Gio 5

Manuel d'utilisation

Dernière mise à jour : Juin 2013.

Version : GIO5/UM-23-13.

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

Table des matières

1 Introduction

Gio 5 est le dernier système d'exploitation client léger Linux proposé par VXL Instruments. *Gio 5* offre la flexibilité, la connectivité, la sécurité, le multimédia et capacités périphériques qui font de lui la solution idéale pour intégrer des grandes et des petites entreprises.

Ce manuel d'utilisation fournit des informations et des instructions pour configurer et utiliser *Gio 5* . Pour l'installation ou la restauration du *Gio 5* sur votre client léger, reportez-vous au Guide d'installation du *Gio 5*.

Fonctionnalités

Les principales fonctionnalités du Gio 5 sont les suivantes :

- Assistance en plusieurs langues :
  - Anglais
  - Français
  - Allemand
  - Espagnol
- Connexions disponibles :
  - Citrix ICA 12.1
  - VMware View 2.0
  - Rdesktop 1.7.1
  - xFree Rdp 1.0.1
  - standards ouverts SSH et SFTP
  - Navigateur Firefox 19.0
- Support réseau :
  - TCP/IP prend en charge IP V4 & IP V6
  - La sécurité réseau 802.1 est prise en charge
    - Le réseau sans fil (WLAN) prend en charge les cryptages suivants
    - WEP 40/128-bit
    - Phrase de sécurité WEP 128-bit
    - Dynamic WEP(802.1 x)
    - WPA & WPA2 Personal
    - WPA & WPA2 Entreprise
  - support client DHCP avec IPV4 et IPV6
  - Vitesse du réseau négociable automatiquement
- Support du lecteur réseau :
  - Samba (l'utilisateur peut le créer comme une connexion)
  - NFS (l'utilisateur peut le créer comme une connexion)
- Support d'affichage :
  - Support de l'affichage mode cloné et étendu
  - Résolution minimum 1024x768
  - Résolution maximum 1920x1200
  - Rotations d'affichage unique (gauche, droite, haut, bas)

    - Rotations du double affichage (gauche, droite, haut, bas)
    - Profondeur de couleur : (16/24/32 bit)
    - Display Power Management System (DPMS) : valeur par défaut 20 min
- Support d'impression :
    - Impression côté serveur (en utilisant le nom du pilote d'imprimante Windows utilisé avec ICA / RDP).
    - Impression réseau.
    - Impression local via Common Unix Printing System (CUPS).
    - Les ports pris en charge pour l'impression sont LPT et USB.
    - Affichage de la file d'attente d'impression et du statut de l'impression.
    - Impression partagée via IPP.
- Support de périphérique externe :
    - Disque dur USB, lecteurs Flash, lecteur CD / DVD USB
    - Webcam USB
    - Haut-parleur, casque audio USB
    - Lecteur de cartes à puce USB support pour Omnikey, lecteur RCS
- Fonctionnalité de sécurité du client :
    - Authentification Windows Active Directories
    - Support multiutilisateurs
- Clavier :
    - Support clavier USB et PS2
    - 93 dispositions de clavier sont prises en charge.
    - Taux de répétition contrôlable.
    - Temporisation contrôlable.
    - Divers variantes et modèles de clavier sont pris en charge.
    - Verrouillage numérique au démarrage
- Souris :
    - Support souris USB et PS2
    - Vitesse d'accélération de la souris contrôlable
    - Bouton gauche de la souris on/off
    - Masquer automatiquement le pointeur de la souris
- Applications locales :
    - Lecteur multimédia Totem
    - Éditeur de Texte Gedit
    - Lecteur PDF Evince
    - Commande du volume mélangeur Alsa
    - Navigateur Internet Fire Fox
- Pilote de l'interface graphique :
    - prend en charge pilote graphique VIA Intégré
    - Pilote GFX v92 pour support graphique
    - Prend en charge le double affichage et Rotation
- Mise à niveau du micrologiciel :
    - Composant individuel de mise à niveau
- Gestion du dispositif de d'assistance du client léger :
    - La gestion du dispositif de d'assistance se fait à travers le logiciel 'XLManage Device Management'.

Assistant de configuration

La fenêtre de l'**Assistant de configuration** apparaît immédiatement après l'installation du Gio 5. Cet assistant vous permet de définir la langue du système, le fuseau horaire et la langue du clavier au démarrage.

Figure 1-1 : Assistant de configuration

Pour définir la langue du système, le fuseau horaire et la langue du clavier au démarrage :

1. Dans la zone de sélection numérique de l'**option Langue** sélectionnez la langue du système.
2. Dans la zone de sélection numérique du **fuseau horaire** sélectionnez le fuseau horaire requis.
3. Dans la zone de sélection numérique du **Type de clavier** sélectionnez la langue du clavier.

Remarque : Sélectionnez l'option **ne plus demander à nouveau** pour ne pas afficher l'assistant de configuration la prochaine fois.

Organisation du manuel d'utilisation

Le contenu de ce manuel est organisé comme indiqué dans le tableau suivant :

Nº chapitre	Chapitre	Description
1	Introduction	Présentation du Gio 5
2	Ordinateur de bureau Gio 5	Description des différents composants de l'ordinateur de bureau et de l'interface.
3	Connectivité	Description des procédures de configuration pour les connexions au réseau et au serveur.
4	Paramètres locaux	Description et procédure pour définir divers paramètres locaux. Configuration des périphériques d'entrée et de sortie, tels que la souris, l'imprimante.
5	Sécurité	Description de la définition de la sécurité et la gestion de serveur.
6	Diagnostic	Description et procédure pour utiliser les outils de diagnostic du Gio 5.
7	Applications utilisateur	Description des diverses applications de l'utilisateur installé dans le Gio 5
8	Glossaire	Liste de mots-clés/sujets utilisés dans ce manuel triés par ordre alphabétique.
9	Index	Définitions des termes techniques utilisés dans ce manuel

Tableau1 : Liste des chapitres

Terminologies

Ce manuel utilise les expressions suivantes pour décrire quelques termes utilisés couramment :

Terminologies	Description
Gio 5	Un client léger Linux avec un système d'exploitation spécifique développé par *VXL Instruments*®.
Client léger /client léger	*Client léger VXL*

Tableau2 : Terminologies

Conventions typographiques

Ce manuel utilise les conventions typographiques suivantes :

Type de texte	Utilisation
Texte en gras	Noms de champ, éléments d'interface utilisateur tels que les boîtes de dialogue et fenêtres
Texte EN PETIT CARACTERE	Messages du système
Texte *en italique*	Noms propres et exemples
Texte en `Courier new`	Syntaxe et entrées de l'utilisateur
Texte en **gras** et EN MAJUSCULES.	Raccourcis clavier. Par exemple, **CTRL+C**
Texte en *Bleu souligné en italique*	Hyperliens externes (ouvre votre navigateur par défaut)

Tableau3 : Conventions typographiques

2 Ordinateur de bureau Gio 5

Un environnement de bureau de l'interface utilisateur graphique fournit des menus et des icônes pour l'interaction avec le système d'exploitation. *Gio 5* est un système d'exploitation basé sur l'interface utilisateur graphique (GUI). Le bureau du *Gio 5* prend en charge l'accélération 3D et composite. Il prend également en charge l'accélération vidéo du réseau. Le bureau *Gio 5* se compose de :

- Icônes du bureau et widgets sur l'écran d'accueil.
- Barre latérale qui permet d'accéder aux caractéristiques du système d'exploitation
- Applications et services actifs sur l'onglet de l'espace de travail.

L'environnement de bureau du Gio 5 comprend les composants suivants :

Figure : 2-1 Ordinateur de bureau Gio 5

- Onglet Espace de travail: Les applications utilisateur qui sont minimisées apparaissent dans l'onglet de l'espace de travail pour un accès rapide.
- Barre latérale : La barre latérale permet d'accéder à la fonctionnalité de système d'exploitation et aux applications. Pour accéder à la barre latérale déplacez le curseur de la souris dans le coin inférieur gauche de l'écran du bureau.

Icônes de la barre latérale	Description
	Informations
	Paramètres
	Alimentation

Informations du système

Vous pouvez afficher les différentes informations spécifiques à votre système comme la version du noyau, l'adresse IP à partir de l'option informations du système. Vous pouvez afficher les informations du système en cliquant sur l'icône **Informations** de la barre latérale. Cliquez sur **Clause de non-responsabilité** ou **licence** pour afficher les détails sur la clause de non-responsabilité et la licence.

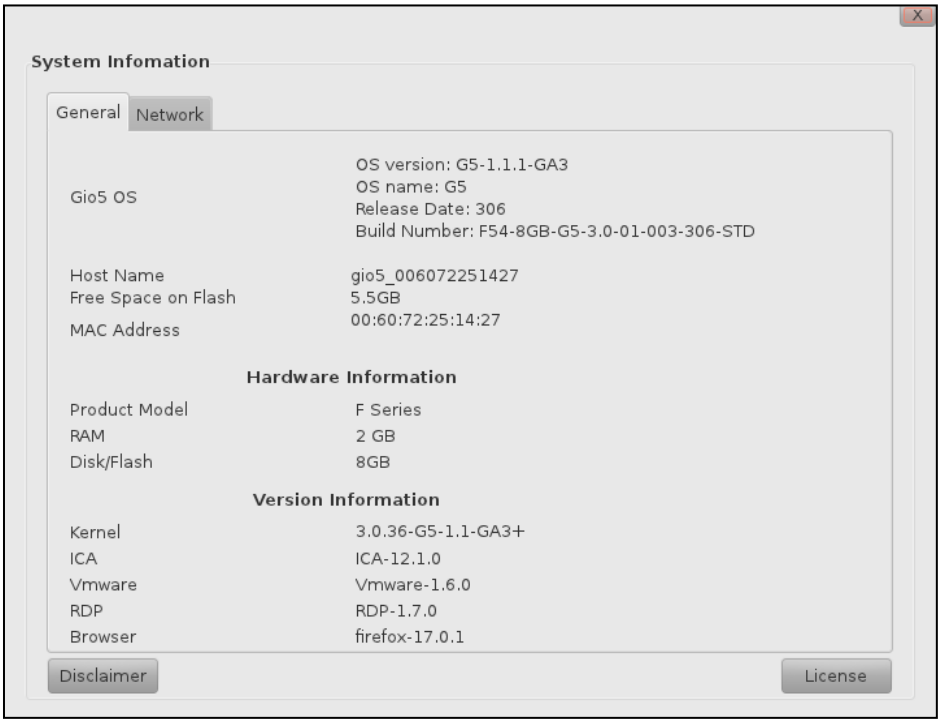

Figure : 2-2 Informations-Générales du système

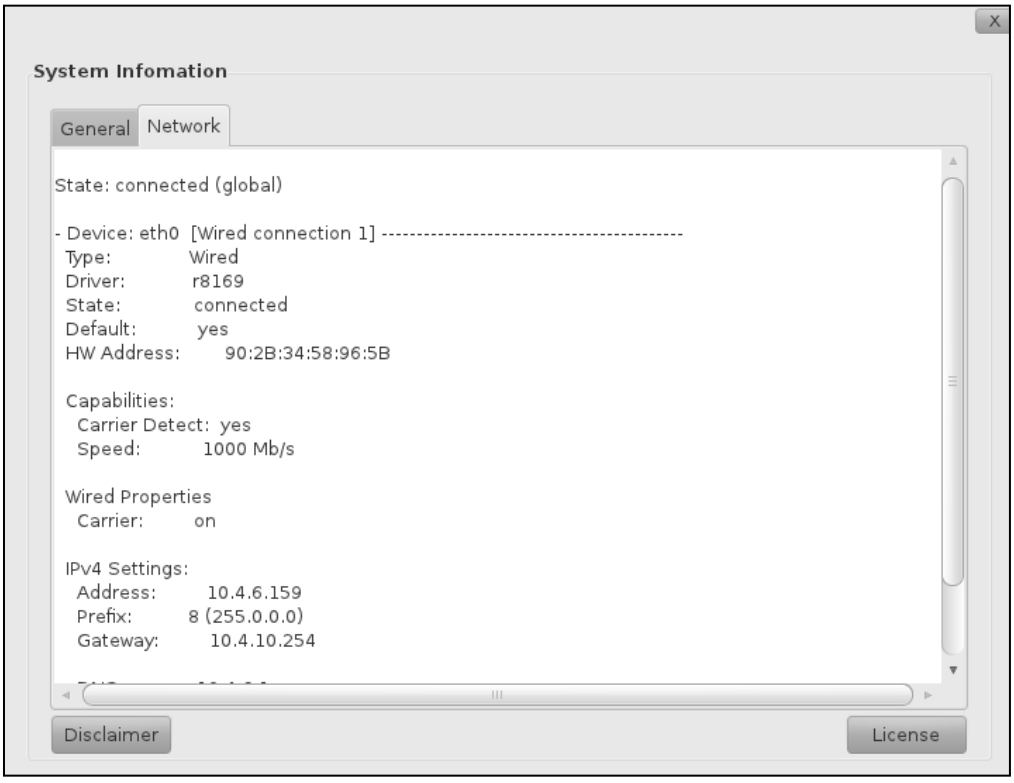

Figure : 2-3 Informations-Réseau du système

Paramètres

Vous pouvez afficher et configurer les paramètres du système d'exploitation de votre *Gio 5* à l'aide de l'option Paramètres. Cette option vous permet de configurer votre réseau, connexions, périphériques d'entrée/sortie, etc. Les chapitres suivants de ce manuel d'utilisation fournissent des instructions et des informations sur divers paramètres.

Pour accéder aux différents paramètres :

1. Cliquez sur l'icône **Paramètres** dans la barre latérale. La boîte de dialogue d'**Authentification** s'affiche.

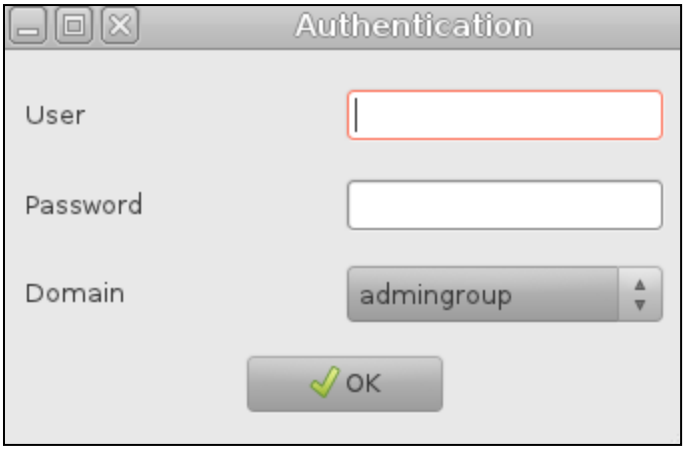

Figure : 2-4 Boîte de dialogue d'authentification

2. Saisissez le nom d'utilisateur et le mot de passe.

3. Sélectionnez le domaine, puis cliquez sur **OK**.

Remarque : Dans le champ **Domaine** sélectionnez **Local** pour l'authentification locale ; sélectionnez un domaine LDAP particulier pour l'authentification sur le serveur LDAP. Pour plus d'informations sur la création du LDAP se reporter à la section " Créer LDAP " page 92.

Arrêter et redémarrer Gio 5

Pour arrêter votre client léger :

1. Dans la barre latérale, cliquez sur l'**icône de l'alimentation**.
2. Dans le menu déroulant, sélectionnez **Arrêter.**

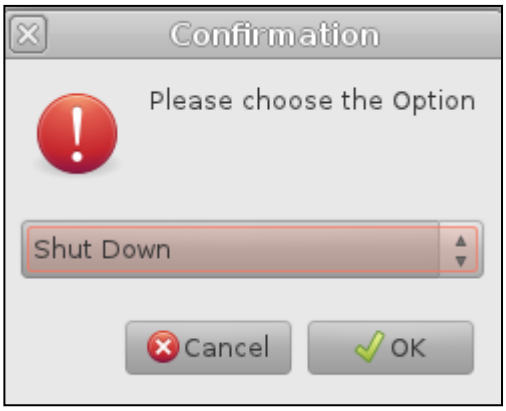

Figure : 2-5 Arrêter

3. Cliquez sur **OK**.

Pour redémarrer votre client léger :

1. Dans la barre latérale, cliquez sur l'**icône de l'alimentation**.
2. Dans le menu déroulant, sélectionnez **Redémarrer**.

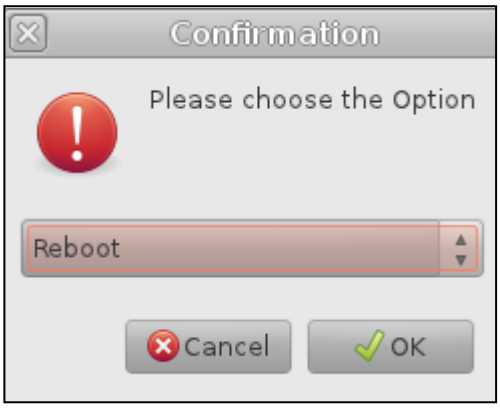

Figure : 2-6 Redémarrer

3. Cliquez sur **OK**.

3 Connectivité

Gio 5 fournit plusieurs options de connectivité pour configurer votre réseau et connecter votre client à un serveur. Les options de connexion de réseau tels que câblée, sans fil et VPN vous permettent de connecter votre client léger à différents environnements d'infrastructure de réseau, vous pouvez configurer votre réseau en fonction de vos préférences en utilisant l'option **Configurer réseau**.

Gio 5 permet à votre client léger de se connecter à un serveur en utilisant les principaux protocoles et outils comme ICA, RDP, VMware View et Citrix Receiver, vous pouvez configurer ces paramètres à l'aide de l'option **Gestionnaire de connexion**.

Vous pouvez gérer votre *Gio 5* de type client léger à partir de l'application de gestion du client léger *VXL Instruments XLmanage*. Vous pouvez établir une connexion avec le serveur de l'application *XLmanage* en utilisant l'option **Connexion XLM**.

Configurer le nom d'hôte

Le nom de l'hôte est un nom personnalisé utilisé pour identifier votre client léger sur le réseau.
Vous pouvez modifier le nom d'hôte en fonction de vos préférences. *Par exemple, Lab Thin Client.*

Pour modifier le nom de l'hôte :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Configurer le nom d'hôte.** La boîte de dialogue du **nom d'hôte** s'affiche.

Figure : 3-1 Nom d'hôte

4. Entrez un nom d'hôte et cliquez sur **Appliquer.** Le client va redémarrer.

Configurer le réseau

L'option **Configurer Réseau** vous permet de configurer votre connexion au réseau. Vous devez configurez votre réseau pour connecter votre client léger à un serveur. Une configuration de réseau correcte garantit que votre client léger est sécurisé et connecté au serveur voulu.

Pour configurer une connexion réseau :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Configurer le réseau,** la fenêtre de connexion réseau s'affiche.

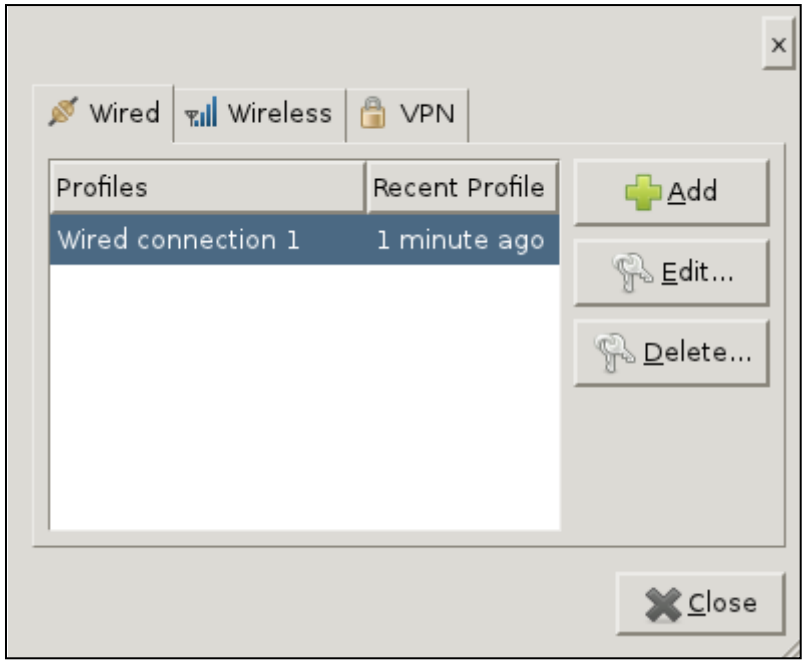

Figure 3-2 : Configurer le réseau

Vous pouvez configurer le type de connexions suivantes :

- Câblé
- Sans fil
- Réseau privé virtuel (VPN)

Connexion câblée

Une connexion câblée, aussi connu comme une connexion Ethernet est l'une des façons la plus rapide de se connecter à un réseau. Dans une connexion câblée, un câble Ethernet relie votre client léger à votre infrastructure de réseau.

Pour configurer une connexion câblée, créez une connexion câblée et configurez IPv4 ou IPv6 avec la sécurité.

Création d'une connexion câblée

Pour créer une connexion câblée :

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Câblée**.
2. Cliquez sur **Ajouter**.

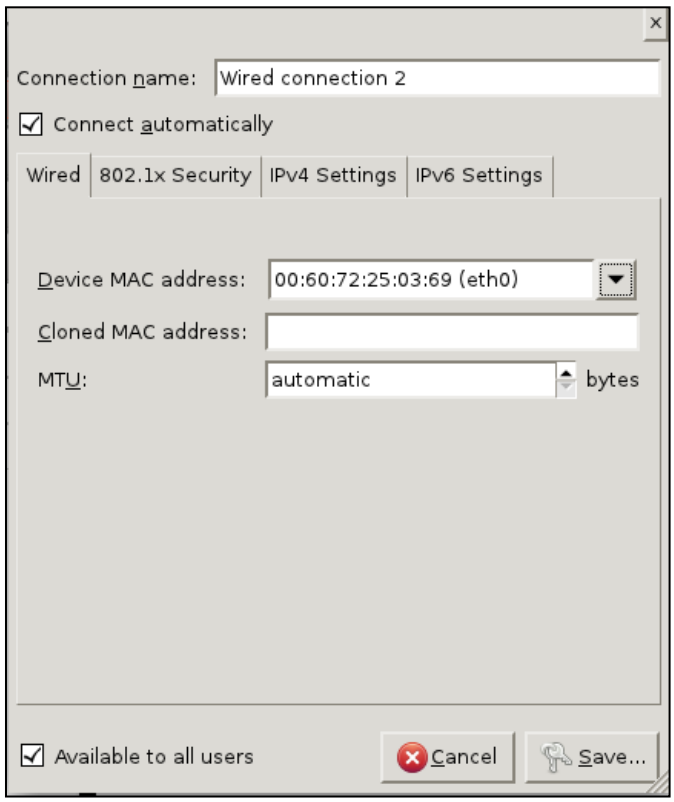

Figure 3-3 : Connexion câblée

3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.

   Remarque : Sélectionnez l'option **Connecter automatiquement** pour en faire votre réseau par défaut.

4. Dans liste déroulante de l'**adresse MAC du périphérique**, sélectionnez l'adresse MAC de votre périphérique.
5. Dans la zone de sélection numérique de la **MTU** configurez une valeur MTU (Unité de transmission maximale). Sélectionnez **Automatique** pour une valeur MTU du réseau par défaut.
6. Cochez la case **Disponible pour tous les utilisateurs** pour permettre à d'autres utilisateurs du client léger de se connecter à ce réseau. Cette option n'est pas sélectionnée par défaut.
7. Cliquez sur **Enregistrer**.

Configurer la sécurité de la connexion câblée

Le *Gio 5* offre des options de protocole de sécurité 802.1x, 802.1x est une norme de sécurité et d'authentification pour les connexions réseau câblées et sans fil. Vous pouvez choisir parmi plusieurs options d'authentification qui font partie de la suite de protocole 802.1x.

Pour configurer la sécurité de la connexion câblée :

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez configurer.
2. Cliquez sur **Éditer.**
3. Cliquez sur l'onglet **Sécurité 802.1x**, cochez la case **Utiliser sécurité 802.1x pour cette connexion**.

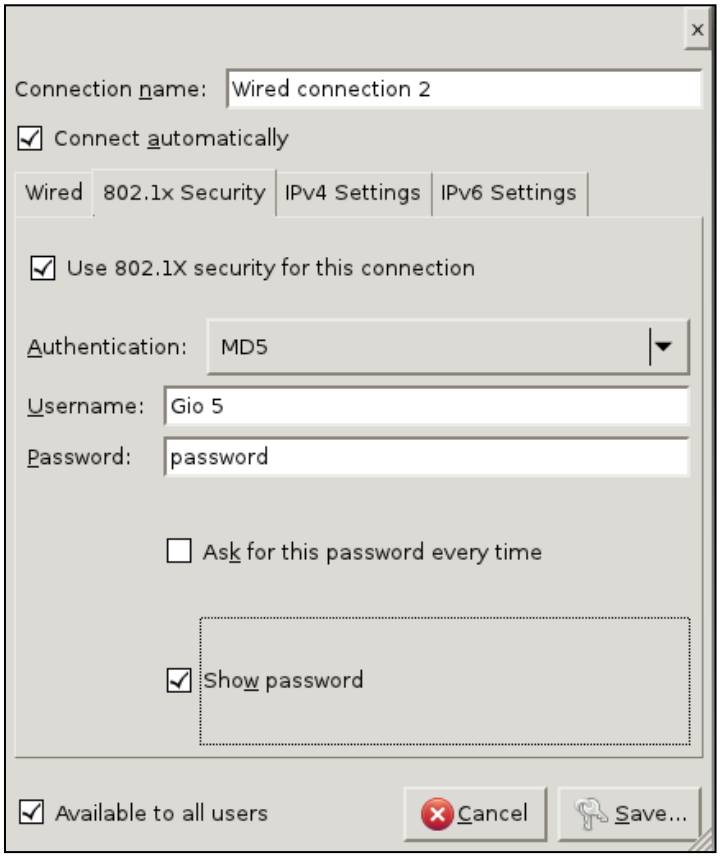

Figure 3-4 : Sécurité de la connexion câblée

4. Dans la liste déroulante **Authentification,** sélectionnez et configurez l'une des options d'authentification suivantes :

   L'option de sécurité par défaut est **MD5**. Si vous préférez l'option d'authentification MD5, effectuez les étapes suivantes.

   Remarque : L'algorithme de résumé de message 5 (MD5) est une fonction de hachage sécurisé.
   Activez cette option pour crypter toutes les communications du réseau en utilisant la fonction MD5. Pour activer cette option :

   a. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

   b. Dans le champ **Mot de passe**, saisissez un mot de passe.

c. Cliquez sur **Enregistrer**.

Remarque : Sélectionnez **Demander ce mot de passe à chaque fois** pour activer l'authentification chaque fois que vous utilisez cette connexion. Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair.

Si vous préférez l'option d'authentification **TLS**, effectuez les étapes suivantes.

Remarque *:* Transport Layer Security (TLS) est un protocole cryptographique pour crypter la communication réseau.

a. Dans le champ **Authentification**, sélectionnez **TLS**.

b. Dans le champ **Identité**, saisissez l'identité du client. *Par exemple, JohnDoeThinClient.*

Remarque *:* L'identité du client peut être un nom en caractères. L'identité du client est utilisée pour autoriser la communication entre le serveur et le client.

c. Sélectionnez un certificat d'utilisateur en cliquant sur le bouton Parcourir à côté du **Certificat de l'utilisateur**.

d. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

e. Sélectionnez une clé privée en cliquant sur le bouton Parcourir à côté de la **Clé privée**.

f. Dans le champ **Mot de passe de la clé privée**, entrez un mot de passe de la clé privée de votre choix.

Remarque : Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair. N'oubliez pas le mot de passe de la clé privée pour une utilisation future.

Si vous préférez l'option d'authentification **Tunneled TLS**, effectuez les étapes suivantes.

Remarque : Tunneled Transport Layer Security (TLS) est un protocole d'autorisation multi-facteur qui contribue à sécuriser votre communication réseau. Pour activer cette option :

a. Dans le champ **Authentification**, sélectionnez **Tunneled TLS**.

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Dans le champ **Certificat CA**, recherchez et sélectionnez un certificat CA .

d. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Note Une méthode d'authentification interne est la méthode d'authentification utilisée pour l'authentification tunneling. Vous pouvez choisir **PAP**, **MSCHAP**, **MSCHAPv2** ou **CHAP**.

e. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

f. Dans le champ **Mot de passe**, saisissez un mot de passe.

Si vous préférez l'option d'authentification **Protected EAP (PEAP)**, effectuez les étapes suivantes.

Remarque : PEAP (Protocole extensibles d'authentification protégé) est un protocole de chiffrement qui propose un chiffrement avancé pour la communication réseau. Pour activer cette option :

a. Dans le champ **Authentification**, sélectionnez **Protected EAP (PEAP)**.

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Dans le champ **Certificat CA**, recherchez et sélectionnez un certificat CA .

d. Dans la liste déroulante de la **Version PEAP** sélectionnez une version PEAP, sélectionnez **Automatique** pour sélectionner la version PEAP automatiquement.

e. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Remarque : Une méthode d'authentification interne est utilisée pour l'authentification tunneling. Vous pouvez choisir **GTC**, **MD5, MSCHAPv2**.

f. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

g. Dans le champ **Mot de passe**, saisissez un mot de passe.

5. Cliquez sur **Enregistrer**.

Remarque : Sélectionnez **Demander ce mot de passe à chaque fois** pour activer l'authentification chaque fois que vous utilisez cette connexion. Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair.

Configurer les paramètres IPv4

Internet Protocol version 4 est une norme de réseau pour transmettre des informations via un réseau. Saisissez une adresse IP appropriée, les informations du masque de réseau et de la passerelle pour assurer une configuration correcte du réseau.

Si vous préférez l'option d'authentification

1. Cliquez sur l'**Onglet IPV4** dans la fenêtre connexions réseau.

Remarque : Par défaut, la **méthode** est définie sur **Automatique (DHCP)**, cliquez sur **Enregistrer** pour configurer automatiquement le réseau.

2. Dans le champ **Méthode**, sélectionnez **Adresses automatiques (DHCP) uniquement** .
3. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
4. Dans le champ **Recherche de domaines**, saisissez un nom de domaine. *Par exemple, vxl.net.*

5. Dans le champ **ID client DHCP,** saisissez un ID client DHCP.
6. Cliquez sur **Enregistrer**.

Pour une configuration manuelle :

1. Dans la liste déroulante **méthode**, sélectionnez **Manuel**.

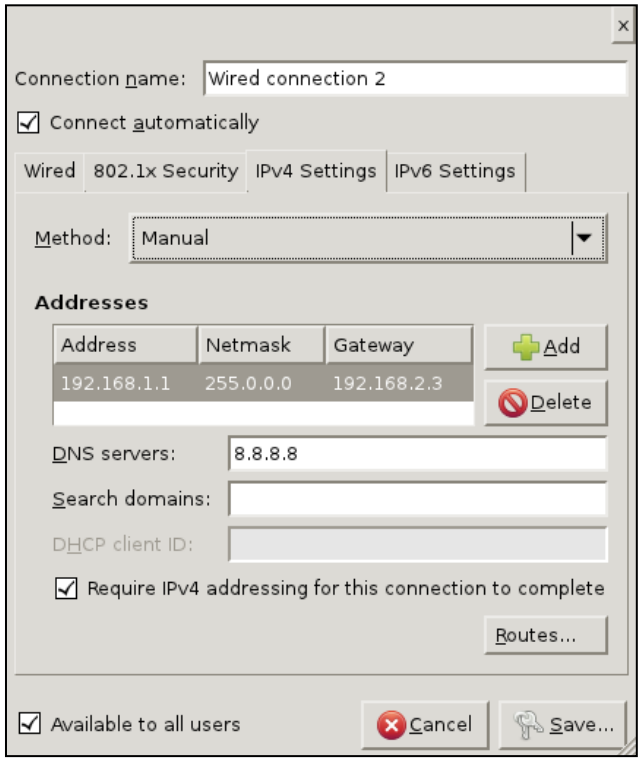

Figure 3-5 : Configuration de la connexion câblée IPv4

2. Cliquez sur **Ajouter**.
3. Dans les champs **Adresse IP**, **Masque réseau** et **Passerelle**, saisissez l'adresse IP, le masque et l'adresse de passerelle du client léger .
4. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
5. Dans le champ **Recherche de domaines**, saisissez un nom de domaine. *Par exemple, vxl.net.*

Remarque : Sélectionnez l'option **L'adressage IPv4 exigé pour cette connexion pour terminer** pour utiliser uniquement les paramètres IPv4 pour votre connexion. Si vous ne sélectionnez pas cette option, les paramètres IPv6 sont utilisés lorsque vous ne fournissez pas les paramètres ipv4.

6. Cliquez sur **Itinéraires** pour gérer les itinéraires IP.

Remarque : Si vous n'ajoutez pas d'itinéraire, un itinéraire par défaut sera attribué pour une communication réseau.

