thin client to a server. Correct network configuration ensures that your thin client is secure and connected to the intended server.

To configure a network connection:

1. On the desktop sidebar, click the **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Configure Network,** the network connection window appears.



Name	Last Used
Auto eth0	1 minute ago

You can configure the following type of connections:

- Wired
- Wireless
- VPN

Wired Connection

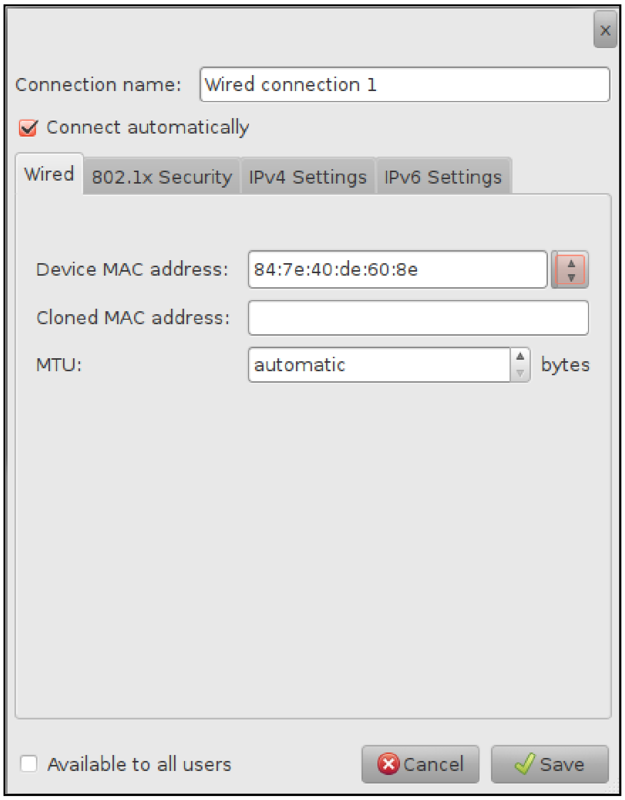
A wired connection, also known as an Ethernet connection is one of the fastest way to connect to a network. In a wired connection, an Ethernet cable connects your thin client to your network infrastructure.

To setup a wired connection, create a wired connection and set up IPv4 or IPv6 with security.

Creating a Wired Connection

To create a wired connection:

1. In the network connections window, click the **Wired** tab.
2. Click **Add**.



Connection name: Wired connection 1

☑ Connect automatically

Device MAC address: 84:7e:40:de:60:8e

Cloned MAC address:

MTU: automatic bytes

□ Available to all users

3. In the **Connection Name** field, enter a connection name.

   Note: Select **Connect Automatically** option to make this your default network.

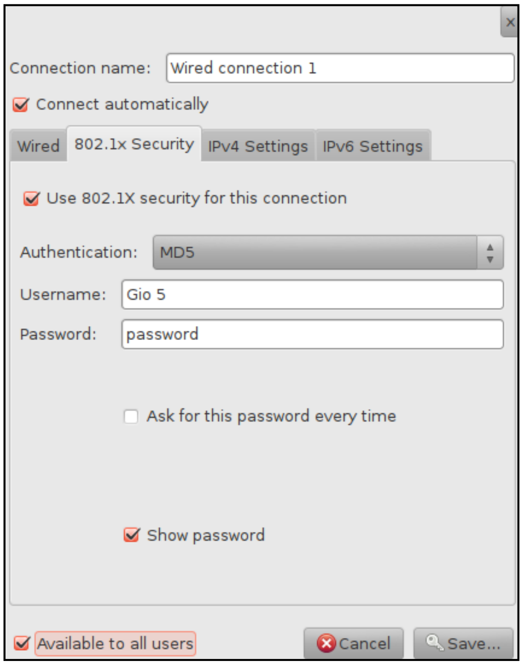
4. From the **Device MAC address** drop-down list, select your device MAC address.
5. From the **MTU** spin box, set an MTU (maximum transmission unit) value. Select **automatic** for default network MTU value.
6. Select the **Available to all users** check box to allow other users of the thin client to connect to this network. This option is not selected by default.
7. Click **Save**.

Configuring Wired Security

Gio 5 provides 802.1x security protocol options, 802.1x is a security and authentication standard for wired and wireless network connections. You can choose from several authentication options that are part of the 802.1x protocol suite.

To configure wired security:

1. From the **Profiles** list, select a connection that you want to configure.
2. Click **Edit**.
3. Click the **802.1x Security** tab, select **Use 802.1x security for this connection** check box.



Connection name: Wired connection 1

☑ Connect automatically

☑ Use 802.1X security for this connection

Authentication: MD5

Username: Gio 5

Password: password

□ Ask for this password every time

☑ Show password

☑ Available to all users

4. From the **Authentication** drop-down list, select and configure one of the following authentication options:

   The default security option is **MD5**. If your preferred authentication option is MD5, perform the following steps.

   Note: The Message Digest 5 (MD5) algorithm is a secure hash function. Enable this option to encrypt all your network communication using the MD5 function. To enable this option:

   a. In the **Username** field, enter a user name.

   b. In the **Password** field, enter a password.

   c. Click **Save.**

   Note: Select **Ask for this password every time** to enable authentication every time you use this connection. Select **Show password** to make the password that you have typed visible in plain text.

   If your preferred authentication option is **TLS**, perform the following steps.

   Note*:* Transport Layer Security (TLS) is a cryptographic protocol to encrypt network communication.

   a. In the **Authentication** field, select **TLS**.

   b. In the **Identity** field, enter the client's identity. *For example, JohnDoeThinClient.*

      Note*:* The client identity can be a name in characters. A client's identity is used for authorization of communication between the server and the client.

   c. Select a user certificate by clicking on the browse button next to **User certificate**.

   d. Select a CA certificate by clicking on the browse button next to **CA certificate**.

e. Select a private key by clicking on the browse button next to **Private key**.

f. In the **Private key password** field, enter a private key password of your choice.

Note: Select **Show password** to make the password that you have typed visible as plain text. Remember the private key password for future use.

If your preferred authentication option is **Tunneled TLS**, perform the following steps:

Note: Tunneled Transport Layer Security (TLS) is a multi-factor authorization protocol that helps to secure your network communication. To enable this option:

a. In the **Authentication** field, select **Tunneled TLS**

b. In the **Anonymous identity** field, enter an anonymous client identity.

Note: The anonymous identity is revealed only to the authentication server.

c. In the **CA certificate** field, browse and select a CA certificate **.**

d. From the **Inner authentication** drop-down list, select an inner authentication method.

Note An inner authentication method is the authentication method used for tunneling authentication. You can choose **PAP**, **MSCHAP**, **MSCHAPv2** or **CHAP**.

e. In the **Username** field, enter a user name.

f. In the **Password** field, enter a password.

If your preferred authentication option is **Protected EAP (PEAP)**, perform the following steps.

Note*:* Protected Extensible Authentication Protocol (PEAP) is an encryption protocol that provides advanced encryption for network communication. To enable this option:

a. In the **Authentication** field, select **Protected EAP (PEAP)**.

b. In the **Anonymous identity** field, enter an anonymous client identity.

Note: The anonymous identity is revealed only to the authentication server.

c. In the **CA certificate** field browse and select a CA certificate**.**

d. From the **PEAP version** drop-down list select a PEAP version, select **Automatic** to select the PEAP version automatically.

e. From the **Inner authentication** drop-down list, select an inner authentication method.

Note: An inner authentication method is used for tunneling authentication. You can choose **GTC**, **MD5**, **MSCHAPv2**.

f. In the **Username** field, enter a user name.

g. In the **Password** field, enter a password.

5. Click **Save**.

> **Note:** Select **Ask for this password every time** to enable authentication every time you use this connection. Select **Show password** to make the password that you have typed visible as plain text.

Configure IPv4 Settings

Internet Protocol version 4 is a network standard for transmitting information over a network. Enter a relevant IP address, netmask and gateway information to ensure correct configuration of the network.

To configure IPv4 Settings:

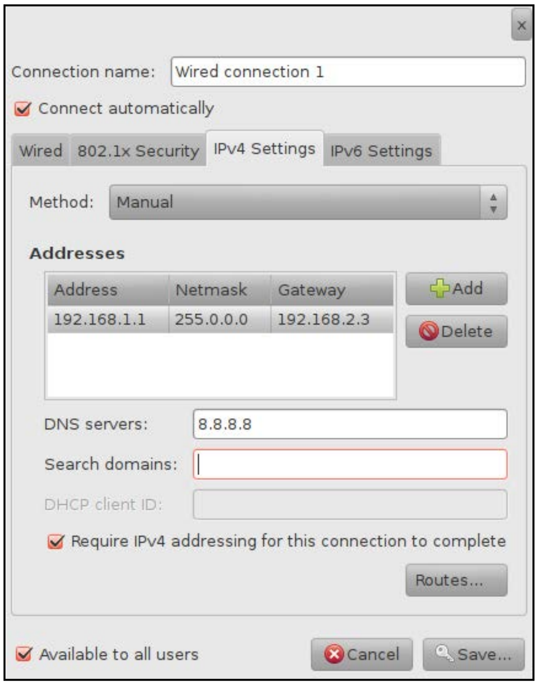
1. Click the **IPV4** tab in the network connections window.

   Note: By default the **method** is set to **Automatic (DHCP)**, click **Save** to configure the network automatically.

2. In the **Method** field, select **Automatic (DHCP) addresses only**.
3. In the **DNS servers** field, enter a DNS server address.
4. In the **Search domains** field, enter a domain name. *For example, vxl.net.*
5. In the **DHCP client ID** field, enter a DHCP client ID.
6. Click **Save**.

   For manual configuration:

1. From the **method** drop-down list, select **Manual**.



Connection name: Wired connection 1

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.1	255.0.0.0	192.168.2.3

DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

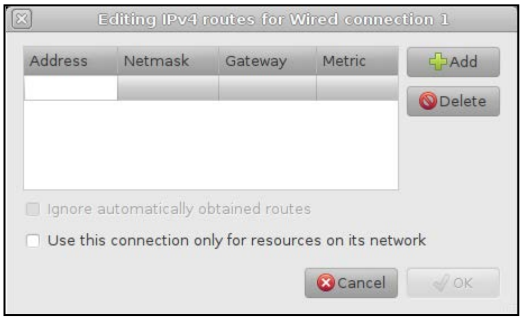
2. Click **Add**.
3. In the **IP Address**, **Netmask** and **Gateway** fields, enter the thin client IP address, netmask and gateway address.
4. In the **DNS servers** field, enter a DNS server address.
5. In the **Search domains** field, enter a domain name. *For example, vxl.net.*

Note: Select the **Require the IPv4 addressing for this connection to complete** to use only the IPv4 settings for your connection. If you do not select this option, IPv6 settings are used when you do not provide the IPv4 settings.

6. Click **Routes** to manage IP routes.

   Note: If you do not add a route, a default route will be assigned for network communication.

7. Click **Add** to enter a route.



Editing IPv4 routes for Wired connection 1

□ Ignore automatically obtained routes

□ Use this connection only for resources on its network

8. Enter the **IP, Netmask and Gateway** address for the routes.

   Note:

   - Select **Ignore automatically obtained routes** to use the routes that you have entered and ignore the routes that are obtained from the router.

   - Select **Use this connection only for resources on its network** option to selectively route network traffic through this connection. If you select this option, you can never use this connection as the default connection.

9. Click **Save**.

Configure IPv6 Settings

Internet Protocol version 6 is the newest version of the Internet Protocol suite. To configure IPv6 settings:

1. Click the **IPV6** tab in the network connections window.

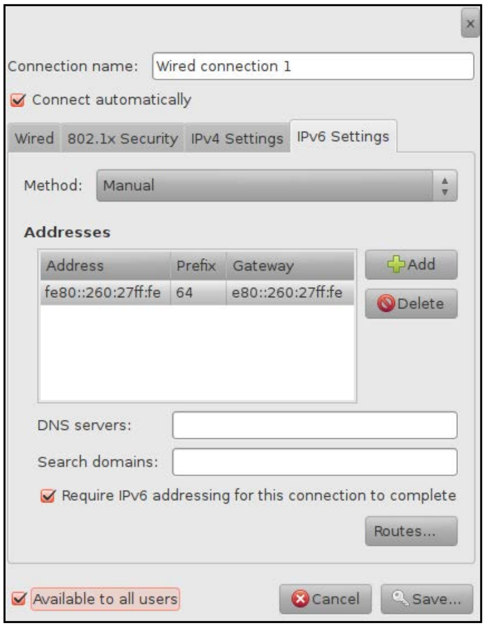
   Note: By default, the **method** is set to **Automatic**; click **Save** to configure the network automatically.

2. In the **method** field, select **Automatic addresses only**.
3. In the **DNS server's** field, enter a DNS server address.
4. In the **Search domains** field, enter a domain name. *For example, vxl.net.in*
5. Click **Save**.

   Note: Select **Automatic, DHCP only** to automatically configure your network using DHCP.

For manual configuration:

1. From the **method** drop-down list, select **Manual**.



Connection name: Wired connection 1

☑ Connect automatically

Method: Manual

Addresses

Address	Prefix	Gateway
fe80::260:27ff:fe	64	e80::260:27ff:fe

DNS servers:

Search domains:

☑ Require IPv6 addressing for this connection to complete

☑ Available to all users

2. Click **Add**.
3. In the **Address**, **Prefix** and **Gateway** fields, enter the thin client IP address, prefix and gateway address.
4. In the **DNS server's** field, enter a DNS server address.
5. In the **Search domains** field, enter a domain name.

   Note: Select the **Require the IPv6 addressing for this connection to complete** to use only the IPv6 settings for your connection. If you do not select this option, IPv4 settings are used when you do not provide the IPv6 settings.

6. Click **Routes** to manage IP routes.

   Note: If you do not add a route, the router will assign a default route for network communication.

7. Click **Add** to enter a route.
8. Enter the IP address, Prefix, Gateway and Metric for the routes.

   Note:

   - Select **Ignore automatically obtained routes** to use the routes that you have entered and ignore the routes that are obtained from the router.
   - Select **Use this connection only for resources on its network** option to selectively route network traffic through this connection. If you select this option, you cannot use this connection as the default connection.

9. Click **Save**.

Deleting a Wired Connection

1. From the **Profiles** list, select a connection that you want to delete.
2. Click **Delete,** the wired connection is deleted.

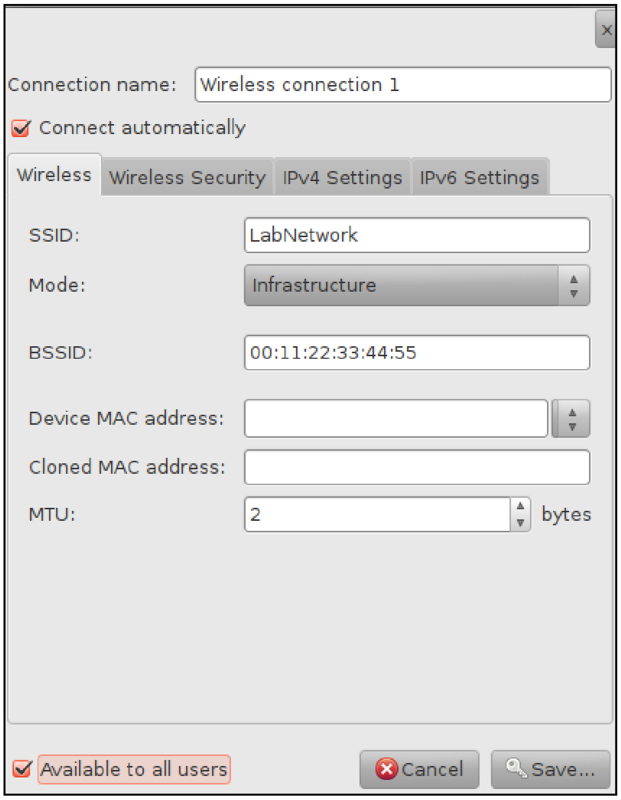
Wireless Connection

A wireless connection is established by connecting your client to a network using radio frequency (RF) signals. The client is connected to the network via a wireless network card to a gateway, access point or a wireless router. In the **Infrastructure** connection, your client is connected to a router or an access point. In the **Ad-hoc connection,** your client is connected to another client within the same subnet.

Note: Wireless connection is currently not available in Gio 5 for J series.

Creating a Wireless Connection

1. In the network configuration window, click the **Wireless** tab.
2. Click **Add**.



Connection name: Wireless connection 1

☑ Connect automatically

SSID: LabNetwork

Mode: Infrastructure

BSSID: 00:11:22:33:44:55

Device MAC address:

Cloned MAC address:

MTU: 2 bytes

☑ Available to all users

3. In the **Connection** name field, enter a connection name.
4. In the **SSID** field, enter a valid SSID.

   Note: The Service Set Identifier (SSID) is the name given to a router that you want to connect to; by default, it is the name of the wireless router manufacturer.

5. From the **Mode** drop-down list, select the mode of connection.

   If the mode of connection is **Infrastructure**, perform the following steps:

   a. In the **BSSID** field, enter a valid BSSID.

      Note: The Basic Service Set Identifier (BSSID) is the MAC address of the Access Point to which you want to connect to; you can retrieve this information from the Access Point’s hardware configuration options.

b. From the **Device MAC address** drop-down list, select the appropriate device MAC address.

c. In the **Cloned MAC address** field, enter your cloned MAC address.

Note: Cloned MAC address must be in the correct MAC address format. You cannot use the same cloned MAC address for more than one client/device on your network. You can clone your router's MAC address only if your router supports this feature.

d. From the **MTU** spin box, set an MTU (maximum transmission unit) value.

e. Select the **Available to all users** check box to allow other users to connect to this network.

f. Click **Save**.

If the mode of connection is **Ad-hoc**, perform the following steps:

a. From the **Band** drop-down list, select the band of operation.

b. From the **Channel** drop-down list, select the channel of operation.

c. In the **BSSID** field, enter a valid BSSID.

Note: The Basic Service Set Identifier (BSSID) is the MAC address of the Access Point to which you intend to connect; you can get this information from the Access Point's hardware configuration options.

d. From the **Device MAC address** drop-down list, select the appropriate device MAC address.

e. In the **Cloned MAC address** field, enter your cloned MAC address.

Note: Cloned MAC address must be in the correct MAC address format. You cannot use the same cloned MAC address for more than one client/device on your network. You can clone your router's MAC address only if your router supports that feature.

f. From the MTU spin box, set an MTU (maximum transmission unit) value.

g. Select the **Available to all users** check box to allow other users to connect to this network.

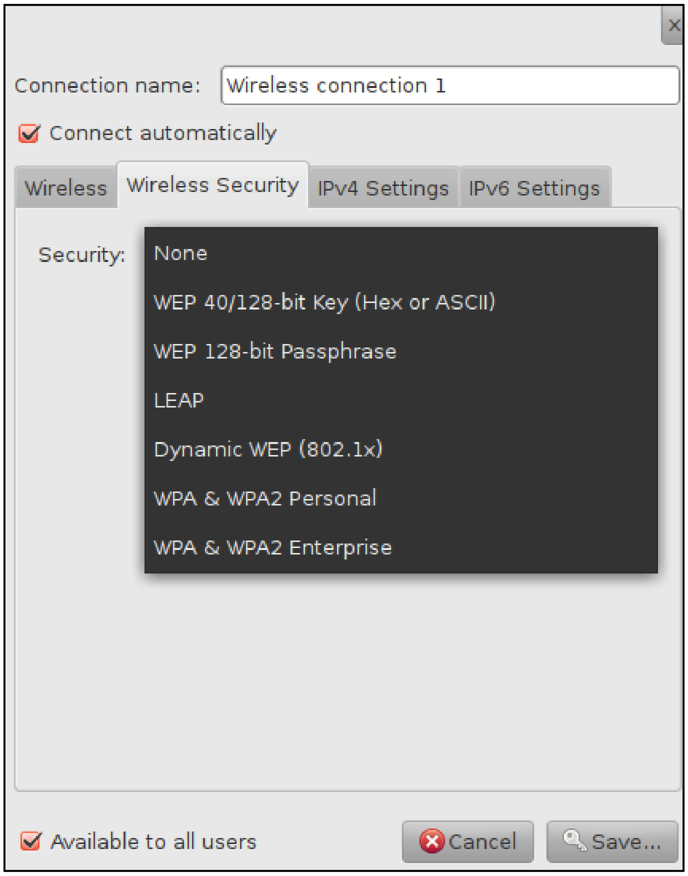
h. Click **Save**.

Configuring Wireless Security

You can select from the following encryption methods:

- **WEP 40/128-bit Key (Hex or ASCII)**: A WEP 40-bit key is a 10 digit key (Hex or ASCII) that can contain numbers 0-9 and the letters A-Z. A WEP 128-bit key is a 26 digit key that can contain numbers 0-9 and letters A-Z
- **WEP 128-bit Passphrase**: A WEP 128-bit passphrase is a plain text of custom length that can be used as a key.
- **LEAP (Lightweight Extensible Authentication Protocol)**: Also known as Cisco-Wireless EAP; provides username/password-based authentication between a wireless client and a RADIUS server like Cisco ACS or Interlink AAA.

  Note: LEAP security is currently not functional.
- **Dynamic WEP (802.1 xs):** Dynamic WEP refers to the combination of 802.1x technology and the Extensible Authentication Protocol. Dynamic WEP changes WEP keys dynamically.
- **WPA & WPA2 Personal:** WPA and WPA2 personal is an alphanumeric encryption key that can contain numbers 0-9 and letters A-Z.
- **WPA & WPA2 Enterprise:** WPA Enterprise uses 802.1x authentication by means of a RADIUS server. This provides for user account certificate based authentication, and is the recommended security for businesses, and other large wireless networks.



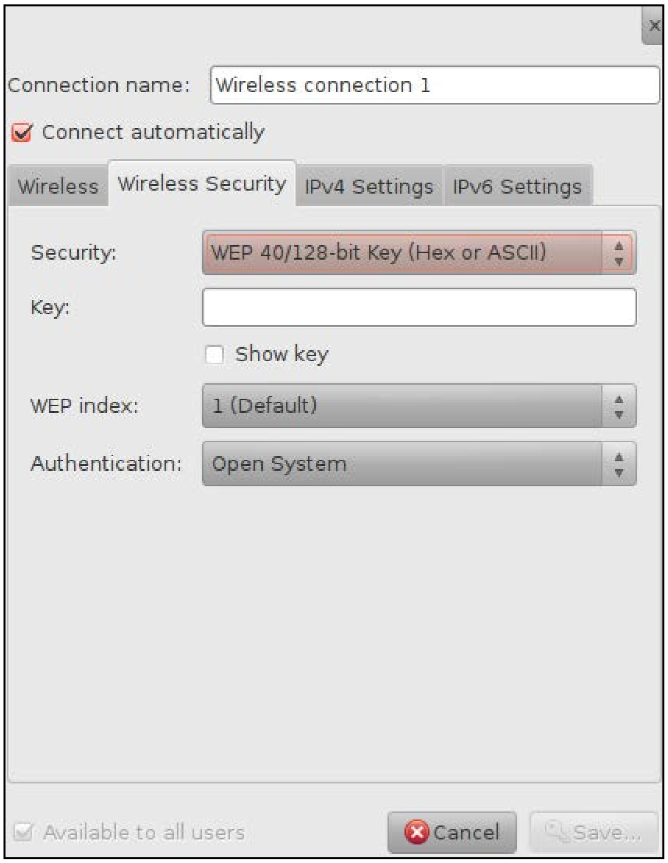
Connection name: Wireless connection 1

☑ Connect automatically

☑ Available to all users

To set up WEP 40/128 bit key or WEP 128 bit Pass Phrase security:

1. In the network configuration window, click the **Wireless Security** tab.
2. From the **Security** drop-down list, select **WEP 40/128 bit ke**y or **WEP 128-bit PassPhrase**.



Connection name: Wireless connection 1

☑ Connect automatically

Security: WEP 40/128-bit Key (Hex or ASCII)

Key:

□ Show key

WEP index: 1 (Default)

Authentication: Open System

☑ Available to all users

Note: Select **None** for unencrypted transmission.

3. In the Key field, enter a valid security key or passphrase.

Note:

- The encryption keys must be generated in the wireless network’s access point or router, the generated keys have to be used here for configuring the network.
- The WPA & WPA2 encryption method is available in the **Infrastructure** connection mode only.

4. Select **Show key** to make the encryption key visible.
5. In the **WEP Index** field select a value from 1 to 4.
6. In the **Authentication** select Open System or Shared Key.

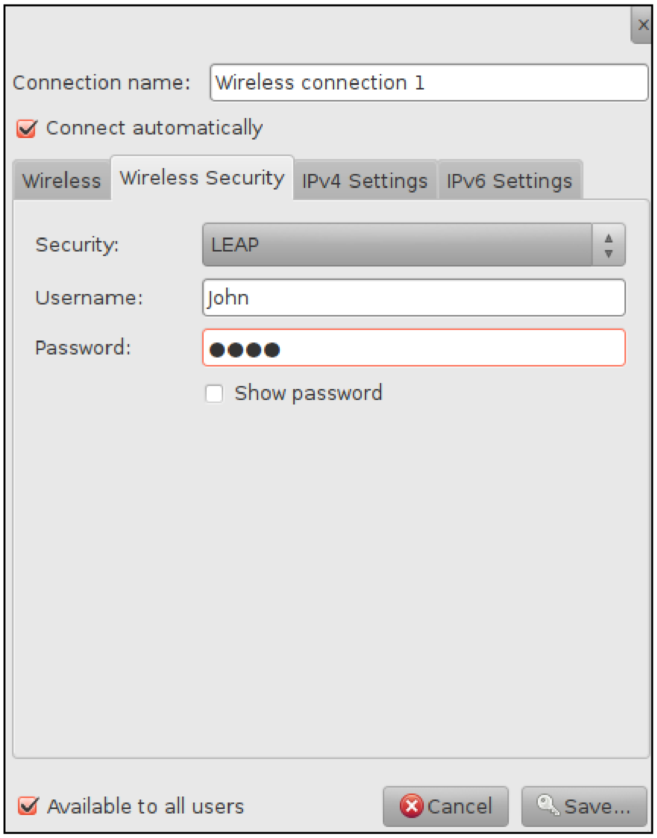
Note: Select **None** for unencrypted transmission.

7. Click **Save**.

To set up LEAP security:

1. In the network configuration window, click the **Wireless Security** tab.

2. From the **Security** drop-down list, select **LEAP**.



Connection name: Wireless connection 1

☑ Connect automatically

Security: LEAP

Username: John

Password: ●●●●

☐ Show password

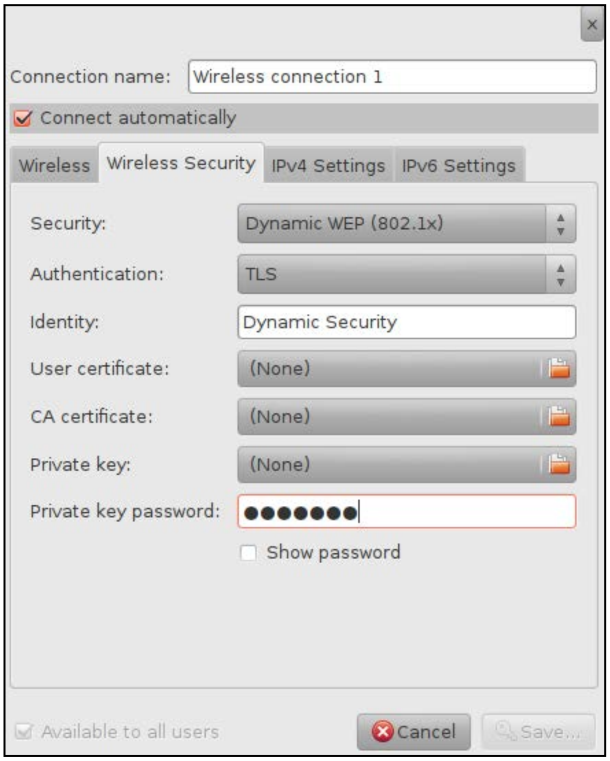
☑ Available to all users

3. In the **Username** field, enter the user name.
4. In the **Password** field, enter the password.
5. Click **Save**.

Note: LEAP security is currently not functional.

To set Dynamic WEP (802.1x):

1. In the network configuration window, click the **Wireless Security** tab.
2. From the **Security** drop-down list, select **Dynamic WEP (802.1x)**.



Connection name: Wireless connection 1

☑ Connect automatically

Security: Dynamic WEP (802.1x)

Authentication: TLS

Identity: Dynamic Security

User certificate: (None)

CA certificate: (None)

Private key: (None)

Private key password: ●●●●●●●

□ Show password

☑ Available to all users

If your preferred authentication option is **TLS**, perform the following steps.

Note*:* Transport Layer Security (TLS) is a cryptographic protocol to encrypt network communication.

a. In the **Authentication** field, select **TLS**.

b. In the **Identity** field, enter the client's identity. *For example, JohnDoeThinClient.*

Note*:* The client identity can be a name in characters. A client's identity is used for authorization of communication between the server and the client.

c. Select a user certificate by clicking on the browse button next to **User certificate**.

d. Select a CA certificate by clicking on the browse button next to **CA certificate**.

e. Select a private key by clicking on the browse button next to **Private key**.

f. In the **Private Key password** field, enter a private key password of your choice.

Note: Select **Show password** to make the password that you have typed visible in plain text. Remember the private key password for future use.

If your preferred authentication option is **LEAP**:

a. From the **Authentication** drop-down list, select **LEAP**.

b. In the **Username** field, enter the user name.

c. In the **Password** field, enter the password.

If your preferred authentication option is **Tunneled TLS**, perform the following steps:

Note: Tunneled Transport Layer Security (TLS) is a multi-factor authorization protocol that helps to secure your network communication. To enable this option:

a. In the **Authentication** field, select Tunneled **TLS**.

b. In the **Anonymous identity** field, enter an anonymous client identity.

Note: The anonymous identity is revealed only to the authentication server.

c. Select a CA certificate by clicking on the browse button next to **CA certificate**.

d. From the **Inner authentication** drop-down list, select an inner authentication method.

Note An inner authentication method is the authentication method used for tunneling authentication. You can choose **PAP**, **MSCHAP**, **MSCHAPv2** or **CHAP**.

e. In the **Username** field, enter a user name.

f. In the **Password** field, enter a password.

If your preferred authentication option is **Protected EAP (PEAP)**, perform the following steps.

Note*:* Protected Extensible Authentication Protocol (PEAP) is an encryption protocol that provides advanced encryption for network communication. To enable this option:

a. In the **Authentication** field, select **Protected EAP (PEAP)**.

b. In the **Anonymous identity** field, enter an anonymous client identity.

Note: The anonymous identity is revealed only to the authentication server.

c. Select a CA certificate by clicking on the browse button next to **CA certificate**.

d. From the **PEAP version** drop-down list select a PEAP version, select **Automatic** to automatically select the PEAP version.

e. From the **Inner authentication** drop-down list, select an inner authentication method.

Note: An inner authentication method is the authentication method used for tunneling authentication. You can choose **MD5, GTC** or **MSCHAPv2**.

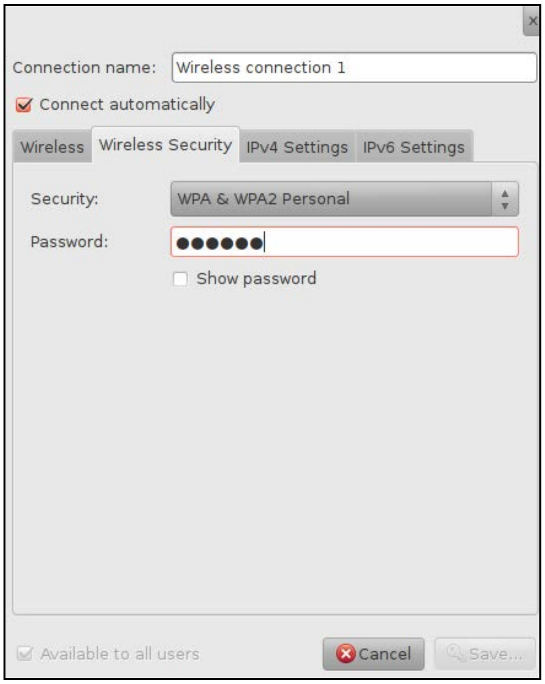
f. In the **Username** field, enter a user name.

g. In the **Password** field, enter a password.

3. Click **Save**.

To setup WPA & WPA 2 Personal security:

1. In the network configuration window, click the **Wireless Security** tab.
2. From the **Security** drop-down list, select **WPA & WPA2 Personal**.



