

XMANAGER 6

Руководство Пользователя

Мощный PC X Сервер для Windows

NetSarang Computer, Inc.

Copyright © 2018 NetSarang Computer, Inc. Все права защищены.

Руководство Xmanager®

Это программное обеспечение и связанные с ним документы произведены NetSarang Computer, Inc. и защищены Авторскими правами. Необходимо согласие от правообладателя при копировании, распространении или цитировании всего, или части этого программного обеспечения и связанных данных.

Это программное обеспечение и руководство могут быть изменены без предварительного уведомления для улучшения функций продукта.

Xlpd™ и Xftp™ являются торговыми марками NetSarang Computer, Inc. Xmanager® и Xshell® являются зарегистрированными торговыми марками NetSarang Computer, Inc. Microsoft Windows® является зарегистрированной торговой маркой Microsoft®. UNIX® является зарегистрированной торговой маркой AT&T Bell Laboratories. SSH® является зарегистрированной торговой маркой SSH Communications Security. Secure Shell является зарегистрированной торговой маркой SSH Communications Security.

Это программное обеспечение включает программные продукты, разработанные в рамках проекта OpenSSL и используемые в OpenSSL Toolkit.

NetSarang Computer, Inc.

4701 Patrick Henry Dr. BLDG 22 Suite 137 Santa Clara, CA 95054 <http://www.netsarang.com>

Содержание

О Xmanager	5
Ключевые Возможности	6
Рекомендации	7
Установка и Удаление.....	7
Начало	9
Запуск с XDMCP	10
Запуск с Xstart	13
Выход из Xmanager	16
Управление Сессиями	17
Сессии Xstart	17
Автоматическая XDMCP Сессия.....	19
Статические XDMCP Сессии.....	20
Настройка Свойств Сессии	22
Свойства XDMCP сессии.....	23
Свойства Xstart Сессии.....	24
Настройки Протокола SSH	26
Настройки Окна Xmanager	32
Настройка Столбцов.....	33
Создание Папки Сессии	33
Экспорт	33
Импорт	33
Соединение	35
Соединение с помощью Xmanager	35
Адресная Строка Xmanager	35
Безопасное XDMCP Соединение.....	36
Соединение с помощью Xstart	38
Настройки Аутентификации Пользователя в Xstart	39
Определение Тэгов Команд Xstart	41
Настройки Брандмауэра.....	42
Решение Проблем Соединения	43
Опции Командной Строки Xmanager сервера.....	44
Параметры Командной Строки Xrcmd.....	45
Настройки Профиля Сервера	47
Управление Профилем.....	47
Оконные режимы	48
Настройки Параметров Соединения	51
Управление Шрифтами	52
Управление Цветом	54
Настройки Клавиатуры	56
Настройки Мыши.....	58
Настройки Звука	59
Несколько Мониторов	59
Настройки Дополнительных Параметров	60
Безопасность	63
Контроль Доступа Хостам.....	63
Аутентификация Пользователя по Публичному Ключу	63
Диалоговое Окно Ключей Пользователя	65
Диалоговое окно Аутентификации SSH Пользователя	65
Управление Ключами Хоста.....	66
Диалоговое Окно Предупреждения Безопасности SSH.....	66
Диалоговое Окно Ключей Хоста	66

Мастер Пароль	67
Управление Вкладками.....	69
Вкладка	69
Группа Вкладок	69
Копирование, Сохранение, и Печать в X Приложениях	71
Журнал Сессии.....	73
Индекс.....	74

О Xmanager

Xmanager® представляет собой мощный и удобный PC X сервер, работающий в среде Windows®. Пользователи могут перенести рабочий стол UNIX/Linux на свой ПК с Windows с помощью **Xmanager**. Кроме того, приложение X может безопасно выполняться через SSH (защищённая оболочка) даже если ПК пользователя находится в частной сети или между пользовательским ПК и удалённым сервером установлен межсетевой экран.

Xmanager предлагает разнообразные функции, такие как настройка множества серверов, мульти-визуальные, мульти-мониторные, многопользовательские настройки, множество XDMCP сессий, и усиление безопасности SSH. **Xmanager** предоставляет множество дополнительных возможностей для опытных пользователей и простой пользовательский интерфейс для начинающих пользователей.

Xmanager состоит из **Xmanager(Xbrowser)**, **Xconfig**, **Xstart** и несколько других утилит. В Версии 6, утилита для создания и управления сессиями, называемая ранее Xbrowser, была переименована в Xmanager. Xmanager как сервер, теперь называется **Сервер Xmanager**.

- **Xmanager** имеет несколько применений:
 - Как программа X сервера для ПК.
 - Xmanager как сервер. Графические приложения, X клиенты удалённых UNIX/Linux хостов могут быть показаны на экране Windows через **Сервер Xmanager**.
 - Утилита сессий, которая управляет сессиями и файлами сессий (в предыдущих версиях это называлось Xbrowser). Используя утилиту Xmanager, пользователи могут создавать сессии Xstart и XDMCP, а также запускать, останавливать, управлять и т. д. сессиями. Несколько сеансов могут быть запущены одновременно из Xmanager и для каждого хоста можно создать ярлыки. Если установлены Xshell и Xftp, их файлами сессий также можно управлять через Xmanager.
- **Xconfig** создаёт и управляет профилями сервера **Xmanager**. Эти профили сервера определяют различные параметры Xmanager, такие как режимы окон, каталоги шрифтов, цвета и т.д.
- **Xstart** обеспечивает непосредственное выполнение одиночных X приложений на ПК пользователя. Поддерживаемые протоколы включают SSH, TELNET, RLOGIN, REXEC, RSH, и LOCAL для соединения с удалённым хостом. Команду удаленного хоста можно удобно выполнить на ПК пользователя Windows через Xstart.

Ключевые Возможности

Этот раздел раскрывает ключевые возможности **Xmanager**.

Соединение и Запуск

- Управление Xmanager (Xstart и XDMCP), Xshell, и Xftp сессиями в одном месте
- Диспетчер сессий - для лёгкого запуска и управления множеством сессий
- XDMCP, SSH, RSH, REXEC, RLOGIN и TELNET протоколы связи
- До 128 соединений X клиентов на сессию Xmanager
- Ярлыки для Xstart и XDMCP сессий
- Расширенные настройки распознавания удалённых приглашений и скрипты удалённых команд в Xstart
- Безопасный XDMCP, для XDMCP соединений за пределы брандмауэров и частных сетей
- Поддержка IPv6
- Поддержка аутентификации Kerberos (MIT Kerberos, Microsoft SSPI)
- Множество вкладок в одном окне
- Множество групп вкладок в одном окне

Установка и Распространение

- Поддержка терминального сервера Windows и Citrix MetaFrame для Windows
- Совместное использование сессий для терминального сервера Windows
- Тихая Установка
- Многопользовательские настройки
- Простое распространение сессий и профилей серверов
- Назначаемый пользователем путь к сессиям
- Выбор темы для программы

Безопасность

- SSH1/SSH2 протоколы с поддержкой аутентификации по публичному ключу
- Создание публичных ключей SSH
- SSH агент аутентификации пользователя
- Контроль доступа по хосту
- XDMCP соединения, использующие безопасный SSH туннель (Безопасный XDMCP)
- Назначенный пользователем Мастер Пароль для подключения дополнительной безопасности для паролей сессий

X Сервер

- Высокопроизводительный X11R7 PC X сервер
- GLX 1.3, OpenGL 1.2 расширения протокола
- Расширения протокола X Rendering
- Поддержка расширения RandR
- Многосерверные настройки
- Многопользовательские настройки

- Поддержка нескольких мониторов
- Поддержка нескольких сетевых адаптеров
- Множество XDMCP сессий
- Автоматическое назначение номера дисплея
- Одно и Многооконный режим
- Панорамирование и автоподнятие в локальном оконном менеджере
- Мультивизуальный
- 256-цветный просмотр в видео устройстве с Истинными Цветами
- Автоматическая подмена цвета для Псевдографического просмотра
- Режим Backing Store
- Полная функция Planemask для 256-цветных приложений
- Колесо мыши
- Эмуляция 3-кнопочной мыши
- Графический редактор клавиатуры
- Смена клавиатуры в режиме реального времени с помощью комбинации клавиш
- Звуковые файлы для XBell звуковых запросов
- База данных локальных ресурсов
- Распечатка окна в Многооконном Режиме
- Автоматическое копирование и вставка между приложениями X и Windows
- Иконка в области уведомлений

Шрифт

- Компилятор шрифта
- Сервер шрифтов
- Форматы шрифта BDF, PCF
- Автоматическая подмена шрифта
- Различные наборы шрифтов для разных языков и приложений X

Рекомендации

- **Процессор:** Intel® совместимый
- **Операционная Система:** Windows 7 SP1 или выше, Windows Server 2008 R2 или выше
- **Свободное Место:** 100MB или более
- **Сеть:** TCP/IP

Установка и Удаление

Программа установки **Xmanager** была создана с использованием InstallShield®. Во время установки может быть изменено большое количество опций. В то же время, в большинстве случаев достаточно просто нажать [Далее].

Для удаления **Xmanager**, используйте стандартные методы установки/удаления программ в Windows. Запустите панель установки или изменения программ из панели управления (или appwiz.cpl в строке поиска) и выберите удаление **Xmanager** из списка.

Даже если программа удалена, регистрационная информация, лог файлы и файлы данных, созданные пользователем не будут удалены. Информация и файлы будут доступны для

использования в случае переустановки программы. Если вы хотите удалить все файлы и регистрационную информацию полностью, удалите следующее:

Регистрационная Информация:

- `\HKEY_CURRENT_USER\Software\NetSarang\Xmanager`

Файл и Папку:

- Папка документов пользователя `\Netsarang Computer\6\Xmanage`

Начало

Xmanager предлагает **Xmanager** и **Xstart**, две основных утилиты для доступа к удалённому хосту UNIX/Linux. **Xmanager** доставляет весь удалённый рабочий стол по XDMCP (X display manager control protocol) на рабочий стол Windows ПК. Другие пользователи, кому нужен доступ только к одиночному X приложению, как альтернативу передачи всей рабочей среды, могут использовать **Xstart** так как он проще и быстрее в сравнении с XDMCP соединением.

Замечание

Запустите **Xmanager - Passive** из папки Tools в папке с установленным **Xmanager**, чтобы запустить **Xmanager сервер** в режиме ожидания для подключения приложений X. Пользователи затем могут запустить удалённое X приложение, используя **Xstart** или другие утилиты.

Запустите **Xmanager - Broadcast** из папки Tools в папке с установленным **Xmanager**, чтобы запустить **Xmanager Broadcast** – сообщения XDMCP Запросов по сети. Хосты, которые ответят на запрос, будут показаны в Окне Выбора. Хост может быть выбран из списка и с ним можно будет установить соединение

Запуск с XDMCP

Для использования **Xmanager сессий**, укажите удалённый UNIX/Linux хост, поддерживающий XDMCP сервис для удалённого X сервера. Как правило, на хосте должен быть запущены **dtlogin**, **kdm**, **gdm**, **lightdm**, или **xdm**. За подробностями о настройках XDMCP сервиса, обратитесь к соответствующей документации UNIX/Linux.

1. Откройте папку **Xmanager** на вашем рабочем столе.

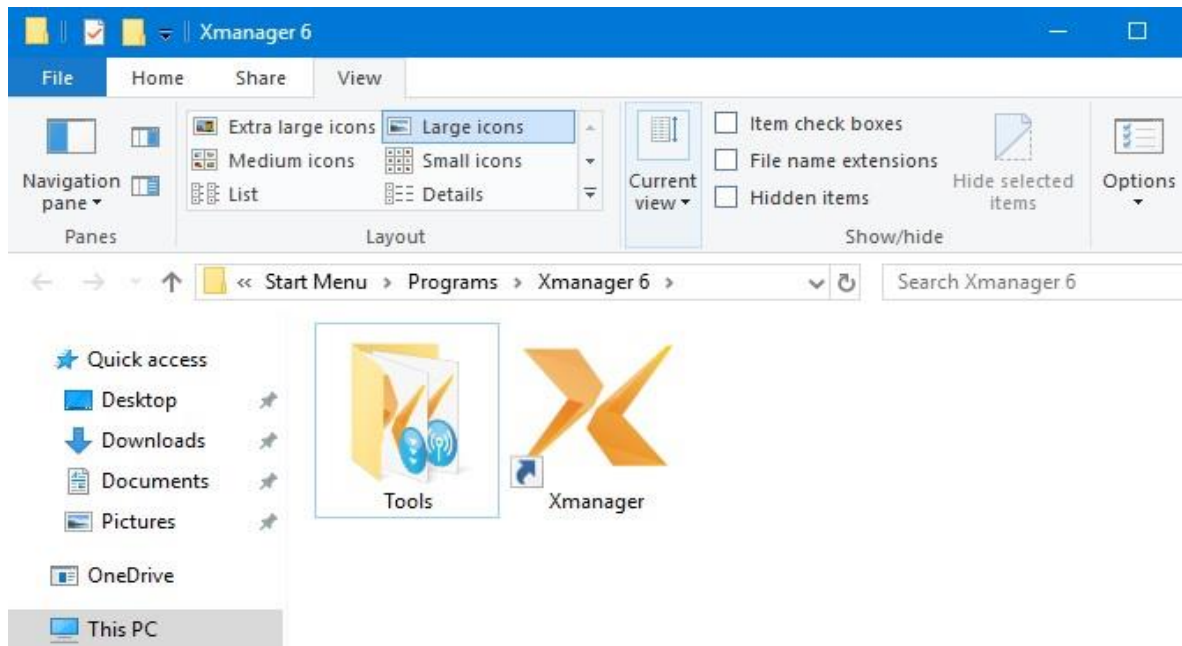


Рис. 1: Папка Xmanager

2. Запустите **Xmanager**.

Замечание

Xmanager автоматически находит все UNIX/Linux хосты в локальной сети. Если UNIX/Linux хост, к которому необходим доступ, находится в другой сети, чем локальный ПК, зарегистрируйте IP адрес UNIX/Linux хоста или широковещательный адрес в диалоговом окне **Опции**. За деталями настройки, обратитесь к разделу 'Автоматическая Сессия XDMCP'.

Если UNIX/Linux хост не показывается в окне **Xmanager**, это означает, что хост не готов к XDMCP соединению.

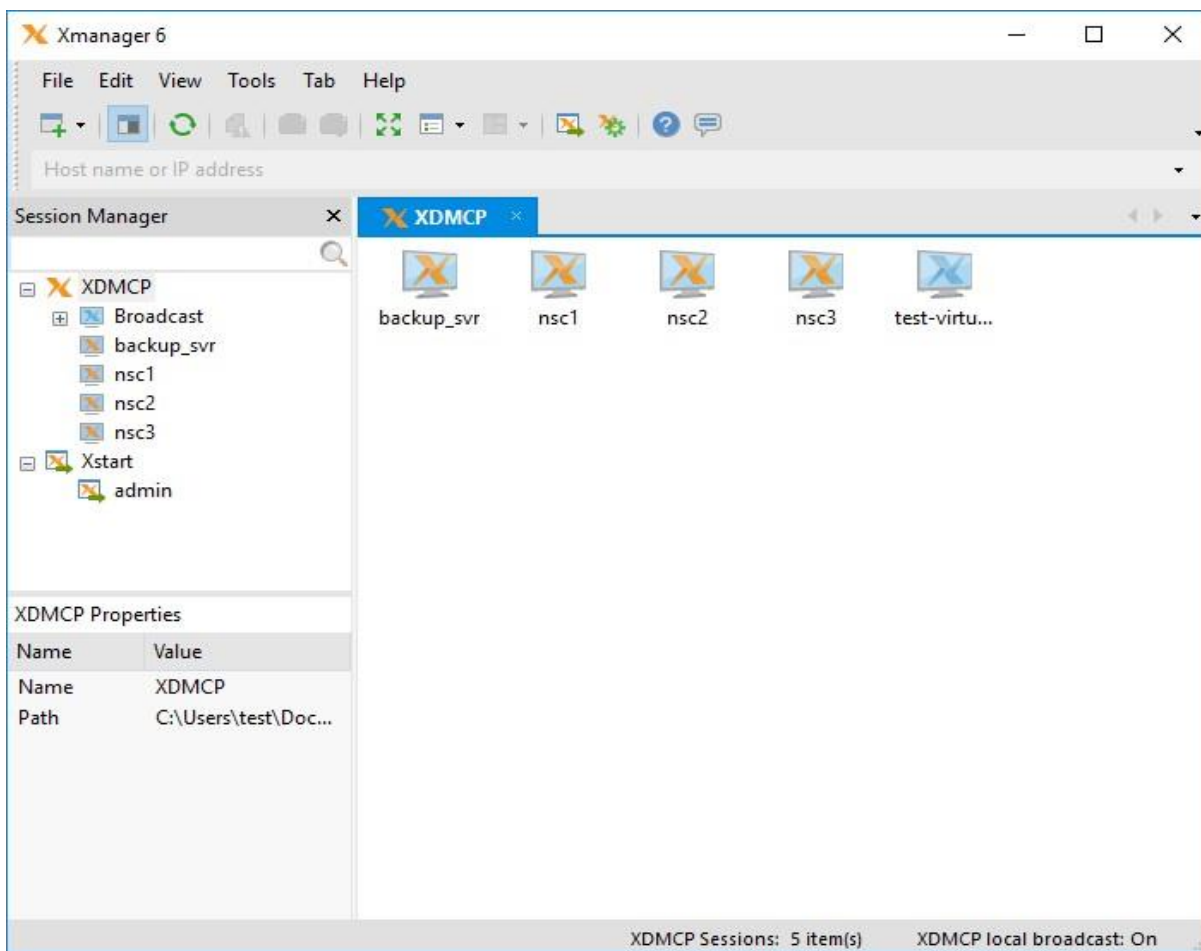


Рис. 2: Основное окно Xmanager

3. Кликните дважды на хост, с которым хотите соединиться. Откроется графическое окно с приглашением ко входу.

Замечание

Если графическое окно не показывается, возможно настроен брандмауэр между ПК пользователя и удалённым хостом.