7. Cliquez sur **Ajouter** pour entrer un itinéraire.

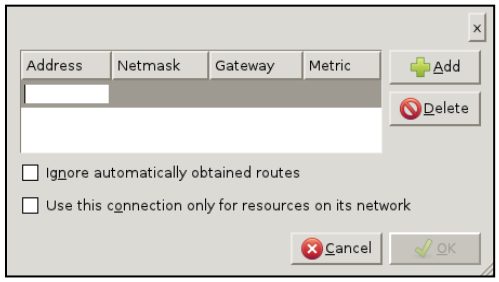

Figure 3-6 : Itinéraire IPv4 pour connexion câblée

8. Entrez l'**adresse IP, le Masque réseau et l'adresse de la Passerelle** pour les itinéraires.

   Remarque :

   - Sélectionnez **Ignorer les itinéraires obtenus automatiquement** pour utiliser les itinéraires que vous avez entré et ignorer les itinéraires qui sont obtenus à partir du routeur.
   - Sélectionnez l'option **Utiliser cette connexion uniquement pour les ressources sur son réseau** pour acheminer de manière sélective le trafic réseau via cette connexion. Si vous sélectionnez cette option, vous ne pourrez jamais utiliser cette connexion en tant que connexion par défaut.

9. Cliquez sur **Enregistrer**.

Configurer les paramètres IPv6

Internet Protocol version 6 est la version la plus récente de la suite de protocoles Internet. Pour configurer les paramètres IPv6 :

1. Cliquez sur l'**Onglet IPV6** dans la fenêtre connexions réseau.

   Remarque : Par défaut, la **méthode** est définie sur **Automatique**, cliquez sur **Enregistrer** pour configurer automatiquement le réseau.

2. Dans le champ **Méthode**, sélectionnez **Adresses automatiques uniquement**.
3. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
4. Dans le champ **Recherche de domaines**, saisissez un nom de domaine. *Par exemple, vxl.net.*
5. Cliquez sur **Enregistrer**.

   Remarque : Sélectionnez **Automatique, DHCP uniquement** pour configurer automatiquement votre réseau via DHCP.

Pour une configuration manuelle :

1. Dans la liste déroulante **méthode**, sélectionnez **Manuel**.

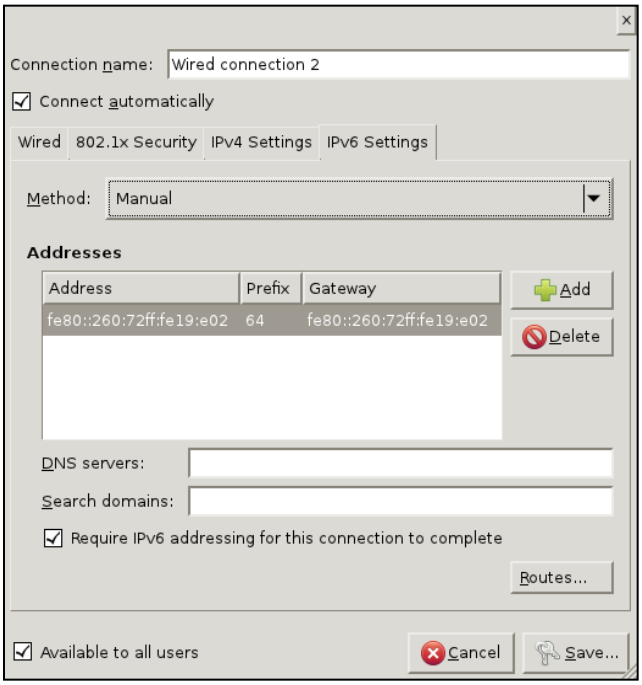

Figure 3-7 : Configuration de la connexion câblée IPv6

2. Cliquez sur **Ajouter**.
3. Dans les champs **Adresse**, **Préfixe** et **Passerelle**, saisissez l'adresse IP, le préfixe et l'adresse de passerelle du client léger.
4. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
5. Dans le champ **Recherche de domaines**, saisissez un nom de domaine.

   Remarque : Sélectionnez l'option **L'adressage IPv6 exigé pour cette connexion pour terminer** pour utiliser uniquement les paramètres IPv4 pour votre connexion. Si vous ne sélectionnez pas cette option, les paramètres IPv4 sont utilisés lorsque vous ne fournissez pas les paramètres IPv6.
6. Cliquez sur **Itinéraires** pour gérer les itinéraires IP.

   Remarque : Si vous n'ajoutez pas d'itinéraire, le routeur va attribuer un itinéraire par défaut pour la communication réseau.
7. Cliquez sur **Ajouter** pour entrer un itinéraire.

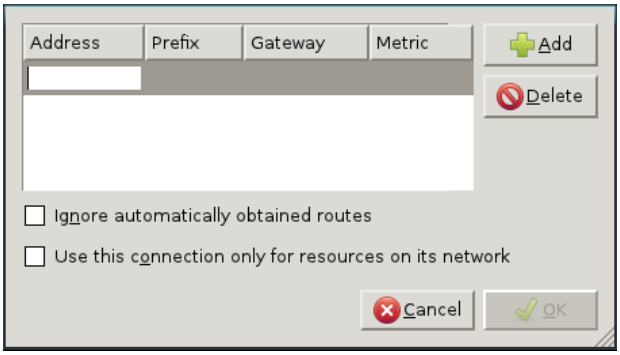

Figure 3-8 : Itinéraire IPv6 pour connexion câblée

8. Entrez l'adresse IP, le préfixe, la passerelle et le métrique pour les itinéraires.

Remarque :

- Sélectionnez **Ignorer les itinéraires obtenus automatiquement** pour utiliser les itinéraires que vous avez entré et ignorer les itinéraires qui sont obtenus à partir du routeur.
- Sélectionnez l'option **Utiliser cette connexion uniquement pour les ressources sur son réseau** pour acheminer de manière sélective le trafic réseau via cette connexion. Si vous sélectionnez cette option, vous ne pourrez pas utiliser cette connexion en tant que connexion par défaut.

9. Cliquez sur **Enregistrer**.

Supprimer une connexion câblée

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez supprimer.
2. Cliquez sur **Supprimer,** la connexion câblée est supprimée.

Connexion sans fil

Remarque : L'option de réseau sans fil n'est pas encore fonctionnelle dans le système d'exploitation série K pour Gio 5.

Une connexion sans fil est établie en connectant votre client à un réseau en utilisant des signaux de fréquences radio (FR). Le client est connecté au réseau via une carte réseau sans fil vers une passerelle, un point d'accès ou un routeur sans fil. Dans la connexion de l'**Infrastructure**, votre client est connecté à un routeur ou un point d'accès. Dans la **connexion Ad-hoc,** votre client est connecté à un autre client au sein d'un même sous-réseau.

Création d'une connexion sans fil

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Sans fil**.
2. Cliquez sur **Ajouter**.

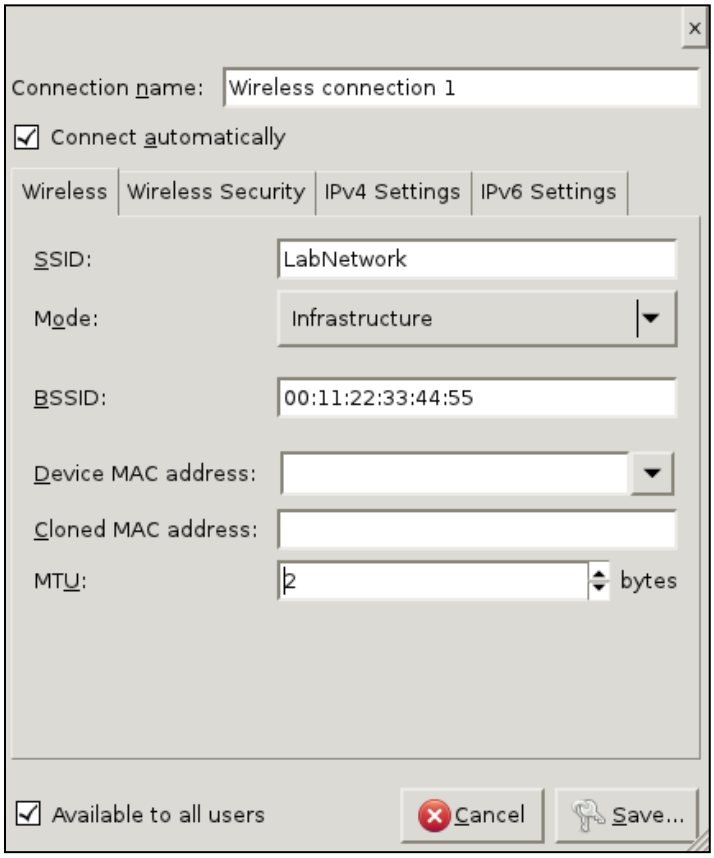

Figure 3-9 : Connexion sans fil

3. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
4. Dans le champ **SSID**, saisissez un SSID valide.

   Remarque : L'identificateur SSID (Service Set Identifier)est le nom donné à un routeur que vous voulez connecter à; par défaut, c'est le nom du fabricant du routeur sans fil.

5. Dans la liste déroulante **Mode**, sélectionnez le mode de connexion.

   Si le mode de connexion est **Infrastructure**, effectuez les opérations suivantes :

a. Dans le champ **BSSID**, saisissez un BSSID valide.

Remarque : L'identificateur BSSID (Basic Service Set Identifier)est l'adresse MAC du point d'accès auquel vous souhaitez vous connecter, vous pouvez trouver cette information sur le point d'accès des options de configuration matérielle.

b. Dans liste déroulante de l'**adresse MAC du périphérique**, sélectionnez l'adresse MAC du périphérique appropriée.

c. Dans le champ **Adresse MAC clonée**, entrez votre adresse MAC clonée.

Remarque : L'adresse MAC clonée doit être dans le bon format d'adresse MAC. Vous ne pouvez pas utiliser la même adresse MAC clonée pour plus d'un client/périphérique sur votre réseau. Vous pouvez cloner l'adresse MAC de votre routeur uniquement si votre routeur prend en charge cette fonctionnalité.

d. Dans la zone de sélection numérique de la **MTU** configurez une valeur MTU (Unité de transmission maximale).

e. Cochez la case **Disponible pour tous les utilisateurs** pour permettre à d'autres utilisateurs de se connecter à ce réseau.

f. Cliquez sur **Enregistrer**.

Si le mode de connexion est **Ad-hoc**, effectuez les opérations suivantes :

a. Dans la liste déroulante **Bande**, sélectionnez la bande de fonctionnement.

b. Dans la liste déroulante **Canal**, sélectionnez le canal de fonctionnement.

c. Dans le champ **BSSID**, saisissez un BSSID valide.

Remarque : L'identificateur BSSID (Basic Service Set Identifier) est l'adresse MAC du point d'accès auquel vous souhaitez vous connecter, vous pouvez trouver cette information sur le point d'accès des options de configuration matérielle.

d. Dans liste déroulante de l'**adresse MAC du périphérique**, sélectionnez l'adresse MAC du périphérique appropriée.

e. Dans le champ de **l'adresse MAC clonée**, entrez votre adresse MAC clonée.

Remarque : L'adresse MAC clonée doit être dans le bon format d'adresse MAC. Vous ne pouvez pas utiliser la même adresse MAC clonée pour plus d'un client/périphérique sur votre réseau. Vous pouvez cloner l'adresse MAC de votre routeur uniquement si votre routeur prend en charge cette fonctionnalité.

f. Dans la zone de sélection numérique de la MTU configurez une valeur MTU (Unité de transmission maximale).

g. Cochez la case **Disponible pour tous les utilisateurs** pour permettre à d'autres utilisateurs de se connecter à ce réseau.

h. Cliquez sur **Enregistrer**.

Configurer la sécurité de la connexion sans fil

Vous pouvez sélectionner l'une des méthodes de cryptage suivantes :

- **Clé WEP 40/128-bit (Hex ou ASCII**) : Une clé WEP 40-bit est une clé de 10 chiffres (Hex ou ASCII) qui peut contenir des chiffres 0-9 et les lettres A-Z. Une clé WEP 128-bit est une clé de 26 chiffres qui peut contenir des chiffres 0-9 et lettres de A à Z
- **Phrase de sécurité WEP 128-bit** : Une phrase de sécurité WEP 128 bit est un texte de longueur personnalisée qui peut être utilisé comme une clé.
- **LEAP (Lightweight Extensible Authentication Protocol**) : Également connu sous le nom de Cisco-Wireless EAP; il fournit une authentification basée sur un nom d'utilisateur/mot de passe, entre un client sans fil et un serveur RADIUS comme le Cisco ACS ou Interlink AAA.

  Remarque : La sécurité LEAP est actuellement non opérationnelle.
- **Dynamic WEP (802.1 xs) :** Dynamic WEP fait référence à la combinaison de la technologie 802.1x et le protocole d'authentification extensible (EAP). Dynamic WEP change les clés WEP de façon dynamique.
- **WPA & WPA2 Personal :** WPA et WPA2 Personal est une clé de cryptage alphanumérique qui peut contenir des chiffres de 0 à 9 et des lettres de A à Z.
- **WPA & WPA2 Enterprise :** WPA Enterprise utilise l'authentification 802.1x par le biais d'un serveur RADIUS. Cela fournit au compte utilisateur une authentification basée sur des certificats, et il est recommandé pour la sécurité des entreprises et d'autres grands réseaux sans fil.

Figure 3-10 : Sécurité sans fil

Pour configurer la clé WEP 40/128 bits ou la phrase de sécurité WEP 128 bits :

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Sécurité sans fil**.
2. Dans la liste déroulante **Sécurité**, sélectionnez clé **WEP 40/128 bits** ou **phrase de sécurité WEP 128-bit**.

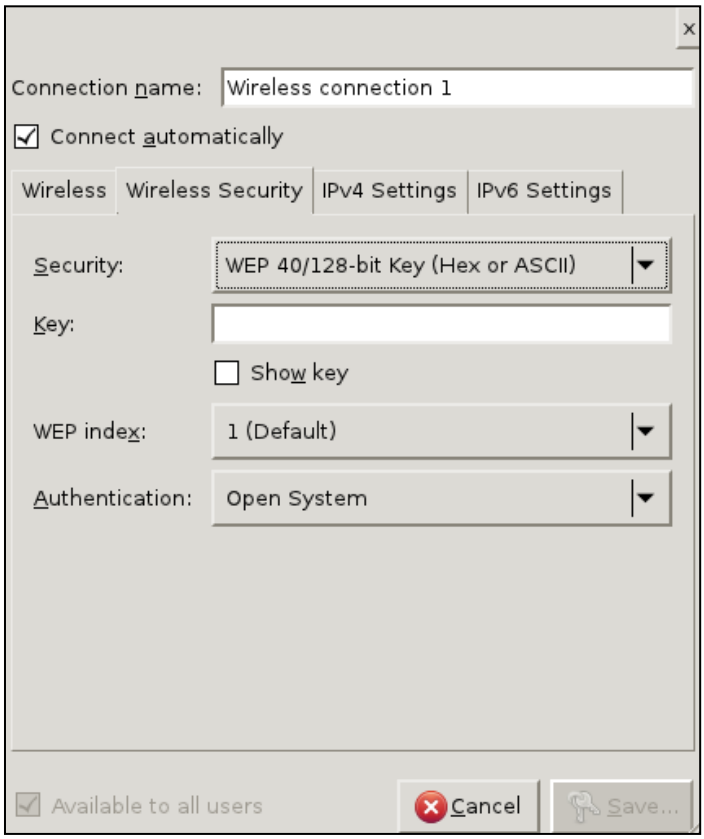

Figure 3-11 : Clé WEP 40/128-bit

Remarque : Sélectionnez **Aucun** pour une transmission non-cryptée.

3. Dans le champ Clé, saisissez une clé ou une phrase de sécurité valide.

Remarque :

- Les clés de cryptage doivent être générées dans le point d'accès du réseau sans fil ou du routeur, les clés générées doivent être utilisées ici pour la configuration du réseau.
- La méthode de cryptage WPA & WPA2 est disponible dans le mode de connexion de l'**Infrastructure** uniquement.

4. Sélectionnez **Afficher clé** pour rendre la clé de cryptage visible.
5. Dans le champ **WEP Index** sélectionnez une valeur de 1 à 4.
6. Dans **Authentification** sélectionnez Système ouvert ou Clé partagée.

Remarque : Sélectionnez **Aucun** pour une transmission non-cryptée.

7. Cliquez sur **Enregistrer**.

Pour configurer la sécurité LEAP :

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Sécurité sans fil**.
2. Dans la liste déroulante **Sécurité**, sélectionnez **LEAP**.

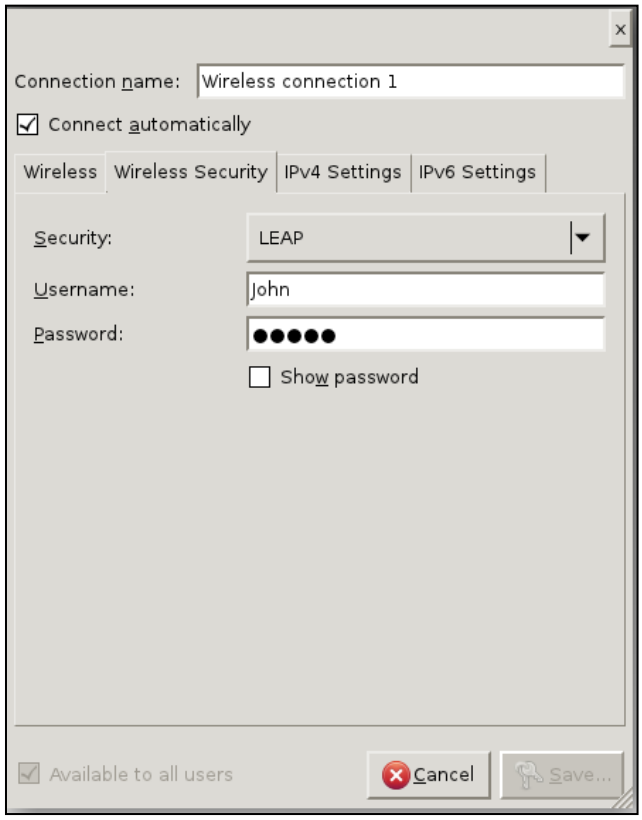

Figure 3-12 : Sécurité LEAP

3. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
4. Dans le champ **Mot de passe**, saisissez un mot de passe.
5. Cliquez sur **Enregistrer**.

Remarque : La sécurité LEAP est actuellement non opérationnelle.

Pour configurer Dynamic WEP (802.1x) :

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Sécurité sans fil**.
2. Dans la liste déroulante **Sécurité**, sélectionnez **Dynamic WEP (802.1x)**.

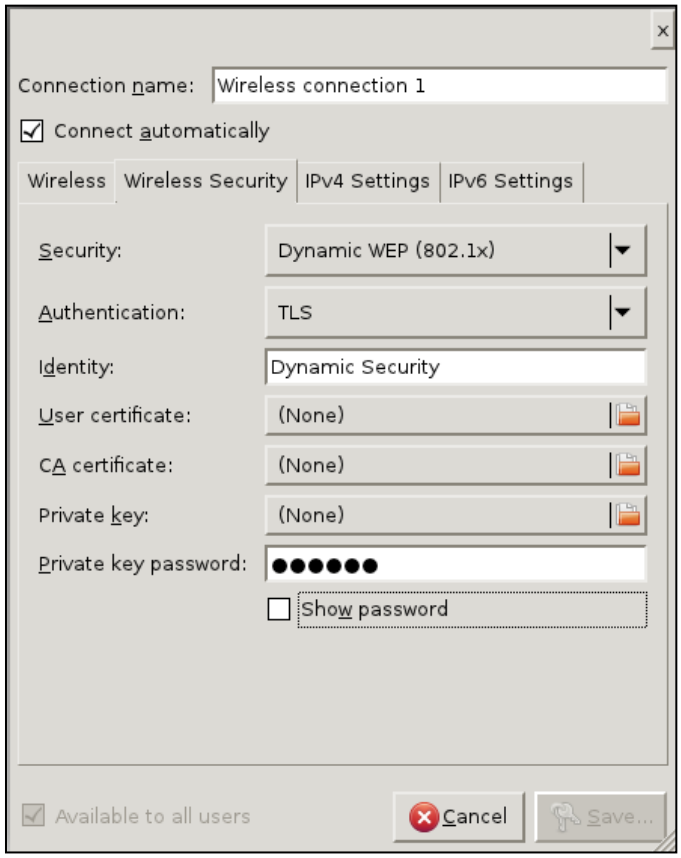

Figure 3-13 : Dynamic WEP (802.1x)

Si vous préférez l'option d'authentification **TLS**, effectuez les étapes suivantes.

Remarque : Transport Layer Security (TLS) est un protocole cryptographique pour crypter la communication réseau.

a. Dans le champ **Authentification**, sélectionnez **TLS**.

b. Dans le champ **Identité**, saisissez l'identité du client. *Par exemple, JohnDoeThinClient.*

   Remarque : L'identité du client peut être un nom en caractères. L'identité du client est utilisée pour autoriser la communication entre le serveur et le client.

c. Sélectionnez un certificat d'utilisateur en cliquant sur le bouton Parcourir à côté du **Certificat de l'utilisateur**.

d. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

e. Sélectionnez une clé privée en cliquant sur le bouton Parcourir à côté de la **Clé privée**.

f. Dans le champ **Mot de passe de la clé privée**, entrez un mot de passe de la clé privée de votre choix.

Remarque : Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair. N'oubliez pas le mot de passe de la clé privée pour une utilisation future.

Si vous préférez l'option d'authentification **LEAP** :

a. Dans la liste déroulante **Authentification**, sélectionnez **LEAP**.

b. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

c. Dans le champ **Mot de passe**, saisissez un mot de passe.

Si vous préférez l'option d'authentification **Tunneled TLS**, effectuez les étapes suivantes.

Remarque : Tunneled Transport Layer Security (TLS) est un protocole d'autorisation multi-facteur qui contribue à sécuriser votre communication réseau. Pour activer cette option :

a. Dans le champ **Authentification**, sélectionnez Tunneled **TLS**.

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

d. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Note Une méthode d'authentification interne est la méthode d'authentification utilisée pour l'authentification tunneling. Vous pouvez choisir **PAP**, **MSCHAP**, **MSCHAPv2** ou **CHAP**.

e. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

f. Dans le champ **Mot de passe**, saisissez un mot de passe.

Si vous préférez l'option d'authentification **Protected EAP (PEAP)**, effectuez les étapes suivantes.

Remarque : PEAP (Protocole extensibles d'authentification protégé) est un protocole de chiffrement qui propose un chiffrement avancé pour la communication réseau. Pour activer cette option :

a. Dans le champ **Authentification**, sélectionnez **Protected EAP (PEAP)**.

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

d. Dans la liste déroulante de la **Version PEAP** sélectionnez une version PEAP, sélectionnez **Automatique** pour sélectionner la version PEAP automatiquement.

e. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Remarque : Une méthode d'authentification interne est la méthode d'authentification utilisée pour l'authentification tunneling. Vous pouvez choisir **MD5, GTC** ou **MSCHAPv2** .

f. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

g. Dans le champ **Mot de passe**, saisissez un mot de passe.

3. Cliquez sur **Enregistrer**.

Pour configurer la sécurité WPA & WPA 2 Personal :

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **Sécurité sans fil**.
2. Dans la liste déroulante **Sécurité**, sélectionnez **WPA & WPA2 Personal**.

Figure 3-14 : WPA & WPA2 Personal

3. Dans le champ **Mot de passe**, saisissez un mot de passe.
4. Cliquez sur **Enregistrer**.

Pour configurer WPA & WPA2 Enterprise :

1. Dans la liste déroulante **Sécurité**, sélectionnez **WPA & WPA2 Enterprise**.

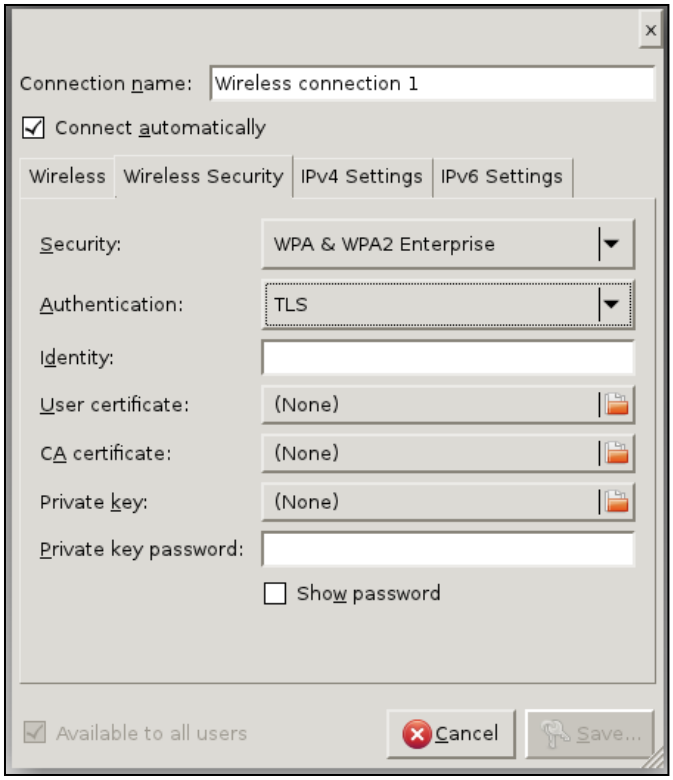

Figure 3-15 : WPA & WPA2 Entreprise

Si vous préférez l'option d'authentification **TLS**, effectuez les étapes suivantes.

Remarque : Transport Layer Security (TLS) est un protocole cryptographique pour crypter la communication réseau.

a. Dans le champ **Authentification**, sélectionnez **TLS**.

b. Dans le champ **Identité**, saisissez l'identité du client. *Par exemple, JohnDoeThinClient.*

   Remarque : L'identité du client peut être un nom en caractères. L'identité du client est utilisée pour autoriser la communication entre le serveur et le client.

c. Sélectionnez un certificat d'utilisateur en cliquant sur le bouton Parcourir à côté du **Certificat de l'utilisateur**.

d. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

e. Sélectionnez une clé privée en cliquant sur le bouton Parcourir à côté de la **Clé privée**.

f. Dans le champ **Mot de passe de la clé privée**, entrez un mot de passe de la clé privée de votre choix.

Remarque : Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair. N'oubliez pas le mot de passe de la clé privée pour une utilisation future.

Si vous préférez l'option d'authentification **LEAP**.

a. Dans la liste déroulante **Authentification**, sélectionnez LEAP.

b. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

c. Dans le champ **Mot de passe**, saisissez un mot de passe.

Si vous préférez l'option d'authentification **Tunneled TLS**, effectuez les étapes suivantes.

Remarque : Tunneled Transport Layer Security (TLS) est un protocole d'autorisation multi-facteur qui contribue à sécuriser votre communication réseau. Pour activer cette option :

a. Dans le champ **Authentification**, sélectionnez **Tunneled TLS**

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

d. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Note Une méthode d'authentification interne est la méthode d'authentification utilisée pour l'authentification tunneling. Vous pouvez choisir **PAP**, **MSCHAP**, **MSCHAPv2** ou **CHAP**.

e. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

f. Dans le champ **Mot de passe**, saisissez un mot de passe.

Si vous préférez l'option d'authentification **Protected EAP (PEAP)**, effectuez les étapes suivantes.

Remarque : PEAP (Protocole extensibles d'authentification protégé) est un protocole de chiffrement qui propose un chiffrement avancé pour la communication réseau. Pour activer cette option :

a. Dans le champ Authentification, sélectionnez **Protected EAP (PEAP)**.

b. Dans le champ **Identité anonyme**, saisissez une identité de client anonyme.

Remarque : L'identité anonyme est révélée uniquement au serveur d'authentification.

c. Sélectionnez un certificat CA en cliquant sur le bouton Parcourir à côté du **Certificat CA**.

d. Dans la liste déroulante de la **Version PEAP** sélectionnez une version PEAP, sélectionnez **Automatique** pour sélectionner la version PEAP automatiquement.

e. Dans la liste déroulante de l'**Authentification interne**, sélectionnez une méthode d'authentification interne.

Remarque : Une méthode d'authentification interne est la méthode d'authentification utilisée pour l'authentification tunneling. Vous pouvez choisir **MD5, GTC** ou **MSCHAPv2**.

f. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.

g. Dans le champ **Mot de passe**, saisissez un mot de passe.

2. Cliquez sur **Enregistrer**.

Configurer les paramètres IPv4

Internet Protocol version 4 est une norme de réseau pour transmettre des informations via un réseau. Saisissez une adresse IP appropriée, les informations du masque de réseau et de la passerelle pour assurer une configuration correcte du réseau.

Pour configurer les Paramètres IPv4 :

1. Cliquez sur l'onglet **Paramètres IPV4** dans la fenêtre des connexions réseau.

Remarque : Par défaut, la **méthode** est définie sur **Automatique (DHCP)**, cliquez sur **Enregistrer** pour configurer automatiquement le réseau.

2. Dans le champ **Méthode**, sélectionnez **Adresses automatiques (DHCP) uniquement** .
3. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
4. Dans le champ **Recherche de domaines**, saisissez un nom de domaine. *Par exemple, vxl.net.*
5. Dans le champ **ID client DHCP,** saisissez un ID client DHCP.
6. Cliquez sur **Enregistrer**.

Pour une configuration manuelle :

1. Dans la liste déroulante **méthode**, sélectionnez **Manuel**.

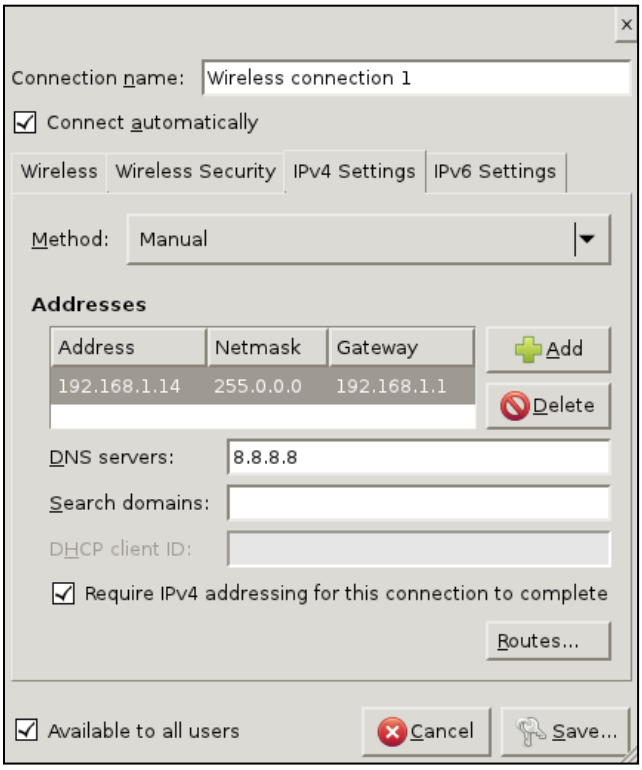

Figure 3-16 : Configuration de la connexion sans fil IPv4

2. Cliquez sur **Ajouter**.
3. Dans les champs **Adresse IP**, **Masque réseau** et **Passerelle**, saisissez l'adresse IP, le masque et l'adresse de passerelle du client léger .
4. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
5. Dans le champ **Recherche de domaines**, saisissez un nom de domaine.
6. Dans le champ **ID client DHCP,** saisissez un ID client DHCP.

   Remarque : Sélectionnez l'option **L'adressage IPv4 exigé pour cette connexion pour terminer** pour utiliser uniquement les paramètres IPv4 pour votre connexion. Si vous ne sélectionnez pas cette option, les paramètres IPv6 sont utilisés lorsque vous ne fournissez pas les paramètres ipv4.

7. Cliquez sur **Itinéraires** pour gérer les itinéraires IP.

   Remarque : Si vous n'ajoutez pas d'itinéraire, le routeur va attribuer un itinéraire par défaut pour le réseau.

8. Cliquez sur **Ajouter** pour entrer un itinéraire.

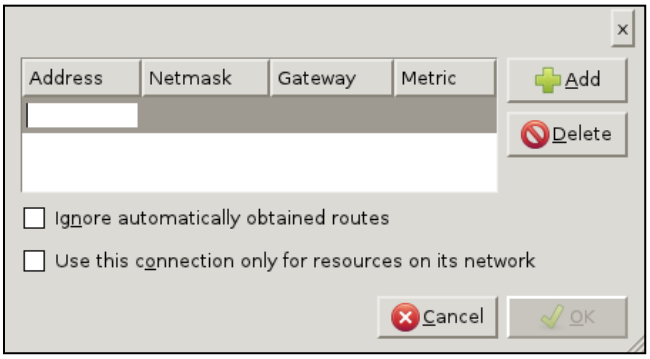

Figure 3-17 : Itinéraire IPv4 pour connexion sans fil

9. Entrez l'adresse IP, le Masque réseau et l'adresse de la Passerelle pour les itinéraires.

   Remarque :

   - Sélectionnez **Ignorer les itinéraires obtenus automatiquement** pour utiliser les itinéraires que vous avez entré et ignorer les itinéraires qui sont obtenus à partir du routeur.
   - Sélectionnez l'option **Utiliser cette connexion uniquement pour les ressources sur son réseau** pour acheminer de manière sélective le trafic réseau via cette connexion. Si vous sélectionnez cette option, vous ne pourrez pas utiliser cette connexion en tant que connexion par défaut.

10. Cliquez sur **Enregistrer**.

Configurer les paramètres IPv6

Internet Protocol version 6 est la version la plus récente de la suite de protocoles Internet. Pour configurer les paramètres IPv6 :

1. Cliquez sur l'onglet **Paramètres IPV6** dans la fenêtre des connexions réseau.

   Remarque : Par défaut, la **méthode** est définie sur **Automatique**, cliquez sur **Enregistrer** pour configurer automatiquement le réseau.