Connection name: Wireless connection 1

☑ Connect automatically

Security: WPA & WPA2 Personal

Password: ●●●●●●

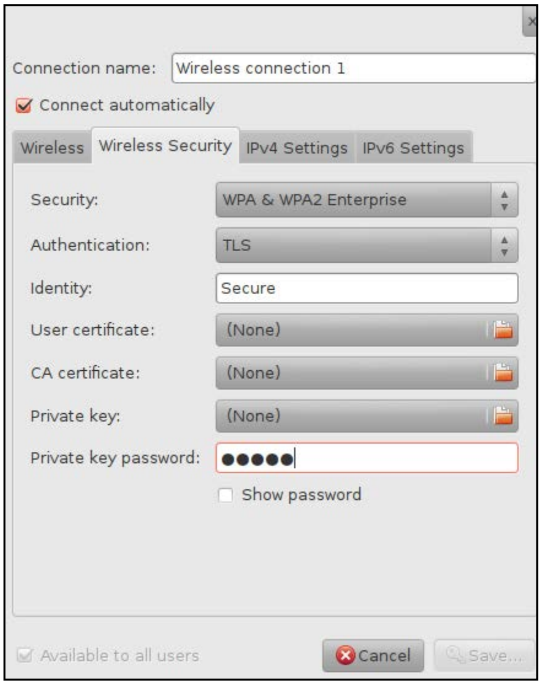
□ Show password

☑ Available to all users

3. In the **Password** field, enter a password.
4. Click **Save**.

To set up WPA & WPA2 Enterprise:

1. From the **Security** drop-down list, select **WPA & WPA2 Enterprise**.



Connection name: Wireless connection 1

☑ Connect automatically

Security: WPA & WPA2 Enterprise

Authentication: TLS

Identity: Secure

User certificate: (None)

CA certificate: (None)

Private key: (None)

Private key password: ●●●●●

□ Show password

☑ Available to all users

If your preferred authentication option is **TLS**, perform the following steps.

Note*:* Transport Layer Security (TLS) is a cryptographic protocol to encrypt network communication.

a. In the **Authentication** field, select **TLS**.

b. In the **Identity** field, enter the client's identity. *For example, JohnDoeThinClient.*

   Note*:* The client identity can be a name in characters. A client's identity is used for authorization of communication between the server and the client.

c. Select a user certificate by clicking on the browse button next to **User certificate**.

d. Select a CA certificate by clicking on the browse button next to **CA certificate**.

e. Select a private key by clicking on the browse button next to **Private key**.

f. In the **Private key password** field, enter a private key password of your choice.

   Note: Select **Show password** to make the password that you have typed visible as plain text. Remember the private key password for future use.

If your preferred authentication option is **LEAP**.

a. From the **Authentication** drop-down list, select LEAP.

b. In the **Username** field, enter the user name.

c. In the **Password** field, enter the password.

If your preferred authentication option is **Tunneled TLS**, perform the following steps:

Note: Tunneled Transport Layer Security (TLS) is a multi-factor authorization protocol that helps to secure your network communication. To enable this option:

a. In the **Authentication** field select **Tunneled TLS**

b. In the **Anonymous identity** field, enter an anonymous client identity.

   Note: The anonymous identity is revealed only to the authentication server.

c. Select a CA certificate by clicking the browse button next to **CA certificate**.

d. From the **Inner authentication** drop-down list, select an inner authentication method.

   Note An inner authentication method is the authentication method used for tunneling authentication. You can choose **PAP**, **MSCHAP**, **MSCHAPv2** or **CHAP**.

e. In the **Username** field, enter a user name.

f. In the **Password** field, enter a password.

If your preferred authentication option is **Protected EAP (PEAP)**, perform the following steps.

Note*:* Protected Extensible Authentication Protocol (PEAP) is an encryption protocol that provides advanced encryption for network communication. To enable this option:

a. In the Authentication field, select **Protected EAP (PEAP**).

b. In the **Anonymous identity** field, enter an anonymous client identity.

Note: The anonymous identity is revealed only to the authentication server.

c. Select a CA certificate by clicking on the browse button next to **CA certificate**.

d. From the **PEAP version** drop-down list select a PEAP version, select **Automatic** to automatically select the PEAP version.

e. From the **Inner authentication** drop-down list, select an inner authentication method.

Note: An inner authentication method is the authentication method used for tunneling authentication. You can choose **MD5**, **GTC** or **MSCHAPv2**.

f. In the **Username** field, enter a user name.

g. In the **Password** field, enter a password.

2. Click **Save.**

Configure IPv4 Settings

Internet Protocol version 4 is a network standard for transmitting information over a network. Enter relevant IP address, netmask and gateway information to ensure correct configuration of the network.

To configure IPv4 Settings:

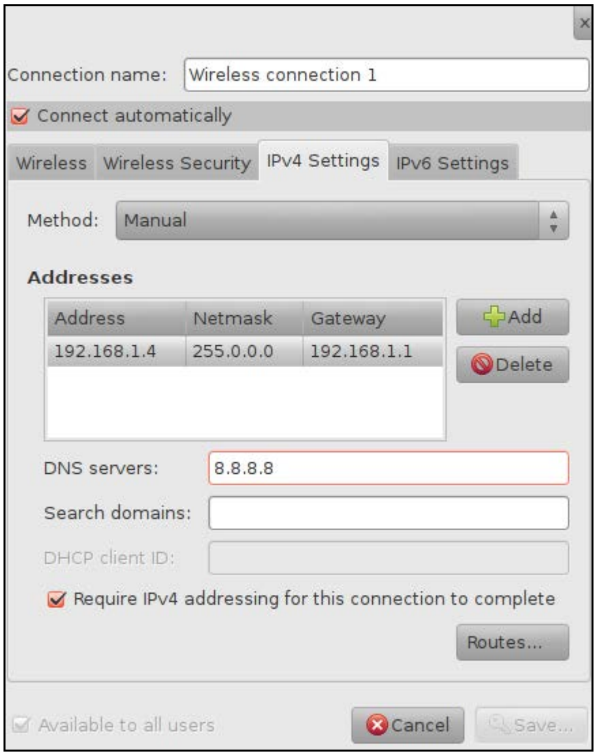
1. Click the **IPV4 Settings** tab in the Network Connections window.

   Note: By default, the **method** is set to **Automatic (DHCP)**; click **Save** to configure the network automatically.

2. In the **method** field, select **Automatic (DHCP) addresses only**.
3. In the **DNS server's** field, enter a DNS server address.
4. In the **Search domains** field, enter a domain name. *For example, vxl.net.in*
5. In the **DHCP client ID** field, enter a DHCP client ID.
6. Click **Save**.

   For manual configuration:

1. From the **method** drop-down list, select **Manual**.



Connection name: Wireless connection 1

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.4	255.0.0.0	192.168.1.1

DNS servers: 8.8.8.8

Search domains:

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

☑ Available to all users

2. Click **Add**.
3. In the **IP Address**, **Netmask** and **Gateway** fields, enter the thin client IP address, netmask and gateway address.
4. In the **DNS servers** field, enter a DNS server address.
5. In the **Search domains** field, enter a domain name.
6. In the **DHCP client ID** field, enter a DHCP client ID.

   Note: Select the **Require the IPv4 addressing for this connection to complete** to use only the IPv4 settings for your connection. If you do not select this option, IPv6 settings are used when you do not provide the IPv4 settings.

7. Click **Routes** to manage IP routes.

   Note: if you do not add a route, the router will assign a default route for the network.

8. Click **Add** to enter a route.
9. Enter the IP, Netmask and Gateway address for the routes.

   Note:

   - Select **Ignore automatically obtained routes** to use the routes that you have entered and ignore the routes that are obtained from the router.
   - Select **Use this connection only for resources on its network** option to selectively route network traffic through this connection. If you select this option, you cannot use this connection as the default connection.

10. Click **Save**.

Configure IPv6 Settings

Internet Protocol version 6 is the newest version of the Internet Protocol suite. To configure IPv6 settings:

1. Click the **IPV6 Settings** tab in the Network Connections window.

   Note: By default, the **method** is set to **Automatic**; click **Save** to configure the network automatically.

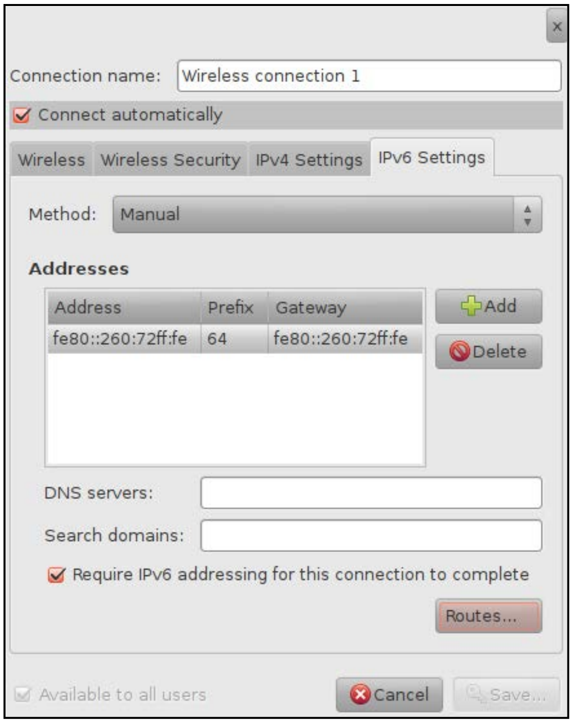
2. In the **method** field, select **Automatic addresses only**.
3. In the **DNS server's** field, enter a DNS server address.
4. In the **Search domains** field, enter a domain name. *For example, vxl.net.in*
5. In the **DHCP client ID** field, enter a DHCP client ID.
6. Click **Save**.

   Note: Select **Automatic, DHCP only** to automatically configure your network using DHCP.

   For manual configuration:

1. From the **method** drop-down list, select **Manual**.
2. Click **Add.**
3. In the **Address**, **Prefix** and **Gateway** fields, enter the thin client IP address, prefix and gateway address.
4. In the **DNS server's** field, enter a DNS server address.
5. In the **Search domains** field, enter a domain name.

   Note: Select the **Require the IPv6 addressing for this connection to complete** to use only the IPv6 settings for your connection. If you do not select this option, IPv4 settings are used when you do not provide the IPv6 settings.



Connection name: Wireless connection 1

☑ Connect automatically

Method: Manual

Address	Prefix	Gateway
fe80::260:72ff:fe	64	fe80::260:72ff:fe

DNS servers:

Search domains:

☑ Require IPv6 addressing for this connection to complete

☑ Available to all users

6. Click **Route** to manage IP routes.

   Note: If you do not add a route, the router will assign a default route for your network.

7. Click **Add** to enter a route.
8. Enter the IP address, prefix, gateway and metric for the routes.

   Note:

   - Select **Ignore automatically obtained routes** to use the routes that you have entered and ignore the routes that are obtained from the router.
   - Select **Use this connection only for resources on its network** option to selectively route network traffic through this connection. If you select this option, you can never use this connection as the default connection.

9. Click **Save.**

Deleting a Wireless Connection

1. From the **Profiles** list, select a connection that you want to delete.
2. Click **Delete,** the wireless connection is deleted.

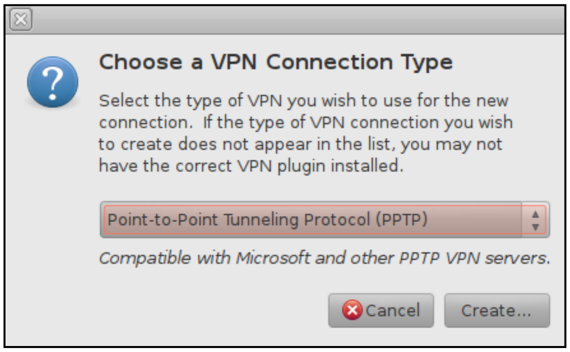
VPN Connection

A VPN (Virtual Private Network) connection is used to connect your client securely to a remote network. VPN connections can be used to connect two geographically distant facilities securely using the public network.

Note: VPN is currently not functional.

Creating a VPN Connection

1. In the network configuration window, click the **VPN** tab.
2. Click **Add**.



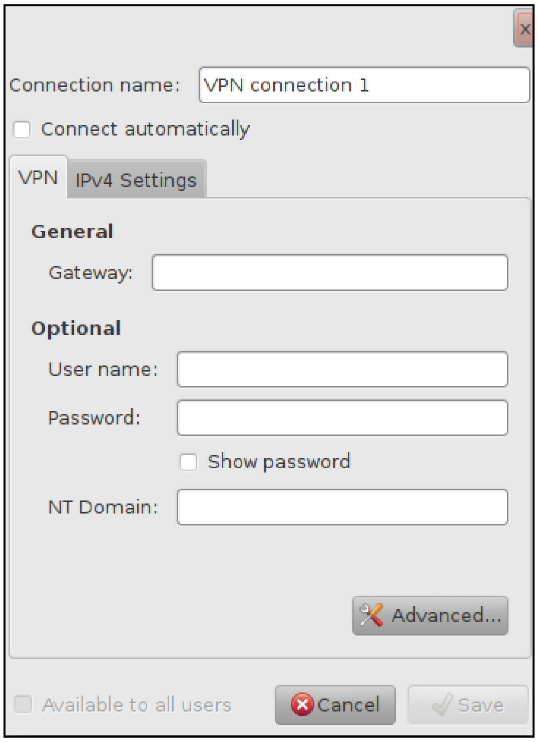
Choose a VPN Connection Type

Select the type of VPN you wish to use for the new connection. If the type of VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

Point-to-Point Tunneling Protocol (PPTP)

Compatible with Microsoft and other PPTP VPN servers.

3. From the **Choose a VPN Connection Type** drop-down list, select a type of VPN connection.
4. Click **Create.**
5. In the **Connection** name field, enter a connection name.



6. Select **Connect automatically** to automatically connect to this network when the client is restarted.
7. In the **Gateway** field, enter a gateway address.

You can make your VPN connections secure by providing the following information:

8. In the **User name** field, enter a user name.
9. In the **Password** field, enter a password.

> **Note:** Select **show password** to make the password that you have typed visible in plain text.

10. In the **NT Domain** field, enter a NT Domain name. The NT Doman name is your network domain name.

To configure advanced VPN settings:

1. Click **Advanced**, PPTP Advanced Options window appears.

Authentication

2. In the **Allow the following authentication methods** selection box, select the required authentication methods.

Security and Compression

3. Select **Use point-to-point encryption** to encrypt VPN data transmission.
4. From the **security** drop-down list, select 128-bit or 40-bit encryption.

> **Note:** 128-bit is more secure than 40-bit encryption.

5. Select **Allow stateful encryption:** This option enables the reuse of information across various encryption algorithms. Selecting this option optimizes the encryption process.

6. Select **BSD data compression:** This option enables data compression using the BSD data compression method. Selecting this option saves bandwidth.
7. Select **Allow Deflate data compression:** This option enables deflate data compression algorithm. Selecting this option compresses data transmitted through the VPN.
8. Select **Use TCP header compression**: This option enables TCP header compression; it improves performance over slow serial links by compressing the TCP headers.

Echo

9. Select **Send PPP echo packets** check box if you want to check for the presence (or absence) of the modem.
10. Click **Save**.

Configuring VPN Connection

1. From the **Profiles** list, select a connection that you want to configure.
2. Click **Edit**.
3. Click **IPv4 Settings**.
4. From the **Method** drop-down list, **Automatic (VPN**) is the default option**.** Click **Save** to configure the connection.

To provide custom DNS address:

1. In the **Method** field select **Automatic (VPN) addresses only**.
2. In **the DNS servers** field, enter a DNS server address.
3. In the **Search domains** field, enter a domain name.
4. Click **Routes** to manage IP routes.
5. Click **Add** to enter a route.

   Note:

   - Select **Ignore automatically obtained routes** to use the routes that you have entered and ignore the routes that are obtained from the router.
   - Select **Use this connection only for resources on its network** option to selectively route network traffic through this connection. If you select this option, you can never use this connection as the default connection.

6. Click **Save.**

Exporting VPN Settings

1. From the **Profiles** list, select a connection that you want to export.
2. Click **Export**.
3. In the **Name** field, enter an appropriate name.
4. Select the location where you want to save the VPN settings.
5. Click **Save**.

Importing VPN Settings

1. Click the **VPN** tab.

2. Click **Import**.
3. Select the **.conf** file to import.
4. Click **Open**. The configuration file will be imported with the settings.

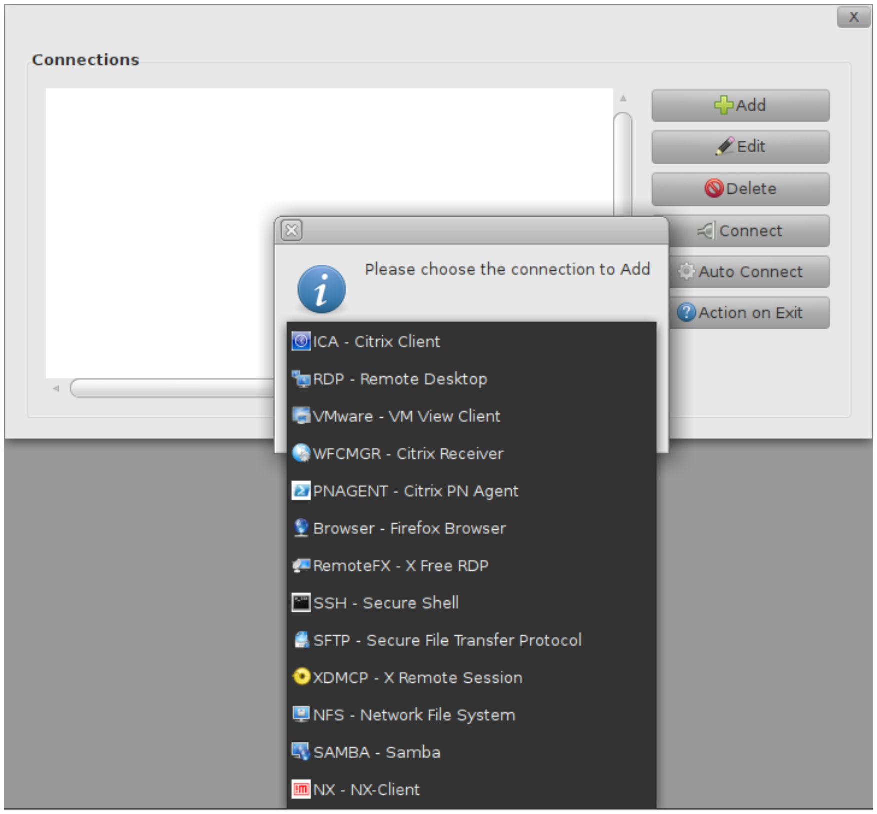
Deleting a VPN Connection

1. From the **Profiles** list, select a connection that you want to delete.
2. Click **Delete**, the VPN connection is deleted.

Connection Manager

Gio 5 provides several options to connect your thin client to a server. The connectivity options provided are:

- ICA – Citrix Client
- RDP – Remote Desktop
- VMware – VM View Client
- WFCMGR – Citrix Receiver
- PNAGENT– Citrix PN Agent
- Browser – Firefox Browser
- Remote FX – X FreeRDP
- SSH – Secure Shell
- SFTP – Secure File Transfer Protocol
- XDMCP – X Remote Session
- NFS – Network File System
- SAMBA – Samba
- NX – NX client



Please choose the connection to Add

Connection Options

You can configure your connection by selecting options that add connection functionality.

Following is a list of connection options available with their information; the options provided may vary based on the connection:

- Map Local Printers: This option maps your local printer with the terminal server. You should have already created and configured a local printer to enable this option. For more information on adding a printer, refer section 'Printer' on page 72.
- Speed Screen BA: This option enables Speed Screen Browser Acceleration, this feature helps to display images faster and thus make the web browsing experience smooth.

  Note: Speed Screen acceleration does not work when *Adobe Flash* content is enabled. If you want to use this feature, you have to disable *Adobe Flash*.
- Speed Screen: This option enables Speed Screen latency reduction; this option is useful when you are using a slow connection with latency of more than 100 ms.
- Enable Audio Input: This option enables audio input to your thin client.
- Use ICA compression: This option enables compression of ICA data stream transmitted over a network.
- Full Screen: This option enables the full screen mode for your connection; your remote desktop will be displayed in full screen.
- Map Serials Ports: This option maps the terminal server serial ports with your thin client serial ports, selecting this option redirects serial port devices connected to your client to the terminal server.
- Map Local Smartcard readers: This option maps your local smartcard reader with the terminal server's smart card reader.
- Activate Enable OSS: This option enables the Off Screen Surface (OSS) feature that enables the ICA Client to draw screen updates to an in-memory bitmap rather than to the screen. This option improves network bandwidth efficiency.
- Approximate Colors: This option enables the use of approximate colors that are available in the client if the exact colors are not available. This feature eliminates color flashing when switching between applications.
- EUKS: This option enables the support for Extended Unicode Keyboard Support (EUKS) on Windows Server.
- Data Compression: This option enables data compression of the RDP data stream.
- Numlock Synchronization: This option enables numlock synchronization between your server and thin client. Use numlock synchronization when you want to use your thin client keyboard to access features of an application running on the server.
- Don't send motion events: This option prevents the transmission of motion events such as movement of the mouse pointer on the screen to the server, only the interface interactions are sent to the server. This option saves bandwidth.
- Force bitmap updates: This option forces the server to send screen updates as bitmaps rather than using higher-level drawing operations. Bitmap updates saves bandwidth.
- Local Smart Card readers: This option maps your local smartcard reader with the terminal server's smart card reader.

- Console Connection: This option allows you to connect to the console of the terminal server; this option requires Windows Server 2003 or Windows Server 2008.
- Hide WM decorations: This option hides the Window Manager decorations.

o Map client Drives (USB:z): This option maps the client drives with the drives in the terminal server.

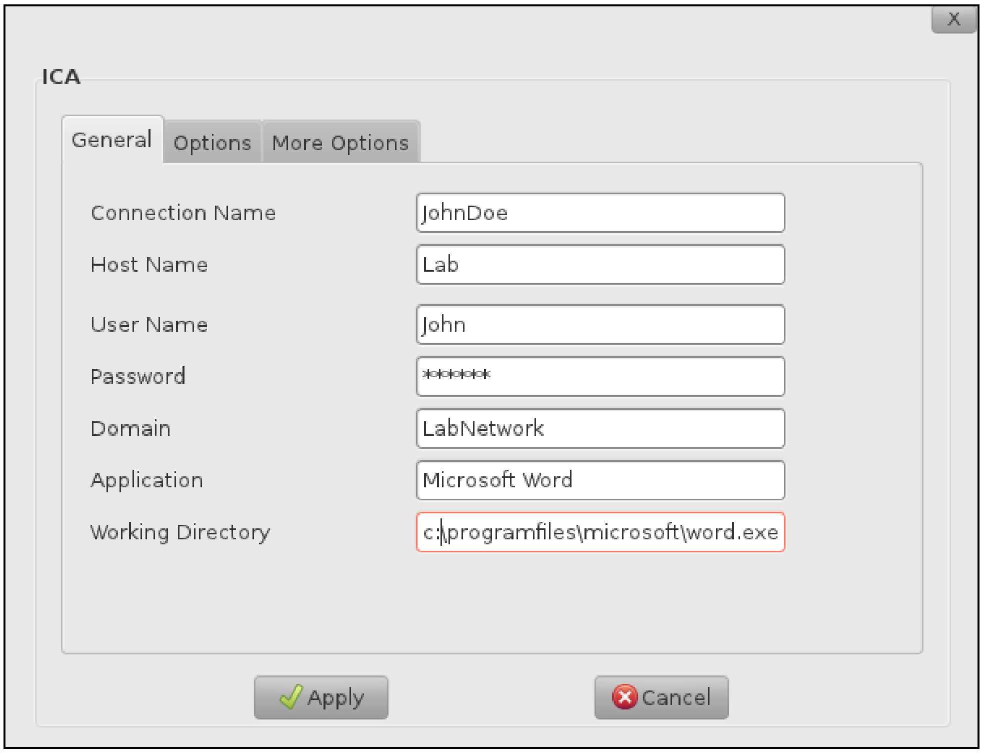
- Keep WM keybindings: This option enables all your Window Manager Hotkeys.
- Enable RemoteFX: This option enables Microsoft RemoteFX, this is a new feature that is included in Windows Server 2008 R2 with Service Pack 1 (SP1). It introduces a set of end-user experience enhancements for Remote Desktop Protocol (RDP) that enable a rich desktop environment within your corporate network.
- Hide Window Decorations: This option hides window decorations such as the graphical high-color window tab and transparency.
- Console audio: This option enables the audio port on the thin client.
- Disable Authentication: This option disables authentication when connecting to this connection. Selecting this option will automatically connect you to the server without any authentication.
- Disable Mouse Motion: This option disables mouse cursor movements. Selecting this option will make the mouse gestures useless.
- Disable Bitmap Cache: This option disables the storage of bitmap images locally in the thin client. Select this option if you have a connection with adequate bandwidth for the connection to work smoothly.
- Disable Wallpaper: This option disables the wallpaper when you are logged on to the remote computer. Selecting this option saves bandwidth.
- Disable Full Window Drag: This option enables the drag copy feature. Select this option when you do not want folder contents to appear when you drag the folder to a new location.
- Disable Theming: Select this option to prevent users from applying desktop themes when connected to the remote server.
- Disable TLS Encryption: This option disables Transport Layer Security encryption for this connection.
- Certificate Verification: This option enables the connection to check for a valid certificate before connecting to the remote server.
- Connect to Console Session: This option starts a non-graphical console session. Select this option to access the server’s command console.
- Disable Checksum with Std RDP Connection: This option disables the checksum validation of the RDP data stream.
- Set Keyboard Layout: This option sets the keyboard layout to the one that is currently used by the thin client.
- Enable Compression: This option enables the compression of the connection data stream.
- Disable Fast path: This option disables fast path. Fast path makes commonly occurring tasks faster by optimizing those processes.
- Disable Offscreen Bitmap: This option disables offscreen bitmap. This option stops the server to change the default client-rendering surface to one of the bitmaps created in the Offscreen Bitmap Cache.

- Enable NSCode: This option enables NSCodec bitmap compression; this option is used when the RDP session color depth is 32 bpp and the bitmap of interest is either 24 bpp (RGB with no alpha channel) or 32 bpp (RGB with an alpha channel).
- Enable Desktop Composition: This option enables Windows interface elements such as transparency.
- Disable Menu Animation: This option disables menu animation such as graphic slide, color change. Selecting this option saves bandwidth.
- Disable Standard RDP Encryption: This option to disables standard RDP encryption.
- Disable N/W level Authentication: This option disables network authentication required before connection to the remote server.

Configuring a Citrix ICA Connection

Independent Computing Architecture (ICA) is a protocol for managing application server systems. ICA provides rules for information transfer between a server and a client. An ICA connection can be configured based on your connection preferences; to configure an ICA connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please, choose the connection to add** drop-down list, select **ICA – Citrix Client**.
6. Click **OK**. The **ICA** window appears.



Connection Name JohnDoe

Host Name Lab

User Name John

Password ******

Domain LabNetwork

Application Microsoft Word

Working Directory c:\programfiles\microsoft\word.exe

7. In the **Connection Name** field, enter a connection name.
8. In the **Host Name** field, enter a host name.
9. In the **User Name** field, enter a user name.
10. In the **Password** field, enter a password.

Note: Please make note of your user name and password. Your user name and password are required later when establishing the ICA connection.

11. In the **Domain** field, enter a domain name.

Note: The domain name is the domain name of the remote server.

12. In the **Application** field, enter the name of the application. *For example, Microsoft Word.*

13. In the **Working Directory** field, enter the path of the working directory. *For example,* `C:\programfiles\microsoft\word.exe`*.*

14. Click **Options** tab.

15. From the **Display Resolution** spin box, select a display resolution.

16. Select the connection options based on your preference. The various connection options are:

    - Map Local Printers
    - Use ICA compression
    - Speed Screen BA
    - Speed Screen
    - Enable Audio Input
    - Map Serials Ports
    - Map Local Smartcard readers
    - Activate Enable OSS
    - Approximate Colors
    - EUKS

    For information about the connection options, see section ‘Connection Options’ on page 35.

17. From the **Desired Color Depth** spin box select the required color depth. You can select **1 (8 bit), 4 (16 bit)** or **8 (24 bit).**

18. From the **HDX Client Redirection** spin box select ON or OFF.

19. From the **Flash Redirection** spin box set the status to Always, Never or Ask.

20. Click **More Options** tab.

21. Enter your preferred values for the following options:

    - **Speed Screen BA Decompressed Cache size**: Enter the value of the decompressed cache allocated to Speed Screen Browser Acceleration.
    - **Speed Screen BA Compressed Cache size**: Enter the value of the compressed cache allocated to Speed Screen Browser Acceleration.
    - **TW2 Stop Watch minimum count**: Enter the minimum ThinWire 2 stop watch count. This is an application user interface synchronization feature.
    - **TW2 Stop Watch scale count**: Enter a ThinWire 2 stop watch scale count. This option regulates the disparity between the speeds of different graphics operations. *For example, some WinCE terminals can scroll quickly but draw relatively slowly. This count provides a scale factor to be applied to values returned by the stopwatch timers to correct this*.

22. Select the preferred option for the following parameters:

    - **Audio Support**: Select the quality of sound. You can select **High Quality, Medium Quality** or **Low Quality** audio. Selecting **Off** will disable audio.

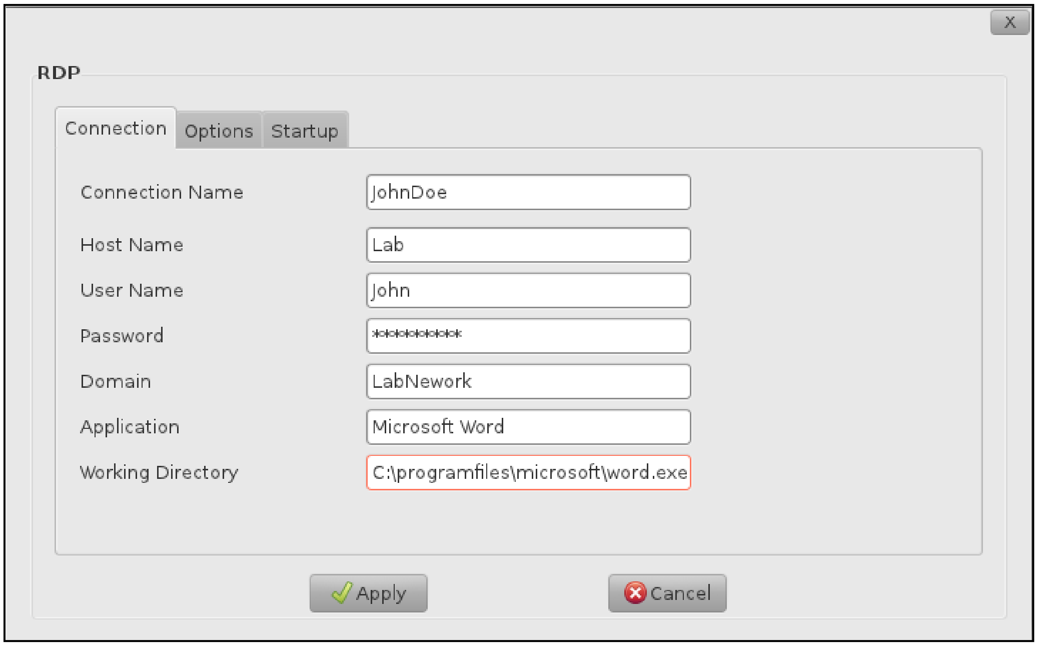
- **Encryption Mode**: Select the encryption mode. You can select **RC5 (128 bit**), **RC5 (128 bit-Login Only)**, **RC5 (40 bit)**, **RC5 (50 bit)** encryption or **Basic**.
- **Transparent Key pass through**: Select to determine how certain key combinations are used when connecting to ICA. You can select **Server with full screen sessions only**: Key combinations apply to the non-seamless ICA session in full screen mode, **Translated/Local:** Key combinations apply to local desktop or **Server:** Key combinations apply to seamless and non-seamless ICA connections.
- **Browser Protocol**: Select a browser protocol for the connection. You can select **TCP+HTTP, SSL/TLS +HTTPS** or **TCP/UDP**.

23. Click **Apply**, the confirmation window appears.
24. Click **Yes**.

Configuring a Microsoft RDP Connection

Remote Desktop Protocol (RDP) is a communication protocol for the Windows operating system. The protocol provides a thin client, access to a Windows desktop or server. To configure an RDP connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list, select **RDP – Remote Desktop**.
6. Click **OK**. The **RDP** window appears.



Connection Name: JohnDoe
Host Name: Lab
User Name: John
Password: *********
Domain: LabNework
Application: Microsoft Word
Working Directory: C:\programfiles\microsoft\word.exe

7. In the **Connection Name** field, enter a connection name.
8. In the **Host Name** field, enter a host name.
9. In the **User Name** field, enter a user name.

10. In the **Password** field, enter a password.

    Note: Please make note of your user name and password. Your user name and password are required later when establishing an RDP connection.

11. In the **Domain** field, enter a domain name.

    Note: The domain name is the domain name of the remote server.