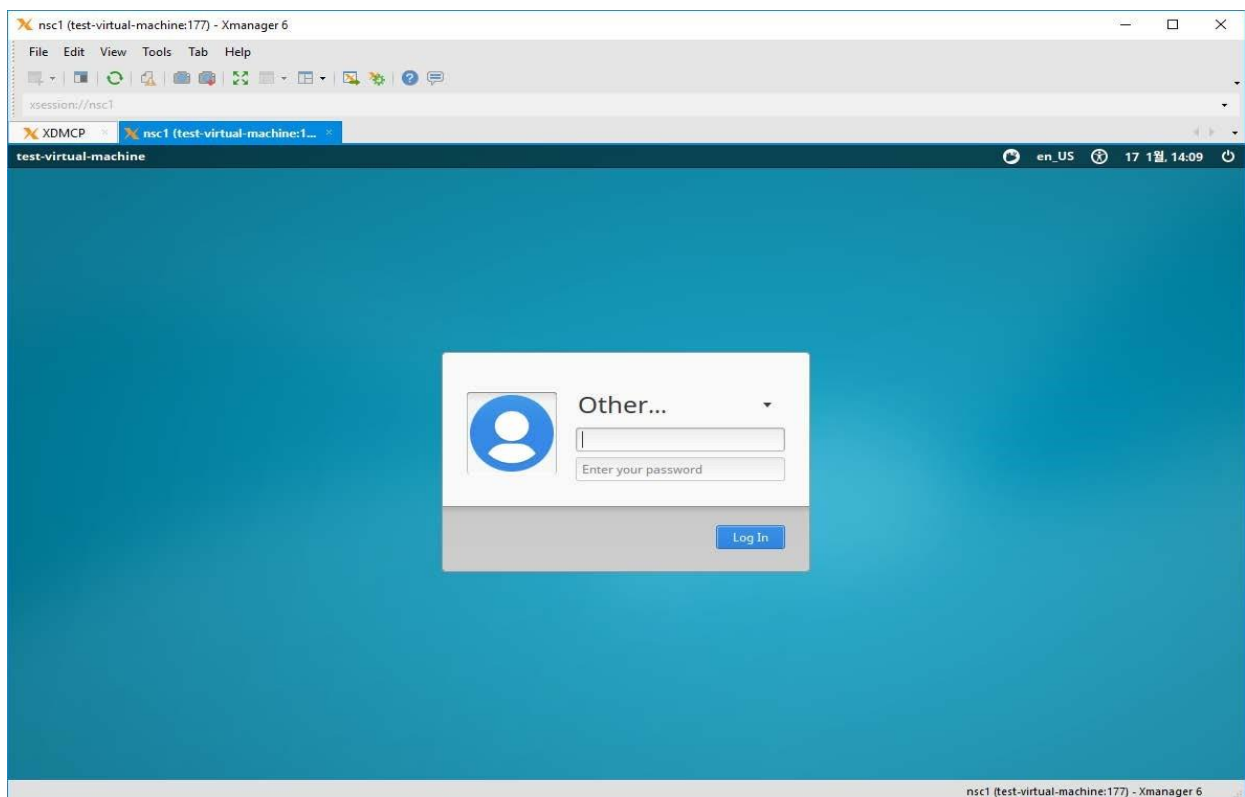


Рис. 3: CentOS приглашение ко входу через XDMCP соединение

4. Войдите на хост, введя имя и пароль зарегистрированного на хосте аккаунта. Откроется удалённый рабочий стол.

Замечание

Если удалённый рабочий стол не показывается после ввода логина и пароля, возможно есть проблемы с настройками учётной записи на хосте.

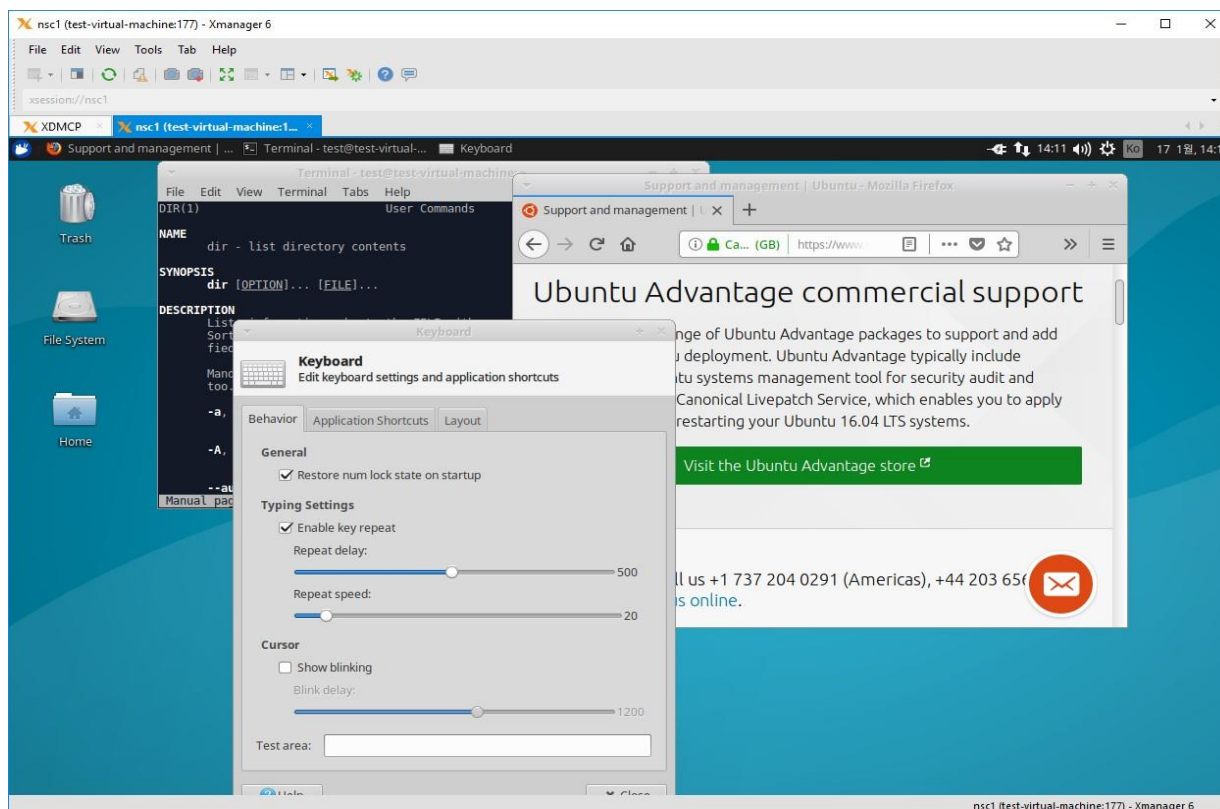


Рис. 4: Рабочий стол UNIX выполняемый в Windows

Если у вас есть проблемы с использованием **Xmanager**, посетите наш сайт техподдержки:

<http://www.netsarang.com/support/main.html>

Дополнительную информацию о настройках XDMCP в UNIX/Linux серверах и советы по использованию, можно найти на странице поддержки клиентов.

Запуск с Xstart

Xstart позволяет пользователям запускать удалённое X приложение. Как только будет создана Xstart сессия, удалённое приложение может быть запущено в любое время, простым кликом на файл сессии в Windows.

1. Запустите **Xstart**, который расположен в папке **Xmanager\Tools**.

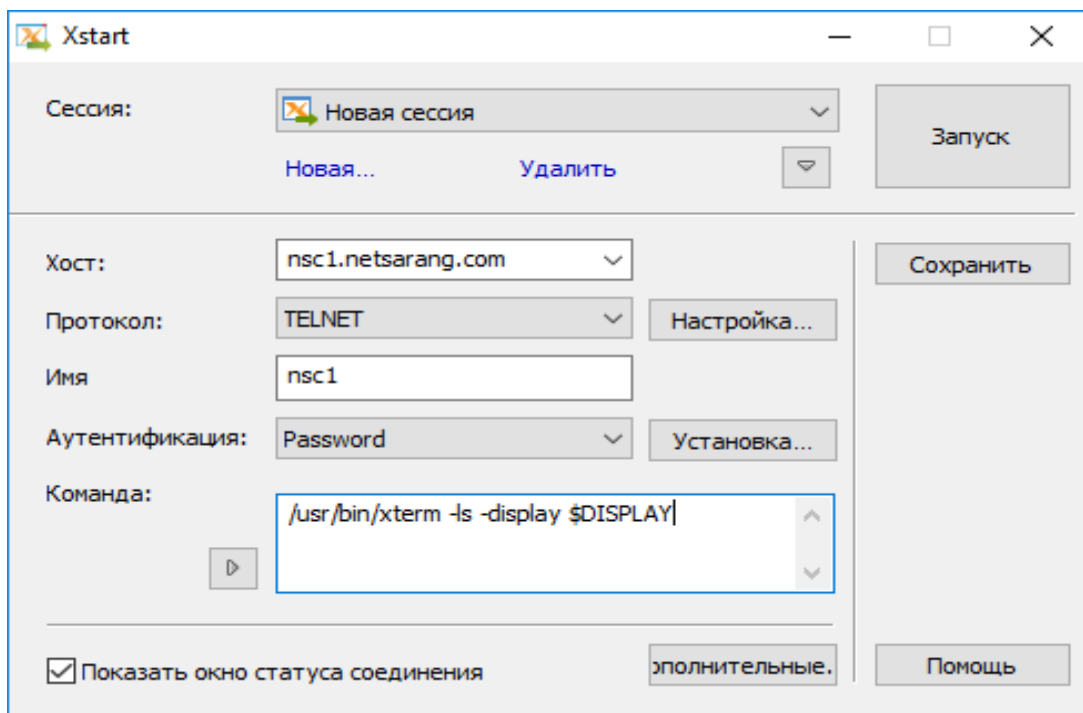


Рис. 5: Основное окно Xstart

2. Нажмите [Новое]. Появится диалоговое окно **Новая Сессия**.

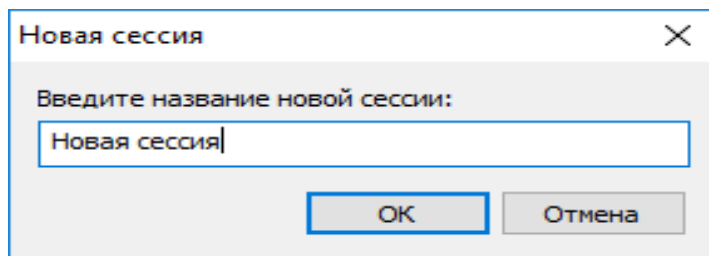


Рис. 6: Диалоговое окно создания Новой Сессии в Xstart

3. Введите название новой сессии и нажмите [ОК].
4. Введите имя удалённого хоста UNIX/Linux или IP адрес в поле [Хост].
5. Выберите один из поддерживаемых хостом протоколов в поле [Протокол].
6. Нажмите [Настройка] для настройки параметров протокола, таких как порт или таймаут.
7. Введите имя пользователя на удалённом хосте в поле [Имя Пользователя].
8. Для сохранения пароля пользователя в настройке сессии, установите тип [Аутентификации] как *Пароль* и нажмите кнопку [Настройка] справа.
Будет показано диалоговое окно **Настройка Пароля**.

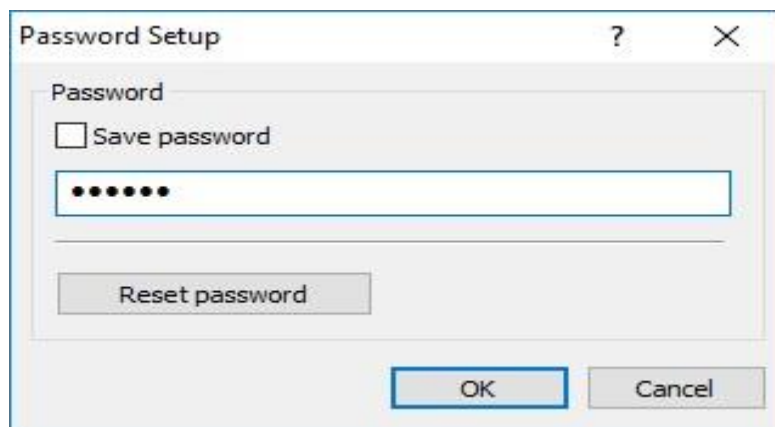


Рис. 7: Диалоговое окно Настройки Пароля

9. Введите команду, которую необходимо выполнить на хосте в поле [Команда]. Для запуска **xterm**, введите следующую команду:
`/usr/bin/X11/xterm -ls -display $DISPLAY`

■ **Замечание**

При нажатии на кнопку ниже надписи [Команда], отобразится удобный список обычно используемых примеров команд xterm для различных UNIX/Linux. Выберите команду xterm, подходящую для выполнения на дистрибутиве UNIX/Linux. Вы также можете добавлять/удалять часто используемые команды, открыв диалоговое окно **Зарегистрированные Команды**.

10. Нажмите [Запуск]. Откроется окно **xterm**.

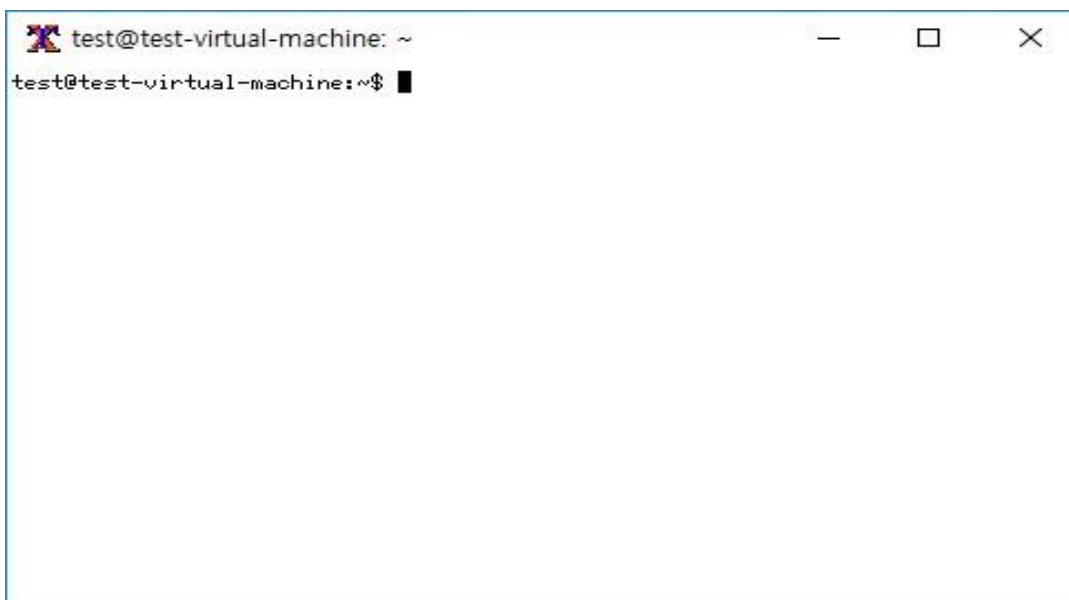


Рис. 8: Окно xterm

Если у вас есть проблемы с использованием **Xstart**, посетите нашу службу техподдержки клиентов:

<http://www.netsarang.com/support/main.html>

Большинство проблем обычно вызваны брандмауэром, ПК пользователя, или настройками сети. В некоторых случаях, пользователи могут пообщаться со своим системным администратором для решения проблемы.

Выход из Xmanager

Для завершения удалённого X приложения, запущенного с помощью **Xstart** или **Xmanager**, выберите [Заккрыть] из системного меню **Xmanager сервера**. О системном меню **Xmanager**, смотрите 'Режим Окна'.

Для Автоматического Выхода из Xmanager сервера, когда Все Удалённые X Приложения Завершены:

1. Выберите [Свойства] из системного меню **Xmanager сервера**. Будет показано диалоговое окно **Свойства Профиля**.
2. Выберите [Выйти из Xmanager, когда все соединения будут закрыты] во вкладке [Основное].
3. **Xmanager сервер** выключится, когда все окна X приложений будут закрыты.

■ Замечание

Если опция [Выйти из Xmanager, когда все соединения будут закрыты] не выбрана, **Xmanager** перезапустится, когда все удалённые X приложения закроются, и будет ожидать подключения нового X приложения.

Управление Сессиями

У сессий сохраняется информация о соединении для подключения к удалённому хосту. При создании сессии, пользователи могут назначать различные параметры и профили сервера для каждого соединения. Типы сессий подразделяются на автоматические сессии XDMCP, статические сессии XDMCP и сессии Xstart.

Значок	Тип Сессии	Описание
	Автоматический XDMCP	Xmanager отправляет широковещательное сообщение в локальную сеть и динамически находит хосты. Чтобы найти узел в другой подсети, введите IP-адрес узла в диалоговом окне Параметры . Все автоматические сессии используют одинаковые настройки, пользователи могут нажать на сессию правой кнопкой, выбрать [Сохранить Как], и сохранить сессию. Затем, нажать правой кнопкой на созданную сессию и выбрать [Свойства]. В этом случае, вновь созданная сессия станет статической XDMCP сессией.
	Статический XDMCP	Статическая сессия, это сессия, созданная пользователем. Статическая сессия может быть создана копированием (сохранением) автоматической сессии или путём создания Новой Сессии. Если удалённый хост не отвечает на XDMCP запросы, отображаемый значок будет тусклым. Пользователи могут создавать ярлыки, изменять настройки для этой сессии, и отсылать эту сессию другим пользователям по e-mail, например.
	Xstart	Xmanager может создавать и управлять Xstart сессиями. Дополнительно, пользователи могут также управлять этими сессиями напрямую в Xstart . Xmanager и Xstart совместно используют все сессии Xstart . Нажав дважды на сессию Xstart, пользователи могут удобно запускать удалённое X приложение на своём Windows ПК.

Замечание

Сессия Xstart полезна при запуске удалённых X приложений X по одному. Эта сессия подключается к удалённому хосту, автоматически выполняет указанную команду, и открывает X приложение на ПК пользователя Windows.

Сессия XDMCP полезна для переноса экрана входа в систему с графическим интерфейсом пользователя и всей рабочей среды удалённого хоста на ПК пользователя с Windows. **Xmanager** поддерживает все графические среды UNIX/Linux, включая CDE, KDE и GNOME.

Сессии Xstart

При создании сессии Xstart, X приложение удалённого хоста может быть выполнено на компьютере пользователя. **Xstart** автоматически осуществляет процесс входа в систему и выполняет X приложение, указанное пользователем.

Пользователи могут создавать Xstart сессии в **Xstart** и в **Xmanager**.