2. Dans le champ **Méthode**, sélectionnez **Adresses automatiques uniquement**.
3. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
4. Dans le champ **Recherche de domaines**, saisissez un nom de domaine. *Par exemple, vxl.net.*
5. Dans le champ **ID client DHCP,** saisissez un ID client DHCP.
6. Cliquez sur **Enregistrer**.

   Remarque : Sélectionnez **Automatique, DHCP uniquement** pour configurer automatiquement votre réseau via DHCP.

   Pour une configuration manuelle :

1. Dans la liste déroulante **méthode**, sélectionnez **Manuel**.
2. Cliquez sur **Ajouter**.
3. Dans les champs **Adresse**, **Préfixe** et **Passerelle**, saisissez l'adresse IP, le préfixe et l'adresse de passerelle du client léger.
4. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.

5. Dans le champ **Recherche de domaines**, saisissez un nom de domaine.

   Remarque : Sélectionnez l'option **L'adressage IPv6 exigé pour cette connexion pour terminer** pour utiliser uniquement les paramètres IPv4 pour votre connexion. Si vous ne sélectionnez pas cette option, les paramètres IPv4 sont utilisés lorsque vous ne fournissez pas les paramètres IPv6.

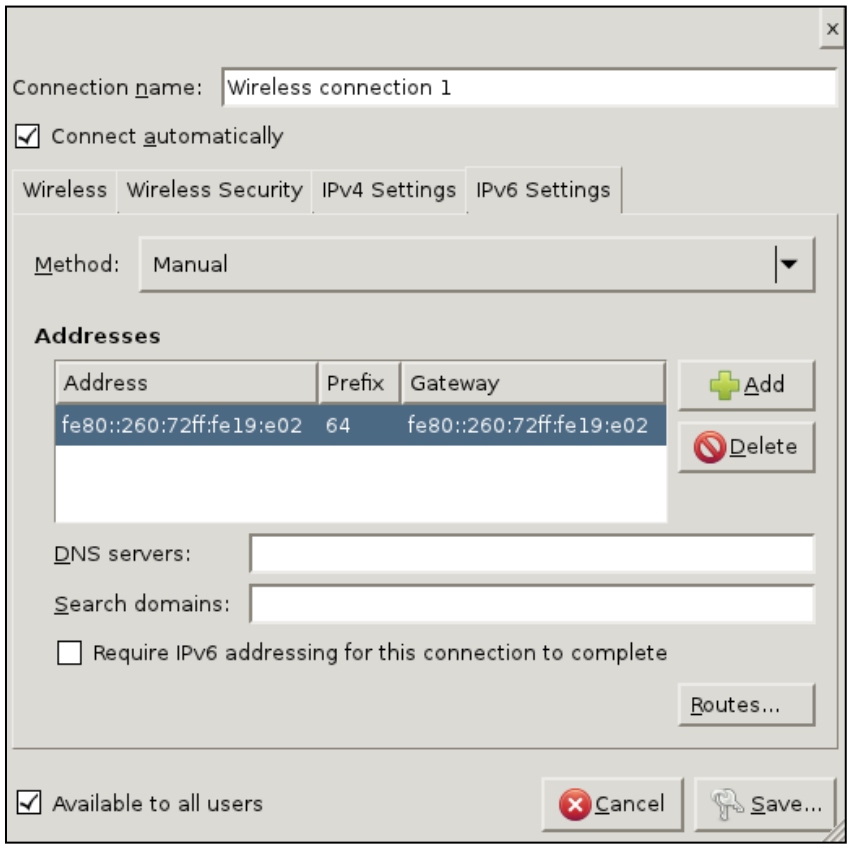

Figure 3-18 : Configuration de la connexion sans fil IPv6

6. Cliquez sur **Itinéraire** pour gérer les itinéraires IP.

   Remarque : Si vous n'ajoutez pas d'itinéraire, le routeur va attribuer un itinéraire par défaut pour votre réseau.

7. Cliquez sur **Ajouter** pour entrer un itinéraire.

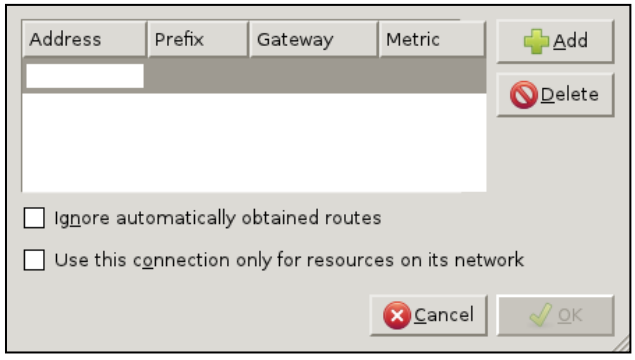

Figure 3-19 : Itinéraire IPv6 pour connexion sans fil

8. Entrez l'adresse IP, le préfixe, la passerelle et le métrique pour les itinéraires.

Remarque :

- Sélectionnez **Ignorer les itinéraires obtenus automatiquement** pour utiliser les itinéraires que vous avez entré et ignorer les itinéraires qui sont obtenus à partir du routeur.
- Sélectionnez l'option **Utiliser cette connexion uniquement pour les ressources sur son réseau** pour acheminer de manière sélective le trafic réseau via cette connexion. Si vous sélectionnez cette option, vous ne pourrez jamais utiliser cette connexion en tant que connexion par défaut.

9. Cliquez sur **Enregistrer**.

Supprimer une connexion sans fil

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez supprimer.
2. Cliquez sur **Supprimer,** la connexion sans fil est supprimée.

Connexion VPN

Une connexion VPN (réseau privé virtuel) est utilisée pour connecter votre client en toute sécurité à un réseau distant. Les connexions VPN peuvent être utilisées pour connecter en toute sécurité deux installations éloignées géographiquement en utilisant le réseau public.

Remarque : Le VPN est actuellement non opérationnel.

Création d'une connexion VPN

1. Dans la fenêtre des connexions réseau, cliquez sur l'onglet **VPN**.
2. Cliquez sur **Ajouter**.

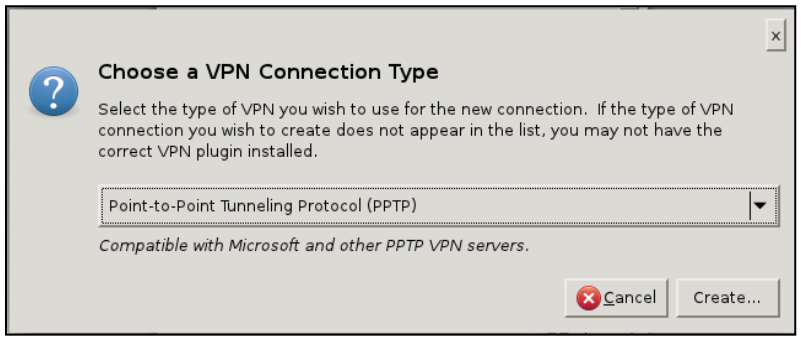

Figure 3-20 : Type de connexion VPN

3. Dans la liste déroulante **Choisir un type de connexion VPN**, sélectionnez un type de connexion VPN.
4. Cliquez sur **Créer.**
5. Dans le champ **Nom de connexion**, saisissez un nom de connexion.

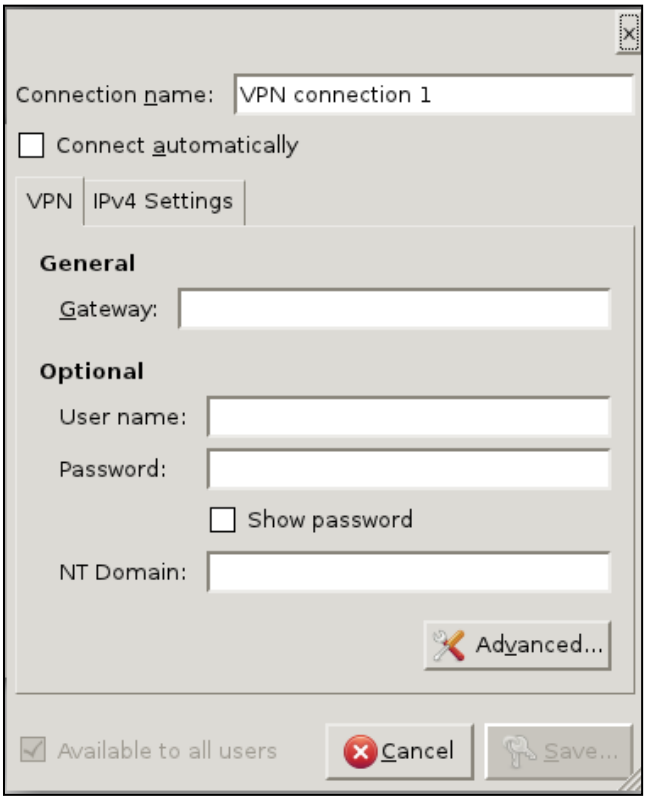

Figure 3-21 : Paramètres VPN

6. Sélectionnez **Connecter automatiquement** pour vous connecter automatiquement à ce réseau lorsque le client est redémarré.
7. Dans le champ **Passerelle**, saisissez une adresse de passerelle.

Vous pouvez sécuriser vos connexions VPN en fournissant les informations suivantes :

8. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
9. Dans le champ **Mot de passe**, saisissez un mot de passe.

   Remarque : Sélectionnez **Afficher le mot de passe** pour rendre le mot de passe que vous avez saisi visible en texte clair.

10. Dans le champ **Domaine NT**, saisissez un nom de domaine NT. Le nom de Domaine NT est votre nom de domaine du réseau.

Pour configurer les paramètres avancés VPN :

1. Cliquez sur **Avancés**, la fenêtre Options avancées PPTP s'affiche.

Authentification

2. Dans la boîte de sélection du champ **Autoriser les méthodes d'authentification suivantes**, sélectionnez les méthodes d'authentification requises.

Sécurité et compression

3. Sélectionnez **Utiliser cryptage de point à point** pour crypter la transmission des données VPN.
4. Dans la liste déroulante **Sécurité**, sélectionnez le cryptage 128-bit ou 40-bit.

Remarque : Le cryptage 128-Bit est plus sûr que le cryptage 40 bits.

5. Sélectionnez **Autoriser cryptage à états :** Cette option permet la réutilisation de l'information entre les différents algorithmes de cryptage. En sélectionnant cette option vous optimisez le processus de cryptage.
6. Sélectionnez la **Compression des données BSD:** Cette option active la compression de données en utilisant la méthode BSD de compression des données. En sélectionnant cette option vous économisez de la largeur de bande.
7. Sélectionnez **Autoriser Dégonfler la compression des données :** Cette option active l'algorithme pour dégonfler la compression de données. En sélectionnant cette option vous compressez les données transmises via le réseau privé virtuel (VPN).
8. Sélectionnez **Utiliser la compression d'en-tête TCP** : Cette option active la compression d'en-têtes TCP ; elle améliore les performances des liens de série lente par la compression d'en-têtes TCP.

Écho

9. Cochez la case **Envoyer paquets écho PPP** si vous voulez vérifier la présence (ou l'absence) du modem.
10. Cliquez sur **Enregistrer**.

Configurer la connexion VPN

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez configurer.
2. Cliquez sur **Éditer.**
3. Cliquez sur **Paramètres IPv4**.
4. Dans la liste déroulante **Méthode**, **Automatique (VPN**) est l'option par défaut**.** Cliquez sur **Enregistrer** pour configurer la connexion.

Pour fournir une adresse DNS personnalisée :

1. Dans le champ **Méthode**, sélectionnez **Adresses automatiques (VPN) uniquement** .
2. Dans le champ **Serveurs DNS**, saisissez une adresse de serveur DNS.
3. Dans le champ **Recherche de domaines**, saisissez un nom de domaine.
4. Cliquez sur **Itinéraires** pour gérer les itinéraires IP.
5. Cliquez sur **Ajouter** pour entrer un itinéraire.

   Remarque :

   - Sélectionnez **Ignorer les itinéraires obtenus automatiquement** pour utiliser les itinéraires que vous avez entré et ignorer les itinéraires qui sont obtenus à partir du routeur.
   - Sélectionnez l'option **Utiliser cette connexion uniquement pour les ressources sur son réseau** pour acheminer de manière sélective le trafic réseau via cette connexion. Si vous sélectionnez cette option, vous ne pourrez jamais utiliser cette connexion en tant que connexion par défaut.

6. Cliquez sur **Enregistrer**.

Exporter les paramètres VPN

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez exporter.
2. Cliquez sur Exporter.
3. Dans le champ **Nom**, saisissez un nom approprié.
4. Sélectionnez l'emplacement où vous souhaitez enregistrer les paramètres VPN.
5. Cliquez sur **Enregistrer**.

Importer les paramètres VPN

1. Cliquez sur l'onglet **VPN**.
2. Cliquez sur **Importer**.
3. Sélectionnez le fichier **.conf** à importer.
4. Cliquez sur **Ouvrir.** Le fichier de configuration sera importé avec les paramètres.

Supprimer une connexion VPN

1. Dans la liste des **Profils**, sélectionnez la connexion que vous souhaitez supprimer.
2. Cliquez sur **Supprimer,** la connexion VPN est supprimée.

Gestionnaire de connexion

Gio 5 fournit plusieurs options pour connecter votre client à un serveur. Les options de connectivité fournies sont les suivantes :

- 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

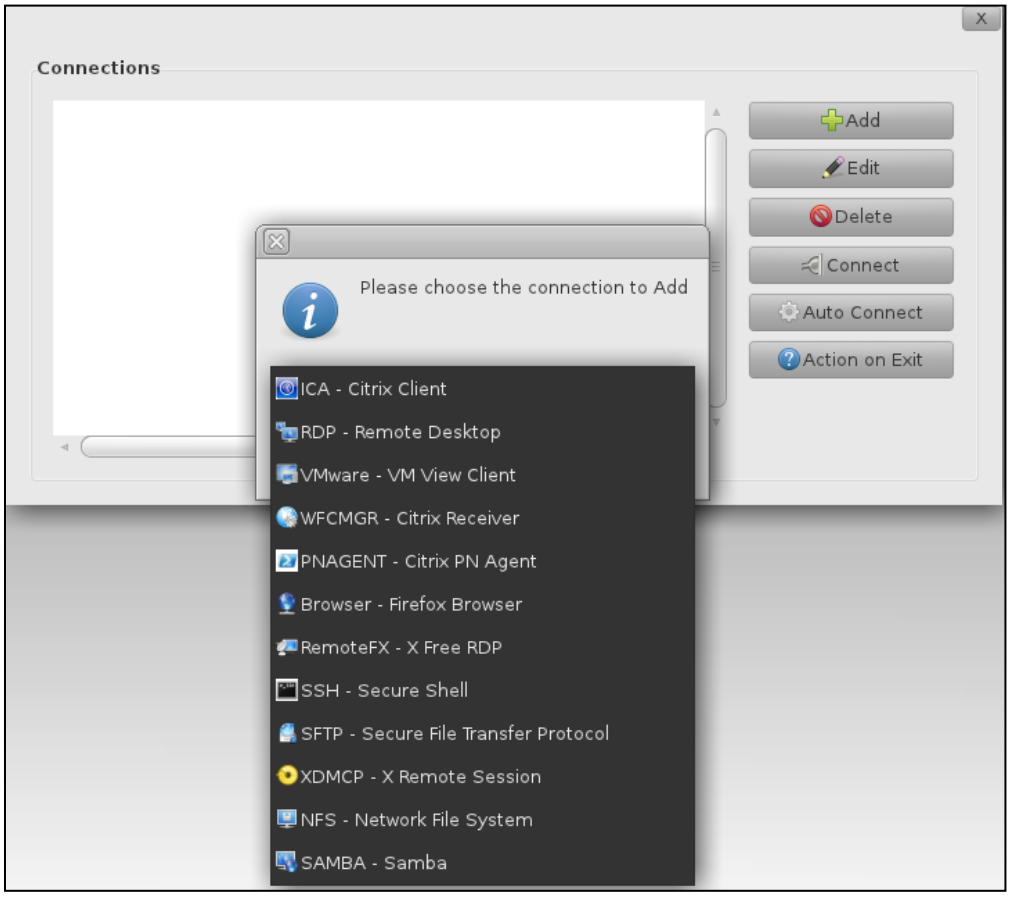

Figure 3-22 : Options de connexion

Options de connexion

Vous pouvez configurer votre connexion en sélectionnant les options qui ajoutent une fonctionnalité de connexion.

Voici une liste des options de connexion disponibles avec leur information ; les options offertes peuvent varier en fonction de la connexion :

- Mapper les imprimantes locales : Cette option associe votre imprimante locale au serveur du terminal. Vous devez déjà avoir créé et configuré une imprimante locale pour activer cette option. Pour plus d'informations sur l'ajout d'une imprimante, consulter la section 'Imprimante' à la page72.
- Vitesse de l'écran BA : Cette option permet l'Accélération de la vitesse de navigation dur l'écran, cette fonction permet d'afficher les images plus vite et rendre la navigation web plus fluide.

  Remarque : L' accélération de la vitesse de l'écran ne fonctionne pas lorsque le contenu *Adobe Flash* est activé. Si vous souhaitez utiliser cette fonctionnalité, vous devez désactiver *Adobe Flash* .
- Vitesse de l'écran : Cette option active la réduction du temps de latence de la vitesse de l'écran ; cette option est utile lorsque vous utilisez une connexion lente avec un temps de latence de plus de 100 ms.
- Activer l'entrée audio : Cette option active l'entrée audio de votre client léger.
- Utiliser la compression ICA : Cette option active la compression du flux de données ICA transmises sur un réseau.
- Plein écran : Cette option active le mode plein écran pour votre connexion ; votre bureau à distance sera affiché en plein écran.
- Mapper les ports série Cette option associe les ports série du serveur du terminal aux ports série de votre client léger, en sélectionnant cette option vous redirigez les ports série des périphériques connectés à votre client vers le serveur du terminal.
- Mapper les lecteurs de carte à puce locaux : Cette option associe vos lecteurs de carte à puce locaux au lecteur de carte à puce du serveur du terminal.
- Activer rendre utilisable OSS : Cette option active la fonctionnalité surface off-screen (OSS) qui permet au de client ICA de dessiner les mises à jour d'écran dans une mémoire bitmap plutôt que sur l'écran. Cette option améliore l'efficacité de la largeur de bande du réseau.
- Couleurs approximatives : Cette option permet d'utiliser des couleurs approximatives qui sont disponibles dans le client si les couleurs exactes ne sont pas disponibles. Cette fonction élimine le clignotement de couleur lors du changement entre les applications.
- EUKS : Cette option permet la prise en charge étendue de clavier Unicode Support (EUKS) sur le serveur Windows.
- Compression des données : Cette option active la compression des données du flux de données RDP.
- Synchronisation du verrouillage numérique : Cette option permet la synchronisation du verrouillage numérique entre votre serveur et le client léger. Utiliser la synchronisation du verrouillage numérique lorsque vous souhaitez utiliser le clavier de votre client léger pour accéder aux fonctionnalités d'une application qui en exécution sur le serveur.
- Ne pas envoyer les événements d'activité : Cette option empêche la transmission des événements d'activité tels que le mouvement du pointeur de la souris sur l'écran

vers le serveur, seules les interactions avec l'interface sont envoyées au serveur. Cette option permet d'économiser la largeur de bande.

- Imposer les mises à jour de bitmap : Cette option force le serveur à envoyer des mises à jour sur l'écran en tant que bitmaps plutôt que d'utiliser opérations de dessin de niveau supérieur. Les mises à jour de bitmaps économisent la largeur de bande.
- Lecteurs de cartes à puce locaux : Cette option associe vos lecteurs de carte à puce locaux au lecteur de carte à puce du serveur du terminal.
- Connexions de la console : Cette option vous permet de vous connecter à la console du serveur du terminal ; cette option nécessite Windows Server 2003 ou Windows Server 2008.
- Masquer les décorations WM : Cette option masque les décorations du gestionnaire de fenêtre.
- Mapper les lecteurs du client(USB:z) : Cette option associe les lecteurs du client avec les lecteurs dans le serveur du terminal.
- Conserver les raccourcis clavier WM Cette option active tous vos raccourcis du gestionnaire de fenêtre.
- Activer RemoteFX : Cette option active Microsoft RemoteFX, c'est une nouvelle fonctionnalité qui est inclue dans Windows Server 2008 R2 avec Service Pack 1 (SP1). Elle introduit un ensemble d'améliorations de l'expérience utilisateur pour RDP (Remote Desktop Protocol) qui active un environnement de bureau riche au sein du réseau de votre entreprise.
- Masquer les décorations de la fenêtre : Cette option masque les décorations de la fenêtre telles que les onglet graphiques en couleurs élevées de la fenêtre et la transparence.
- Console audio : Cette option active le port audio sur le client léger.
- Désactiver l'authentification : Cette option désactive l'authentification lorsque vous vous connectez à cette connexion. En sélectionnant cette option, vous vous connecter automatiquement au serveur sans aucune authentification.
- Désactiver les mouvements de souris Cette option désactive les mouvements du curseur de la souris. En sélectionnant cette option vous rendrez les mouvements de la souris inutiles.
- Désactiver le cache Bitmap : Cette option désactive le stockage d'images bitmap localement dans le client léger. Sélectionnez cette option si vous avez une connexion avec une largeur de bande passante adéquate pour que la connexion fonctionne sans heurts.
- Désactiver le papier peint : Cette option désactive le papier peint lorsque vous êtes connecté sur l'ordinateur distant. En sélectionnant cette option vous économisez de la largeur de bande.
- Désactiver le Full Window Drag : Cette option permet d'activer la fonction glisser-copier. Sélectionnez cette option lorsque vous ne souhaitez pas que le contenu du dossier s'affiche lorsque vous faites glisser le dossier vers un nouvel emplacement.
- Désactiver les thèmes : Sélectionnez cette option pour empêcher les utilisateurs d'appliquer des thèmes de bureau lorsqu'ils sont connectés au serveur distant.
- Désactiver le cryptage TLS Cette option désactive le cryptage Transport Layer Security pour cette connexion.
- Vérification du certificat : Cette option permet à la connexion de vérifier la présence d'un certificat valide avant d'établir la connexion au serveur distant.

- Se connecter à la session de la console Cette option démarre une session de la console non-graphique. Sélectionnez cette option pour accéder à la console de commande du serveur.
- Désactiver Checksum avec une connexion RDP Std : Cette option désactive la validation du contrôle du flux de données RDP.
- Définir la configuration du clavier Cette option définit les paramètres la configuration du clavier de celui qui est actuellement utilisé par le client léger.
- Activer la compression : Cette option active la compression du flux de données de la connexion.
- Désactiver le chemin rapide : Cette option désactive le chemin rapide. Le chemin rapide permet généralement aux tâches d'être exécutées plus rapidement en optimisant ces processus.
- Désactiver le bitmap Offscreen Cette option désactive le bitmap Offscreen. Cette option empêche le serveur de modifier le rendu de surface par défaut du client vers l'un des bitmaps créés dans Offscreen Bitmap Cache.
- Activer NSCode : Cette option active la compression bitmap NSCodec ; cette option est utilisée lorsque la profondeur de couleur de la session RDP est de 32 bpp et le bitmap d'intérêt est 24 bpp (RVB sans canal alpha) ou 32 bpp (RVB avec un canal alpha).
- Activer la composition du bureau Cette option active les éléments de l'interface Windows tels que la transparence.
- Désactiver l'animation du menu : Cette option désactive l'animation du menu comme le glissement graphique, le changement de couleur. En sélectionnant cette option vous économisez de la largeur de bande.
- Désactiver le cryptage RDP Standard : Cette option désactive le cryptage RDP standard.
- Désactiver l'authentification au niveau du réseau : Cette option désactive l'authentification réseau requise avant la connexion au serveur distant.

Configurer la connexion Citrix ICA

Independent Computing Architecture (ICA) est un protocole de gestion des systèmes de l'application du serveur. ICA fournit des règles pour le transfert de données entre un serveur et un client. Une connexion ICA peut être configurée en fonction de vos préférences de connexion ; pour configurer une connexion ICA :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **ICA – Citrix Client**
6. Cliquez sur **OK**. La fenêtre **ICA** s'affiche.

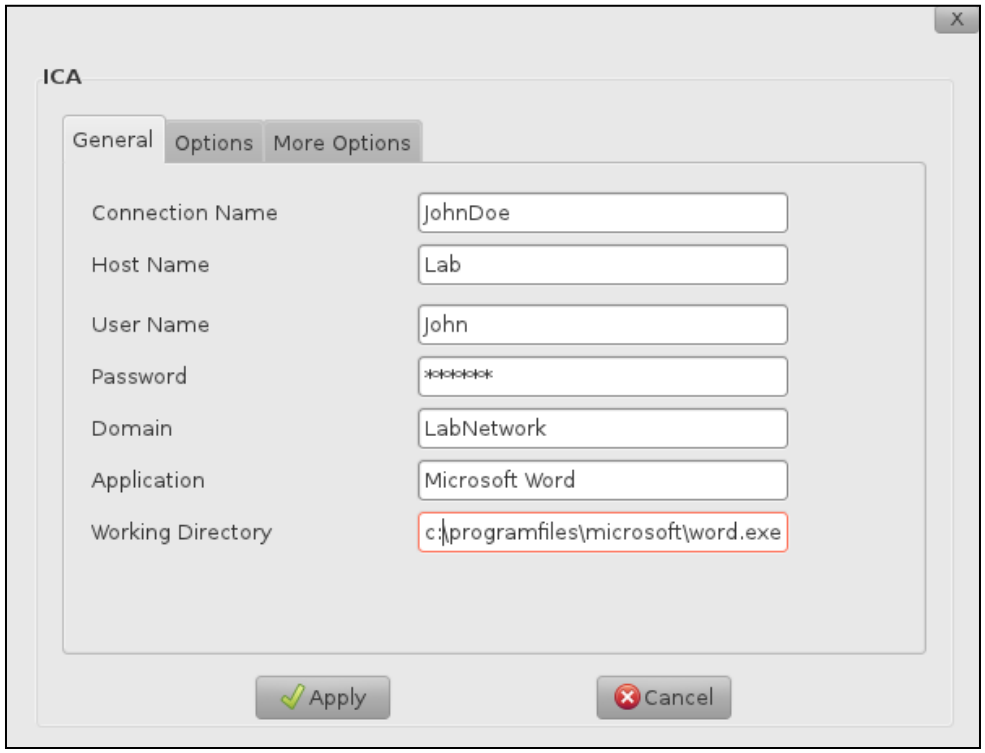

Figure 3-23 : Configurer la connexion ICA

7. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
8. Dans le champ **Nom de l'hôte**, saisissez un nom d'hôte.
9. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
10. Dans le champ **Mot de passe**, saisissez un mot de passe.

    Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion ICA.

11. Dans le champ **Domaine**, saisissez un nom de domaine.

    Remarque : Le nom de domaine est le nom de domaine du serveur distant.

12. Dans le champ **Application**, saisissez le nom de l'application. *Par exemple, Microsoft Word.*
13. Dans le champ **Répertoire de travail**, entrez le chemin d'accès au répertoire de travail. *Par exemple,* `C:\programfiles\microsoft\word.exe`*.*
14. Cliquez sur l'onglet **Options**.
15. Dans la zone de sélection numérique de la **Résolution d'affichage**, sélectionnez une résolution d'affichage.
16. Sélectionnez les options de connexion en fonction de vos préférences. Les différentes options de connexion sont les suivantes :

    - Mapper les imprimantes locales
    - Utiliser la compression ICA
    - Vitesse de l'écran BA
    - Vitesse de l'écran
    - Activer l'entrée audio
    - Mapper les ports série
    - Mapper les lecteurs de carte à puce locaux
    - Activer rendre utilisable OSS
    - Couleurs approximatives
    - EUKS

    Pour plus d'informations sur les options de connexion, reportez-vous à la section 'Options de connexion' à la page39.

17. Dans la zone de sélection numérique de la **Profondeur de couleurs souhaitée**, sélectionnez la profondeur de couleur. Vous pouvez sélectionner **1 (8 bits), 4 (16 bits)** ou **8 (24 bits).**
18. Cliquez sur l'onglet **Plus d'options**.
19. Saisissez vos valeurs préférées pour les options suivantes :

    - Vitesse écran BA taille du cache décompressé Entrer la valeur de la mémoire cache décompressée attribué à l'accélération de navigation.
    - **Vitesse écran BA taille du cache compressé** Entrer la valeur de la mémoire cache compressée attribué à l'accélération de navigation.
    - **Comptage minimal du chronomètre TW2 :** Saisissez le comptage minimal du chronomètre ThinWire 2. Il s'agit d'une fonction de synchronisation de l'application de l'interface utilisateur.
    - **Échelle de comptage du chronomètre TW2 :** Saisissez l'échelle de comptage du chronomètre ThinWire 2. Cette option permet de contrôler la disparité entre les vitesses des différentes opérations graphiques. *Par exemple, certains terminaux WinCE peuvent faire défiler rapidement mais rédige relativement lentement.* Ce nombre constitue un facteur d'échelle à appliquer aux valeurs renvoyées par les minuteries du chronomètre pour corriger cela.

20. Sélectionnez l'option préférée pour les paramètres suivants :

    - **Support audio** : Sélectionnez la qualité du son. Vous pouvez sélectionnez **Haute qualité, qualité moyenne** ou **faible qualité** audio. En sélectionnant **Off** vous désactiverez le son.

    - **Mode de cryptage** : Sélectionnez le mode de cryptage. Vous pouvez sélectionnez le cryptage **RC5 (128 bits**), **RC5 (128 bits- Connexion uniquement)** , RC**5 (40 bits)** ou **RC5 (50 bits)**.

    - **Transparent Key pass through** : Sélectionnez cette option pour déterminer comment certaines combinaisons de touches sont utilisées lors de la connexion ICA. Vous pouvez sélectionner **Serveur avec sessions en plein écran uniquement** : Les combinaisons de touches s'appliquent aux session ICA non-transparentes en mode plein écran, **Traduit/Local :** Les combinaisons de touches s'appliquent au bureau local ou au **Serveur** : Les combinaisons de touches s'appliquent aux connexions ICA transparentes et non transparentes..

    - **Protocole du navigateur** : Sélectionnez un protocole du navigateur pour la connexion. Vous pouvez sélectionner **TCP+HTTP, SSL/TLS+HTTPS** ou **TCP/UDP.**

21. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
22. Cliquez sur **Oui**.

Configurer une connexion Microsoft RDP

Remote Desktop Protocol (RDP) est un protocole de communication pour le système d'exploitation Windows. Le protocole fournit à un client léger, l'accès à un bureau ou un serveur Windows. Pour configurer une connexion RDP :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **RDP – Remote Desktop.**
6. Cliquez sur **OK**. La fenêtre **RDP** s'affiche.

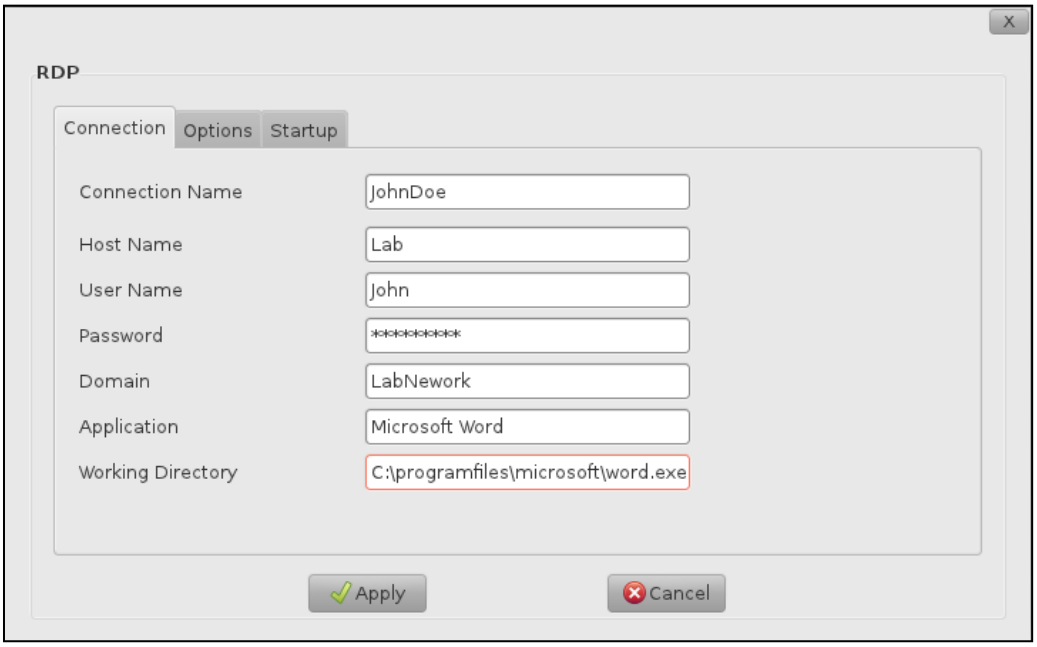

Figure 3-24 : Configurer la connexion RDP

7. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
8. Dans le champ **Nom de l'hôte**, saisissez un nom d'hôte.
9. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
10. Dans le champ **Mot de passe**, saisissez un mot de passe.

    Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion RDP.

11. Dans le champ **Domaine**, saisissez un nom de domaine.

    Remarque : Le nom de domaine est le nom de domaine du serveur distant.