12. In the **Application** field, enter the name of the application. *For example, Microsoft Word.*
13. In the **Working Directory** field, enter the path of the working directory. *For example, C:\programfiles\microsoft\word.exe.*
14. Click **Options** tab**.**
15. From the **Display Resolution** spin box, select a display resolution based on your monitor properties
16. From the **Color Depth** spin box, select a color depth. Greater color depth will render more vibrant images
17. From the **Audio Forwarding** spin box, select local or remote audio forwarding. Selecting **off** will disable this option
18. From the **RDP Protocol Version** drop-down list, select **RDP4** or **RDP5** version of the protocol
19. Select the connection options based on your preference. The various connection options are:

    - Map serial ports
    - Data Compression
    - Force bitmap updates
    - Map client Drivers (USB:z)
    - Don't send motion events
    - Numlock Synchronization
    - Local Smart Card readers
    - Console Connections
    - Hide WM decorations

For information about the connection options, see section 'Connection Options' on page 35.

20. Click the **Startup** tab**.**
21. Select the services that have to be launched when your client starts up, the services that you can choose are:

    - **Keep WM keybindings**: This option keeps the same window hotkeys as the previous session.
    - **Printer Name**: Select the printer name from the drop-down list. You have to configure your printer before you can select it here.
    - **Windows Printer Driver Name**: Specify the path and file name of the driver.

22. Click **Apply**, the confirmation window appears.
23. Click **Yes**.

Configuring a VMware View Client Connection

VMware View is a commercial desktop-virtualization product developed by VMware. VMware View allows a user to connect to a remote virtual machine. To configure a VMware View connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list, select **VMware – VM View Client.** The **VMware** window opens.
6. In the **Connection Name** field, enter a connection name.
7. In the **Host Name** field, enter a host name.
8. In the **User Name** field, enter a user name.
9. In the **Password** field, enter a password.

   Note: Please make note of your user name and password. Your user name and password are required later when establishing a *VMware View* connection.

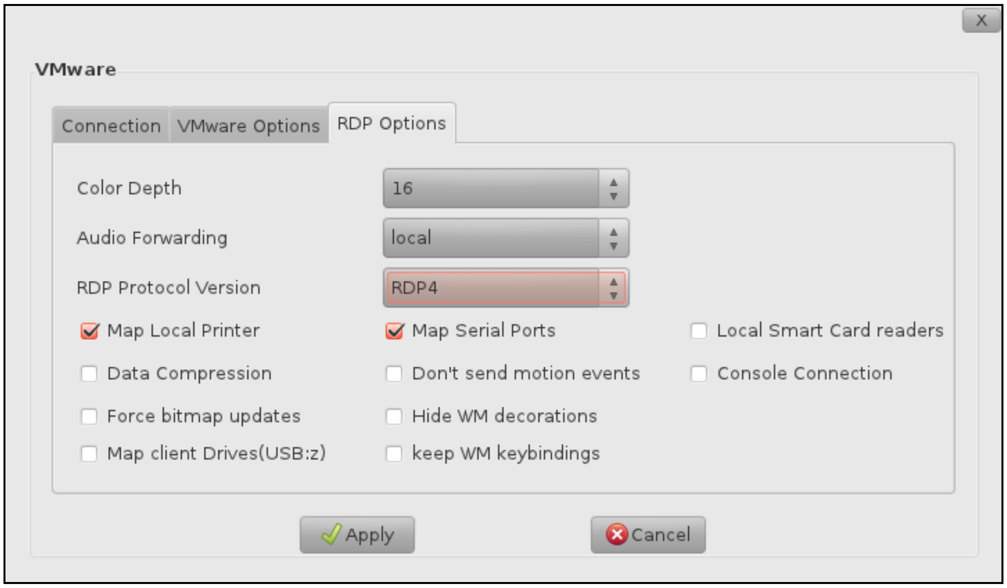
10. In the **Domain** field, enter a domain name.

    Note: The domain name is the domain name of the remote server.

11. Click **VMware Options** tab.
12. From the **Preferred Connection Protocol** spin box, select **RDP** or **PCOIP** protocol.
13. In the **Desktop Name** field, enter the desktop name.
14. Click **RDP Options** tab.
15. From the **Color Depth** spin box, select a color depth. Greater color depth will render images that are more vibrant.
16. From the **Audio Forwarding** spin box, select **local** or **remote**. Selecting **off** will disable this option.
17. From the **RDP Protocol Version** drop-down list, select if you want to use **RDP4** or **RDP5** version of the protocol.
18. Select the connection options based on your preference. The various connection options are:

    - Map Local Printer
    - Data Compression
    - Force bitmap updates
    - Map client Drives (USB:z)
    - Map Serial Ports
    - Don’t send motion events

- Hide WM decorations
- Keep WM keybindings
- Local Smart Card readers
- Console Connection



Color Depth: 16

Audio Forwarding: local

RDP Protocol Version: RDP4

☑ Map Local Printer
☑ Map Serial Ports
□ Local Smart Card readers
□ Data Compression
□ Don't send motion events
□ Console Connection
□ Force bitmap updates
□ Hide WM decorations
□ Map client Drives(USB:z)
□ keep WM keybindings

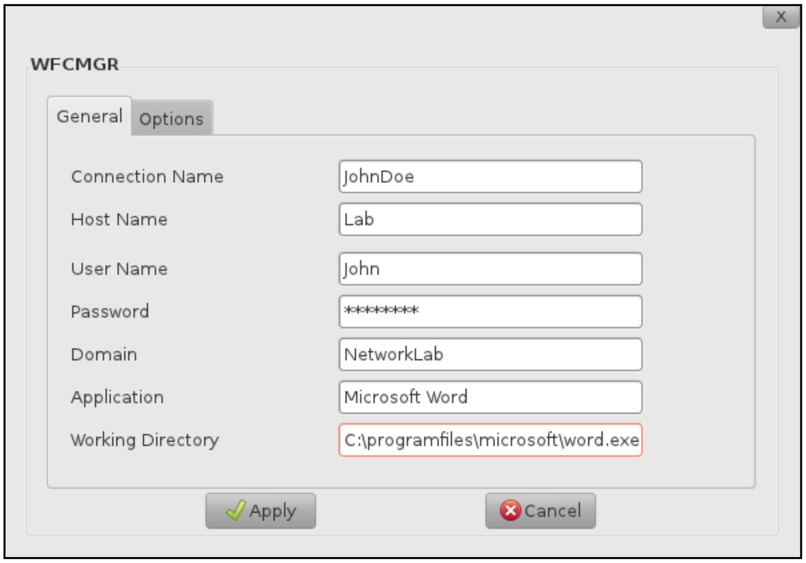
For information about the connection options, see section ‘Connection Options’ on page 35.

19. Click **Apply**, the confirmation window appears.
20. Click **OK**.

Configuring a Citrix Receiver Connection (WFCMGR)

Citrix Receiver is a commercial desktop-virtualization product developed by Citrix; it allows you to run applications hosted on a remote server. To configure a Citrix Receiver connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Clicks **Add**.
5. From the **Please, choose the connection to add** drop-down list, select **WFCMGR – Citrix Receiver**.
6. Click **OK**. The **WFCMGR** window appears.



Connection Name	JohnDoe
Host Name	Lab
User Name	John
Password	********
Domain	NetworkLab
Application	Microsoft Word
Working Directory	C:\programfiles\microsoft\word.exe

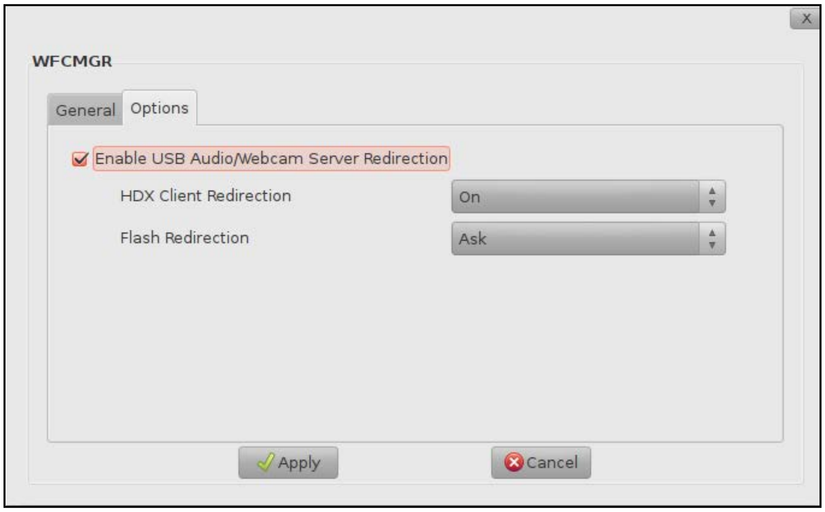
7. In the **Connection Name** field, enter a connection name.
8. In the **Host Name** field, enter a host name.
9. In the **User Name** field, enter a user name.
10. In the **Password** field, enter a password.

> **Note:** Please make note of your user name and password. Your user name and password are required later when establishing the connection.

11. In the **Domain** field, enter a domain name.

> **Note:** The domain name is the domain name of the remote server.

12. In the **Application** field, enter the name of the application. *For example, Microsoft Word.*
13. In the **Working Directory** field, enter the path of the working directory. *For example, C:\programfiles\microsoft\word.exe.*
14. Click the **Options** tab.



☑ Enable USB Audio/Webcam Server Redirection

HDX Client Redirection: On

Flash Redirection: Ask

15. Select **Enable USB Audio/Webcam Server Redirection** to map USB headphones, speakers and webcam to server.

    For more information on **Enable USB Audio/Webcam Server Redirection** option refer section ‘Enable USB Audio/Webcam Server Redirection’ on page 47.

    Note: Selecting this option disables audio play back on Windows Media Player.

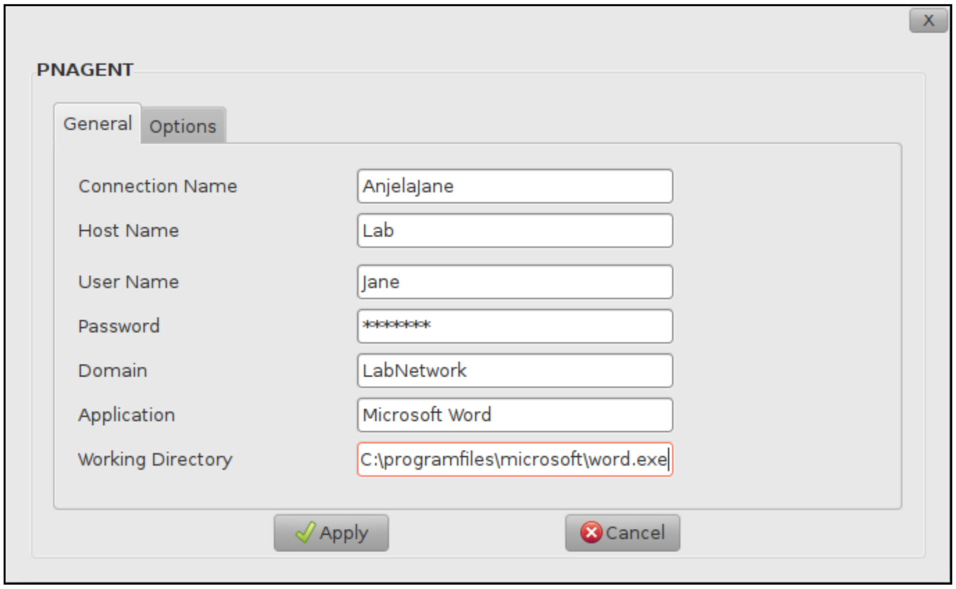
16. From the **HDX Client Redirection** spin box, select **On** to get a high definition desktop virtualization user experience. T he video and audio rendered in the XenDesktop is from the client.

    Note: If **HDX Client Redirection** is off then the video and audio rendered in the XenDesktop is from the server.

17. From the **Flash Redirection** spin box, select **Always** to always view the Optimization for flash redirection option in Internet Explorer browser.
18. Click **Apply**, the confirmation window appears.
19. Click **OK**.

Configuring a Citrix PNAGENT connection

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list,
   select **PNAGENT- Citrix PN Agent ..**
6. Click **OK**. The **PNAGENT** window appears.



PNAGENT

Connection Name: AnjelaJane
Host Name: Lab
User Name: Jane
Password: *******
Domain: LabNetwork
Application: Microsoft Word
Working Directory: C:\programfiles\microsoft\word.exe

7. In the **Connection Name** field, enter a connection name.
8. In the **Host Name** field, enter a host name.
9. In the **User Name** field, enter a user name.
10. In the **Password** field, enter a password.

    Note: Please make note of your user name and password. Your user name and password are required later when establishing the ICA connection.

11. In the **Domain** field, enter a domain name.

    Note: The domain name is the domain name of the remote server.

12. In the **Application** field, enter the name of the application. *For example, Microsoft Word.*
13. In the **Working Directory** field, enter the path of the working directory. *For example,* `C:\programfiles\microsoft\word.exe`*.*
14. Click the **Options** tab.
15. Select **Enable USB Audio/Webcam Server Redirection** to map USB headphones, speakers and webcam to server.

    For more information on **Enable USB Audio/Webcam Server Redirection** option refer section ‘Enable USB Audio/Webcam Server Redirection’ on page 47.

    Note: Selecting this option disables audio play back on Windows Media Player.

16. Click **Apply**. The confirmation window appears.
17. Click **OK**.

Enable USB Audio/Webcam Server Redirection

If the **Enable USB Audio/Webcam Server Redirection** option is not selected:

- Do not connect multiple USB audio devices at the same time.
- Ensure that USB Audio device is connected to the USB port of the Thin Client before using windows media player.
- Do not unplug the audio device while playing a media file on Windows Media Player.
- Citrix HDX WebCamera is the default name of any webcam connected to the thin client.
- Citrix HDX Audio is the default name of any Audio device connected to the thin client.
- The internal MIC on USB webcams will not be available for recording.

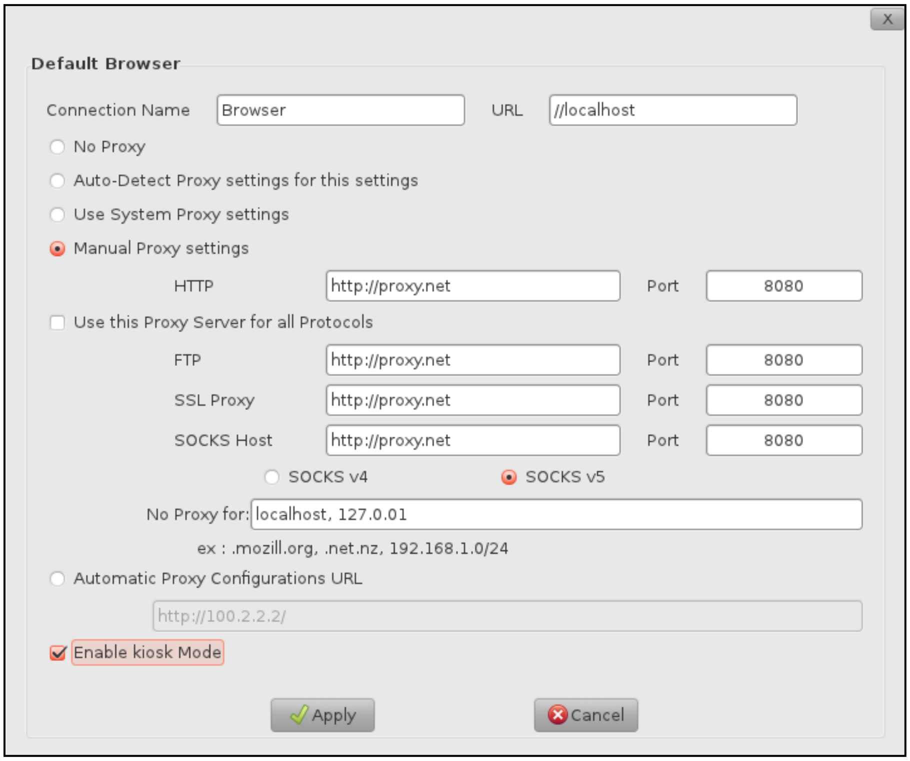
If the **Enable USB Audio/Webcam Server Redirection** option is selected:

- USB audio output will not be available through Windows Media Player.
- The name of the USB webcam connected to Thin Client is displayed under Devices **and Printer** in the server's OS.
- The name of the USB audio device connected to the Thin Client is displayed in **Sound** section of server's OS. You can make it as a default sound device.
- The Internal MIC on USB webcams can be used for recording.

Configuring a Firefox Browser Connection

A Browser connection enables the thin client to access web-based services through a thin client browser. This connection is well suited for thin client kiosks using a web application hosted on a server. To set up a browser connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Click **Add**.
5. From the **Please, choose the connection to add** drop-down list, select **Browser – Firefox Browser**.
6. Click **OK**. The **Default Browser** window appears



Default Browser

Connection Name: Browser URL: //localhost

○ No Proxy

○ Auto-Detect Proxy settings for this settings

○ Use System Proxy settings

● Manual Proxy settings

HTTP: http://proxy.net Port: 8080

□ Use this Proxy Server for all Protocols

FTP: http://proxy.net Port: 8080

SSL Proxy: http://proxy.net Port: 8080

SOCKS Host: http://proxy.net Port: 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.01

ex : .mozill.org, .net.nz, 192.168.1.0/24

○ Automatic Proxy Configurations URL

http://100.2.2.2/

☑ Enable kiosk Mode

7. In the **Connection Name** field, enter a connection name of your preference.
8. In the **URL** field, enter the URL of the server.
9. You can choose from the following proxy settings for your connections.

   - **No Proxy**: Disable proxy. This is the default option.
   - **Auto-Detect Proxy settings for this settings**: Auto-detect the proxy settings and configure it for this connection.
   - **Use System Proxy settings**: Use the proxy settings already available in the thin client.
   - **Manual Proxy settings**: Select this option to enter manual proxy settings based on your preference. Follow these steps to configure manual proxy settings:

    a. In the **HTTP** field, enter a HTTP address; enter the port number in the corresponding **port** field.

    b. Select **Use this proxy Server for all Protocols** to use this proxy universally for the connections that use different protocols such as HTTP, FTP.

    c. In the **FTP** field, enter an FTP address; enter the port number in the corresponding **port** field.

    d. In the **SSL Proxy** field, enter a SSL Proxy address; enter the port number in the corresponding **port** field.

    e. In the **SOCKS Host** field, enter a SOCKS Host address; enter the port number in the corresponding **port** field.

    f. Select either **SOCKS v4** or **SOCKS v5** based on your preference; these are the two different versions of the SOCKS protocol.

    g. In the **No Proxy for** field, enter the name or IP address for which you do not want to use the proxy settings.

- **Automatic Proxy Configurations URL**: Select this option to automatically configure your proxy settings from a remote location. Enter the URL of the remote location.

10. Select **Enable kiosk** to launch the browser connection as a Kiosk connection.
11. Click **Apply**. The confirmation window appears.
12. Click **OK**.

Configuring a RemoteFX (X FreeRDP) Connection

RemoteFX is a technology that enhances the visual experience of the Remote Desktop Protocol connection. FreeRDP is an open source implementation of the Microsoft RDP protocol, released under the Apache license. To setup a FreeRDP connection:

1. On the desktop sidebar, click **Settings**.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Click **Add**.
5. From the **Please, choose the connection to add** drop-down list, select **Remote FX – X Free RDP**.
6. Click **OK**. The **Remote FX** window appears.
7. In the **Connection Name** field, enter a connection name of your preference.
8. In the **Server** field, enter the IP address of the server.
9. In the **Port Number** field, enter a valid port number.
10. In the **User Name** field, enter a user name of your preference.
11. In the **Password** field, enter a password of your preference.

    Note: Please make note of your user name and password. Your user name and password are required later when establishing the connection.

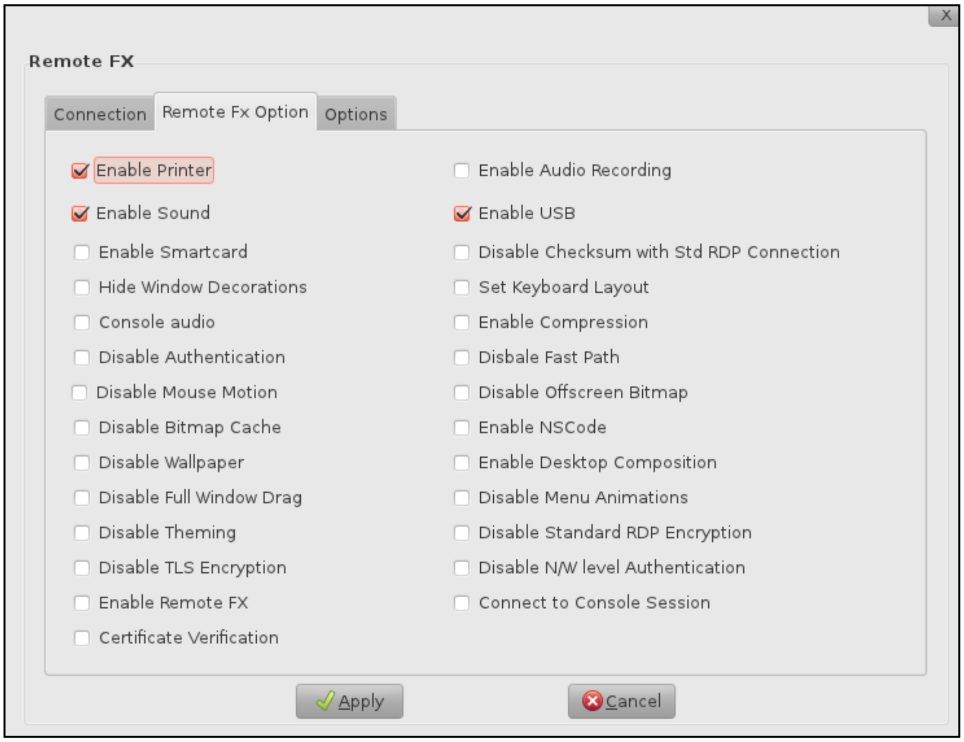
12. In the **Domain** field, enter a domain name.

13. In the **Domain Password**, enter the password of your domain.
14. In the **Working directory** field, enter a working directory path. *For example,* `C:\programfiles\microsoft\word.exe`.
15. In the **Start-up Shell** field, enter a start up application. This option starts a specified application instead of the default explorer.
16. In the **Window Title** field, enter the Window Title that must appear for this connection. You can choose a Window Title of your preference.
17. Click **RemoteFx Option** tab.
18. Select from the following options for your connection based on your preference:

    - Enable Printer
    - Enable Sound
    - Enable Smartcard
    - Hide Window Decorations
    - Console audio
    - Disable Authentication
    - Disable Mouse Motion
    - Disable Bitmap Cache
    - Disable Wallpaper
    - Disable Full Window Drag
    - Disable Theming
    - Disable TLS Encryption
    - Enable Remote FX
    - Certificate Verification
    - Enable Audio Recording
    - Enable USB
    - Disable Checksum with Std RDP Connection
    - Set Keyboard Layout
    - Enable Compression
    - Disable Fast Path
    - Disable Offscreen Bitmap
    - Enable NSCode
    - Enable Desktop Composition
    - Disable Menu Animations
    - Disable Standard RDP Encryption

- Disable N/W level Authentication
- Connect to Console Session

For information about the connection options, see section ‘Connection Options’ on page 35.



☑ Enable Printer
☑ Enable Sound
☐ Enable Smartcard
☐ Hide Window Decorations
☐ Console audio
☐ Disable Authentication
☐ Disable Mouse Motion
☐ Disable Bitmap Cache
☐ Disable Wallpaper
☐ Disable Full Window Drag
☐ Disable Theming
☐ Disable TLS Encryption
☐ Enable Remote FX
☐ Certificate Verification

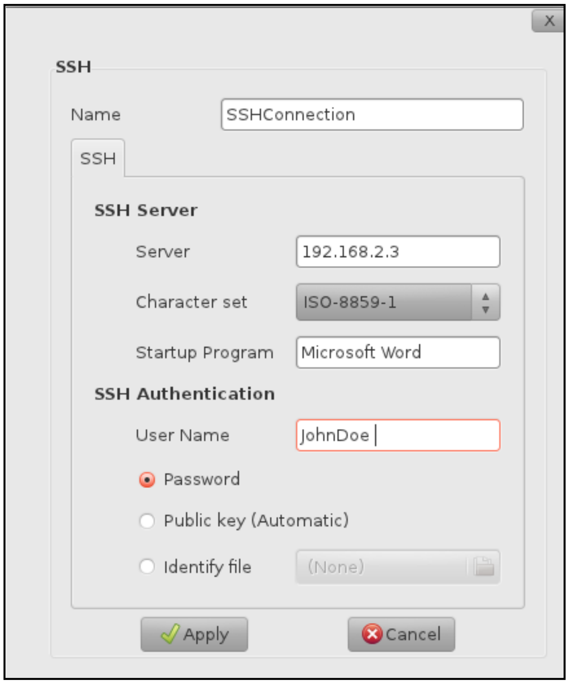
☐ Enable Audio Recording
☑ Enable USB
☐ Disable Checksum with Std RDP Connection
☐ Set Keyboard Layout
☐ Enable Compression
☐ Disbale Fast Path
☐ Disable Offscreen Bitmap
☐ Enable NSCode
☐ Enable Desktop Composition
☐ Disable Menu Animations
☐ Disable Standard RDP Encryption
☐ Disable N/W level Authentication
☐ Connect to Console Session

19. Click **Options** tab.
20. In the **Load a Virtual Channel Plugin** field, enter the path from which the virtual plugin is to be loaded.
21. In the **Load on Extension** field, enter a name of the application to load.
22. In the **Remote App to Connect** field, enter the remote application name.
23. From the **Remote FX mode** drop-down list, select video or image mode.
24. From the **Set Geometry** drop-down list, select a monitor resolution based on your monitor. The connection supports resolution up to 1600x1200.
25. From the **Performance Flags** drop-down list, select the type of network that you are using for your connection. The options are: **broadband**, **modem** or **LAN**.
26. From the **Graphics Rendering** drop-down list, select **Software** or **Hardware** graphics rendering.
27. From the **NTLM Protocol Version** drop-down list, select the version of NTLM protocol.
28. From the **Force Protocol Security** drop-down list, select a security protocol for the connection. The options are **rdp**, **tls** and **nla**. The default security protocol is **nla**.
29. From the **Set Color Depth in Bit** drop-down list, select **8 bit**, **15 bit**, **16 bit**, **24 bit** or **32 bit** color depth. Greater color depth value will display more vibrant images.
30. Click **Apply**. The confirmation window appears.
31. Click **Yes**.

Configuring a Secure Shell (SSH) Connection

SSH is a network protocol that allows you to securely transmit information between your thin client and terminal server. To set up an SSH connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please, choose the connection to add** drop-down list, select **SSH – Secure Shell**.
6. Click **OK**. The **SSH** window appears.



SSH

Name: SSHConnection

SSH Server

Server: 192.168.2.3

Character set: ISO-8859-1

Startup Program: Microsoft Word

SSH Authentication

User Name: JohnDoe

● Password

○ Public key (Automatic)

○ Identify file (None)

7. In the **Name** field, enter the name of the SSH connection.
8. In the **Server** field, enter the IP address or domain name of the SSH server.
9. From the **Character set** drop-down list, select a character set of your choice. *For example, you may select ISO-8859-1.*
10. In the **Startup Program** field, enter the name of the startup program. *For example, Microsoft Word.*
11. In the **User Name** field, enter the user name for SSH authentication.
12. Select from the following authentication methods: **Password, Public key (automatic), Identity file**.

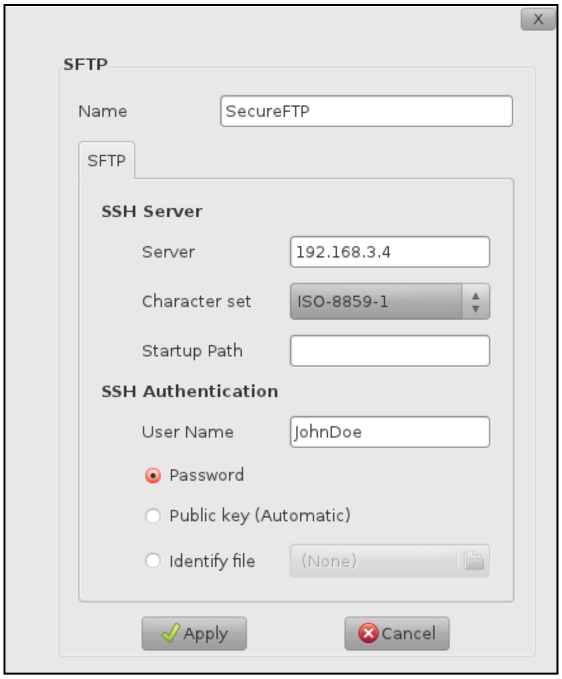
    Note: To select an identity file for authentication, click on the browse button next to **Identity file** and then click **Open**.

13. Click **Apply**. The confirmation window appears.
14. Click **Yes**.

Configuring a Secure File Transfer Protocol (SFTP) Connection

Secure File Transfer Protocol (SFTP) is a network protocol that provides secure file access, transfer and management over a network. To set up an SFTP connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list, select **SFTP – Secure File Transfer Protocol**.
6. Click **OK**. The **SFTP** window appears.



SFTP

Name: SecureFTP

SSH Server

Server: 192.168.3.4

Character set: ISO-8859-1

Startup Path:

SSH Authentication

User Name: JohnDoe

● Password

○ Public key (Automatic)

○ Identify file (None)

7. In the **Name** field, enter the name of the SFTP connection.
8. In the **Server** field, enter the IP address or domain name of the SSH server.
9. From the **Character set** drop-down list, select a character set of your choice. *For example, you may select ISO-8859-1.*
10. In the **Startup Path** field, enter the name of the startup program.
11. In the **User Name** field, enter the user name for SSH authentication.
12. Select from the following authentication methods: **Password, Public key (automatic), Identity file**.

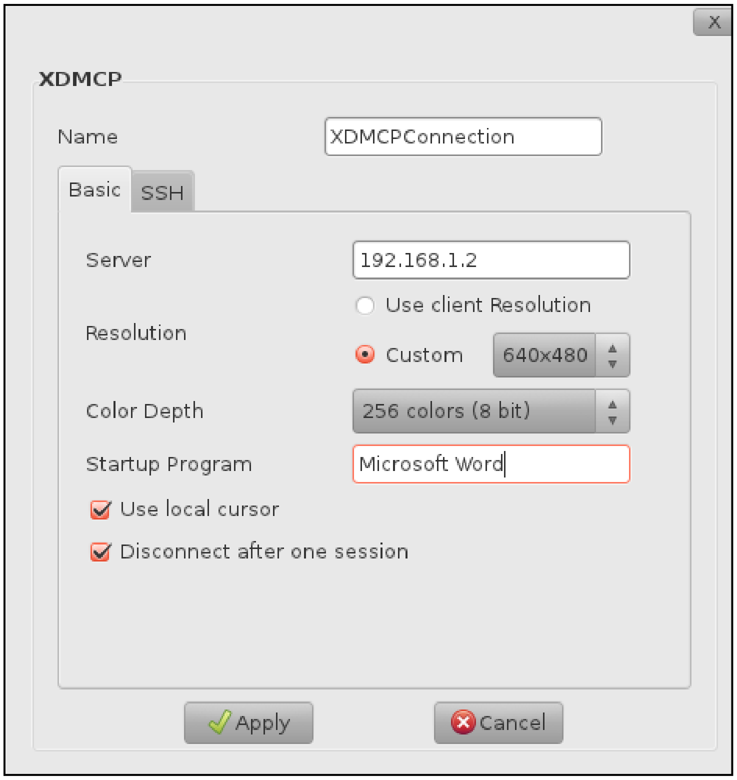
    Note: To select an identity file for authentication, click on the browse button next to Identity file and then click **Open**.

13. Click **Apply**. The confirmation window appears.
14. Click **Yes**.

Configuring an XDMCP Connection

XDMCP is a remote desktop protocol that can be used to access remote Linux desktops and servers. To set up an XDMCP connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list, select **XDMCP – X Remote Session**.
6. Click **OK**. The **XDMCP** window appears.



XDMCP

Name: XDMCPConnection

Basic | SSH

Server: 192.168.1.2

Resolution: ○ Use client Resolution ● Custom 640x480

Color Depth: 256 colors (8 bit)

Startup Program: Microsoft Word

☑ Use local cursor

☑ Disconnect after one session

7. In the **Name** field, enter the name of the XDMCP connection.
8. Click the **Basic** tab.
9. In the **Server** field, enter the IP address of XDMCP server.
10. For setting up the resolution of the client:

    - Select **Use client Resolution** for default client monitor resolution.

      or

    - Select a custom resolution from the **Custom** drop-down list.

11. From the **Color Depth** drop-down list, select a color depth based on your preference. Greater color depth will render images that are more vibrant.
12. In the **Startup Program** field, enter a start up program name.
13. Select **Use local cursor** to enable the use of the local thin client cursor.