Для Создания Сессии с Xstart:

1. Запустите **Xstart**, расположенный в Папке **Xmanager**.
2. Нажмите [Новая]. Будет показано диалоговое окно **Новая Сессия**.
3. Введите новое имя сессии и нажмите [OK].
4. Введите удалённое имя хоста UNIX/Linux или IP address в [Хост].
5. Выберите один из поддерживаемых протоколов в поле [Протокол].
6. Нажмите [Настройка] для настройки параметров протокола, таких как порт или таймаут.
7. Введите Имя Пользователя удалённого хоста в поле [Имя Пользователя].
8. Для сохранения пароля пользователя в файле сессии, установите [Аутентификация] как *Пароль* и нажмите кнопку [Установка] справа. Будет показано диалоговое окно **Установка Пароля**.
9. Введите команду, которая будет выполнена на удалённом хосте в поле [Команда]. Для запуска **xterm**, введите следующую команду:
`/usr/bin/X11/xterm -ls -display $DISPLAY`

Замечание

Нажмите кнопку внизу поля [Команда] для просмотра списка основных используемых xterm команд, работающих для различных типов UNIX/Linux хостов. Выберите xterm команду, относящуюся к UNIX/Linux хосту, с которым хотите соединиться. Пользователи также могут добавлять/удалять часто используемые команды в диалоговом окне **Зарегистрированные Команды**.

\$DISPLAY преобразовывается в IP адрес ПК и номер дисплея, который ждёт Xmanager сервер. В то же время, если используется протокол SSH, DISPLAY указывается автоматически, в соответствии с протоколом проброса X11, то есть опция '-display \$DISPLAY' не используется. Xstart не будет делать преобразование \$DISPLAY во время доставки команды.

10. Нажмите [Сохранить].

Для Создания Сессии с Xmanager:

1. Запустите **Xmanager** в Папке **Xmanager**.
2. Укажите на [Новая] в меню [Файл] и выберите [Сессия Xstart]. Будет показано диалоговое окно **Свойства Новой Сессии**.
3. Введите имя [Сессии] во вкладке [Основное]. Убедитесь, что не вводите название сессии, совпадающее с уже существующим файлом сессии.
4. Введите удалённое имя хоста UNIX/Linux или IP адрес в поле [Хост].
5. Выберите один из протоколов, поддерживаемых хостом в поле [Протокол].
6. Нажмите [Настройка] для настройки параметров протокола, таких как номер порта или таймаут.
6. Введите имя пользователя на удалённом компьютере [Имя Пользователя].
7. Введите пароль пользователя в поле [Пароль].
8. Введите команду, которая будет выполнена на удалённом хосте в поле [Команда]. Для запуска **xterm**, введите следующую команду:
`/usr/bin/X11/xterm -ls -display $DISPLAY`

9. Нажмите [OK].

 Замечание

Пользователи могут также создавать сессии Xstart, с помощью Мастера Создания Сессий **New Session Wizard** предоставляемого в **Xmanager**. Убедитесь, что категория сессии **Xmanager** установлена как **Xstart**, затем укажите [Новая] в меню [Файл] и выберите [Создание Новой Сессии] чтобы открыть Мастера Создания Новой Сессии.

Для Создания Ярлыка для Сессий Xstart:

1. Запустите **Xstart**.
2. Выберите сессию из списка [Сессии].
3. Нажмите кнопку стрелки для открытия меню и затем нажмите [Создать Ярлык]. Будет показано диалоговое окно **Просмотр Папки**.
4. Выберите папку в которой создать ярлык.

Автоматическая XDMCP Сессия

Xmanager отправляет широковещательное сообщение XDMCP в локальную сеть, или в сеть, указанную пользователем, и показывает хосты, которые ответили на сообщение. Эти сессии создаются автоматически Xmanager и пользователям нет необходимости создавать их вручную. Поэтому эти сеансы называются автоматическими сеансами.

В основном, все UNIX/Linux системы поддерживают сервис XDMCP, и не должно быть проблем поиска хостов в окне **Xmanager**. В некоторых случаях, указанный удалённый хост не поддерживает XDMCP сервис и, как результат, не показывается в **Xmanager**. В этом случае, обратитесь к системному администратору по поводу этого хоста и запросите поддержку XDMCP сервиса для него.

Xmanager предоставляет возможность поиска хостов в других сетях. Кроме того, он предлагает возможность отключить функцию широковещания в случае, если в локальной сети слишком много хостов.

Для Поиска Хостов в Другой Сети:

1. Запустите **Xmanager**.
2. Выберите [Параметры] в меню [Инструменты]. Будет показано диалоговое окно **Параметры**.
3. Введите имя хоста или IP адрес для поиска в секции [Поиск] или введите широковещательный адрес для поиска всех доступных хостов (например 192.168.0.255).
4. Нажмите [Добавить].
5. Нажмите [OK].

Для Выключения Широковещательных Запросов:

1. Запустите **Xmanager**.
2. Выберите [Параметры] в меню [Инструменты]. Будет показано диалоговое окно **Параметры**.
3. Отключите опцию [Искать Локальные Хосты (через XDMCP Broadcast)].
4. Нажмите [OK].

■ **Замечание**

Если в локальной сети пользователя слишком много хостов и только ограниченное количество хостов для использования, может быть удобным отключить опцию [Искать локальные хосты (через XDMCP Broadcast)] и добавить только необходимые хосты в список для поиска.

Статические XDMCP Сессии

В дополнение к автоматическим сессиям, **Xmanager** предлагает возможность создания статических сессий, таких как Пассивные, XDMCP Запросы, XDMCP Широковещательные, XDMCP Непрямые, и Безопасные XDMCP. В отличие от автоматических сессий, статические сессии показываются в окне **Xmanager** все время и могут быть созданы, изменены, или удалены пользователем. В отличие от сессии XDMCP, пассивные сессии пассивно ожидают запросов X приложений, но сгруппированы с XDMCP сессиями по факту того, что они не Xstart сессии.

Для Создания Пассивных Сессий:

1. Запустите **Xmanager**.
2. Выберите XDMCP в категории сессии слева.
3. Укажите [Новая] в меню [Файл] и выберите [Создание Новой Сессии]. Будет показано окно **Создания Новой Сессии**.
4. Выберите *None (Пассивная)* в [Метод] и нажмите [Далее].
5. Выберите профиль сервера [Профиль X Сервера] и нажмите [Далее].
6. Введите название сессии в поле [Имя].
7. Нажмите [Конец].

■ **Замечание**

При выполнении Пассивной сессии, Xmanager переходит в режим, при котором он ожидает соединения от X приложений. Пользователи могут затем запустить удалённое X приложение с помощью Xstart или терминальной программы, такой как telnet.

Для Создания XDMCP Запроса/Широковещательной/Непрямой/Безопасной XDMCP Сессии:

1. Запустите **Xmanager**.
2. Выберите XDMCP в категории сессии.
3. Укажите на [Новая] в меню [Файл] и выберите [Создание Новой Сессии]. Будет показано **Создание Новой Сессии**.
4. Выберите *XDMCP Запрос*, *XDMCP Широковещательная*, *XDMCP Непрямая*, или *Безопасная XDMCP* в [Метод].

■ **Замечание**

XDMCP Запрос соединения осуществляются прямо на указанный хост и пользователю в окно будет выведено графическое приглашение ко входу.

XDMCP Широковещательные соединения, это метод, когда Xmanager открывает диалоговое окно Выбора и список хостов доступных для соединения.

XDMCP Непрямые соединения похожи на XDMCP Широковещательные. Только диалоговое окно Выбора отображается удалённым хостом, а не **Xmanager**.

Безопасные XDMCP соединения могут быть использованы если Xmanager находится за брандмауэром или в приватной сети, а удалённый хост находится за пределами брандмауэра или приватной сети, и поэтому пользователи не могут установить прямое XDMCP соединение. Если SSH сервер работает на этом удалённом хосте, соединения XDMCP с ним могут быть выполнены с использованием SSH проброса для безопасного XDMCP соединения.

5. Введите имя удалённого хоста или его IP адрес в поле [Хост] и нажмите [Далее].
6. Выберите профиль сервера из [Профиль X Сервера] и нажмите [Далее].
7. Введите название сессии в поле [Имя].
8. Нажмите [Конец].

Для Создания Ярлыка Для Статических Сессий:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на Сессию.
3. Выберите [Создать Ярлык].

Для Отправки Сессии по E-mail:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на сессию.
3. Укажите на [Кому] и выберите [E-Mail Получатель].

Для Переноса Сессии в Xmanager:

1. Нажмите на сессию во внешней папке.
2. Перенесите её в окно **Xmanager**.

■ **Замечание**

Только статические сессии, сохранённые в файле, могут быть перенесены. Автоматические сессии перенести нельзя.

Чтобы Поделиться Сессиями с Другими Пользователями:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на сессию.
3. Выберите [Поделиться].

 Замечание

Эта задача требует прав администратора. Общие сессии будут перенесены в папку Общие. По умолчанию, Общие папки в Xmanager отключены. Общие сессии можно увидеть, перейдя в меню [Инструменты] и выбрав [Параметры].

Для Сохранения Автоматических Сессий в качестве Статических:

1. Запустите **Xmanager**.
2. Выберите автоматическую сессию и нажмите на нее правой кнопкой.
3. Выберите [Сохранить Как].

Настройка Свойств Сессии

Файл сессии имеет базовые настройки соединения, такие как имя хоста и номер порта. Дополнительно, пользователи могут изменить XDMCP настройки, адрес подключения, профиль сервера, и номер дисплея.

Для Изменения Информации о Соединении в Файле Сессии:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на файл сессии.
3. Выберите [Свойства]. Будет показано диалоговое окно **Свойства Сессии**.
4. Измените информацию о соединении в разделе [Соединение] во вкладке [Основное].

 Замечание

За подробностями о XDMCP сессии и свойствах Xstart сессии, обратитесь к разделам 'Свойства XDMCP Сессии' и 'Свойства Xstart Сессии' соответственно.

Чтобы Выделить Номер Дисплея:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на файл сессии.
3. Выберите [Свойства]. Будет показано диалоговое окно **Свойства Сессии**.
4. Нажмите вкладку [X Сервер].
5. Выключите [Выделить номер дисплея автоматически].
6. Введите номер дисплея [Номер Дисплея].
7. Нажмите [ОК].

 Замечание

В случае, когда номер дисплея выделяется автоматически, каждая сессия содержит номер дисплея, начиная с номера по умолчанию, установленного в профиле. При выполнении нескольких сессий Xmanager, каждая сессия получает уникальный номер дисплея, и он показывается в строке заголовка Xmanager (например. [:0.0]). Первый номер, это номер дисплея, в второе число, это номер экрана. В Xmanager, номер экрана всегда 0.

Номер Дисплея должен быть в пределах -4976 и 32767. Xmanager получает номер TCP порта, добавляя 6000 к номеру дисплея. Например, если пользователь ввёл 10 в [Номер

Дисплея], Xmanager соединяется с X приложением используя TCP порт 6010. Некоторые UNIX сервера не могут распознать трехзначные номера. Поэтому рекомендуется использовать номер, меньше чем 100. Некоторые системы не поддерживают порт по умолчанию для X, начинающийся с 6000. В этом случае, пользователи могут использовать обратные значения (-), например как порт 5999(-1), 5998(-2), и т.д.

Для Назначения Специального Профиля для Сессии:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на файл сессии.
3. Выберите [Свойства]. Будет показано диалоговое окно **Свойства Сессии**.
4. Нажмите вкладку [X Сервер].
5. Выберите профиль из списка [Профиль Сервера].
6. Нажмите [OK].

Свойства XDMCP сессии

Ниже приведено описание элементов, связанных с подключением, в свойствах XDMCP сессии. Элементы отображаются во вкладке [Основное] Диалогового окна **Свойств XDMCP Сессии**.

Метод

Методы соединения сессии следующие: *None (Пассивная), XDMCP Запрос, XDMCP Широковещательная, XDMCP Непрямая, и Безопасная XDMCP*.

За описанием каждого метода соединения, обратитесь к разделу 'Статические XDMCP Сессии'.

Хост

Введите имя или IP адрес удалённого хоста для соединения.

Выберите графический менеджер для работы с удалённым хостом. Большинство UNIX/Linux дистрибутивов используют **dtlogin**, **kdm**, **gdm**, **lightdm**, или **xdm** в качестве графического менеджера.

Номер Порта

Введите удалённый номер порта графического менеджера. Порт по умолчанию UDP 177.

Использовать По умолчанию

Установите значение по умолчанию для порта UDP 177.

Локальный адрес

Выберите один из IP адресов системы пользователя. Этот параметр используется только если в системе пользователя используется несколько IP адресов.

Если выбран *Авто Выбор* из списка, **Xmanager** ищет IP адрес, подходящий для подключения. Если **Xmanager** не может найти подходящий адрес, откроется диалоговое окно **Выбор IP** для пользователя для непосредственного указания IP адреса.

Графический менеджер на удалённом хосту соединится по IP адресу, указанному пользователем. Если указан несоответствующий IP адрес, графический менеджер не сможет соединиться с **Xmanager** и приглашение ко входу не будет показано.

Адрес Соединения

Этот параметр необходим, когда пользователи соединяются с помощью проброса порта в ограниченном сетевом окружении, таким, как брандмауэр или прокси сервер, когда адрес автоматического соединения не работает должным образом из-за настроек сервера XDM, даже если выбрано безопасное соединение XDMCP. Когда пользователь Windows находится в частной сети с брандмауэром, Xmanager не может получить приглашение удаленного входа с подключением XDMCP, так как брандмауэр блокирует входящие подключения. Таким образом, графический менеджер не сможет подключиться к Xmanager на ПК пользователя Windows. Чтобы использовать эту функцию, пользователи должны выделить порт прослушивания в брандмауэре и перенаправить входящие соединения на ваш Windows.

Тип IP Адреса

Выберите *Назначенный Пользователем* при использовании прокси сервера или при попытке XDMCP соединения в окружении, заблокированном брандмауэром. При использовании Безопасного XDMCP, в случае, если *Автоматическое соединение с адресом* не удалось, выберите *IP адрес SSH сервера* или *Loopback Адрес (127.0.0.1)*.

IP Адрес

Если [Тип Адреса] выбран как *Назначенный Пользователем*, введите прокси сервер или IP адрес брандмауэра. Удалённый графический менеджер попытается соединиться, используя этот адрес и прокси сервер пробросит соединение на систему пользователя.

Номер Порта

Если [Тип Адреса] выбран как *Назначенный Пользователем*, укажите номер TCP порта, выделенного на прокси сервере и готового к пробросу порта.

Например, давайте предположим, что компьютер пользователя использует 192.168.1.100, частный IP-адрес, а сервер брандмауэра использует 192.168.1.1, частный IP-адрес. Кроме того, брандмауэр использует внешний IP-адрес 210.100.xxx.10 для внешнего подключения к Интернету, а IP-адрес узла UNIX - 210.100.xxx.100.

В этом случае вам необходимо настроить брандмауэр для пересылки входящих соединений (210.100.xxx.10, номер порта 6010) в Xmanager (192.168.1.100, номер порта 6010) в Windows. Это называется проброс порта. Для подобной настройки, обратитесь к системному администратору брандмауэра.

Теперь введите 210.100.xxx.100 в поле [Хост] поля [Соединение] и выберите как *Назначенный Пользователем* [Тип адреса] в [Адрес Соединения]. Затем введите 210.100.xxx.10 в [IP-адрес] и введите 6010 в [Номер порта]. Нажмите вкладку [X Сервер], снимите флажок [Автоматически назначать номер дисплея] и введите 10 (TCP 6010) в [Номер дисплея].

Процесс настройки [Адреса Подключения] при подключении к внешнему хосту через маршрутизатор, описан в разделе `Настройки, связанные с брандмауэром`.

Свойства Xstart Сессии

Ниже приведено описание элементов, связанных с подключением в свойствах сессии Xstart. Элементы отображаются на вкладке [Общие] диалогового окна Свойств Xstart Сессии.

Хост

Введите удалённое имя хоста UNIX/Linux или IP адрес. Быстрее и стабильнее ввести IP адрес вместо имени хоста, так как в этом случае Xstart не будет подключаться к серверу имён.

Протокол

Выберите протокол соединения с удалённым хостом. **Xstart** поддерживает *SSH*, *TELNET*, *RSH*, *REXEC*, *RLOGIN* и *LOCAL* протоколы. Перед выбором протокола, убедитесь, что удалённый хост поддерживает этот протокол.

SSH это протокол для безопасных соединений с удалённым хостом. SSH поддерживает Аутентификацию по Публичному Ключу, мощное шифрование данных, и функции проброса X11. Используя протокол SSH, удаленное приложение X может быть безопасно выполнено с использованием мощного шифрования, даже в сетевой среде, уязвимой для безопасности. Кроме того, SSH обеспечивает удобное подключение к хосту, расположенному на другой стороне брандмауэра. Таким образом, пользователь в частной сети может запустить приложение X в другой сети, используя функцию пересылки X11.

TELNET это базовый протокол для использования удалённых терминалов. Он поддерживается большинством серверов, таких как UNIX, Linux и VMS. Он обычно не используется в новых системах из-за низкой степени безопасности.

RSH это простой протокол для соединений с удалённым хостом и запуском указанных команд. Ему не нужен пароль и его следует использовать осторожно из-за проблем с безопасностью.

REXEC это протокол запуска команд на удалённом хосте. Его функционирование схоже с предыдущим протоколом RSH, с одним отличием, что REXEC требует пароль для соединения.

RLOGIN это простая программа для соединения с удалённым хостом и получения оболочки входа.

Также, как и TELNET, RLOGIN аутентифицирует пользователя похожим образом что и RSH.

LOCAL используется для запуска X приложений, установленных на ПК пользователя, а не на удалённом хосте.

Замечание

Для TELNET, RSH, REXEC, и RLOGIN, последние версии UNIX/Linux не разрешают соединение с настройками по умолчанию.

Настройка

Откройте диалоговое окно **Настройка Протокола** в соответствии с выбранным протоколом и установите порт для соединения, таймаут и другие параметры протокола.

Имя Пользователя

Введите имя пользователя на удалённом хосте.

Аутентификация

Выберите метод аутентификации из списка: *Пароль*, *Публичный Ключ*, *Интерактивный Ввод с Клавиатуры*, *GSSAPI* и *PKCS11*. Если выбранные методы аутентификации не поддерживаются SSH сервером, появится окно, с вопросом о методе аутентификации пользователя во время соединения.

■ Замечание

Если на ПК, где запущен Xshell, используется поддерживаемый Xshell Kerberos модуль, Xshell может соединяться с SSH сервером только автоматически, если используется аутентификация GSSAPI.

Выполнение Команды

Введите команду, которая будет выполнена на удалённом хосте.