12. Dans le champ **Application**, saisissez le nom de l'application. *Par exemple, Microsoft Word.*
13. Dans le champ **Répertoire de travail**, entrez le chemin d'accès au répertoire de travail. *Par exemple, C:\programfiles\microsoft\word.exe.*
14. Cliquez sur l'onglet **Options**.
15. Dans la zone de sélection numérique de la **Résolution d'affichage**, sélectionnez une résolution d'affichage en fonction des propriétés de votre moniteur
16. Dans la zone de sélection numérique de la **Profondeur de couleur**, sélectionnez la profondeur de couleur. Une plus grande profondeur des couleurs rendra les images plus éclatantes.
17. Dans la zone de sélection numérique du **Transfert Audio**, sélectionnez un transfert audio local ou distant. En sélectionnant **Off** vous désactiverez cette option.
18. Dans la liste déroulante **Version du protocole RDP**, sélectionnez la version du protocole **RDP4** ou **RDP5**
19. Sélectionnez les options de connexion en fonction de vos préférences. Les différentes options de connexion sont les suivantes :

- Mapper les ports série
- Compression des données
- Imposer les mises à jour de bitmap
- Mapper les lecteurs du client(USB:z)
- Ne pas envoyer les événements d'activité
- Synchronisation du verrouillage numérique
- Lecteurs de cartes à puce locaux
- Connexions de la Console
- Masquer les décorations WM

Pour plus d'informations sur les options de connexion, reportez-vous à la section 'Options de connexion' à la page39.

20. Cliquez sur l'onglet **Démarrage**.
21. Sélectionnez les services qui doivent être lancés lorsque votre client démarre, les services que vous pouvez choisir sont :
    - **Conserver les raccourcis clavier WM** Cette option permet de conserver les même raccourcis de la fenêtre de la session précédente.
    - **Nom de l'imprimante** : Sélectionnez le nom de l'imprimante dans la liste déroulante. Vous devez configurer votre imprimante pour que vous puissiez la sélectionner ici.
    - **Nom du pilote d'imprimante Windows :** Spécifiez le chemin d'accès et le nom de fichier du pilote.
22. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
23. Cliquez sur **Oui**.

Configurer une connexion VMware View Client

VMware View est un produit commercial de virtualisation de bureau développé par VMware. VMware View permet à un utilisateur de se connecter à une machine virtuelle distante. Pour configurer une connexion VMware View :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **VMware – VM View Client** La fenêtre VMware s'ouvre.
6. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
7. Dans le champ **Nom de l'hôte**, saisissez un nom d'hôte.
8. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
9. Dans le champ **Mot de passe**, saisissez un mot de passe.

Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion *VMware View*.

10. Dans le champ **Domaine**, saisissez un nom de domaine.

    Remarque : Le nom de domaine est le nom de domaine du serveur distant.

11. Cliquez sur l'onglet **Options VMware**.
12. Dans la zone de sélection numérique du **Protocole de connexion préféré**, sélectionnez le protocole **RDP** ou **PCOIP.**
13. Dans le champ **Nom du bureau**, saisissez le nom du bureau.
14. Cliquez sur l'onglet **Options RDP**.
15. Dans la zone de sélection numérique de la **Profondeur de couleur**, sélectionnez la profondeur de couleur. Une plus grande profondeur des couleurs rendra les images plus éclatantes.
16. Dans la zone de sélection numérique du **Transfert Audio**, sélectionnez **local** ou **distant**. En sélectionnant **Off** vous désactiverez cette option.
17. Dans la liste déroulante de la Version du **protocole RDP,** sélectionnez la version du protocole que vous souhaitez utiliser **RDP4** ou **RDP5**
18. Sélectionnez les options de connexion en fonction de vos préférences. Les différentes options de connexion sont les suivantes :

    - Mapper les imprimantes locales
    - Compression des données
    - Imposer les mises à jour de bitmap
    - Mapper les lecteurs du client(USB:z)
    - Mapper les ports série
    - Ne pas envoyer les événements d'activité
    - Masquer les décorations WM
    - **Conserver les raccourcis clavier WM**
    - Lecteurs de cartes à puce locaux
    - Connexion de la console

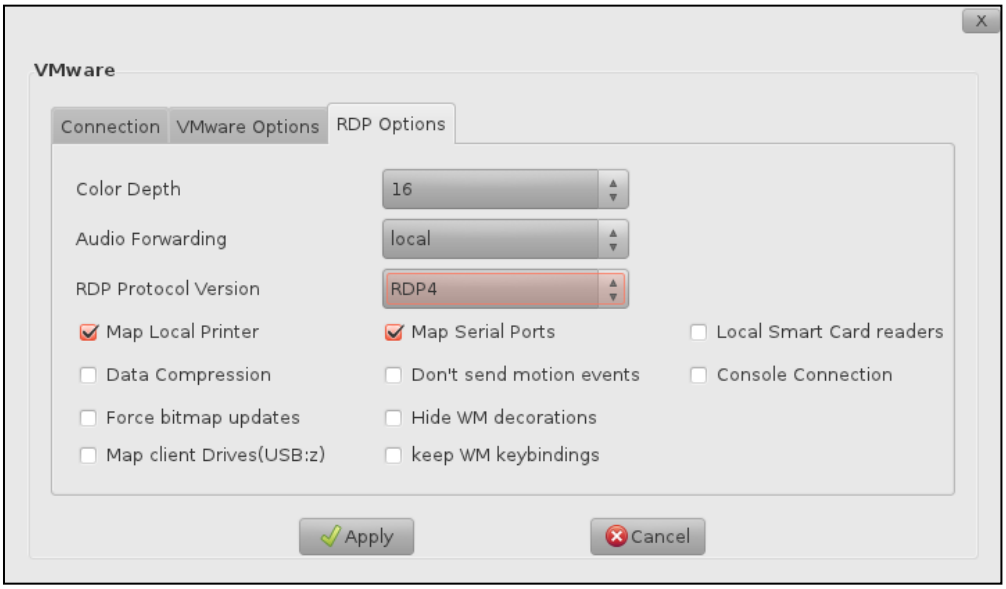

Figure 3-25 : Configurer la connexion VMware

Pour plus d'informations sur les options de connexion, reportez-vous à la section 'Options de connexion' à la page39.

19. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
20. Cliquez sur **OK**.

Configurer une connexion Citrix Receiver (WFCMGR)

Citrix Receiver est un produit commercial de virtualisation de bureau développé par Citrix ; il vous permet d'exécuter des applications hébergées sur un serveur distant. Pour configurer une connexion Citrix Receiver :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **WFCMGR – Citrix Receiver.**
6. Cliquez sur **OK**. La fenêtre **WFCMGR** s'affiche.

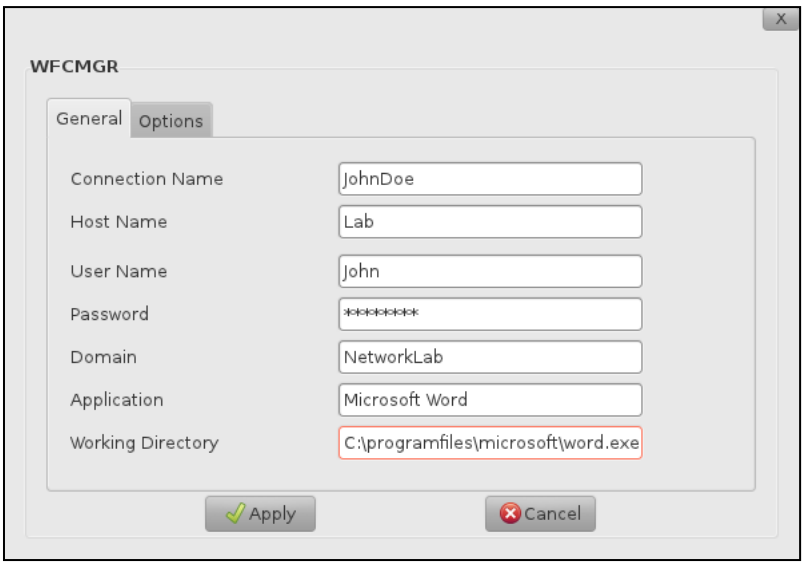

Figure 3-26 : Configurer la connexion WFCMGR

7. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
8. Dans le champ **Nom de l'hôte**, saisissez un nom d'hôte.
9. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
10. Dans le champ **Mot de passe**, saisissez un mot de passe.

    Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion.

11. Dans le champ **Domaine**, saisissez un nom de domaine.

    Remarque : Le nom de domaine est le nom de domaine du serveur distant.

12. Dans le champ **Application**, saisissez le nom de l'application. *Par exemple, Microsoft Word.*
13. Dans le champ **Répertoire de travail**, entrez le chemin d'accès au répertoire de travail. *Par exemple, C:\programfiles\microsoft\word.exe.*
14. Cliquez sur l'onglet **Options**.

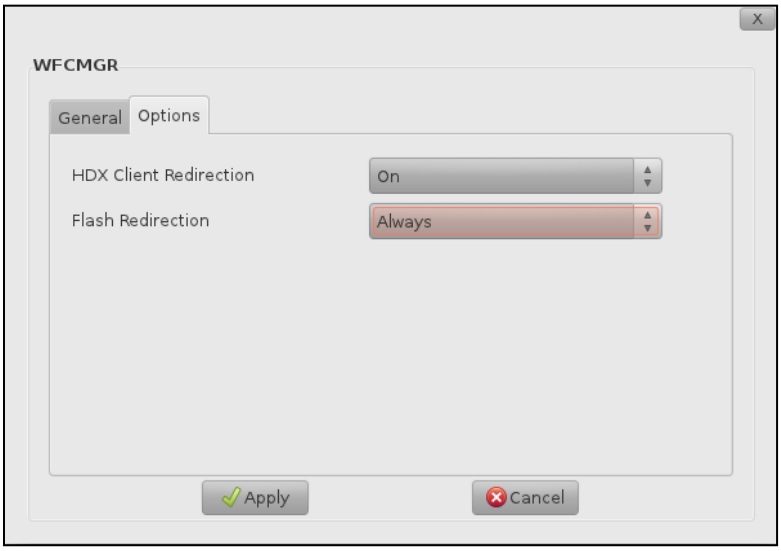

Figure 3-27 : Options de connexion WFCMGR

15. Dans la zone de sélection numérique **Redirection du client HDX**, sélectionnez **On** pour obtenir une expérience utilisateur de virtualisation du bureau haute définition.
16. Dans la zone de sélection numérique **Redirection Flash**, sélectionnez l'option de votre choix.
17. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
18. Cliquez sur **OK**.

Configurer la connexion Citrix PNAGENT

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter** , sélectionnez **PNAGENT- Citrix PN Agent.**
6. Cliquez sur **OK**. La fenêtre **PNAGENT** s'affiche.

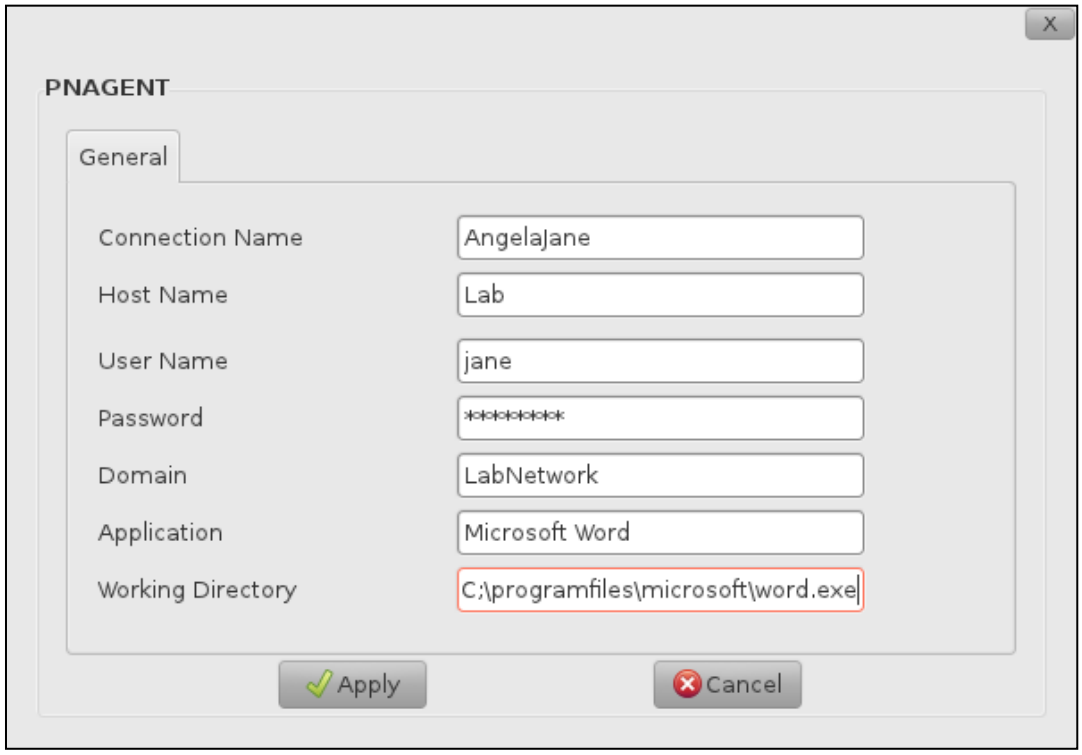

Figure 3-28 : Configurer la connexion ICA

7. Dans le champ **Nom de connexion**, saisissez un nom de connexion.
8. Dans le champ **Nom de l'hôte**, saisissez un nom d'hôte.
9. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
10. Dans le champ **Mot de passe**, saisissez un mot de passe.

    Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion ICA.

11. Dans le champ **Domaine**, saisissez un nom de domaine.

    Remarque : Le nom de domaine est le nom de domaine du serveur distant.

12. Dans le champ **Application**, saisissez le nom de l'application. *Par exemple, Microsoft Word.*
13. Dans le champ **Répertoire de travail**, entrez le chemin d'accès au répertoire de travail. *Par exemple,* `C:\programfiles\microsoft\word.exe`.
14. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
15. Cliquez sur **OK**.

Configurer la connexion via un navigateur Firefox

Une connexion via un navigateur Web permet au client léger d'accéder aux services sur le web via le navigateur d'un client léger. Cette connexion convient aux kiosques du client léger en utilisant une application web hébergée sur un serveur. Pour configurer une connexion via un navigateur :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **Navigateur – Navigateur Firefox.**
6. Cliquez sur **OK**. L**e Navigateur par défaut** s'affiche

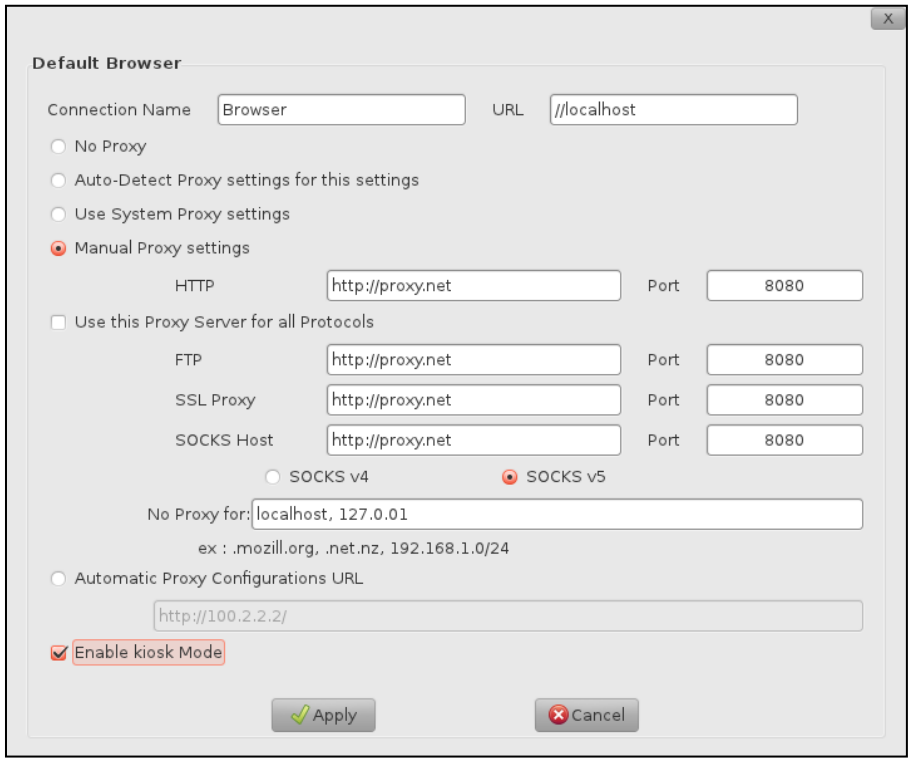

Figure 3-29 : Configurer la connexion via un navigateur

7. Dans le champ **Nom de connexion**, saisissez un nom de connexion de votre choix.
8. Dans le champ **URL**, saisissez l'URL du serveur.
9. Vous pouvez choisir les paramètres proxy suivants pour vos connexions.

   - **Aucun proxy** : Désactivez le proxy. Ceci est l'option par défaut.
   - **Détection automatique des paramètres de proxy pour ces paramètres** : Détecter automatiquement les paramètres de proxy et les configurer pour cette connexion.
   - **Utiliser les paramètres de proxy du système** : Utiliser les paramètres de proxy déjà disponibles dans le client léger.

- **Paramètres manuels de proxy** : Sélectionnez cette option pour entrer manuellement les paramètres de proxy en fonction de vos préférences. Suivez ces étapes pour configurer manuellement les paramètres de proxy :

    a. Dans le champ **HTTP**, saisissez une adresse HTTP ; saisissez le numéro de port dans le champ de **port** correspondant**.**

    b. Sélectionnez **Utiliser ce serveur proxy pour tous les protocoles** pour utiliser ce serveur proxy universellement pour les connexions qui utilisent différents protocoles tels que HTTP, FTP.

    c. Dans le champ **FTP**, saisissez une adresse FTP ; saisissez le numéro de port dans le champ de **port** correspondant**.**

    d. Dans le champ **SSL Proxy**, saisissez une adresse SSL Proxy ; saisissez le numéro de port dans le champ de **port** correspondant**.**

    e. Dans le champ **Hôte SOCKS**, saisissez une adresse Hôte SOCKS ; saisissez le numéro de port dans le champ de **port** correspondant**.**

    f. Sélectionnez **SOCKS v4 ou SOCKS v5** en fonction de vos préférences ; ce sont les deux versions différentes du protocole SOCKS.

    g. Dans le champ **Pas de proxy pour**, entrez le nom ou l'adresse IP pour laquelle vous ne voulez pas utiliser les paramètres de proxy.

- **Configurations D'URL de proxy automatique** : Sélectionnez cette option pour configurer automatiquement vos paramètres de proxy à partir d'un emplacement distant. Entrez l'URL de l'emplacement distant.

10. Sélectionnez **Activer kiosque** pour utiliser cette connexion dans le mode kiosque. Les kiosques sont des machines autonomes qui fournissent une interface personnalisée comme un navigateur.
11. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
12. Cliquez sur **OK**.

Configuration d'une connexion RemoteFX (X FreeRDP)

RemoteFX est une technologie qui améliore l'expérience visuelle de la connexion Remote Desktop Protocol. FreeRDP est une implémentation en open source du protocole Microsoft RDP, distribué sous la licence Apache. Pour configurer une connexion FreeRDP :

1. Sur la barre latérale du bureau, cliquez sur **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **Remote FX – X Free RDP.**
6. Cliquez sur **OK**. La fenêtre **Remote FX** s'affiche.
7. Dans le champ **Nom de connexion**, saisissez un nom de connexion de votre choix.
8. Dans le champ **Serveur**, saisissez l'adresse IP du serveur.
9. Dans le champ **Numéro de port**, saisissez un numéro de port valide.
10. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur de votre choix.
11. Dans le champ **Mot de passe**, saisissez un mot de passe de votre choix.

Remarque : Veuillez prendre note de votre nom d'utilisateur et votre mot de passe. Votre nom d'utilisateur et le mot de passe sont requis plus tard lors de l'établissement de la connexion.

12. Dans le champ **Domaine**, saisissez un nom de domaine.
13. Dans le **Mot de passe du domaine**, saisissez le mot de passe de votre domaine.
14. Dans le champ **Répertoire de travail**, saisissez un chemin d'accès au répertoire de travail. *Par exemple,* `C:\programfiles\microsoft\word.exe`.
15. Dans le champ **Start-up Shell**, saisissez une application de démarrage. Cette option démarre une application spécifiée au lieu de l'explorateur par défaut.
16. Dans le champ **Titre de la fenêtre**, saisissez le titre de la fenêtre qui doit apparaître pour cette connexion. Vous pouvez choisir le titre de la fenêtre de votre choix.
17. Cliquez sur l'onglet **Options RemoteFx**.
18. Sélectionnez l'une des options suivantes pour votre connexion en fonction de vos préférences :

    - Activer l'imprimante
    - Activer le son
    - Activer Smartcard
    - Masquer les décorations de la fenêtre
    - Console audio
    - Désactiver l'authentification
    - Désactiver les mouvements de souris
    - Désactiver le cache Bitmap
    - Désactiver le papier peint
    - Désactiver le Full Window Drag
    - Désactiver les thèmes
    - Désactiver le cryptage TLS
    - Activer Remote FX
    - Vérification du certificat
    - Activer l'enregistrement audio
    - Activer l'USB
    - Désactiver Checksum avec une connexion RDP Std
    - Définir la configuration du clavier
    - Activer la compression
    - Désactiver le chemin rapide
    - Désactiver le bitmap Offscreen

- Activer NSCode
- Activer la composition du bureau
- Désactiver les animations du menu
- Désactiver le cryptage RDP Standard
- Désactiver l'authentification au niveau du réseau
- Se connecter à la session de la console

Pour plus d'informations sur les options de connexion, reportez-vous à la section 'Options de connexion' à la page39.

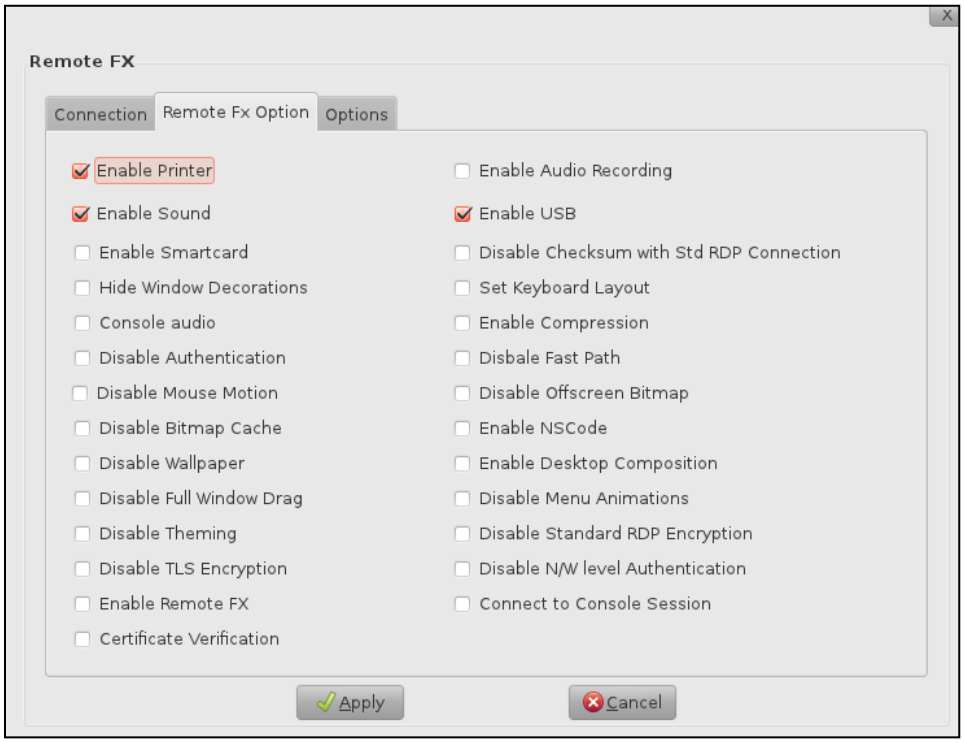

Figure 3-30 : Configurer la connexion FreeRDP

19. Cliquez sur l'onglet **Options**.
20. Dans le champ **Charger un canal virtuel de plug-in**, saisissez le chemin à partir duquel le plugin virtuel doit être chargé.
21. Dans le champ **Charger dans l'extension**, saisissez le nom de l'application à charger.
22. Dans le champ **Application à distance à connecter**, saisissez le nom de l'application à distance.
23. Dans la liste déroulante **mode Remote FX**, sélectionnez le mode vidéo ou image.
24. Dans la liste déroulante **Définir la géométrie**, sélectionnez une résolution de moniteur en fonction de votre moniteur La connexion prend en charge une résolution allant jusqu'à 1600x1200.
25. Dans la liste déroulante **Indicateurs de performance**, sélectionnez le type de réseau que vous utilisez pour votre connexion. Les options sont les suivantes : **Haut débit**, **modem** ou **réseau local (LAN).**

26. Dans la liste déroulante **Rendu graphique**, sélectionnez rendu graphique **Logiciel** ou **Matériel**.
27. Dans la liste déroulante **Version du protocole NTLM**, sélectionnez la version du protocole NTLM**.**
28. Dans la liste déroulante **Imposer le protocole de sécurité**, sélectionnez un protocole de sécurité pour la connexion. Les options sont **rdp** , **tls** et **nla**. Le protocole de sécurité par défaut est **nla**.
29. Dans la liste déroulante **Définir la profondeur de couleur en Bit**, sélectionnez la profondeur de couleur **8 bits, 15 bits, 16 bits, 24 bits ou 32 bits**. Une plus grande profondeur des couleurs rendra les images plus éclatantes.
30. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
31. Cliquez sur **Oui**.

Configurer une connexion Secure Shell (SSH)

SSH est un protocole de réseau qui vous permet de transmettre de façon sécurisée les informations entre votre client léger et le serveur du terminal. Pour configurer une connexion SSH :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **SSH – Secure Shell.**
6. Cliquez sur **OK**. La fenêtre **SSH** s'affiche.

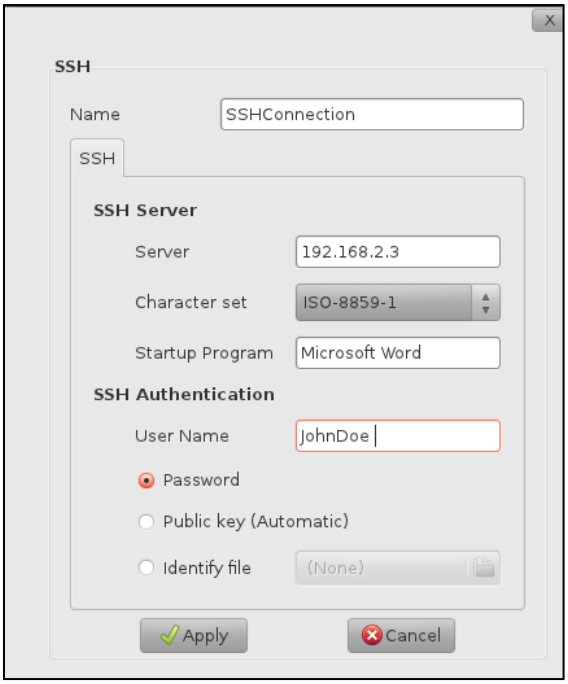

Figure 3-31 : Configurer la connexion SSH

7. Dans le champ **Nom**, saisissez le nom de la connexion SSH.
8. Dans le champ **Serveur**, saisissez l'adresse IP et le nom du serveur SSH.

9. Dans la liste déroulante **Jeu de caractères**, sélectionnez un jeu de caractères de votre choix. *Par exemple, vous pouvez sélectionner ISO-8859-1.*
10. Dans le champ **Programme de démarrage**, saisissez le nom du programme de démarrage. *Par exemple, Microsoft Word.*
11. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur pour l'authentification SSH.
12. Sélectionnez l'une des méthodes d'authentification suivantes : **Mot de passe, Clé publique (automatique), Fichier d'identité**.

    Remarque : Pour sélectionner un fichier d'identité pour l'authentification, cliquez sur le bouton Parcourir à côté du **Fichier d'identité**, puis cliquez sur **Ouvrir** .
13. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
14. Cliquez sur **Oui**.

Configurer une connexion SFTP (Protocole de transfert de fichiers sécurisé)

Le protocole de transfert de fichiers sécurisé (SFTP) est un protocole de réseau qui fournit un accès au fichiers, un transfert et une gestion d'un réseau sécurisés. Pour configurer une connexion SFTP :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **SFTP – Protocole de transfert de fichiers sécurisé.**
6. Cliquez sur **OK**. La fenêtre **SFTP** s'affiche.

Figure 3-32 : Configurer la connexion SFTP

7. Dans le champ **Nom**, saisissez le nom de la connexion SFTP.

8. Dans le champ **Serveur**, saisissez l'adresse IP et le nom du serveur SSH.
9. Dans la liste déroulante **Jeu de caractères**, sélectionnez un jeu de caractères de votre choix. *Par exemple, vous pouvez sélectionner ISO-8859-1.*
10. Dans le champ **Chemin de démarrage**, saisissez le nom du programme de démarrage.
11. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur pour l'authentification SSH.
12. Sélectionnez l'une des méthodes d'authentification suivantes : **Mot de passe, Clé publique (automatique), Fichier d'identité**.

    Remarque : Pour sélectionner un fichier d'identité pour l'authentification, cliquez sur le bouton Parcourir à côté du Fichier d'identité, puis cliquez sur **Ouvrir**.
13. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
14. Cliquez sur **Oui**.

Configurer une connexion XDMCP

XDMCP est un protocole de bureau à distance qui peut être utilisé pour accéder à aux ordinateurs de bureau et aux serveurs Linux à distance. Pour configurer une connexion XDMCP :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **XDMCP – X Remote Session.**
6. Cliquez sur **OK**. La fenêtre **XDMCP** s'affiche.

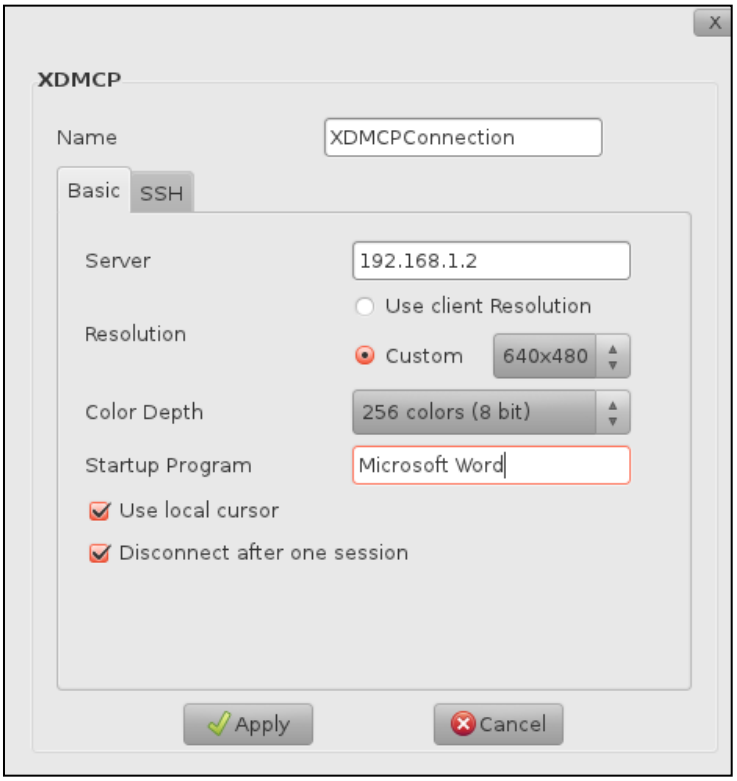

Figure 3-33 : Configurer la connexion XDMCP

7. Dans le champ **Nom**, saisissez le nom de la connexion XDMCP.
8. Cliquez sur l'onglet **Basic**.
9. Dans le champ **Serveur**, saisissez l'adresse IP du serveur XDMCP.
10. Pour configurer la résolution du client :
    - Sélectionnez **Utiliser la résolution du client** pour la résolution du moniteur du client par défaut.

      ou

    - Sélectionnez une résolution personnalisée dans la liste déroulante **Personnaliser**.
11. Dans la liste déroulante **Profondeur de couleur**, sélectionnez la profondeur de couleur de votre choix Une plus grande profondeur des couleurs rendra les images plus éclatantes.
12. Dans le champ **Programme de démarrage**, saisissez le nom du programme de démarrage.
13. Sélectionnez **Utiliser curseur local** pour permettre l'utilisation du curseur du client léger local.
14. Sélectionnez **Déconnecter après une session** pour déconnecter cette connexion XDMCP après une session. Votre connexion XDMCP ne sera pas automatiquement reconnectée pour les connexions consécutives.
15. Cliquez sur **Appliquer** si vous ne voulez pas configurer SSH pour cette connexion. Votre connexion XDMP est configurée.
16. Pour configurer SSH, cliquez sur l'onglet **SSH**.

17. Sélectionnez **Activer tunnel SSH** pour activer un cryptage via un tunnel SSH pour cette connexion.
18. Sélectionnez **Tunnel via Adresse de bouclage** pour activer le tunneling via le adresse de bouclage XDMCP.
19. Sélectionner **Même serveur sur le port 22** pour sélectionner le serveur sur le port 22 par défaut.
20. Sélectionnez **Personnaliser** pour saisir l'adresse IP d'un serveur SSH.
21. Dans la liste déroulante **Jeu de caractères**, sélectionnez un jeu de caractères. *Par exemple, vous pouvez sélectionner ISO-8859-1.*
22. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur pour l'authentification SSH.
23. Sélectionnez l'une des méthodes d'authentification suivantes : **Mot de passe, Clé publique (automatique), Fichier d'identité**.