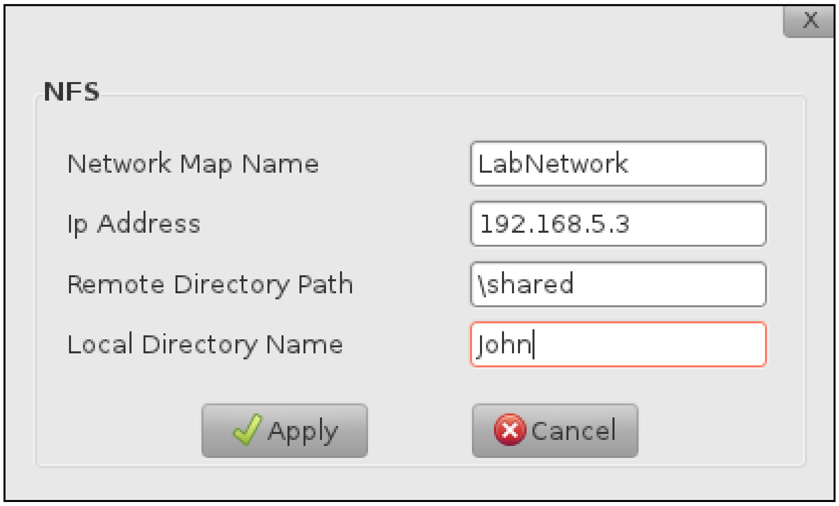
14. Select **Disconnect after one session** to disconnect this XDMCP connection after one session. Your XDMCP connection will not be automatically reconnected for consequent connections.
15. Click **Apply** if you do not want to configure SSH for this connection. Your XDMP connection is configured.
16. For setting up SSH, click **SSH** tab.
17. Select **Enable SSH tunnel** to enable an encrypted SSH tunnel for this connection.
18. Select **Tunnel via loopback Address** to enable tunneling via the XDMCP loopback address.
19. Select **Same server at port 22** to select the server at port 22 by default.
20. Select **Custom** to enter the IP address of an SSH server.
21. From the **Character set** drop-down list, select a character set. *For example, you may select ISO-8859-1.*
22. In the **User Name** field, enter the user name for SSH authentication.
23. Select one of the following authentication methods: **Password**, **Public key (automatic)**, **Identity file**.

    Note: To select an identity file for authentication, click on the browse button next to **Identity file** and then click **Open**.
24. Click **Apply.** The confirmation window appears.
25. Click **Yes**.

Configuring a Network File System Connection

A network drive is a storage unit connected to a network and shared by users in that network. A Network File System is used to read and write files on a network drive.
To set up a Network File System connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the **Connections** window appears.
4. Click **Add**.
5. From the **Please choose the connection to add** drop-down list, select **NFS – Network File System**.
6. Click **OK**. The **NFS** window appears.



Network Map Name: LabNetwork
Ip Address: 192.168.5.3
Remote Directory Path: \shared
Local Directory Name: John

7. In the **Network Map Name** field, enter the name of the NFS network map.
8. In the **IP Address** field, enter the IP address or hostname of the NFS server.
9. In the **Remote Directory Path** field, enter the shared folder name.
10. In the **Local Directory Name** field, enter a folder name.

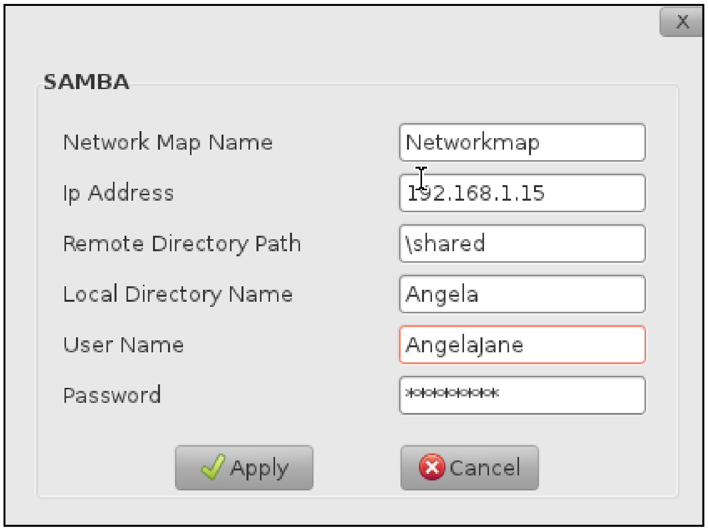
    Note: A folder with the name specified in **Local Directory Name** field is created in \media. This folder is redirected in all connections.

11. Click **Apply**. The confirmation window appears.
12. Click **Yes**.

Configuring a Samba Connection

Samba provides access to Microsoft Windows based file and print services for your thin client. To set up a Samba connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Clicks **Add**.
5. From the **Please choose the connection to add** drop-down list, select **SAMBA – Samba**.
6. Click **OK**.



SAMBA

Network Map Name	Networkmap
Ip Address	192.168.1.15
Remote Directory Path	\shared
Local Directory Name	Angela
User Name	AngelaJane
Password	********

7. In the **Network Map Name** field, enter the name of the NFS network map.
8. In the **IP Address** field, enter the IP address of the Samba server.
9. In the **Remote Directory Path** field, enter the shared folder name.
10. In the **Local Directory Name** field, enter a folder name.

    Note: A folder with the name specified in **Local Directory Name** field is created in \media. This folder is redirected in all connections.

11. In the **User Name** field, enter the username.
12. In the **Password** field, enter the password.
13. Click **Apply**. The confirmation window appears.
14. Click **Yes**.

Configuring a NX-Client Connection

NX- Client connection allows you to run remote X11 sessions even across slow or low-bandwidth network connections. It allows you to start sessions from clients running on Windows, Linux, Mac OS X and Solaris platforms to servers running on Linux or Solaris.

To configure NX-Client connection:

1. On the desktop sidebar, click **Settings**.

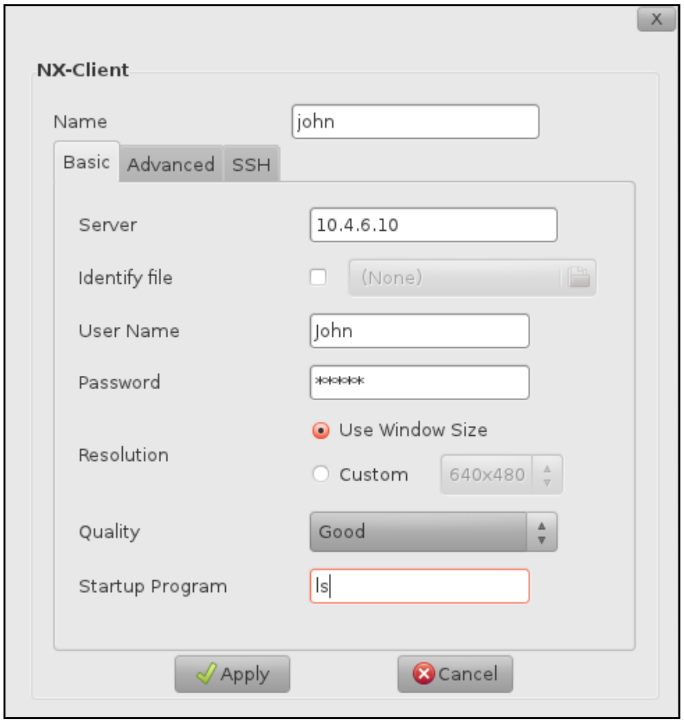
2. Click the **Connectivity** drop-down arrow.

3. Click **Connection Manager**, the **Connections** window appears.

4. Click **Add**.

5. From the **Please choose the connection to add** drop-down list, select **NX – NX-Client**.

6. Click **OK**. The **NX-Client** window appears.



NX-Client

Name: john

Server: 10.4.6.10

Identify file: ☐ (None)

User Name: John

Password: *****

Resolution: ● Use Window Size ○ Custom 640x480

Quality: Good

Startup Program: ls

7. In the **Name** field, enter a connection name.

8. In the **Server** field, enter the server IP address.

9. Select **Identify file** field, and select the SSH public key certificate.

Note: You need not enter the Password if you select **Identify file** option.

10. In the **User Name** field, enter a user name.

11. In the **Password** field, enter a password.

Note: Please make note of your user name and password. Your user name and password are required later when establishing a connection.

12. In the **Resolution** choose default server resolution or specify the resolution.

13. In the **Quality** field, select the quality of the connection.

14. In the **Startup Program** field, enter the path of the startup program. *For example, C:\programfiles\microsoft\word.exe. in windows server. Linux commands such as Ls, cat, vi filename, ps in Linux server .*

15. Click A**dvanced** tab and select the following options if required.

- **Disable clipboard sync**: Select this option to disable cut, copy and paste function between client and server

- **Disable encryption**: Select this option to disable encryption of data between client and server.
- **Use local cursor**: Select this option to enable the use of the local system cursor.

16. For setting up SSH, click **SSH** tab.
17. Select **Enable SSH tunnel** to enable an encrypted SSH tunnel for this connection.
18. Select **Tunnel via loopback Address** to enable tunneling via the loopback address.
19. Select **Same server at port 22** to select the server at port 22 by default.
20. Select **Custom** to enter the IP address of an SSH server.
21. From the **Character set** drop-down list, select a character set. *For example, you may select ISO-8859-1.*
22. In the **User Name** field, enter the user name for SSH authentication.
23. Select one of the following authentication methods: **Password**, **Public key (automatic)**, **Identity file**.

    Note: To select an identity file for authentication, click on the browse button next to **Identity file** and then click **Open**.
24. Click **Apply**, the confirmation window appears.
25. Click **Yes**.

Editing a Connection

You can edit a connection to change settings and options. To edit a connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Select the connection you want to edit.
5. Click **Edit**.
6. Modify the settings based on your new preferences.
7. Click **Apply**, the confirmation window appears.
8. Click **OK**.

Connecting to a Server

You can connect to a server once you have configured your connection. To connect to a server connection:

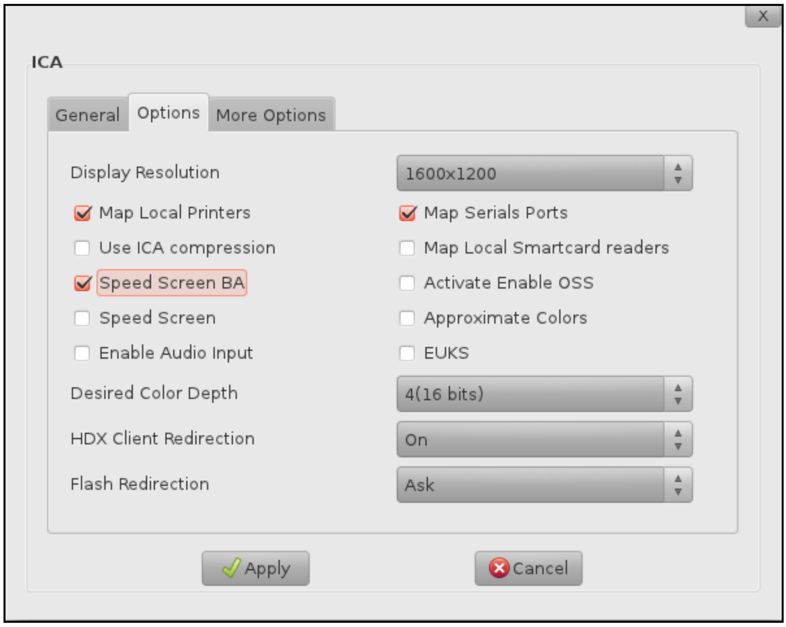
Note: To launch a connection from the desktop, double-click on the connection icon.

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Select one of following connections to connect:

ICA

Select the ICA connection and click **Connect**. The remote desktop window appears.

Note: For ICA connection (XenApp) you will be able to switch between the launched connection and Gio 5 operating system only when the Display Resolution is set to a particular resolution apart from full screen.



Display Resolution: 1600x1200

☑ Map Local Printers
☑ Map Serials Ports
☐ Use ICA compression
☐ Map Local Smartcard readers
☑ Speed Screen BA
☐ Activate Enable OSS
☐ Speed Screen
☐ Approximate Colors
☐ Enable Audio Input
☐ EUKS

Desired Color Depth: 4(16 bits)

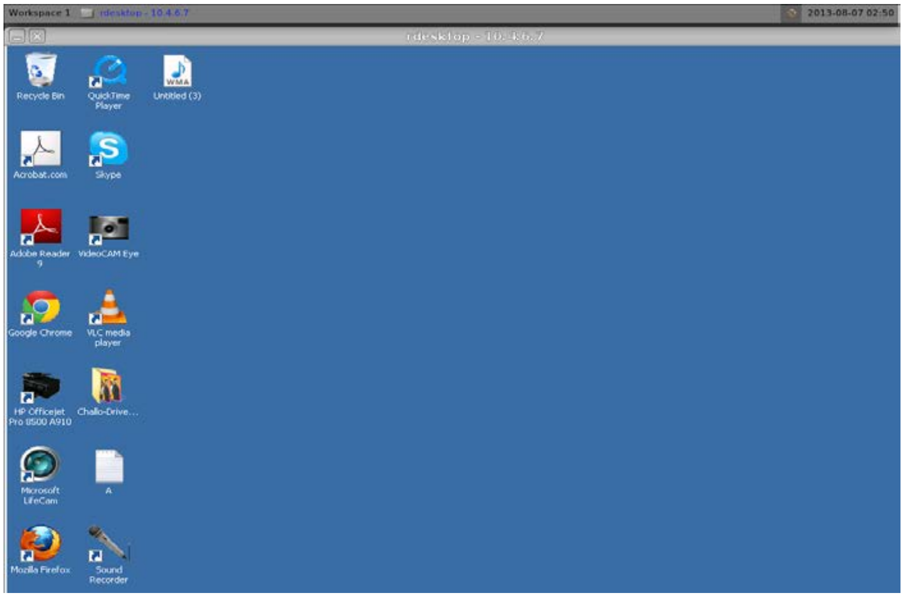
HDX Client Redirection: On

Flash Redirection: Ask

RDP

Select the RDP connection and click **Connect**. The remote desktop window appears.

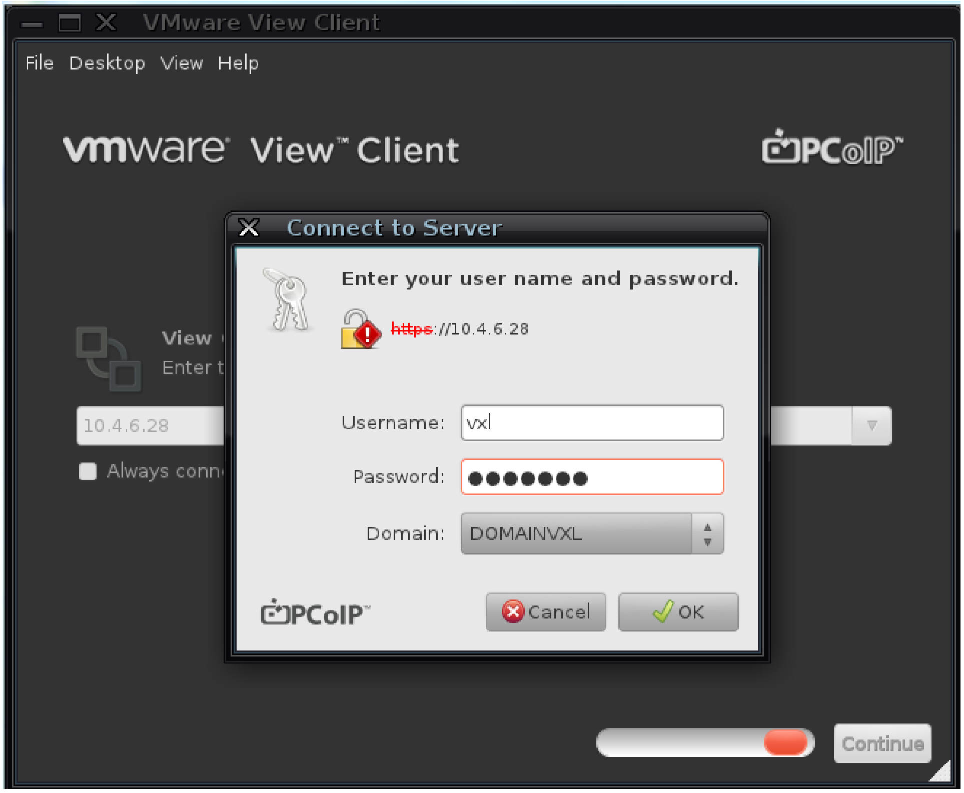
Note: Press the hotkeys CTRL+ALT+ENTER and click minimize to switch from a launched RDP connection to GIO 5 operating system.



VMware View Client

1. Select VMware connection and click **Connect,** the **VMware View Client** window appears
2. In the **Enter the name of a View Connection Server** drop-down list, enter or select a server IP address.

   Note: Select the **Always connect to this server at startup** to connect to this server every time this connection is started.
3. Click **Continue**. The **Connect to Server** window appears.



Enter your user name and password.

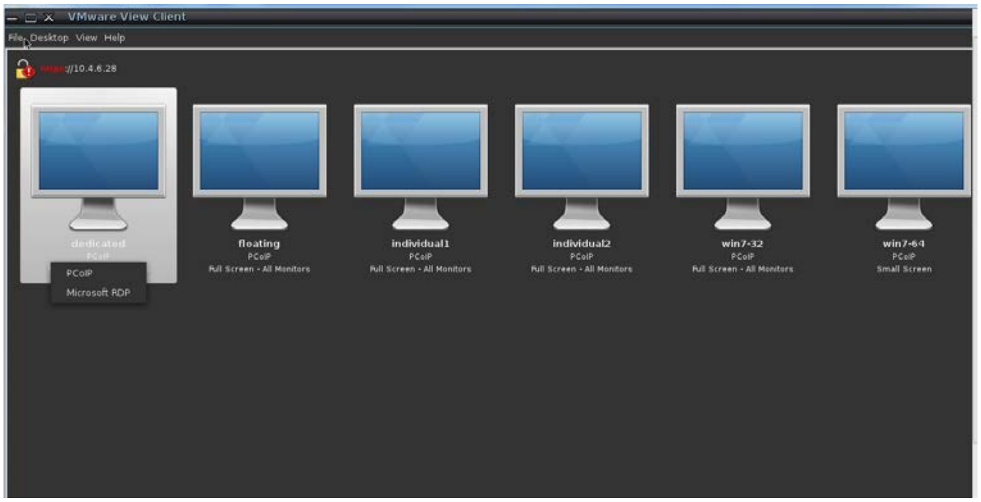
~~https~~://10.4.6.28

Username: vxl

Password: ●●●●●●●

Domain: DOMAINVXL

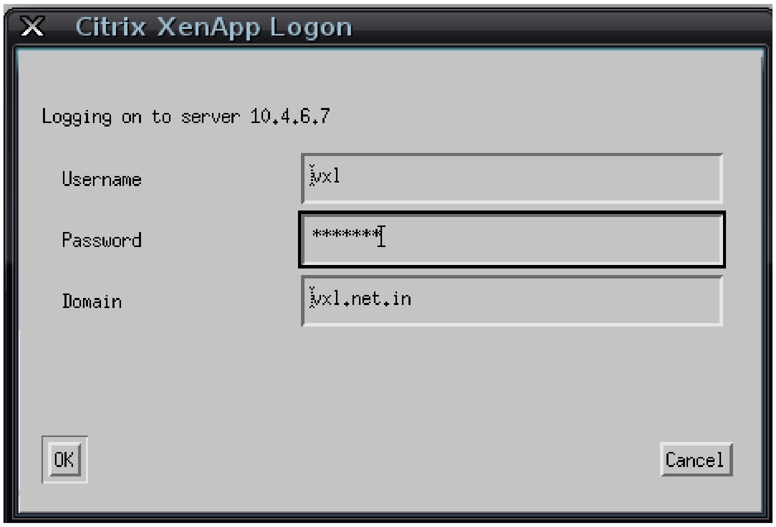
4. Enter **Username** and **Password** and click **OK**.
5. Select a virtual machine from the list of available virtual machines. The selected virtual machine’s desktop window appears.



6. From the desktop drop-down list in the taskbar, select **disconnect** to disconnect from the current virtual machine.
7. To exit the VMware View client, click **File > Quit**.

WFCMGR Citrix Receiver

1. Click **Connect,** the **Citrix XenApp Logon** window appears.



Logging on to server 10.4.6.7

Username vxl

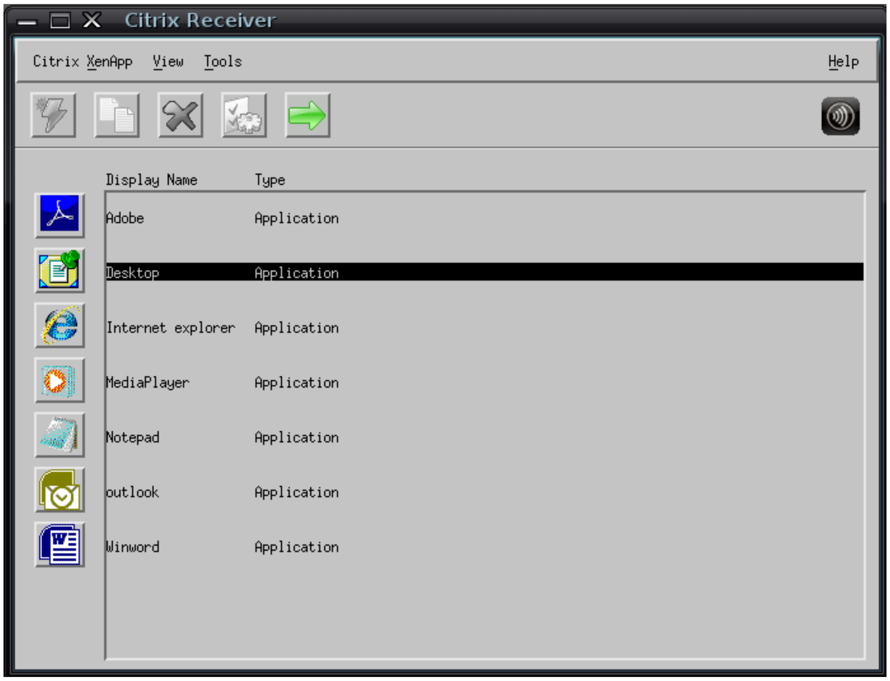
Password *******

Domain vxl.net.in

2. In the **Username** field, enter the user name.
3. In the **Password** field, enter the password.
4. In the **Domain** field, enter the domain name.

   Note: Select **Save Password** if you want to save the password for use in the next session.

5. Click **OK**. The **Citrix Receiver** window appears.
6. From the list of application provided, select the application that you want to launch.



Display Name	Type
Adobe	Application
Desktop	Application
Internet explorer	Application
MediaPlayer	Application
Notepad	Application
outlook	Application
Winword	Application

7. Click **Citrix XenApp**, click **Connect to selection**. The selected application is launched.

Browser – Firefox Browser

Click **Connect**. The remote desktop window appears.

Remote FX – X Free RDP

Click **Connect**. The remote desktop window appears.

SSH – Secure Shell

Click **Connect**. The remote desktop window appears.

SFTP – Secure File Transfer Protocol

Click **Connect**. The remote desktop window appears.

XDMCP – X Remote Session

Click **Connect**. The remote desktop window appears.

NFS – Remote File System

Click **Connect**. The remote desktop window appears.

SAMBA – Samba

Click **Connect**. The remote desktop window appears.

NX – NX Client

Select the NX connection and click **Connect**. The remote desktop window appears.

Deleting a Connection

You can edit a connection to change settings and options. To edit a connection:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Connection Manager**, the Connections window appears.
4. Select the connection you want to delete.
5. Click **Delete**, the confirmation window appears.
6. Click **OK**.

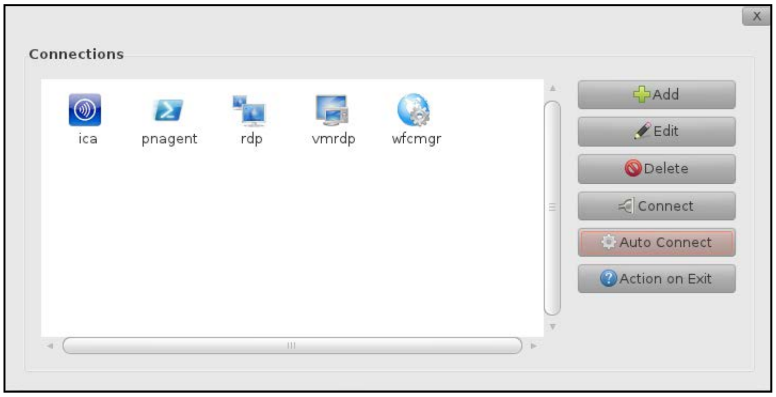
Auto Connect

The Auto Connect option allows you to connect to a particular connection directly on boot-up.

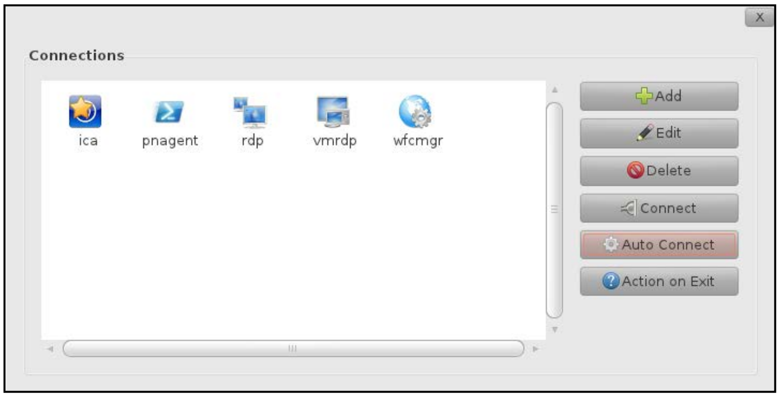
Note: The **Auto Connect** option can be set for only one connection at a time.

To set up auto connect:

1. From the **Connections** window select a connection of your choice.



2. Click **Auto Connect**.



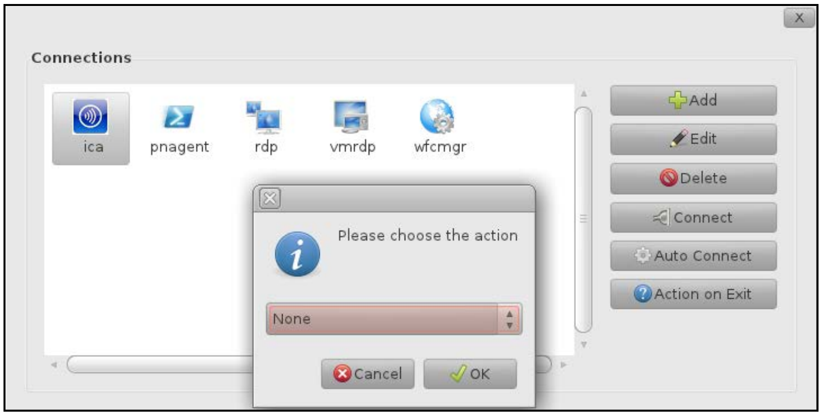
Action on Exit

This option allows you to set the client to reboot or shutdown on logging out of a session.

Note: The **Action on Exit** option can be set for only one connection at a time.

To set action on exit:

1. From the **Connections** window select a connection of your choice.
2. Click **Action on Exit.**



Please choose the action

None

3. Select **Reboot**, **Shutdown or Reconnect**.
4. Click **OK.**

Connection Task Manager

The **Connections Task Manager** lists out all the connections created. This allows you to start or disconnect an existing connection. The minimized connections are listed under the **Active Connections** tab this allows you to easily switch between connections.

To access the Connections Task Manager press the hot keys **Ctrl + Alt + G**.

To start an existing connection, from the **Connection Task Manager** window select a connection and click **Start**.

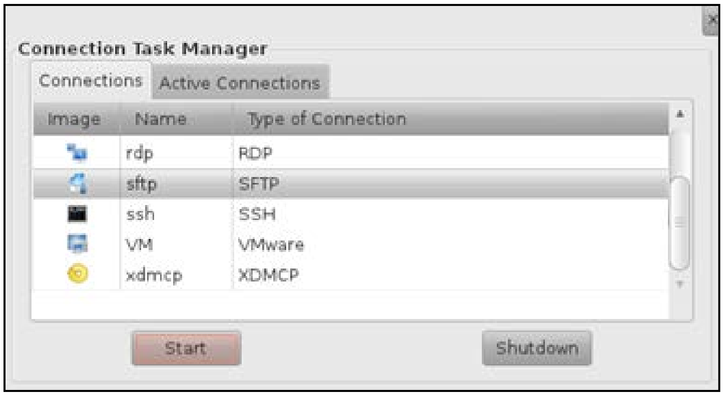


Image	Name	Type of Connection
	rdp	RDP
	sftp	SFTP
	ssh	SSH
	VM	VMware
	xdmcp	XDMCP

To shutdown the Thin Client, from the **Connection Task Manager** window click **Shutdown**.

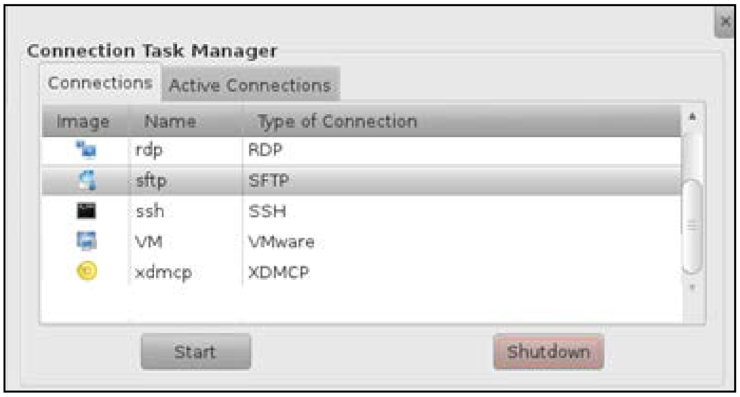


Image	Name	Type of Connection
	rdp	RDP
	sftp	SFTP
	ssh	SSH
	VM	VMware
	xdmcp	XDMCP

To disconnect a connection, from the **Connections Task Manager** window click **Active Connections** tab, select a connection and click **Disconnect**.

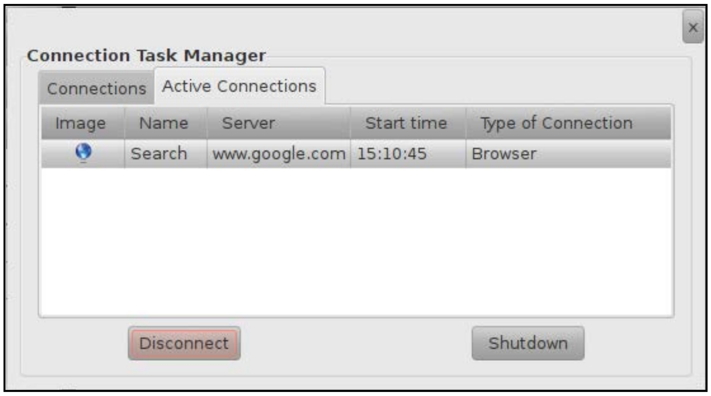


Image	Name	Server	Start time	Type of Connection
	Search	www.google.com	15:10:45	Browser

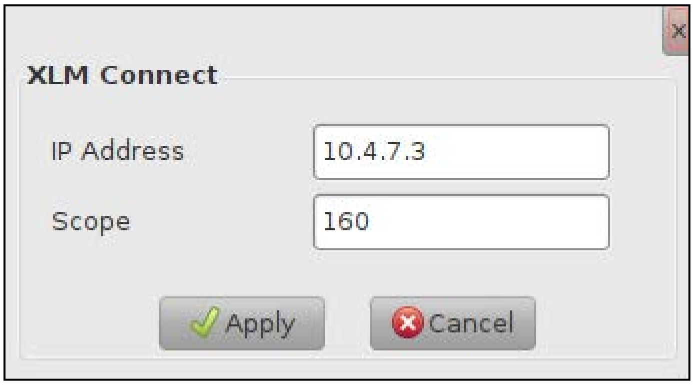
Note: Currently, you can disconnect only RDP and Browser sessions.

XLM Connect

Note: XLM is not supported in this release of Gio 5 for J Series.

You can configure your client to work with the XLmanage application. To configure your client with XLmanage:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **XLM Connect**, the **XLM Connect** window appears.



IP Address 10.4.7.3

Scope 160

4. In the **IP Address** field, enter your IP address.
5. In the **Scope** field, enter the scope ID. The IP scope is the IP address of XLmanage server.

   Note: You can connect to XLmanage only when an XLmanage server is configured and is running.

6. Click **Apply**. The Confirmation dialog box appears.
7. Click **Yes**.

Client Configuration

Gio 5 can be configured manually or by using a Configuration (INI) file.

The two ways of configuring Gio 5 using a configuration file are:

- DHCP Scope Configuration
- Manual Configuration.

This section explains these two types of configuration in detail. For information on generating an INI file, refer the *Configuration File Generator* User Manual.