Например, если пользователь запускает **xterm**, команда на выполнение будет следующая:

```
/usr/bin/X11/xterm -display $DISPLAY
```

Переменная "\$DISPLAY" преобразуется в соответствующее значение с помощью **Xstart**. Обычно оно преобразуется в "192.168.1.100:0.0" если IP адрес у вашей системы Windows "192.168.1.100". Для непосредственного указания IP и номера дисплея, команда будет выглядеть так:

```
/usr/bin/X11/xterm -display 192.168.1.100:0.0
```

Также можно пользоваться переменными '\$PCADDR' и '\$DISPNO'. В этом случае, выполняемая команда будет выглядеть следующим образом:

```
/usr/bin/X11/xterm -display $PCADDR:$DISPNO
```

Если на ПК пользователя используется несколько IP адресов, **Xstart** автоматически изменит их на соответствующие значения. Если используется SSH protocol, DISPLAY автоматически установится в соответствии с протоколом проброса X11, и параметр '-display \$DISPLAY' не потребуется. В этом случае, попытка изменения переменной \$DISPLAY через команду будет игнорирована Xstart.

Зарегистрированная Команда (Кнопка Клавиши Направления)

Нажмите эту кнопку для выбора predetermined в меню команд. Выбрав команду в меню, пользователи могут ввести длинную команду просто одним кликом.

Выберите [Добавить/Удалить] для вызова диалогового окна **Зарегистрированные Команды**. В диалоговом окне, зарегистрируйте часто используемые команды.

Показывать окно статуса соединения

Выберите этот пункт для проверки статуса соединения или сообщений, переданных с удалённого хоста. Этот параметр полезен при диагностике причины, почему **Xstart** не может запустить X приложение. Хотя окно состояния соединения показывает простой ввод/вывод, оно не подходит для работы терминала, связанной с состоянием соединения или сообщениями об ошибках.

Настройки Протокола SSH

Установите параметры конфигурации, относящиеся к SSH-для Xstart сессии или безопасной XDMCP сессии в которых выбран протокол SSH.

■ Замечание

Для установки протокола SSH, укажите протокол как *SSH* в 'Свойствах Xstart Сессии' вкладки [Основное] и нажмите [Установка]. Как альтернатива, пользователи могут указать метод соединения как *Безопасный XDMCP* в 'Свойствах XDMCP Сессии' вкладки [Основное] и нажать [Установка].

Настройка Безопасного XDMCP

Вкладка SSH

SSH сервер не является XDMCP сервером

Безопасный XDMCP это метод соединения, который позволяет X клиентам соединяться с **Xmanager** на ПК пользователя через SSH туннель. Если SSH сервис не запущен на XDMCP хосте, необходим прокси сервер для проброса SSH. Этот параметр и позволяет настроить такой SSH прокси сервер.

Хост

Введите имя хоста или IP адрес прокси сервера для SSH проброса. В этом случае, пользователям необходимо настроить SSH прокси сервер так, чтобы он был привязан не только к loopback адресу (127.0.0.1) но и к внешним интерфейсам, чтобы разрешить внешние соединения.

Номер Порта

Введите Номер Порта для использования в SSH соединении.

Использовать По Умолчанию

Установить [Номер Порта] как 22, порт по умолчанию для SSH протокола.

Предпочитаемая Версия

Установить версию протокола SSH для использования. Рекомендуется SSH2, так как он предлагает большую безопасность и лучшую функциональность, чем SSH1.

Отправлять сигналы поддержки соединения

Отправлять сигналы поддержки соединения на удалённый хост. Эта функция используется для предотвращения разъединения, пока пользователь временно отсутствует. В некоторых сетевых средах, шлюз или брандмауэр могут сбрасывать соединение без предупреждения, когда соединение находится в режиме ожидания определённый период времени.

Имя Пользователя

Установите имя пользователя, используемое для соединения с удалённым SSH сервером.

Метод

Выберите метод, используемый для аутентификации пользователя. Поддержка SSH методов аутентификации включает в себя Пароль, Публичный Ключ, Интерактивный Ввод, GSSAPI, и PKCS#11. При использовании GSSAPI или PKCS#11 методов, нажмите кнопку [Установка] и введите требуемую информацию.

Пароль

Если выбран метод Пароль или Интерактивный Ввод, здесь надо ввести пароль.

Ключ Пользователя

Если выбран метод Публичный Ключ, пользователь должен указать какой ключ использовать. Нажмите [Просмотр] для выбора ключа пользователя. Пользователи могут также создавать, изменять, удалять, импортировать и экспортировать ключи пользователя из диалогового окна

Ключи Пользователя. За дополнительной информацией, касающейся Публичных Ключей и управления ключами пользователя, обратитесь к разделу “**Аутентификация Пользователя по Публичному Ключу**” и “**Диалоговое Окно Ключей Пользователя**”.

Парольная Фраза

Если выбран метод аутентификации по Публичному Ключу, здесь надо ввести парольную фразу для ключа пользователя. Парольная фраза для ключа пользователя может быть изменена в диалоговом окне Ключ Пользователя.

Использование SSH агента аутентификации (Xagent)

Если вы решите использовать Xagent, сначала будет предпринята попытка аутентификации с помощью открытого ключа. **Xagent** это SSH агент аутентификации. **Xagent** хранит пользовательские ключи, которые используются для аутентификации с открытым ключом, и при необходимости передает ключ клиенту SSH.

Xagent ведет список всех пользовательских ключей клиента SSH и, если необходимо, запрашивает у пользователя ключевую фразу. После ввода правильной ключевой фразы, **Xagent** расшифровывает ключ, и он сохраняется в памяти. Таким образом, с помощью **Xagent** пользователи могут вводить ключевую фразу один раз и использовать ключ несколько раз.

Вкладка Параметры

Шифрование

Алгоритмы шифрования используются для шифрования и дешифрования сетевого трафика. Пользователи могут выбрать свои предпочтительные алгоритмы из списка. Если выбран <Список шифров>, можно попробовать несколько алгоритмов в порядке предпочтения. Чтобы изменить <Список шифров>, нажмите [Изменить].

MAC

MAC (Message Authentication Code) (Имитовставка) гарантирует, что данные, передаваемые по сети, не будут изменены третьим лицом. Это обеспечивает повышенную безопасность протокола SSH2 в сравнении с SSH1. Пользователи могут выбрать свои предпочтительные алгоритмы MAC из списка. Если выбрано <MAC List>, можно попробовать несколько алгоритмов в порядке предпочтения. Чтобы изменить <MAC List>, нажмите [Правка].

Обмен Ключами

Это опции для первоначального обмена ключами SSH. Пользователь может выбрать нужный алгоритм из списка. Имейте в виду, что, если сервер не поддерживает выбранный алгоритм, соединение будет прервано.

Сжатие передаваемых данных (с использованием ZLIB сжатия)

Выберите эту опцию, чтобы сжать весь трафик данных с помощью алгоритма ZLIB. Сжатие обеспечит лучшую производительность в медленной сетевой среде. В зависимости от используемого приложения X, объём передаваемых по сети данных может быть сокращён на 15–80%.

Вкладка Пробросов

Безопасные XDMCP сессии или Xstart сессии с SSH протоколом, используют проброс X11 (TCP/IP проброс с использованием протокола SSH) для запуска X приложений. Пользователи

могут также использовать обычный проброс (SSH проброс) и могут просматривать, добавлять, редактировать и удалять каналы SSH пробросов, зарегистрированные в сессии.

Окно Списка

Этот раздел показывает список правил перенаправления TCP/IP, сохранённые в текущем файле сессии.

Добавить

Пользователи могут добавлять новые правила перенаправления TCP/IP.

Тип(Направление):

- При использовании Локального Проброса, соединения через локальный порт ПК будут перенаправлены на указанный порт другого хоста.
- При использовании Удалённых Пробросов, соединения на порт удалённого хоста, будут перенаправлены на указанный порт другого хоста.
- Динамические Пробросы работают по тому же принципу, что и Локальные за исключением того, что не указывается хост назначения. Для справки, динамическая пересылка использует протокол SOCKS с номером порта по умолчанию 1080.

Исходный Хост: Это хост для приема пакетов во время проброса. Если вы используете Локальный Проброс, пользователи обычно вводят здесь localhost. Если введён IP-адрес, он может быть установлен отдельно для каждого сетевого устройства.

Слушающий Порт: Это номер порта хоста для приема пакетов во время проброса. Если в качестве исходного хоста был введен IP-адрес, его можно установить отдельно для каждого сетевого устройства.

Принимать только локальные подключения: Если эта опция включена, доступ к указанному порту будет заблокирован для других ПК или хостов. Будет обработаны только локальные запросы пробросов.

Хост Назначения: Введите имя хоста или IP-адрес, на слушающий порт которого будут перенаправляться поступившие пакеты.

Порт Назначения: Это номер порта конечного хоста, на который будут перенаправляться поступающие пакеты на порт исходного хоста.

Описание: Введите описание для этого правила проброса.

Правка

Изменить выбранное правило проброса из списка.

Удаление

Удаление выбранного правила проброса из списка.

Настройка Протокола SSH Xstart сессий

Вкладка Основное

Предпочтительная Версия

Выберите версию протокола SSH для использования. Рекомендуется использовать SSH2, поскольку он обеспечивает более высокую безопасность и больше функциональных возможностей, чем SSH1.

Номер Porta

Введите номер порта для использования в SSH соединении.

Порт По Умолчанию

Установить [Номер Porta] как 22, порт SSH протокола по умолчанию.

Отсылать Сигнал Поддержки Соединения

Отправьте сигнал поддержки соединения на удаленный хост. Эта функция используется для предотвращения отключения, когда пользователь временно отсутствует. В некоторых сетевых средах шлюз или система брандмауэра могут прерывать соединения без уведомления, если соединение не используется в течение определенного периода времени.

Метод

Выберите метод, который будет использоваться для аутентификации пользователя. Поддерживаемые методы аутентификации SSH включают пароль, открытый ключ, интерактивную клавиатуру, GSSAPI и PKCS#11. При использовании методов GSSAPI или PKCS#11, нажмите кнопку [Установка] и введите необходимую информацию.

Ключ Пользователя

Если выбран метод с Публичным Ключом, пользователь может указать, какой ключ использовать. Нажмите [Просмотр], чтобы выбрать ключ пользователя. Пользователи также могут создавать, изменять, удалять, импортировать и экспортировать пользовательские ключи из диалогового окна Ключ Пользователя. Для получения дополнительной информации о публичных ключах и управлении пользовательскими ключами см. "**Аутентификация Пользователя с Публичным Ключом**" и "**Диалоговое окно пользовательских ключей**".

Парольная Фраза

Если выбран метод аутентификации по Публичному Ключу, здесь надо ввести парольную фразу для ключа пользователя. Парольная фраза для ключа пользователя может быть изменена в диалоговом окне Ключ Пользователя.

Использование SSH агента аутентификации (Xagent)

Если вы решите использовать Xagent, сначала будет предпринята попытка аутентификации с помощью открытого ключа. **Xagent** это SSH агент аутентификации. **Xagent** хранит пользовательские ключи, которые используются для аутентификации с открытым ключом, и при необходимости передает ключ клиенту SSH.

Xagent ведет список всех пользовательских ключей клиента SSH и, если необходимо, запрашивает у пользователя ключевую фразу. После ввода правильной ключевой фразы, **Xagent** расшифровывает ключ, и он сохраняется в памяти. Таким образом, с помощью **Xagent** пользователи могут вводить ключевую фразу один раз и использовать ключ несколько раз.

Вкладка Параметры

Шифрование

Алгоритмы шифрования используются для шифрования и дешифрования сетевого трафика. Пользователи могут выбрать свои предпочтительные алгоритмы из списка. Если выбран <Список шифров>, можно попробовать несколько алгоритмов в порядке предпочтения. Чтобы изменить <Список шифров>, нажмите [Изменить].

MAC

MAC (Message Authentication Code) (Имитовставка) гарантирует, что данные, передаваемые по сети, не будут изменены третьим лицом. Это обеспечивает повышенную безопасность протокола SSH2 в сравнении с SSH1. Пользователи могут выбрать свои предпочтительные алгоритмы MAC из списка. Если выбрано <MAC List>, можно попробовать несколько алгоритмов в порядке предпочтения. Чтобы изменить <MAC List>, нажмите [Правка].

Обмен Ключами

Это опции для первоначального обмена ключами SSH. Пользователь может выбрать нужный алгоритм из списка. Имейте в виду, что, если сервер не поддерживает выбранный алгоритм, соединение будет прервано.

Сжатие передаваемых данных (с использованием ZLIB сжатия)

Выберите эту опцию, чтобы сжать весь трафик данных с помощью алгоритма ZLIB. Сжатие обеспечит лучшую производительность в медленной сетевой среде. В зависимости от используемого приложения X, объём передаваемых по сети данных может быть сокращён на 15–80%.

Выделять терминал перед выполнением команды

Эта опция выбирается, когда вы хотите выделить виртуальный терминал на удалённом хосте, а затем выполнить в нём команду. Виртуальные терминалы требуются несколькими приложениями X. При выделении виртуальных терминалов переменные среды оболочки устанавливаются в соответствии с общей средой входа в систему.

Вкладка Пробросов

Безопасные XDMCP сессии или Xstart сессии с SSH протоколом, используют проброс X11 (TCP/IP проброс с использованием протокола SSH) для запуска X приложений. Пользователи могут также использовать обычный проброс (SSH проброс) и могут просматривать, добавлять, редактировать и удалять каналы SSH пробросов, зарегистрированные в сессии

Окно Списка

Этот раздел показывает список правил перенаправления TCP/IP, сохранённые в текущем файле сессии.

Добавить

Пользователи могут добавлять новые правила перенаправления TCP/IP.

Тип(Направление):

- При использовании Локального Проброса, соединения через локальный порт ПК будут перенаправлены на указанный порт другого хоста.
- При использовании Удалённых Пробросов, соединения на порт удалённого хоста, будут перенаправлены на указанный порт другого хоста.

- Динамические Пробросы работают по тому же принципу, что и Локальные за исключением того, что не указывается хост назначения. Для справки, динамическая пересылка использует протокол SOCKS с номером порта по умолчанию 1080.

Исходный Хост: Это хост для приема пакетов во время проброса. Если вы используете Локальный Проброс, пользователи обычно вводят здесь localhost. Если введен IP-адрес, он может быть установлен отдельно для каждого сетевого устройства.

Слушающий Порт: Это номер порта хоста для приема пакетов во время проброса. Если в качестве исходного хоста был введен IP-адрес, его можно установить отдельно для каждого сетевого устройства.

Принимать только локальные подключения: Если эта опция включена, доступ к указанному порту будет заблокирован для других ПК или хостов. Будут обработаны только локальные запросы пересылки.

Хост Назначения: Введите имя хоста или IP-адрес, на слушающий порт которого будут перенаправляться поступившие пакеты

Порт Назначения: Это номер порта конечного хоста, на который будут перенаправляться поступающие пакеты на порт исходного хоста.

Правка

Изменить выбранное правило проброса из списка.

Удаление

Удаление выбранного правила проброса из списка.

Настройки Окна Xmanager

Окно Xmanager похоже на Проводник и содержит меню, стандартные кнопки, адресную строку, рабочее пространство, и строку статуса.

Рабочее пространство состоит из дерева категорий сессий и списка ярлыков. Категории сессий включают XDMCP сессии, Xstart сессии, Xshell сессии, и Xftp сессии.

Опция скрытия и показа Xshell и Xftp сессий находится в диалоговом окне **Опции** вкладки [Сессии]. Дополнительно, можно назначить папки XDMCP сессий и Xstart сессий. Если кто-то из пользователей укажет сетевую папку как путь к сессиям, все пользователи смогут пользоваться одинаковыми сессиями.

Для Изменения Пути к Сессиям:

1. Запустите **Xmanager**.
2. Выберите [Параметры] в меню [Инструменты]. Будет показано диалоговое окно **Параметры**.
3. Нажмите вкладку [Сессии].
4. Введите папку сессий, которую надо изменить в пункте [Путь к Сессии].

Замечание

Для восстановления изначального пути, нажмите [Восстановить Путь к Сессии По Умолчанию].

Настройка Столбцов

Диалоговое окно настройки **Столбцов**, позволяет вам управлять размещением столбцов в **Xmanager** в режиме [Подробного] просмотра сессий.

Для Изменения Показываемых Столбцов

1. Запустите **Xmanager**.
2. Выберите [Столбцы] в меню [Вид]. Откроется диалоговое окно **Столбцы**.
3. Выберите или снимите выбор столбца для показа/скрытия.

Создание Папки Сессии

Пользователи могут подключаться ко всем сессиям одновременно, управляя сессиями с помощью папки. Кроме того, управление сессиями, создание, удаление, категоризация и т. д. становится намного проще при использовании папок сессий.

Для Создания Новой Папки Сессии:

1. Запустите **Xmanager**.
2. Укажите [Новая] в меню [Файл] и выберите [Папка].
3. Введите название папки.

Экспорт

Экспортированные сессии сохраняются в одном удобном файле. Когда этот файл импортируется на другом компьютере, на котором установлен Xmanager, импортированные сеансы могут использоваться без дополнительной настройки.

Для Экспорта Сессий:

1. Запустите **Xmanager**.
2. Выберите [Экспорт] из меню [Файл]. Будет показан мастер Импорта/Экспорта Сессий.
3. Выберите продукт для которого экспортируются сессии и нажмите [Далее].
4. Выберите место, куда сохранить экспортируемый файл сессий и нажмите [Далее]. Будет показан результат экспорта сессий.
5. Нажмите [Конец] для завершения экспорта сессий.

Импорт

Xmanager может импортировать сессии из предыдущих версий или сессий, экспортированных с других компьютеров.

Для Импорта Сессий:

1. Запустите **Xmanager**.
2. Выберите [Импорт] из меню [Файл]. Будет показан мастер Импорта/Экспорта Сессий.
3. Укажите точный путь к файлу или нажмите [...] для его поиска.

4. В поле [Действие] пользователь может выбрать, как преобразовать файл сессии. Некоторая информация из оригинального файла сессии, возможно не сможет быть сконвертирована во время преобразования.
5. Выберите что делать с файлом сессии [Если такой уже существует]. Результат будет показан.
6. Нажмите [Далее] для перехода к следующему этапу. Будет показан продукт, включённый в файл и количество сессий.
7. Выберите продукт для которого импортировать сессию и нажмите [Далее]. Сессии будут импортированы и результат будет показан.
8. Нажмите [Конец] для завершения импорта сессий.

Соединение

Ниже подробно описано, как использовать Xmanager и Xstart для подключения к удаленному хосту. В общем, Xmanager используется для подключения к удаленному хосту с использованием протоколов XDMCP. Xstart используется при запуске отдельных приложений X на удаленном хосте.

Соединение с помощью Xmanager

Xmanager отправляет широковещательный XDMCP запрос в локальную сеть или к конкретному хосту и автоматически показывает хосты, которые отвечают на запрос.