    Remarque : Pour sélectionner un fichier d'identité pour l'authentification, cliquez sur le bouton Parcourir à côté du **Fichier d'identité**, puis cliquez sur **Ouvrir** .
24. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
25. Cliquez sur **Oui**.

Configurer une connexion Network File System (système de fichiers réseau)

Un lecteur réseau est une unité de stockage connectée à un réseau et partagée par les utilisateurs de ce réseau. Un système de fichiers réseau est utilisé pour lire et écrire des fichiers sur un lecteur réseau.
Pour configurer une connexion Network File System :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre **Connexions** s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **NFS – Network File System.**
6. Cliquez sur **OK**. La fenêtre **NFS** s'affiche.

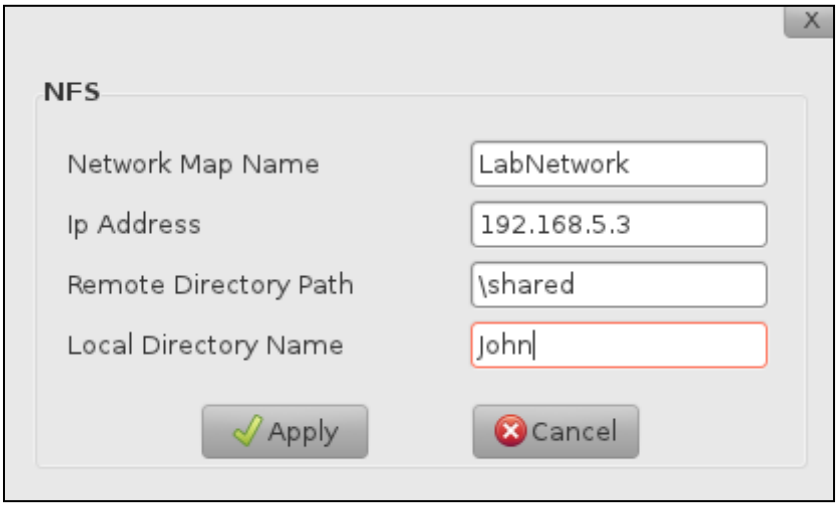

Figure 3-34 : Configurer la connexion NFS

7. Dans le champ **Nom de la carte réseau**, saisissez le nom de la carte réseau NFS.
8. Dans le champ **Adresse IP**, saisissez l'adresse IP et le nom d'hôte du serveur NFS.
9. Dans le champ **Chemin du répertoire à distance**, saisissez le nom du dossier partagé.
10. Dans le champ **Nom du répertoire local**, saisissez un nom de dossier.

    Remarque : Un dossier avec le nom spécifié dans le champ **Nom du répertoire local** est créé dans le répertoire \media. Ce dossier est redirigé dans toutes les connexions.
11. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
12. Cliquez sur **Oui**.

Configurer une connexion Samba

Samba permet d'accéder aux fichiers et aux services d'impression Microsoft Windows pour votre client léger. Pour configurer une connexion Samba :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Cliquez sur **Ajouter**.
5. Dans la liste déroulante **Veuillez choisir la connexion à ajouter,** sélectionnez **SAMBA – Samba.**
6. Cliquez sur **OK**.

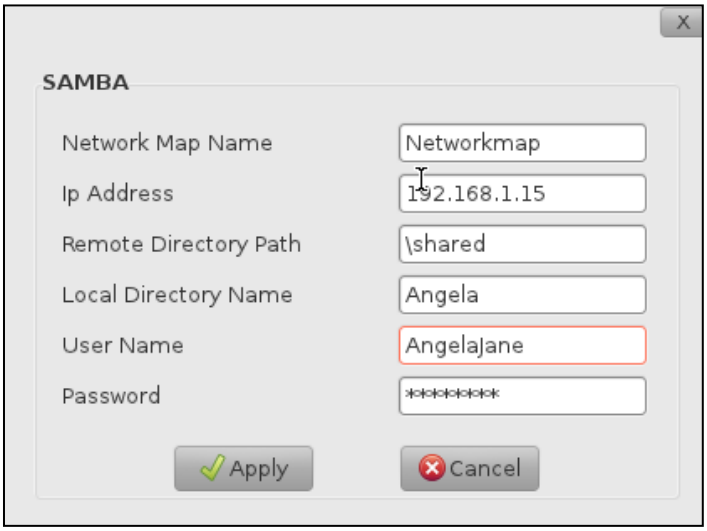

Figure 3-35 : Configurer la connexion Samba

7. Dans le champ **Nom de la carte réseau**, saisissez le nom de la carte réseau NFS.
8. Dans le champ **Adresse IP**, saisissez l'adresse IP et le nom du serveur Samba.
9. Dans le champ **Chemin du répertoire à distance**, saisissez le nom du dossier partagé.
10. Dans le champ **Nom du répertoire local**, saisissez un nom de dossier.

    Remarque : Un dossier avec le nom spécifié dans le champ **Nom du répertoire local** est créé dans le répertoire \media. Ce dossier est redirigé dans toutes les connexions.
11. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
12. Dans le champ **Mot de passe**, saisissez un mot de passe.
13. Cliquez sur **Appliquer**. La fenêtre de confirmation s'affiche.
14. Cliquez sur **Oui**.

Éditer une connexion

Vous pouvez éditer une connexion pour modifier les paramètres et les options. Pour éditer une connexion :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Sélectionnez la connexion que vous souhaitez modifier.
5. Cliquez sur **Éditer.**
6. Modifiez les paramètres en fonction de vos nouvelles préférences.
7. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
8. Cliquez sur **OK**.

Connexion à un serveur

Vous pouvez vous connecter à un serveur lorsque vous avez configuré votre connexion. Pour se connecter à une connexion au serveur :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4. Sélectionnez l'une des connexions suivantes pour vous connecter :

ICA

Sélectionnez la connexion ICA, puis cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

RDP

Sélectionnez la connexion RDP, puis cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

VMware View Client

1. Sélectionnez la connexion VMware puis cliquez sur **Connecter,** la **VMware View Client** s'affiche.
2. Dans la liste déroulante **Saisir le nom d'un serveur View Connection**, saisissez ou sélectionnez une adresse IP du serveur.

   Remarque : Sélectionnez **Toujours se connecter à ce serveur au démarrage** pour vous connecter à
   ce serveur à chaque que cette connexion est démarrée.
3. Cliquez sur **Continuer**. La fenêtre **Connexion au serveur** s'affiche.

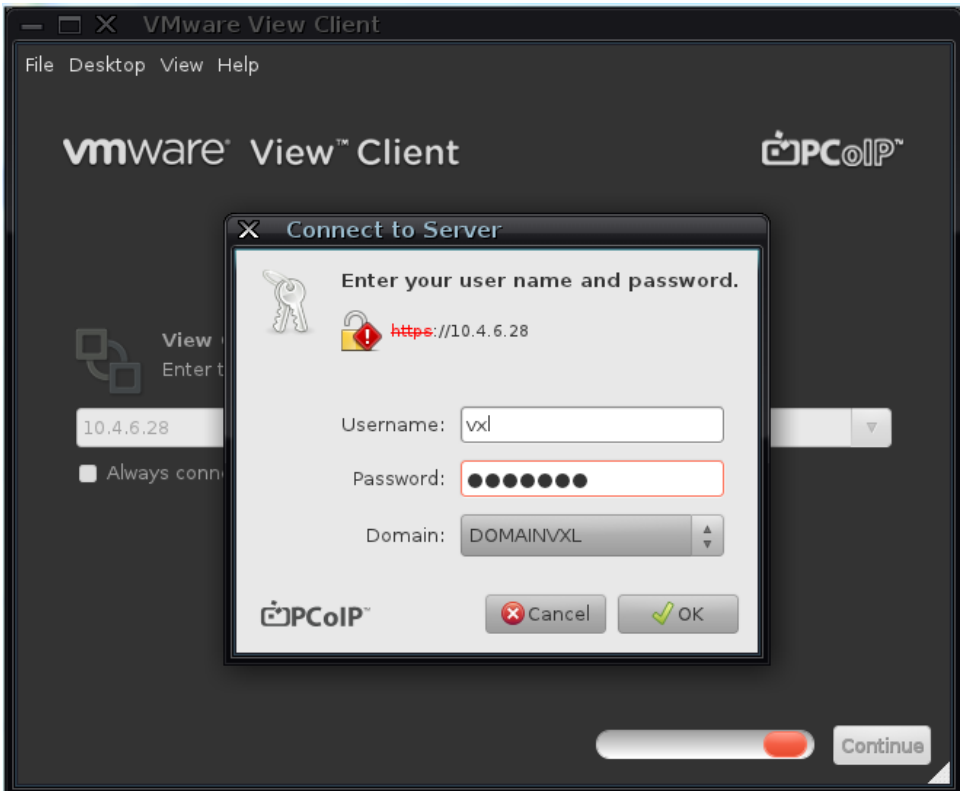

Figure 3-36 : Configurer une connexion VMware View Client

4. Saisissez le **Nom d'utilisateur** et le **Mot de passe**, puis cliquez sur **OK**.
5. Sélectionnez une machine virtuelle dans la liste des machines virtuelles disponibles. La fenêtre du bureau de la machine virtuelle sélectionnée s'affiche.

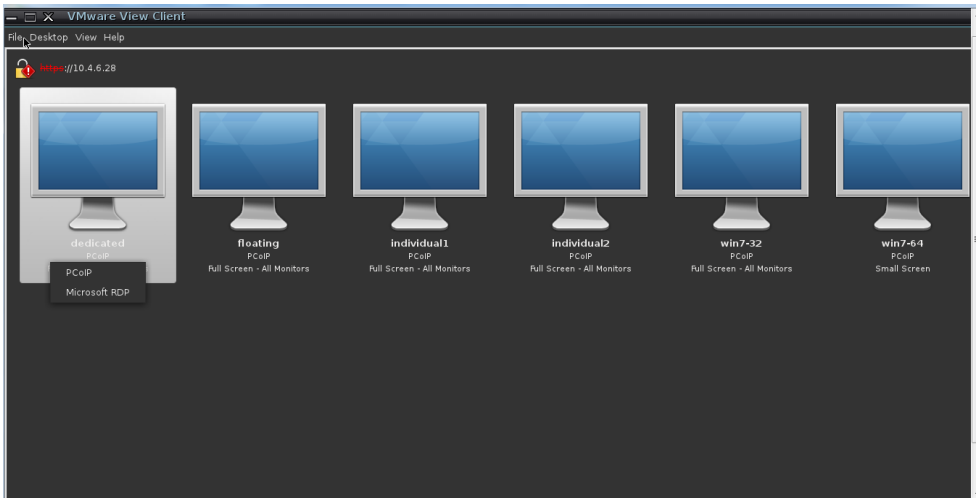

Figure 3-37 : Machines virtuelles

6. Dans la liste déroulante du bureau dans la barre des tâches, sélectionnez **déconnecter**
   pour vous déconnecter de la machine virtuelle actuelle.
7. Pour quitter le VMware View client, cliquez sur **Fichier > Quitter**.

WFCMGR Citrix Receiver

1. Cliquez sur **Connexion,** la fenêtre d'**ouverture de session Citrix XenApp** s'affiche.

Figure 3-38 : Ouverture de session Citrix XenApp

2. Dans le champ **Nom d'utilisateur**, saisissez un nom d'utilisateur.
3. Dans le champ **Mot de passe**, saisissez un mot de passe.
4. Dans le champ **Domaine**, saisissez le nom du domaine.

   Remarque : Sélectionnez **Enregistrer mot de passe** si vous souhaitez enregistrer le mot de passe à utiliser lors de la prochaine session.
5. Cliquez sur **OK**. La fenêtre **Citrix Receiver** s'affiche.
6. Dans la liste d'application fournie, sélectionnez l'application que vous souhaitez lancer.

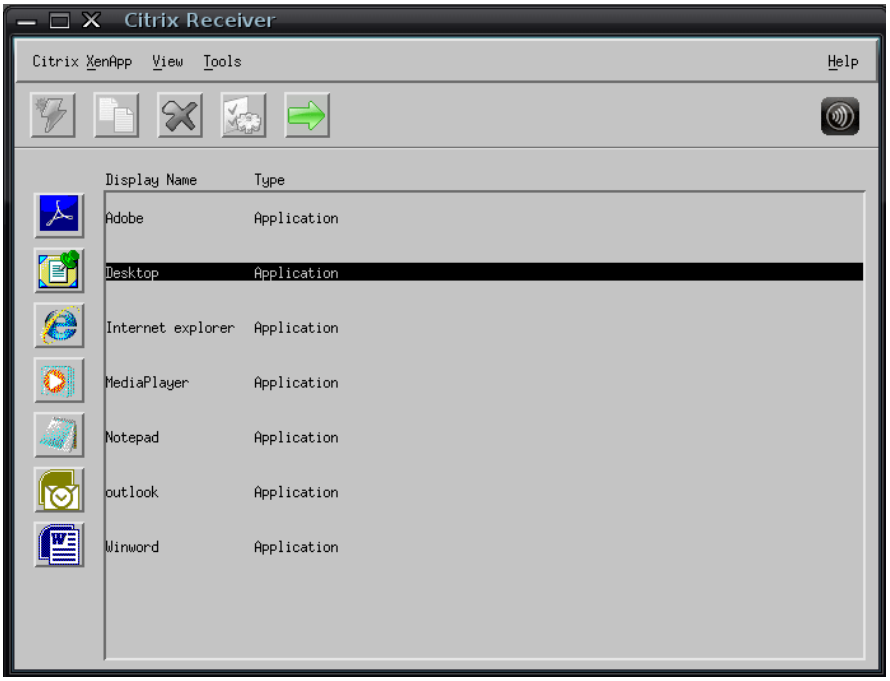

Figure 3-39 : Citrix Receiver

7. Cliquez sur **Citrix XenApp**, cliquez sur **Se connecter à sélection**. L'application sélectionnée est lancée.

Navigateur - Navigateur Firefox

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

Remote FX - X libre RDP

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

SSH : Secure Shell

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

SFTP - Protocole de transfert de fichiers sécurisé

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

XDMCP - X Session distante

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

NFS - Système de fichiers à distance

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

SAMBA – Samba

Cliquez sur **Connecter**. La fenêtre du bureau distant s'affiche.

Effacer une connexion

Vous pouvez éditer une connexion pour modifier les paramètres et les options. Pour éditer une connexion :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Gestionnaire de connexion,** la fenêtre Connexions s'affiche.
4.
5. Cliquez sur **Supprimer**, la fenêtre de confirmation s'affiche.
6. Cliquez sur **OK**.

Connexion automatique

L'option Connexion automatique vous permet de vous connecter à une connexion donnée directement au démarrage.

Pour configurer une connexion automatique :

1. Dans la fenêtre de **connexion** sélectionnez une connexion de votre choix.

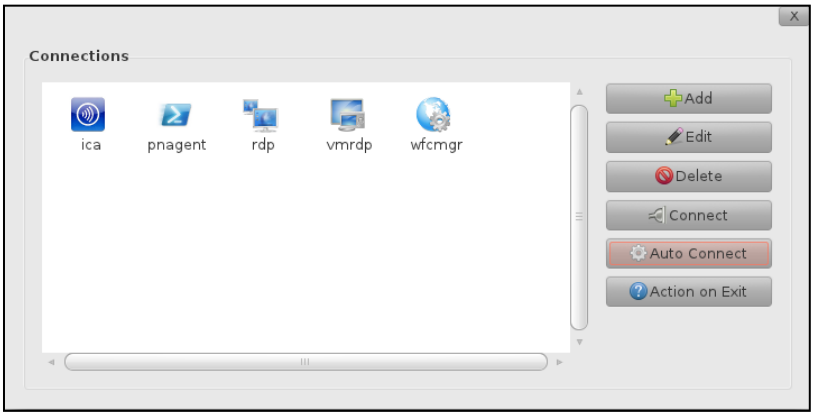

Figure : 3-40 Sélectionnez Connexion

2. Cliquez sur **Connexion automatique**.

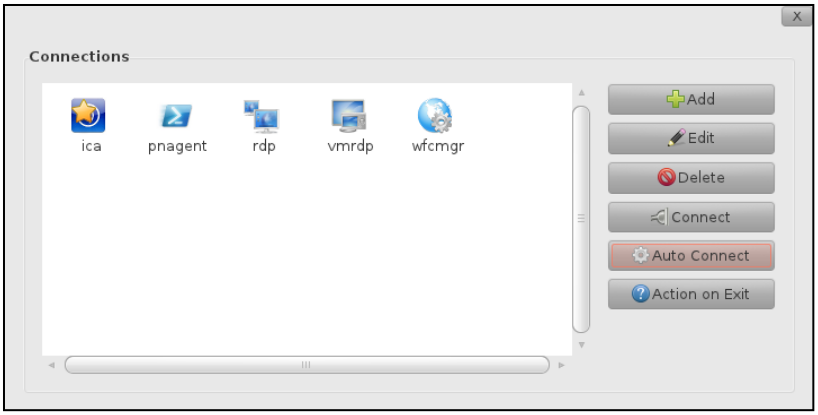

Figure : 3-41 Connexion automatique

Action de Sortie

Cette option vous permet de configurer le client pour redémarrer ou arrêter lorsque vous fermez une session.

Pour définir l'action de sortie :

1. Dans la fenêtre de **connexion** sélectionnez une connexion de votre choix.
2. Cliquez sur **Action de Sortie**.

Figure 3-42 : Action de Sortie

3. Sélectionnez **Redémarrer** ou **Arrêter .**
4. Cliquez sur **OK**.

Remarque : L'option Action de sortie n'est pas fonctionnelle pour le moment.

XLM Connect

Vous pouvez configurer votre client pour fonctionner avec l'application XLmanage. Pour configurer votre client avec XLmanage :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **XLM Connect**, la fenêtre **XLM Connect** s'affiche.

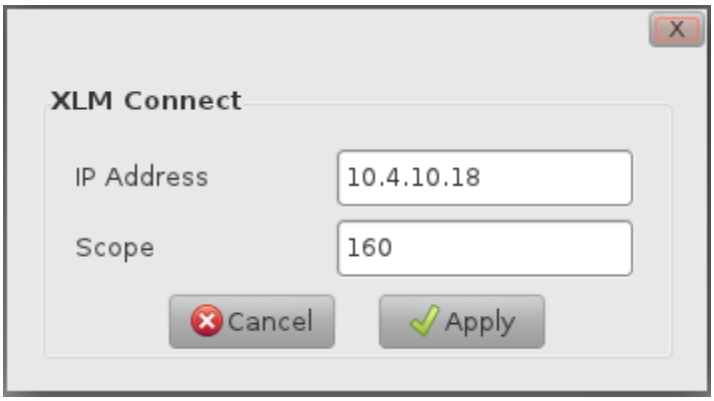

Figure 3-43 : Configurer la connexion XLmanage

4. Dans le champ **Adresse IP**, saisissez votre adresse IP.
5. Dans le champ **Portée**, saisissez l'ID de la portée. L'IP de la portée est l'adresse IP du serveur XLmanage.

   Remarque : Vous pouvez vous connecter à XLmanage uniquement lorsqu'un serveur XLmanage est configuré et est en cours d'exécution.
6. Cliquez sur **Appliquer**. La boîte de dialogue de confirmation s'affiche.
7. Cliquez sur **Oui**.

Emplacement

L'option Emplacement vous permet de préciser l'emplacement physique du client léger,

Par exemple : Le numéro de l'étage, numéro du bureau, etc.

Pour entrer le numéro de l'emplacement du client léger :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **connectivité**.
3. Cliquez sur **Emplacement**, la fenêtre de l'**Emplacement** s'affiche.

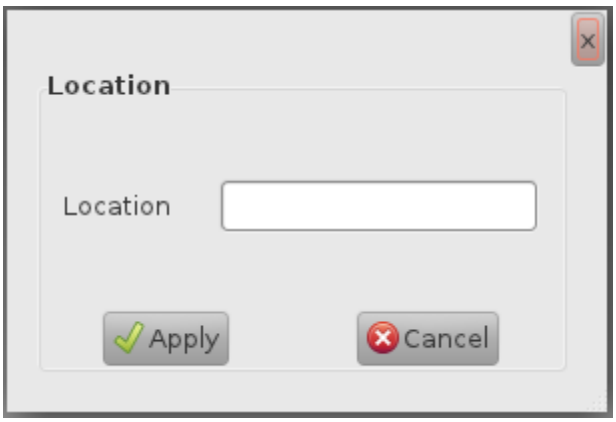

Figure : 3-44 Emplacement

4. Saisissez l'emplacement et cliquez sur **Appliquer**.
5. La fenêtre de **Confirmation** s'affiche, cliquez sur **Oui**.

4 Paramètres locaux

Vous pouvez configurer *les* paramètres locaux du *Gio 5* manuellement. Les différents paramètres que vous pouvez configurer sont les suivantes :

- Périphériques
- Affichage
- Paramètres du système
- Mise à niveau du micrologiciel
- Comptes d'utilisateur
- Restaurer les paramètres par défaut
- Verrouillage de l'écran
- Importer des certificats

Ce chapitre fournit des instructions étape par étape pour configurer les paramètres locaux suivants.

Périphériques

L'option Périphériques vous permet de configurer la souris, le clavier et l'imprimante.

Souris

Pour configurer la souris :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Périphériques**, puis cliquez sur **Souris**. La fenêtre Paramètres de la souris s'affiche.

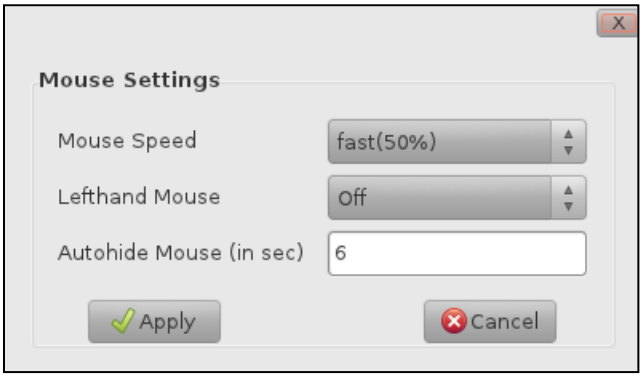

Figure 4-1 : Configuration les paramètres de la souris

4. Sélectionnez ou saisissez des valeurs pour les champs suivants :
   - **Vitesse de la souris** : La valeur de vitesse de déplacement de la souris détermine la rapidité à laquelle le curseur se déplace en réponse aux

mouvements de la souris. Sélectionnez une vitesse de déplacement de la souris en fonction de vos préférences.

- Souris Main gauche : Régler cette option sur **On** pour que votre souris s'adapte à la main gauche. Cette option rend le bouton droit de la souris le bouton principal de sélection et le bouton gauche de la souris, le bouton secondaire de la souris.
- **Masquer automatiquement la souris (en sec) :** Masquer le curseur de la souris pendant une durée spécifiée en secondes.

5. Cliquez sur **Appliquer**. La boîte de dialogue de confirmation s'affiche.
6. Cliquez sur **Oui**.

Clavier

Pour configurer le clavier :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Périphériques**, puis cliquez sur **Clavier**. La fenêtre **Clavier** s'affiche.

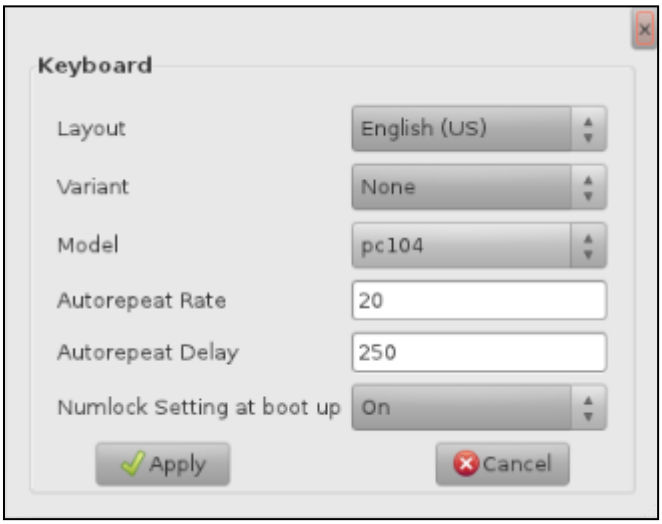

Figure 4-2 : Configurer les paramètres du clavier

4. Sélectionnez ou saisissez des valeurs pour les champs suivants :
   - **Configuration** : Sélectionnez la configuration du clavier.
   - **Variable** : Sélectionnez le type de variable du clavier. Le type de clavier par défaut est **qwerty**.
   - **Modèle** : Sélectionnez le modèle du clavier.
   - **Taux de répétition automatique** : Spécifiez la fréquence à laquelle le clavier va répéter une touche si vous appuyez sur elle en continu.
   - **Différer la répétition automatique** : Spécifier la durée du délai (ms) au bout duquel la touche se répète.
   - **Paramètres du verrouillage numérique lors du démarrage** : Activer ou désactiver la touche Verr Num au démarrage.

5. Cliquez sur **Appliquer**. La boîte de dialogue de confirmation s'affiche.
6. Cliquez sur **Oui**.

Imprimante

Le *Gio 5* prend en charge l'impression locale et en réseau ; vous pouvez soit imprimer à l'aide de l'imprimante connectée à votre client léger ou utiliser une imprimante qui est connectée au réseau. Le *Gio 5* utilise *le* Common UNIX Printing System (CUPS) pour traiter l'impression des travaux, CUPS se compose du spouleur d'impression et du planificateur qui utilise le protocole d'impression Internet (IPP) pour la mise en file d'attente et l'impression.

Ajouter une imprimante locale

Connectez une imprimante locale à votre client léger via un port série.

Pour ajouter une imprimante locale :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Périphériques**, puis cliquez sur **Imprimante**. La fenêtre **Imprimante** s'affiche.
4. Cliquez sur **Ajouter**. La fenêtre **Sélectionner périphérique** s'affiche**.**
5. Sous **Périphériques**, sélectionnez le **Port série.**
6. Sélectionnez des valeurs pour les champs suivants :
    - **Débit en bauds** : Sélectionnez un débit en bauds en fonction l'imprimante que vous utilisez. Le débit en bauds est le nombre de symboles transmis par seconde. Un débit en bauds élevé permettra à plus d'information d'être transférée par seconde. Le débit en bauds est généralement fourni par le fabricant de l'imprimante.
    - **Parité :** Sélectionnez une parité **Impaire** ou **Paire**. Sélectionnez **Aucun** pour ne pas vérifier la parité. La parité est fournie comme étant un mécanisme de vérification d'erreur, si le serveur d'impression et le client s'accordent sur une parité paire, alors les bits de parité impaire sont considérés comme erronés.
    - **Bits de données** : Sélectionnez le nombre de bits de données par caractère. Vous pouvez sélectionner 7 bits ou 8 bits, Linux utilise le jeu de caractères ASCII qui exige au moins sept bits. Il est recommandé d'utiliser au moins huit bits; cela permet même à des textes non-anglais d'être facilement transmis.
    - **Contrôle du flux :** Sélectionnez un type de contrôle de flux. Le contrôle du flux régule le flux de caractères. **XON/XOFF (Logiciel), RTS/CTS (Matériel) et DTR/DSR (Matériel)** sont les options fournies. Sélectionnez **Par défaut** pour désactiver le contrôle de débit.
7. Cliquez sur **Faire suivre**. La fenêtre **Choisir Pilote** s'affiche.
8. Choisissez le pilote à partir de l'une des options suivantes :
    - Sélectionner l'imprimante à partir de la base de données.
    - Fournir fichier PPD.
    - Rechercher un pilote d'imprimante à télécharger.
9. Une fois l'imprimante ajoutée, vous pouvez imprimer une page de test.

Ajouter une Imprimante réseau

Si une imprimante réseau est connectée à votre réseau. Vous pouvez configurer et utiliser cette imprimante. Pour ajouter une imprimante réseau :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Périphériques**, puis cliquez sur **Imprimante**. La fenêtre **Imprimante** s'affiche.
4. Cliquez sur **Ajouter**. La fenêtre **Sélectionner périphérique** s'affiche.

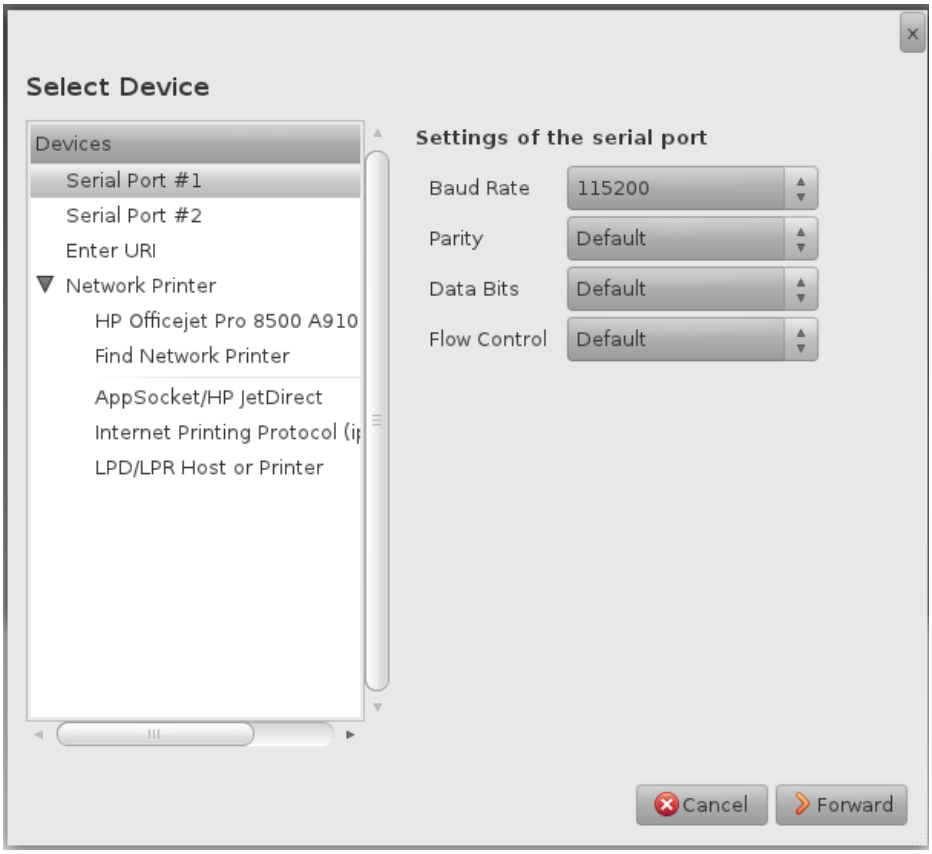

Figure 4-3 : Ajouter une Imprimante réseau

5. Cliquez sur **Imprimante réseau** pour effectuer les options suivantes .
   - Se connecter à une imprimante sur le réseau.
   - Trouver et se connecter à une imprimante réseau.
   - Se connecter à l'imprimante App Socket/HP Jetdirect.
   - Se connecter à une imprimante via IPP (Internet Printing Protocol).
   - Se connecter à un hôte ou une imprimante LDP/LPR.
   - Se connecter à une imprimante Windows via SAMBA
6. Une fois l'imprimante ajoutée, vous pouvez imprimer une page de test.

Éditer les Propriétés de l'imprimante

Pour modifier les propriétés d'une imprimante, dans la fenêtre **Imprimante** sélectionnez une imprimante, cliquez sur **Propriétés.**

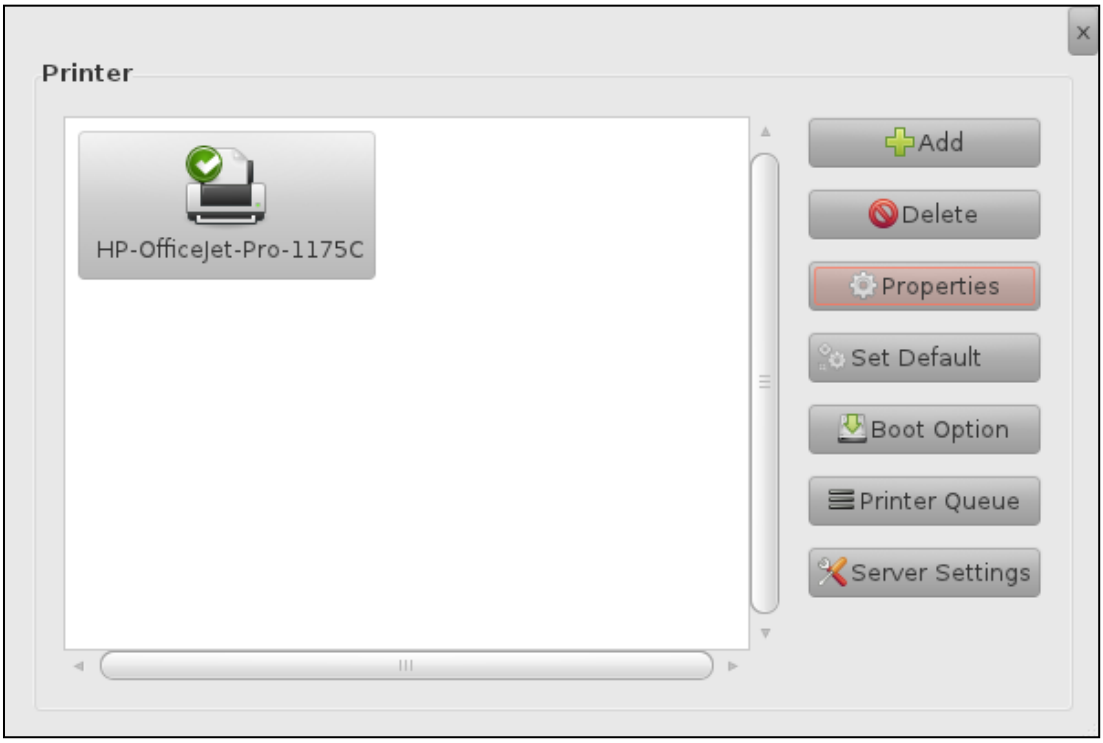

Figure 4-4 : Option des Propriétés

Vous pouvez éditer les options suivantes :

Paramètres

1. Cliquez sur **Paramètres** pour modifier les paramètres de base de l'imprimante.
2. Dans le champ Description, saisissez la description de l'imprimante.
3. Dans le champ **Emplacement**, saisissez l'emplacement où est installée l'imprimante.
4. Dans le champ **URI du périphérique**, saisissez l'URI où est installé le périphérique. *Par exemple, série : /dev/ttys0?baud=115200.*
5. Dans le champ **Marque et Modèle**, saisissez la marque et le modèle de l'imprimante.
6. Dans le champ **Statut de l'imprimante**, saisissez le statut présent de l'imprimante.
7. Pour imprimer une page de test, cliquez sur l'icône **Imprimer page de test**.
8. Pour imprimer une page de test automatique, cliquez sur l'icône **Imprimer page de test automatique**.
9. Pour nettoyer les têtes d'impression de cette imprimante, cliquez sur **Nettoyer les têtes d'impression**.