DHCP Scope ID Configuration

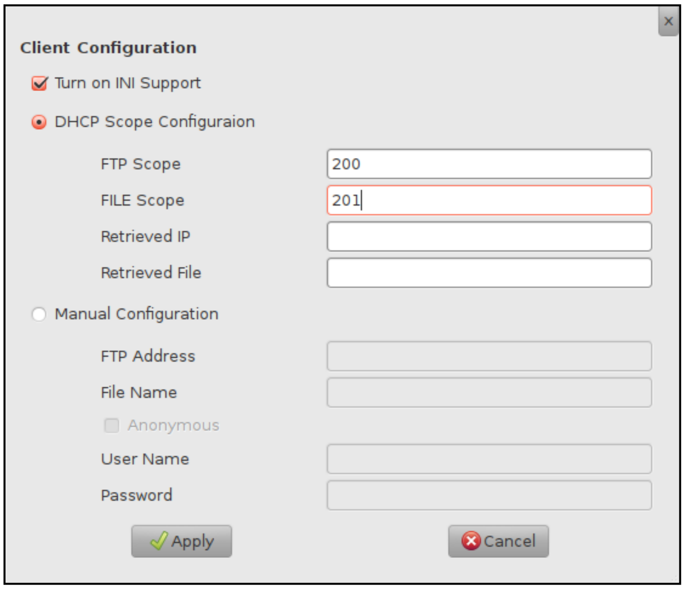
DHCP Scope ID configuration is a configuration process in which scope Ids are used to fetch the configuration files.

Note: If the DHCP scope IDs are configured in the DHCP server, the client gets the parameter values automatically.

After specifying the scope ID, reboot the client to fetch the configuration file. Every time the client boots, it downloads the configuration file and accordingly configures the client.

To perform DHCP scope configuration:

1. On the desktop sidebar, click the **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Client Configuration**, the **Client Configuration** window appears.



Client Configuration

☑ Turn on INI Support

● DHCP Scope Configuraion

FTP Scope: 200

FILE Scope: 201

Retrieved IP:

Retrieved File:

○ Manual Configuration

FTP Address:

File Name:

□ Anonymous

User Name:

Password:

4. Select **Turn on INI Support** and then select **DHCP Scope Configuration.**
5. In the **FTP Scope** field, enter the scope ID of the DHCP Server where the INI file is available.
6. In the **File Scope** field, enter the scope id of the INI file path. The **Retrieved IP** and **Retrieved File** fields display the retrieved IP address and file respectively.
7. Click **Apply. T**he confirmation window appears, click **Yes.**
8. Reboot the client. The client is configured.

Note: If you require multiple configuration files for multiple users, then configure the DHCP server with distinct scope IDs for each configuration file and use the relevant scope IDs in the Xtona client.

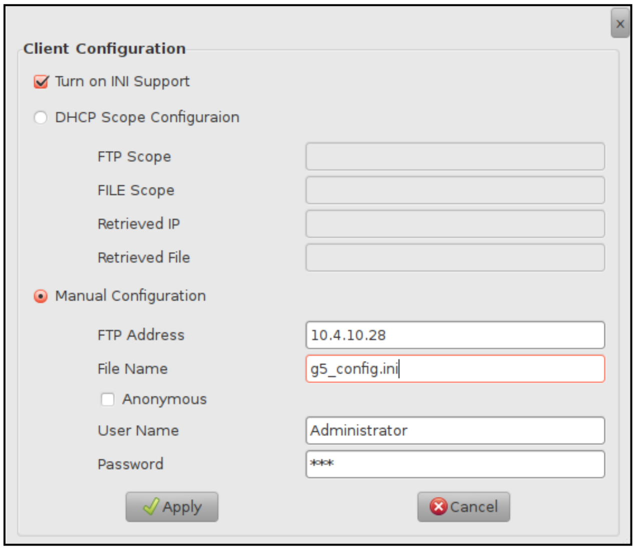
Manual Configuration

This is a manual configuration process to fetch the configuration file placed in the FTP server.

Note: File and folder name should not contain spaces or special characters.

To perform Manual configuration:

1. On the desktop sidebar, click the **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Client Configuration**, the **Client Configuration** window appears.



Client Configuration

☑ Turn on INI Support

○ DHCP Scope Configuraion

FTP Scope

FILE Scope

Retrieved IP

Retrieved File

● Manual Configuration

FTP Address: 10.4.10.28

File Name: g5_config.ini

□ Anonymous

User Name: Administrator

Password: ***

4. Select **Turn on INI Support** and then select **Manual Configuration.**
5. In the **FTP Address** field, enter the IP address of the FTP Server where the INI file is available.
6. In the **File** name field specify the path and file name.
7. In the **User Name field**, enter the user name of the FTP Server.
8. In the **Password** field, enter the password.

   Note: Select Anonymous if the FTP server is not password protected.
9. Click **Apply.** The confirmation window appears, click **Yes.**
10. Reboot the client. The client is configured.

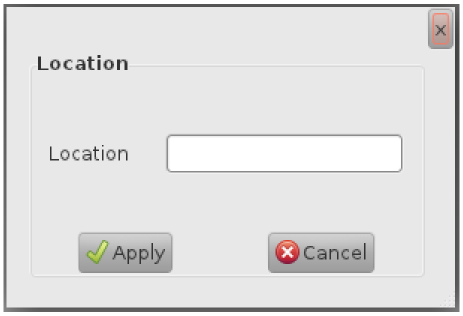
Location

The Location option allows you to mention the physical location of the thin client,

Example: Floor number, cubical number etc.

To enter the location of the thin client:

1. On the desktop sidebar, click the **Settings** icon.
2. Click the **Connectivity** drop-down arrow.
3. Click **Location**, the **Location** window appears.



Location

Location:

4. Enter the location and click **Apply**.
5. The **Confirmation** window appears, click **Yes**.

4 Local Settings

You can configure *Gio 5* local settings manually. The various settings that you can configure are:

- Devices
- Display
- System Settings
- Firmware Upgrade
- User Accounts
- Restore Factory Defaults
- Screen Lock
- Import Certificates

This chapter provides step-by-step instructions to configure the following local settings.

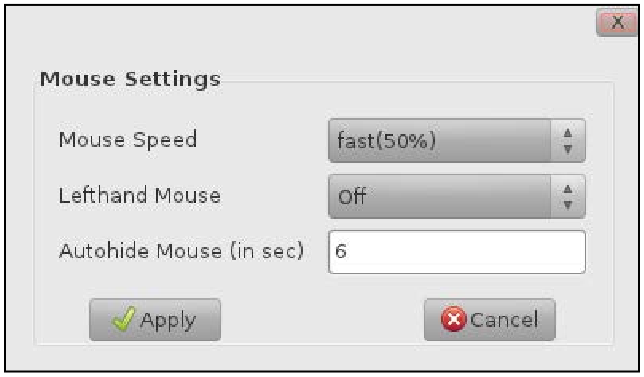
Devices

The Devices option allows you to set up the mouse, keyboard and printer.

Mouse

To set up the mouse:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Devices** and then click **Mouse**. The **Mouse Settings** window appears.



Mouse Settings

Mouse Speed: fast(50%)

Lefthand Mouse: Off

Autohide Mouse (in sec): 6

4. Select or enter values for the following fields:

   - **Mouse speed**: The mouse speed value determines how fast the cursor moves in response to the movements of the mouse. Select a mouse speed based on your preference. By default, fast (50%) is selected.
   - **Lefthand Mouse**: Set this option **On** to make your mouse left-hand friendly. Setting this option makes the right mouse button the primary select button and

the left mouse button as the secondary mouse button. By default Off is selected.

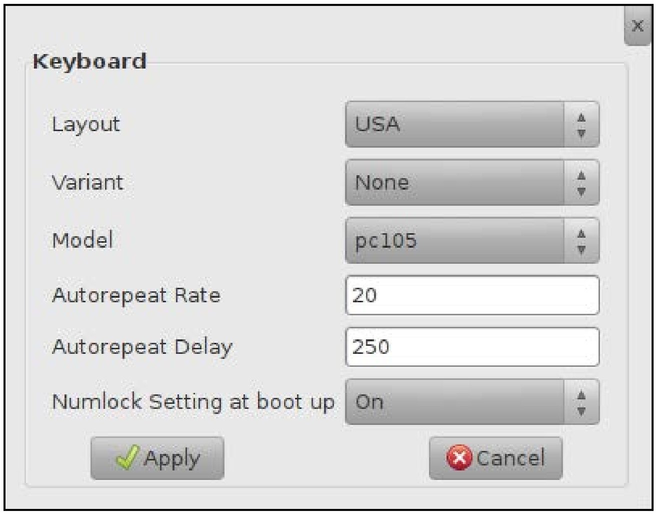
- **Autohide Mouse (in sec)**: Hide the mouse cursor for a specified time interval in seconds. Default time interval is 6 sec.

5. Click **Apply**. The confirmation dialog box appears.
6. Click **Yes**.

Keyboard

To setup the keyboard:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Devices,** and then click **Keyboard**. The **Keyboard** window appears.



Keyboard

Layout	USA
Variant	None
Model	pc105
Autorepeat Rate	20
Autorepeat Delay	250
Numlock Setting at boot up	On

4. Select or enter values for the following fields:

   - **Layout**: Select the required keyboard layout. By default, **USA** is selected.
   - **Variant**: Select the keyboard variant type. The default type of keyboard is **qwerty**.
   - **Model**: Select the keyboard model. By default, pc104 is selected.
   - **Autorepeat Rate**: Specify the rate at which the keyboard will repeat a keystroke if you press it continuously. The default auto repeat rate is 20.
   - **Autorepeat Delay**: Specify the time delay (ms) after which the keystroke will repeat. The default auto repeat delay is 250.
   - **Numlock Settings at boot up**: Enable or disable Numlock on boot-up. By default, Numlock is ON. Click **Apply**. The confirmation dialog box appears.

5. Click **Yes**.

Printer

Gio 5 supports local and network printing; you can either print using the printer connected to your thin client or use a printer that is connected to the network. *Gio 5* uses the Common UNIX Printing System (CUPS) to handle printing jobs, CUPS consists of print spooler and scheduler that uses the Internet Printing Protocol (IPP) for queuing and printing.

Adding a Local Printer

Connect a local printer to your thin client through the USB port.

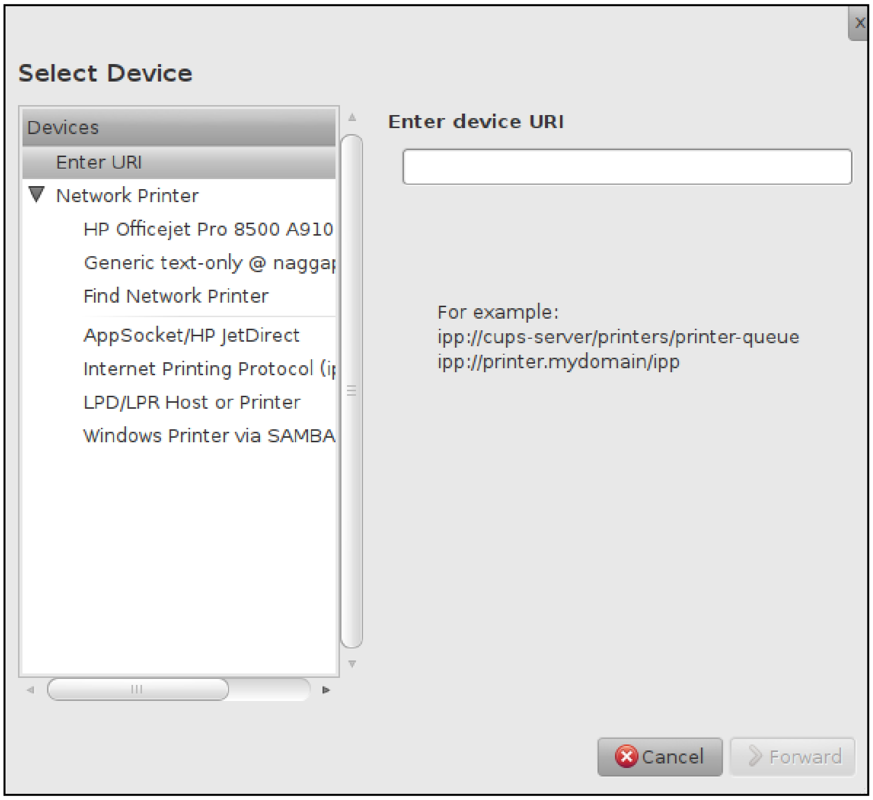
To add a local printer:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Devices** and then click **Printer**. The **Printer** window appears.
4. Click **Add.** The **Select Device** window appears**.**
5. Click **Forward**. The **Choose Driver** window appears.
6. Choose the driver from one of the following options:
    - Select Printer from Database.
    - Provide PPD file.
    - Search for a printer driver to download.
7. Once the printer is added, you can print a test page.

Adding a Network Printer

If a network printer is connected to your network. You can configure and use that printer. To add a network printer:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Devices** and then click **Printer**. The **Printer** window appears.
4. Click **Add**. The **Select Device** window appears.

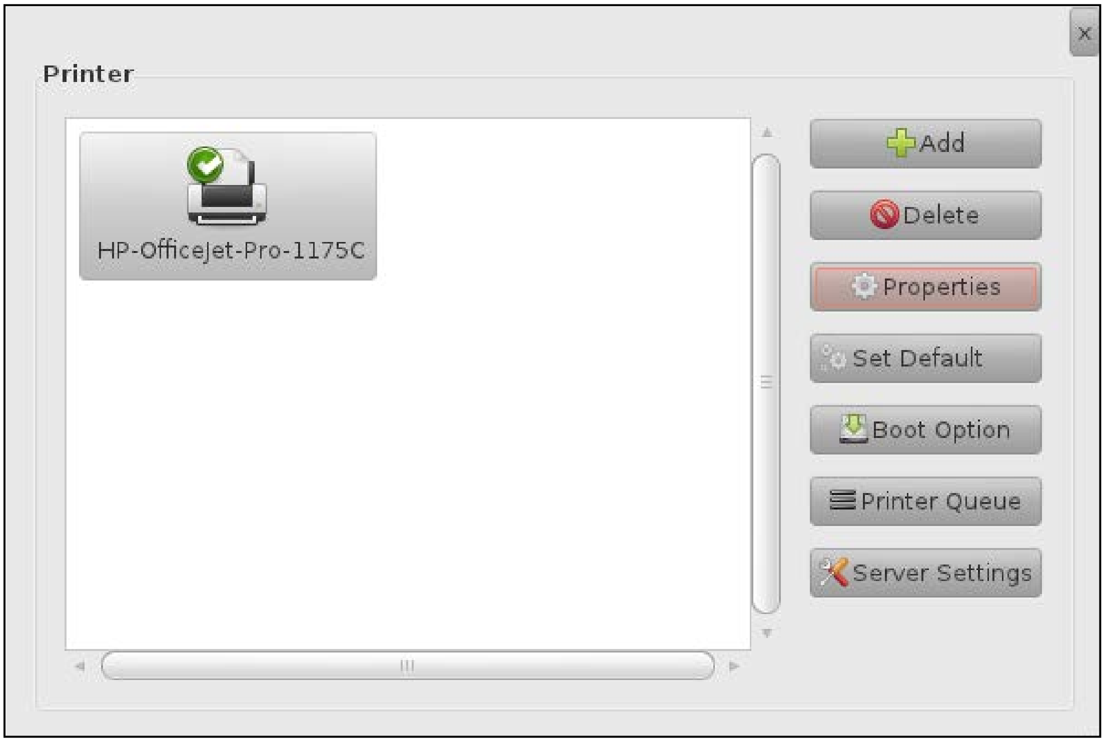


For example:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp

5. Click **Network Printer** to perform the following options**.**
   - Connect to a printer on the network.
   - Find and connect to a network printer.
   - Connect to App Socket/HP jetDirect printer.
   - Connect to a printer using Internet Printing Protocol (IPP).
   - Connect to an LDP/LPR host or printer.
   - Connect to a Windows printer via SAMBA
6. Once the printer is added, you can print a test page.

Editing the Printer Properties

To edit the properties of a printer, in the **Printer** window select a printer click **Properties**.



You can edit the following options:

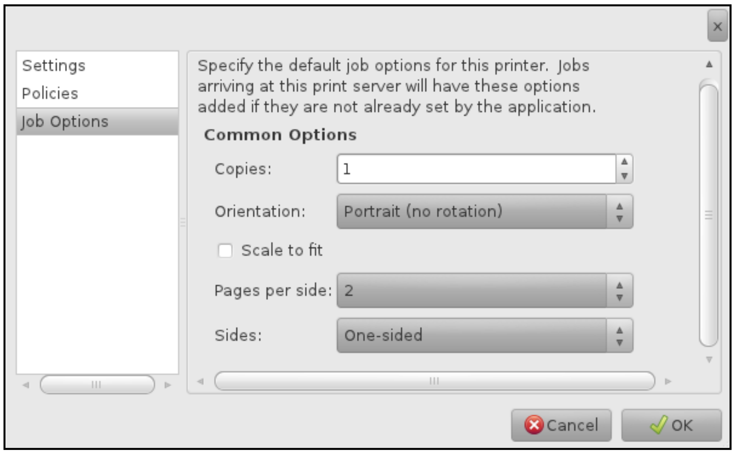
Settings

1. Click **Settings** to change the basic printer settings.
2. In the **Description** field, enter the description of the printer.
3. In the **Location** field, enter the location where the printer is installed.
4. In the **Device URI** field, enter the URI where the device is installed.
   For example, serial: /dev/ttys0?baud=115200.
5. In the **Make and Model** field, enter the make and model of the printer.
6. In the **Printer State** field, enter the present state of the printer.
7. To print a test page, click on the **Print Test Page** icon.
8. To print a self-test page, click on the **Print Self-Test** Page icon.
9. To clean the print heads of this printer, click **Clean Print Heads**.

Policies

1. Click **Policies** to change the printing policies applicable to this printer.
2. Select **Enabled** to enable the printer to print documents and files.
3. Select **Accepting jobs** to allow the printer to take up new print jobs from the spooler.
4. Select **Shared** to share this printer over the network.

Job Options



Specify the default job options for this printer. Jobs arriving at this print server will have these options added if they are not already set by the application.

Common Options

Copies: 1

Orientation: Portrait (no rotation)

□ Scale to fit

Pages per side: 2

Sides: One-sided

1. Click **Job Options** to edit the page setup and job options. Jobs arriving at this printer will have these options if not already set by the application.
2. From the **Copies** spin box, select the number of copies to be printed.
3. From the **Orientation** spin box, select the orientation to be **Portrait**, **Landscape**, **Reverse landscape** or **Reverse portrait**.
4. Select the **Scale to fit** option to rescale the document or file to the size of the paper present in the printer. You can print up to 16 pages per side.
5. From the **Pages per side** spin box, select the number of pages to be printed per side.
6. From the **Sides** spin box, select if you want the printer to print **One-sided**, **Two-sided (long edge)** or **Two-sided (short edge)**.

Setting the Default Printer

To set the default printer:

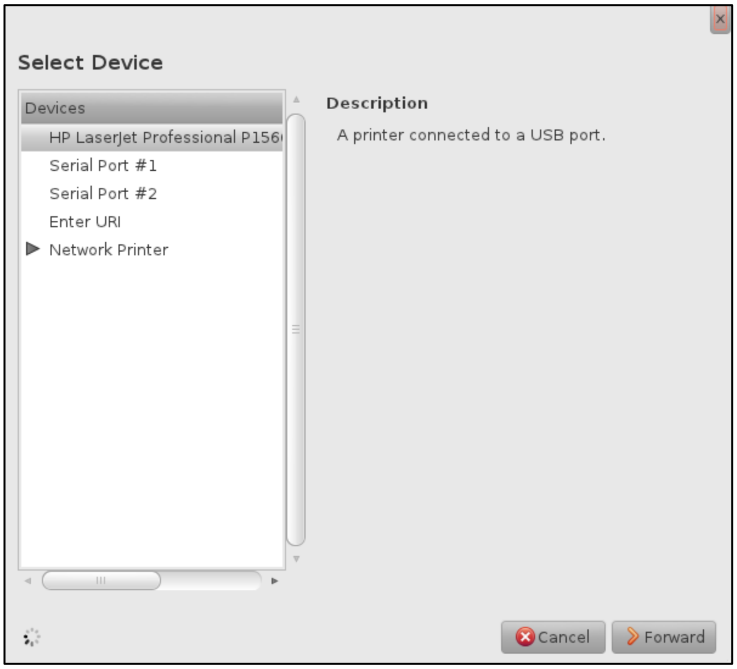
1. Select a printer that you want to assign as default.
2. Click **Set Default**.

Note: The default printer will take up the printing jobs from the spooler unless specified otherwise from the user application.

Boot Option

The boot option window allows you to set the printer driver options. The three available options are:

- Detect Automatically: The printer driver will be detected automatically. This option is selected by default.

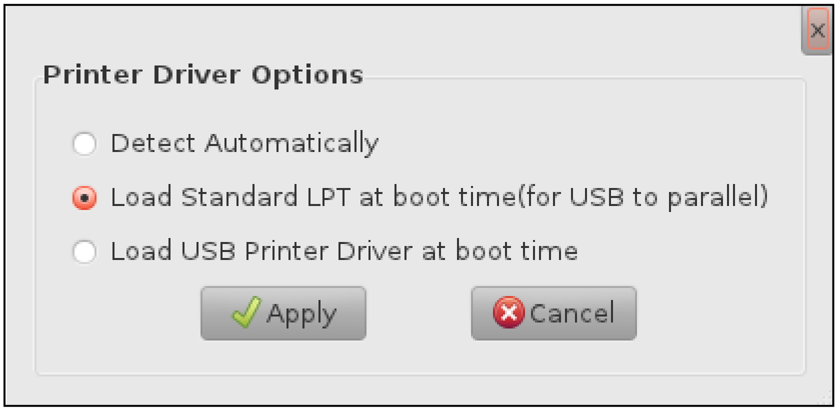


A printer connected to a USB port.

- Load Standard LPT at boot time (for USB to parallel Use this option for an LPT printer.
- Load USB printer driver at boot time: Use this option is the USB printer is not detected automatically.

To connect an LPT printer:

1. Connect the LPT printer.
2. On the desktop sidebar, click **Settings** icon.
3. Click **Local Settings** drop-down arrow.
4. Click **Devices** and then click **Printer**. The **Printer** window appears.
5. Click **Boot Option.** The **Printer Driver Options** window appears**.**



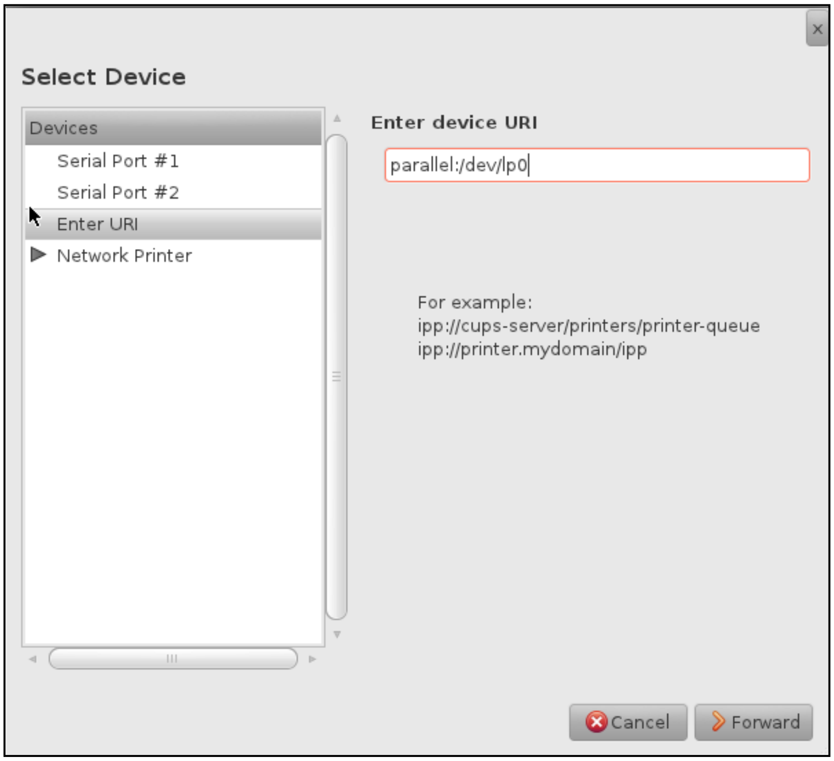
Printer Driver Options

○ Detect Automatically

● Load Standard LPT at boot time(for USB to parallel)

○ Load USB Printer Driver at boot time

6. Select **Load Standard LPT at boot time (for USB to parallel),** click **Apply**.
7. Reboot the client
8. Click **Local Settings**>**Devices>Printer**>**Add.**



Select Device

Enter device URI

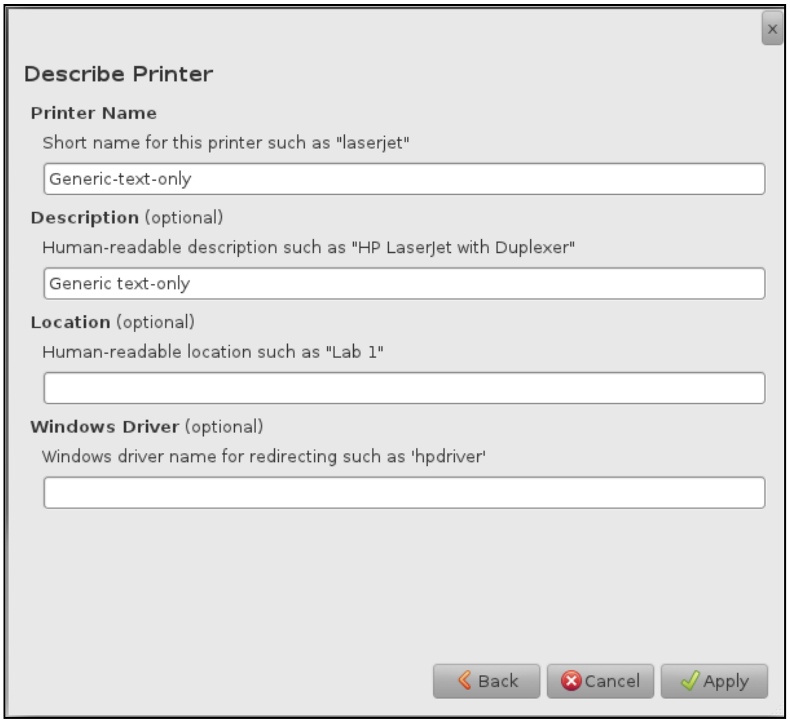
parallel:/dev/lp0

For example:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp

9. Click **Enter URL**.

10. In the **Enter device URL** field if device is connected to the parallel port enter *parallel:/dev/lp0,* if printer is connected to USB to parallel port converter enter *paralle:/dev/usblp0.*

11. Click **Forward** until the below screen appears.



Describe Printer

Printer Name
Short name for this printer such as "laserjet"
Generic-text-only

Description (optional)
Human-readable description such as "HP LaserJet with Duplexer"
Generic text-only

Location (optional)
Human-readable location such as "Lab 1"

Windows Driver (optional)
Windows driver name for redirecting such as 'hpdriver'

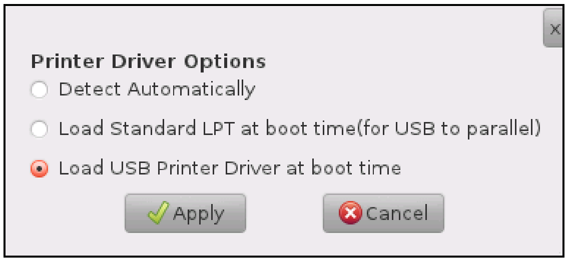
12. In the **Windows Driver** field, enter the driver name of the printer configured in the Server.

Note: The Windows Driver field is case sensitive.

13. Click **Apply.**

To connect an USB printer that is not detected automatically:

1. Connect the USB printer.
2. On the desktop sidebar, click **Settings** icon.
3. Click **Local Settings** drop-down arrow.
4. Click **Devices** and then click **Printer**. The **Printer** window appears.
5. Click **Boot Option.** The **Printer Driver Options** window appears**.**



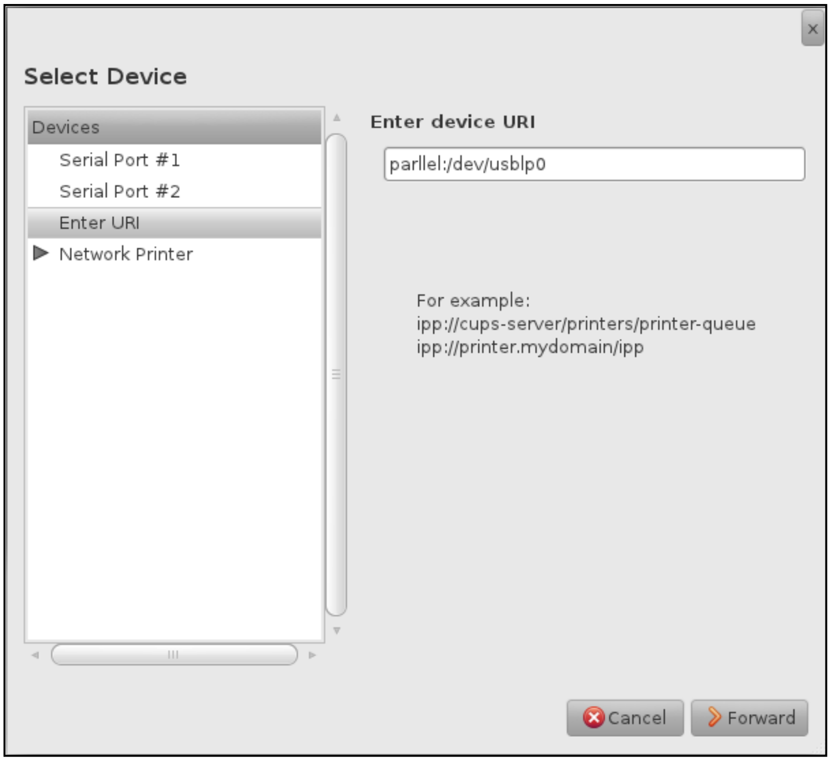
Printer Driver Options

○ Detect Automatically

○ Load Standard LPT at boot time(for USB to parallel)

● Load USB Printer Driver at boot time

6. Select **Load USB Printer Driver at boot time,** click **Apply**.
7. Reboot the client
8. Click **Local Settings**>**Devices>Printer**>**Add.**

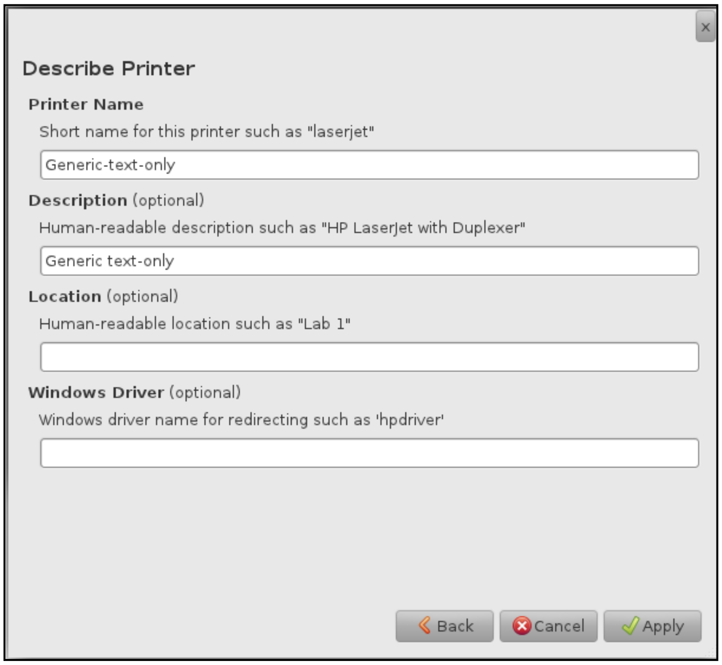


Select Device

Enter device URI: parllel:/dev/usblp0

For example:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp

9. Click **Enter URL**.
10. In the **Enter device URL** field enter *parallel:/dev/usblp0.*
11. Click **Forward** until the below screen appears.



Describe Printer

Printer Name

Short name for this printer such as "laserjet"

Generic-text-only

Description (optional)

Human-readable description such as "HP LaserJet with Duplexer"

Generic text-only

Location (optional)

Human-readable location such as "Lab 1"

Windows Driver (optional)

Windows driver name for redirecting such as 'hpdriver'

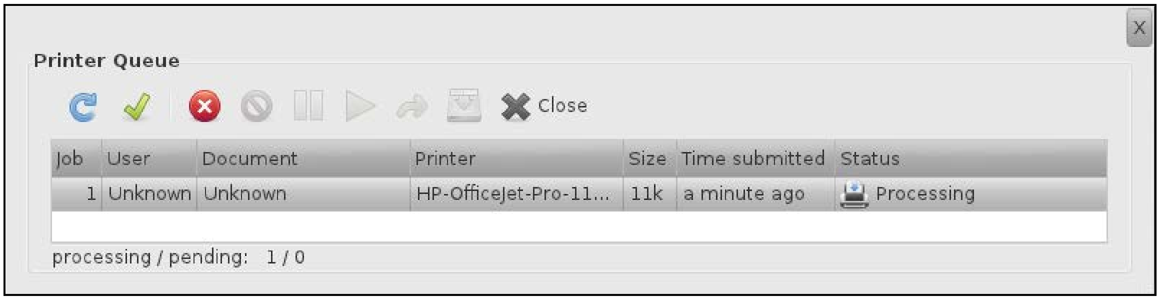
12. In the **Windows Driver** field, enter the windows driver name.
13. Click **Apply.**

Printer Queue

The Printer Queue displays active print jobs along with user, document, printer, size, time submitted and status information.