Для Соединения с XDMCP Хостом:

1. Запустите **Xmanager**. Будут автоматически показаны хосты для соединения.

■ Замечание

Для показа списка хостов, доступных для соединения в локальной сети, должен быть включён пункт [Искать локальные хосты (Широковещательный XDMCP)]. За настройками поиска локальных хостов в сети, обратитесь к разделу 'Автоматические XDMCP Сессии'.

2. Нажмите дважды на хост для соединения. **Xmanager сервер** запустится и осуществит соединение с хостом по протоколу XDMCP.

■ Замечание

Для обновления списка хостов, доступных для XDMCP соединения, нажмите [Просмотр] - > [Обновить].

Для Соединения с Хостом из Адресной Строки:

1. Запустите **Xmanager**.
2. Введите имя хоста или IP адрес для соединения в адресной строке.
3. Нажмите Ввод.

■ Замечание

За дополнительной информацией об использовании адресной строки, обратитесь к разделу 'Адресная Строка Xmanager'.

Адресная Строка Xmanager

Адресная строка Xmanager это удобный путь для соединения с хостом на лету. Правила ввода адреса в адресной строке следующие:

имя_хоста (или ip_адрес)

xdmcp://имя_хоста

```

xstart://название_сессии

xsession://название_сессии

ssh://[имя_пользователя[:пароль]@]имя_хоста[:порт] [/]

telnet://[имя_пользователя[:пароль]@]имя_хоста[:port] [/]

rlogin://[имя_пользователя[:пароль]@]имя_хоста[:port] [/]

ftp://[имя_пользователя[:пароль]@]имя_хоста[:port] [/]

sftp://[имя_пользователя[:пароль]@]имя_хоста[:port] [/]

```

Используемые протоколы это *xdmcp*, *xstart*, *xsession*, *ssh*, *telnet*, *rlogin*, *ftp* и *sftp*. Если протокол не указан, *xdmcp* будет использован в качестве протокола по умолчанию. Протокол *xdmcp* использует порт UDP 177 как порт по умолчанию.

В таблице приведены примеры использования:

Пример	Описание
<i>foobar.com</i> <i>xdmcp://foobar.com</i>	Соединиться с <i>foobar.com</i> используя XDMCP протокол.
<i>xstart://mysession</i>	Запустить Xstart сессию с названием <i>mysession</i> .
<i>xsession://cdesession</i>	Запустить статическую сессию с названием <i>cdesession</i> .
<i>ssh://myhost:22/</i>	Запустить Xshell и соединиться с <i>myhost</i> портом 22 по протоколу SSH. Для запуска этой команды, на компьютере должен быть установлен Xshell .
<i>telnet://user:pass@myhost</i>	Запустить Xshell и соединиться с <i>myhost</i> по протоколу TELNET. Имя пользователя и пароль будут переданы автоматически после соединения. Для запуска этой команды, Xshell должен быть установлен на компьютере.
<i>rlogin://user@myhost</i>	Запустить Xshell и соединиться с <i>myhost</i> по протоколу RLOGIN. Имя пользователя будет передано автоматически после соединения. Для запуска этой команды, Xshell должен быть установлен на компьютере.
<i>ftp://anonymous@myhost</i>	Запустить Xftp и соединиться с <i>myhost</i> используя FTP протокол. Имя пользователя будет передано автоматически после соединения. Для запуска этой команды, Xftp должен быть установлен на компьютере.
Пример	Описание
<i>sftp://user:pass@myhost/</i>	Запустить Xftp и соединиться с <i>myhost</i> портом 22 используя SFTP (secure shell fire transfer protocol). Имя пользователя и пароль будут переданы автоматически после соединения. Для запуска этой команды Xftp должен быть установлен на компьютере.

Безопасное XDMCP Соединение

Безопасное XDMCP соединение это более безопасное и простое XDMCP соединение, использующее SSH протокол. Протоколы SSH обеспечивают не только безопасное

соединение, но и удобное соединение X11 в сетевых средах, заблокированных брандмауэром, сервером маскарда или шлюзом NAT. Чтобы использовать Безопасный XDMCP, сервер SSH должен работать на удалённом сервере, и должна быть активирована функция пересылки X11.

Для OpenSSH сервера, измените файл настроек (/etc/ssh/sshd_config) следующим образом:

```
X11Forwarding yes
```

Для Secure Shell Communications Security server, измените файл настроек (/etc/ssh2/sshd2_config) следующим образом:

```
AllowX11Forwarding yes
```

Для Создания Безопасной XDMCP Сессии:

1. Запустите **Xmanager**.
2. Нажмите [XDMCP Сессия] в [Новая]
3. Выберите [Метод] как *Безопасный XDMCP* в диалоговом окне **Свойства Сессии** и введите необходимую информацию в поле [Адрес Соединения].

Замечание

Если хост показан в списке XDMCP сессий, вы можете легко создать Безопасную XDMCP сессию нажав правой кнопкой на хост и выбрав [Сохранить как SSH Соединение] в контекстном меню.

Для Установки Безопасной XDMCP Сессии, если XDMCP Хост Не на SSH Сервере:

1. Кликните правой кнопкой на желаемой XDMCP сессии и нажмите [Свойства]. Будет показано диалоговое окно **Свойства Сессии**.
2. Установите [Метод] как Безопасный XDMCP, и нажмите [Установка] справа. Будет показано диалоговое окно **Настройка Безопасного XDMCP**.
3. Активирует [Хост] выбрав [SSH сервер отличается от XDMCP сервера].
4. Введите имя хоста SSH сервера или IP адрес в поле [Хост].
5. Введите информацию о пользователе в поле [Аутентификация Пользователя].
6. Нажмите [OK] для сохранения.

Замечание

Если SSH сервер отличается от XDMCP хоста, введите имя хоста SSH сервера или IP адрес для проброса. В этом случае пользователю необходимо настроить SSH прокси сервер, который будет настроен не только на loopback адрес (127.0.0.1), но также и на внешних интерфейсах. Для OpenSSH, установите значение GatewayPorts в yes в файле настроек SSH сервера.

Для Соединения через Безопасную XDMCP Сессию:

1. Запустите **Xmanager**.
2. Нажмите дважды на Безопасную XDMCP сессию.

Соединение с помощью Xstart

Xstart поддерживает SSH, TELNET, RLOGIN, REXEC, RSH, и LOCAL протоколы. Для использования каждого протокола, соответствующий демон сервиса должен быть запущен на удаленном хосте. LOCAL протокол используется когда X приложение находится на ПК пользователя.

Для запуска X приложения через протокол SSH:

1. Запустите **Xstart** из папки **Инструменты** в папке **Xmanager**.
2. Нажмите [Новая]. Откроется диалоговое окно **Новая Сессия**.
3. Введите имя новой сессии и нажмите [OK].
4. Введите имя или IP адрес UNIX/Linux хоста в поле [Хост].
5. Выберите **SSH** из списка [Протокол].
6. Нажмите [Установка] для установки дополнительных параметров SSH протокола, таких как номер порта или параметры шифрования.

Замечание

За дополнительной информацией о настройках Протокола SSH, смотрите '**Настройки Протокола SSH для Xstart сессий**'.

7. Введите имя пользователя на удалённом сервере в поле [Имя Пользователя].
8. Выберите метод аутентификации в [Аутентификация] и установите пароль, если нужно.

Замечание

За дополнительной информацией о настройке каждого метода аутентификации, смотрите '**Настройки Аутентификации Пользователя в Xstart**'.

9. Введите команду для запуска на удалённом хосте, в поле [Команда]. Для запуска **xterm**, введите команду следующим образом:

```
/usr/bin/X11/xterm -ls
```

Замечание

Для SSH соединений, переменная DISPLAY автоматически установится в значение, предоставленное SSH сервером.

10. Нажмите [Запуск].

Для Запуска Удаленного X Приложения по Протоколу TELNET:

1. Запустите **Xstart**.
2. Нажмите [Новая]. Откроется диалоговое окно **Новая Сессия**.
3. Введите имя новой сессии и нажмите [OK].
4. Введите имя или IP адрес UNIX/Linux хоста в поле [Хост].
5. Выберите **TELNET** из списка [Протокол].

6. Нажмите [Установка] для установки параметров протокола TELNET, таких как порт или таймаут.

 Замечание

Метод соединения для RLOGIN, REXEC, и RSH протоколов схожи с соединением по протоколу TELNET. Установите порт и таймаут в диалоговом окне **Настройки Протокола**. Порт по умолчанию для каждого протокола:

TELNET:	23
REXEC:	512
RLOGIN:	513
RSH:	514

После успешного входа, будет предоставлена командная оболочка, назначенная в соответствии с протоколами TELNET и RLOGIN серверов на удалённом хосте и **Xstart** выполнит команду в приглашении оболочки. **Xstart** закрывает соединение после указанного таймаута и оболочка закрывается в то же самое время. Если таймаут выставлен в 0, соединение не закрывается, пока **Xmanager** запущен. Если оболочка закрывается, X приложение, выполняющееся в оболочке, может также закрыться.

7. Введите имя пользователя на удалённом хосте [Имя Пользователя].
8. Только *Пароль* может быть выбран в поле [Аутентификация]. Нажмите [Установка] для ввода пароля.
9. Введите команду, которая будет выполнена на удалённом хосте в поле [Команда]. Для запуска **xterm**, введите следующую команду:

```
/usr/bin/X11/xterm -ls -display $DISPLAY
```

10. Нажмите [Запуск].

Для Запуска Локального X Приложения с Помощью Xstart:

1. Запустите **Xstart**.
2. Нажмите [Новая]. Откроется диалоговое окно **Новая Сессия**.
3. Введите имя новой сессии и нажмите [ОК].
4. Выберите *ЛОКАЛЬНАЯ* из списка [Протокол].
5. Введите полный путь к команде в поле [Команда].
6. Нажмите [Запуск].

Настройки Аутентификации Пользователя в Xstart

Для Установки Пароля или Интерактивного Ввода с Клавиатуры:

1. Запустите **Xstart**.
2. Выберите *Пароль* или Интерактивный Ввод в поле [Аутентификация] и нажмите [Установка]. Будет показано диалоговое окно **Установка Пароля**.
3. Введите пароль.

4. Выберите [Сохранить пароль] и нажмите [OK] для сохранения введенного пароля в сессии.
5. Для удаления пароля, нажмите [Сбросить Пароль].

 Замечание

Интерактивный ввод с помощью клавиатуры, работает путём ввода требуемого значения в сообщении, отправляемом с сервера SSH. Обычно используется, когда часто меняется пароль или используется OTP. Если иное не указано сервером, начальное значение пароля совпадает с паролем учётной записи пользователя.

Для Установки Публичного Ключа:

1. Запустите **Xstart**.
2. Выберите *Публичный Ключ* в поле [Аутентификация] и нажмите [Установка]. Будет показано диалоговое окно **Настройка Аутентификации по Публичному Ключу**.
3. Выберите ключ пользователя, участвующий в аутентификации.
4. Введите парольную фразу.

 Замечание

Для дополнительной информации по настройке публичного ключа, смотрите 'Аутентификация Пользователя по Публичному Ключу'.

Для максимальной безопасности, вводите парольную фразу во время каждого соединения вместо сохранения её в сессии. При указании ввода пароля каждый раз, 'Диалоговое окно SSH аутентификации пользователя', будет запрашивать пароль при каждой попытке соединения.

Для Установки Kerberos:

Xmanager поддерживает MIT Kerberos и Microsoft's SSPI. Эта статья предполагает, что у вас уже есть работающий Kerberos сервер и клиент. Когда сессия открывается, она попытается использовать реквизиты Kerberos для указанного пользователя. Это должен быть тот же пользователь, что и в Network Identity Manager.

1. Запустите **Xstart**.
2. Для [Аутентификации], выберите GSSAPI и нажмите [Установка]. Появится диалоговое окно **Установка GSSAPI**.
3. Выберите тип GSSAPI аутентификации для использования.

 Замечание

Если ПК, на котором работает Xmanager использует поддерживаемый Xmanager модуль Kerberos, Xmanager может только автоматически авторизоваться на SSH сервере если выбрана аутентификация GSSAPI. Для соединения с другим сервером, использующим Kerberos аутентификацию с сервера, тоже использующего Kerberos аутентификацию, выберите параметр 'Разрешить Передачу Полномочий GSSAPI'.

Для установки PKCS#11:

1. Запустите **Xstart**.
2. Для [Аутентификации], выберите PKCS#11 и нажмите [Установка]. Появится диалоговое окно **Установка PKCS#11**.
3. Введите путь к промежуточной программе, которая соединяется с аппаратным токеном, который содержит ключ пользователя. Или нажмите [...] для её поиска.
4. Если на аппаратном токене установлен пин код, введите его.

Определение Тэгов Команд Xstart

Xstart предоставляет функции тэгов команд для автоматизации повторяющихся команд. Теги команд вводятся в поле [Команда].

Тэг	Описание
<%CR%>	Послать символ CR (Возврат Каретки, \r).
<%LF%>	Послать символ LF (Перевод Строки, \n).
<%SEND="string"%>	Отправить строку символов. Xstart не преобразовывает переменные DISPLAY и PCADDR в строку символов.
<%WAIT="string1 string2"%>	Ожидание строки string1 или string2.
<%SLEEP=n%>	Заснуть на n секунд.
<%POPUP="string"%>	Открыть окно Результата Удалённого Выполнения , если получена указанная строка.

Все теги обрабатываются последовательно, за исключением тега POPUP, который действителен до полного выполнения команды.

Замечание

Тэги команд поддерживаются протоколами TELNET и RLOGIN. Для их использования в протоколе SSH, выберите [Выделять терминал перед выполнением команды] во вкладке [Опции] в диалоговом окне **Установка SSH протокола**. При выделении терминала, переменные окружения оболочки устанавливаются в те же самые, что и при обычном входе.

Пример

1. Следующая команда это пример нескольких последовательных входов. Вход на хост через **Xstart**, и соединение на другой хост по **telnet** и запуск там **xterm**:

```
telnet host2<%CR%><%WAIT="login:"%>root<%CR%>  
<%WAIT="Password:"%>password<%CR%><%WAIT="$"%>xterm -ls -display $DISPLAY
```

2. Следующая команда является примером отображения окна **Результата удаленного выполнения**, когда отображается строка символов "assword:". Эта команда полезна, когда срок действия пароля истекает в фиксированном цикле, и

перед отображением приглашения командной строки необходимо ввести новый пароль.

```
<%POPUP="assword:"%>xterm -ls -display $DISPLAY
```

Настройки Брандмауэра

Специальные настройки требуются, если удаленный хост находится в другой сети на противоположной стороне шлюза или если между ПК пользователя и удаленным хостом установлен межсетевой экран. Это связано с тем, что **Xmanager** является серверной программой, а удаленные приложения X подключаются к **Xmanager** на ПК пользователя.

Опция поддержки связи для сохранения соединений, которая поддерживается протоколами SSH, полезна, когда брандмауэр принудительно завершает соединение, которое простаивает в течение заданного периода времени.

Переадресация портов требуется для подключений XDMCP, когда вы находитесь в частной сети и подключаетесь к удаленному хосту через маршрутизатор. После того как вы настроили переадресацию портов на маршрутизаторе, вы должны настроить адрес подключения для XDMCP.

Для Использования Опции Поддержки Связи для SSH Соединений в Брандмауэре:

1. Запустите **Xstart**.
2. Выберите сессию из списка [Сессий].
3. Выберите **SSH** из списка [Протокол].
4. Нажмите [Установка]. Будет показано окно **Установка Протокола SSH**.
5. Нажмите вкладку [Основное].
6. Выберите [Отсылать сигнал поддержки связи].
7. Нажмите [OK].

Для Установки Проброса Porta на Маршрутизаторе:

1. Соединитесь с маршрутизатором и перейдите на страницу настройки проброса порта.
2. Пробросить внешний диапазон портов TCP 6000 ~ 6010 на 6000 ~ 6010 порты на ПК пользователя, если IP адрес ПК пользователя 192.168.1.2:

Порт маршрутизатора	ПК Порт	Адрес
6000	6000	192.168.1.2
6001	6001	192.168.1.2
...		
6010	6010	192.168.1.2

Замечание

Номер порта маршрутизатора не обязательно должен совпадать с номером порта ПК. Однако X приложения пытаются установить соединение с IP-адресом и соответствующим портом маршрутизатора. Поскольку маршрутизатор пересылает пакеты на порт ПК в соответствии с правилами переадресации портов, номер дисплея, указанный в файлах сеансов **Xmanager**, должен совпадать с портом, указанным в правилах переадресации портов маршрутизатора. Номер дисплея **Xmanager**, добавленный к 6000, становится номером порта.

3. Сохраните настройки.
4. В сессии Xstart, значения, относящиеся к опциям –display, должны быть назначены как номера дисплея, относящиеся к IP адресу маршрутизатора и номеру порта ПК, определённого в настройках проброса порта роутера. Для XDMCP сессий, необходимо установить [Адрес Соединения].

 Замечание

За подробностями настройки проброса порта, обратитесь к описанию вашего маршрутизатора.

Для Установки Адреса Соединения для XDMCP Сессии:

1. Запустите **Xmanager**.
2. Нажмите правой кнопкой на сессию, для которой необходимо установить адрес соединения.
3. Выберите [Свойства].
4. Нажмите вкладку [Основное].
5. Выберите *Назначенный Пользователем* [Тип Адреса] в поле [Адрес Соединения].
6. Введите IP адрес роутера в поле [Адрес Соединения] в [IP Адрес].
7. Введите порт, назначенный в качестве порта проброса на роутере в поле [Адрес Соединения] [Номер Порта].

 Замечание

Номер порта, это порт на стороне маршрутизатора, который настроен для проброса порта от роутера до ПК пользователя.

8. Нажмите вкладку [X Сервер].
9. Деактивируйте значение [Выделять номер дисплея автоматически] в поле [Номер Дисплея].
10. Введите номер дисплея в поле [Номер Дисплея] в соответствии с номером порта ПК, назначенного в настройках порта проброса на маршрутизаторе.

 Замечание

Номер дисплея соответствует номеру порта ПК, предназначенного для проброса с маршрутизатора на ПК. Номер порта минус 6000 и будет номер дисплея.

11. Нажмите [ОК].

Решение Проблем Соединения

Даже если вы выполнили все шаги выше, соединение с удалённым хостом может не состояться из-за пользовательских настроек. В этом разделе кратко представлены методы решения проблем, связанных с подключением.