Polices

1. Cliquez sur **Polices** pour modifier les polices d'impression applicables à cette imprimante.

2. Sélectionnez **Activé** pour permettre à l'imprimante d'imprimer des documents et des fichiers.
3. Sélectionnez **Accepter les travaux** pour permettre à l'imprimante de prendre des nouveaux travaux d'impression à partir du spouleur.
4. Sélectionnez **Partagée** pour partager cette imprimante sur le réseau.

Options de tâche

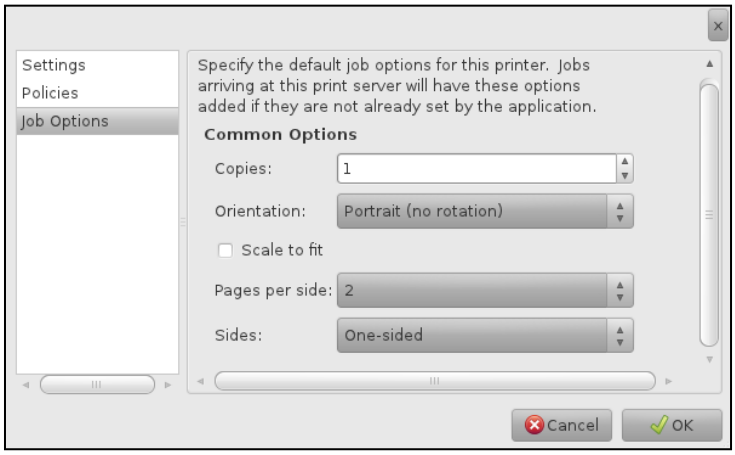

Figure 4-5 : Options de tâche de l'imprimante

1. Cliquez sur **Options de tâche** pour modifier la configuration de la page et les options de tâche. Les tâches qui arrivent dans cette imprimante auront ces options si elles ne sont pas déjà définies par l'application.
2. Dans la zone de sélection numérique **Copie**s, sélectionnez le nombre de copies à imprimer.
3. Dans la zone de sélection numérique **Orientation**, sélectionnez l'orientation souhaitée **Portrait** , **Paysage**, **Paysage inversé** ou **Portrait inversé**.
4. Sélectionnez l'option **Mettre à l'échelle** pour redimensionner le document ou le fichier à la taille du papier présent dans l'imprimante. Vous pouvez imprimer jusqu'à 16 pages par côté.
5. Dans la zone de sélection numérique **Pages par côté**, sélectionnez le nombre de pages à imprimer par côté.
6. Dans la zone de sélection numérique **Côtés**, sélectionnez si vous souhaitez que l'imprimante imprime **Recto**, **Recto-verso (bord long)** ou **Recto-verso (bord court)**.

Configurer l'imprimante par défaut

Pour configurer l'imprimante par défaut :

1. Sélectionnez l'imprimante que vous voulez affecter par défaut.
2. Cliquez sur **Définir par défaut**

Remarque : L'imprimante par défaut va prendre les travaux l'impression à partir du spouleur sauf si spécifié autrement, à partir de l'application de l'utilisateur.

Option de démarrage

La fenêtre d'option de démarrage vous permet de définir les options du pilote de l'imprimante. Les trois options disponibles sont les suivantes :

- Détecter automatiquement : Le pilote de l'imprimante sera automatiquement détecté. Cette option est sélectionnée par défaut.
- Charger Standard LPT au moment du démarrage (pour USB vers un Parallèle Utilisez cette option pour une imprimante LPT.
- Charger le pilote de l'imprimante USB au moment du démarrage : Utilisez cette option si l'imprimante USB n'est pas détectée automatiquement.

Pour connecter une imprimante LPT :

1. Connectez l'imprimante LPT.
2. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
3. Cliquez sur la flèche déroulante **Paramètres locaux**.
4. Cliquez sur **Périphériques**, puis cliquez sur **Imprimante**. La fenêtre **Imprimante** s'affiche.
5. Cliquez sur **Option de démarrage**. La fenêtre des options du pilote de l'imprimante s'affiche**.**

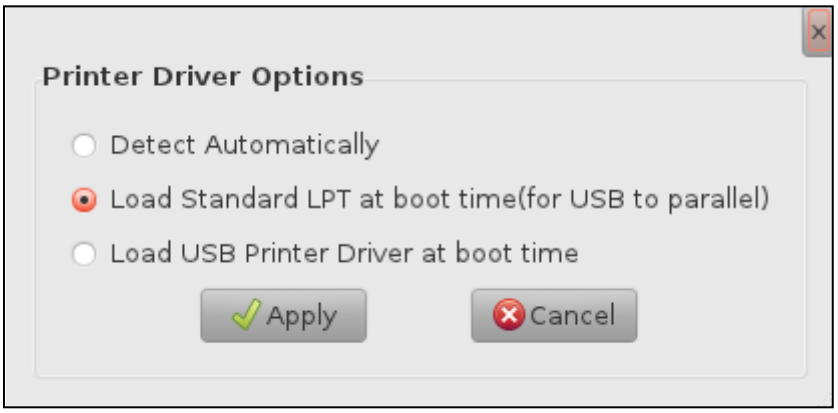

Figure 4-6 : Charger Standard LPT au moment du démarrage

6. Sélectionnez Charger **Standard LPT au moment du démarrage (pour USB vers parallèle),** cliquez sur **Appliquer**.
7. Redémarrez le client
8. Cliquez sur **Paramètres locaux > Périphériques >Imprimante** > **Ajouter.**

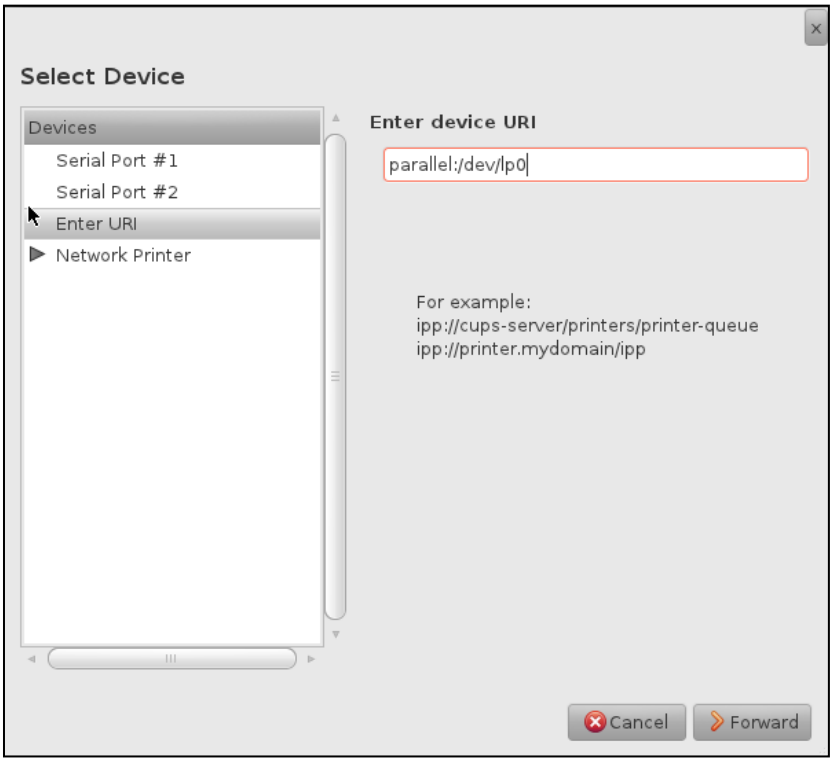

Figure 4-7 : Saisir l'URL

9. Cliquez sur **Saisir l'URL** .
10. Dans le champ **Saisir l'URL du périphérique** saisissez *parallel:/dev/lp0.*
11. Cliquez sur **Avancer** jusqu'à ce que l'écran ci-dessous apparaisse.

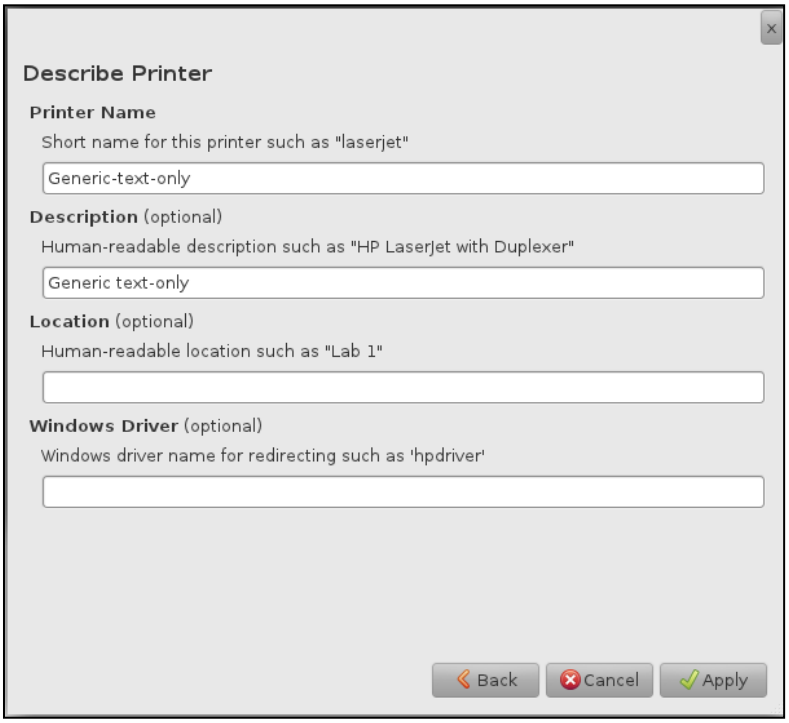

Figure 4-8 : Nom du pilote Windows

12. Dans le champ **Pilote Windows**, saisissez le nom du pilote Windows.

13. Cliquez sur **Appliquer**.

Pour connecter une imprimante USB qui n'est pas détectée automatiquement :

1. Connectez l'imprimante USB.
2. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
3. Cliquez sur la flèche déroulante **Paramètres locaux**.
4. Cliquez sur **Périphériques**, puis cliquez sur **Imprimante**. La fenêtre **Imprimante** s'affiche.
5. Cliquez sur **Option de démarrage**. La fenêtre des options du pilote de l'imprimante s'affiche**.**

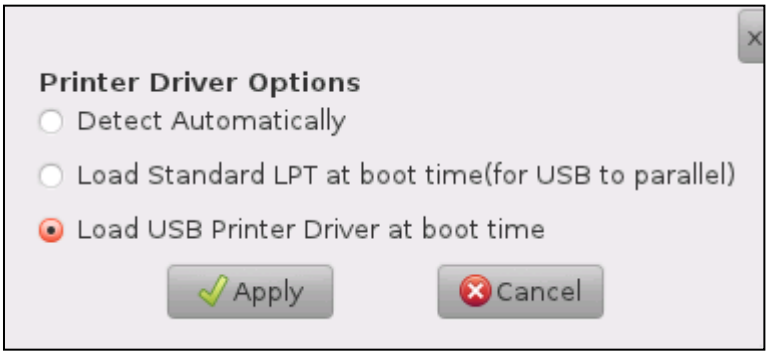

Figure 4-9 : Charger le pilote de l'imprimante USB au moment du démarrage

6. Sélectionnez **Charger le pilote de l'imprimante USB au moment du démarrage,** cliquez sur **Appliquer**
7. Redémarrez le client
8. Cliquez sur **Paramètres locaux > Périphériques >Imprimante** > **Ajouter.**

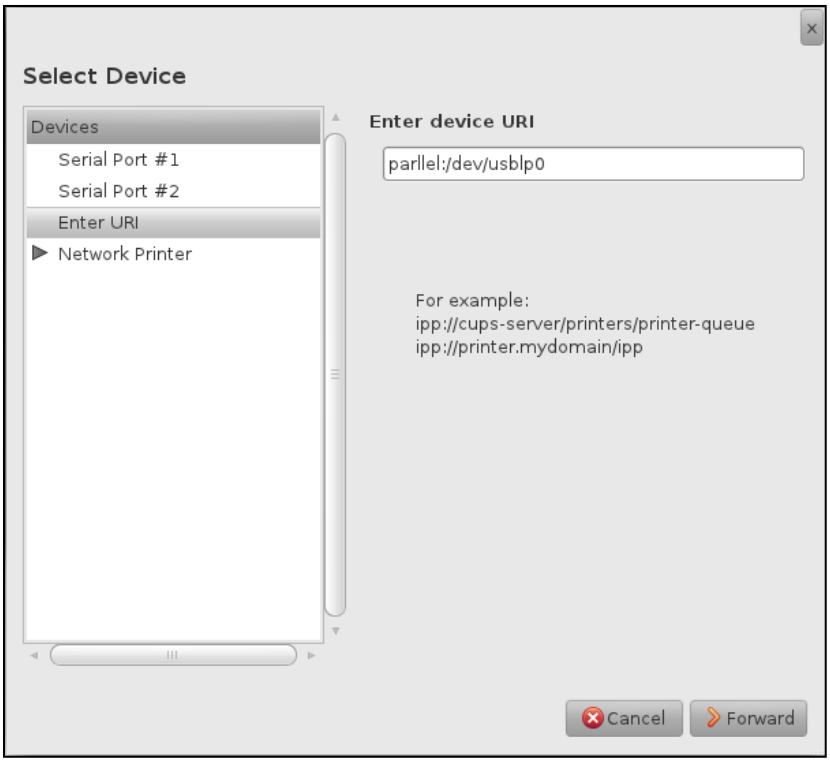

Figure 4-10 : Saisir l'URL

9. Cliquez sur **Saisir l'URL** .
10. Dans le champ **Saisir l'URL du périphérique** saisissez *parallel:/dev/usblp0.*
11. Cliquez sur **Avancer** jusqu'à ce que l'écran ci-dessous apparaisse.

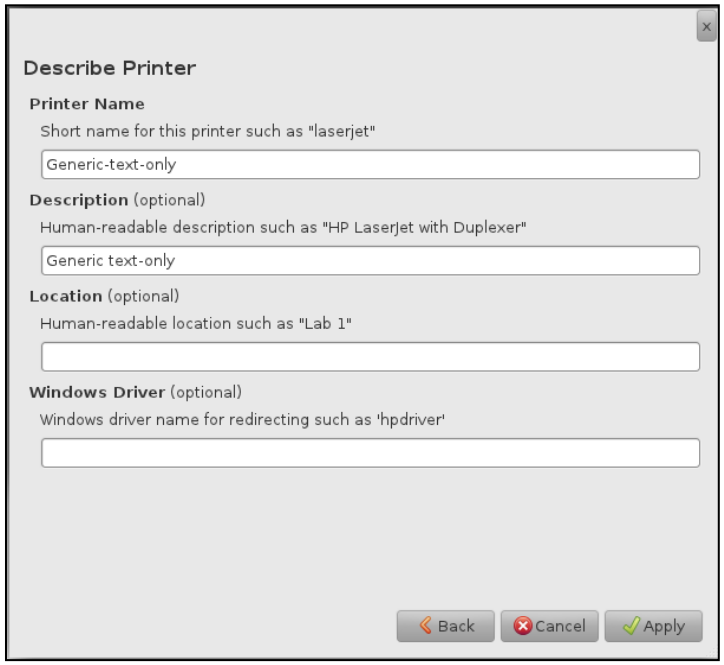

Figure 4-11 : Nom du pilote Windows

12. Dans le champ **Pilote Windows**, saisissez le nom du pilote Windows.
13. Cliquez sur **Appliquer**.

File d'attente de l'imprimante

La file d'attente de l'imprimante affiche les travaux d'impression actifs avec l'utilisateur, le document, l'imprimante, la taille, l'heure à laquelle il a été soumis et les informations sur le statut.

La fenêtre de la file d'attente de l'imprimante vous permet d'effectuer les tâches suivantes :

- Actualiser la liste des travaux.
- Afficher les travaux d'impression terminés.
- Annuler un travail d'impression.
- Arrêter le processus d'impression.
- Reprendre le processus d'impression.

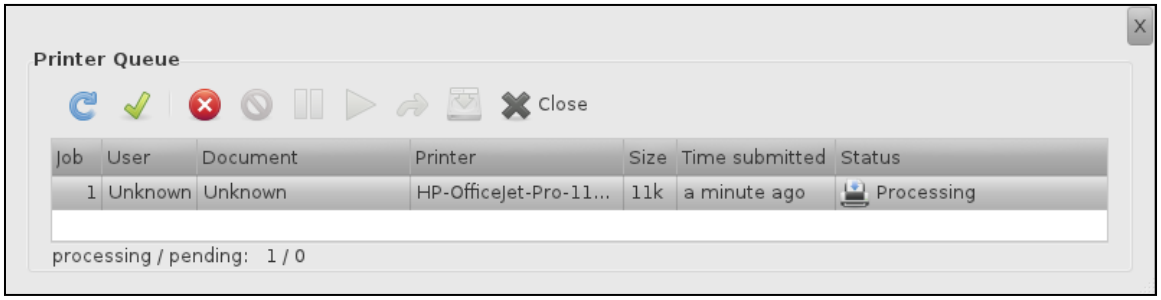

Figure 4-12 : File d'attente de l'imprimante

Paramètres du serveur

La fenêtre des paramètres du serveur vous permet de configurer un client sur le réseau en tant que serveur d'impression.

Pour configurer un client en tant que serveur d'impression :

1. Dans la fenêtre de l'**Imprimante**, cliquez sur **Paramètres du serveur**.
2. Sélectionnez **Publier imprimantes partagées connectées à ce système** .

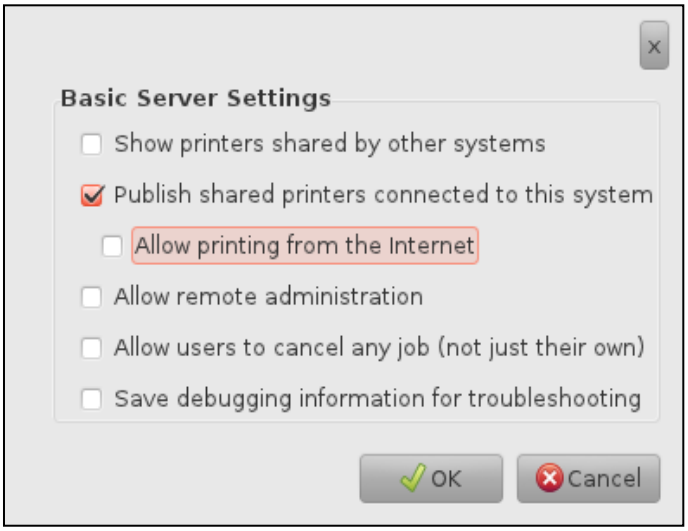

Figure 4-13 : Paramètres du serveur

3. Sélectionnez les options suivantes si nécessaire :

- Afficher les imprimantes partagées par d'autres systèmes.
- Autoriser l'impression à partir d'Internet.
- Autoriser l'administration à distance
- Autoriser les utilisateurs à annuler tout travail
- Enregistrer les informations de débogage pour le dépannage.

4. Cliquez sur **OK**.

Pour connecter un client au serveur d'impression :

1. Dans le client, cliquez sur **Paramètres locaux**>**Périphériques>Imprimante**>**Ajouter.**

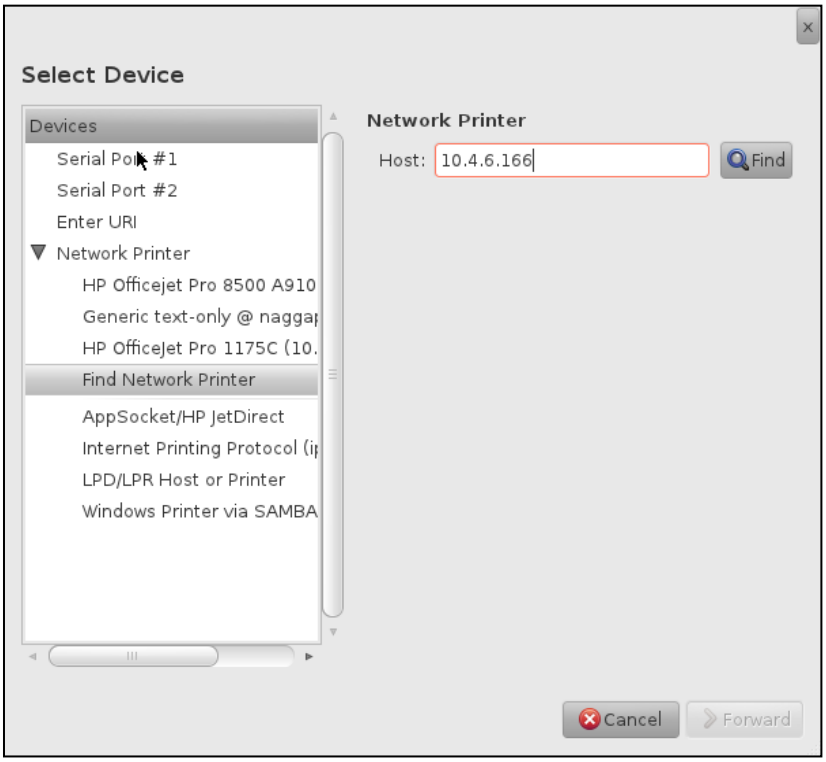

Figure 4-14 : Nom d'hôte du serveur d'impression

2. Cliquez sur **Rechercher l'imprimante réseau**
3. Dans le champ **Hôte** saisissez le nom d'hôte ou l'adresse IP du serveur d'impression et cliquez sur **Rechercher**. La fenêtre suivante s'affiche.

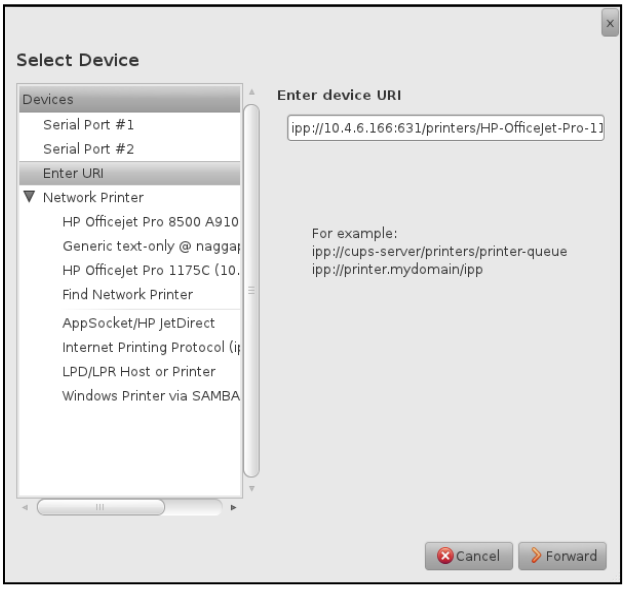

Figure 4-15 : URL du périphérique

4. Cliquez sur Saisir l'URL et cliquez sur **Suivant**.
5. Continuez à cliquer sur **Suivant** jusqu'à ce que la configuration soit terminée, puis cliquez sur **Appliquer**.

Affichage

L'option d'affichage vous permet de définir les propriétés d'affichage.

Pour définir les propriétés d'affichage :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Affichage**. La fenêtre **Affichage** s'affiche.

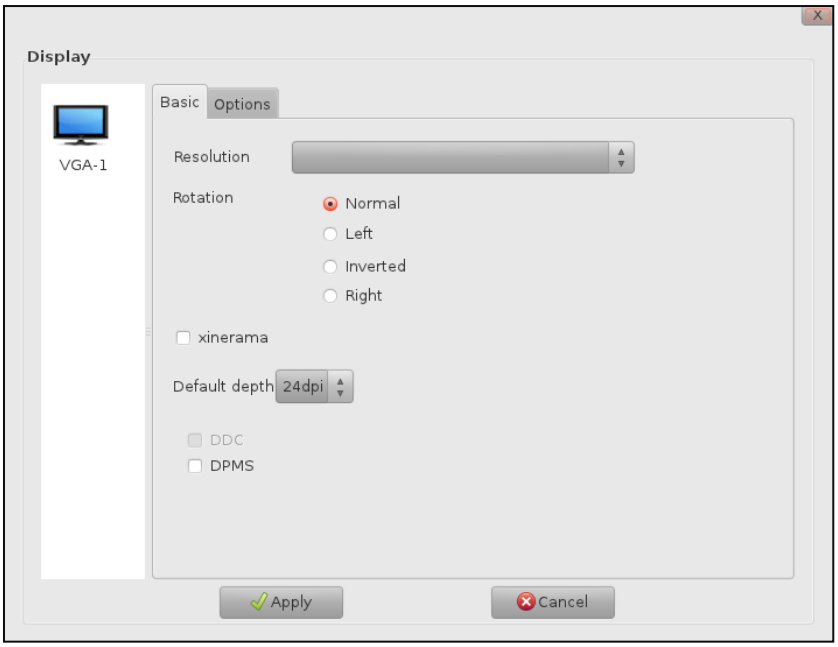

Figure 4-16 : Fenêtre d'affichage

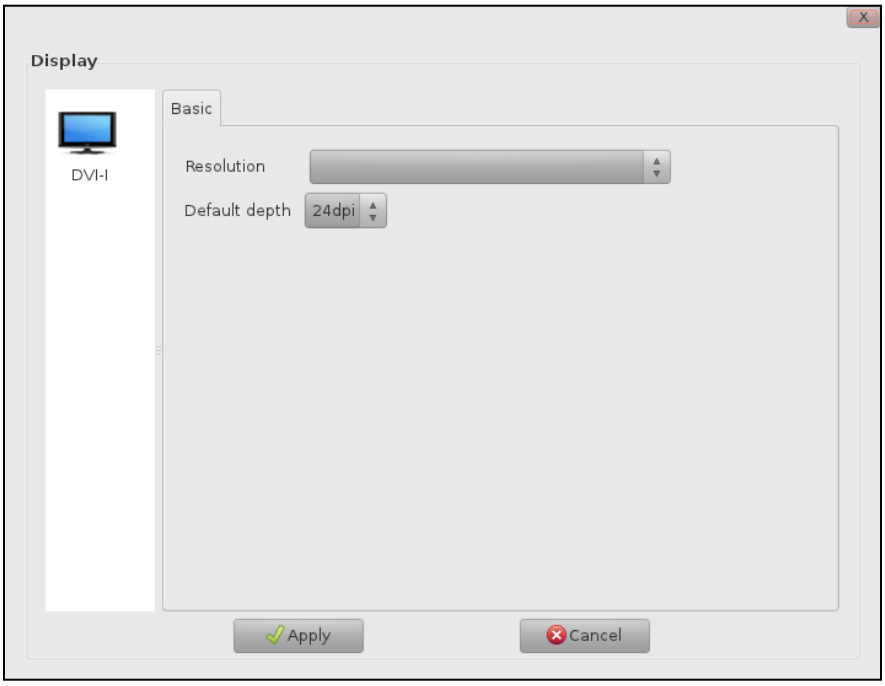

Figure 4-17 : Fenêtre d'affichage pour Gio 5 K Series et système d'exploitation du PC GIO

4. Dans la section **Affichage**, sélectionnez le moniteur requis.
5. Cliquez sur l'onglet **Basique** et saisissez les valeurs pour les champs suivants :
   - Résolution : Sélectionnez la résolution requise.
   - Rotation : Sélectionnez le type de rotation (gauche, droite, inversé, normal).
   - xinerama : Sélectionnez cette option pour utiliser deux ou plusieurs écrans physiques en un seul grand écran virtuel.
   - Profondeur par défaut : Sélectionnez la profondeur par défaut.
   - DDC : Sélectionnez si vous souhaitez utiliser le protocole d'affichage du canal d'affichage des données, il définit les règles de communication entre la carte graphique et l'écran du client.
   - DPMS : Sélectionnez cette option pour activer gestion de l'alimentation de la carte graphique.

     Remarque : Les options Rotation, xinerama, DDC et DPMS ne sont pas disponibles pour le
     Gio 5 K Series et système d'exploitation du PC GIO.
6. Cliquez sur l'onglet **Options**.

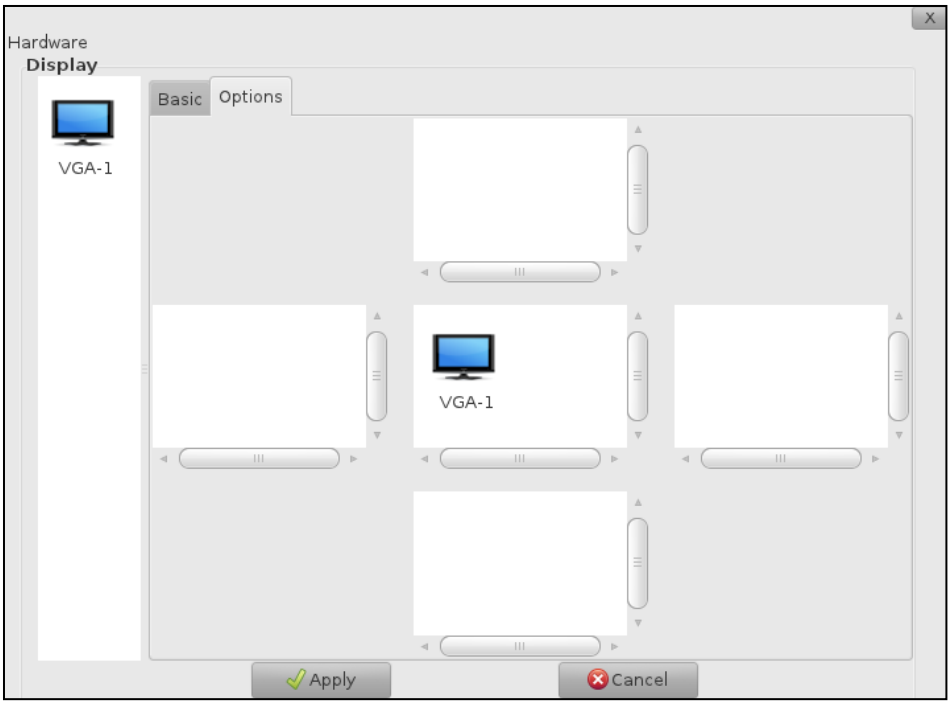

Figure 4-18 : Options d'affichage

Remarque : L'onglet **Options** n'est pas disponible pour le Gio 5 K Series et système d'exploitation du PC GIO.

7. Lorsque deux écrans sont connectés, cliquez et faites glisser l'icône du moniteur pour définir la rotation.
8. Cliquez sur **Appliquer**. La boîte de dialogue de **Confirmation** s'affiche.

9. Cliquez sur **Oui**.

Paramètres du système

L'option Paramètres du système vous permet de configurer les propriétés suivantes du système :

- Langue
- Date et heure
- Apparence

Langue

Pour définir la langue du système :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Paramètres du système > Langue**. La fenêtre **Langue** s'affiche.

Figure 4-19 : Langue

4. Sélectionnez la langue requise, puis cliquez sur **Définir par défaut.**

Date et heure

Pour configurer l'heure et la date, vous pouvez sélectionner un fuseau horaire, spécifiez un serveur NTP ou la saisir manuellement. Vous pouvez configurer l'heure et la date dans la fenêtre **Date et heure**.

Pour afficher la fenêtre **Date et heure** :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Paramètres du système > Date et heure** . La fenêtre **Date et heure** s'affiche.