The printer queue window allows you to perform the following tasks:

- Refresh the job list.
- View completed print jobs.
- Cancel a print job.
- Stop the printing process.
- Resume the printing process.



Printer Queue

Job	User	Document	Printer	Size	Time submitted	Status
1	Unknown	Unknown	HP-OfficeJet-Pro-11...	11k	a minute ago	Processing

processing / pending: 1 / 0

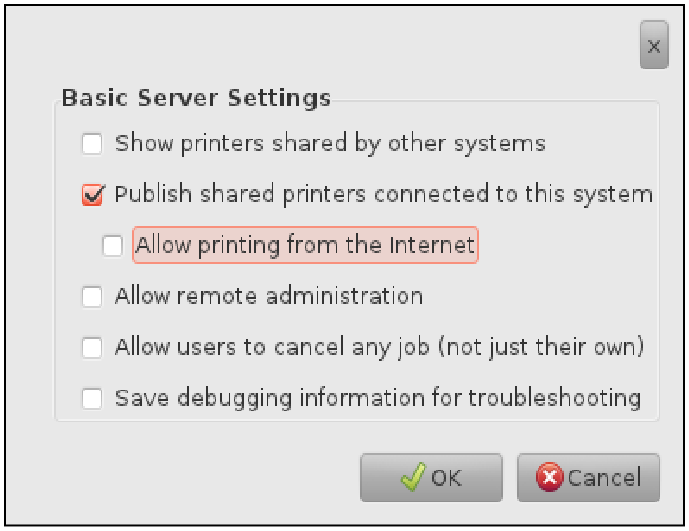
Server Settings

The server settings window allows you to set a client on the network as a Print Server. This option supports IPP printing.

To set a client as Print Server:

1. In the **Printer** window, click **Server Settings**.

2. Select **Publish shared printers connected to this system**.



Basic Server Settings

☐ Show printers shared by other systems

☑ Publish shared printers connected to this system

☐ Allow printing from the Internet

☐ Allow remote administration

☐ Allow users to cancel any job (not just their own)

☐ Save debugging information for troubleshooting

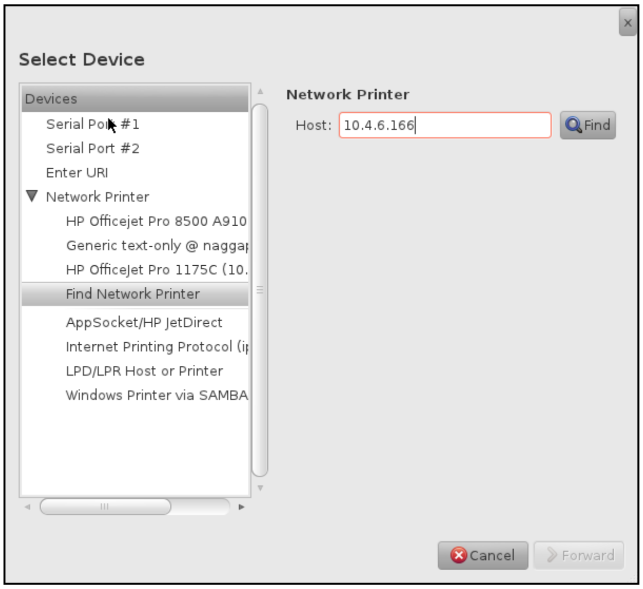
3. Select the following options if required:

- Show printers shared by other systems.
- Allow printing from the internet.
- Allow remote administration
- Allow users to cancel any job
- Save debugging information for troubleshooting.

4. Click **OK**.

To connect a client to the print server:

1. In the client click **Local Settings**>**Devices>Printer**>**Add.**



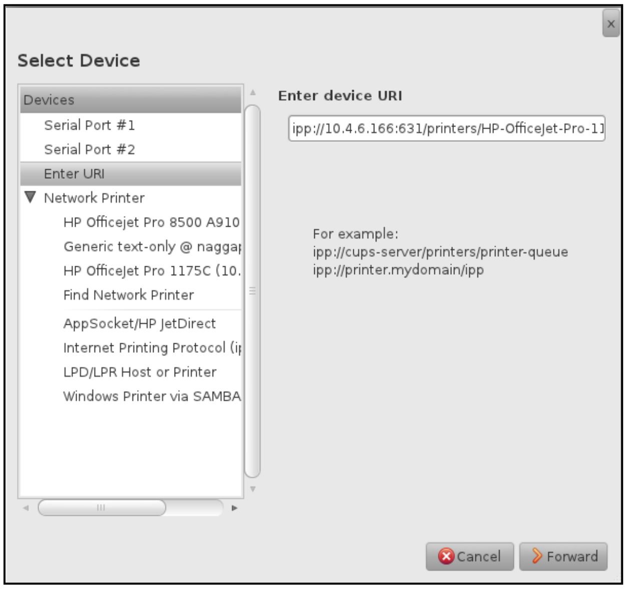
Select Device

Network Printer

Host: 10.4.6.166

2. Click **Find Network Printer**

3. In the **Host** field enter the host name or IP address of the Print Server and click **Find**. The following window appears.



Select Device

Enter device URI

ipp://10.4.6.166:631/printers/HP-OfficeJet-Pro-11

For example:
ipp://cups-server/printers/printer-queue
ipp://printer.mydomain/ipp

4. Click Enter URL and click **Forward**.
5. Continue clicking **Forward** until the configuration is complete and then click **Apply**.

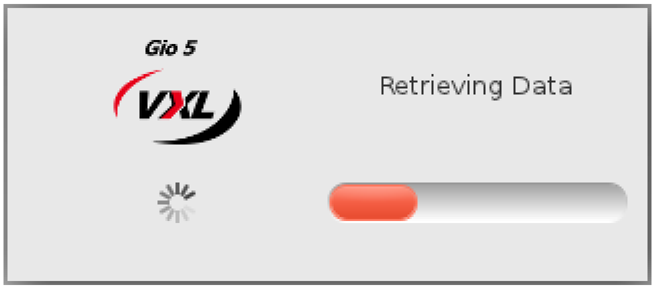
Display

Display option allows you to set the display properties and configure dual monitors.

Basic Setup

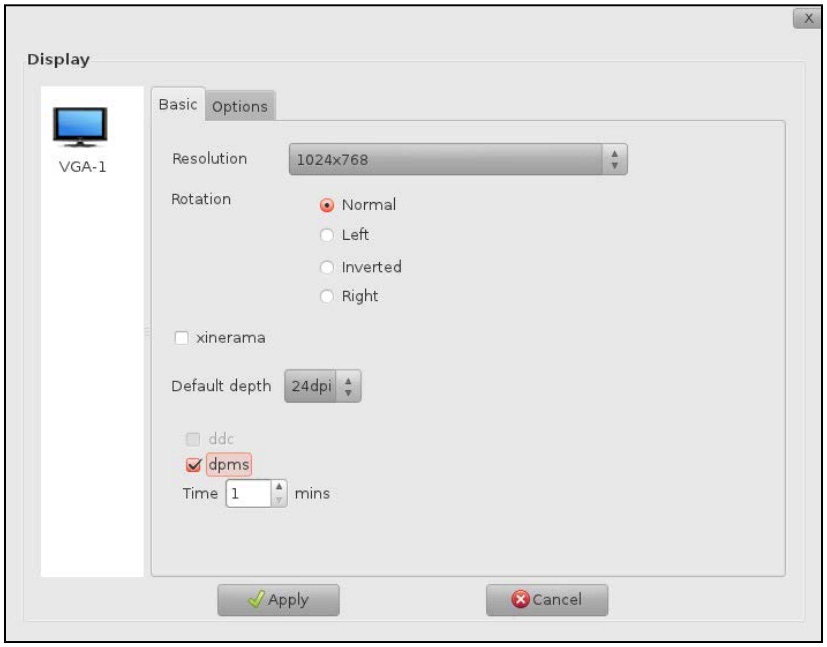
To set the display properties:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Display**. Retrieving data message appears.



Retrieving Data

The **Display** window appears.



Resolution 1024x768

Rotation ● Normal ○ Left ○ Inverted ○ Right

□ xinerama

Default depth 24dpi

□ ddc

☑ dpms

Time 1 mins

4. Under **Display** section, select the required monitor.
5. Click the **Basic** tab and select the required options.
    - Resolution: Select the required resolution.
    - Rotation: Select the rotation type (left, right, inverted, normal).
    - xinerama: Select this option to use two or more physical displays as one large virtual display.
    - Default Depth: Select the default depth.
    - DDC: Select to use the Display Data Channel display protocol, it defines the rules of communication between the graphics adapter and the client's display.
    - DPMS: Select this to enable graphics card power management. In the **Time** field select the idle time after which the monitor shuts down.
6. Click Apply. The Confirmation dialog box appears.
7. Click Yes.

Dual Monitor Setup

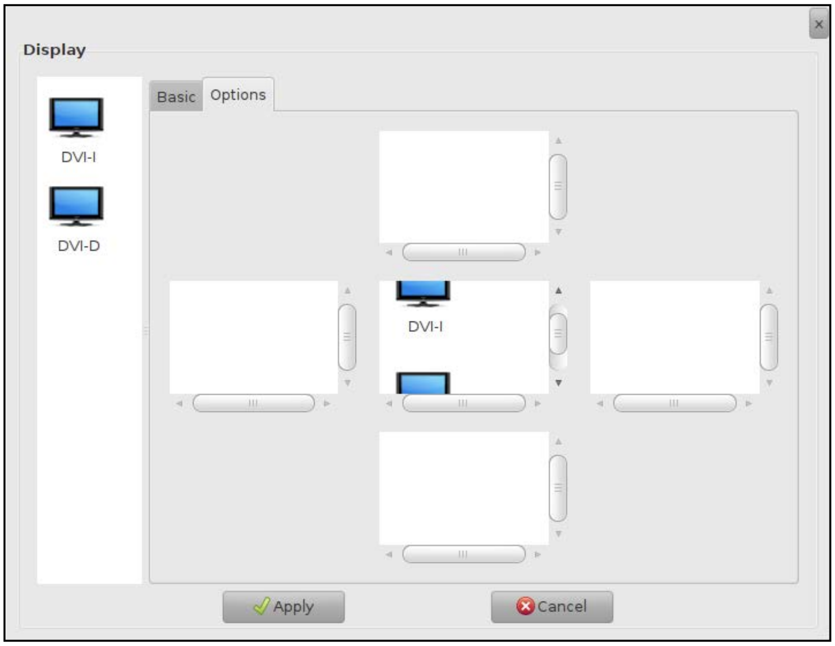
You can set up dual monitors in two modes **Mirror** and **Extended**.

Mirror mode will duplicate your Monitor1 display on Monitor2.

Extended mode will extend your Monitor1's screen area to Monitor2. This enables you to have a wider screen area to use multiple applications.

To set up mirror mode:

1. Ensure that two monitors are connected to the thin client.
2. In the **Display** window, click the **Options** tab.

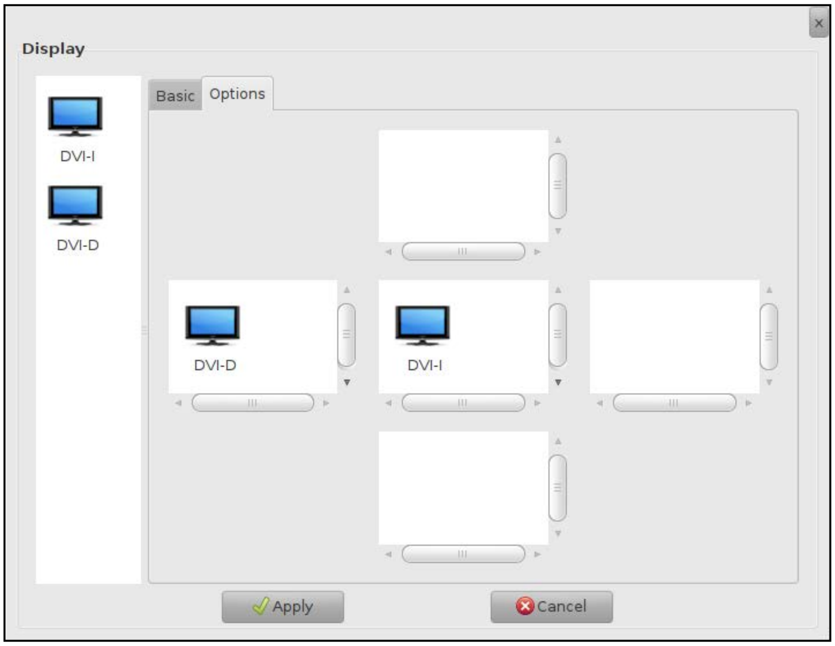


Note: Mirror mode is the default mode when dual monitors are connected.

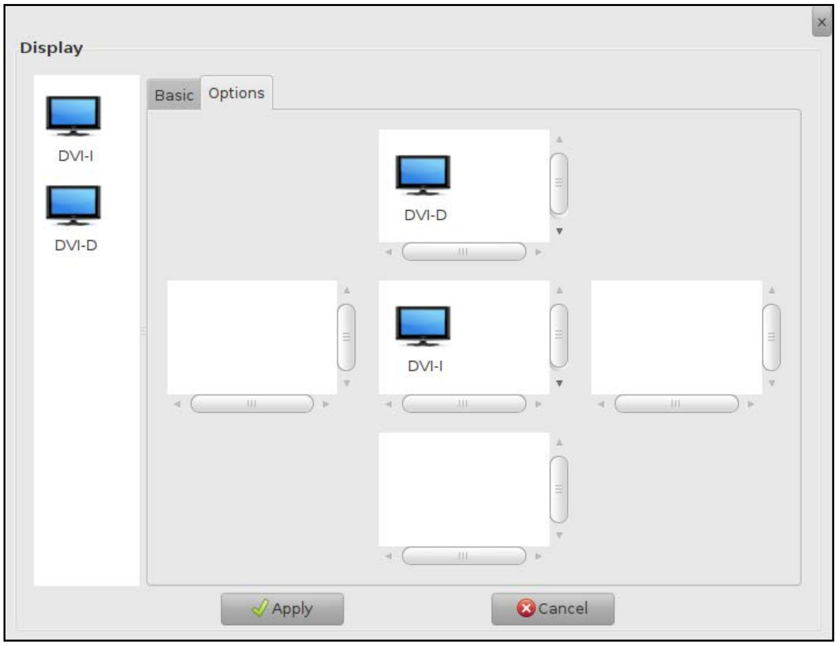
3. If the monitors are in different position boxes click and drag the monitors into the same position box.
4. Click **Apply**. The **Confirmation** dialog box appears.
5. Click **Yes**.

To set up extended mode:

1. Ensure that two monitors are connected to the thin client.
2. In the **Display** window, click the **Options** tab.
3. Click and drag a monitor to the right or left position box as required.



Note: You can also drag the monitor to the top or bottom position boxes for vertical extended view.



4. Click **Apply**. The **Confirmation** dialog box appears.
5. Click **Yes**.

System Settings

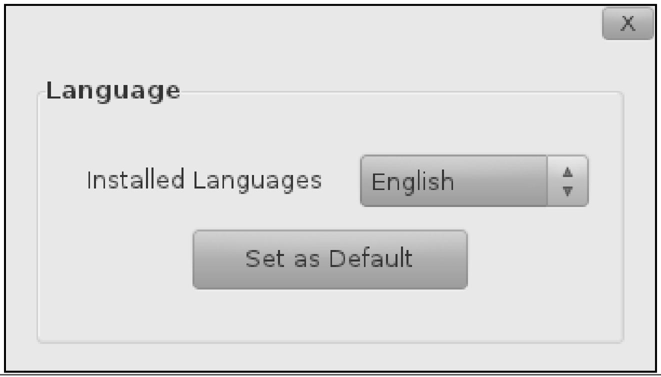
The System Settings option allows you to set up the following system properties:

- Language
- Date and Time
- Appearance

Language

To set the system language:

1. On the desktop sidebar, click the **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **System Settings** > **Language**. The **Language** window appears.



Installed Languages: English

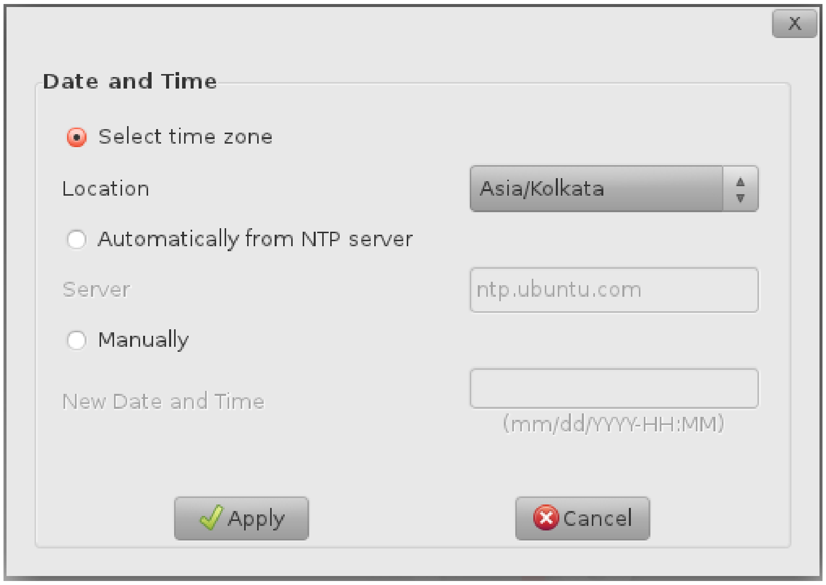
4. Select the required language and click **Set as Default**.

Date and Time

To set up time and date, you can select a time zone, specify an NTP server or enter manually. You can setup time and date from the **Date and Time** window.

To view **Date and Time** window:

1. On the desktop sidebar, click the **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **System Settings** > **Date & Time**. The **Date and Time** window appears.



Date and Time

● Select time zone

Location: Asia/Kolkata

○ Automatically from NTP server

Server: ntp.ubuntu.com

○ Manually

New Date and Time: (mm/dd/YYYY-HH:MM)

Time Zone

A *Time Zone* is a geographical region that has a uniform standard time for legal, commercial, and social purposes.

To setup time using Time zone:

1. In the **Date and Time** window, select **Select time zone** option.
2. In the **Location** field, select the required time zone location.
3. Click **Apply**. The **Confirmation** dialog box appears.
4. Click **Yes**.

NTP Server

NTP is an internet protocol used to synchronize the clocks of computers to a time reference.

To setup time using NTP Server:

1. In the **Date and Time** window, select **Automatically from NTP Server** option.
2. In the **Server** field, enter the NTP server URL.
3. Click **Apply**. The **Confirmation** dialog box appears.
4. Click **Yes**.

Manual setup

You can manually enter date and time in mm/dd/yyyy-hh:mm format.

To manually enter date and time:

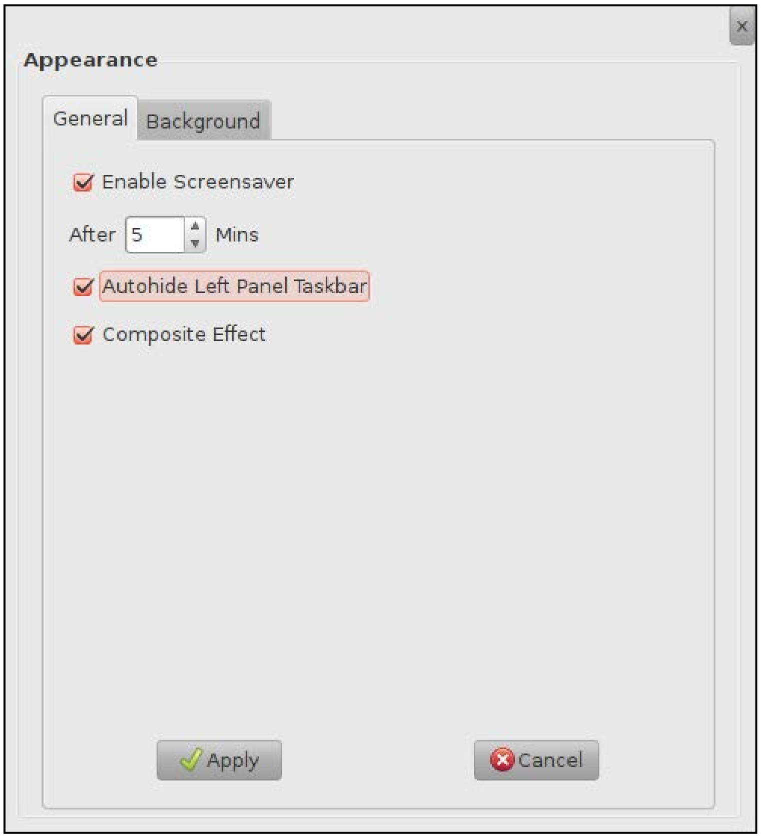
1. In the **Date and Time** window, select **Manually**.
2. In the **New Date and Time** field, enter mm/dd/yyy-HH:MM.
3. Click **Apply**. The **Confirmation** dialog box appears.
4. Click **Yes**.

Appearance

You can change the desktop background image and set the screensaver using this option. The screen shots taken is displayed under the Screenshots tab.

To set the general settings:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **System Settings** > **Appearance**. The **Appearance** window appears.
4. Click the **General** tab.



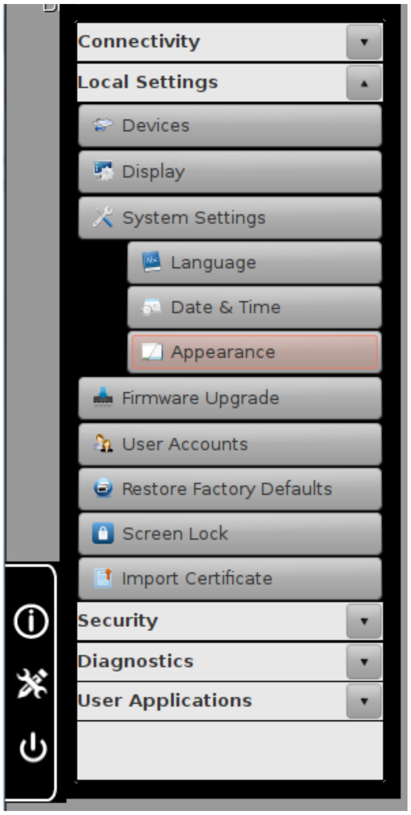
☑ Enable Screensaver

After 5 Mins

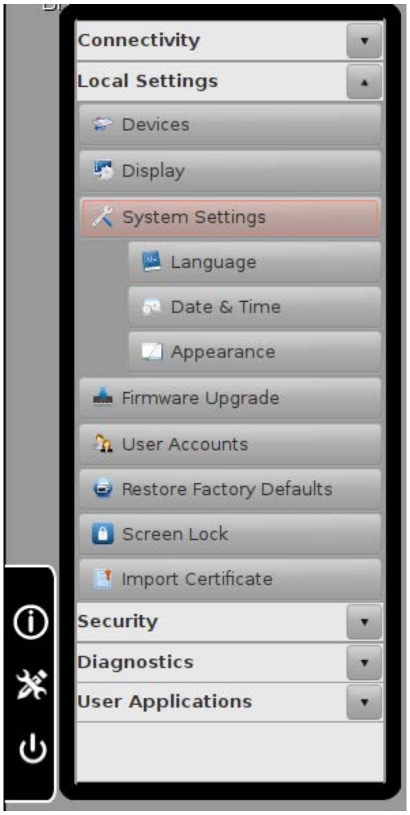
☑ Autohide Left Panel Taskbar

☑ Composite Effect

5. Select **Enable Screensaver**.
6. Set the time interval in minutes after which the screensaver appears.
7. Select **Autohide Left Panel Taskbar** to hide the taskbar on boot up.
8. Select **Composite Effect** for a transparent User Interface effect.



Normal Effect

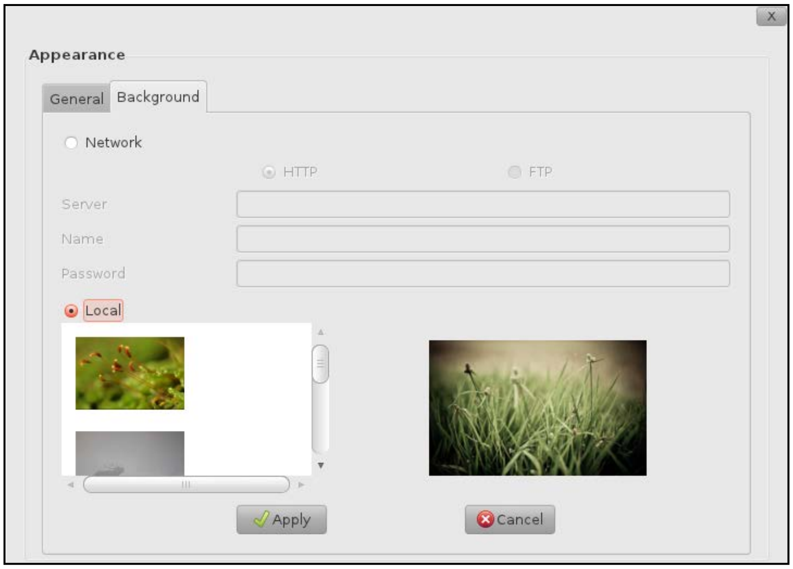


Composite Effect

9. Click **Apply** and then click **Yes**.

To change the desktop background image:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **System Settings** > **Appearance**. The **Appearance** window appears.



4. Click the **Background** tab
5. Select Network to browse and choose an image from the HTTP or FTP server.

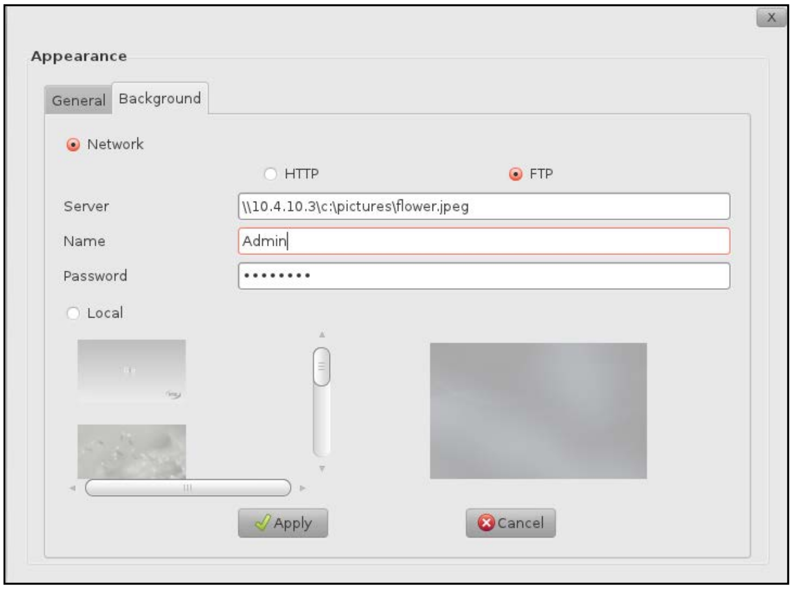
- If you select **HTTP**: In the **Server** field enter the Server IP address and image path.

- If you select **FTP:**

a. In the **Server** field enter the Server IP address and image path.

b. In the **Name** field, enter the Server User Name.

c. In the **Password** field, enter the Server Password.



Appearance

General | Background

● Network

○ HTTP ● FTP

Server: \\10.4.10.3\c:\pictures\flower.jpeg

Name: Admin

Password: •••••••••

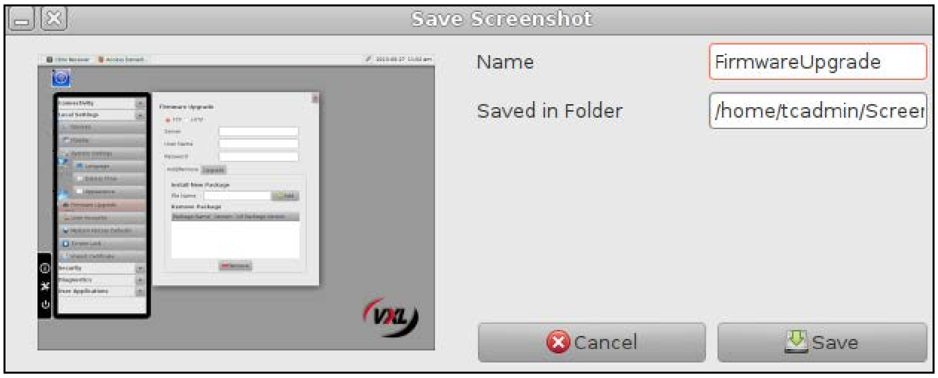
○ Local

6. Select Local to set a local image as background.
7. Click **Apply**. The **Confirmation** dialog box appears**.**
8. Click **Yes**.

Screenshots

To capture screenshots:

1. Press the **Print Screen** key. The **Save screenshot** window appears.



Save Screenshot

Name: FirmwareUpgrade

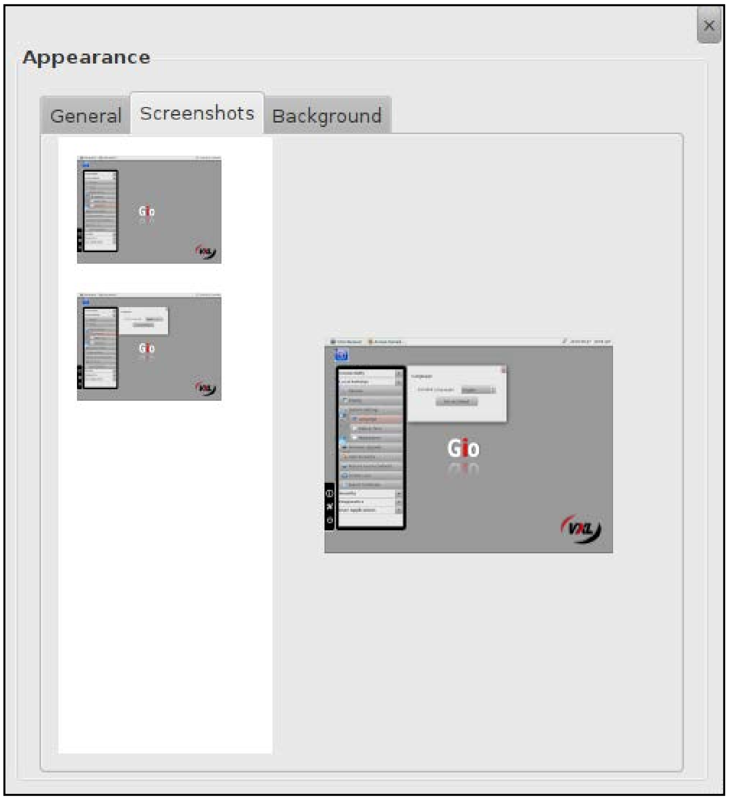
Saved in Folder: /home/tcadmin/Screer

2. In the **Name** field, enter a name for the screenshot.
3. In the **Saved in Folder** field, specify the path and folder where the screenshots are to be saved.

To view the captured screen shots:

1. On the desktop sidebar, click Settings icon.
2. Click **Local Settings** drop-down arrow.
3. Click **System Settings > Appearance**. The **Appearance** window appears.
4. Click the **Screenshots** tab.

Note: The **Screenshots** tab appears only when a screen shot is taken.



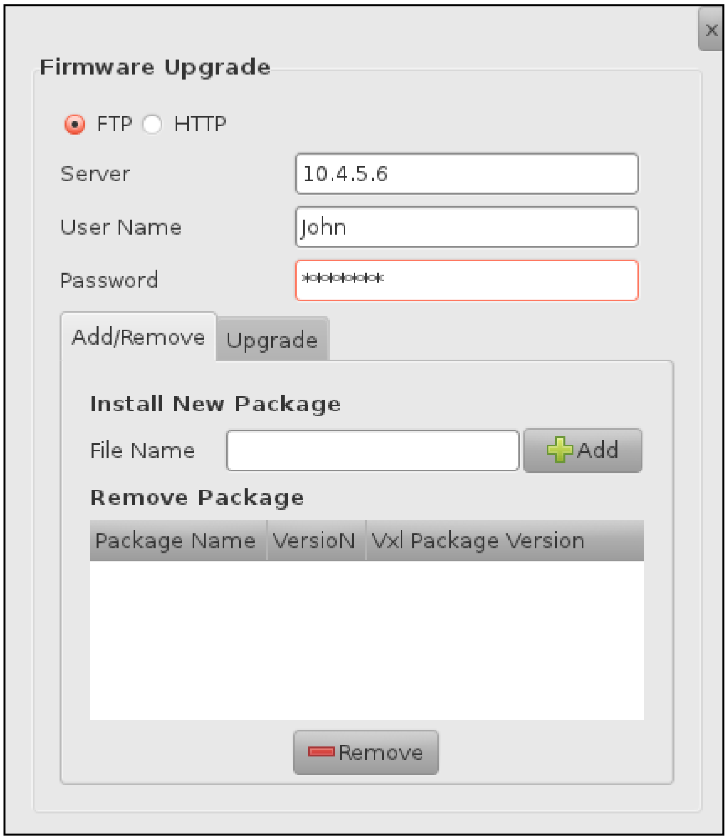
Firmware Upgrade

The firmware upgrade option allows you to upgrade the Gio5 operating system. You can upgrade a firmware (Package upgrade) from an FTP or HTTP server.