Для Решения Проблем с XDMCP Соединениями:

1. Проверьте следующее:

- Выполняются ли **dtlogin**, **kdm**, **gdm**, **lightdm**, или **xdm** на удалённом хосте?
- Показывается ли окно входа?
- Удалённый хост в другой сети?
- Есть ли брандмауэр между удалённым хостом и ПК пользователя?
- Настроен ли брандмауэр на ПК пользователя?
- Адрес ПК пользователя может быть некорректно установлен на сервер имён.
- Переменная **DISPLAY** может быть настроена в скрипте командной оболочки пользовательского аккаунта.

2. Посмотрите сообщения журнала.

- Для просмотра файла журнала **Xmanager**, перейдите на [Журнал] в главном окне системного меню **Xmanager сервера** и выберите [Файл].
- Если окно приглашения ко входу не показывается в графической среде CDE, проверьте `/var/dt/Xerrors` файл. Если вход не удался, проверьте `$HOME/.dt/startlog` и `$HOME/.dt/errorlog` файлы.

■ **Замечание**

Дополнительные сведения о файлах журналов можно получить в разделе 'Журнал Сессии'.

Для решения Проблем Соединения Xstart:

1. Запустите **Xstart**.
2. Выберите [Показывать окно статуса соединения].
3. Нажмите [Запуск]. Откроется окно **Xrcmd: Результат удалённого выполнения**.
4. Прочитайте сообщение и определите причину проблемы.

■ **Замечание**

Окно **Результата удалённого выполнения**, это информационное окно статуса соединения. Возможен ввод простых команд. Однако существует много ограничений при выполнении задач, таких как эмуляция терминала. Это окно показывает процесс только до запуска программы, включающей команду выполнения, что является целью **Xstart**.

Опции Командной Строки Xmanager сервера

Xmanager сервер (Xmanager.exe) поддерживает опции командной строки для стыковки с другими приложениями пользователя. Когда пользователь запускает напрямую **Xmanager**, методы соединения и номера дисплея должны быть указаны в качестве параметра. Правила ввода командной строки **Xmanager** следующие:

```
Xmanager [-query имя_хоста|-broadcast|-indirect имя_хоста] [:цифра]
```

Команда	Описание
Xmanager	Запуск в пассивном режиме с использованием [Xstart Профиля По Умолчанию]. Номер дисплея установлен в 0, значение по умолчанию. Если это значение недоступно, будет автоматически присвоено другое значение.
Xmanager :1	Запуск в пассивном режиме с использованием [Xstart Профиля По Умолчанию]. Номер дисплея установлен в 1. Если это значение недоступно, будет автоматически присвоено другое значение.
Xmanager -query хост	Соединение с указанным хостом с использованием метода XDMCP Запрос. Будет использован [XDMCP Профиль По Умолчанию]. Номер дисплея установлен в 0, значение по умолчанию. Если это значение недоступно, будет автоматически присвоено другое значение.
Xmanager -query хост :2	Соединение с указанным хостом с использованием метода XDMCP Запрос. Будет использован [XDMCP Профиль По Умолчанию]. Номер дисплея установлен в 2. Если значение не доступно, выполнение остановится.
Xmanager -broadcast	Показать XDMCP хосты, доступные для соединения в диалоговом окне Выбор , направив Широковещательное сообщение XDMCP в локальную сеть. Будет использован [XDMCP Профиль По Умолчанию]. Номер дисплея установлен в 0, значение по умолчанию. Если это значение недоступно, будет автоматически присвоено другое значение.
Xmanager -indirect хост	Соединение с хостом с использованием Непрямого метода XDMCP соединения. Удалённый хост откроет окно Выбора через Xmanager сервер . Будет использован [XDMCP Профиль По Умолчанию]. Номер дисплея установлен в 0, значение по умолчанию. Если это значение недоступно, будет автоматически присвоено другое значение.

Параметры Командной Строки Xrcmd

Xstart предоставляет параметры командной строки, которые позволяют продвинутым пользователям интегрировать программу с их приложениями. В действительности, **Xstart** только предоставляет пользовательский интерфейс для создания и управления сессиями. Когда пользователь открывает сессию с помощью **Xstart**, он выполняет команду **Xrcmd.exe** и перенаправляет информацию о сессии. Поэтому для прямых подключений, должен быть использован **Xrcmd.exe**, не **Xstart**. **Xrcmd** можно найти в папке, где установлен **Xmanager**.

The Xrcmd Command Line Rules are As Follows:

```
Xrcmd -protocol ssh|telnet|rexec|rsh|rlogin|local -host имя_хоста
      [-user имя_пользователя] [-password пароль] [-userkey ключ]
```

```
[-passphrase пароль_ключа] [-shell] [-zlib] [-status]
[-result] [-dispno nnn] [-timeout nnn] [-port nnn]
-command удалённая_команда
```

Замечание: `-command` параметр должен находиться в конце.

Параметры:

Tag	Description
<code>-protocol</code> <i>протокол</i>	Назначает протокол соединения
<code>-host</code> <i>имя_хоста</i>	Назначает удалённый хост
<code>-user</code> <i>имя_пользователя</i>	Назначает имя пользователя на удалённом хосте
<code>-password</code> <i>xxxx</i>	Назначает пароль пользователя на удалённом хосте
<code>-userkey</code> <i>ключ</i>	Назначает название ключа пользователя. Этот параметр используется только для SSH соединений.
<code>-passphrase</code> <i>пароль_ключа</i>	Вводит парольную фразу ключа. Этот параметр используется только для SSH соединений.
<code>-shell</code>	Выполняет команду после запуска оболочки (терминала). Этот параметр применяется только для SSH соединений.
<code>-zlib</code>	Сжимать сетевые данные согласно zlib алгоритма. Этот параметр применяется только для SSH соединений.
<code>-status, -result</code>	Показывает окно Результата удалённого выполнения .
<code>-dispno nnn</code>	Назначает номер дисплея в Xmanager сервер . Если этот параметр не установлен, Xmanager сервер автоматически присвоит нужное значение.
<code>-timeout nnn</code>	Закрывает соединение после <i>nnn</i> секунд.
<code>-port nnn</code>	Назначает номер порта для соединения. Если этот параметр не установлен, будет использован порт по умолчанию для протокола.
<code>-command</code> <i>команда</i>	Назначает команду, которая будет выполнена на удалённом хосте.

Пример:

```
Xrcmd -protocol telnet -host mylinux -user myname -status
-command /usr/bin/X11/xterm -ls
```

Xrcmd соединится с *mylinux* по протоколу *telnet* и зайдет с именем пользователя *myname*. Затем будет выполнена команда *xterm* на удалённом хосте. Статус соединения может быть проверен с помощью окна **Результата удалённого выполнения** во время соединения.

Настройки Профиля Сервера

Профиль сервера содержит параметры **Xmanager сервера**, такие как режим окна, шрифты, цвета, и параметры безопасности.

Xconfig показывает все профили **Xmanager**, доступные для использования. Пользователи могут индивидуально назначать профиль для XDMCP и Xstart сессий.

Общий профиль отображается со значком в форме руки и может быть изменен только пользователями с разрешениями системного администратора. Для профиля XDMCP по умолчанию или профиля Xstart по умолчанию значок помечается черной галочкой сверху. Дважды щелкните значок, чтобы изменить свойства каждого профиля.

Управление Профилем

Когда пользователь создаёт сессию, изначально, ей будет присвоен профиль по умолчанию. **Xmanager** поддерживает профиль по умолчанию Xstart и XDMCP профиль по умолчанию. Xstart профиль по умолчанию применяется, когда [Профиль Сервера] установлен как *Авто Выбор* в сессии Xstart. XDMCP профиль по умолчанию применяется, когда [Профиль Сервера] устанавливается как *Авто Выбор* в XDMCP сессии. Все автоматические XDMCP сессии используют XDMCP профиль по умолчанию.

Для Создания Профиля Сервера:

1. Запустите **Xconfig**.
2. Выберите [Новый] в меню [Файл]. Новый профиль будет создан в окне **Xconfig**.
3. Нажмите дважды на новый профиль. Будет показано диалоговое окно **Свойства профиля**.
4. Установите параметры.
5. Нажмите [OK].

Для Установки Профиля в качестве Xstart Профиля По Умолчанию:

1. Запустите **Xconfig**.
2. Нажмите правой кнопкой на профиль, который необходимо установить в качестве **Xstart** профиля по умолчанию.
3. Выберите [Установить, как **Xstart** профиль по умолчанию].

Для Установки Профиля в качестве XDMCP Профиля По Умолчанию:

4. Запустите **Xconfig**.
5. Нажмите правой кнопкой на профиль, который необходимо установить в качестве XDMCP профиля по умолчанию.
6. Выберите [Установить, как XDMCP профиль по умолчанию].

Для Совместного Использования Профиля с Другими Пользователями:

1. Запустите **Xconfig**.
2. Нажмите правой кнопкой на профиль для того, чтобы сделать его общим.

3. Выберите [Сделать Общим]. Значок в форме руки будет добавлен к значку профиля сервера.

Для Экспорта Профиля в Папку:

1. Запустите **Xconfig**.
2. Нажмите на профиль мышкой и перенести его во внешнюю папку.

Для Импорта Профиля в Xconfig:

1. Запустите **Xconfig**.
2. Нажмите на профиль мышкой и перенести его из внешней папки в **Xconfig**.

Оконные режимы

Xmanager поддерживает Режим Одного Окна (в основном используется в сессиях XDMCP) и Многооконный Режим (в основном используется в сессиях Xstart). В Режиме Одного Окна, Вы можете настроить размер основного окна и добавить полосу прокрутки, когда рабочий стол X больше, чем рабочий стол Windows.

В Многооконном режиме вы можете выбрать оконный менеджер и фон рабочего стола. Кроме того, вы можете установить панорамирование и функцию автоматического поднятия, чтобы активировать окно на фокусе мыши.

Замечание

В Режиме Одного Окна, **Xmanager сервер** открывает одно большое окно. Открытие сессии с помощью 'Открыть в новом окне,' означает открытие в совершенно новом окне, и 'Открыть в новой вкладке,' которая означает открытие в новой вкладке в Xmanager, и оба используют Режим Одного Окна. Доступ к системному меню можно получить через строку заголовка 'Открыть в новом окне' и через меню вкладок через 'Открыть в новой вкладке.'

В Многооконном режиме, значок **Xmanager сервера** создаётся в области уведомлений. Для доступа к системному меню Xmanager, нажмите правой кнопкой на значок в области уведомлений.

Для Использования Xmanager в Режиме Одного Окна:

1. Запустите **Xconfig**.
2. Нажмите дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Режим Одного Окна* из [Выбрать Режим Окна].
5. Нажмите [OK].

Для Установки Размера Главного Окна в Режиме Одного Окна:

1. Запустите **Xconfig**.
2. Нажмите дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Режим Одного Окна* из списка [Выбрать Режим Окна].
5. Нажмите [Установки]. Будет показано диалоговое окно **Настройки Оконного Режима**

6. Нажмите на вкладку [Режим Одного Окна].
7. Выберите необходимый размер из списка [Размер Окна].
8. Нажмите [ОК].

 Замечание

Для *Размера Рабочего Стола*, запустите Xmanager сервер по размеру рабочего стола, за исключением панели задач.

Для *Полного Экрана*, запустите Xmanager сервер по размеру всего экрана без строки заголовка и оконной рамки. Панель управления Windows также не будет показана.

Для использования Многооконного режима:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Многооконный Режим* из списка [Выбор Оконного Режима].
5. Нажмите [ОК].

Для Использования Панорамирования в Многооконном Режиме:

1. Запустите **Xconfig**.
2. Нажмите Дважды На профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Многооконный режим* из списка [Выбор Оконного Режима].
5. Нажмите [Установки]. Будет показано диалоговое окно **Настройки Оконного Режима**.
6. Нажмите на вкладку [Многооконный Режим].
7. Выберите [Использовать Панораму].
8. Нажмите [Настройки Панорамы] для установки параметров.
9. Установите скорость и положение в диалоговом окне **Настройки Панорамы**.
10. Нажмите [ОК].

 Замечание

Панорамирование можно использовать только при использовании локального оконного менеджера.

Эта опция полезна, когда размер окна больше рабочего стола, а некоторые области окна расположены за пределами рабочего стола. Каждый раз, когда указатель мыши перемещается в области панорамы, окно панорамы перемещается в области рабочего стола на пиксели, обозначенные в скорости панорамирования.

Для Использования Авто Поднятия в Многооконном Режиме:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Многооконный Режим* из списка [Выбор Оконного Режима].

5. Нажмите [Установки]. Будет показано диалоговое окно **Настройки Оконного Режима**.
6. Нажмите на вкладку [Многооконный Режим].
7. Выберите [Поднимать Окно Автоматически].
8. Нажмите [OK].

ДляВыбораФонавМногооконномРежиме:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Многооконный Режим* из списка [Выбор Оконного Режима].
5. Нажмите [Установки]. Будет показано диалоговое окно **Настройки Оконного Режима**.
6. Нажмите на вкладку [Многооконный Режим].
7. Выберите Фон из списка [Фон Окна].
8. Нажмите [OK].

Замечание

Когда установлен *Фон Windows*, фон управляется Windows. В этом режиме, фон окна X не используется.

Когда установлен режим Фон Окна X, фон управляется Xmanager. Фон изменяется на основное окно X, указатель мыши меняется на форму X указателя. В этом режиме, значки Windows на рабочем столе не могут быть использованы.

Фон Окна X(Прозрачный) работает также, как и режим Фон Окна X. Он выглядит как Фон Windows, и вы будете видеть значки на рабочем столе Windows, но значки не будут активны.

ДляВыбораОконногоМенеджеравМногооконномРежиме:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Основное].
4. Выберите *Многооконный Режим* из списка [Выбор Оконного Режима].
5. Нажмите [Установки]. Будет показано диалоговое окно **Настройки Оконного Режима**.
6. Нажмите вкладку [Многооконный Режим].
7. Выберите оконный менеджер из списка [Оконный Менеджер].
8. Нажмите [OK].

Замечание

Оконный менеджер управляет X приложениями. Он добавляет строку заголовка, рамку, и системное меню в окно. Дополнительно, он предлагает функции изменения размера окна, передвижения окна, и закрытия окна. Локальный оконный менеджер выглядит как Windows и добавляет строку заголовка и рамку к X приложению, как и к программе Windows. Удалённые оконные менеджеры, такие как dtwm, mwm и fvwm, выполняются на удалённом хосте и выглядят не так из локального оконного менеджера.

Xmanager поддерживает *Автоматическое Переключение*, *Только Удалённое*, и *Только Локальное* для режимов оконного менеджера.

В режиме *Автоматического Переключения*, оконный менеджер меняется автоматически. Первоначально, Xmanager запускает локальный оконный менеджер, и когда удалённый оконный менеджер пытается соединиться с Xmanager, локальный оконный менеджер автоматически закрывается. И если удалённый оконный менеджер закрывается пользователем, локальный оконный менеджер запустится снова.

В режиме *Только Удалённый*, локальный оконный менеджер не выполняется. Запустите удалённый оконный менеджер для управления окнами X приложений.

В режиме *Только Локальный*, соединение удалённому оконному менеджеру не разрешено. Все окна X приложений управляются также, как и приложениями Windows.

При использовании сред удалённого рабочего стола пользователя, при запуске `gnome-session`, `startkde`, и других команд, оконный режим должен быть установлен в *Автоматическое Переключение* или *Только Удалённый*.

Настройки Параметров Соединения

Функция поддержки связи используется, когда соединение неожиданно закрывается во время простоя. В некоторых сетевых средах, шлюз или брандмауэр принудительно отключают соединение, если за определённый промежуток времени отсутствует передача данных.

Функция автоматического закрытия используется для автоматического закрытия Xmanager, когда за определённый промежуток времени от пользователя не поступает никаких вводимых данных.

Для Сохранения Связи:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Соединение].
4. Выберите [Отсылать TCP пакеты поддержки связи во время бездействия сети].
5. Введите время ожидания в режиме бездействия (в секундах) в поле [Таймаут].

Для Установки Автоматического Закрытия:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Соединение].
4. Выберите [Закрывать сессию во время бездействия].
5. Введите время ожидания в режиме бездействия (в минутах) в поле [Таймаут].

■ **Замечание**

Когда Xmanager закрывается во время автоматического закрытия, все X приложения могут неожиданно завершиться и может произойти потеря важных данных.

Управление Шрифтами

Xmanager предоставляет шрифты, необходимые в большинстве систем и приложений. Однако пользователям может потребоваться добавить новые шрифты напрямую.

Для Загрузки и Установки Дополнительных Пакетов Шрифтов:

1. Перейдите на страницу загрузки **Xmanager**:
<http://www.netsarang.com/download/font.html>
2. Загрузите дополнительные пакеты шрифтов для установки.
3. Запустите пакеты шрифтов на системе пользователя.
4. Установите пакет шрифтов согласно инструкций, выводимых во время процесса установки.

■ **Замечание**

Когда дополнительные пакеты шрифтов установлены, папка шрифтов будет автоматически добавлена во все серверные профили, так, что новую папку шрифтов не нужно будет регистрировать отдельно для каждого профиля сервера при использовании **Xconfig**.

Для преобразования BDF Шрифта в PCF Шрифт:

1. Запустите программу **bdftopcf.exe** как в следующем примере:
`C:\tmp> %XMANAGER_INSTALL_DIR%\bdftopcf new.bdf -o new.pcf`

Для Создания или Обновления файла FONTS.DIR, используйте программу Mkfntdir.exe:

1. Перейдите в папку со шрифтами и запустите программу **mkfntdir.exe**:
`%XMANAGER_INSTALL_DIR%\Fonts\NewFonts> ..\..\mkfntdir`

Для Создания и Использования Папки Шрифтов:

1. Создайте новую папку в следующей папке:
`%XMANAGER_INSTALL_DIR%\Fonts`
2. Скопируйте новый файл шрифтов в созданную папку.
3. Запустите программу **mkfntdir.exe** в созданной папке:
`%XMANAGER_INSTALL_DIR%\Fonts\NewFonts> ..\..\mkfntdir`
4. Запустите **Xconfig**.
5. Дважды кликните на профиль, которому необходимо добавить новые шрифты. Будет показано диалоговое окно **Свойства Профиля**.
6. Нажмите на вкладку [Шрифт].

7. Нажмите [Добавить Папку Шрифтов]. Будет показано диалоговое окно **Просмотр Папки**.
8. Выберите новую папку со шрифтами.
9. Нажмите [OK].
10. Перезапустите **Xmanager**.

Для Использования Сервера Шрифтов:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Шрифт].
4. Нажмите [Добавить Сервер Шрифтов]. Будет показано диалоговое окно **Добавить Сервер Шрифтов**.
5. Введите имя сервера шрифтов или IP адрес в поле [Хост].
6. Введите номер порта сервера шрифтов в поле [Порт].
7. Нажмите [OK].