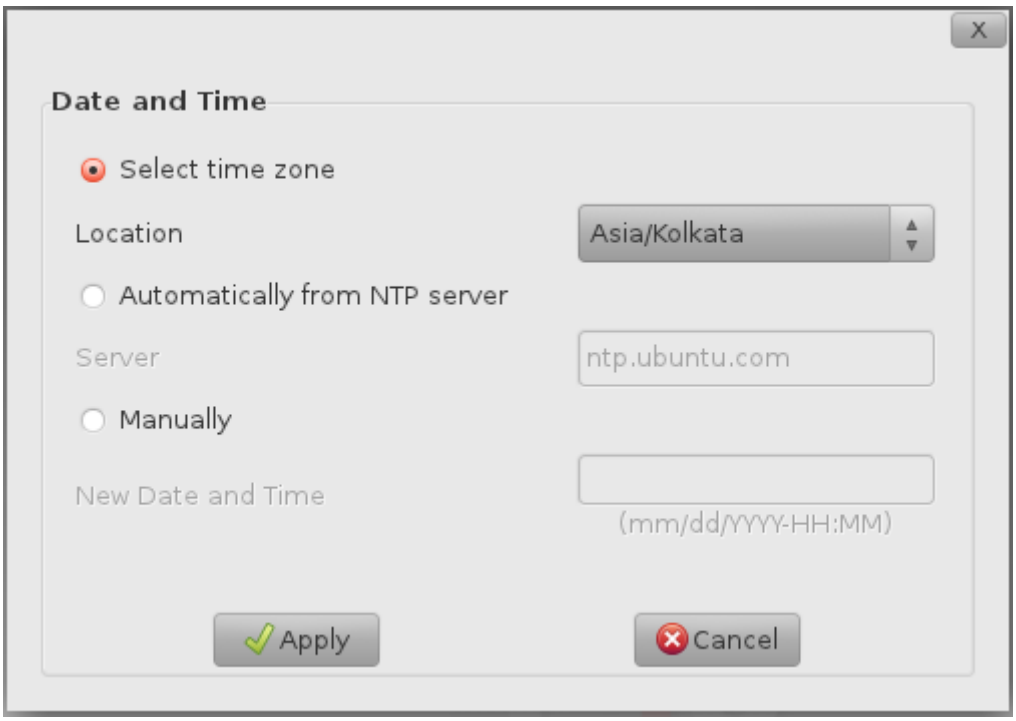

Figure 4-20 : Définir Date et heure

Fuseau horaire

Un *fuseau horaire* est une région géographique qui a un horaire uniforme pour des raisons juridiques, commerciales, sociales.

Pour configurer l'heure en utilisant le fuseau horaire :

1. Dans la fenêtre **Date et Heure**, sélectionnez l'option **Sélectionner fuseau horaire.**
2. Dans le champ **Emplacement**, sélectionnez l'emplacement du fuseau horaire souhaité.
3. Cliquez sur **Appliquer**. La boîte de dialogue de **Confirmation** s'affiche.
4. Cliquez sur **Oui**.

Serveur NTP

NTP est un protocole internet utilisé pour synchroniser les horloges des ordinateurs à une heure de référence.

Pour configurer l'heure en utilisant le serveur NTP :

1. Dans la fenêtre **Date et Heure**, sélectionnez l'option **Automatiquement à partir du serveur NTP.**
2. Dans le champ **Serveur**, saisissez l'URL du serveur NTP.
3. Cliquez sur **Appliquer**. La boîte de dialogue de **Confirmation** s'affiche.
4. Cliquez sur **Oui**.

Configuration manuelle

Vous pouvez saisir manuellement la date et l'heure dans le format mm/jj/aaaa et hh:mm.

Pour saisir manuellement la date et l'heure :

1. Dans la fenêtre **Date et Heure**, sélectionnez l'option sélectionner **Manuellement.**
2. Dans le champ **Nouvelle date et heure**, saisissez mm/dd/yyy-HH:MM.
3. Cliquez sur **Appliquer**. La boîte de dialogue de **Confirmation** s'affiche.
4. Cliquez sur **Oui**.

Apparence

Vous pouvez modifier l'image d'arrière-plan du bureau et configurer l'économiseur d'écran en utilisant cette option :

Pour modifier l'image d'arrière-plan du bureau :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Paramètres du système > Apparence**. La fenêtre **Apparence** s'affiche.

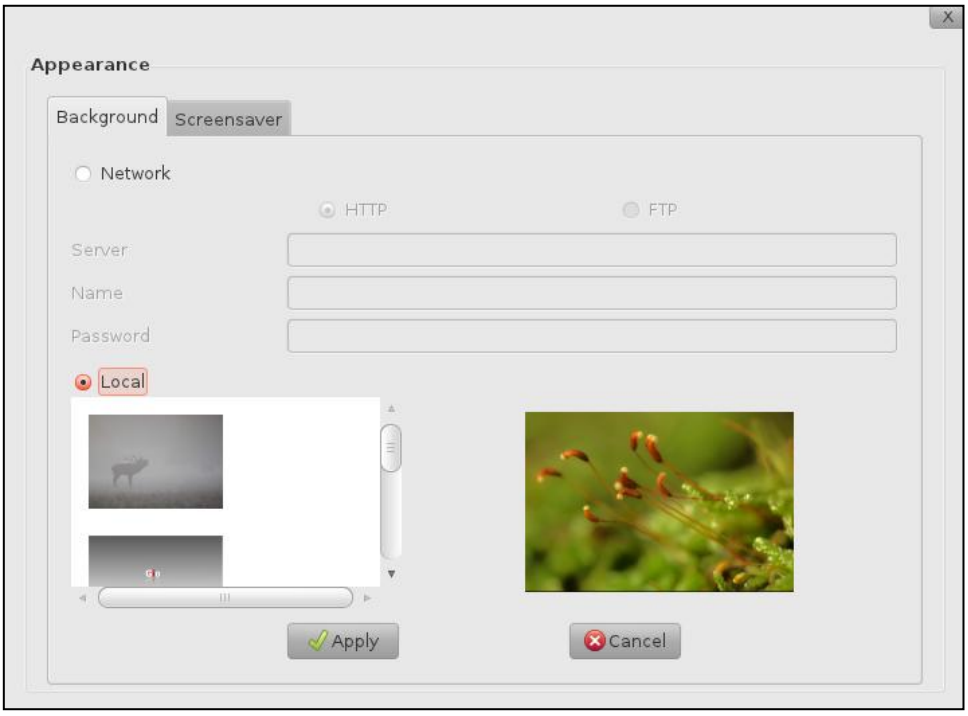

Figure 4-21 : Configurer Image d'arrière-plan

4. Cliquez sur l'onglet **Arrière-plan**.
5. Sélectionnez Réseau pour parcourir et choisissez une image à partir du serveur HTTP ou FTP.

   - Si vous sélectionnez **HTTP** : Dans le champ **Serveur**, saisissez l'adresse IP du serveur et le chemin de l'image.
   - Si vous sélectionnez **FTP :**

   a. Dans le champ **Serveur**, saisissez l'adresse IP du serveur et le chemin de l'image.

   b. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du serveur.

c. Dans le champ **Mot de passe**, saisissez le mot de passe du serveur.

6. Sélectionnez Local pour définir une image locale comme arrière-plan.
7. Cliquez sur **Appliquer**. La boîte de dialogue de **Confirmation** s'affiche.
8. Cliquez sur **Oui**.

Pour configurer l'économiseur d'écran

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Paramètres du système > Apparence**. La fenêtre **Apparence** s'affiche.
4. Cliquez sur l'onglet **Économiseur d'écran**.

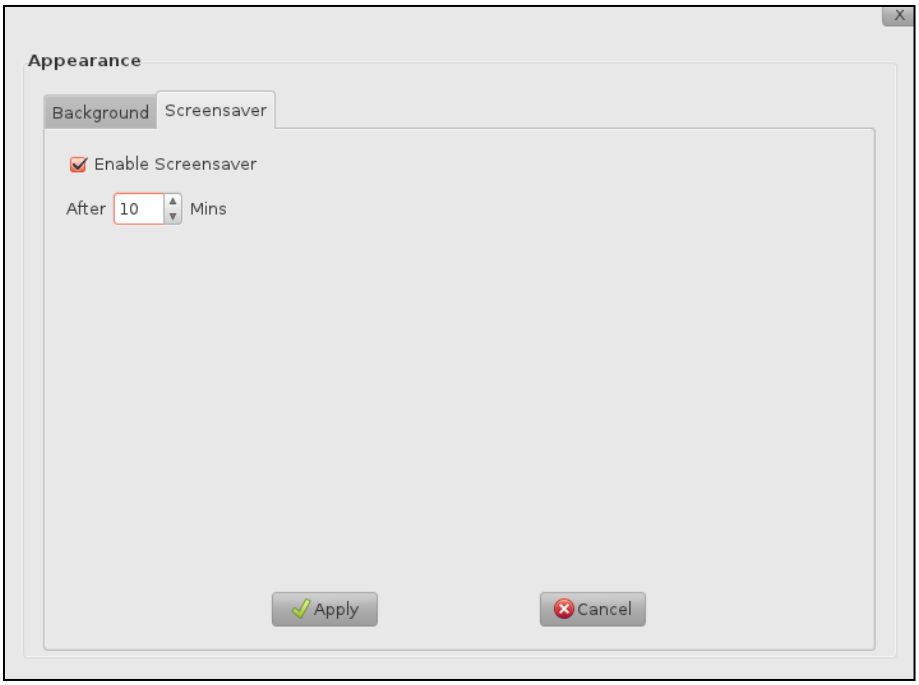

Figure 4-22 : Configurer l'économiseur d'écran

5. Sélectionnez **Activer l'économiseur d'écran**.
6. Définissez l'intervalle de temps en minutes au bout duquel l'économiseur d'écran apparaît.
7. Cliquez sur **Appliquer**.

Mise à niveau du micrologiciel

L'option de mise à niveau du micrologiciel vous permet d'effectuer la mise à niveau du système d'exploitation du Gio5. Vous pouvez mettre à niveau le micrologiciel à partir d'un serveur FTP ou HTTP.

Pour la mise à niveau du micrologiciel à l'aide d'une URL :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez **Mise à jour du micrologiciel** La fenêtre **Mise à jour du micrologiciel** s'affiche.

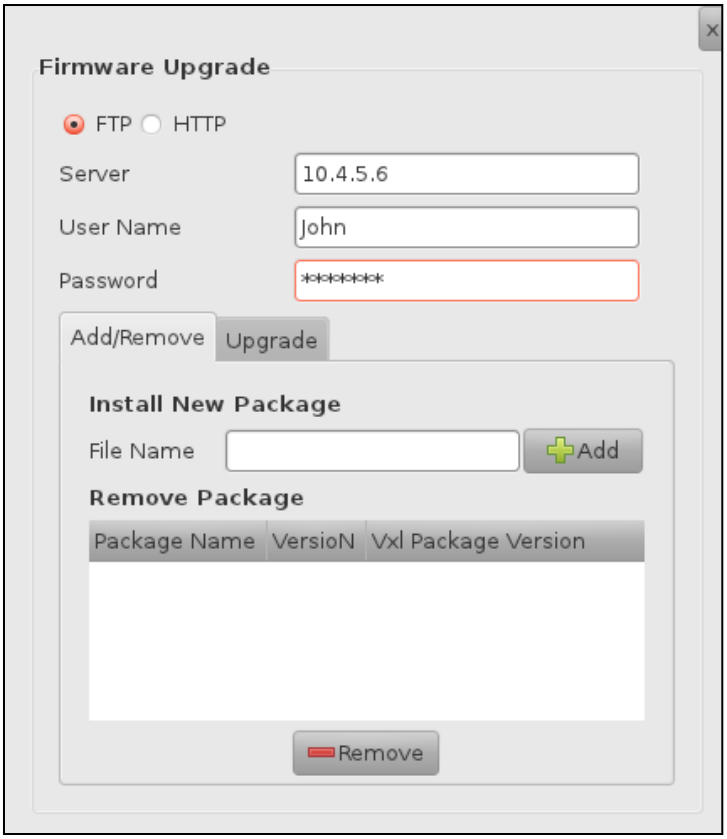

Figure 4-23 : Mise à niveau du micrologiciel

4. Sélectionnez le type de protocole (**FTP** ou **HTTP**).
5. Dans le champ **Serveur**, saisissez l'adresse IP du serveur dans laquelle la mise à niveau du micrologiciel est disponible.
6. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du serveur.
7. Dans le champ **Mot de passe**, saisissez le mot de passe du serveur.
8. Cliquez sur l'onglet **Ajouter/Supprimer**.
9. Dans le champ **Nom de fichier** saisissez le chemin d'accès et le nom de fichier du package.
10. Cliquez sur **Ajouter**.

Remarque : Pour supprimer un package, sélectionnez le package et cliquez sur Supprimer.

11. Cliquez sur l'onglet **Mise à jour**.
12. Sélectionnez le package requis et cliquez sur **Mise à jour**.

Comptes d'utilisateur

L'option Comptes d'utilisateurs vous permet de gérer les comptes utilisateur et les groupes.

Vous pouvez ajouter un nouvel utilisateur ou un groupe ou supprimer un utilisateur ou un groupe existant.

Pour ajouter un nouvel utilisateur :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur Comptes d'utilisateur. La fenêtre **Utilisateurs et Groupe** s'affiche.

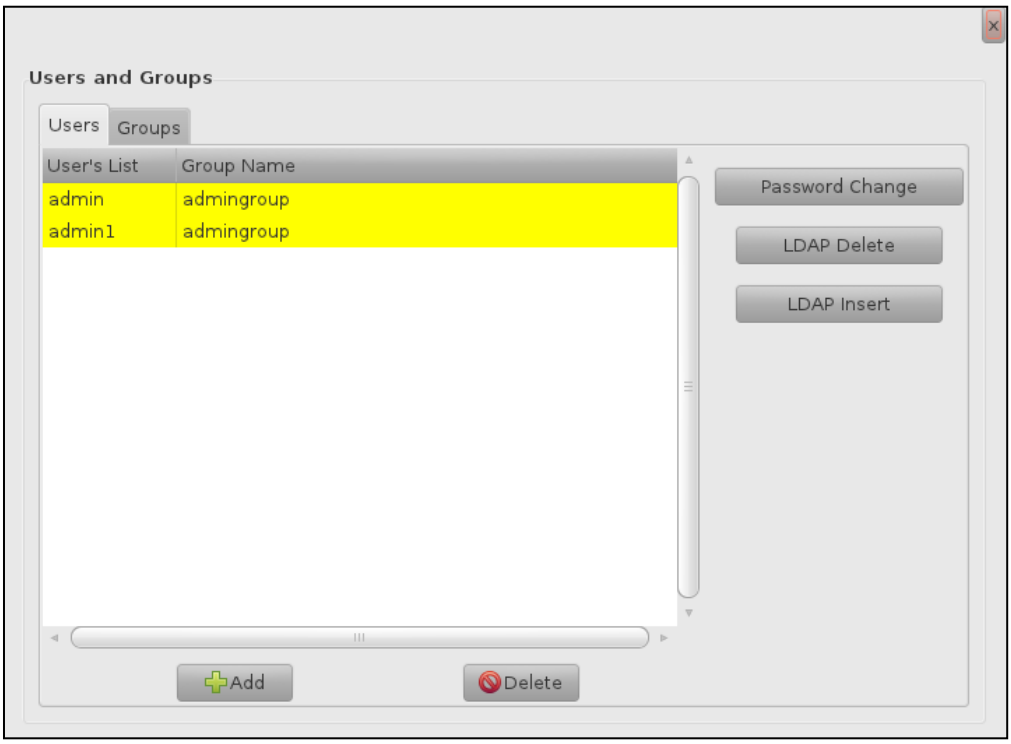

Figure 4-24 : Utilisateurs et groupes

4. Cliquez sur **Ajouter**. La fenêtre **Nouvel utilisateur** s'affiche.
5. Saisissez des valeurs pour les champs suivants :
   - **Nom d'utilisateur** : Saisissez un nom d'utilisateur.
   - **Mot de passe :** Saisissez un mot de passe.
   - **Retaper le mot de passe** : Confirmez le mot de passe en le ressaisissant le mot de passe.
   - **Nom du groupe** : Sélectionnez un groupe.
6. Cliquez sur **OK**.

Pour supprimer un compte d'utilisateur existant :

1. Dans la fenêtre **Utilisateurs et groupes**, sélectionnez l'utilisateur à supprimer.
2. Cliquez sur **Supprimer**. Un message de confirmation s'affiche. Cliquez sur **Oui**.

Pour modifier le mot de passe de l'utilisateur :

1. Sélectionnez un utilisateur particulier et cliquez sur **Modifier le mot de passe**.
2. Dans le champ **Mot de passe actuel**, saisissez un mot de passe actuel.
3. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe.
4. Dans le champ **Confirmation**, ressaisissez le nouveau mot de passe.
5. Cliquez sur **OK**.

Pour créer LDAP :

Lightweight Directory Access Protocol (LDAP) est un protocole d'application pour l'accès et le maintien des informations du répertoire. Cette option vous permet de rechercher des utilisateurs et des groupes dans un domaine particulier.

1. Dans la fenêtre **Utilisateurs et Groupes**, cliquez sur Insérer **LDAP**. La boîte de dialogue de Insérer **LDAP** s'affiche.

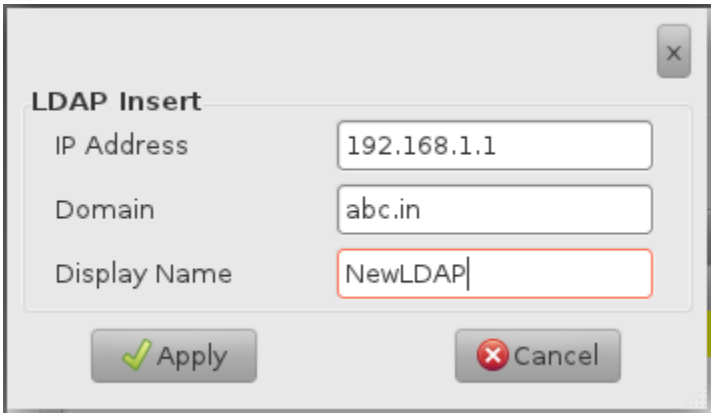

Figure 4-25 : Configurer LDAP

2. Dans le champ **Adresse IP**, saisissez l'adresse IP.
3. Dans le champ **Domaine**, saisissez le nom du domaine.
4. Dans le champ **Nom de l'affichage**, saisissez le nom de l'affichage.
5. Cliquez sur **Appliquer**. Un message de confirmation s'affiche, cliquez sur **Oui**.

Pour supprimer un LDAP :

1. Dans la fenêtre **Utilisateurs et Groupes**, cliquez sur supprimer **LDAP**. La fenêtre **supprimer LDAP** s'affiche.
2. Sélectionnez un LDAP et cliquez sur **Supprimer**.

Pour ajouter un groupe :

1. Dans la fenêtre **Utilisateurs et Groupes**, cliquez sur l'onglet **Groupes**.
2. Cliquez sur **Ajouter**. La fenêtre **Groupe** s'affiche.

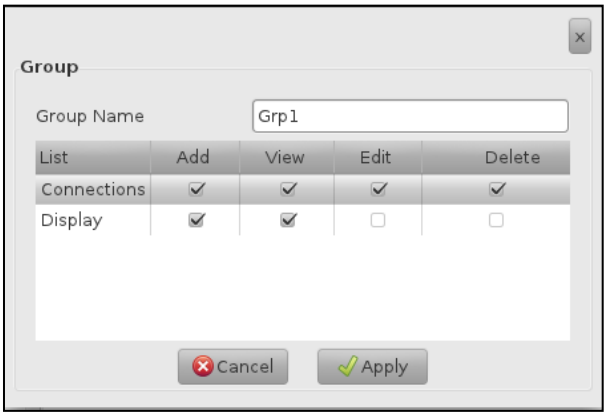

Figure 4-26 : Ajouter un groupe

3. Dans le champ **Nom du groupe**, saisissez le nom du groupe.
4. Sélectionnez les autorisations requises (**Ajouter**, **Afficher**, **Modifier ou supprimer)** et cliquez sur **Appliquer**.

Réinitialisation des paramètres d'usine

Cette option entraîne une réinitialisation des paramètres d'usine du logiciel et un redémarrage immédiat. Le réseau, l'écran, le clavier, la souris, le fuseau horaire, le compte utilisateur et les paramètres de langue du système sont réinitialisés.

Pour effectuer une réinitialisation d'usine:

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.
3. Cliquez sur **Restaurer les paramètres d'usine par défaut** La fenêtre de **Confirmation** s'affiche.

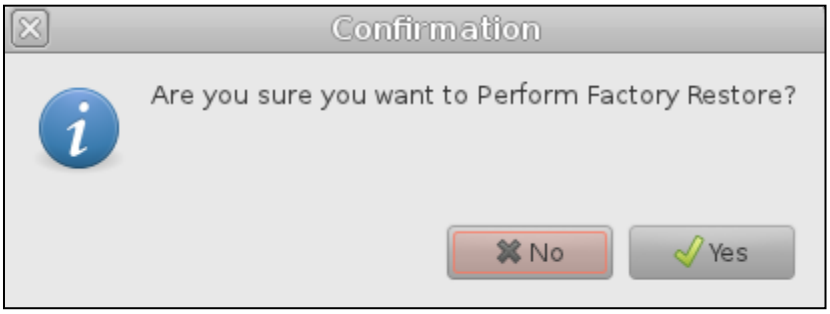

Figure 4-27 : Restaurer les paramètres d'usine

4. Cliquez sur **Oui**. Le système va redémarrer.

Verrouillage de l'écran

L'option de verrouillage d'écran vous permet de verrouiller votre écran chaque fois que nécessaire.

Pour verrouiller votre écran :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.

3. Cliquez sur **Verrouillage de l'écran.**

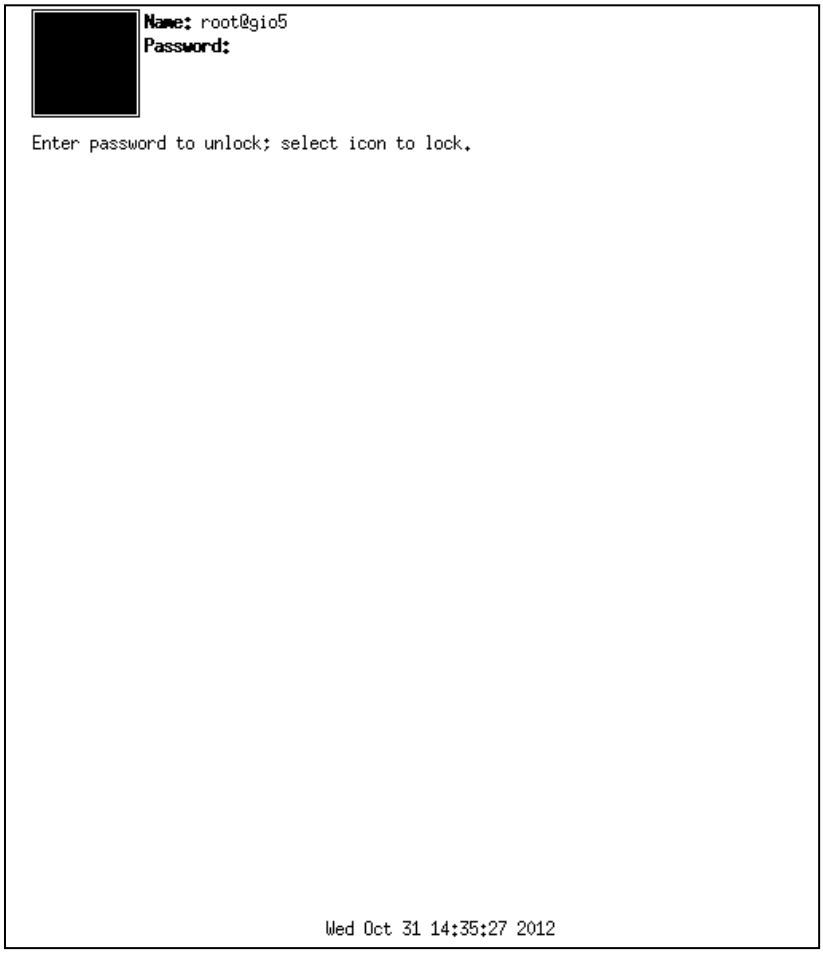

Figure 4-28 : Activer le verrouillage de l'écran

4. L'écran est maintenant verrouillé. Saisissez votre mot de passe, puis cliquez sur **Soumettre** pour déverrouiller l'écran.

Importer des certificats

Les certificats apportent une autre couche d'authentification pour une connexion. Des certificats de sécurité sont parfois nécessaires pour se connecter à des serveurs utilisant le protocole de cryptage SSL*. Par exemple, vous avez besoin d'un certificat pour vous connecter dans le cas d'une connexion Citrix WFCMGR qui utilise SSL.* Les certificats sont générés par le serveur et peuvent être importé vers votre client pour l'authentification.

Les certificats peuvent être importés à partir du réseau ou à partir du client local.

Pour importer des certificats à partir du client local :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.

3. Cliquez sur **Importer Certificats**. La boîte de dialogue **Certificats** s'affiche.

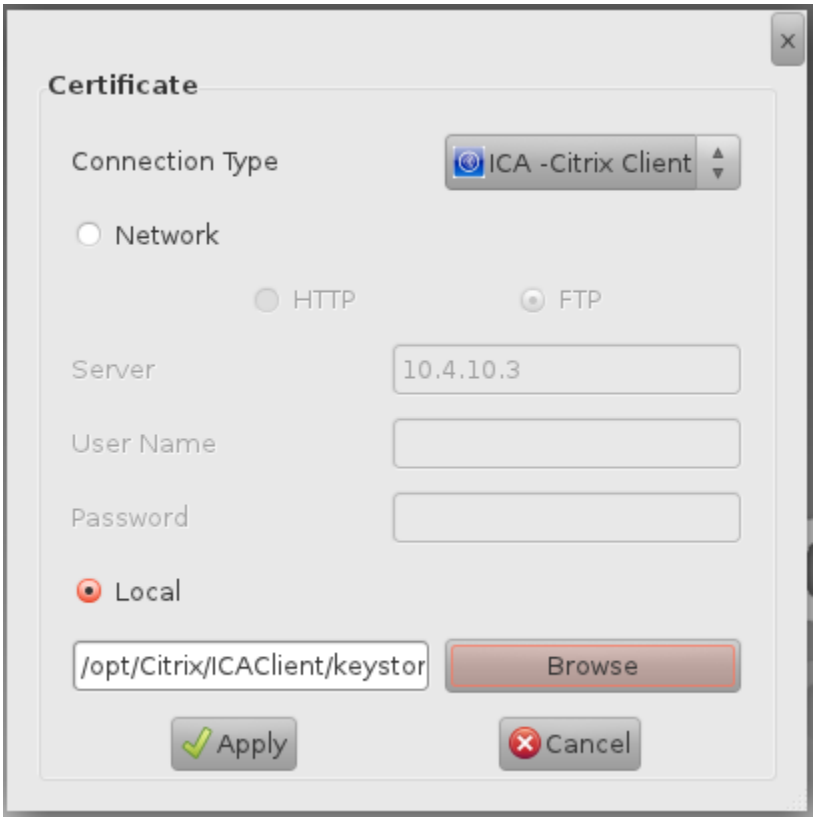

Figure 4-29 : Importer un certificat localement

4. Dans le champ **Type de connexion,** sélectionnez le type de connexion pour laquelle vous souhaitez importer les certificats.
5. Sélectionnez l'option Local.
6. Cliquez sur **Parcourir**, localisez et sélectionnez le certificat.
7. Cliquez sur **Appliquer**.

Pour importer des certificats à partir du réseau :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Paramètres locaux**.

3. Cliquez sur **Importer Certificats**. La boîte de dialogue **Certificats** s'affiche.

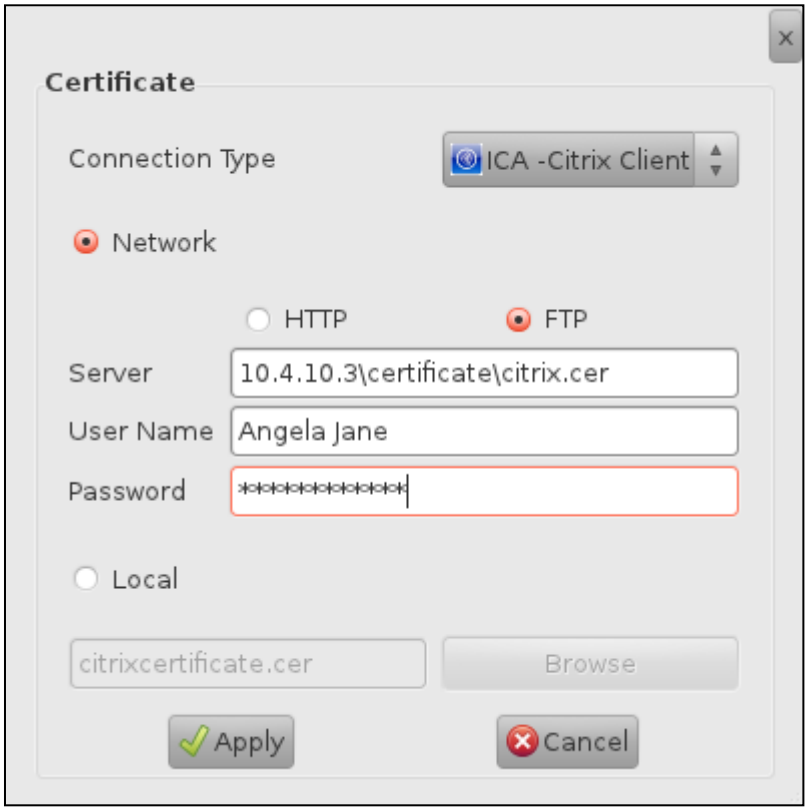

Figure 4-30 : Importer un certificat localement

4. Dans le champ **Type de connexion,** sélectionnez le type de connexion pour laquelle vous souhaitez importer les certificats.
5. Sélectionnez l'option **Réseau**.
6. Sélectionnez le type de serveur HTTP ou FTP.
   - Si vous sélectionnez **HTTP** : Dans le champ **Serveur**, saisissez l'adresse IP du serveur et le chemin du certificat.
   - Si vous sélectionnez **FTP :**

   d. Dans le champ **Serveur**, saisissez l'adresse IP du serveur et le chemin du certificat.

   e. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du serveur.

   f. Dans le champ **Mot de passe**, saisissez le mot de passe du serveur.
7. Cliquez sur **Appliquer**.

5 Sécurité

Le *Gio 5* offre des fonctionnalités de sécurité avancées pour veiller à ce que votre client est à l'abri de menaces et d'attaques. Vous pouvez sécuriser votre client léger en utilisant les services de gestion du serveur et les paramètres de proxy *du Gio 5*.

Services de gestion du serveur

Pour démarrer les services de gestion du serveur :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Sécurité**.
3. Cliquez sur **Gestion de serveur**, la fenêtre des **Paramètres du serveur** s'affiche.

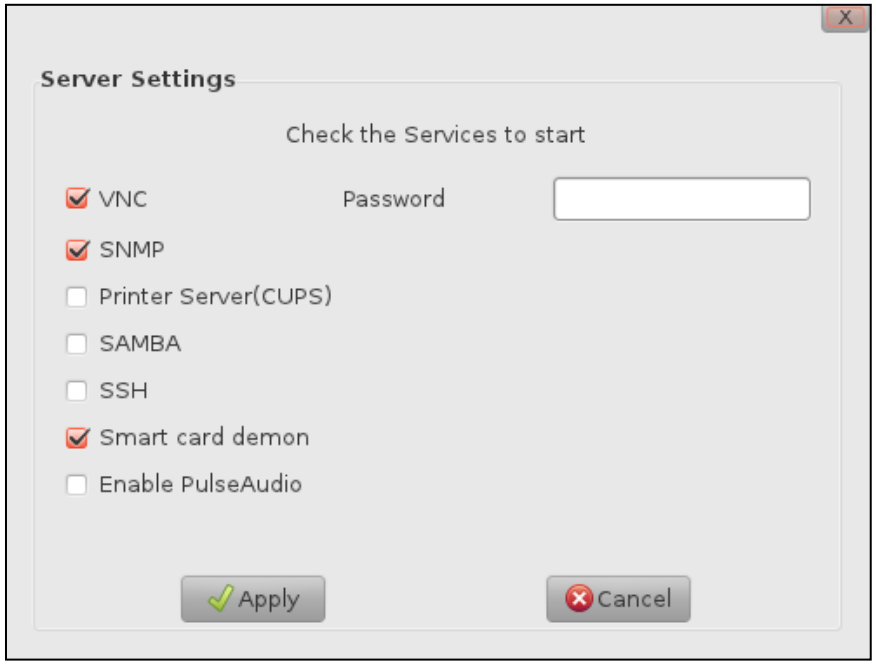

Figure 5-1 : Paramètres du serveur

4. Dans la liste suivante, sélectionnez les services à démarrer :

   - **VNC** : Virtual Network Computing (VNC) est un bureau graphique de système de partage qui utilise le protocole RFB (remote framebuffer) pour contrôler à distance un autre ordinateur. Dans le champ **Mot de passe**, saisissez un mot de passe pour VNC.
   - **SNMP** : Simple Network Management Protocol (SNMP) est un protocole qui permet de gérer les périphériques sur les réseaux IP. *Par exemple, les routeurs et les passerelles.*
   - **PrinterServer (CUPS)** : Common UNIX Printing System (CUPS) est le principal mécanisme d'impression de l'impression et les services d'impression Ubuntu.