Note: Complete image upgrade is currently not supported.

To upgrade firmware using a URL:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Firmware Upgrade**. The **Firmware Upgrade** window appears.



Firmware Upgrade

● FTP ○ HTTP

Server: 10.4.5.6

User Name: John

Password: *******

Package Name	VersioN	Vxl Package Version

4. Select the protocol type (**FTP** or **HTTP**).
5. In the **Server** field, enter the IP address of the Server where the firmware upgrade is available.
6. In the **User Name** field, enter the username of the server.
7. In the **Password** field, enter the password of the server.
8. Click the **Add/Remove** tab.
9. In the **File Name** field enter the path and file name of the package.
10. Click **Add**.

    Note: To remove a package, select the package and click Remove. Click the **Upgrade** tab.

11. Select the required package and click **Upgrade**.

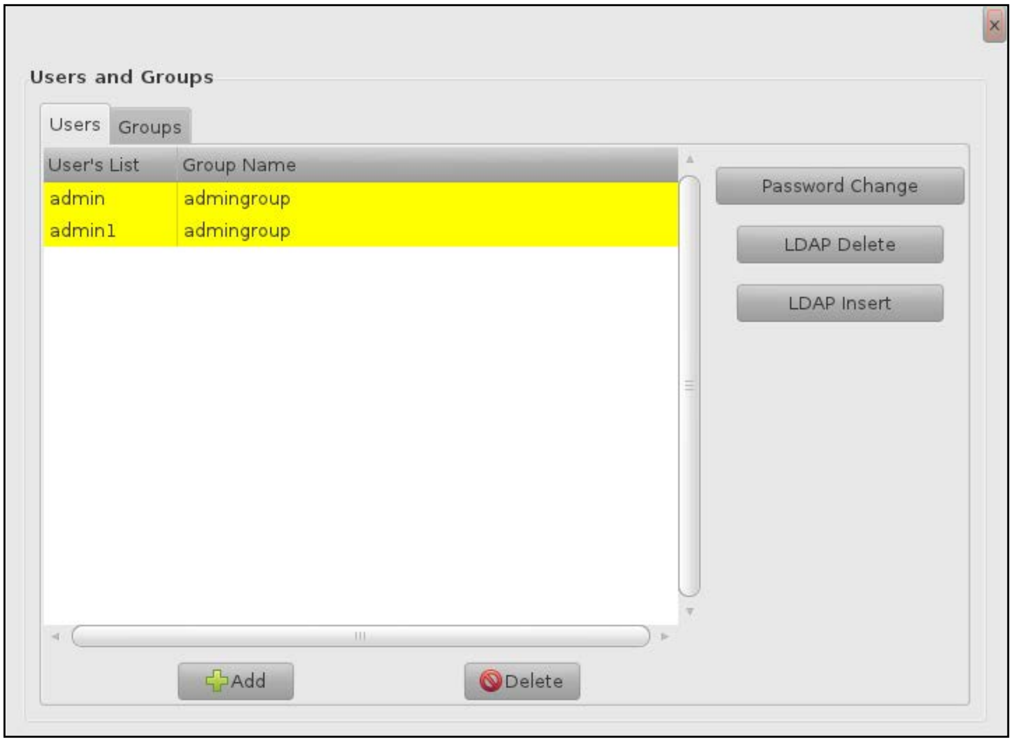
User Accounts

The User Accounts option allows you to manage user accounts and groups.

You can add a new user or group or delete an existing user or group.

To add a new user:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **User Accounts**. The **Users and Groups** window appears.



User's List	Group Name
admin	admingroup
admin1	admingroup

4. Click **Add**. The **New User** window appears.
5. Enter values in the following fields:
   - **Username**: Enter a username.
   - **Password**: Enter a password.
   - **Re-type Password**: Confirm the password by retyping the password.
   - **Group Name**: Select a group.
6. Click **OK**.

To delete an existing user account:

1. In the **Users and Groups** window, select the User to be deleted.
2. Click **Delete**. A confirmation message appears. Click **Yes**.

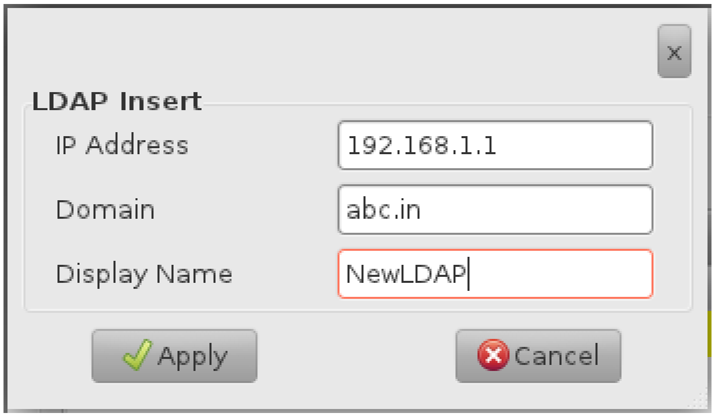
To change user password:

1. Select a particular user and click **Password change**.
2. In the **Current Password** field, enter the current password.
3. In the **New Password** field, enter the new password.
4. In the **Confirmation** field, retype the new password.
5. Click **OK**.

To create LDAP:

Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining directory information. This option allows you to search for users and groups in a particular domain.

1. In the **Users and Groups** window, click **LDAP** Insert. The **LDAP** insert dialog box appears.



LDAP Insert

IP Address: 192.168.1.1

Domain: abc.in

Display Name: NewLDAP

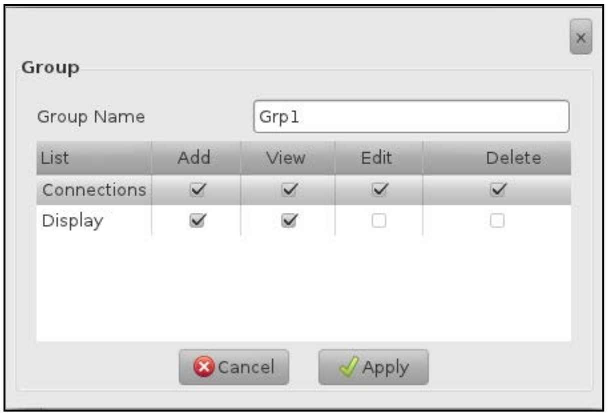
2. In the **IP Address** field, enter IP address.
3. In the **Domain** field, enter the domain name.
4. In the **Display Name** field, enter the display name.
5. Click **Apply**. A confirmation message appears, click **Yes**.

To delete an LDAP:

1. In the **Users and Groups** window click **LDAP delete**. The **Delete LDAP** window appears.
2. Select an LDAP and click **Delete**.

To add a group:

1. In the **Users and Groups** window, click **Groups** tab.
2. Click **Add**. The **Group** window appears.



Group

Group Name: Grp1

List	Add	View	Edit	Delete
Connections	☑	☑	☑	☑
Display	☑	☑	□	□

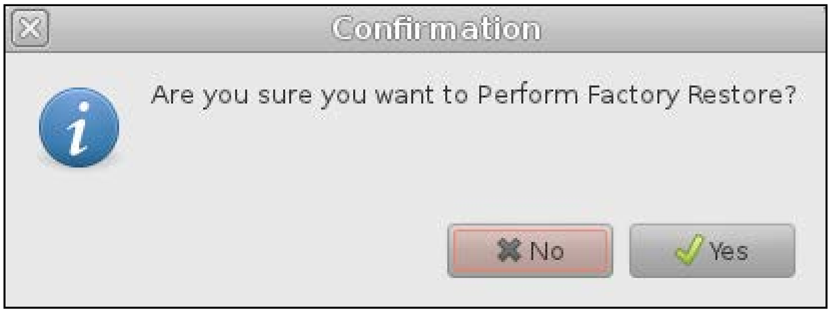
3. In the **Group Name** field, enter the group name.
4. Select the required permissions (**Add**, **View**, **Edit** or **Delete)** and click **Apply**.

Factory Reset

This option causes a software factory reset and an immediate reboot. The network, display, keyboard, mouse, time zone, user account and system language settings are reset.

To perform a factory reset:

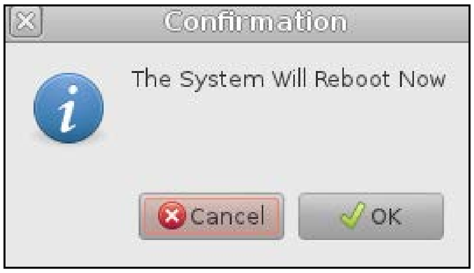
1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.
3. Click **Restore Factory Defaults.** The **Confirmation** window appears.



Confirmation

Are you sure you want to Perform Factory Restore?

4. Click **Yes.** The system will reboot now message appears.



Confirmation

The System Will Reboot Now

5. Click **OK**.

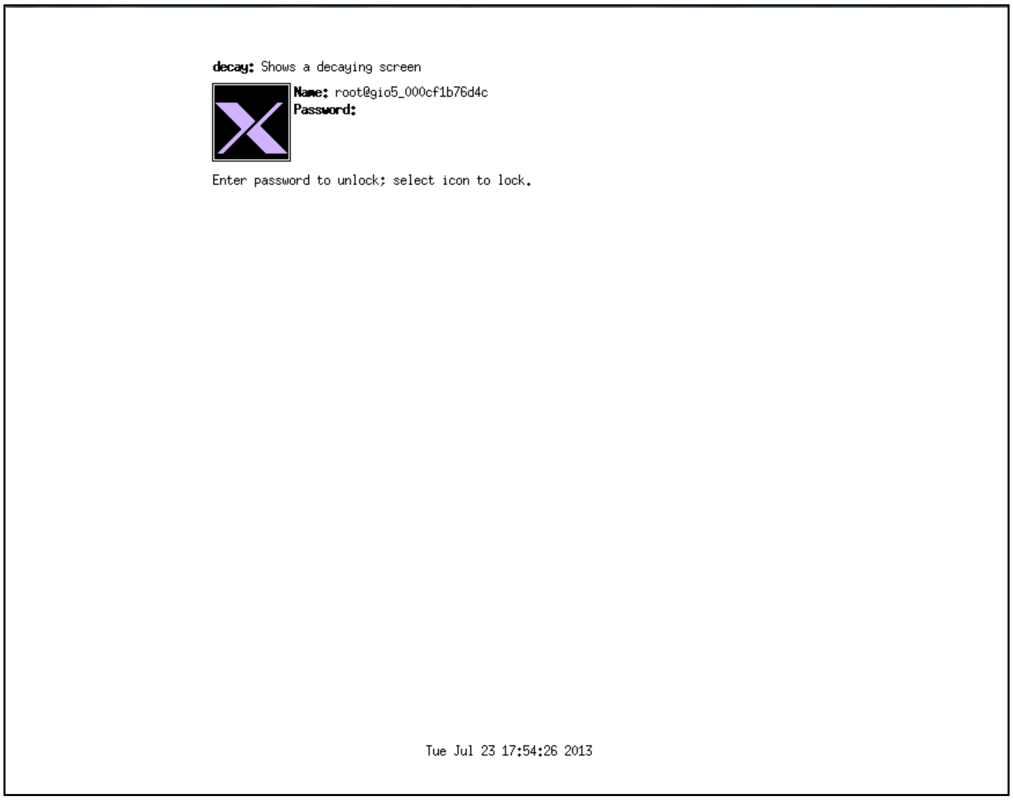
Screen Lock

The Screen Lock option allows you to lock your screen whenever required.

To lock your screen:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.

3. Click **Screen Lock**.



decay: Shows a decaying screen

Name: root@gio5_000cf1b76d4c
Password:

Enter password to unlock; select icon to lock.

Tue Jul 23 17:54:26 2013

4. The Screen is now locked. Enter your password and click **Submit** to unlock the screen.

Import Certificates

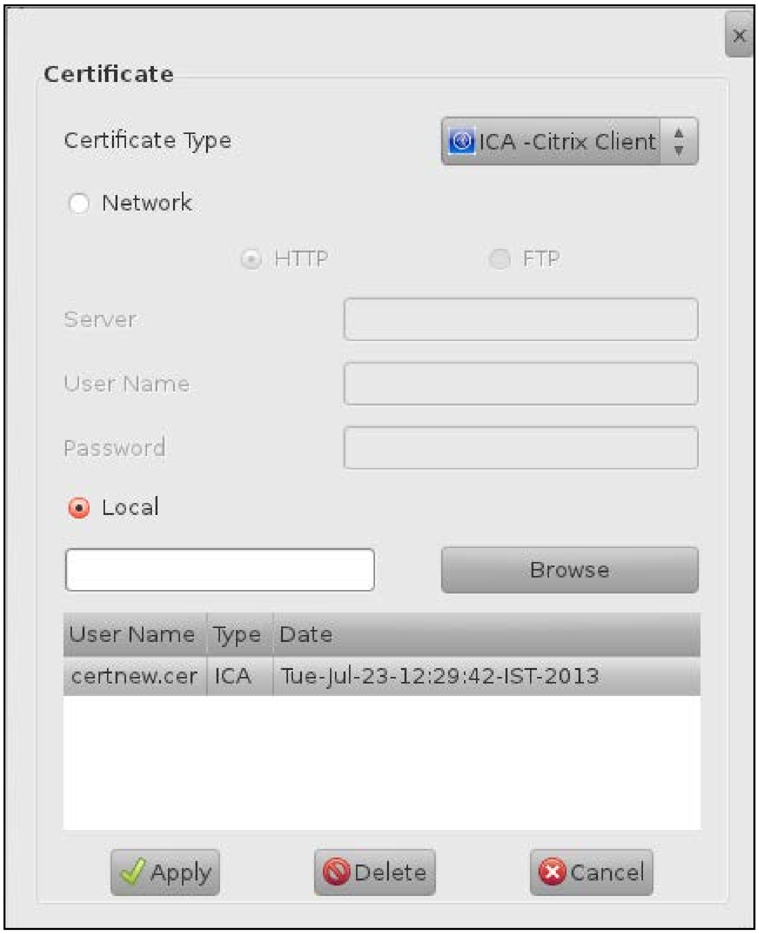
Certificates provide another layer of authentication for a connection. Security certificates are sometimes required to connect to servers using the SSL encryption protocol*. For example, you need a certificate to connect in case of a Citrix WFCMGR connection using SSL*. The certificates are generated by the server and can be imported to your client for authentication.

Certificates can be imported from the network or from the local client.

To import certificates from the local client:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.

3. Click **Import Certificates**. The **Certificate** dialog box appears.



Certificate

Certificate Type: ICA -Citrix Client

○ Network

● HTTP ○ FTP

Server

User Name

Password

● Local

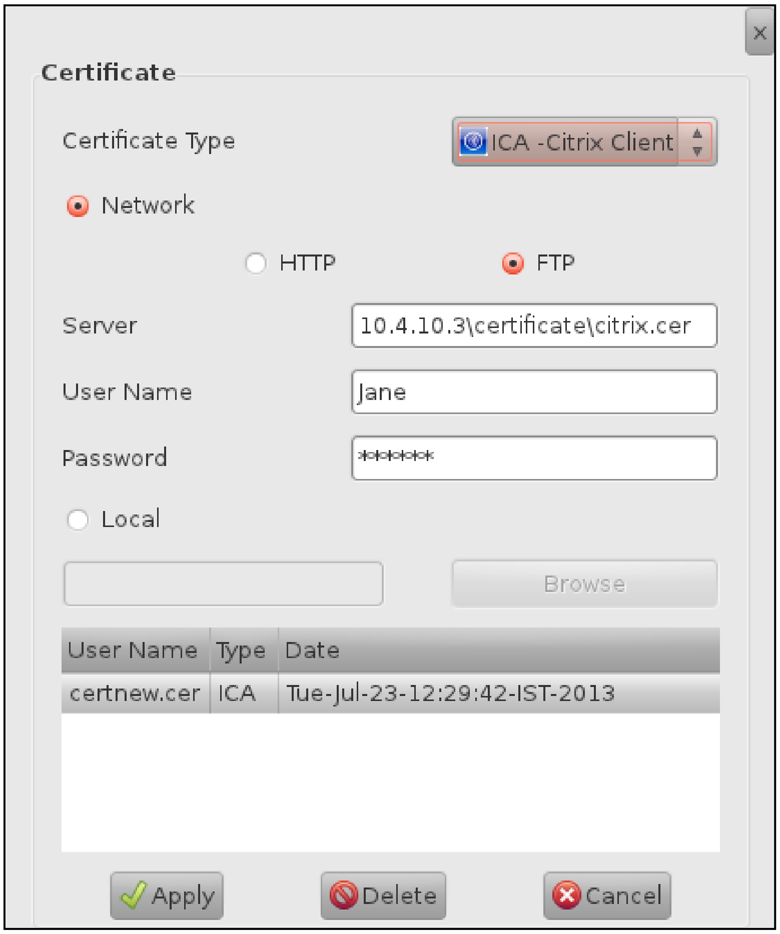
User Name	Type	Date
certnew.cer	ICA	Tue-Jul-23-12:29:42-IST-2013

4. In the **Connection Type** field, select the type of connection for which you want to import certificates.
5. Select the Local option.
6. Click **Browse**, locate and select the certificate.
7. Click **Apply**.

To import certificates from the network:

1. On the desktop sidebar, click **Settings** icon.
2. Click **Local Settings** drop-down arrow.

3. Click **Import Certificates**. The **Certificate** dialog box appears.



Certificate

Certificate Type: ICA -Citrix Client

● Network

○ HTTP ● FTP

Server: 10.4.10.3\certificate\citrix.cer

User Name: Jane

Password: ******

○ Local

User Name	Type	Date
certnew.cer	ICA	Tue-Jul-23-12:29:42-IST-2013

4. In the **Connection Type** field, select the type of connection for which you want to import certificates.
5. Select **Network** option.
6. Select the Server type HTTP or FTP.

- If you select **HTTP**: In the **Server** field enter the Server IP address and certificate path.
- If you select **FTP:**

a. In the **Server** field enter the Server IP address and certificate path.

b. In the **User Name** field, enter the Server User Name.

c. In the **Password** field, enter the Server Password.

7. Click **Apply**.

Note: The previously imported certificates are listed specifying the type and date.

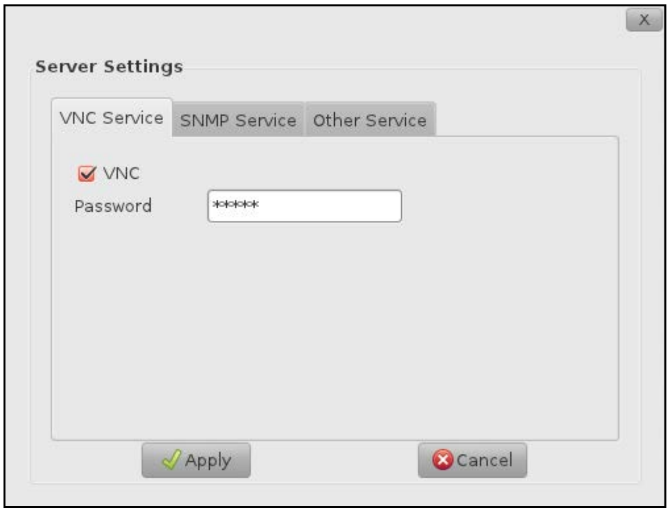
5 Security

Gio 5 has advanced security features to ensure that your client is safe from threats and attacks. You can secure your thin client by using the *Gio 5* server management services and proxy settings.

Server Management Services

To start server management services:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Security** drop-down arrow.
3. Click **Server Management**, the **Server Settings** window appears.



☑ VNC

Password *****

4. From the following list, select the required services:

   - **VNC**: Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the RFB protocol (remote framebuffer) to remotely control another computer. In the **Password** field, enter a password for VNC.

   - **SNMP**: Simple Network Management Protocol (SNMP) is a protocol to manage devices on IP networks. *For example, routers and gateways.* In the **Network/Subnet** field, enter the network or subnet IP address. In the **Password** field, enter a password for SNMP.

   - **PrinterServer (CUPS)**: Common UNIX Printing System (CUPS) is a primary printing mechanism for Ubuntu printing and print services.

   - **SAMBA:** SAMBA is the standard Windows interoperability suite of programs for Linux.

   - **Smart Card Demon:** This option allows you to access the smart card reader installed on the server.

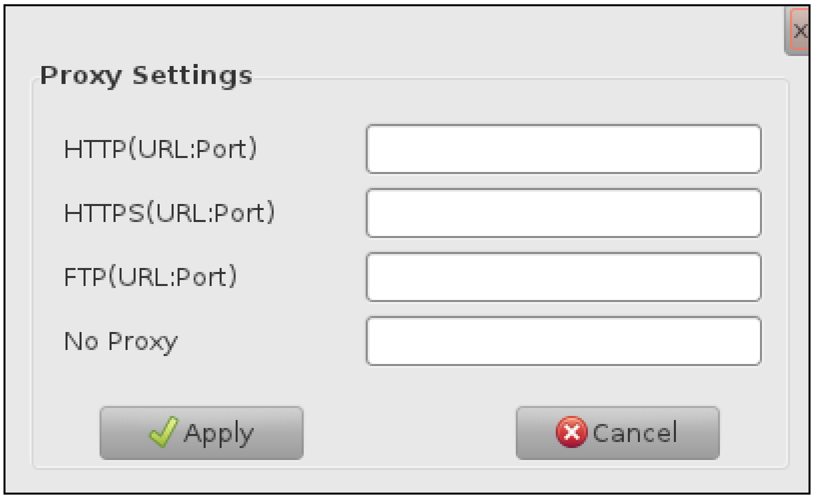
   - **Enable Pulse Audio:** Pulse Audio is a POSIX cross-platform network sound server.

5. Click **Apply**, the confirmation window appears.
6. Click **Yes**.

Server Proxy Settings

To configure the Server proxy settings:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Security** drop-down arrow.
3. Click **Server Proxy Settings**, the **Proxy Settings** window appears.



Proxy Settings

HTTP(URL:Port)

HTTPS(URL:Port)

FTP(URL:Port)

No Proxy

4. In the **HTTP** field, enter the HTTP URL and port number.
5. In the **HTTPS** field, enter the URL and port number.
6. In the **FTP** field, enter the URL and port number.
7. In the **No Proxy** field, enter the localhost or URL. You can enter more than one URL separated by a comma (,).

   Note: The URL or IP address specified in the **No Proxy** field will not connect through the proxy server.
8. Click **Apply**. The Confirmation dialog box appears.
9. Click **Yes**.

6 Diagnostics

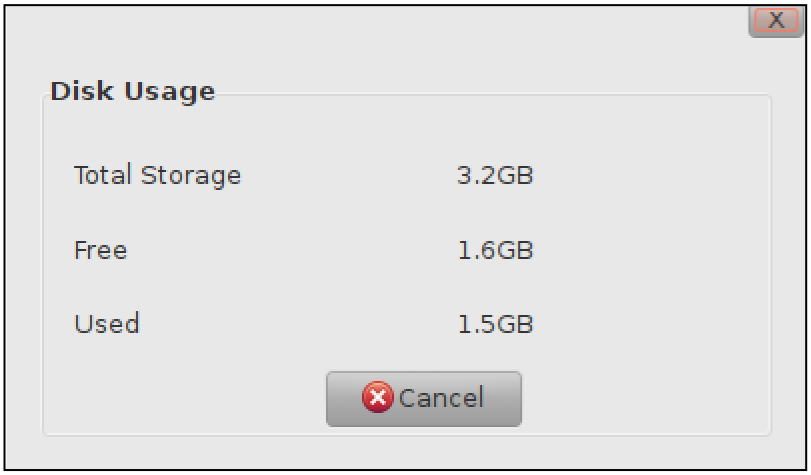
The diagnostics feature allows you to view the memory and network status information; you can launch the following memory and diagnostic tools:

Memory Log

The memory log tool provides system memory information such as total storage, free and used memory.

To access the Memory Log tool:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **Diagnostics** drop-down arrow.
3. Click **Memory Log**, the **Disk Usage** window appears. The current memory status appears.



Disk Usage

Total Storage	3.2GB
Free	1.6GB
Used	1.5GB

Network Log

The network log tool allows you to run network diagnostic tools to retrieve your network specific information.

To access the Network Log tool:

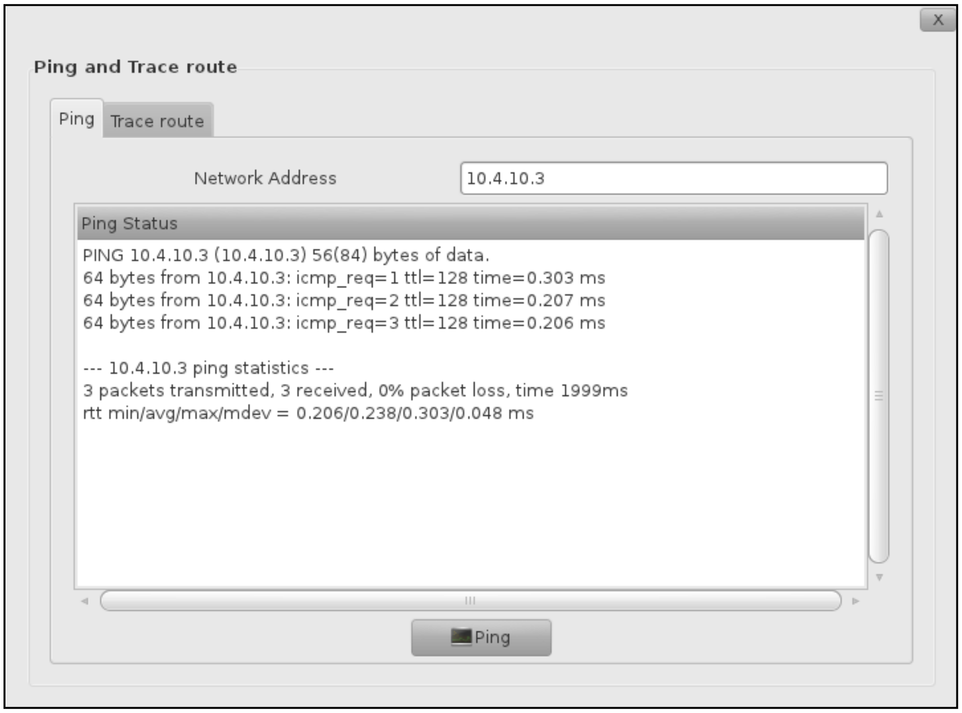
1. On the desktop sidebar, click **Settings** icon.
2. Click the **Diagnostics** drop-down arrow.
3. Click **Network Log**.
4. Select one of the following tools:
    - Ping & Trace route
    - DNS Lookup

Using Ping & Trace route Tool

Ping is a computer network administration utility used to test the availability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol network.

To access the ping and traceroute tool:

1. Click **Ping & Traceroute**, the **Ping and Traceroute** window appears.
2. In the **Network Address** field, enter the network address of the node you want to ping.
3. Click **Ping**, the ping result is displayed in the **Ping Status** section.

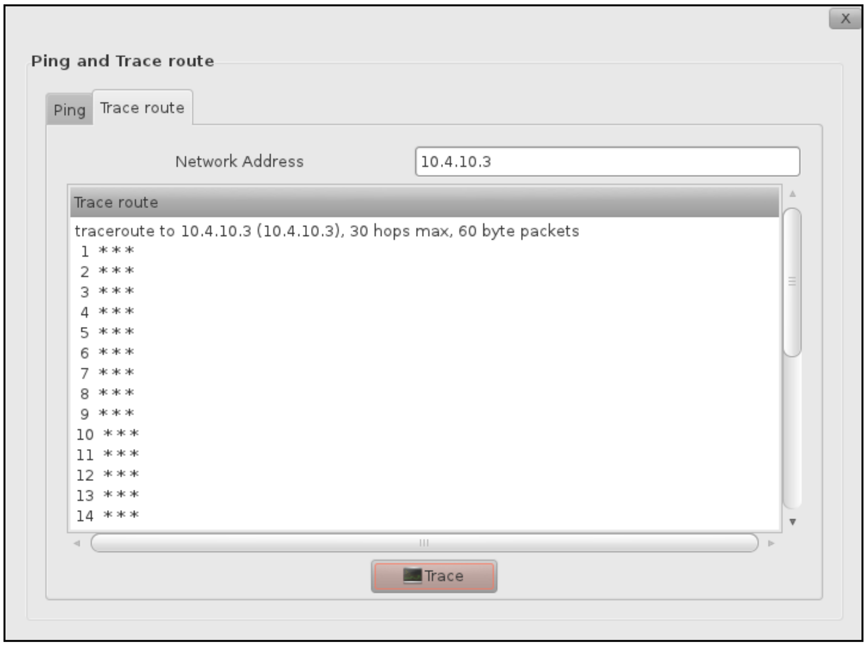


Network Address: 10.4.10.3

```
PING 10.4.10.3 (10.4.10.3) 56(84) bytes of data.
64 bytes from 10.4.10.3: icmp_req=1 ttl=128 time=0.303 ms
64 bytes from 10.4.10.3: icmp_req=2 ttl=128 time=0.207 ms
64 bytes from 10.4.10.3: icmp_req=3 ttl=128 time=0.206 ms

--- 10.4.10.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.206/0.238/0.303/0.048 ms
```

4. Click the **Trace route** tab.
5. In the **Network Address** field, enter the network address of the node for which you want to trace the route.

6. Click **Trace**, the trace result is displayed in the **Trace route** section.



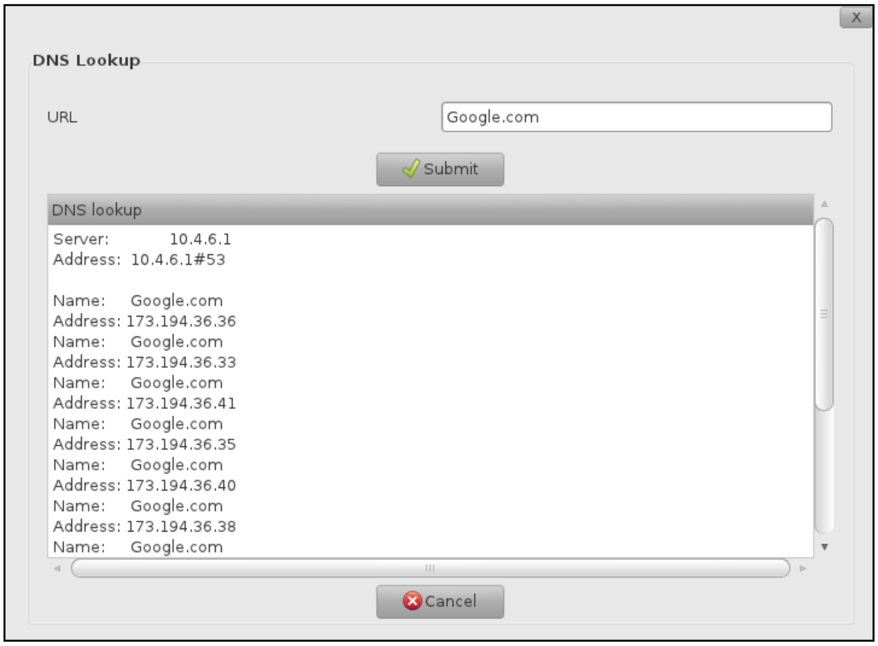
Network Address: 10.4.10.3

```
traceroute to 10.4.10.3 (10.4.10.3), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
```

Using DNS Lookup

DNS lookup tool is a tool used to determine the domain name of an IP address. To access the DNS lookup tool:

1. Click **DNS Lookup**, the **DNS Lookup** window appears.



URL: Google.com

```
Server:         10.4.6.1
Address:  10.4.6.1#53

Name:    Google.com
Address: 173.194.36.36
Name:    Google.com
Address: 173.194.36.33
Name:    Google.com
Address: 173.194.36.41
Name:    Google.com
Address: 173.194.36.35
Name:    Google.com
Address: 173.194.36.40
Name:    Google.com
Address: 173.194.36.38
Name:    Google.com
```

2. In the **URL** field, enter a URL.
3. Click **Submit**, the DNS Lookup result is displayed in the **DNS lookup** section.