Замечание

Проверьте, что сервер шрифтов работает на удалённом сервере. Обычно программа сервера шрифтов называется **xfs** и порт по умолчанию у неё 7100.

Для Изменения шрифта По Умолчанию:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Шрифт].
4. Введите название шрифта для использования его в качестве основного [Шрифт По Умолчанию].
5. Нажмите [OK].

Замечание

Шрифт по умолчанию используется, когда приложение X не определяет шрифт для отображения текста.

Для Замены Шрифта другим Шрифтом, когда Шрифт не Найден:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Шрифт].
4. Выберите [Автоматическая Подмена Шрифта].
5. Нажмите [OK].

Для Показа Диалогового Окна Ошибки Шрифта:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Шрифт].

4. Выберите [Показывать Диалог Отсутствия Шрифта].

■ **Замечание**

Сообщение о пропущенном шрифте используется для поиска шрифта, когда шрифт, используемый удалённым приложением X, недоступен в Xmanager. Информация об отсутствии шрифта всегда записывается в журнал Xmanager. Даже если в Xmanager шрифт недоступен, сообщение об отсутствующем шрифте может не отображаться некоторыми приложениями X. В этом случае найдите необходимые шрифты, обратившись к журналу или сообщениям об ошибках соответствующего приложения X.

5. Нажмите [OK].

Управление Цветом

Визуализация, это независимая от устройства цветовая система, которая определяет формат цвета **Xmanager** и количество поддерживаемых цветов. **Xmanager** поддерживает *PseudoColor*, *StaticColor*, *DirectColor*, *TrueColor*, *GrayScale*, и *StaticGray*, шесть визуализаций, поддерживаемых в стандартах X window.

В визуализации *PseudoColor*, все X приложения могут использовать только 256 цветов и, следовательно, выполнение приложения может завершиться неудачей из-за неадекватного количества цветов. Используйте параметр [Автоматическая замена цвета (PseudoColor)] для успешного запуска приложения в случае, если цветовая палитра недостаточна из-за другой программы.

Windows использует 20 системных цветов в 256-цветном режиме для отображения строк заголовка, оконных рам и значков. В некоторых приложениях X вся 256-цветная палитра используется для правильного отображения цветов. В этом случае рабочий стол и значки Windows могут мигать. Выберите параметр [Сохранить системные цвета (20 цветов)], чтобы это предотвратить.

Кроме того, **Xmanager** предоставляет базу данных RGB, которая используется для изменения имен цветов на соответствующие значения RGB. Пользователи могут редактировать базу данных с помощью текстового редактора.

Для Изменения Визуализации Сервера По Умолчанию:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Цвета].
4. Выберите соответствующую визуализацию из списка [Выбрать Визуализацию По Умолчанию].
5. Нажмите [OK].

■ **Замечание**

Если визуализация по умолчанию установлена как *Авто Обнаружение*, Xmanager выберет подходящую визуализацию в соответствии с видео устройством. В 256-цветном режиме (8 бит), будет установлено как *PseudoColor*. В режиме истинного цвета (16 бит или выше), будет установлено как *TrueColor*. Визуализация по умолчанию используется в главном окне X window и большинстве приложений.

Для Поддержки Exact StoreColor Запросов (PseudoColor):

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Цвет].
4. Выберите [Exact StoreColor (PseudoColor)].
5. Нажмите [OK].

Замечание

Когда видео устройство с истинными цветами работает с визуализацией PseudoColor, StoreColor вызывает перегрузки и ухудшает общую производительность. Xmanager поддерживает параметр отключающий Exact StoreColor.

Для Работы Видео Устройства с Истинными Цветами с 256-цветной Визуализацией:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Цвета].
4. Выберите PseudoColor из списка [Выберите Визуализацию По Умолчанию].
5. Нажмите на вкладку [Расширенное].
6. Выберите [When Mapped] в [Backing Store].
7. Нажмите [OK].

Замечание

Некоторые старые CAD программы работают в 256-цветной системе, и таким образом визуализация по умолчанию должна быть изменена на PseudoColor для успешного выполнения.

Для Изменения в RGB Формате в Визуализации с Истинными Цветами:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Цвет].
4. Выберите [RGB в Обратной Последовательности (Настоящие Цвета)].
5. Нажмите [OK].

Замечание

Эта функция полезна, когда приложение X требует специальный RGB формат.

Для Изменения или Редактирования Базы Данных RGB Цветов:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Цвет].
4. Нажмите [Изменить] или [Просмотр] в поле [Набор Цветов].
5. Нажмите [OK].

Настройки Клавиатуры

Пользователи могут создавать или изменять файл клавиатуры, назначить горячую клавишу для изменения файла клавиатуры в реальном времени и редактировать файл клавиатуры с помощью редактора клавиатуры. **Xmanager** предоставляет файлы клавиатуры, созданные заранее для большинства языков и клавиатур. Таким образом, пользователи могут найти и использовать клавиатуру, соответствующую их приложению. Если соответствующий файл клавиатуры не может быть найден, аналогичный файл клавиатуры можно выбрать и отредактировать. Если XKEYBOARD расширение включено в 'Настройках Расширенных Параметров' 'Профиля Сервера', пользовательские настройки клавиатуры не будут применяться.

Для Добавления Файла Клавиатуры в Список Клавиатур:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Клавиатуры]. Будет показано диалоговое окно **Настройки Клавиатуры**.
5. Нажмите [Добавить]. Будет показано диалоговое окно **Добавить Клавиатуру**.
6. Выберите файл клавиатуры.
7. Нажмите [OK].

Чтобы Сделать Указанную Клавиатуру как Клавиатуру По Умолчанию:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Клавиатуры]. Будет показано диалоговое окно **Настройки Клавиатуры**.
5. Выберите клавиатуру, которую хотите сделать клавиатурой по умолчанию в [Списке Клавиатур].
6. Нажмите [Установить По умолчанию].
7. Нажмите [OK].

Для Изменения Файла Клавиатуры в Реальном Времени:

1. Нажмите Ctrl+Alt+K при запущенном **Xmanager**. Будет показано диалоговое окно **Выбор Клавиатуры**.
2. Нажмите клавишу 'K' несколько раз при нажатых Ctrl+Alt для выбора клавиатуры.
3. Отпустите все клавиши.

Замечание

Пользователи могут видеть только файлы клавиатуры в диалоговом окне **Настройка Клавиатуры** [Список Клавиатур].

Для Редактирования Файла Клавиатуры:

1. Запустите **Xconfig**.

2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Клавиатуры]. Будет показано диалоговое окно **Настройки Клавиатуры**.
5. Выберите клавиатуру для редактирования из поля [Список Клавиатур].
6. Нажмите [Правка]. Откроется **Редактор Клавиатур**.
7. Кликните дважды на клавишу, которую хотите изменить в клавиатурной раскладке. Будет показано диалоговое окно **Редактировать Клавишу**.

 Замечание

В диалоговом окне **Редактировать Клавишу**, измените статус клавиши и keySYM.

Repeat генерирует повтор той же клавиши, если пользователь нажал клавишу. Эта функция используется в большинстве клавиш, за исключением вспомогательных клавиш, таких как Shift, Alt и Ctrl.

Latch генерирует событие Нажатия Клавиши или Отпускания Клавиши, когда клавиша нажата и потом отпущена. Клавиша должна быть нажата и отпущена дважды для генерации событий Нажатия Клавиши и Отпускания Клавиши. В основном, эта функция используется для клавиш CapsLock или NumLock.

В поле [KeySYM], Normal, Shift, ModeSwitch, и Shift ModeSwitch keySYMs устанавливаются для клавиши.

Normal используется, когда нажимается клавиша и не нажата никакая другая вспомогательная клавиша.

Shift используется, когда клавиша нажимается одновременно с нажатой клавишей Shift.

ModeSwitch используется, когда клавиша нажимается одновременно с нажатой клавишей ModeSwitch.

Shift ModeSwitch используется, когда нажимается клавиша, и одновременно нажимаются Shift и ModeSwitch клавиши.

Для Создания Нового Файла Клавиатуры:

1. Откройте Редактор Клавиатуры.
2. Выберите [Новый] из меню [Файл]. Будет показано диалоговое окно **Выбрать Тип Клавиатуры**.
3. Выберите необходимый тип клавиатуры и нажмите [ОК].

 Замечание

В диалоговом окне **Выбрать Тип Клавиатуры**, список [Тип Клавиатуры] покажет все типы клавиатур, доступных для использования в Xmanager. Каждая клавиатура имеет

различные раскладки и количество клавиш. Необходимо выбрать тип клавиатуры, аналогичный используемому.

4. Отредактируйте клавиатуру в выбранной раскладке.

Настройки Мыши

Xmanager поддерживает 3-кнопочную эмуляцию: прокрутку с помощью колеса мыши и изменение средней и правой кнопок мыши.

Для Использования 2-х Кнопочной мыши как 3-х Кнопочную:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Мыши]. Будет показано диалоговое окно **Настройки Мыши**.
5. Выберите [Одновременное нажатие правой и левой кнопок].
6. Выберите временной интервал между правой и левой кнопками в поле [Скорость Нажатия].
7. Нажмите [OK].

■ Замечание

В режиме эмуляции 3-х кнопок, мышь работает так, как будто нажата средняя кнопка, при одновременном нажатии правой и левой кнопок. Скорость нажатия, это время ожидания между нажатием одной из кнопок и затем нажатием следующей.

Для Прокрутки в X Приложениях с Использованием Колеса Мыши:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Мыши]. Будет показано диалоговое окно **Настройки Мыши**.
5. Выберите [Использовать Колесо Мыши].
6. Нажмите [OK].

■ Замечание

Для прокрутки с помощью колеса мыши, событие 4-й кнопки генерируется при прокрутке вверх и 5-й кнопки при прокрутке вниз. Нажатие правой кнопки может быть недоступно в некоторых X приложениях, таких как рабочий стол CDE.

Для Изменения Позиций Правой и Средней Кнопок:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Мыши]. Будет показано диалоговое окно **Настройки Мыши**.
5. Выберите [Использовать Правую Кнопку как Среднюю].

6. Нажмите [OK].

 Замечание

Выберите этот параметр, если средняя кнопка используется более часто, чем правая.

Для Использования Цветного Указателя Мыши:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Мыши]. Будет показано диалоговое окно **Настройки Мыши**.
5. Выберите [Использовать Цвет в Указателе Мыши].
6. Нажмите [OK].

Настройки Звука

В диалоговом окне **Настройки Звука**, выберите типы звонка и назначьте звуковые файлы. В диалоговом окне **Свойства Профиля**, откройте диалоговое окно, нажав на кнопку [Настройки Звука] во вкладке [Устройства].

Тип Звонка

Выберите нужное аудио устройство для звонков, запрашиваемых X приложением. Выберите один из трёх типов звонка: *Звуковая Карта*, *Динамик ПК*, и *Ничего*.

Если выбрана *Звуковая Карта*, необходимо назначить соответствующий звуковой файл (.wav). Если выбрано *Ничего*, звуковых сигналов не будет.

Звуковой Файл

Показывает звуковые файлы (.wav) которые будут использованы для звуковых запросов X приложений.

Просмотр

Выберите звуковой файл в диалоговом окне **Просмотр**.

Несколько Мониторов

Xmanager позволяет пользователям выбрать монитор для вывода рабочего стола X Window на много-мониторных системах. **Xmanager** может работать некорректно, если на одном мониторе 8-битные цвета и на другом больше чем 8-бит. Всегда рекомендуется, чтобы каждый монитор использовал не меньше, чем 16-битные цвета или больше.

Для Выбора Монитора для Рабочего Стола X:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].

4. Нажмите [Настройки Монитора]. Будет показано диалоговое окно **Настройки Монитора**.
5. Выберите монитор из списка [Использовать Монитор].
6. Нажмите [ОК].

 Замечание

Список мониторов показывает все мониторы, доступные для использования, включая *Авто-Обнаружение* и *Виртуальный Экран*.

Виртуальный Экран, это виртуальная прямоугольная область, которая включает все мониторы.

При выборе *Авто-обнаружения*, Xmanager выбирает *Виртуальный Экран* в Многооконном Режиме и основной монитор в Режиме Одного Окна.

Для Использования Всех Мониторов как Один Рабочий Стол X:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Монитора]. Будет показано диалоговое окно **Настройки Монитора**.
5. Выберите *Виртуальный Экран* из списка [Использовать Монитор].

 Замечание

Виртуальный Экран показывается только, если в системе несколько мониторов. *Виртуальный Экран* создает главный размер окна и рабочее пространство, которые зависят от разрешения и расположения мониторов. Главное окно, это наибольшая прямоугольная область, состоящая из нескольких мониторов.

6. Нажмите [ОК].

Для Показа Окна Выбора Монитора при Запуске:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Устройства].
4. Нажмите [Настройки Монитора]. Будет показано диалоговое окно **Настройки Монитора**.
5. Выберите [Показать Окно Выбора Монитора при Запуске].
6. Нажмите [ОК].

Настройки Дополнительных Параметров

Установите расширение X протокола и других расширенных параметров во вкладке [Расширенные] диалогового окна **Свойства Профиля**. Для использования параметра копирования и вставки, смотрите 'Копирование, Сохранение и Печать в X Приложении'.

Копирование и Вставка Автоматически

Когда эта опция включена, **Xmanager** копирует и вставляет тексты или изображения между приложением X и приложением Windows. Когда приложение X копирует тексты или изображения, содержимое немедленно передается в буфер обмена Windows. И наоборот, когда новое содержимое добавляется в буфер обмена Windows, содержимое немедленно пересылается в X Selection. Тексты и изображения могут быть скопированы в оба, либо в Буфер Обмена, либо в X Selection. Выбор может потребоваться в зависимости от приложения X.

X Selection

Используйте X Selection при копировании и вставке содержимого между Windows и приложением X.

Cut Buffer

Используйте X Selection при копировании и вставке содержимого между Windows и приложением X.

Копирование и Вставка при Изменении Фокуса

Запускайте копирование и вставку только при изменении фокуса между **Xmanager** и другим приложением Windows. Когда фокус находится в **Xmanager**, содержимое может быть скопировано несколько раз из X-приложений. Затем содержимое вставляется в буфер обмена Windows, когда фокус ввода изменяется на другую программу Windows. При использовании этой опции **Xmanager** в терминале Windows, копирование и вставка могут работать неправильно.

Предупреждение об изменении Дисплея

Показывать диалоговое окно при изменении цвета или разрешения рабочего стола Windows. Если цвет или разрешение изменяется, **Xmanager** должен быть перезапущен.

Увеличение Производительности

Xmanager выполняется с максимальной производительностью. Xmanager выбирает самый быстрый метод для сложных операций рисования.

Однако некоторые графические изображения могут отображаться неправильно в зависимости от видеоустройства или приложений пользователя.

Разрешать Старые Ошибки X11

Выберите этот параметр, если удаленное приложение X создано в версии более ранней, чем X11R6, и, следовательно, не работает успешно в Xmanager.

Принимать Esound Запросы

Этот параметр позволяет принимать удалённые запросы Esound. Esound использует порт TCP 16001.

Подробные Сообщения Журнала

Используйте этот параметр для включения подробных сообщений журнала, если это необходимо для технической поддержки.

Backing Store

Выберите подходящий режим Backing Store.

Backing Store это функция для сохранения скрытых оконных областей в памяти. Когда окно скрыто за другим окном, оно должно быть перерисовано при его вызове. Сохраняя скрытую область в памяти, **Xmanager** может восстановить область быстрее, чем приложение может нарисовать ее снова.

Используя этот метод, **Xmanager** уменьшает объем передаваемых по сети данных в медленных сетевых средах. **Xmanager** поддерживает четыре Backing Store режима.

В режиме *Не Использовать*, функция Backing Store выключена и скрытые поля будут всегда перерисовываться.

При Запросе не использует функцию Backing Store. Однако по запросу X-приложения Xmanager ограниченно использует функцию Backing Store для окон X-приложения. В режиме *При Наложении*, функция Backing Store работает во всех окнах исключая скрытые или свернутые окна.

В режиме *Всегда*, функция Backing Store работает во всех окнах, включая скрытые или свернутые. Этот параметр требует большое количество системной памяти и графических ресурсов.

X Расширения

Выберите X расширения для использования.

Xmanager поддерживает BIG-REQUEST, DAMAGE, DEC-XTRAP, DOUBLE-BUFFER, Extended-VisualInformation, MIT-SUNDRY-NONSTANDARD, Multi-Buffering, RandR, RECORD, RENDER, SECURITY, SHAPE, SYNC, TOG-CUP, XC-APPGROUP, XC-MISC, XEVIE, XFIXES, Xinerama, XInput, XKeyboard, и XTEST расширения протоколов. В частности, он поддерживает протокол расширения Render и улучшенную графическую среду для приложений X.

База Данных X Ресурсов

Показать путь к базе данных X ресурсов для чтения при старте **Xmanager**.

Изменить

Показать диалоговое окно **Открыть** для изменения базы данных ресурсов на другой файл.

Просмотр

Просмотр содержимого базы данных ресурсов в Блокноте.

Безопасность

Xmanager поддерживает безопасные соединения, предоставляя контроль доступа хостам и протоколы SSH. Контроль доступа хостам предотвращает соединения от неавторизованных хостов. Однако, сетевые пакеты между **Xmanager** и приложением X не кодируются и уязвимы для вторжений.

Xmanager также поддерживает SSH протокол для безопасности. SSH соединения могут применяться в обоих Xstart и Безопасных XDMCP сессиях.

Базы данных ключей хоста и ключей пользователя, создаваемые **Xmanager**, могут быть использованы в **Xshell** и **Xftp** программах. Когда создается публичный ключ, он может быть использован всеми программами, без дополнительной настройки.

Контроль Доступа Хостам

Контроль доступа хостам, управляет списком надёжных хостов и разрешает только X приложения из надёжных для соединения с **Xmanager**. Когда приходит запрос от неавторизованного хоста, **Xmanager** показывает диалоговое окно с вопросом, разрешить ли соединение?

Для Использования Функции Контроля Доступа Хостам:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Безопасность].
4. Выберите [Включить Контроль Доступа].
5. Введите авторизованные хосты в списке [Доверенные Хосты].
6. Нажмите [OK].

Для Показа Сообщения с Предупреждением для Неавторизованных Соединений:

1. Запустите **Xconfig**.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Безопасность].
4. Выберите [Предупреждать о Неавторизованных Соединениях].
5. Нажмите [OK].

Аутентификация Пользователя по Публичному Ключу

Для Открытия Управления Ключами Пользователя:

1. Запустите **Xmanager**.
2. Нажмите [Управления Ключами Пользователя] в меню [Инструменты].