- **SAMBA :** Samba est solution d'interopérabilité avec Windows disponible sur les systèmes Linux.
- **SSH :** Secure Socket Shell, est une commande d'interface UNIX et un protocole de connexion sécurisé pour avoir accès à un ordinateur distant.
- **Activer Pulse Audio :** Pulse Audio est un serveur de son du réseau multiplateforme POSIX.

5. Cliquez sur **Appliquer**, la fenêtre de confirmation s'affiche.
6. Cliquez sur **OK**.

Paramètres du serveur Proxy

Pour configurer les Paramètres du serveur Proxy :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Sécurité**.
3. Cliquez sur **Paramètres du serveur Proxy**, la fenêtre des **Paramètres du Proxy** s'affiche.

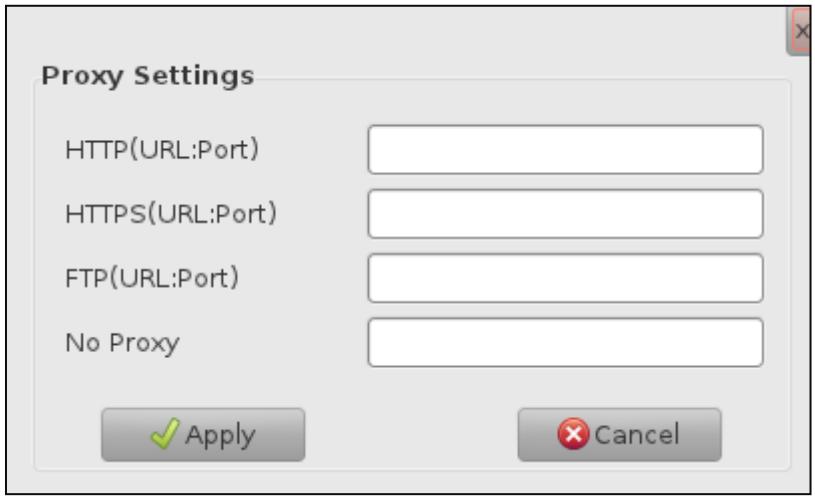

Figure 5-2 : Paramètres du serveur Proxy

4. Dans le champ **HTTP**, saisissez l'URL HTTP et le numéro de port.
5. Dans le champ **HTTPS**, saisissez l'URL et le numéro de port.
6. Dans le champ **FTP**, saisissez l'URL et le numéro de port.
7. Dans le champ **Aucun Proxy**, saisissez l'hôte local ou l'URL. Vous pouvez entrer plus d'une URL séparées par une virgule (,).

   Remarque : L'URL ou l'adresse IP spécifiée dans le champ **Aucun Proxy** ne se connectera pas via le serveur proxy.
8. Cliquez sur **Appliquer**. La boîte de dialogue confirmation s'affiche.
9. Cliquez sur **Oui**.

6 Diagnostic

La fonction de diagnostic vous permet d'afficher la mémoire et les informations sur l'état du réseau ; vous pouvez lancer les outils de mémoire et de diagnostic suivants :

Journal de la mémoire

Le journal de la mémoire fournit des informations sur la mémoire du système comme le stockage total, la mémoire libre et utilisée.

Pour accéder à l'outil du journal de la mémoire :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Diagnostic**.
3. Cliquez sur **Journal de mémoire**, la fenêtre **Utilisation du disque** s'affiche. L'état actuel de la mémoire s'affiche.

Figure 6-1 : Journal de la mémoire

Journal du réseau

Le journal de réseau vous permet d'exécuter des outils de diagnostic sur le réseau pour récupérer votre informations spécifiques sur le réseau.

Pour accéder à l'outil du journal du réseau :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Diagnostic**.
3. Cliquez sur **Journal du réseau**.
4. Sélectionnez l'un des outils suivants :
   - Ping et Trace route
   - DNS Lookup

Utiliser l'outil Ping et Trace route

Ping est un utilitaire d'administration du réseau informatique utilisé pour tester la disponibilité d'un hôte sur un réseau de protocole Internet (IP) et pour mesurer le temps d'aller-retour des messages envoyés à partir de l'hôte d'origine vers un ordinateur de destination. Traceroute est un outil de diagnostic de réseau de l'ordinateur pour afficher la voie (chemin) et mesurer des retards de paquets à travers un réseau de protocole Internet de transit.

Pour accéder à l'outil ping et traceroute :

1. Cliquez sur **Ping et Traceroute ,** la fenêtre **Ping et Traceroute** s'affiche.
2. Dans le champ **Adresse du réseau**, saisissez l'adresse réseau du nœud auquel vous souhaitez envoyer une commande ping.
3. Cliquez sur **Ping,** le résultat de la commande ping s'affiche dans la section **Statut du Ping**.

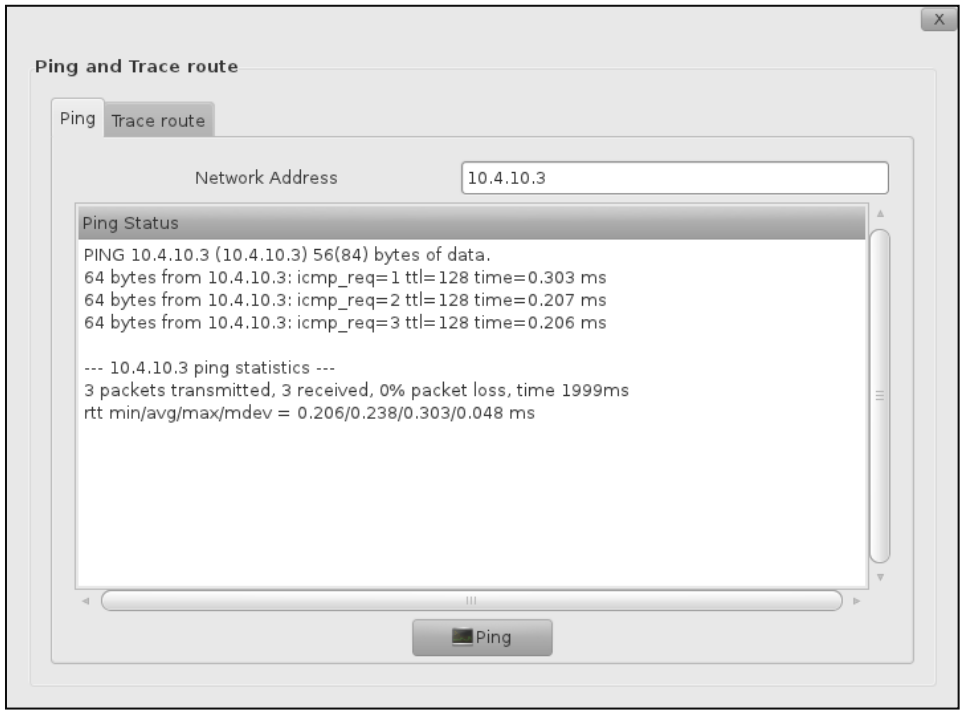

Figure 6-2 : Ping

4. Cliquez sur l'onglet **Trace route**.
5. Dans le champ **Adresse du réseau**, saisissez l'adresse réseau du nœud auquel vous souhaitez envoyer une commande Trace route.

6. Cliquez sur **Trace,** le résultat de la commande Trace s'affiche dans la section **Trace route**.

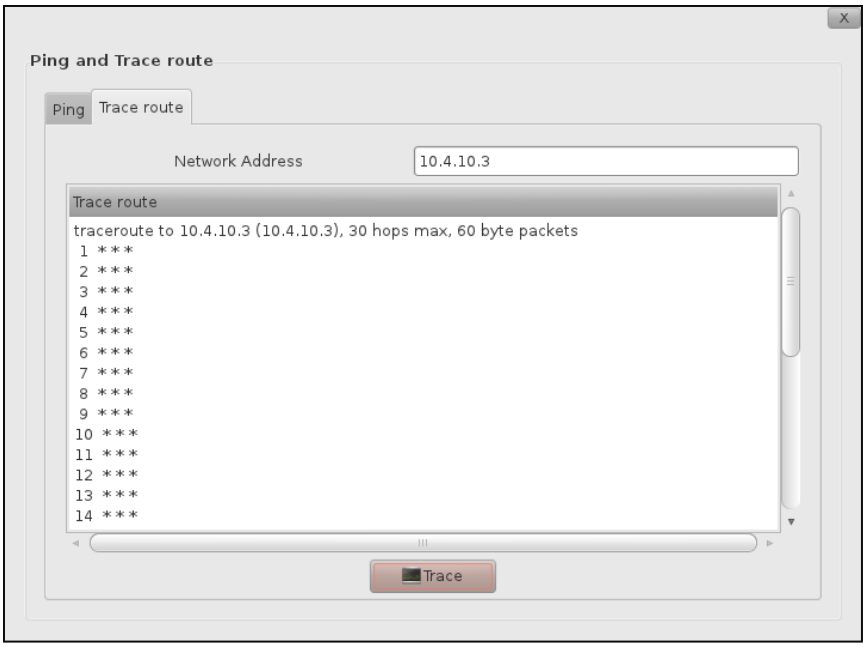

Figure 6-3 : Trace Route

Utiliser DNS Lookup

DNS lookup est un outil utilisé pour déterminer le nom du domaine d'une adresse IP. Pour accéder à l'outil DNS lookup :

1. Cliquez sur **DNS Lookup ,** la fenêtre **DNS Lookup** s'affiche.

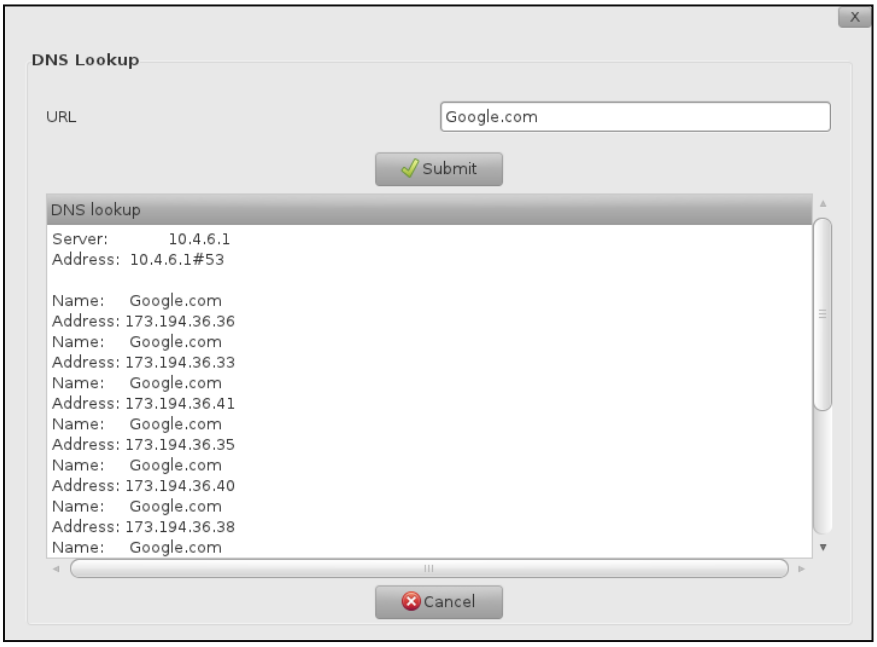

Figure 6-4 : Outil DNS Lookup

2. Dans le champ **URL**, saisissez une URL.

3. Cliquez sur Soumettre , le résultat DNS Lookup est affiché dans la section **DNS lookup**.

7 Applications utilisateur

Le *Gio 5* dispose d'un certain nombre d'applications utiles pour les utilisateurs préinstallées. Les applications comme l'éditeur de texte, le lecteur multimédia, le navigateur web vous permettent de créer et d'éditer du texte, de lire des fichier vidéo ou audio et de naviguer sur le web.

Pour accéder aux diverses applications utilisateur :

1. Sur la barre latérale du bureau, cliquez sur l'icône **Paramètres.**
2. Cliquez sur la flèche déroulante **Applications utilisateur**.
3. Sélectionnez dans la liste suivante des applications utilisateur :

   - **Lecteur multimédia** : Cette application peut lire des fichiers vidéo et audio. Le lecteur multimédia par défaut du *Gio 5* est le populaire Totem Movie Player 3.0.1.

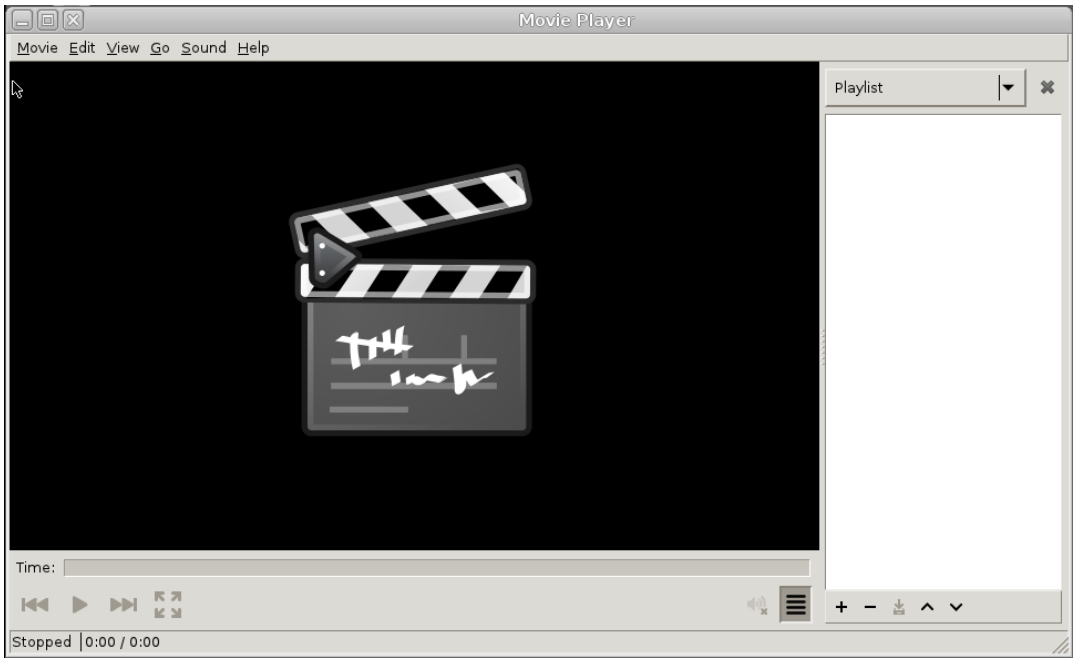

Figure 7-1 : Lecteur multimédia Totem

   - **Éditeur de texte** : Cette application vous offre fonctions de base d'édition de texte, vous pouvez saisir, modifier et enregistrer du texte en utilisant cette application.

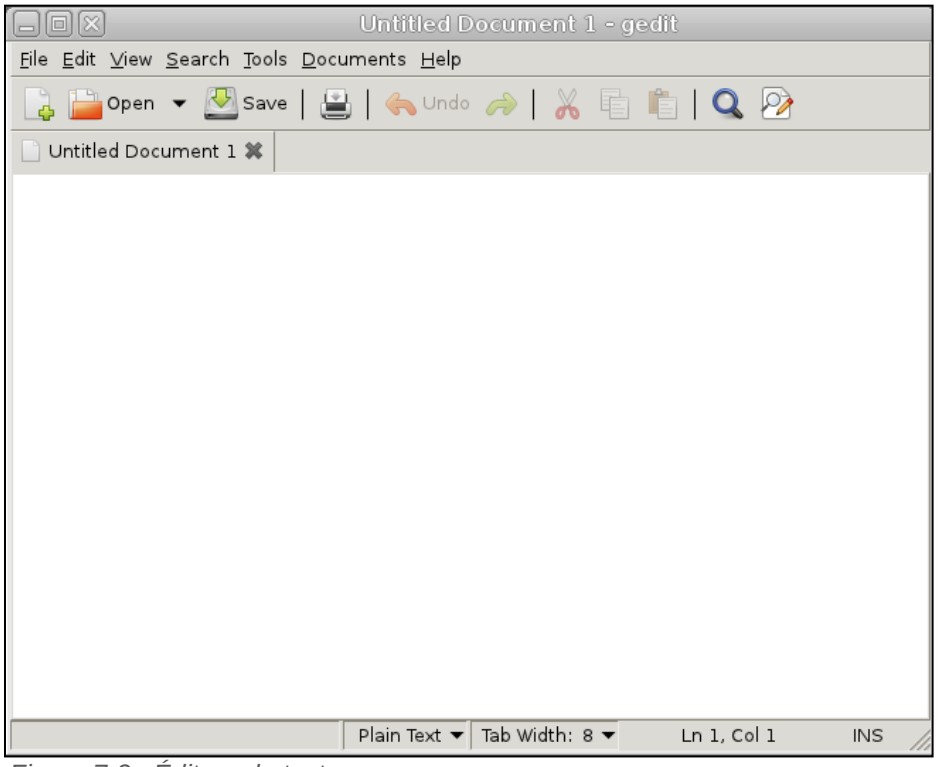

Figure 7-2 : Éditeur de texte

- **Réglage du volume** : Cette application vous permet de définir les paramètres de son système.

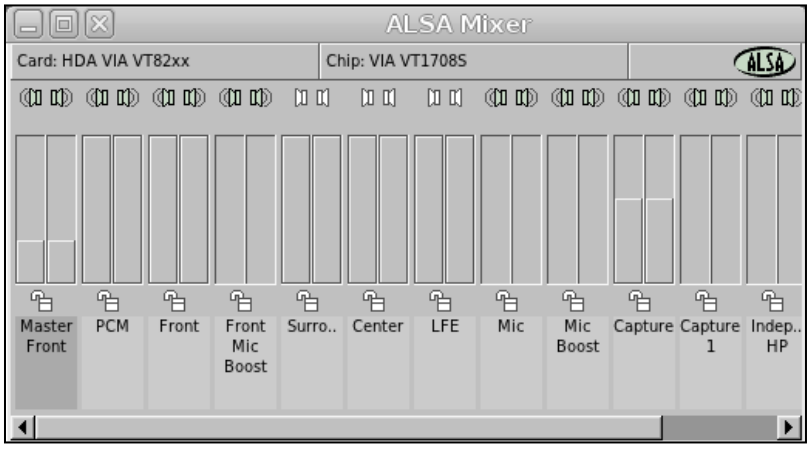

Figure 7-3 : Réglage du volume

- **Calibrage de l'écran tactile** : Cette application vous permet de calibrer votre moniteur à écran tactile.

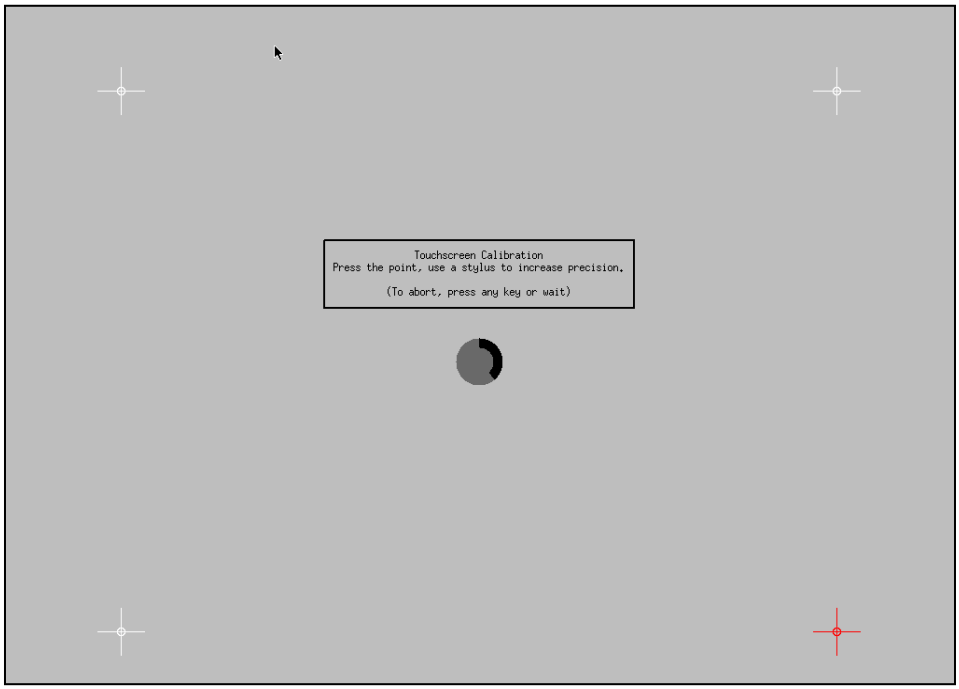

Figure 7-4 : Calibrage

Pour calibrer votre moniteur à écran tactile, appuyez sur les quatre coins en surbrillance de l'écran.

Remarque : Vous pouvez utiliser cette application uniquement lorsque vous avez connecté un moniteur à écran tactile à votre client.

- Lecteur de PDF : Cette application vous permet d'afficher les documents PDF (Portable Document Format).

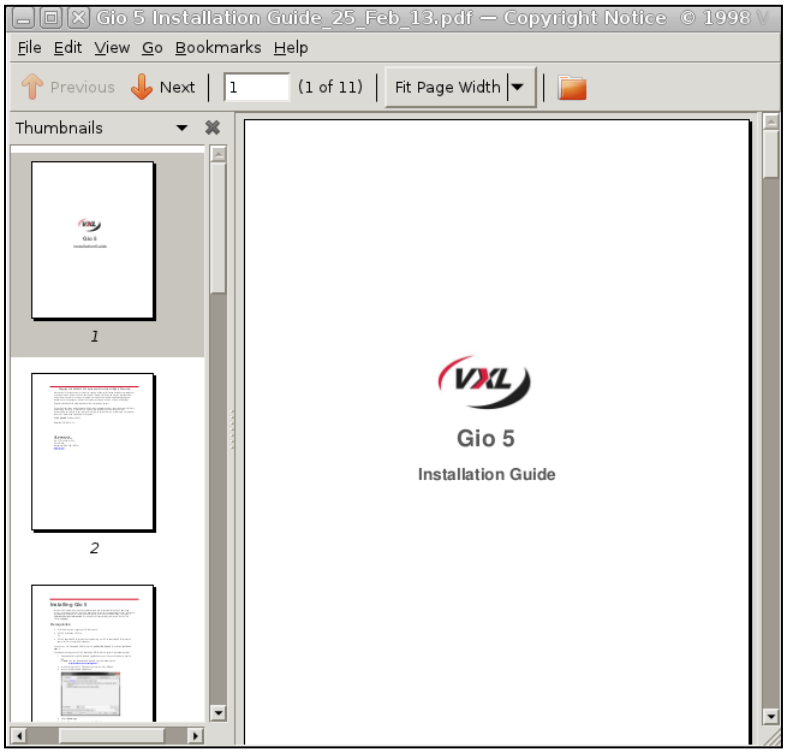

Figure 7-5 : Visualisation de fichiers

Glossaire

Mots clés	Description
CUPS	CUPS est le système basé sur des standards, open source pour l'impression pour des systèmes d'exploitation UNIX®.
Cache	La mémoire **cache** est un composant qui stocke des données de manière transparente, afin que les futures demandes de ces données puissent être servies plus rapidement. Les données qui sont stockées dans une mémoire cache peuvent être des valeurs qui ont été calculées précédemment ou des doublons de valeurs initiales qui sont stockées ailleurs.
Dynamic Host Configuration Protocol (DHCP)	Un protocole utilisé par les administrateurs de réseau pour gérer de manière centralisée et automatiser l'affectation des adresses IP dans un réseau. Sans le protocole DHCP, une adresse IP fixe doit être attribuée manuellement à chaque ordinateur du réseau.
Domain Name System (DNS)	La méthode utilisée pour traduire les noms de domaine Internet en adresses IP. Un nom de domaine est un " pseudonyme " pertinent et facile -à- mémoriser pour une adresse IP. La méthode DNS est basé sur des serveurs DNS, qui contiennent des listes de noms de domaine et d'adresses IP prédéfinis et pouvant être mis à jour. Sans ce système, les utilisateurs devraient toujours se rappeler et utiliser les adresses IP pour accéder aux ordinateurs du réseau ou pour naviguer sur Internet.
Télécharger	La transmission d'un fichier d'un système informatique à un autre, généralement dans un système informatique plus petit. Pour un utilisateur Internet, le téléchargement d'un fichier demande et reçoit à partir d'un autre ordinateur (ou à partir d'une page Web sur un autre ordinateur).
Cryptage	Une mesure de sécurité qui consiste à convertir les données en une forme qui ne peut pas être facilement comprise par des systèmes non autorisés. Le cryptage simple consiste à substituer des lettres par des chiffres et de faire tourner les lettres de l'alphabet. Le cryptage plus complexe est basé sur des algorithmes informatiques qui réarrangent les bits de données dans les signaux numériques. Un algorithme de décryptage approprié (clé) récupère le contenu d'une transmission cryptée.
Micrologiciel	Un programme d'ordinateur ou logiciel stocké dans PROM ou EPROM.
File Transfer Protocol (FTP)	Un protocole pour échanger des fichiers entre ordinateurs sur Internet. Comme *Hyper Text Transfer Protocol (*HTTP) qui transfère les pages web, et *Simple Mail Transfer Protocol (SMTP)* qui transfère les e-mails, FTP est un protocole d'application qui utilise le protocole TCP/IP pour transférer des fichiers d'un ordinateur à un autre.
Passerelle	Un point dans le réseau qui fait office d'entrée vers un autre réseau. Les ordinateurs qui contrôlent le trafic dans un réseau ou chez un fournisseur d'accès à Internet sont des nœuds de passerelle. Dans un réseau d'entreprise, serveurs de

Mots clés	Description
	passerelle généralement agissent également en tant que proxy et serveurs de pare-feu. Un serveur de passerelle est souvent associé à un routeur qui sait où un paquet entrant doit être dirigé, et à un commutateur qui fournit la trajectoire réelle à l'intérieur et hors de la porte d'entrée pour un paquet donné.
Groupes	Une liste des principaux groupes où les clients sont organisés de manière logique conformément aux exigences. Le groupement gère les clients plus efficacement en les organisant et en les classant par groupes principaux et sous-groupes. N'importe quel client peut appartenir à un seul sous-groupe ou groupe.
Graphical User Interface (GUI)	Une interface graphique (plutôt que purement textuelle) de l'utilisateur à un ordinateur. Un élément GUI comprend des fenêtres, des menus déroulants, des boutons, des barres de défilement, des images d'icônes et des assistants.
Independent Computing Architecture (ICA)	Une technologie développée par *Citrix Systems Inc* qui fournit une base pour la conversion d'un périphérique client vers un client léger. Il fonctionne en séparant la logique de l'application de l'interface utilisateur. Alors que l'application s'exécute uniquement sur le serveur, les utilisateurs du client peuvent visualiser et travailler avec l'interface de l'application, alors qu'en fait, l'application est réellement en exécution sur le serveur.
Internet	Un système mondial de réseaux informatiques dans lequel un utilisateur d'un ordinateur reçoit des informations à partir de n'importe quel autre ordinateur. Physiquement, l'Internet utilise une partie des ressources totales des réseaux publics de télécommunications qui existent actuellement et un ensemble de protocoles appelé TCP/IP. La partie la plus largement utilisée de l'Internet est le World Wide Web (*WWW ou Web*). La caractéristique remarquable du WWW est l'hypertexte, une méthode instantanée de références croisées. Les pages Web peuvent être affichées ou parcourues à l'aide des navigateurs comme Netscape Navigator et Microsoft Internet Explorer.
Adresse IP	Un nombre de 32 bits unique qui identifie l'expéditeur ou le destinataire des informations qui sont envoyées dans un paquet à travers Internet. Lorsqu'il y a une demande pour une page HTML ou un e-mail est envoyé, la partie IP du TCP/IP inclut l'adresse IP du demandeur ou de l'expéditeur du message. À l'autre extrémité, le destinataire peut visualiser l'adresse IP de la page Web du demandeur ou l'expéditeur du courrier électronique et peut réagir en envoyant un message en utilisant l'adresse IP reçue. L'adresse IP est généralement exprimée sous la forme de quatre nombres décimaux, chaque représentant huit bits, séparés par des points. L'adresse est souvent séparée par des par points ou elle est connue sous le nom de notation décimale à point *Exemple : 192.16.4.12.*
Réseau local (LAN)	Un groupe d'ordinateurs et de périphériques associés partageant une ligne de communication commune et les ressources d'un seul processeur ou serveur au sein d'une

Mots clés	Description
	petite zone géographique *Par exemple, dans un immeuble de bureaux.*
Adresse MAC (Media Access Control Address)	Le numéro de matériel unique d'un ordinateur sur un réseau.
MD5	L'algorithme de résumé de message 5 (MD5) est une fonction de hachage sécurisé.
Réseau	Série de points ou de nœuds interconnectés par des chemins de communication. Ils peuvent s'interconnecter avec d'autres réseaux et contenir des sous-réseaux. Les topologies de réseau les plus courantes comprennent : les topologies Bus, Star et Token Ring. Les réseaux peuvent également être caractérisés en termes de distance spatiale comme les réseaux LAN, MAN et WAN.
Nom du domaine NT	Le nom de domaine NT est le nom du domaine des systèmes d'exploitation Windows NT.
Numéro de port	Un numéro qui identifie le processus spécifique à laquelle une connexion Internet ou un autre message réseau doit être transmis quand il atteint un serveur. Pour les protocoles TCP et UDP, un numéro de port est un nombre de 16 bits qui est inclus dans l'en-tête ajouté à une unité de message. Ce numéro de port est passé logiquement entre le client et les couches de transport de serveur et physiquement entre la couche de transport et la couche IP et transmis. *Par exemple, lorsqu'un client demande à un serveur un fichier pour être servi par le serveur FTP, la couche TCP dans le client ajoute le nombre 21 à la demande (21, est par convention le numéro de port 16bits associé à une requête FTP). Au niveau du serveur, la couche TCP lit le numéro de port (21) et transfère la requête au programme FTP*.
Protocole	C'est une spécification de plusieurs règles pour un type de communication particulier. Il existe entre chaque couche fonctionnelle et des couches correspondantes à l'autre extrémité de la communication. Les deux points d'extrémité doivent reconnaître et respecter un protocole. *Exemples : TCP/IP, HTTP et FTP*.
Vitesse de l'écran	La réduction du temps de latence de la vitesse de l'écran accélère la transmission d'images à partir du serveur terminal vers le client.
Sous-réseau	Un ordinateur ou un programme qui fournit des services à d'autres ordinateurs ou programmes. Dans le contexte client/serveur, un serveur est un programme qui attend et répond aux demandes des programmes du client du même ou d'autres ordinateurs.
Transmission Control Protocol / Internet Protocol (TCP/IP)	Une partie distincte d'un réseau ayant tous les ordinateurs dans un lieu géographique dans un bâtiment ou sur le même réseau LAN. Les réseaux divisés en sous-réseaux peuvent se connecter à Internet avec une seule adresse de réseau partagée. Sans sous-réseaux, chaque sous-réseau doit avoir une connexion distincte à l'Internet, ce qui leur permet de recourir inutilement aux rares numéros de réseau que l'Internet a à

Mots clés	Description
	attribuer.
Client léger	Un dispositif informatique « low-cost » gérée de façon centralisée dépourvu de périphériques typiques tels que les CD-ROM et lecteurs de disquettes. Le terme provient du fait que les petits ordinateurs en réseaux ont tendance à être des clients et non des serveurs. Comme l'idée est de limiter les capacités de ces ordinateurs aux applications essentielles, ils ont tendance à être "léger" en termes d'applications client pré-chargées.
VMware View Client	VMware View est un produit commercial de virtualisation de bureau développé par VMware, Inc. VMware View offre des fonctionnalités de bureau à distance aux utilisateurs en utilisant la technologie de virtualisation de VMware.
Réseau privé virtuel (VPN)	Un réseau privé virtuel (VPN) est une technologie permettant l'utilisation d'Internet ou tout autre réseau intermédiaire pour connecter des ordinateurs à des réseaux informatiques distants isolées qui seraient autrement inaccessibles.
Réseau étendu (WAN)	Un réseau informatique qui s'étend sur une zone géographique relativement vaste. Il se compose de deux ou plusieurs réseaux locaux. Les ordinateurs connectés au réseau WAN sont souvent reliés par des réseaux publics, tels que le système téléphonique. Ils peuvent aussi être connectés par lignes louées ou des satellites. Le plus grand WAN qui existe est l'Internet.
WEP	WEP (Wired Equivalent Protocol) est une norme obsolète de la sécurité des réseaux sans fil. Parfois appelée à tort « Wireless Encryption Protocol » (Wireless Encryption Protocol).
WPA et WPA2	L'accès protégé Wi-Fi (WPA) et Wi-Fi Protected Access II (WPA2) sont deux protocoles de sécurité et des programmes de certification de sécurité développés par l'Alliance Wi-Fi pour sécuriser les réseaux informatiques sans fil.
XLmanage	XLmanage est une application de gestion de client léger développée par VXL Instruments.

Index

INDEX

Historique de révision

Version	Détails de la modification	Date
GIO5/UM-23-13	Inclus l'assistant de Configuration, la Connexion automatique et la de section Action de sortie. Mise à jour des connexions WFCMGR and Remote FX, des sections Apparence et Gestionnaire du serveur.	6 juin 2013
GIO5/UM-23-13	Inclus PN Agent, File d'attente de l'imprimante et informations des Paramètres du serveur d'impression.	28 Mar 2013
GIO5/UM-10-13	Inclus Gio 5 pour K series et GioPC référence.	8 Mar 2013
GIO5/UM-8-13	Mises à jour des sections sur l'imprimante et le clavier .	21 Fev 2013