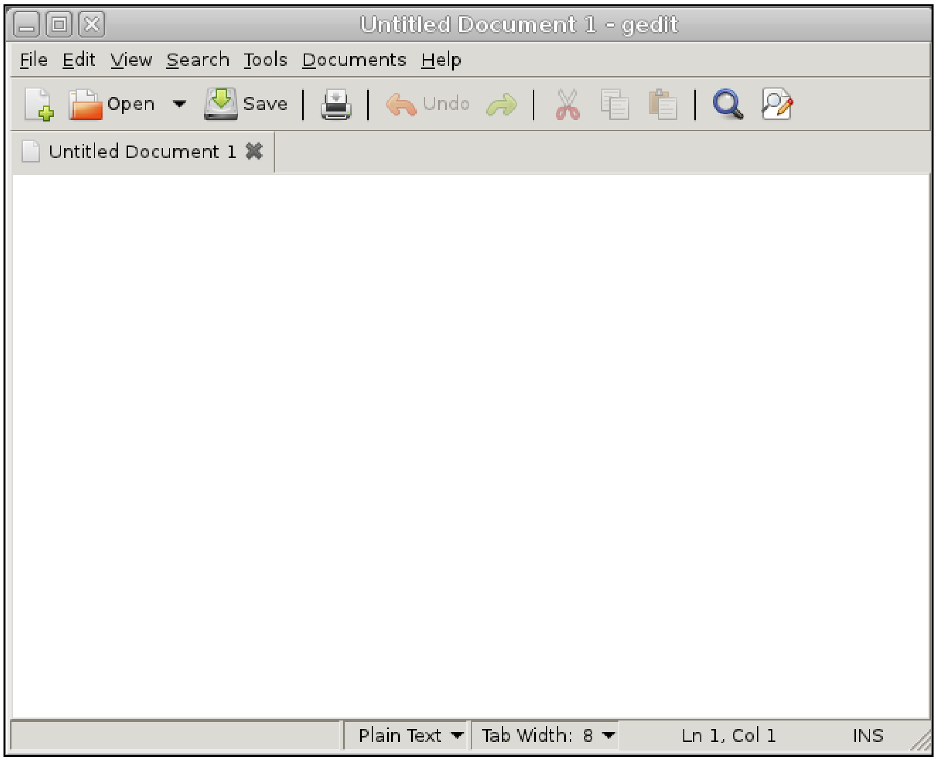
7 User Applications

Gio 5 is pre-installed with a number of useful user applications such as text editor, volume control, touch screen calibrator and web browser

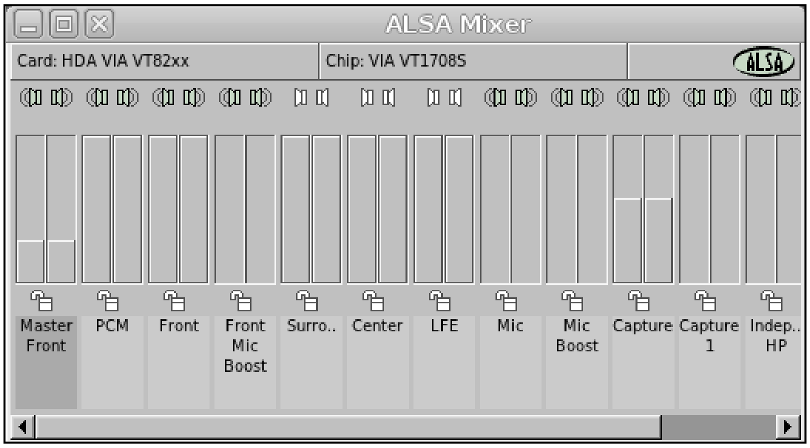
To access the various user applications:

1. On the desktop sidebar, click **Settings** icon.
2. Click the **User Applications** drop-down arrow
3. Select from the following list of user applications:

- **Text Editor**: This application provides you with basic text editing capabilities; you can type, edit and save text using this application.


Untitled Document 1 - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Untitled Document 1
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

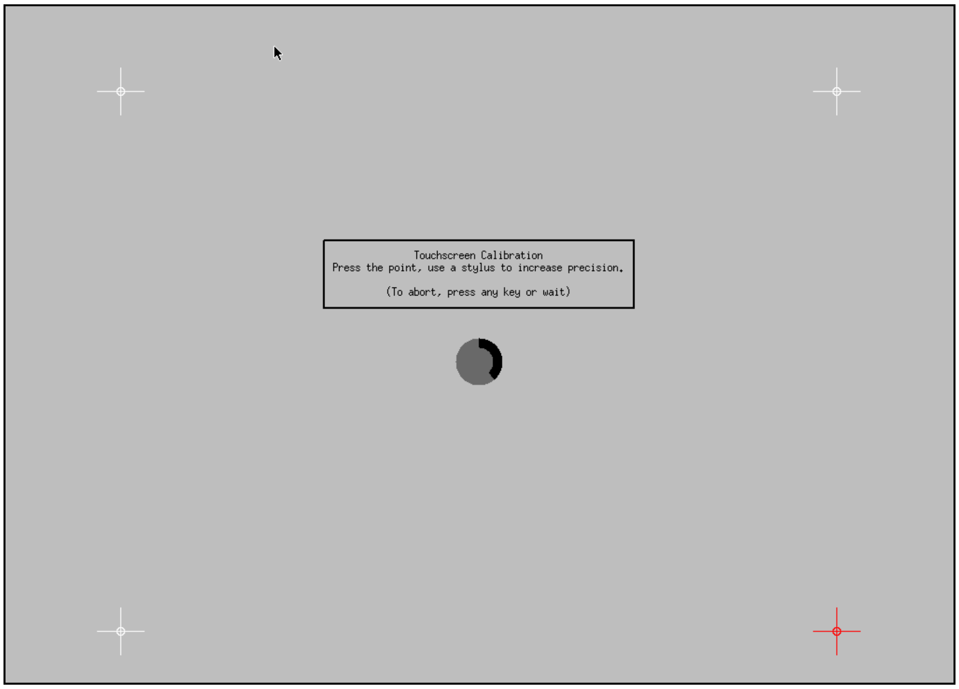
Volume Control: This application allows you to set the system sound settings.



Card: HDA VIA VT82xx

Chip: VIA VT1708S

- **Touchscreen Calibrator**: This application allows you to calibrate your touchscreen monitor.



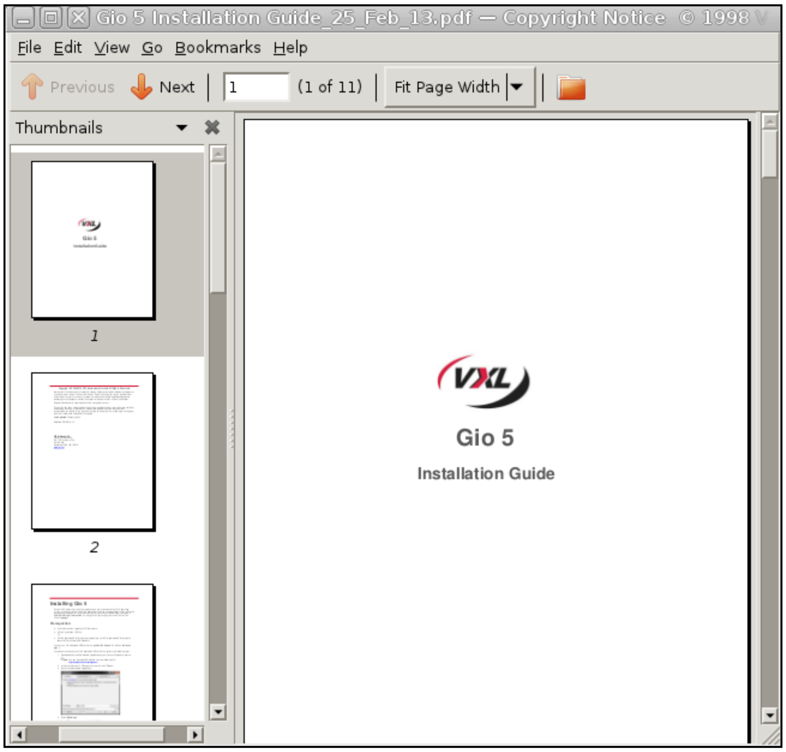
Touchscreen Calibration
Press the point, use a stylus to increase precision.

(To abort, press any key or wait)

To calibrate your touchscreen monitor, tap the four highlighted corners of the screen.

Note: You can use this application only when you have connected a touchscreen monitor to your client.

- PDF Reader: This application allows you to view Portable Document Format (PDF) documents.


Gio 5 Installation Guide_25_Feb_13.pdf — Copyright Notice © 1998 V
File Edit View Go Bookmarks Help
Previous
Next
1
(1 of 11)
Fit Page Width
Thumbnails
1
2
Gio 5
Installation Guide

Appendix GIO5 Configuration File

Setting up DHCP Scope ID for Automatic Configuration of GIO5

Requirements:

- DHCP Server with scope id configured.
- FTP Server that contains the configuration file.

Placing the Configuration File in the FTP server

The path where the Configuration file is available should be FTP configured. Place the INI file in the FTP root directory or FTP root subdirectories.

DHCP Server Scope ID Configuration

By default, the client is configured for 174 and 175 scope IDs. You can change these scope settings depending upon the DHCP server scope id configuration.

Information about the FTP server and configuration file path is obtained from the following DHCP scope- id:

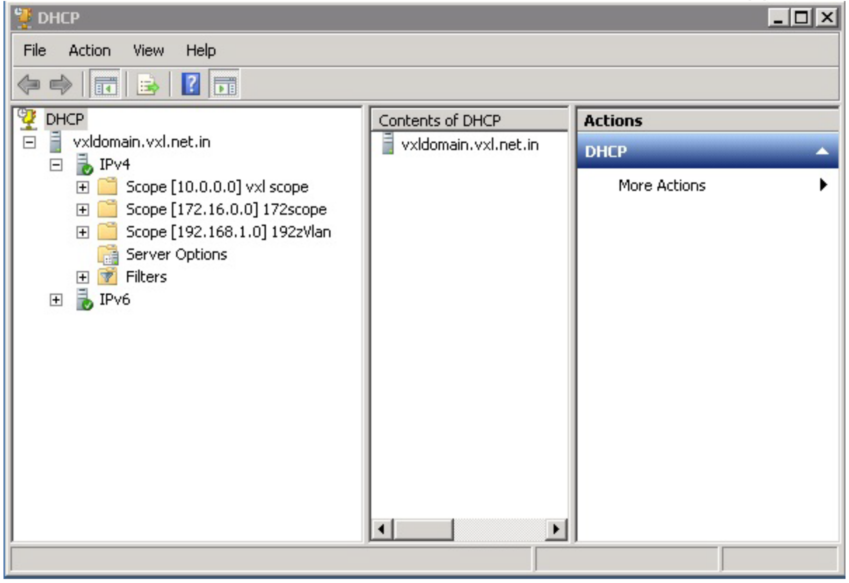
- 174: The FTP server IP Address or URL.
- 175: File name with extension or folder and file name with extension.

  If config.xml file is not mentioned the default config.xml file will be used.

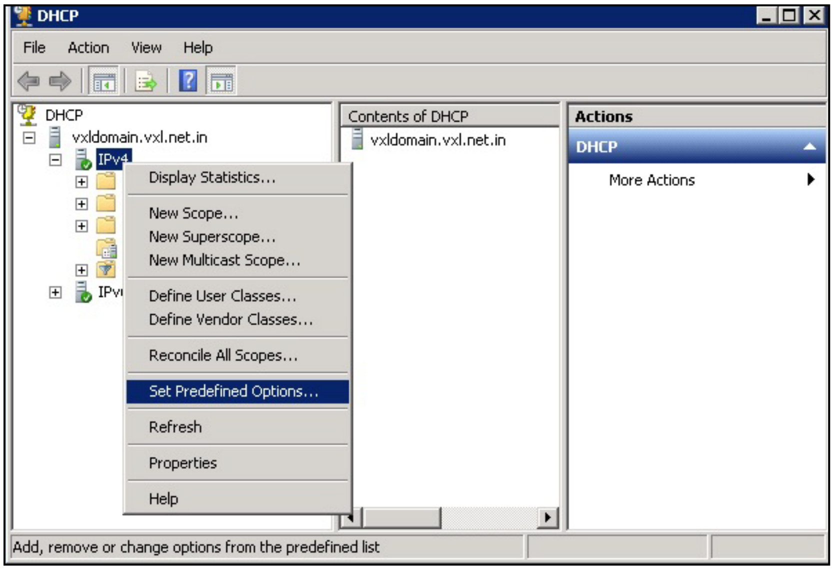
The automatic fetching of configuration file on the clients and automatic configuration is done using the DHCP scope options. The DHCP Server provides the configuration details. Ensure that the DHCP service is running.

To add new DHCP scope ids on the DHCP server:

1. On the DHCP server, click **Start** > **DHCP.** The **DHCP** window appears**.**

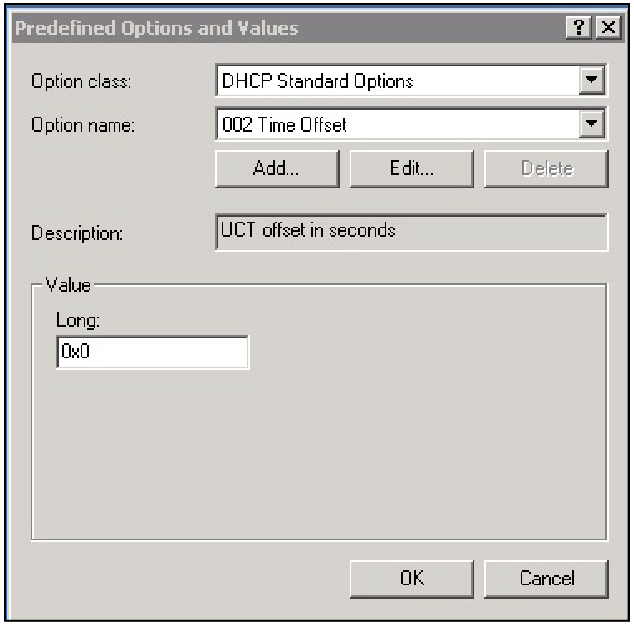


2. Right-click on **IPv4** and select **Set Predefined Options**.



Add, remove or change options from the predefined list

The **Predefined Options and Values** dialog box appears.



Option class: DHCP Standard Options

Option name: 002 Time Offset

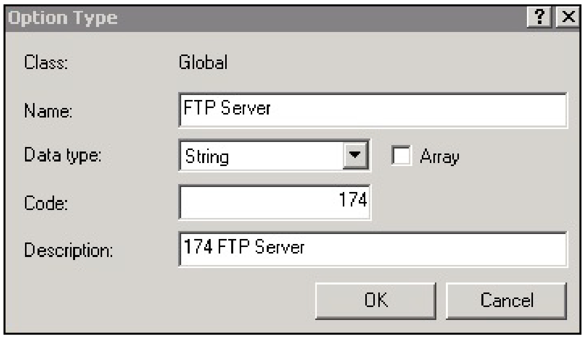
Description: UCT offset in seconds

Long: 0x0

3. In the **Option class** field, select **DHCP Standard Options** from the drop down list.

Note: Do not change the default value in the **Option name** field.

4. Click **Add.** The **Option Type** dialog box appears.



Option Type

Class: Global

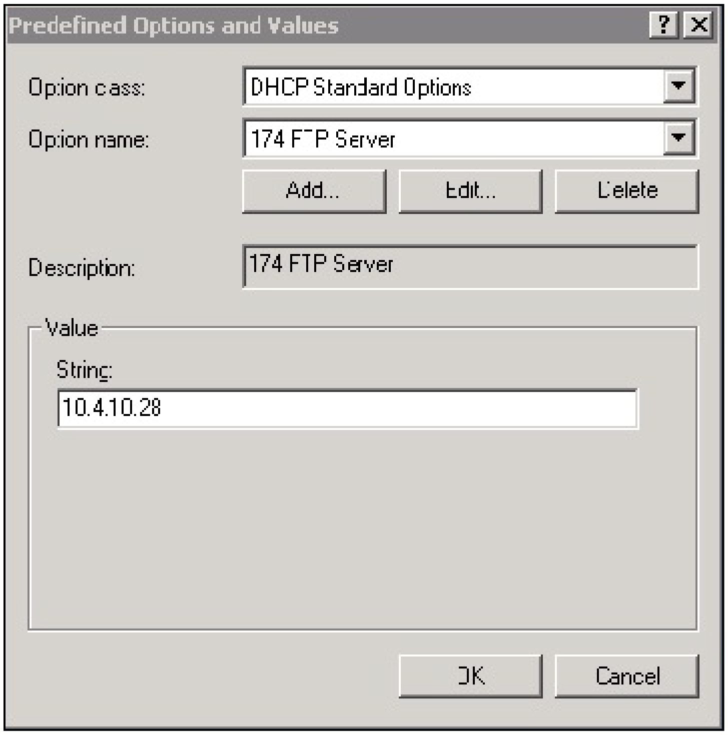
Name: FTP Server

Data type: String ☐ Array

Code: 174

Description: 174 FTP Server

5. Enter FTP server name in the **Name** field.
6. Select String in the **Data type** field.
7. Enter 200 in the **Code** field.
8. Enter a description in the **Description** field and click **OK**.



Predefined Options and Values

Opion cass: DHCP Standard Options

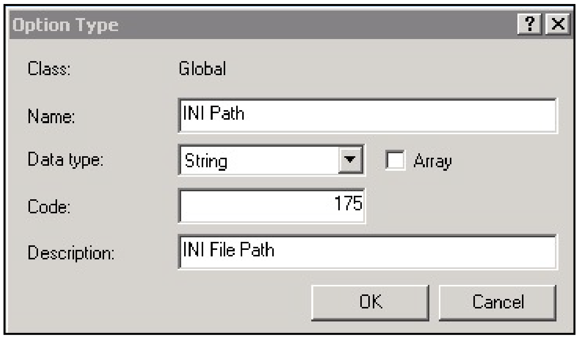
Opion name: 174 F¯P Server

Description: 174 FTP Server

Value

Strinc: 10.4.10.28

9. Enter the FTP server IP address in the **String field** and click OK.
10. Similarly, create scope ids for INI path with the values as shown in the below screens.



Option Type

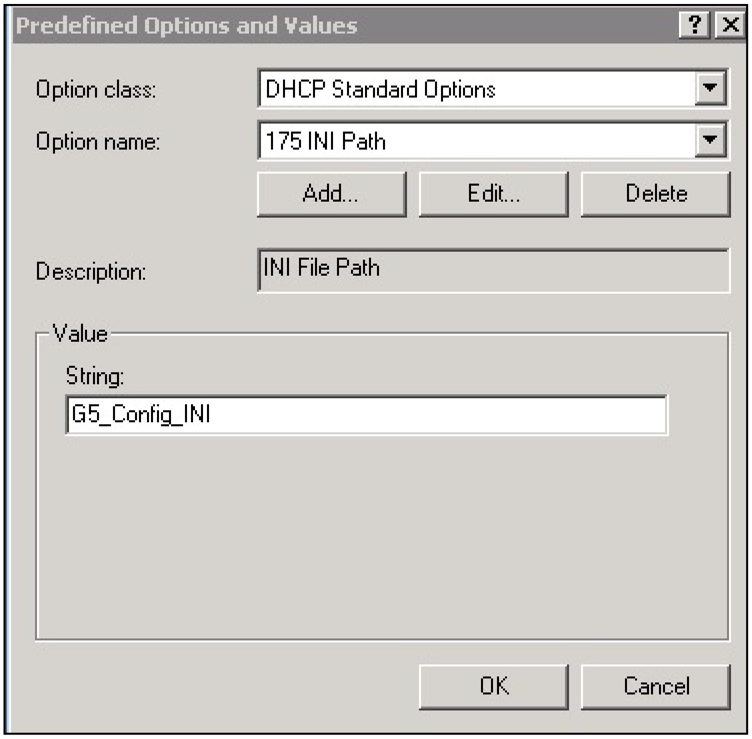
Class: Global

Name: INI Path

Data type: String □ Array

Code: 175

Description: INI File Path



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 175 INI Path

Description: INI File Path

Value

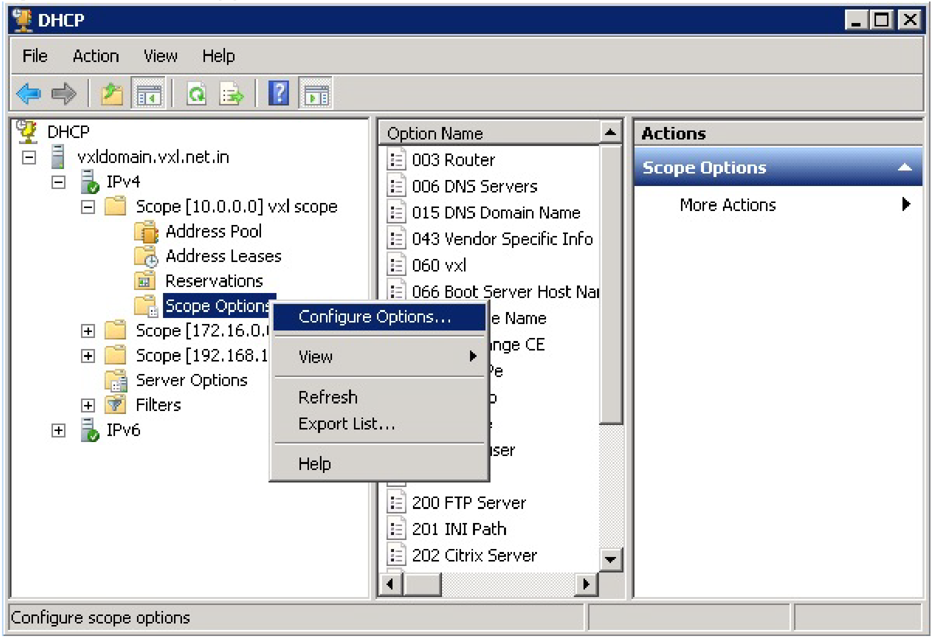
String: G5_Config_INI

If the INI file is in the FTP root mention the file name with extension in the **String** field.

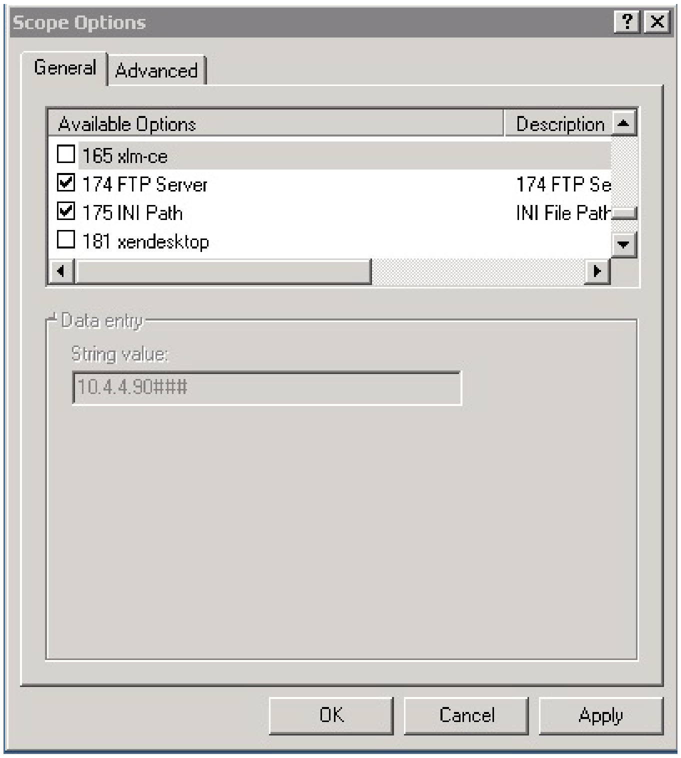
If the INI file is in the FTP root subdirectory mention the folder name and file name with extension in the **String** field.

To enable the created scope options (200/201/202):

1. On the tree pane, right-click **Scope Options** and select **Configure Options.** The **Scope Options** window appears.



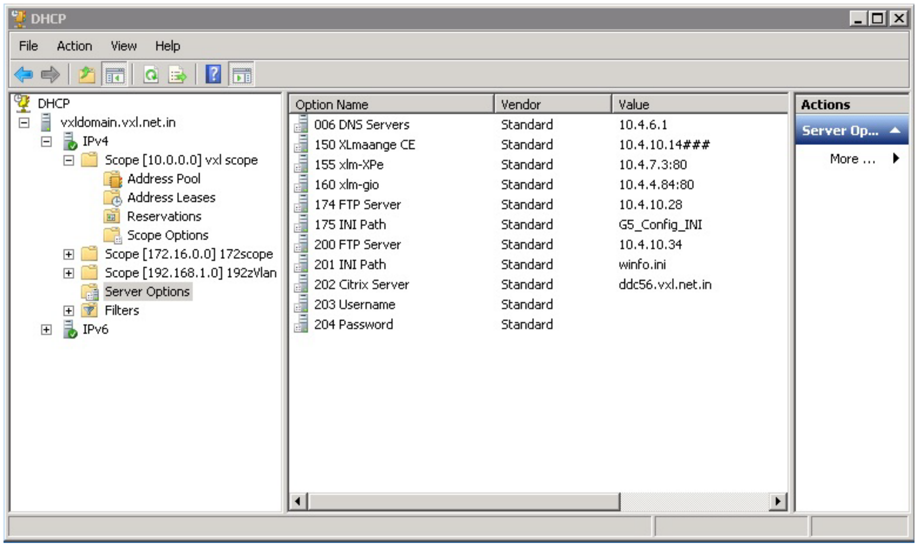
2. Select the FTP server scope id and FTP file server path scope id.



Available Options	Description
□ 165 xlm-ce	
☑ 174 FTP Server	174 FTP Se
☑ 175 INI Path	INI File Path
□ 181 xendesktop	

String value: 10.4.4.90###

3. Click **Apply** and then click **OK.** The selected server entry is displayed in the **Option Name** field on the central pane.



Option Name	Vendor	Value
006 DNS Servers	Standard	10.4.6.1
150 XLmaange CE	Standard	10.4.10.14###
155 xlm-XPe	Standard	10.4.7.3:80
160 xlm-gio	Standard	10.4.4.84:80
174 FTP Server	Standard	10.4.10.28
175 INI Path	Standard	G5_Config_INI
200 FTP Server	Standard	10.4.10.34
201 INI Path	Standard	winfo.ini
202 Citrix Server	Standard	ddc56.vxl.net.in
203 Username	Standard	
204 Password	Standard	

Reboot the Client

Once the client is rebooted, it will get the values from the defined scope id and downloads the configuration file and configures the client.

Creating and Using GIO5 Configuration File

You can generate the configuration file by using the GIO5 Config File Generator application provided by VXL Instruments.

Note: Ensure that the GIO5 image is compatible with GIO5 Config File Generator application.

For more information on generating a configuration files, refer the GIO5 Config File Generator user manual.

Glossary

Key Words	Description
CUPS	CUPS is the standards-based, open source printing system for UNIX$^{®}$-like operating systems.
Cache	A **cache** is a component that transparently stores data so that future requests for that data can be served faster. The data that is stored within a cache might be values that have been computed earlier or duplicates of original values that are stored elsewhere.
Dynamic Host Configuration Protocol (DHCP)	A protocol used by network administrators to centrally manage and automate the assignment of IP addresses in a network. Without DHCP, a fixed IP address needs to be assigned manually to each computer in the network.
Domain Name System (DNS)	The method used to translate Internet domain names into IP addresses. A domain name is a meaningful and easy-to-remember 'handle' for an IP address. The DNS method is based on DNS servers, which contain pre-defined and maintainable lists of domain names and IP addresses. Without this system, users would have to always remember and use IP addresses to access network computers or to browse the Internet.
Download	The transmission of a file from one computer system to another, usually in a smaller computer system. For an Internet-user, downloading a file is requesting and receiving from another computer (or from a Web page on another computer).
Encryption	A security measure that involves converting data to a form that cannot be easily understood by unauthorized systems. Simple encryption involves substituting letters for numbers and rotating letters in the alphabet. More complex encryption is based on computer algorithms that rearrange the data bits in digital signals. A correct decryption algorithm (key) recovers the contents of an encrypted transmission.
Firmware	A computer-program or software stored in PROM or EPROM.
File Transfer Protocol (FTP)	A protocol to exchange files between computers on the Internet. Like *Hyper Text Transfer Protocol (*HTTP) which transfers web pages, and *Simple Mail Transfer Protocol (*SMTP) which transfers email, FTP is an application protocol that uses the TCP/IP protocol to transfer files from one computer to another.
Gateway	A point in the network that acts as an entrance to another network. Computers that control traffic within a network or at an Internet Service Provider are gateway nodes. In an enterprise network, gateway servers usually also act as proxy and firewall servers. A gateway server is often associated with a router that knows where an incoming packet must be directed, and a switch that furnishes the actual path in and out of the gateway for a given packet.
Groups	A list of main groups where the clients are logically organized as per the requirement. Grouping manages clients more efficiently by organizing and

Key Words	Description
	classifying them under main groups and sub-groups. Any client can belong to only one sub-group or group.
Graphical User Interface (GUI)	A graphical (rather than purely textual) user interface to a computer. A GUI element includes windows, pull-down menus, buttons, scroll bars, icon images and wizards.
Independent Computing Architecture (ICA)	A technology developed by *Citrix Systems Inc* that provides a foundation for converting a client device to a Thin Client. It functions by separating the application logic from the user interface. While the application executes solely on the server, client-users can view and work with the interface of the application, when in fact the application actually executes on the server.
Internet	A worldwide system of computer networks in which a user from one computer gets information from any other computer. Physically, the Internet uses a portion of the total resources of the currently existing public telecommunication networks and a set of protocols called TCP/IP. The most widely used part of the Internet is the World Wide Web (*WWW or Web*). The outstanding feature of WWW is hypertext, a method of instant cross-referencing. Web pages can be viewed or browsed using browsers such as Netscape Navigator and Microsoft Internet Explorer.
IP Address	A unique 32-bit number that identifies the sender or receiver of information that is sent in a packet across the Internet. When there is a request for an HTML page or an e-mail is sent, the IP part of TCP/IP includes the IP address of the requestor or sender in the message. At the other end, the recipient can view the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the received IP address. The IP address is usually expressed as four decimal numbers, each representing eight bits, separated by periods. This is sometimes known as dot-address or dotted quad notation *Example: 192.16.4.12.*
Local Area Network (LAN)	A group of computers and associated devices sharing a common communication line and the resources of a single processor or server within a small geographic area *Example, within an office building.*
Media Access Control Address (MAC Address)	The unique hardware number of a computer in a network.
MD5	The Message Digest 5 (MD5) algorithm is a secure hash function.
Network	Series of points or nodes interconnected by communication paths. They can interconnect with other networks and contain sub-networks. The most common network topologies include: Bus, Star and Token Ring topologies. Networks can also be characterized in terms of spatial distance as LANs, MANs, and WANs.
NT Domain Name	NT domain name is the domain name of Windows NT based operating systems.

Key Words	Description
Port Number	A number that identifies the specific process to which an Internet or other network-message needs to be forwarded when it reaches a server. For the TCP and UDP protocols, a port number is a 16-bit number that is included in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the IP layer and forwarded on. *For example, When a client requests a server, for a file to be served from FTP of the server, the TCP layer in the client appends the number 21 to the request (21, is by convention the 16-bit port number associated with an FTP request). At the server, the TCP layer reads the port number (21) and forwards the request to the FTP program*.
Protocol	A special set of rules that end-points during communication in a telecommunication connection. It exists between each functional layer and in the corresponding layers at the other end of communication. Both end-points need to recognize and observe a protocol. *Examples: TCP/IP, HTTP and FTP*.
Speed Screen	Speed Screen latency reduction speeds up the transmission of images from the terminal server to the client.
Subnet	A computer or program that provides services to other computers or programs. In the client/server context, a server is a program that awaits and fulfills requests from client programs in the same or other computers.
Transmission Control Protocol / Internet Protocol (TCP/IP)	A separate part of a network having all computers in one geographical location in a building or on the same LAN. Networks divided into subnets can connect to the Internet with a single shared network address. Without subnets, each physical sub-network needs to have a separate connection to the Internet, resulting in unnecessary use of scarce network numbers that the Internet has to assign.
Thin Client	A low-cost, centrally managed computing device devoid of typical peripheral devices such as CD-ROM and diskette drives. The term derives from the fact that small computers in networks tend to be clients and not servers. Since the idea is to limit the capabilities of these computers to only essential applications, they tend to remain ‘thin’ in terms of pre-loaded client-applications.
VMware View Client	VMware View is a commercial desktop-virtualization product developed by VMware, Inc. VMware View provides remote desktop capabilities to users using VMware's virtualization technology.
VPN	A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible.
Wide Area Network (WAN)	A computer network that spans a relatively large geographical area. It consists of two or more LANs. Computers connected in WAN are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.

Key Words	Description
WEP	Wired Equivalent Protocol is a deprecated wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol".
WPA and WPA2	Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.
XLmanage	XLmanage is a thin client management application developed by VXL Instruments.

Index

Revision History

Version	Change Details	Authors	Date
GIO5J/UM-40-13	Creation	Anupama, Nagappan and Praveen	4/10/2013