Замечание

Пользователь может экспортировать, импортировать, переименовывать, удалять, и создавать ключи пользователя в 'Диалоговом Окне Ключей Пользователя'.

Для Создания Ключа Пользователя:

1. Запустите **Xmanager**.
2. Выберите [Создание Нового Ключа Пользователя] из меню [Инструменты].
3. Создайте ключ пользователя согласно выводимых инструкций в процессе создания Нового Ключа Пользователя.

■ Замечание

Зарегистрируйте публичный ключ на сервере на последнем этапе создания ключа. Методы регистрации немного отличаются в зависимости от типа ключа.

- *SSH1*: Скопируйте текст публичного ключа и сохраните его в `$HOME/.ssh/authorized_keys` файле. Выполните следующую команду для выключения прав на запись в файлы и папки.

```
$ cd  
$ chmod go-w . .ssh .ssh/authorized_keys
```
- *SSH2-OpenSSH*: OpenSSH сервера используют этот формат. Скопируйте текст публичного ключа и сохраните его в `$HOME/.ssh/authorized_keys2` файле. Выполните следующую команду для выключения прав на запись в файлы и папки.

```
$ cd  
$ chmod go-w . .ssh .ssh/authorized_keys2
```
- *SSH2-IETF SECSH*: Некоторые коммерческие SSH сервера, такие как `ssh.com` сервер, используют этот формат. Сохраните публичный ключ под внутренним именем, таким как `mypublickey.pub` и скопируйте его в `$HOME/.ssh2` папку. Добавьте следующую строку в `$HOME/.ssh2/authorization` файл:
Key mypublickey.pub
Выполните следующую команду для выключения прав на запись в файлы и папки.

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

Для Регистрации Публичного Ключа на Сервере:

1. Откройте диалоговое окно **Ключи Пользователя**.
2. Выберите ключ пользователя для регистрации.
3. Нажмите [Свойства]. Будет показано диалоговое окно **Свойства Ключа Пользователя**.
4. Нажмите на вкладку [Публичный Ключ].
5. Выберите тип, который соответствует удалённому SSH серверу из списка [Формат Публичного Ключа].
6. Сохраните публичный ключ, выбрав [Сохранить как файл] или скопируйте содержимое ключа и зарегистрируйте ключ на сервере, используя один из методов регистрации публичного ключа выше.

Для Изменения Парольной Фразы Ключа Пользователя:

1. Откройте диалоговое окно **Ключи Пользователя**.
2. Выберите ключ пользователя, для которого необходимо изменить парольную фразу.
3. Выберите [Свойства]. Будет показано диалоговое окно **Свойства Ключа Пользователя**.

4. Нажмите на вкладку [Основное].
5. Выберите [Изменить Парольную Фразу].

Диалоговое Окно Ключей Пользователя

Диалоговое окно **Ключей Пользователя** позволяет пользователям создавать и управлять ключами пользователя. Откройте это диалоговое окно, выбрав [Управление Ключами Пользователя] из меню [Инструменты].

Импорт

Выберите файл ключа пользователя и импортируйте его, открыв диалоговое окно **Открыть**. В данный момент, **Xmanager** может читать RSA ключи протокола SSH1, RSA/DSA/ECDSA/ED25519 key протокола OpenSSH SSH2, ключи SSH.COM, и форматы пользовательских ключей NetSarang.

Экспорт

Сохраните файл выбранного ключа пользователя, открыв диалоговое окно **Сохранить**. Экспортируемые типы файлов, это пользовательские ключи NetSarang, OpenSSH SSH2. Формат пользовательских ключей NetSarang может использоваться в программах, разработанных NetSarang Computer, Inc.

Удаление

Удаление выбранного ключа пользователя из базы данных.

Переименование

Переименование выбранного ключа пользователя. Название ключа должно быть действительным именем файла.

Свойства

Показывает атрибуты ключа пользователя. Тип, длина, отпечаток, и публичный ключ может быть просмотрен. Дополнительно, можно изменить парольную фразу ключа.

Генерация

Открывает **Создание Нового Ключа Пользователя**.

Диалоговое окно Аутентификации SSH Пользователя

Диалоговое окно **Аутентификации SSH Пользователя** позволяет пользователям выбирать соответствующий метод аутентификации. Если парольная фраза не сохранена в сессии, это диалоговое окно будет показано, в случае необходимости получить информацию об аутентификации от пользователя.

Пароль

Парольная аутентификация используется для разрешения пользователю войти на сервер, введя пароль пользовательского аккаунта. По причине безопасности, некоторые сервера не поддерживают этот метод аутентификации.

Публичный Ключ

Аутентификация по Публичному Ключу, требует, чтобы публичный ключ пользователя был зарегистрирован на SSH сервере. Для входа с использованием этого метода, выберите необходимый ключ пользователя из списка ключей пользователя.

Интерактивный Ввод с Клавиатуры

Интерактивный Ввод с Клавиатуры, работает как запрос пароля с сервера и корректный ответ на него пользователя.

Управление Ключами Хоста

Ключ хоста, это публичный ключ удалённого хоста, с помощью которого пользователи могут проверить хост по его отпечатку. Во время соединения, удалённый хост отправляет свой публичный ключ **Xmanager'y**. Для хостов, которые соединяются в первый раз и ключ хоста не сохранён в базе данных, будет показано диалоговое окно **Предупреждения Безопасности SSH**. Если ключ хоста действительный и безопасный, можно сохранить ключ хоста в базе данных ключей хостов.

Для Открытия Окна Управления Ключами Хоста:

1. Запустите **Xmanager**.
2. Нажмите [Управление Ключами Хоста] в меню [Инструменты].

Диалоговое Окно Предупреждения Безопасности SSH

Диалоговое окно **Предупреждения Безопасности SSH** показывается, когда ключ хоста не сохранён в базе данных ключей хоста, или отпечаток ключа удалённого хоста отличается от сохранённого отпечатка ключа хоста.

Принять На Время Сеанса

Принять ключ хоста только на время этого соединения. Ключ хоста не будет сохранён и такое же диалоговое окно будет открыто при следующем соединении. Эта функция полезна, если ключ хоста часто изменяется или соединение с сервером происходит нечасто.

Принять и Сохранить

Сохранить ключ хоста и продолжить процесс соединения. Диалоговое окно не будет показано при следующем соединении. Эта функция полезна, когда отпечаток правильный и происходит частое соединение с этим хостом.

Отмена

Ключ хоста не принят и соединение отменено.

Диалоговое Окно Ключей Хоста

Диалоговое окно ключей хоста позволяет управлять ключами хостов, соединения с которыми разрешены.

Импорт

Импортировать ключ хоста открыв диалоговое окно **Открыть**. Импортированные ключи хоста будут сохранены в базе данных ключей хоста и будут показаны в диалоговой панели **Ключи Хоста**. Файлы, сохранённые в формате публичных ключей SECSH могут быть импортированы.

Экспорт

Экспорт выбранных ключей хоста с помощью диалогового окна **Сохранить**. Экспортированные ключи сохраняются в формате публичных ключей SECSH и могут быть использованы в других программах.

Удаление

Удаление выбранных ключей хоста из базы данных.

Просмотр

Открыть выбранные ключи хоста в Блокноте.

Мастер Пароль

Мастер Пароль может быть использован для сохранения паролей более безопасно, используя назначенный пользователем мастер пароль. **Xmanager** сохраняет всю информацию о пароле в зашифрованном формате. В то же время, когда пароли шифруются фиксированным ключом, есть риск перехвата его хакерами. Когда мастер пароль включён и установлен, он замешивается в шифрование пароля сессии, добавляя дополнительный уровень безопасности.

Мастер пароль использует назначенное пользователем ключевое слово для шифрования секции пароля в данных сессии. Когда мастер пароль включён, **Xmanager** запрашивает мастер пароль каждый раз при старте нового экземпляра **Xmanager** и открытия сессии. Если корректный мастер пароль не введён, пароль сессии не будет использован и должен быть введён вручную для исключения неавторизованного доступа.

■ Замечание

Убедитесь, что запомнили ваш мастер пароль. Если вы его потеряете, не существует возможности получения информации о паролях, сохранённых в файлах сессии. Настройки Мастер Пароля применяются одновременно к Xmanager, Xshell, и Xftp сессиям.

Для Включения Мастер Пароля:

1. Войдите в меню **Инструменты** и выберите **Установить Мастер Пароль**.
2. В Диалоговом окне **Мастер Пароль**, введите новый мастер пароль в поле **Новый Пароль**.
3. В поле **Подтверждение Пароля**, введите пароль еще раз.
4. Нажмите **ОК** для сохранения изменений.

Как только мастер пароль будет включён, все сессии, сохранённые в месторасположении по умолчанию, будут перешифрованы с использованием нового мастер пароля.

Для Изменения Мастер Пароля:

1. Войдите в меню **Инструменты** в **Xmanager** и затем выберите **Установить Мастер Пароль**.
2. В области Изменения нажмите **Изменить**, для открытия диалогового окна Изменения Мастер Пароля.

3. Введите текущий пароль в поле **Текущий Пароль**.
4. Введите новый мастер пароль в поле **Новый Пароль**.
5. Введите новый мастер пароль еще раз в поле **Подтверждение Пароля**.
6. Нажмите **ОК** для сохранения изменений.

Для Выключения Мастер Пароля:

1. Войдите в меню **Инструменты** в **Xmanager** и затем выберите **Установить Мастер Пароль**.
2. Нажмите кнопку **Удалить**, для открытия диалогового окна Удаления Мастер Пароля.
3. В диалоговом окне Удаления Мастер Пароля, введите мастер пароль и нажмите **ОК**

Для Сброса Мастер Пароля

1. Войдите в меню **Инструменты** и выберите **Установить Мастер Пароль**.
2. Нажмите кнопку **Сброс** в диалоговом окне Мастер Пароль.
3. В диалоговом окне Сброс Мастер Пароля, нажмите **Сброс Мастер Пароля** и нажмите **ОК**.

 Замечание

Сброс мастер пароля можно использовать в случае, если вы забыли свой мастер пароль или вы хотите очистить все пароли, запомненные в файлах сессий.

Управление Вкладками

Xmanager предоставляет мощную возможность управления вкладками. Пользователи могут соединяться с множеством хостов и сравнивать их рядом в одном окне. Эта система вкладок является уникальной возможностью Xmanager, которую не найти в других PC X Серверах.

Каждая вкладка сопоставляется с одним экземпляром Xmanager и принадлежит группе вкладок. В группе вкладок находится набор вкладок. Один экземпляр окна Xmanager может иметь несколько групп вкладок, которые могут быть организованы в любом порядке.

Вкладка

Сессии с вкладками в Xmanager выполняются в соответствии с параметрами, как если бы 'Режим Окна' был бы установлен в Режим Одного Окна.

Для Открытия Сессии в Новой Вкладке

1. Нажмите [Инструменты] из меню Файл
2. В качестве Действия По Умолчанию, выберите **Открыть Во Вкладке**.
3. Нажмите дважды на сессию в Xmanager.

Замечание

Вы можете вручную открыть сессию в новом окне, щелкнув правой кнопкой мыши по сессии и выбрав параметр **Открыть в Новом Окне**. То, что вы выбираете в контекстном меню, переопределит настройку действия для открытия по умолчанию.

Для Закрытия Вкладки

4. Нажмите кнопку **x** на вкладке.

Группа Вкладок

Группа вкладок, это набор из нескольких вкладок. В данный момент видна только одна вкладка из группы вкладок. Вы можете управлять несколькими группами вкладок в одном окне **Xmanager**, позволяя сравнивать различные вкладки бок о бок без переключения между приложениями.

Для Создания Новой Группы Вкладок

1. Откройте новую сессию, нажав правой кнопкой на сессию и затем выбрав **Открыть в Новой Вкладке**.
2. Нажмите на вкладку и перенесите ее на край окна **Xmanager**. Это создаст зону для размещения вкладки, которая покажет, как будет создана новая группа вкладок.
3. Отпустите вкладку в углу, где вы хотите создать новую группу вкладок.

Для Переноса Вкладки в Другую Группу Вкладок

1. Выберите вкладку, где вы хотите перенести в новую группу вкладок.
2. Пока нажимаете левую кнопку мыши, перенесите вкладку в другую группу вкладок

3. Отпустите вкладку в новую группу вкладок.

Для Закрытия Группы Вкладок

1. Выберите группу вкладок, которую хотите закрыть.
2. Нажмите правой кнопкой мыши на группу вкладок в фоне.
3. Выберите параметр **Закрыть Эту Группу Вкладок**.

Для Расположения Всех Вкладок Вертикально

1. Пока открыто несколько вкладок, нажмите правой кнопкой на вкладку.
2. Укажите на **Расположение** и затем выберите **Расположить Вертикально**.

Для Расположения Всех Вкладок Горизонтально

1. Пока открыто несколько вкладок, нажмите правой кнопкой на вкладку.
2. Укажите на **Расположение** и затем выберите **Расположить Горизонтально**.

Для Расположения Всех Вкладок Плиткой

1. Пока открыто несколько вкладок, нажмите правой кнопкой на вкладку.
2. Укажите на **Расположение** и затем выберите **Расположить Плиткой**.

Для Объединения Всех Групп Вкладок

1. Если в одном окне отображается несколько групп вкладок, нажмите правой кнопкой на вкладку.
2. Укажите на **Расположение** и затем выберите **Объединить Все Вкладки**.

Копирование, Сохранение, и Печать в X Приложениях

Автоматически копируйте строки символов между приложением X и буфером обмена Windows с помощью **Xmanager**. Кроме того, при использовании локального менеджера окон, изображения приложений X могут быть скопированы в буфер обмена Windows, сохранены в виде растровых файлов и распечатаны на принтере.

Для Установки Автоматического Копирования и Вставки:

1. Запустите Xconfig.
2. Кликните дважды на профиль. Будет показано диалоговое окно **Свойства Профиля**.
3. Нажмите на вкладку [Расширенное].
4. Выберите [Копировать и Вставлять Автоматически] из списка [Настройки].
5. Нажмите [OK].

Для Копирования Строки Символов из Xterm в Блокнот Windows:

1. Выберите строку символов, которую хотите скопировать из окна xterm, левой кнопкой мыши.
2. Запустите Блокнот.
3. Выберите [Вставить] из меню [Правка].

Для Копирования Строки Символов из Блокнота Windows в Xterm:

1. Выберите строку символов, которую хотите скопировать из Блокнота левой кнопкой мыши.
2. Выберите [Копировать] из меню [Правка].
3. Запустите **xterm**.
4. Нажмите среднюю кнопку мыши или левую и правую одновременно в окне **xterm**.

Для Копирования Окна X Приложения в Буфер Обмена:

1. Укажите на [Копировать] в строке заголовка системного меню и выберите [Окно] или [Содержимое]. Снимок окна будет скопирован в буфер обмена.

Замечание

Эту функцию можно использовать, когда локальный оконный менеджер работает в Многооконном Режиме.

Для Сохранения Окна X приложения как Растровый Файл:

1. Укажите на [Сохранить] в строке заголовка системного меню и выберите [Окно] или [Содержимое]. Будет показано диалоговое окно **Сохранить Как**.
2. Введите требуемое имя файла в [Имя Файла].
3. Нажмите [OK].

Замечание

Эту функцию можно использовать, когда локальный оконный менеджер работает в Многооконном Режиме

Для Печати Окна X Приложения:

1. Укажите на [Печать] в строке заголовка системного меню и нажмите [Окно] или [Содержимое]. Будет показано диалоговое окно **Печать**.
2. Нажмите [Печать].

 Замечание

Эту функцию можно использовать, когда локальный оконный менеджер работает в Многооконном Режиме

Журнал Сессии

Сессии **Xmanager** записывают отладочную информацию в файлы. Когда несколько сессий **Xmanager** используются одновременно, каждый журнал сессии сохраняется под своим именем таким как X0.LOG и X1.LOG. Номер в файле журнала указывает на номер дисплея сессии **Xmanager**.

Проверка файлов журнала поможет в случае возникновения проблем при использовании **Xmanager**.

Для Просмотра Файла Журнала Текущей Сессии:

1. Нажмите правой кнопкой на иконку **Xmanager** в области уведомлений, или нажмите на иконку **Xmanager** в строке заголовка главного окна **Xmanager**.
2. Укажите на [Журнал] в системном меню и выберите [Файл]. Файл журнала откроется в Блокноте.

Замечание

В Многооконном Режиме, иконка Xmanager создастся в области уведомлений. В Режиме Одного Окна, Xmanager откроет одно основное окно.

Для Открытия Папки, где Сохраняются все Файлы Журналов Сессий:

1. Нажмите правой кнопкой на иконку **Xmanager** в области уведомлений, или нажмите на иконку **Xmanager** в строке заголовка главного окна **Xmanager**.
2. Укажите на [Журнал] в системном меню и выберите [Папка]. Откроется папка журнала.

Замечание

Откройте папку журнала, выбрав [Открыть Папку Журнала] из меню [Файл] **Xmanager**.

Индекс

- Backing Store, 63
- Kerberos, 40
- LOCAL, 25
- MAC, 28
- PseudoColor, 56
- REXEC, 25
- RLOGIN, 25
- RSH, 25
- SSH, 25
- TELNET, 25
- Xagent, 30
- Xconfig, 5
- XDMCP, 10
- Xmanager, 5
- Xstart, 5
- ZLIB сжатие, 28
- Автоматический XDMCP, 17
- Адрес Соединения, 24
- Адресная Строка Xmanager, 36
- База Данных RGB, 56
- Безопасное XDMCP соединение, 37
- Выполнение Команды, 26
- Зарегистрированная Команда, 26
- Импорт, 34
- Исходный Хост, 29
- Локальный адрес, 23
- Межсетевой экран, 42
- Метод, 23
- Настройка Безопасного XDMCP, 27
- Настройка Столбцов, 33
- Несколько Мониторов, 60
- Номер Дисплея, 22
- Номер Порта, 23, 24
- Обмен Ключами, 28
- Пароль, 27
- Парольная аутентификация, 66
- Парольная Фраза, 28
- Пассивная Сессия, 20
- Печать, 73
- Поделиться Сессиями, 21
- Протокол, 25
- Публичный Ключ, 66
- Путь к Сессиям, 32
- Слушающий Порт, 29
- Соединение, 35
- Статический XDMCP, 17
- Тип IP Адреса, 24
- Тэги команд, 41
- Управление Цветом, 55
- Установка GSSAPI, 41
- Установка PKCS#11, 41
- Хост, 23
- Хост Назначения, 29
- Шифрование, 28, 31
- Экспорт Сессий, 33